Citrix Receiver for Linux 13.2

Dec 18, 2015

This pdf file includes the Citrix Receiver for Linux 13.2 documentation. You can save a local copy of this file and use it offline. Use the built-in Search and Bookmark features to find what you need.

About Receiver for Linux 13.2.x

Jun 05, 2015

Citrix Receiver for Linux is a software client that lets you access your desktops, applications, and data easily and securely from many types of Linux devices. Working with a Citrix-enabled IT infrastructure, Receiver gives you the mobility, convenience, and freedom you need to get your work done.

Receiver for Linux 13.2.1

What's new in this release

- This release provides a security fix by upgrading OpenSSL to version 1.0.1n.
- Additional RPM installation packages.

Fixed issues in this release

- Russian time zone information can be updated in Receiver for Linux. [LC1971] 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.
  - You must install Microsoft hotfix KB2998527 for Windows and then update the time zone data for Linux.
- When setting any local city, Receiver for Linux might return incorrect information about the city. For example, Receiver for Linux returns information on "America/Bahia_Banderas" when looking information on "America/Bahia. [LC2980]
- When users receive a new Lotus Notes email, the message window might take focus from the keyboard input window in Receiver for Linux. [LC3059]
- When using the "-span" parameter to show a desktop session in full-screen mode, if the span covers more than two monitors, the desktop session appears on a single monitor only. [LC3122]

Known issues in this release

- Flash redirection is not available on 64 bit clients. If this capability is important in your environment please contact the Citrix Product Management team or alternately use the support forums for additional guidance. [0582627]
- The ARMEL browser plugin (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 plugin, which allows a fallback mechanism to take over. [0580782]
- 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). [0585295]
- When running on SLED 11sp3, launching storebrowse or selfservice from a terminal may 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. [0582512]
- 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. [0586967]

- 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 following command: **gst-inspect-0.10 -- gst-disable-registry-fork --version**. After executing this command you should be able to re-run the tarball setup without experiencing a system hang. [0587640]
- In some Gnome desktop environments, a client may experience a crash when launching 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.") [0587922]
- 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. [0588009]
- Windows Media Player on a Windows 7 desktop may fail to play audio/video when launched 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 the Troubleshooting topic. [0588298]

Windows Media Player fails to play files in certain formats

Receiver for Linux 13.2

What's new in this release

- When used in conjunction with the centralized customization and branding capabilities of the StoreFront 3.0, users of this Receiver for Linux release will receive a centrally managed app and desktop selection experience from StoreFront. This is the same consistent user experience that can be received by the Windows and Mac desktop Receivers and HTML5 and Chrome web Receivers when associated with the StoreFront 3.0 release.
- Full 64-bit packages
- Russian language support

Fixed issues in this release

Known issues in this release

- 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 [#403729]:

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

- If Receiver for Linux gives a segmentation fault when accessing smart cards, this may 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 -I

  If this also gives a segmentation fault, you should contact the supplier of the driver. You could 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]

- When working with XenDesktop in full screen mode in Receiver for Linux, the local screensaver may not activate. This is a

third-party issue, and the behavior may vary depending on the client operating system. [#496398]

- 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 may 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]

- On some low performance devices in a full screen session, the logon process with smart card authentication may take longer than expected and a timeout occurs. You may 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. It does not apply to armhf. [#498037]

- If you insert the wrong smart card when trying to connect to a StoreFront store, you may see an error message such as "protocol error" or "Specified store not found", which does not explain the issue. [#496904]

- 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. [#0558649]
  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 be tested against all possible OS environments.

- 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. [#0559817]
- When using Linux Receiver X1 to remove an app, the app persists and when logging out and returning to the store. [#0561719]

  The Linux Receiver XI user interface introduced at this release offers server level control of subscribed apps and desktops in the form of mandatory apps through StoreFront; apps are automatically subscribed for the user by the server (referred to mandatory apps). Users can add and remove additional apps, but not the mandatory apps provided by StoreFront.
- List store output has changed with the addition of a store friendly name. The following command lines list stores [#0567833]:

  . /util/storebrowse -l

  ./util/storebrowse --liststores

  The output of both options is identical. For example:

  'https://my.examplestore.net/Citrix/Store/discovery' 'Store' 'Store'
  '149397992' '"My Default GW",https://my.defaultgateway.com'
  '"Alternative Gateway",https://
  my.alternativegateway.com,"Alternative Gateway
  2",my.alternativegateway2.com'
  'https://my.secondexamplestore.net/Citrix/Second/discovery'
  'Second' '401460086' '"Alternative Gateway",https://
  my.alternativegateway.com' '"My Default GW",https://
  my.defaultgateway.com,"Alternative Gateway
  2",my.alternativegateway2.com'
  storebrowse lists stores in the following format, where \t is a Tab character.
  '<store URL>'\t'<Store Name>'\t'<Store Friendly Name>'\t'<Unique Store ID>'\t'"<Current
  Gateway Name>",<Current Gateway URL>'\t'"<Alternative Gateway
  1 Unique Name>",<Alternative Gateway 1 URL>, ... "<Alternative
  Gateway n Name>",<Alternative Gateway n URL>'

System requirements

May 12, 2015

This topic describes the system and user requirements for installing Citrix Receiver for Linux.

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 20 MB of free disk space for the installed version of Receiver and at least 40 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.

The version of the Adobe Flash plug-in running on the user device must be either the same as or later than the version running on the XenApp or XenDesktop server to support client-side rendering. If this is not the case, only server-side rendering is available.

Citrix recommends always upgrading to the latest version of the plug-in to obtain the latest functionality and security-related fixes.

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.

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 sufficent for HDX MediaStream Windows Media Redirection.

Note: You can download GStreamer from http://gstreamer.freedesktop.org. Use of certain codecs may require a license from the manufacturer of that technology. You should consult with your corporate legal department to determine if the codecs you plan to use require additional licenses.

Phillips SpeechMike

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

Smart card support

To configure smart card support in 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 PNAgent), or with the "legacy PNAgent" site that can be provided by a StoreFront server.

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. To ensure Receiver for Linux locates the 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 the 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 behaviour 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.

Availability of Receiver for Linux 13.2 Technology Preview features

In order for your users to experience the Citrix Receiver Technology Preview features, they must connect to stores hosted on StoreFront 3.0 Technology Preview servers.

Some of the features and functionality of Receiver are available only when connecting to newer versions of XenApp and XenDesktop and may also require the latest hotfixes for those products.

Citrix Servers

- XenApp (any of the following products):
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5, Feature Pack 2, for Windows Server 2008 R2
  - Citrix XenApp 6.5, Feature Pack 1, for Windows Server 2008 R2

- Citrix XenApp 6.5 for Windows Server 2008 R2
- Citrix XenApp 6 for Windows Server 2008 R2
- Citrix XenApp 5 for Windows Server 2008
- Citrix XenApp 4, feature pack 2, for Unix operating systems

- XenDesktop (any of the following products):
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
  - XenDesktop 5.6, Feature Pack 1
  - XenDesktop 5.6
  - XenDesktop 5.5
  - XenDesktop 5
- Citrix VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
- You can use Citrix Receiver for Linux 13.3 browser-based access in conjunction with StoreFront Receiver for Web and Web Interface, with - or without - the NetScaler Gateway plug-in.
  StoreFront:

  - StoreFront 3.0.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 in conjunction with the NetScaler VPN client:

  - Web Interface 5.4 for Windows web sites.
    Provides access to virtual desktops and apps from a Web browser.

  - Web Interface 5.4 for 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 in conjunction with StoreFront.
  - Offer to install from Citrix Receiver for Web site (configured with StoreFront).
  - Offer to install Receiver from Citrix Web Interface 5.4.
  - Deploy using Active Directory (AD) Group Policy Objects (GPOs).
  - Deploy using Microsoft System Center 2012 Configuration Manager.

Browser

- Internet Explorer
  Connections to Receiver for Web or to Web Interface support the 32-bit mode of Internet Explorer. For the Internet Explorer versions supported, see StoreFront system requirements and Web Interface system requirements.

- Mozilla Firefox 18.x (minimum supported version)
- Google Chrome 21 or 20 (requires StoreFront).

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 information about domain-joined and non-domain-joined devices, refer to the XenDesktop 7 documentation.

- For secure remote or local connections:
  - Citrix NetScaler Gateway 10.5
  - Citrix NetScaler Gateway 10.1
  - Citrix Access Gateway Enterprise Edition 10
  - Citrix Access Gateway Enterprise Edition 9.x
  - Citrix Access Gateway VPX

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

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

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

About secure connections and certificates

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

Private (self-signed) certificates

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

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

Installing root certificates on user devices

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

Wildcard certificates

Wildcard certificates are used in place of individual server certificates for any server within the same domain. 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.

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 in order 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 sh hdxcheck.sh to run the script.

Install and set up

Oct 07, 2015

The following packages are available for 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. 2.1.328635_amd64.deb	Self-service support, 64-bit x86_64
icaclient_13. 2.1.328635_i386.deb	Self-service support, 32-bit x86
icaclient_13. 2.1.328635_armhf.deb	Self-service support, ARM HF
icaclient_13. 2.1.328635_armel.deb	Self-service support, ARM EL
icaclientWeb_13.2.1.328635_amd64.deb	Web Receiver only, 64-bit x86_64
icaclientWeb_13. 2.1.328635_i386.deb	Web Receiver only, 32-bit x86
icaclientWeb_13. 2.1.328635_armhf.deb	Web Receiver only, ARM HF
icaclientWeb_13. 2.1.328635_armel.deb	Web Receiver only, ARM EL
ctxusb_2.5.328635_amd64.deb	USB package, 64-bit x86_64
ctxusb_2.5.328635_i386.deb	USB package, 32- bit x86
ctxusb_2.5. 328635_armhf.deb	USB package, ARM HF
ctxusb_2.5.328635_armel.deb	USB package, ARM EL
Redhat packages (Redhat, SUSE, Fedora etc.)	
ICAClient-rhel-13.2.1.328635-0.x86_64.rpm	Self-service support, RedHat (including Linux VDA) based, 64-bit x86_64

ICAClient-rhel-13.2.1.328635-0.i386.rpm	Self-service support, RedHat based, 32-bit x86
ICAClient-suse-13.2.1.328635-0.x86_64.rpm	Self-service support, SUSE based, 64-bit x86_64
ICAClient-suse-13.2.1.328635-0.i386.rpm	Self-service support, SUSE based, 32-bit x86
ICAClient-suse11sp3-13.2.1.328635-0.x86_64.rpm	Self-service support, SUSE 11 sp3 (including Linux VDA) based, 64-bit x86_64
ICAClient-suse11sp3-13.2.1.328635-0.i386.rpm	Self-service support, SUSE 11 sp3 based, 32-bit x86
ICAClientWeb-rhel-13.2.1.328635-0.x86_64.rpm	Web Receiver only, RedHat based, 64-bit x86_64
ICAClientWeb-rhel-13.2.1.328635-0.i386.rpm	Web Receiver only, RedHat based, 32-bit x86
ICAClientWeb-suse-13.2.1.328635-0.x86_64.rpm	Web Receiver only, SUSE based, 64-bit x86_64
ICAClientWeb-suse-13.2.1.328635-0.i386.rpm	Web Receiver only, SUSE based, 32-bit x86
ctxusb-2.5.328635-1.x86_64.rpm	USB package, 64-bit x86_64
ctxusb-2.5.328635-1.i386.rpm	USB package, 32-bit x86
Tarballs (Script install for any distribution)	
linuxx64-13.2.1.328635.tar.gz	64-bit Intel
linuxx86-13.2.1.328635.tar.gz	32-bit Intel
linuxarm-13.2.1.328635.tar.gz	ARM EL
linuxarmhf-13.2.1.328635.tar.gz	ARM HF

The difference between packages that offer support for Web Receiver and those 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 only require Web Receiver support, or your distribution doesn't have the necessary packages to support self-service then install the Web Receiver only package.

Note: If your distribution allows, install Receiver from the Debian package or RPM package. These files are generally easier to use because they automatically install any required packages. If you want to control the installation location, install Receiver from the tarball package.

To install Receiver for Linux from a Debian package

If you are installing Receiver from the Debian package on Ubuntu, you may 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 windows.

3. Run the installation for the following 3 packages by typing **dpkg -i packagename.deb**. For example:

- dpkg -i icaclient_13.2.1.328635 _amd64.deb
- dpkg -i icaclientWeb_13.2.1.328635_amd64.db
- dpkg -i ctxusb_2.5.328635_amd64.deb

4. Install andy missing dependencies by typing sudo **apt-get -f install**.
5. Accept the EULA license.

To install Receiver for Linux from an RPM package

If you are installing 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 get 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.) you should 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 setup 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.3

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 3 packages by typing zypper in packagename.rpm.

3. Open a terminal window.

    For SUSE installations:

    zypper in ICAClient-suse-13.2.1.328635-0.x86_64.rpm

    zypper in ICAClient-suse-11sp3-13.2.1.328635-0.i386.rpm

    zypper in ctxusb-2.5.328635-1.x86_64.rpm

    For Red Hat installations:

    yum localinstall ICAClient-rhel-13.2.1.328635-0.i386.rpm

    yum localinstall ICAClientWeb-rhel-13.2.1.328635-0.i386.rpm

    yum localhost ctxusb-2.5.328365.rpm

4. Accept the EULA.

To install Receiver for Linux from a tarball package
Note: The tarball package does not perform dependency checking or installation of dependencies. All system dependencies will need to be resolved separately.

1. Open a terminal window.
2. Uncompress 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.

Note: To ensure the integration performs well when Receiver is installed in a non-default location, set the location in $ICAROOT in $HOME/.profile or $HOME/.bash_profile

8. If you have previously installed GStreamer, you can choose whether to integrate GStreamer with Receiver and so provide support for HDX Mediastream Multimedia Acceleration. To integrate Receiver with GStreamer, type y at the prompt.

9. f you are logged on as a privileged user (root), then you can 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 Receiver for Linux installation

Feb 10, 2015

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

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

To customize a Receiver for Linux installation

1. Expand the 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 Receiver package. For example, you might add a new 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 new TLS root certificate to the package, see
   — Install root certificates on user devices
   in Citrix eDocs. For more information about built-in certificates, see
   — Configure and enable SSL and TLS
   in Citrix eDocs.
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 may 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
   - Sub-package (which should 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 Receiver for Linux

Jul 15, 2013

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

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

To start 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 Receiver).

To start Receiver from the Linux desktop

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

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

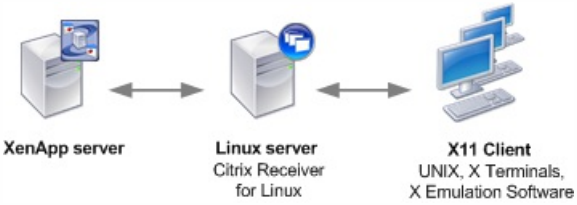
Use Receiver for Linux as an ICA-to-X proxy

Sep 24, 2014

You can use a workstation running Receiver as a server and redirect the output to another X11-capable device. You may want to do this to deliver Microsoft Windows applications to X terminals or to UNIX workstations for which Receiver is not available. Note that the Receiver software is available for many X devices, and installing the software on these devices is the preferred solution in these cases. Running the Receiver in this way, as an ICA-to-X proxy, is also referred to as server-side ICA.

When you run 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. This means that you can run multiple copies of Receiver simultaneously on one system with each sending its output to a different device.

This graphic shows a system with 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 Receiver on the Linux server that usually supplies the X applications to the X terminals
- If you want to deploy UNIX workstations for which 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:

- Audio will not be 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 need to access the UNIX printer from the server manually using LPD printing, or use a network printer.

To start 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 Receiver is installed. At a command prompt, type selfservice &

To uninstall Citrix Receiver for Linux

Sep 18, 2014

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

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 the Citrix Receiver for Linux you must be logged in as the same user who performed installation.

Connect

Sep 22, 2014

Receiver 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 Receiver UI

The Receiver 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 the same name is used for multiple stores on the StoreFront server, the Accounts page will make the stores appear identical. To avoid confusing users this way, administrators should use unique store names when configuring the store. For PNAgent, the store URL is displayed and uniquely identifies the store.
After connecting to a store, users can search for desktops and applications or browse them by clicking + (the plus sign) on the Receiver home page. Clicking a desktop or application icon copies the resource to the home page, from where users can start it with another click. A connection is created when they do so.

Configure connection settings

You can configure a number of default settings for connections between Receiver and XenApp and XenDesktop servers. You can also change those settings for individual connections, if required.

The rest of this section of eDocs contains procedures that support typical tasks performed by users of Receiver. Although the tasks and responsibilities of administrators and users can overlap, the term “user” is employed in this section of eDocs 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 Receiver using configuration files

Connect to resources from a command line or browser

Sep 18, 2014

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 the store is available on the server. 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 may need to change the server location or SOCKS proxy details. See Connect through a proxy server for details.

To create a connection from a web browser

If you are configuring Mozilla, Netscape, or Chrome, connection configuration is normally carried out automatically during installation.

If you need to 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, you need to modify the browser configuration accordingly.

1. For the .mailcap file modification, in $HOME, create or modify the .mailcap file and add the line:
   application/x-ica; /opt/Citrix/ICAClient/wfica.sh %s; x-mozilla-flags=plugin:Citrix ICA

2. For the MIME file modification, in $HOME, create or modify the .mime.types file and add the line:
   application/x-ica ica

   The x- in front of the format ica indicates that ica is an unofficial MIME type not supported by the Internet Assigned Numbers Authority (IANA).

Troubleshoot connections to resources

Sep 18, 2014

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 ends the session and closes any open applications.
- Disconnecting from a session. This 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 Receiver 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 Receiver using configuration files

Aug 16, 2013

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 different files depending on the effect you want the changes to have.

Be aware that, 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 changes to all Receiver users

If you want the changes to apply to all 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 default value, the value in module.ini is not used.

Apply changes to new Receiver users

If you want the changes to apply to all future new Receiver users, modify the configuration files in the $ICAROOT/config directory. For changes to apply to all connections, update wfclient.ini in this directory.

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. 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. If you want changes to apply to all Receiver users, modify module.ini.

For any given connection, the files are generally 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 they are not set by a server.

Configure Citrix XenApp (formerly PNAgent) connections using Web Interface

Jul 15, 2013

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: config.xml 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 Receiver. For the system to recognize the file type of the published content and for users to view it through Receiver, a published application must be associated with the file type of the published file. For example, to view a published Adobe PDF file using Receiver, an application such as Adobe PDF Viewer must be published. Unless a suitable application is published, users cannot view the published content.

Optimize

Aug 16, 2013

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

- Mapping user devices
- Configuring USB support
- Improving performance over low-bandwidth connections
- Improving multimedia performance
- Optimizing the performance of screen tiles

Mapping user devices

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 users home directory or /tmp, as well as 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 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. For information on this, see Set preferences.

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

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

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

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 might create slower logon times in some environments. In this situation, you may wish 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 being those 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 Receiver for Linux supports the Citrix PS Universal Printer Driver. So, in most cases no local configuration is required for users to print to network printers or printers that are attached locally to user devices. You may, however, need to 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 Receiver, start a server connection and log on to a computer running XenApp.
2. On the Start menu, click Settings > Printers.
3. On the File menu, click Add Printer.

   The Add Printer wizard appears.
4. Use the wizard to add a network printer from the Client Network, Client domain. In most cases, this will be a standard printer name, similar to those created by native Remote Desktop Services, such as "HP LaserJet 4 from clientname 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 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 eDocs.

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. Note that XenApp does not support USB redirection of mass storage devices and requires special configuration to support audio devices. Refer to 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, although in most cases 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 may have a network interface card attached to the system board by internal USB. Remoting this would not be appropriate. The following types of USB device are not supported by default for use in a XenDesktop session:

- Bluetooth dongles
- Integrated network interface cards
- USB hubs

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

To allow the remoting of USB devices to virtual desktops, enable the USB policy rule. For more information, see the 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 the mass storage device is redirected to the virtual desktop, the user must remove and re-insert 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 may 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, Configure 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 may also appear as mass storage devices and it may be possible to configure a camera to use either class, through setup menus provided by the camera itself.

Note that if a camera appears as a mass storage device, client drive mapping is used and USB support is not required.

Printers (Class 07)

In general most printers are included in this class, although some use vendor-specific protocols (class ff). Multi-function printers may have an internal hub or be composite devices. In both cases the printing element generally uses the Printers class and the scanning or fax element uses another class; for example, Still Imaging.

Printers normally work appropriately without USB support.

Mass Storage (Class 08)

The most common mass storage devices are USB flash drives; others include USB-attached hard drives, CD/DVD drives, and SD/MMC card readers. There are a wide variety of devices having internal storage which also present a mass storage interface; these include media players, digital cameras, and mobile phones. Known subclasses include:

- 01 Limited flash devices
- 02 Typically CD/DVD devices (ATAPI/MMC-2)
- 03 Typically tape devices (QIC-157)
- 04 Typically floppy disk drives (UFI)
- 05 Typically floppy disk drives (SFF-8070i)
- 06 Most mass storage devices use this variant of SCSI

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

Important: Some viruses are known to propagate actively using all types of mass storage. 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 may 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 may be providing the connection to the virtual desktop itself.

Human Interface Devices (Class 03)

Includes a wide variety of both input and output devices. Typical Human Interface Devices (HIDs) are keyboards, mice, pointing devices, graphic tablets, sensors, game controllers, buttons, and control functions.

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

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

USB Hubs (Class 09)

USB Hubs allow extra devices to be connected to the local computer. It is not necessary to access these devices remotely.

Smart card (Class 0b)

Smart card readers include contactless and contact smart card readers, and also USB tokens with an embedded smart card equivalent chip.

Smart card readers are accessed using smart card remoting and do not require USB support.

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 may be providing critical network access, or connecting critical peripherals such as Bluetooth keyboards or mice.

The default USB policy does not allow these devices. However, there may be particular devices it is appropriate to provide access to using USB support.

Updating the list of USB devices available for remoting

You can update the range of USB devices available for remoting to desktops by editing the list of default rules contained in the usb.conf file located 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 will be offered to the server. The rules on the server will then control which of these will 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 new policy rules, refer to 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

Tag	Description
SubClass	SubClass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, be aware of the following:

- Rules are case-insensitive.
- Rules may 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.

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 make a number of changes to 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 additional 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 Services 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 to 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		
		High	Medium	Low
	High	High	Medium	Low

Audio quality on server	Medium	Medium	Medium	Low
	Low	Low	Low	Low

If UDP audio is enabled but the resultant quality is not medium, audio transmission will use TCP not UDP.

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 may 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 may take a long time.
- **Avoid playing multimedia content**. Playing multimedia content uses a lot of 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

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 additional 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 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 Receiver.
   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 will play on the device. You can verify that a plugin is installed and operational using the gst-launch utility. If gst-launch can play the URL, the required plugin is operational. For example, run `gst-launch-0.10 playbin2 uri=http://example-source/file.wmv` and check the video plays correctly.
3. When installing Receiver on the device, select the GStreamer option.

Note the following 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 should specify a standard URL that does not reference these file types. Use gst-launch to verify that a given URL is valid.

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

   - **HDXFlashEnableServerSideContentFetching=Disabled | 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 megabytes (MB). This can be any size between 25 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**.

- **HDXFlashServerSideContentCacheType=Persistent | 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. To let Receiver sessions handle keyboard and mouse input inside and outside of any windows that play Flash content, in /config/module.ini change FlashV2=Off to FlashV2=On.

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, or Microsoft Office Communicator.

1. Ensure your user device meets the feature requirements.
2. Ensure 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 may 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.

Improving the user experience

Jan 31, 2011

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

- Setting preferences
- Configuring ClearType font smoothing
- Configuring special folder redirection
- Setting up server-client content redirection
- Controlling keyboard behavior
- Using xcapture
- Reconnecting users automatically
- Ensure session reliability

Setting preferences

You can set preferences by clicking Preferences on the Receiver 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 a new account to Receiver 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 Receiver.

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 a new 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).

1. On the General page of the Preferences dialog box, select a mode in Display desktop in.

To reconnect sessions automatically

Receiver can reconnect to desktops and applications that you become disconnected from (for example, if there is a network infrastructure issue).

1. 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.

1. 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.

1. 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 Sub-pixel 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 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 is defined by the FontSmoothingTypePref setting.
1	No smoothing
2	Standard smoothing
3	ClearType (horizontal sub-pixel) smoothing

Both standard smoothing and ClearType smoothing increase Receiver's bandwidth requirements significantly.

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	
2	Standard smoothing
3	ClearType (horizontal sub-pixel) 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. This is particularly important if, for example, a mobile user needs to log 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

This is a two-part procedure. 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.
   - You must 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.
- You must 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 Receiver 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 Receiver provided that the path includes RealPlayer and at least one of Firefox, Mozilla, or Netscape.

Note: RealPlayer for Linux can be obtained from http://proforma.real.com/real/player/unix/unix.html.

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 Receiver

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 will create 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 Receiver 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 Receiver).

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 you use this in conjunction 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, Receiver 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. Receiver 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, Receiver 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 will take precedence if there is a connection problem. Session reliability attempts to re-establish a connection to the existing session. It may take up to 25 seconds to detect a connection problem, and then takes a configurable period of time (the default is 180 seconds) to attempt the re-connection. 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.

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. Receiver users cannot override the server settings. For more information on these, see your XenApp and XenDesktop documentation.

Secure

Feb 16, 2015

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 need to 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 required.

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 Receiver and the server. No configuration of Receiver is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

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

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

The FQDN must list, in sequence, the following three components:
- Host name
- Intermediate domain
- Top-level domain

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

Connecting 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, or, if the user selects SSL/TLS+HTTPS browsing, to the Citrix XML Service.

If you configure SSL Relay to listen on a port other than 443, you must specify the non-standard listening port number to 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 are the default values, which are implemented in code. Adjust them as you require.

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

Note: This version of Receiver for Linux disables the use of the SSLv3 protocol.

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, 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
GeoTrust_Global_CA.pem	GeoTrust

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.

Important: Receiver does not support keys of more than 4096 bits. You must ensure that the Certificate Authority root and intermediate certificates, and your server certificates, are less than or equal to 4096 bits long.
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 need to 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):
   1. Copy the file to $ICAROOT/keystore/cacerts.
   2. Run the following command:
      `$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 need to install intermediate certificates to support smart card users, follow these steps before adding a StoreFront store.

1. Obtain the intermediate certificate(s) 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):
   1. Copy the file(s) to $ICAROOT/keystore/intcerts.
   2. Run the following command as the user who installed the package:
      $ICAROOT/util/ctx_rehash

Enabling smart card support

Receiver for Linux provides support for a number of 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.
- You must install the appropriate driver for your smart card.
- You must install the PC/SC Lite package.
- You must 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, you must 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 XenDesktop and XenApp 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>. Note that 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 will likely 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.

Troubleshoot

May 28, 2013

This article contains information to help administrators troubleshoot issues with Receiver for Linux.

Connection issues

You may encounter the following connection issues.

Windows Media Player fails to play files in certain formats

Receiver may 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 one is present. This should be detected and cause 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 Receiver, and as a result, the server will either request another format or render 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 selfservice 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 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 may need to configure the server with a Client Access License (CAL). For

more information about licensing, see Licensing Your Product.

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 will try to use the original color depth. Otherwise, the server will try to start a new session with the requested color depth, leaving the original session in a disconnected state. However, the second connection may 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, but note that 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 may be a problem with random number generation in the Linux kernel. To work around this, run an entropy-generating daemon such as rngd (which is hardware-based) or haveged (from Magic Software).

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>
```

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 a number of 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 grahics, create a file in the xorg.conf.d called **20-intel.conf** with the following contents:

```
Section "Device"
        Identifier    "Intel Graphics"
        Driver        "intel"
        Option        "AccelMethod" "sna"
        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 eample:

```
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). You will need to install the "ComprizConfig Settings Manager."

  Run "ComprizConfig Settings Manager"
  Under "General->Composition", uncheck "Undirect Fullscreen Windows"
  Note: "ComprizConfig 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
  ```

To provide full icon compatibilityIncorrect 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 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 is a known limitation when using the X Windows System with PseudoColor 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 rapidly 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.

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 will have 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 will not be visible to the window manager, will not have an icon and can not 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 will use the _NET_WM_FULLSCREEN_MONITORS message to request an appropriate window layout from the window manager, if it is supported. Otherwise, it will use 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: You must 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"
```

Note that this change affects both XenApp and XenDesktop sessions.

If you have already started selfservice or storebrowse you must 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

This occurs because 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.

To work around this, 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 may 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 may also encounter the following additional 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, add *PrintLogThreshold* with the value 6 to the [WFClient] section. The default valuefor *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 needs to access a serial port, the application may 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; in the case of UUCP-style locks, there may 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 and the error message “Application default file could not be found or is out of date” appears, this may be because 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 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 Downloading and installing

Receiver for Linux.

If Receiver was previously installed in the default location, remove the /opt/Citrix/ICAClient or $HOME/ICAClient/platform directory before reinstalling.

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 find the Citrix 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

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 a 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.

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 new 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 may 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 new 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 new 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.

Command-line parameters

Mar 03, 2015

The tables below list Receiver for Linux command-line parameters.

Note: A list of the parameters can be obtained typing **wfica** or **storebrowse** with the **-?**, **-help**, or **-h** options.

wfica

You can use a connection file simply by typing its name after **wfica** without any of the following options.

To	Type
Specify the custom connection to use from the Connection file. Note: With the new self-service UI, you cannot set up a custom connection in this way.	-desc description -description description
Specify a desktop file used for launch.	-desktop filename
Specify a connection file.	-file connection filename
Set alternative protocol file. This enables the use of an alternative module.ini.	-protocolfile filename
Set alternative client configuration file. This enables the use of an alternative wfclient.ini.	-clientfile filename
Display a different name for Receiver, specified by name, wherever that name appears. The default name is the device name. However, if you use a Sunray device, the default name is derived from the device's MAC address. This is overridden by the ClientName entry in .ICAClient/wfclient.ini, which is itself overridden by issuing the -clientname name command.	-clientname name
Show this list of parameters.	-help
Display version information.	-version
Show error numbers and string.	-errno
Set the location of Receiver installation files. This is equivalent to setting the ICAROOT environment variable.	-icaroot directory
Suppress connection dialog boxes.	-quiet

To	Type
Log connection process.	-log
Enable key logging.	-keylog
Set session geometry.	-geometry WxH+X+Y
Set color depth.	-depth <4 | 8 | 16 | 24 | auto>
Set monitor spanning.	-span [h][o] [a | mon1[,mon2[,mon3,mon4]]]
Use private colormap.	-private
Use shared colormap.	-shared
Specify a string to be added to a published application.	-param string
Specify the UNIX path to be accessed through client drive mapping by a published application.	-fileparam unixpath
Specify a user name.	-username username
Specify a disguised password.	-password password
Specify a clear text password.	-clearpassword "clear password"
Specify a domain.	-domain domain
Specify an initial program.	-program program
Specify a directory for the initial program to use.	-directory directory
Turn on sound.	-sound
Turn off sound.	-nosound
Set drive mapping overrides. These are of the form A$=path, where path can contain an environment variable (for example A$=$HOME/tmp). This option must be repeated	-drivemap string

To	Type
for each drive to be overridden. For the override to work, there must be an existing mapping, although it need not be enabled.	

Tip: All wfica command line options can also be specified in the environment variable WFICA_OPTS, allowing them to be used with the Receiver native UI or with Citrix StoreFront.

storebrowse

The following table documents the options that you can use with the storebrowse utility.

Option	Description	Notes
-L, --launch	Specifies the name of the published resource to which you want to connect. This launches a connection to a published resource. The utility then terminates, leaving a successfully connected session.	
-E, --enumerate	Enumerates the available resources.	By default, the resource name, display name, and folder of the resource are displayed. Additional information can be displayed, by using the --details option.
-S, --subscribed	Lists the subscribed resources.	By default, the resource name, display name, and folder of the resource are displayed. Additional information can be displayed using the --details option.
-M, --details Use in conjunction with the -E or -S option.	Selects which attributes of published applications are returned. This option takes an argument that is the sum of the numbers corresponding to the required details: Publisher(0x1), VideoType(0x2), SoundType(0x4), AppInStartMenu(0x8), AppOnDesktop(0x10), AppIsDesktop(0x20), AppIsDisabled(0x40), WindowType(0x80), WindowScale(0x100), DisplayName(0x200), and AppIsMandatory(0x10000). CreateShortcuts(0x100000) can be used in conjunction with -S, -s, and -u to create menu entries for subscribed applications. RemoveShortcuts(0x200000) can be used with -S to delete all menu entries.	Some of these details are not available through storebrowse. If this is the case, the output is 0. Values can also be expressed in decimal as well as hexadecimal (for example, 512 for 0x200).
-v, --version	Writes the version number of storebrowse to the standard output.	
-?, -h, --help	Lists the usage for storebrowse.	An abbreviated version of this table appears.

Option	Description	Notes
-U, --username	Passes the user name to the server.	These options are deprecated and may be removed in future releases. They work with Program Neighborhood Agent sites but are ignored by StoreFront sites. Citrix recommends that you do not use these options and instead let the system prompt users for their credentials.
-P, --password	Passes the password to the server.	
-D, --domain	Passes the domain to the server.	
-r, --icaroot	Specifies the root directory of the Receiver for Linux installation.	If not specified, the value is determined at run time.
-i, --icons Use in conjunction with the -E, or -S option.	Fetches desktop or application icons, in PNG format, of the size and depth given by the best or size argument. If the best argument is used, the best sized icon available on the server is fetched. You can convert this to any size required. The best argument is the most efficient for storage and bandwidth, and can simplify scripting. If the size argument is used, an icon is fetched of the specified size and depth. In both cases, icons are saved in a file for each of the resources that the –E or -S option returns.	The best argument creates an icon of the form <resource name>.png. The size argument is of the form WxB, where W is the width of the icon (all icons are square, so only one value is needed to specify the size), and B is the color depth (that is, the number of bits per pixel). W is required but B is optional. If it is not specified, icons of all available image depths are fetched for that size. The files that are created are named <resource name>_WxWxB.png.
-u, --unsubscribe	Unsubscribes the specified resource from the given store.	
-s, --subscribe	Subscribes the specified resource from the given store.	If you use a different Receiver, subscriptions on Program Neighborhood Agent servers are lost.
-W [r|R], --reconnect [r|R]	Reconnects disconnected and active sessions.	r reconnects all disconnected sessions for the user. R reconnects all active and disconnected sessions.
-WD, --disconnect	Disconnects all sessions.	Only affects sessions to the store specified on the command line.
-WT, --logoff	Logs off all sessions.	Only affects sessions to the store specified on the command line.
-l, --liststores	Lists the known StoreFront stores, that is those that storebrowse can contact. These are the stores registered with the ServiceRecord proxy. Also lists Program Neighborhood sites.	

Option	Description	Notes
-a, --addstore	Registers a new store, including its gateway and beacon details, with the Service Record daemon.	Returns the full URL of the store. If this fails, an error is reported.
-g, --storegateway	Sets the default gateway for a store that is already registered with the Service Record daemon.	This command takes the following form: `./util/storebrowse --storegateway "<unique gateway name>" '<store URL>'` Important: The unique gateway name must be in the list of gateways for the specified store.
-d, --deletestore	Deregisters a store with the Service Record daemon.	
-c, --configselfservice	Gets and sets the self-service UI settings that are stored in StoreCache.ctx. Takes an argument of the form `<entry[=value]>`. If only entry is present, the setting's current value is printed. If a value is present, it is used to configure the setting.	Example: `storebrowse --configselfservice SharedUserMode=True` Important: Both entry and value are case sensitive. Commands that use this option will fail if the case is different to the documented case of the setting itself (in StoreCache.ctx).
-C, --addCR	Reads the provided Citrix Receiver (CR) file, and prompts the user to add each store.	The output is the same as -a but might contain more than one store, separated by newlines.
-K, --killdaemon	Terminates the storebrowse daemon process.	All credentials and tokens are purged.

pnabrowse

Important: The pnabrowse utility is deprecated but can still query Program Neighborhood Agent sites that run the Web Interface for lists of servers and published resources, and lets you connect to a published resource. Citrix discourages the use of pnabrowse with StoreFront stores; use storebrowse instead. storebrowse can prompt for credentials from sites and stores. The -U, -P and -D options only work with Program Neighborhood Agent sites.
An optional argument of pnabrowse specifies the server to connect to. This may be either:

- The name of the XenApp server, for options -S and -A.
- The URL of the server running Web Interface, for options -E and -L.

The pnabrowse utility returns an exit value indicating success or failure, and can use the following options with XenApp:

Option	Description
-S	List servers, one per line.
-A	List published applications, one per line.

Option	Description
-m	Used in conjunction with -A, this expands the information returned about published applications to include Publisher,Video Type, Sound Type, AppInStartMenu, AppOnDesktop, AppIsDesktop, AppIsDisabled, Window Type, WindowScale, and Display Name.
-M	Used in conjunction with -A, this selects individual columns of information returned about published applications. It takes a argument (1-1023) which is the sum of the numbers corresponding to the required details: Publisher(1), Video Type(2), Sound Type(4), AppInStartMenu(8), AppOnDesktop(16), AppIsDesktop(32), AppIsDisabled(64), Window Type(128), Window Scale(256), and DisplayName(512).
-c	When appended to option -A, create files specifying the minimum information the client engine needs to connect to published applications; for example, application name, browse server, window resolution, color depth, audio, and encryption settings. File names are formatted as follows: /tmp/xxx_1.ica, /tmp/xxx_2.ica where xxx is replaced by the decimal process identifier for the pnabrowse process.
-d	Used in conjunction with -L to specify the XDG desktop file.
-e	Shows error numbers.
-i	Include paths to files containing icon images for published applications in the output from option -A. Either .xpm or .png files are returned depending on the use of the size (WxB) option: • -i returns 16x16 icons in XPM format at 4 bits per pixel • -iWxB returns WxW icons in PNG format at B bits per pixel
-f	Include Citrix XenApp folder names for published applications in the output from option -A.
-u	Specify a user name for authenticating the user to a proxy server.
-p	Specify a password for authenticating the user to a proxy server.

The following options provide Citrix XenApp (Program Neighborhood Agent) Services functionality and can be used with both XenApp and XenDesktop functionality:

Option	Description
-D	Specify a domain for authenticating the user to the server running the Web Interface or the server running the Citrix XenApp (Program Neighborhood Agent) Service.
-E	Invoke Citrix XenApp and enumerate all published resources. If you specify both -E and -L, the last option on the command line takes effect. The utility then terminates, possibly leaving a connection open. For each resource the following details are written to standard output, enclosed in single quotation marks

Option	Description
	and separated by tab characters: Name: The display name from the Access Management Console Application Properties dialog box. Folder: The Program Neighborhood folder from the Access Management Console Application Properties dialog box. Type: Either Application or Content. Icon: The full path name of an .xpm format icon file.
-L	Specify the name of the published resource to which you want to connect. This invokes Citrix XenApp and launches a connection to a published resource. If you specify both -E and-L, the last option on the command line takes effect. The utility then terminates, possibly leaving a connection open.
-N	Specify a new password. This option must be used with existing credentials and is valid only when the existing password has expired, as indicated by the exit code 238: E_PASSWORD_EXPIRED.
-P	Specify a password for authenticating the user to the server running the Web Interface or the server running the Citrix XenApp (Program Neighborhood Agent) Service.
-U	Specify a user name for authenticating the user to the server running the Web Interface or the server running the Citrix XenApp (Program Neighborhood Agent) Service.
-WD	Disconnects all active sessions for the user.
-WT	Terminates all sessions for the user.
-Wr	Reconnects to all disconnected sessions for the user.
-WR	Reconnects to all sessions (active or disconnected) for the user.
-k	Use an existing Kerberos ticket to authenticate, rather than user name, password, and domain. This requires configuration of the client and server. For more information, see the *— Using Kerberos with Citrix Receiver for Linux Guide* . This is available from Citrix under a non-disclosure agreement.

The following common options are used:

Option	Description
-q	Quiet mode; do not print error messages.
-r	Include raw icon data for published applications in the output from options -E or -A.

Option	Description
-V	Displays version details.
-h	Print a usage message listing the options.
-?	Print a usage message listing the options.