Receiver for Linux 12.1

2015-03-08 04:25:10 UTC

Contents

Receiver for Linux 12.1

About this Release

Citrix Receiver for Linux provides users with access to resources published on XenApp or XenDesktop servers. It combines ease of deployment and use, and offers quick, secure access to applications, content, and virtual desktops. Users can connect to resources published on XenApp servers using either individual ICA connections or, if using Citrix XenApp, predefined ICA connection configurations from servers running the Web Interface. Users can also connect to virtual desktops provided by XenDesktop, enabling them to use those virtual desktops as if they were connecting to a local Windows desktop.

What's new

- **HDX MediaStream Flash Redirection**. HDX MediaStream Flash Redirection has been enhanced to provide:
  - Support for both ARM and x86 32-bit thin clients.
  - Support for both Debian and openSUSE 32-bit distributions. Previously, support was available only for Ubuntu and Fedora 32-bit distributions.
  - Support for Internet Explorer 9.

    Note: Only 32-bit versions of Internet Explorer are supported server-side.
  - Support for KDE desktops.
  - Fallback to server-side rendering when Flash is using either the Real Time Messaging Protocol (RTMP) or Real Time Media Flow Protocol (RTMFP). Note that server-side content fetching must be enabled to allow fallback to server-side rendering.
  - Keyboard and mouse handling both inside and outside of windows playing Flash content within a session.

  Note: HDX MediaStream Flash Redirection is supported only when connecting to XenDesktop 5.5 or XenApp 6.5.
- **HDX MediaStream Windows Media Redirection enhancements**. HDX MediaStream Windows Media Redirection has been enhanced to provide:
  - **Support for end-to-end flow control and frame dropping capability**. This improves the user experience when the bandwidth available for viewing a Windows media video (WMV, MPEG, AVI, DivX, etc.) is less than what is required by the bit rate of the video, an issue increasingly experienced by customers as videos are recorded at higher resolution.

    Note: This feature is supported only when connecting to XenDesktop 5.5.
  - **Improved support for existing audio and video codecs**. Various enhancements improve the user experience, providing smoother playback of audio and video clips in the following formats:
    - AC3, MPEG AAC, and AMR audio formats
    - WMV-VC1, Intel Indeo 5, MS CRAN, NV11, H.264, and H.263 video formats
  - **Configurable text-based translation table**. Receiver includes a configurable text-based translation table, MediaStreamingConfig.tbl, for translating Windows-specific media format GUIDs into MIME types Gstreamer can use.

Known Issues

- Japanese characters are not displayed correctly in Receiver's user interface when running on Fedora 14. This problem occurs because Japanese X fonts are not installed on Fedora 14, by default. As a workaround, you can install Japanese X JIS fonts manually. [#0035091]

- Users logging off from Receiver may see a large number of error messages in syslog when running on Ubuntu 10.10. This is caused by a known issue with the PulseAudio sound server and is specific to Ubuntu 10.10. There is no workaround for this issue. It does not, however, affect a users ability to connect to and use hosted applications and desktops. [#0252173]

- HDX Mediastream Flash Redirection does not work when running on Ubuntu 11.04 if a user is logged on as root. As a workaround, users should not log on as root if they want to use HDX Mediastream Flash Redirection when running Receiver on Ubuntu 11.04. [#0140460]

- When a user launches Internet Explorer in seamless mode, windows playing Flash content are displayed with some dislocation. [BUG0283200]

- Users may experience issues when playing video content on the YouTube Web site. Video content may freeze during playback. [#0285173]

- Adobe Flash Player may exit unexpectedly when playing video content if version 11.2 of the Adobe Flash plug-in is installed on the user device. As a workaround, install version 11.1 of the plug-in on the user device. [#0300029]

- Uses may experience the following issues with the Flash context menu:

  - The context menu is not displayed in full-screen sessions. [#0287965]

  - The About Citrix HDX MediaStream for Flash... option is not displayed. [#0283188]

  - Users cannot change settings in the Settings dialog box, accessed from the context menu. [#0300275]
- Occasionally the Flash hosting process crashes with an X error. If this occurs, the URL for the Web site running Flash content may be added to the Dynamic Blacklist. As a workaround:

  1. Click Cancel if an X error-related error dialog appears to continue working in the session.

  2. Check whether or not the Web site’s URL has been added to the Dynamic Blacklist. If it has, edit the Registry, removing the URL from the following location:

     - For Internet Explorer 7, 8, or 9 in non-protected mode: HKEY_CURRENT_USER\Software\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\DynamicBlacklist

     - For Internet Explorer 8 or 9 in protected mode: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\InternetRegistry\REGISTRY\USER\User-specific SID Path\Software\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\DynamicBlacklist

  Note that if you click Quit in the X error-related dialog box, the session is disconnected. [#0286195]

- Windows playing Flash content remain open for some time after closing Internet Explorer 9 when connecting to Web sites using heavy scripting in latency driven networks. [#0289085]

- Flash content may occasionally appear in windows measuring 200x200 pixels. As a workaround, perform any Internet Explorer action in the window to restore that window to actual size. [#0288781]

- Flash content may occasionally appear as black. As a workaround, perform any Internet Explorer action in the window to restore that window to its original state. [#0288899]

- Flash content is not visible when moving published applications running in seamless windows. [# 0159246]

- Attempting to run Receiver for Linux on openSUSE 12.1 fails with a segmentation fault. As a workaround, start Receiver for Linux with the following environment variables set:

  MALLOC_PERTURB_=0

  MALLOC_CHECK_=0

  [#0276978]

Issues Fixed in This Release

The following issues have been fixed since the previous release of this product:

- URLs and documents specified in the LongCommandLine of an ICA file fail to open in applications when session sharing is configured.

- Setting "EnableOSS" to "Off" in appsrv.ini is not enforced.

- Upgrading USB support from version 11.100 to version 12.x fails on Debian distributions.

- Fixes a loss of audio playback when HDX Flash Acceleration is enabled.

- Users cannot enter keyboard input outside an area displaying flash content when client-side rendering is enabled.

- Users may experience delays when launching Flash-intensive Web sites for the first time.

- Processes running on thin client devices terminate unexpectedly when running Flash-intensive Web sites due to a lack of available memory.

System Requirements

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

Device Requirements

- Linux kernel version 2.6.29 or above, with glibc 2.7 or above, gtk 2.12.0 or above, libcap1 or libcap2, and udev support.
- OpenMotif 2.3.1 or above, if you intend to run the native graphical user interface (wfcmgr).
- LibPCSCLite 1.5.6
- ALSA (libasound2), Speex and Vorbis codec libraries.
- 6 MB of free disk space for the installed version of Receiver and up to 13 MB if you expand the installation package on the disk. You can check the available disk space by typing one of the following commands in a terminal window:

  df -k <ENTER>

  df <ENTER>

  Note: If you are using the Web Interface to deploy Receiver, refer to the Web Interface documentation for more information.
- 256 color video display or higher.
- TCP/IP networking.

HDX 3D Pro Requirements

Requirements for HDX 3D Pro features differ, depending on whether you are using CPU or GPU decoding.

- CPU decoding of both CPU and GPU codecs requires:
  - 2GHz single core machine for use with a single monitor.
  - 2GHz dual core machine for use with dual monitors
- GPU decoding of GPU codecs requires:
  - A Video Acceleration API (VAAPI)-compatible graphics card
  - libva 1.0.1 or later
  - For NVIDIA graphics cards, NVIDIA drivers, version 190 or later
  - Video Decode and Presentation API for UNIX (VDPAU), version 0.2 or later

HDX MediaStream Flash Redirection Requirements

HDX MediaStream Flash Redirection requires:

- libcurl 7.18.2 or later.
- libflashplayer.so (Adobe Flash plug-in) version 10.0 or later.

  Note:

  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 later

HDX MediaStream Windows Media Redirection Requirements

HDX MediaStream Windows Media Redirection requires:

- GStreamer 0.10.15 or later

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 own attorneys to determine if the codecs you plan to use require additional licenses.

Phillips SpeechMike Requirements

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.

Availability of Receiver for Linux 12.1 features

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.

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 the Web Interface through one of the supported browsers or Receiver's native user interface (wfcmgr).

Checking Your Device Meets the System Requirements

Citrix provides a script, hdxcheck.sh, as part of the Receiver installation package that checks whether or not your device meets the system requirements necessary to utilize all the functionality provided by 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.

Installing Receiver for Linux

Receiver for Linux is available in Red Hat Package Manager (RPM) , Debian and .tar.gz formats.

RPM and Debian packages are generally easier to use, because they automatically install any other required packages. However, they give you no control over the location of the installed files.

You can download Receiver for Linux in all of these formats from the support pages of the Citrix Web site (http://www.citrix.com/).

If changing the location of the installation is necessary in your environment, then install Receiver from the .tar.gz file.

To install Receiver for Linux from a RPM package

1. Log on as a privileged (root) user.
2. Open a terminal window.
3. Run the installation by typing rpm -i *packagename*.rpm.

   Note: Run the same command to install both the main Receiver package and the USB support package, replacing *packagename* with the name of the package you are installing.

To install Receiver for Linux from a Debian package

1. Log on as a privileged (root) user.
2. Open a terminal window.
3. Run the installation by typing dpkg -i *packagename*.deb

   Note: Run the same command to install both the main Receiver package and the USB support package, replacing *packagename* with the name of the package you are installing.

To install Receiver for Linux from a .tar.gz file or CD

1. Open a terminal window.
2. Uncompress the .tar.gz file and extract the contents into a temporary directory. For example, for Linux platforms, type: `tar xvfz packagename.tar.gz`
3. Type `./setupwfc` and press ENTER to run the setup program.
4. Type `1` (Install Citrix Receiver for Linux 12.1) and press ENTER.
5. Type the path and name of the required installation directory (and press ENTER) or press ENTER to install 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*

   (where *platform* is a system-generated identifier for the installed operating system. For example, $HOME/ICAClient/linuxx86 for the Linux/x86 platform).

   Note: If you do not accept the default location, you must also specify the installation directory in the environment variable *ICAROOT* after installation.
6. When prompted to proceed, type `y` and press ENTER.
7. Type `1` to accept the Client Software License Agreement and press ENTER. If you have a supported Web browser installed, you are prompted to choose installation of the plug-in. If you require the plug-in, press `y`.
8. If you have KDE or GNOME installed, then you can choose whether to integrate them with Receiver. Type `y` at the prompt to integrate Receiver with KDE or GNOME.
9. 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.
10. If 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), then the following warning is displayed: `USB support cannot be installed by non-root users. Run the installer as root to access this install option.`
11. When the installation is complete, the main installation menu appears again. To exit from the setup program, type `3` and press ENTER.

If you did not accept the default installation directory in step 5, then you must specify the full path and name of the installation directory in the environment variable *ICAROOT*.

Customizing a Receiver for Linux Install

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.

To customize a Receiver for Linux install

1. Expand the Receiver package file into an empty directory. The package file is called *platform-major.minor.build*.tar.gz (for example, linuxx86.12.1.*nnnn*.tar.gz for the Linux/x86 platform).

2. Make the required changes to the Receiver package. For example, you might want to add some connection definitions so that each installation of Receiver already contains a standard set of connections. You can add connection definitions to the appsrv.ini template file located in: *platform*/*platform*.cor/config/appsrv.ini (for example, linuxx86/linuxx86.cor/config/appsrv.ini for the Linux/x86 platform). Alternatively, you might add a new SSL 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. See Configuring and Enabling Receiver for SSL and TLS for more information about built-in certificates. To add a new SSL root certificate to the package, copy the .crt file into *platform*/*platform*.cor/keystore/cacerts (for example linuxx86/linuxx86.cor/keystore/cacerts for the Linux/x86 platform).

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.

Integrating Receiver for Linux with KDE and GNOME

During installation, you can choose to integrate Receiver into the K Desktop Environment (KDE) and the GNU Network Object Model Environment (GNOME). If KDE or GNOME is present, the installation creates a menu option from which users can start Receiver.

The menu entries and desktop shortcuts are created dynamically by Citrix XenApp.

Note: For best operation, set $ICAROOT in $HOME/.profile or $HOME/.bash_profile, unless Receiver is installed in the default location.

Supporting Faster Graphics

Display performance for graphics is improved using ThinImage functionality. For this feature to function correctly, ensure that the user device's installation includes the libjpeg.so JPEG library. This library is present in typical Linux installations, but may be missing in installations for Linux terminals and network boot images.

If libjpeg.so is missing from your system, Citrix recommends that you contact your distributor for a suitable installation package and installation instructions.

Starting Receiver for Linux

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

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/wfcmgr` 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 any desktop environment for Linux by navigating to it using a file manager.

If you are using KDE or GNOME, you can also start Receiver from the menu. Receiver may reside in different menus depending on your Linux distribution. The menu locations for some popular distributions are noted below.

- KDE
  - Red Hat, Fedora, Ubuntu, Kubuntu, Gentoo, Arch, and SuSE distributions: On the K menu, click Applications > Internet > Citrix Receiver
  - Mandriva distributions: On the K menu, click Networking > Citrix Receiver
  - Other distributions: On the K menu, click Applications > Citrix Receiver
- GNOME
  - All distributions: On the Internet menu, click Citrix Receiver

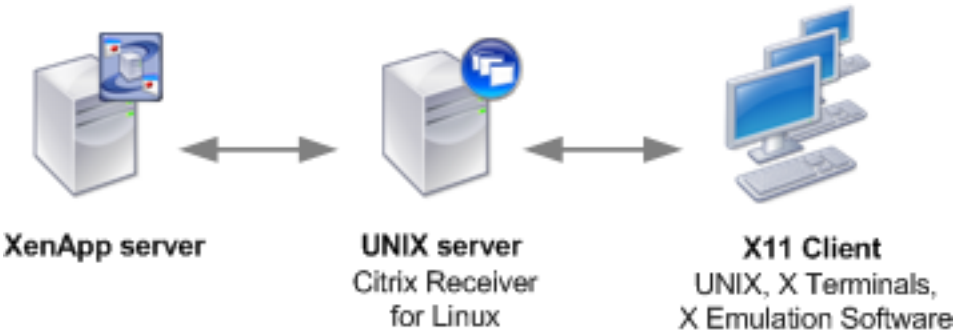
Clicking the Citrix Receiver option on a menu in the KDE or GNOME environment starts Receiver.

Using Receiver for Linux as an "ICA to X Proxy" ("Server Side ICA")

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.

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.

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 DISPLAYenvironment 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 DISPLAYenvironment 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 `wfcmgr &`

Note: If you get font errors on the local X display when you start Receiver, start the font server on the proxy server.

To uninstall the Citrix Receiver for Linux

1. Run the setup program by typing `/usr/lib/ICAClient/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.

Creating Connections

Users can create two types of connections to servers:

- A connection to a *server desktop* lets a user access the desktop of a server. The user can run any applications available on the desktop, in any order.

  Note: Users cannot connect to hosted desktops provided by XenDesktop through a custom connection. Users must connect using either the Web Interface or Citrix XenApp.

- A connection to a *published application* lets a user access a predefined application and its associated environment. The user can run published applications in seamless mode, where each application appears in its own resizable window as if it is running locally.

To create a connection

1. Start Receiver.
2. On the Connections menu, click New.
3. Click Server or Published Application.
4. Do one of the following:
   - For a server desktop, type the name or IP address of the server or click Browse to select from a list of servers.
   - For a published application, type the name of the published application or click Browse to select from a list of published applications.
5. If you type the name of the server or published application, type a unique description for the entry in the Description box. The description is used to identify the connection in the Connection view. If you select a server or published application from the list, a default description is added automatically.
6. Click OK.

   After you create a connection with the appropriate network connection properties set up, the description appears in the Connection view.

   Note: This is the simplest way to create a connection entry. When you follow these steps, you set the essential items you need to connect to the server from the workstation. You can configure other default properties for a connection using the Tools > Setting menu. You can also change the properties for an individual connection, if required.

Viewing Connection Entries

By default, Receiver displays the Connection view, which lists all the connection entries created by a user, including connections to published applications and server desktops. Immediately after installing Receiver, this list may be empty.

If users want to view the connections that are set up automatically to applications and content published on a XenApp Services site, they can do so using the Citrix XenApp view.

To view resources published through Web Interface

On the View menu, click Citrix XenApp View and log on if prompted.

A list of resources on the server appears.

As part of the publication process, only those resources defined for the Receiver user appear.

A folder icon indicates a folder containing other published resources. When navigating resources in a folder, an up arrow icon indicates the parent folder.

For more information about the publication process, see the XenApp or XenApp for UNIX documentation.

To view connections created on the user device

On the View menu, click Connection View.

Opening a Connection

Users can connect to servers in a number of ways:

- From the Connection view
- Using Citrix XenApp (only for connections to published resources):
  - From the Citrix XenApp view
  - From menu items created by Citrix XenApp
  - From desktop items created by Citrix XenApp (often these are located in a folder called "Citrix" or "Citrix App Service Center")
- From a command line
- From a Web browser

To open a connection from the Connection view

1. Select the name of the connection you want to open.
2. Do one of the following:
   - On the Connections menu, click Connect.
   - Click the Connect button on the toolbar.

To open an application from the Citrix XenApp view

1. In the Citrix XenApp view, select the application to which you want to connect.
2. Do one of the following:
   - On the Citrix XenApp menu, click Connect.
   - Click the Connect button on the toolbar.

To open a connection from a command line

At a command prompt, type:

`/opt/Citrix/ICAClient/wfica -desc “`*`description`*`”`

where *description* is the full text from the Description box of the connection entry. If the description contains spaces, enclose it in quotation marks in the standard manner for Linux.

Note: If users cannot connect to a server, administrators may need to change the server location or SOCKS proxy details. See Configuring ICA Browsing and Connecting Through a Proxy Server for details.

To open a connection using a Web browser

If you are using Firefox, Mozilla, or Netscape, Web browser configuration to enable ICA session connection is normally carried out automatically during installation.

If you need to set up .mailcap and MIME files for Firefox, Mozilla, or Netscape 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).

Managing Your Connections

Users can control and investigate connections with the Connection Center. This feature enables users to:

- Close applications
- Log off or disconnect from sessions
- Manage connection windows
- View connection transport statistics for sessions

The Connection Center is a useful productivity tool that enables users and administrators to troubleshoot slow or problematic connections. Users can also use it to minimize and restore their connection windows.

To access the Connection Center

On the Tools menu, click Connection Center.

The active sessions are listed and a summary of all the connections, showing the total number of servers and applications in use, appears at the bottom of the Connection Center dialog box.

To manage a connection window

In the Connection Center, select a session from the list and choose from the following tasks.

To	Click
End the selected session and close any open applications	Logoff
Refresh the list of sessions and remove any closed applications	Refresh
Display the Connection Center Status dialog box, which contains statistics for the selected session	Properties
Cut the selected connection to the server without closing any open applications (unless the server is configured to close applications on disconnection)	Disconnect
Close the selected application	Terminate
Minimize the window used by the selected application or session	Iconify

Display the window used by the selected application or session	Restore

To view information about a session

1. On the Tools menu, click Connection Center.

2. Select a session and click Properties. The Connection Center Status dialog box displays the following information:

Box	Description
Connected to server	Server used for the connection. You can specify the server by clicking Connections > Properties and selecting the Network page.
as user	Account used to log on to server. “Anonxxx” indicates an anonymous connection. You can specify the account by clicking Connections > Properties and selecting the Login page.
Encryption Level	Type of encryption. You can specify the encryption level by clicking Connections > Properties and selecting the Connection page.
Client Version	Client version number.
Bytes	Number of incoming or outgoing bytes transported along the connection.
Frames	Number of incoming or outgoing frames transported along the connection.
Bytes/Frame	Number of bytes divided by number of frames.
Frame errors	Number of incoming or outgoing frames that were incorrectly transported along the connection.

These statistics are available only for sessions, not published applications. However, if the published application is the only connection within a session, the details displayed when you select this session from the Connection Center apply to the published application.

Configuring Connections

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.

Information in this section 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 chapter to distinguish typical user tasks from those typically performed by administrators.

Configuring Default Connection Settings

You can configure settings that apply to all your connections, using Receiver's native user interface (wfcmgr). These settings are also used as defaults for any new connections you create. For example, you may want to customize the default window size if you prefer all new connections to appear in larger or smaller windows than the original setting.

To configure default connection settings

On the Tools menu, click Settings. The Settings dialog box has pages corresponding to the properties you can control including:

- The Preferences page, where you specify the settings for keyboard options, alert sounds, and digital dictation support that apply to all connection entries. See Configuring Default Keyboard, Sound, and Digital Dictation Support Settings.
- The Window page, where you specify the window settings to use for all new connection entries. See To configure default window settings.
- The Server Location page, where you specify the server address for the server that will report the data collector. See Configuring ICA Browsing.
- The Keyboard Shortcuts page, where you define alternative key combinations for system keyboard shortcuts. See To configure keyboard shortcuts.
- The Disk Cache page, where you define settings for the disk cache. See To configure disk cache settings.
- The Drive Mapping page, where you set up drive mappings. See Mapping Client Drives.
- The COM Ports page, where you configure COM port mapping. See To configure client COM port mapping.
- The Firewall page, where you configure firewalls and a SOCKS proxy. See Connecting Through a Proxy Server.
- The Auto Reconnect page, where you specify settings for HDX Broadcast auto-client reconnect. See Reconnecting Users Automatically.
- The Citrix XenApp page, where you identify the server running the XenApp Services site. See Configuring Citrix XenApp.
- The Secure Gateway page, where you can specify a Secure Gateway relay server for Receiver to use when connecting to the server. See Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay.

Configuring Default Keyboard, Sound, and Digital Dictation Support Settings

Use the Preferences page in the Settings dialog box to configure the following default connection settings:

- **Keyboard options**. Sets the default keyboard layout and type.
- **Alert sounds**. Enables or disables the playing of Windows alert sounds on the user device.
- **Digital dictation support**. Enables or disables client-side microphone input.

To configure default keyboard, sound, and digital dictation support settings

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Preferences.
3. Configure the following settings, as required:
   - Keyboard Layout. Click Browse to select your input locale from the list. Input locale is the language in which you want to type. If you select User Profile, the server chooses the input locale.
   - Keyboard Type (Client). Click Browse to select your correct workstation keyboard type from the list.

     Note: If you are using a Sun keyboard, by default the left Meta key acts as a Windows key, and the right Meta key acts as a Menu key. The Meta keys are marked with a diamond.
   - Keyboard Type (Server). Click Browse to select the specific physical keyboard type you are using from the list. If you are using a Japanese keyboard, select it. For all others, use the default (standard 105 key keyboard).
   - Enable Windows Alert Sounds. When enabled, allows Windows alert sounds to be played using the user device sound system.
   - Allow Audio Input. When enabled, provides support for HDX Realtime Multimedia Conferencing and client-side microphone input.

     Note: You must select Allow Audio Input if you want to configure digital dictation support for individual connections. For more information, see To configure digital dictation support.

To configure default window settings

Use the Window page in the Settings dialog box to configure default window settings for all connections.

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Window.
3. Configure the following settings, as required:
    - Default Window Size. Select from Fixed Size, Percentage of Screen Size, or Full Screen.
    - Default Window Colors. Select from 16, 256, 32 Thousand, 16 Million, or Automatic. Automatic enables Receiver to select the best available color depth for the connection. Before selecting a new color mode, ensure that it is supported on your user device.
    - Default 256 Color Mapping. Choose between Private - Exact Colors and Shared - Approximate Colors. If you select Private - Exact Colors, Receiver uses a private colormap on PseudoColor displays to display the exact colors sent by the server. This may, however, cause color flashing when moving between windows. To avoid this, use Shared - Approximate Colors to eliminate color flashing when switching context. Note that if other applications allocate all 256 colors, Receiver may use a private colormap.

Configuring a Default Network Protocol

You can set up a default network protocol to control the way Receiver searches for servers and how it communicates with them.

Note: The network protocol you specify also affects the way in which ICA browsing works. For more information, see Configuring ICA Browsing

To configure a default network protocol

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Server Location.
3. Select your required network protocol from the Network Protocol list.
4. Click OK.

Configuring ICA Browsing

ICA browsing (also called server location) is the mechanism by which Receiver discovers an appropriate server to host a given application. The way in which browsing works depends on which network protocol is configured, as follows:

- TCP/IP+HTTP and SSL/TLS+HTTPS. The default server address is ica. When ICA browsing, Receiver searches for ica.domainname, where *domainname* is one of the default domain names configured for Receiver. This feature enables the Domain Name Server (DNS) administrator or Windows Internet Naming (WINS) administrator to configure a host record that maps “ica” to the address of the data collector. For example, when Receiver sends a request for an application, the data collector responds with the address of a server on which the application is published. Receiver uses the HTTP or HTTPS protocol to contact servers.

- TCP/IP. The default setting for server location is auto-locate. Receiver attempts to contact all of the servers on the subnet by broadcasting on the UDP protocol. Alternatively, you can set a specific address for the server that functions as the data collector.

You can define up to three groups of servers to contact for ICA browsing: a primary and two backups. Each group can contain between one and five servers. Receiver attempts to contact each of the servers in turn.

To configure ICA browsing

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Server Location.
3. Select the required network protocol from the Network Protocol list.
4. Select the required server group from the Server Group list.
5. Click Add.
6. Enter the name or IP address of a server. For the TCP/IP+HTTP and SSL/TLS+HTTPS protocols, if you do not enter an IP address, you must have a server on your network mapped to the default name of ica.domainname, where *domainname* is one of the default domain names configured for Receiver. TCP/IP+HTTP and SSL/TLS+HTTPS server location do not support the (Auto-Locate) function.
7. To define other server groups, select the required group from the Server Group list and repeat Steps 5 and 6.
8. Click OK.

To configure keyboard shortcuts

Alternative keyboard shortcuts are used to control the behavior of Receiver and as substitutes for the standard Windows keyboard shortcuts for a published application. For example, if you want to close the current window on a Windows PC, you press ALT+F4. This key combination also closes a window in X Windows. Keyboard shortcut functionality enables you to map common key combinations like ALT+F4 to a key combination such as ALT+CTRL+F4 that is ignored by your local operating system. When you press this new combination, Receiver sends ALT+F4 to the server, closing the current window on the server.

If a keyboard shortcut includes plus or minus signs, use the numeric keypad to enter these signs instead of the main keypad to ensure the shortcut works correctly.

1. On the Tools menu, click Settings.

2. From the drop-down list, choose Keyboard Shortcuts to display the Keyboard Shortcuts page.

3. Select whether you want the key combinations to apply locally or remotely by choosing an option from the Handling of keyboard shortcuts drop-down list:

   Note: It might be necessary to set the user device keyboard type to LINUX to pass the keyboard shortcuts to remote sessions. See Configuring Default Keyboard, Sound, and Digital Dictation Support Settings for information about configuring the keyboard type.

   - Translated applies keyboard shortcuts to the local desktop rather than the remote desktop. For example, pressing ALT+TAB switches between all the windows currently open on the local desktop, including both local and remote windows.

   - Direct applies keyboard shortcuts to the remote desktop rather than the local desktop. For example, pressing ALT+TAB switches between all the windows currently open on the remote desktop, excluding any windows open on the local desktop.

     If you select Direct, keyboard shortcut translations are disabled to ensure that the keystrokes are applied to the remote desktop.

   - Direct in full screen desktops only applies keyboard shortcuts to the remote desktop rather than the local desktop when the remote session is running in full screen mode. If the session is running in any other window size mode, keyboard shortcuts are applied to the local desktop rather than the remote desktop.

     If you select Direct in full screen desktops only and the remote session is running in full screen mode, keyboard shortcut translations are disabled to ensure that the keystrokes are applied to the remote desktop.

4. Adjust the keyboard shortcut settings as required:

   - You can define alternative key combinations for the keyboard shortcuts ALT+F1 to ALT+F12, ALT+TAB, and ALT+SHIFT+TAB, which are reserved for use by X Windows. By default, these key combinations are generated by CTRL+SHIFT+F1 to

CTRL+SHIFT+F12, ALT+MINUS SIGN, and ALT+SHIFT+PLUS SIGN, but you can change the definitions by selecting alternative keys from the pop-up menus.

If you select a key combination for a shortcut, this particular combination appears dimmed on the pop-up menus for the other shortcuts.

- Any ALT key combinations not used by your X Window manager can be used as normal within the ICA session.

- You can define an additional combination for Toggle SpeedScreen (default SHIFT+F12). This enables you to turn SpeedScreen Local Text Echo on and off within a session. .

- You can also define a key combination to switch off remote key handling (default CTRL+F2). If a remote desktop is running in full screen mode, it is possible to lose control of the local desktop because all keystrokes are applied remotely. This key sequence temporarily applies keyboard shortcuts to the local desktop, until the remote window regains focus.

Note: If you want to use the PC key combination CTRL+ALT+DELETE during the session, use the key combination CTRL+ALT+ENTER or CTRL+ALT+RETURN.

To configure disk cache settings

Use the Disk Cache page in the Settings dialog box to control the location, size, and contents of the disk cache.

Note: The disk cache is used only if it is enabled for a particular connection. See Improving Performance over a Low-Bandwidth Connection for details.

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Disk Cache to display the Disk Cache page.
3. Select the settings you require. You can:
   - Set the maximum size of the cache by adjusting the Bitmap Cache Size value.
   - Change the location of the cache by clicking the Change button and browsing to your desired location for the Disk Cache Directory. If you change the location of a cache on a workstation, make sure that you clear the old cache first.
   - Set the minimum size of bitmaps to cache by adjusting the The minimum size bitmap that will be cached is slider. The size setting appears next to the slider.
   - Clear the cache by clicking the Clear Cache Now button. Citrix recommends that you do not clear the cache if any server connections are open. Before clearing the cache, verify that all server connections are closed.

Configuring Settings for Individual Connections

You can configure settings for individual connections, if required.

To configure settings for an individual connection

1. In the Connection view, select the connection entry that you want to change.
2. On the Connections menu, click Properties. The Properties dialog box has pages corresponding to the properties you can control, including:

   - The Network page, where you can change the settings required to establish a connection with the server. See To change network properties for a connection.
   - The Connection page, where you can control the connection between the server and Receiver; for example, to improve performance by reducing bandwidth. See Improving Performance over a Low-Bandwidth Connection. You can also use the Connection page to configure middle button paste functionality and digital dictation support. See Configuring Middle Button Paste Functionality and To configure digital dictation support.
   - The Firewall page, where you can specify proxy server settings. See Connecting Through a Proxy Server.
   - The Window page, where you can specify the window size and number of colors used for the ICA session. See To configure default window settings.
   - The Application page, where you can specify an application to run when you connect to the server. See To specify an application to run at connection.
   - The Login page, where you can specify your logon details so that you do not have to type them each time you connect to a server. See Configuring Logon Properties.
   - The Auto Reconnect page, where you specify settings for HDX Broadcast auto-client reconnect. See Reconnecting Users Automatically.
   - The Secure Gateway page, where you can specify a Secure Gateway server for Receiver to use when connecting to XenApp or XenDesktop. See Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay.
   - The File Associations page, where you can link file types with particular applications. See Configuring File Type Associations.

   Note: The File Associations option is not visible by default. You must configure Receiver to make this option visible. See Configuring File Type Associations for information about making this option visible.

To change network properties for a connection

Use the Network page in the Properties dialog box to specify a connection with a server and the network protocol to use.

1. In the Connection view, select the connection entry that you want to change.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Network.
4. Adjust the following properties, as required:
    - Change the description for a connection in the Description box.
    - To configure a connection to a different server, click Server. To configure a connection to a different published application, click Published Application. You can specify a server either by its name or its IP address. To get a list of servers or published applications, click Browse.
    - To change the protocol used when locating the data collector, see Configuring ICA Browsing.

Configuring Middle Button Paste Functionality

You can make Windows applications running on the server behave more like UNIX applications by configuring Receiver to enable middle button paste functionality.

To configure middle button paste functionality

1. In the Connection view, select the connection entry for which you want to enable middle button paste.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Connection.
4. Select the Enable Middle Button Paste check box.

To configure digital dictation support

XenApp and XenDesktop support client-side microphone input. This enables you to publish dictation software for use in sessions. Using local microphones, users can record dictations with applications running on the server.

For example, a user away from the office can establish a session to record notes using a laptop. Later in the day the user can retrieve the notes for review or transcription from the desktop device back at the office.

For information about configuring this feature on the server, see the XenApp and XenDesktop documentation.

Important: Before configuring digital dictation support for a connection, confirm that the Allow Audio Input check box is selected on the Preferences page of the Settings dialog box.

1. In the Connection view, select the name of the connection for which you want to configure digital dictation support.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Connection.
4. Select the Enable Audio Input check box and the Enable Sound check box.

To specify an application to run at connection

You can specify an application to run automatically when you connect to a server. If you specify an application, you do not see the desktop of the server when you connect and the connection closes when you exit the application.

1. In the Connection view, select the connection entry that you want to change.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Application.
    - In the Application box, specify the pathname of an application to run after connecting to a server
    - In the Working Directory box, specify the pathname of a directory to use with the application

    Note: If the entry you are configuring is a connection to a published application, the Application page is not available.

Configuring Logon Properties

You can store your logon details for a server connection so that you do not need to type them each time you connect.

To configure logon properties

1. In the Connection view, select the connection entry that you want to change.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Login.
4. Type your Username and Domain (optional) for the connection. Although you can also provide your password, for security reasons it is not good practice to configure the connection in this way. Instead, it is better to type your password when establishing the connection.
5. To enable smart card logon, select Allow Smart Card Logon. For more information about using smart cards with Receiver, see Enabling Smart Card Support.

Customizing Receiver Using Configuration Files

You can update many common settings using Receiver's user interface. To change more advanced or less common settings, you can also modify Receiver's configuration files. These configuration files are read each time a user launches a connection. You can update various different files depending on the effect you want the changes to have.

Important: From Version 10.x, for each entry in appsrv.ini and 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.

Applying 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.

Applying 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. For changes to apply to specific connections, modify appsrv.ini in this directory. These files are copied to new users' $HOME/.ICAClient directories when they first start Receiver, if the files do not exist there already.

Applying changes to specific connections for particular users. If you want the changes to apply to a specific connection for a particular user, modify the appsrv.ini file in that user's $HOME/.ICAClient directory. This file contains a section for each connection the user set up.

Applying 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 both existing and future connections for that user.

Validating configuration file entries. If you want to limit the values for entries in appsrv.ini and 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 appsrv.ini takes precedence over a value in wfclient.ini, which in turn takes precedence over a value in module.ini.

Configuring Citrix XenApp

Citrix XenApp enables users to connect to published resources (that is, published applications, desktops, and published content) through a server running a XenApp Services site. Citrix XenApp also creates the menu and desktop items through which users access published resources.

Users connect to published content and published applications from the Citrix XenApp view.

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 Citrix XenApp, it reads the configuration data from the server. After that, Citrix XenApp updates its settings and user interface periodically, at intervals specified in the config.xml file. This arrangement enables the server administrator to easily control the options that users see, and gives users the flexibility to adjust their own desktops, if allowed.

To update Citrix XenApp settings immediately

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Citrix XenApp.
3. Click Refresh Settings.

Important: config.xml affects all connections defined by the Web Interface server.

Publishing Content

Typically, Receiver connects to applications and desktops. Receiver can also open specific files associated with an application. In this case, the administrator publishes a file, rather than an application. This process is referred to as publishing content, and is a useful way to share any type of electronic information with network users.

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.

Customizing Desktop Access to Published Resources

If the Web Interface server is set up to allow it, users can adapt KDE or GNOME desktop access to their published resources. With full control over customization, users can:

- Choose to have available resources displayed in a menu
- Create desktop shortcuts to the resources
- Specify how Receiver refreshes the list of resources

Administrators can limit the degree to which users can customize these features by using Web Interface to disable one or more of the five pages of the Citrix XenApp dialog box in Receiver.

To customize the KDE or GNOME desktop on the user device

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Citrix XenApp.
3. To display published resources on the KDE or GNOME menu system, on the Application Display page, select Show applications in menu. Your local desktop system controls in which menu the resources appear.
4. To display published resources on the desktop, on the Application Display page, select Show applications in desktop folder. By default, no name is provided and each resource appears as an individual desktop shortcut. You can put resources in a desktop folder by entering a name in the box.
5. If the Application Refresh page is available, you can also define how Receiver updates the display of any menus, desktop items, and published resources in the Citrix XenApp view. Click one or more options on the Application Refresh page:
    - Refresh list at start. The display updates when you restart Receiver.
    - Refresh list when remote application launches. The display updates when a new connection is launched to a published application.
    - Refresh list on hourly interval. The display updates at intervals specified by the number of hours in the box.
6. Click OK.

Specifying the Web Interface Server

Because Citrix XenApp uses Web Interface as the access mechanism to published resources, you must set up Citrix XenApp to point to the Web Interface server. You can enable users to change the server location from Receiver if, for example, they need to access resources through more than one Web Interface server.

Alternatively, you can use Web Interface to fix the location so that users cannot modify it. Use this option if, for example, you do not want users to access resources through more than one Web Interface server.

To change the location of the server from Receiver

Note: Before users can change the server location, the administrator must ensure that the Server page in the Citrix XenApp dialog box is visible, and that the appropriate settings are enabled through Web Interface. For more information, see the Web Interface documentation.

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Citrix XenApp and then choose Server.
3. Click Change.
4. In the Citrix XenApp Configuration dialog box, enter the URL of the configuration file on the server that you want to use, or select a previously entered URL from the drop-down list.

   Note: You can enter just the server name, not the fully qualified URL, in the Citrix XenApp Configuration dialog box. Receiver reads the configuration file from the default location on that server.
5. Click Update.
6. On the Citrix XenApp page, click OK.

Specifying a Logon Method

You can use Web Interface to define the logon methods that are available to users when they access published resources. By default, Citrix XenApp prompts users to provide their credentials and then reuses them each time they connect to a resource, but you can also enable anonymous logons or password saving.

Depending on the logon choices that you enable, users can select a logon method for the resources that they access through Citrix XenApp. Although a variety of methods can be selected, only Anonymous logon, Prompt user, and Pass-through authentication (using Kerberos) are supported by Receiver.

Note: Only supported logon methods are displayed in the Logon mode drop-down list offered to the user in the Citrix XenApp dialog box.

To select a logon method for accessing published resources from Citrix XenApp

Important: Before users can choose logon methods, the administrator must decide what logon methods are appropriate and specify these using Web Interface. The administrator must also ensure that the Server page in the Citrix XenApp dialog box is visible, and that the appropriate settings are enabled on the Web Interface server. For more information, see the Web Interface documentation.

1. On the Tools menu of the Connection view, click Settings.
2. From the drop-down list, choose Citrix XenApp and then choose Server.
3. Under Logon mode, select the logon method you want to use for all of your connections. Only supported logon methods specified in config.xml appear.
4. Click OK.

Configuring Workspace Control

Workspace control provides users with the ability to disconnect quickly from all running applications, reconnect to applications, or log off from all running applications. You can move among user devices and gain access to all of your applications when you log on. For example, health care workers in a hospital can move quickly among workstations and access the same set of applications each time they log on to XenApp. These users can disconnect from multiple applications at one user device and open all the same applications when they reconnect at a different user device.

Workspace control is available only to users connecting to published resources with Citrix XenApp or through Web Interface.

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

Note: Workspace control is not available for resources published on servers running Citrix XenApp for UNIX.

If the workspace control configuration settings of the Web Interface are configured to allow users to override the server settings, users can configure workspace control using the in the Application Reconnection page in the Citrix XenApp dialog box. The following options are available on the Application Reconnection page:

- Enable automatic reconnection at logon allows users to reconnect to only disconnected applications or both disconnected and active applications
- Enable automatic reconnection from Reconnect menu allows users to reconnect to only disconnected applications or both disconnected and active sessions
- Customize Log Off button allows users to configure whether or not the log off command will include logging them off from applications that are running in the session

If users log on with smart cards or smart cards with pass-through authentication, you must set up a trust relationship between the Web Interface server and any other server in the farm that the Web Interface accesses for published applications. For more information, see the XenApp and Web Interface documentation.

Configuring Session Options

You can define the window size, color depth, and sound quality for sessions. using the Citrix XenApp Session Options page.

The preferences users set for color depth and sound quality affect the amount of bandwidth each session consumes. To limit bandwidth consumption, you can prevent users from overriding the server settings for some or all of the options on this page. When you prevent users from overriding the server settings, the settings configured on the Web Interface server are applied to connections from each user device.

To configure session option settings

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Citrix XenApp, and then choose Session Options.
3. Configure the session options settings you want to use for all of your connections. You can:
   - Change the Window Size
   - Adjust the Colors
   - Adjust the level of Audio
   - Configure the Handling of keyboard shortcuts
4. Click OK.

Supporting NDS Users

Users can choose to use their Novell Directory Services credentials to access a published resource using Citrix XenApp, if the server to which they are connecting supports NDS.

Important: Browsing the NDS tree requires that the Novell library, /usr/lib/libldapsdk.so, is installed on the user device. This is provided by the NLDAPsdk package, part of the eDirectory product, and is available from Novell's download page at www.novell.com.

To use NDS if the tree name is not in DNS

Novell suggests entering the configured NDS tree name into the Domain Name Server (DNS) to enable the client to look up the IP address for the NDS server. If the NDS tree name is not entered into DNS, use the following procedure to specify the name or IP address of the NDS server.

1. Do one of the following:
   - Open the configuration file, wfclient.ini, in the $HOME/.ICAClient directory to enable a specific user to access the NDS server
   - Open the configuration file, wfclient.ini, in the $ICAROOT/config directory to enable all users to access the NDS server—all users in this case being those who use the wfcmgr program after the change
2. In the [WFClient] section of the file, add the following line: `NDSTree=server1`*`:ppp`* `server2`*`:ppp`* `server3`*`:ppp`*

   where *:ppp* is an optional port number and server1, server2, and so on are either names of NDS servers, or IP addresses of NDS servers. You can use a mixture of server names and IP addresses, with a space separating the entries.

   Note: New entries in wfclient.ini must also be added to the All_Regions.ini configuration file. See Customizing Receiver Using Configuration Files for more information.

3. Save and close the file.

   Note: Citrix XenApp always tries to access the tree name sent by the the Web Interface server before checking the configuration file for server details.

Optimizing Your Receiver Environment

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

- Reconnecting Users Automatically
- Mapping User Devices
- Configuring USB Support
- Improving Performance over a Low-Bandwidth Connection
- Improving Multimedia Performance with HDX

Reconnecting Users Automatically

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

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

By default, Receiver waits 36 seconds before attempting to reconnect to a disconnected session and attempts to reconnect to that session three times. You can change these settings for all connections or for an individual connection.

To configure HDX Broadcast auto-reconnect settings

- For all connections, select Tools > Settings
- For an individual connection, select the connection entry to configure. Select Connections > Properties > Auto-Reconnect.

1. Select Enable Auto-Reconnect.
2. Enter values for Maximum Retries and Seconds Delay Before Retrying Reconnect
3. Click OK.

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.

To configure client COM port mapping

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

1. On the Tools menu, click Settings.
2. From the drop-down list, choose COM Ports to display the COM Ports page.
3. To map a COM port, click Add.
4. In the Files list, click the name of the device for which you want to configure COM port mapping.
5. Click OK.

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 makes 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. 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 filesystem 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 automatic 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 andXenDesktop documentation.

To specify drives and directories to map at logon

1. On the Tools menu, click Settings.

2. Choose Drive Mapping from the drop-down menu. For each drive letter, the Drive Mapping list shows the disk or pathname of the user device directory mapped to the drive. In the Enable/Read/Write columns, icons display whether each mapped drive is enabled for use and what type of access the user will have to the drive.

3. Select the check box in the Enable column next to an available drive letter and then click the box for the drive.

4. Click Modify. A standard UNIX file selection dialog box appears. Select the UNIX directory you want to map and click OK. Alternatively, you can simply type the directory path in the box next to the required drive letter.

5. The mapped directory appears in the Drive Mapping list. If the drive letter you selected is not available on the Windows server, the specified directory is mapped to another free drive letter at logon.

6. Specify the access for the drive by clicking the corresponding read/write icons. You can use:

Icon	Meaning
(Pair of glasses)	Read access
(Pair of glasses, with question mark)	Prompt for read access on first access per session
(Pair of glasses, obscured by cross)	No read access
(Pencil)	Write access
(Pencil, with question mark)	Prompt for write access on first access per session
(Pencil, obscured by cross)	No write access

7. Ensure that Enable Drive Mapping is selected.

8. Click OK. Log off from any server connections already established and reconnect. The same drive mapping and access settings will apply to all connection entries.

To enable dynamic mapping of client drives during a session

1. On the Tools menu, click Settings.
2. Choose Drive Mapping from the drop-down menu.
3. Select Enable Dynamic Drive Mapping.
4. Click OK.

Note: When dynamic client drive mapping is enabled, Receiver monitors the /media and /mnt/media directories for new mounts.

To view mapped client drives when connected to a Windows server

1. From your session, double-click My Computer on the remote desktop. When connected to published applications, users can access local drives in the same way as they would when running applications locally.

To manually map a client drive on a Windows server

Mapped drives that do not appear after logon can be manually mapped from within an ICA session. Use the following procedure to manually map a client drive:

1. In the Connection view, select the connection you want to open.
2. On the Connections menu, click Connect and log on to the server.
3. On the server, start Windows Explorer.
4. On the Tools menu, click Map Network Drive. The Map Network Drive dialog box appears.
5. In the Drive list, select a server drive letter. This drive letter represents the mapped client drive. Click Browse.
6. In the Browse For Folder dialog box, expand Client Network.
7. Expand Client, and select the appropriate entry for your directory from the list of available client drives.
8. If you want to have this drive available to you each time you log on to this server, select Reconnect at logon. Click OK.

To configure drive mapping for floppy disks

You can manually map floppy drives on servers for access within a session. To do this, access DOS formatted floppies mounted on your user device using the following command:

```
mount -t vfat /dev/fd0 /mnt/floppy
```

Then select the /mnt/floppy directory in the Drive Mapping dialog box.

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, configure the Citrix 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 wfcmgr 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 (:).

   Note: New entries in wfclient.ini must also be added to the All_Regions.ini configuration file. See Customizing Receiver Using Configuration Files for more information.

3. Save and close the file.

Mapping Client Printers on XenApp for Windows

In most cases, no 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 to play sounds through a Windows-compatible sound device installed on the user device. You can set audio quality on a per-connection basis on the XenApp server and users can set it on 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.

Users can enable or disable client audio mapping and set the audio quality for a connection on the user device. If the user device and server audio quality settings are different, the lower setting is used.

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

To configure audio mapping for a connection

1. In the Connection view, select the name of the connection for which you want to map audio.
2. On the Connections menu, click Properties.
3. Choose Connection from the drop-down menu.
4. Select the Enable Sound check box.
5. Select High, Medium, or Low quality depending on the available bandwidth.

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 Customizing 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 remoted to their virtual desktop. USB devices available for remoting include flash drives, smartphones, PDAs, printers, scanners, MP3 players, security devices, and tablets. Desktop Viewer users can control whether USB devices are available on the virtual desktop using a preference in the toolbar.

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

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

- Keyboards
- Mice
- Smart cards

Note: Specialist USB devices (for example, Bloomberg keyboards and 3D mice) can be configured to use USB support. For information on configuring 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 Updating 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, remoted 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 remoted to the virtual desktop. The virtual desktop is responsible for controlling the USB device and displaying it in the user interface.

Mass Storage Devices

If a user disconnects from a virtual desktop when a mass storage device is still plugged in to the local desktop, that device is not remoted to the virtual desktop when the user reconnects. To ensure the mass storage device is remoted 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: Mass storage devices can also be accessed through client drive mapping, and so USB support is not required.

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 by editing the default usb.conf file. For more information see, To 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.

Content Security (Class 0d)

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

Video (Class 0e)

The video class covers devices that are used to manipulate video or video-related material, such as webcams, digital camcorders, analog video converters, some television tuners, and some digital cameras that support video streaming.

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.

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 are applied before the default rules when a virtual desktop starts. This allows you to override the default rules provided by XenDesktop.

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=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
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
```

Configuring Start-Up Modes

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

```
[WfClient]

DesktopApplianceMode = Boolean
```

where *Boolean* can have one of the following values:

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 a Low-Bandwidth Connection

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.

- **Change your Receiver configuration**. Changing your Receiver configuration 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.
- **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.

Changing Your Receiver Configuration

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

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

  User side: Connections > Properties > Connection page

  Server side: SpeedScreen Latency Reduction Manager

- **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.

  User side: Connections > Properties > Connection page

  Server side: Citrix Audio Quality and Image Compression policy settings.

- **Enable disk caching**. Disk caching stores commonly used bitmaps (images) locally on the user device so that the bitmaps are not transferred over the server connection every time they are needed.

  User side: Connections > Properties > Connection page

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

  User side: Connections > Properties > Window page

  Server side: XenApp Services site > Session Options

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

  User side: Connections > Properties > Window page

  Server side: XenApp Services site > Session Options

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

  User side: Connections > Properties > Connection page

  Server side: Citrix Audio quality policy setting

Changing Receiver Use

ICA technology is highly optimized and typically does not have high CPU and bandwidth requirements. However, if you are using a very low-bandwidth connection, 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 with HDX

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

- HDX MediaStream Windows Media Redirection
- HDX MediaStream Flash Redirection
- HDX 3D Pro
- HDX RealTime Webcam Video Compression

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 running on 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
- Blacklist 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 streams GStreamer parameters
- Manage and deploy custom configurations depending on the media file types supported by GStreamer on a user device.

To implement Windows Media Redirection, you must install GStreamer, an open-source multimedia framework, on each user device that requires it. Typically, you install GStreamer before you install the Receiver software. This enables you to select the GStreamer option during the installation to ensure that Windows Media Redirection is integrated into the Receiver software.

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

To configure 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.

To configure HDX 3D Pro GPU decoding

HDX 3D Pro supports both GPU (hardware-based) and CPU (software-based) decoding. If GPU decoding is not available, Receiver automatically falls back to CPU decoding.

1. Ensure your user device meets the feature requirements. For more information, see System Requirements

2. Enable GPU decoding, by setting EnableH264HWAcceleration to "True" in wfclient.ini.

To 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, as follows:
   a. Select Allow Audio Input on the Tools > Settings > Preferences page.
   b. Select Enable Audio Input on the Connection > Properties > Connection page.

Important: You must ensure you enable audio input in both locations.

Disabling 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 Customizing 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.

Improving the User Experience

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

- Expired Password Support
- ClearType Font Smoothing
- File Type Association
- Special Folder Redirection
- Server-Client Content Redirection
- xcapture

Configuring Support for Expired Passwords

If support for expired passwords is enabled on the Web Interface server, users are prompted to change their password when connecting to hosted applications and desktops from the Citrix XenApp view.

For more information about configuring support for expired passwords on the Web Interface server, see the Web Interface documentation.

If users connect to the domain controller directly to change expired passwords, Kerberos must be installed and configured on the user device. The exact configuration steps required are dependent upon how Kerberos is installed in your environment. Citrix recommends, however, adding suitable records to the Domain Name System (DNS) to avoid having to configure each user device with the locations of Key Distribution Centers. For more information, see your Kerberos documentation

If users connect to your XenApp farm or XenDesktop site to change expired passwords, Citrix recommends you implement secure connections using, for example, SSL.

Note: If you are using Novell Directory Services (NDS) authentication, expired password support is not available.

Specifying the Kerberos Realm

If users connect to the domain controller directly to change expired passwords, Receiver requires the name of the Kerberos realm that corresponds to the relevant Windows domain. If the realm name is an upper-case version of the domain name, Receiver finds it automatically. If the realm name is not an upper-case version of the domain name, add the following parameter to the [WFClient] section of wfclient.ini:

Realm_*WindowsDomainName=KerberosRealmName*

For example, if Kerberos should use the realm COMPANY.LOCAL to access the Windows domain abc, add the line:

Realm_abc=COMPANY.LOCAL

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 configuration file wfclient.ini.

The entry for font smoothing takes the form:

`FontSwitchingType = number`

where *number* can take one of the following values:

0 or 1	No smoothing
2	Standard smoothing
3	ClearType (horizontal sub-pixel) smoothing

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

Configuring File Type Associations

You can configure Receiver to enable users to open specific file types with published appications automatically. File type association determines which application on the server to use with particular file types, and automatically opens the associated application when a user clicks on that file type.

File type associations can be either dynamic (received from the XenApp Services site), or static (configured on the File Associations page of the Properties dialog box).

Note: If a user tries to open a file using dynamic file type associations while not logged on to a server, a logon prompt is displayed. If the user cancels the logon, the application launch is also cancelled.

By default, file type associations are dynamic, but if your environment does not have a XenApp Services site you can set up static file type associations on Receiver. These file type associations persist between sessions.

Dropped files must reside on a mapped file system to enable the server to access them. Users can drop files onto the main Receiver window, the Receiver manager icon, or onto another desktop icon, with the following results:

- **Dropping files onto the main Receiver window**. In most cases, if a user drops a file onto the main client window, the file type associations determine which application to open. However, certain types of files are treated differently. If an .ica file is dropped onto the main Receiver window, Receiver makes the connection specified in the file. If a .pnagent file or a .desktop file is dropped on the main Receiver window, Receiver launches the application specified in the file.

- **Dropping files onto the Receiver manager icon**. If a user drops an .ica file onto the Receiver manager icon, Receiver makes the connection specified in the file. If other file types are dropped onto the Receiver manager icon, the file type associations determine which application to open.

  Note: This functionality is not available if you are using the GNOME desktop environment.

- **Dropping files onto another desktop icon**. If a user drops a file onto another desktop icon, Receiver responds only if the icon corresponds to a Citrix published resource. For published application icons, Receiver always uses dynamic file type associations to check whether the file type is supported by the application. If so, Receiver opens the file using the selected application. If not, the user is asked whether to continue opening the chosen application. For published content icons, the user is advised that the icon is not an application, and Receiver offers the option of opening the file with a suitable application.

  Note: This functionality is not available if you are using the GNOME desktop environment.

To configure Receiver to use static or dynamic file type associations

1. Choose and open a configuration file according to which users you want your changes to affect. See Customizing Receiver Using Configuration Files for information about how updates to particular configuration files affect different users.

2. In the [WFClient] section of the file, set the value for `UseDynamicFileTypeAssociation`. `False` makes the File Associations option visible in the Properties drop-down list and sets Receiver to use static file type associations, and `True` sets Receiver to use dynamic file type associations.

   Note: If this line does not appear in either wfclient.ini or module.ini, Receiver uses static file type associations.

3. Save and close the file.

To set up static file type associations for individual connections

1. On the View menu, click Connection View to display the available connections.

2. Select the connection for which you want to set up file associations.

3. On the Connections menu, click Properties.

4. From the drop-down list, choose File Associations.

5. Click Add.

6. Select the required application and file type combination from the list and click OK.

   Note: A file type cannot be associated with more than one published application. However, you can associate more than one file type with a single application.

7. Click OK.

8. Ensure that the published application and file type are associated for content redirection. For more information, see the XenApp documentation.

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 wfclient.ini, 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 wfclient.ini (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 Web page 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.

Using xcapture

Receiver 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 start xcapture from the main Receiver window

On the Tools menu, click xcapture.

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.

Securing Receiver Communication

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

- A SOCKS proxy server or secure proxy server (also known as *security proxy server*, HTTPS proxy server, or SSL tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Receiver and servers. Receiver supports SOCKS and secure proxy protocols.
- Secure Gateway or SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using Receiver through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

Connecting Through a Proxy Server

Proxy servers are used to limit access to and from your network, and to handle connections between Receiver and your XenApp or XenDesktop deployment. 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.

Note: To ensure a secure connection, enable TLS/SSL.

Using Auto-Client Proxy Detection

If you are deploying Receiver in an organization with many proxy servers, consider using auto-client proxy detection. Auto-client proxy detection communicates with the local Web browser to discover the details of the proxy server. It is also useful if you cannot determine which proxy server will be used when you configure Receiver.

Auto-client proxy detection can be used with Firefox, Mozilla, and Netscape 4.0 or later.

To configure auto-client proxy detection by default

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Firewall.
3. Select Use Browser settings.
4. Click OK.

To configure auto-client proxy detection for a server connection

1. In the Connection view, select the connection for which you want to specify auto-client proxy detection.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Firewall.
4. Select Use Browser settings.

   Important: If the list appears dimmed, clear the Use default check box to stop using the default protocol, and then select Use Browser settings.
5. Click OK.

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.

To specify a default secure proxy server

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Firewall.
3. Select Secure (HTTPS).
4. Type the proxy name or IP address in the Proxy Address box and the port number in the Port box for the secure proxy server.
5. Enter the user name and password to use when connecting to the proxy server in the Username and Password boxes if required.
6. Click OK.

To specify a secure proxy server for an individual connection

1. In the Connection view, select the connection for which you want to specify a secure proxy server.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Firewall.
4. Select Secure (HTTPS).

   Important: If the list appears dimmed, clear the Use default check box to stop using the default protocol, and then select Secure (HTTPS).
5. Type the proxy name or IP address in the Proxy Address box and the port number in the Port box for the secure proxy server.
6. Enter the user name and password to use when connecting to the proxy server in the Username and Password boxes if required.
7. Click OK.

Connecting Through a SOCKS Proxy Server

To specify a default SOCKS proxy manually

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Firewall.
3. Select SOCKS.
4. Type the proxy name or IP address in the Proxy Address box and the port number in the Port box for the SOCKS proxy server.
5. Enter the user name and password to use when connecting to the proxy server in the Username and Password boxes if required.
6. Click OK.

To specify a SOCKS proxy for a server connection manually

1. In the Connection view, select the connection for which you want to specify a SOCKS proxy server.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Firewall.
4. Select SOCKS.

   Important: If the list appears dimmed, clear the Use default check box to stop using the default protocol, and then select SOCKS.
5. Type the proxy name or IP address in the Proxy Address box and the port number in the Port box for the SOCKS proxy server.
6. Enter the user name and password to use when connecting to the proxy server in the Username and Password boxes if required.
7. Click OK.

Configuring Automatic Proxy Detection

This setting detects a proxy server automatically by querying http://wpad/wpad.dat/ for proxy information. This feature means administrators do not have to spend time supporting incorrect or dynamic configurations; however, the administrator must set up the correct proxy information on http://wpad/wpad.dat/ to enable Receiver to collect it successfully.

To configure automatic proxy detection by default

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Firewall.
3. Select Automatically detect proxy.
4. Click OK.

To configure automatic proxy detection for an individual connection

1. In the Connection view, select the connection for which you want to specify automatic proxy detection.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Firewall.
4. Select Automatically detect proxy.

   Important: If the list appears dimmed, clear the Use Default check box to stop using the default protocol, and then select Automatically detect proxy.
5. Click OK.

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 both SSL and TLS protocols.

- SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.

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

Connecting with 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 (Sucure 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*.

To specify a default Secure Gateway server

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Secure Gateway to display the Secure Gateway page.

   Note: The Secure Gateway option appears dimmed unless the default network protocol on the Server Location page is SSL/TLS + HTTPS server location.
3. Type the fully qualified domain name of the Secure Gateway server in the Secure gateway address box, and the port number in the Port box.
4. Click OK.

To specify a Secure Gateway for a server connection

1. In the Connection view, select the connection for which you want to specify a Secure Gateway server.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Secure Gateway to display the Secure Gateway page.

   Note: The Secure Gateway option appears dimmed unless the default network protocol on the Server Location page is SSL/TLS + HTTPS server location.
4. Type the fully qualified domain name of the Secure Gateway server in the Secure gateway address box, and the port number in the Port box.
5. Click OK.

Connecting with Citrix SSL Relay

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

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

You can use Citrix SSL Relay to secure communications:

- Between an SSL/TLS-enabled user device and a server. Connections using SSL/TLS encryption are marked with a padlock icon in the main Receiver window.
- 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 SSL/TLS encryption, see the Web Interface documentation.

Configuring and Enabling Receiver for SSL and TLS

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

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

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

For more information about the Secure Gateway for Windows or Citrix SSL Relay, see the XenApp documentation.

Installing Root Certificates on User Devices

To use SSL or TLS, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate. Receiver supports the following certificates:

Certificate	Issuing Authority
Class4PCA_G2_v2.crt	VeriSign Trust Network
Class3PCA_G2_v2.crt	VeriSign Trust Network
BTCTRoot.crt	Baltimore Cyber Trust Root
GTECTGlobalRoot.crt	GTE Cyber Trust Global Root
Pcs3ss_v4.crt	Class 3 Public Primary Certification Authority
SecureServer.crt	Secure Server Certification Authority

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.

To install a root certificate, copy any new Certificate Authority (root) certificate files to the subdirectory keystore/cacerts in the installation directory ($ICAROOT). To enable Receiver to use the new certificate, you must restart wfcmgr after adding the certificate.

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.

To configure SSL or TLS as the default protocol

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Server Location.
3. Select SSL/TLS + HTTPS server location from the Network Protocol list.

   Note: You can specify this protocol for all connections or for individual server groups and servers using the Server Group list and Address List.
4. Click OK.

To configure Receiver to use SSL or TLS for a single connection

1. In the Connection view, select the connection for which you want to use SSL.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Network.
4. Select SSL/TLS + HTTPS server location from the Network Protocol list.

   Important: If the list appears dimmed, clear the Use Default check box to stop using the default protocol, and then select SSL/TLS + HTTPS server location from the Network Protocol list.
5. Select the server location through one of the following methods:
   - Select the Use Default check box.
   - Enter the fully qualified domain name of the machine to use for server browsing in the Server Location box.
6. Click OK.

Connecting to a Server Through 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, use the information provided in this topic to configure the firewall settings.

To connect across an address-translating firewall

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Firewall.
3. Select the Use alternate address for firewall connection check box.
4. Add the external Internet address of a server that is on the subnet to which you want to connect to the Address List on the Server Location page. For more information, see Configuring ICA Browsing.

Using ICA Encryption

Encryption increases the security of your server connection. By default, basic encryption is enabled on all connections. Receiver must be configured to use the minimum encryption level required by the server, or greater. To enable encryption levels higher than Basic, the server must support ICA encryption.

To change the encryption settings

1. In the Connection view, select the connection for which you want to change encryption settings.
2. On the Connections menu, click Properties.
3. From the drop-down list, choose Connection.
4. From the Encryption Level list, choose an encryption level.
5. Click OK.

Note: You can configure the server to allow connections from Receiver that use only basic or advanced encryption. For more information about configuring the server to check encryption levels before allowing connections, see the XenApp documentation.

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.

For more information about configuring smart card support on your servers, see the XenApp documentation.

Note: Smart card data is security-sensitive and should be transmitted over a secure authenticated channel such as SSL/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 reader
- You must install the PC/SC Lite package (including the Resource Manager daemon and shared library), available for download from http://www.linuxnet.com/

Important: If you are using the SunRay terminal with SunRay server software Version 2.0 or above, you must install the PC/SC SRCOM bypass package, available for download from http://www.sun.com/.

To configure smart card support

1. Do one of the following:
   - In the Connection view, click New on the Connections menu to configure a new connection.
   - Select an existing connection entry you want to configure. On the Connections menu, click Properties.
2. From the drop-down list, choose Login.
3. Click Allow Smart Card Logon.
4. Click OK.

Troubleshooting

This section contains information to help administrators troubleshoot any issues with Receiver for Linux, as follows:

- Known Issues
- Common Error Messages
- Sending Diagnostic Information to Citrix Support

Known Issues

The following topics describe known issues with Receiver for Linux in various different categories and how to go about resolving them.

Connection Issues

The following are known connection issues.

I cannot connect properly to a published resource or desktop session

If, when establishing a connection to a Windows server, a dialog box appears with the message “Connecting to server…” but no subsequent connection window appears, you may need to configure the server with a Client Access License (CAL). For more information about licensing, see Licensing Your Product.

I have problems using network address translation with SSL/TLS through a firewall

A valid SSL/TLS relay host must be specified for SSL/TLS to work correctly when the Firewall setting Use alternate address for firewall connection is selected.

For information about specifying an SSL/TLS relay host, see Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay.

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.

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 ...;
```

My seamless connections do not share sessions

Seamless connections can share sessions with other seamless connections. For sessions started using Citrix XenApp or the Web Interface, session sharing occurs as directed by the server. However, locally defined sessions, shown in Connection View, will not share unless they have the same user name and domain credentials. For seamless connections, these credentials should be specified to enable sharing to occur. To override this behavior set the following line in wfclient.ini or module.ini - see Customizing Receiver Using Configuration Files for information about how updates to particular configuration files affect different users:

```
SessionSharingLoose=True
```

This enables sessions without prespecified credentials to share with existing sessions.

Display Issues

The following are known display issues.

I experience problems with over-scrolling when using published applications

Note: These problems do not occur when connecting to servers running Citrix Presentation Server 4.5 or later or Citrix XenApp.

To prevent over-scrolling

1. Open the configuration file, wfclient.ini, in the $HOME/.ICAClient directory.
2. In the [Thinwire 3.0] section of the file, type:

   ```
   TW2StopwatchMinimum=100
   ```

   Note: You must also add the new entries in wfclient.ini to the All_Regions.ini configuration file. See Customizing Receiver Using Configuration Files for more information.
3. Save and close the file. The lowest effective value is likely to be 100, but you may need to experiment with this value to find the optimum solution.

Incorrect keystrokes are displayed 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 Configuring Default Keyboard, Sound, and Digital Dictation Support Settings.

Ghosting occurs when I minimize or maximize a window

With some applications (including Microsoft Outlook), ghost windows can appear when maximizing or iconifying local, seamless windows (for example, when you use the ALT+F9 shortcut key combination on a connection window). The ghost windows may appear to display the contents of another window and may be difficult to remove.

To prevent ghosting, use the Iconify button on the server window rather than on the local window.

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 window outlines only when moving a window.

Running in seamless mode using different window managers

Seamless mode removes local window manager decorations such as the title bar and borders, and instead uses decorations sent from the server. Different window managers use different ways of removing window decorations.

Receiver sets the _MOTIF_DECORATIONS hint to remove the decorations. It also sets the class of all seamless windows to “Wfica_Seamless”, so that a window manager that does not recognize the Motif hint can be told to remove the decorations through resource file entries.

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)
   ```

Note: You must add the new entries in wfclient.ini to the All_Regions.ini configuration file. See Customizing Receiver Using Configuration Files for more information.

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. Otherwise, use the following procedure to prevent color flashing.

To prevent color flashing with a 256-color connection

1. In the Connection view, select the connection entry that causes the flashing.
2. From the Properties page, select Window from the drop-down list to display the Window page.
3. Select Shared - Approximate Colors and click OK.

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.

I have problems entering Polish characters on US English keyboards

Appropriately configured Microsoft Windows servers enable users to set the input locale to “Polish (Programmers)” to enter accented Polish characters using a US English keyboard. This can also be configured on Receiver.

To allow the entry of accented Polish characters on US English keyboards

Note: This setting is not recommended for use with any other keyboard layout.

1. On the Tools menu, click Settings.
2. Select Preferences from the drop-down list to display the Preferences page.

3. Set the Keyboard Layout to Polish (Programmers) and click OK.
4. Open the wfclient.ini configuration file.
5. Edit the following line in the [WFClient] section: `UnicodeKeyboard=Off`
6. Save and close the file.

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 can’t see any menu entries relating to Receiver when using the GNOME window manager

If you install Receiver as a non-privileged user, the desktop integration features are not fully enabled. To see the menu entries, install Receiver as a privileged user (root).

I have user interface problems when using GNOME 2.0 on SuSE 10.x

Using the xorg-x11-fonts-cyrillic font package in the GNOME desktop environment on SuSE 10.x systems can cause font loading to fail in certain applications, including Receiver. This can cause problems in the user interface such as missing characters, and the following error message may appear when starting Receiver:

“Warning: Cannot convert string "-gnu-*-*-*-*-*-*-120-*-*-*-*-iso10646-1,-*-gothic-medium-r-normal-*-*-120-*-*-*-*-ksc5601.1987-0,-*-helvetica-medium-r-*-*-*-120-75-75-*-*-iso8859-1,-*-ming-*-*-*-*-*-*-140-*-*-*-*-big5-0,-isas-fangsong ti-medium-r-normal--16-160-72-72-c-160-gb2312.1980-0,-*-helvetica-medium-r-normal--0-*-75-75-p-*-koi8-r,-*-helvetica-medium-r-*-*-*-120-75-75-*-*-iso8859-6,-*-arial-medium-r-*-*-*-120-75-75-*-*-iso8859-6,-*-helvetica-medium-r-*-*-*-120-75-75-*-*-*-*,-*-*-medium-r-*-*-*-120-75-75-*-*-*-*,-*-*-medium-r-*-*-*-120-*-*-*-*-*-*" to type FontSet”

To avoid these problems, remove the xorg-x11-fonts-cyrillic font package from your system. This improves the appearance of the user interface even in sessions that use Cyrillic characters.

Alternatively, modify Receiver startup to run the command xset fp rehash before launching Receiver or run the xset fp rehash command manually before starting Receiver. Note that running the xset fp rehash command in GNOME startup programs does not always fix this problem because the problem often does not occur until after the startup scripts are run.

I have problems displaying Arabic characters on Fedora Core 5

Only a limited number of fonts in Fedora Core 5 support Arabic characters, most of which cannot be used in a UTF-8 locale. The standard Arabic desktop environment is a UTF-8 locale, and the available fonts are unsuitable for use with Receiver.

One workaround is to run Receiver in a non-UTF-8 locale. The alternative is to download and install the GNU Unifont font; however this must be done manually because there is no Fedora Core 5 package that includes this font.

I want to make a session that spans multiple monitors

A new command line multi-monitor display control option, -span, enables you to do this. It allows full-screen sessions to span multiple monitors.

Important: -span has no effect on Seamless or normal windowed sessions (including those in maximised windows).

The - span option has the following format:

```
-span [h][o][a|mon1[,mon2[,mon3,mon4]]]
```

If `h` is specified, then a list of monitors is printed on stdout. And if that is the whole option value, wfica then exits.

If `o` is specified, then 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, then the remainder of the command line is ignored. This is used as a dummy value to prevent the following part of the command line being incorrectly treated as the option value.

If the option value ends here or is not present, then Receiver will attempt to create a session that covers the entire display.

Otherwise, it is assumed that the remainder of the 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 the 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 wfcmgr 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.

Browser Issues

The following are known 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 Setting up Server-Client Content Redirection.

When accessing published resources, my browser prompts me to save a file

Browsers other than Mozilla, Firefox, and Netscape 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 the Web Interface

Details vary among browsers, but you must either configure the browser to use the Citrix plug-in for Netscape, npica.so, or 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.

I want to enable the ICA browser plug-in on the Konqueror Web browser

The Konqueror browser does not automatically use the ICA browser plug-in to start ICA sessions. To enable the plug-in, Konqueror must scan for new plug-ins. For information about how to perform this scan, see Konqueror's online help.

I have problems launching published applications using Mozilla 1.4.x

Using Mozilla 1.4.x can cause launching published applications to fail. To fix this problem, Citrix recommends using Mozilla 1.6 or later.

I experience poor response times when viewing certain Web sites with Microsoft Internet Explorer

If Web pages continually redraw, this can affect performance. Setting the number of screen areas tracked to prevent redundant drawing of bitmap images can fix this problem. Three hundred is an adequate value for 1024 x 768 sessions.

You can set the number of screen areas tracked in the appsrv.ini configuration file or the wfclient.ini file.

To set the number of screen areas tracked by editing appsrv

1. Open appsrv.ini.
2. Add the following lines to the section for the relevant connection:

   ```
   EnableOSS=Off

   TwRedundantImageItems=300
   ```

   Note: You must also add the new entries in appsrv.ini to the All_Regions.ini configuration file. See Customizing Receiver Using Configuration Files.
3. Save and close the file.

To set the number of screen areas tracked by editing wfclient

1. Open wfclient.ini.
2. Add the following lines to the [WFClient] section:

   ```
   EnableOSS=Off

   TwRedundantImageItems=300
   ```

   Note: You must also add the new entries in wfclient.ini to the All_Regions.ini configuration file. See Customizing Receiver Using Configuration Files.

I have problems using Firefox with Fedora Core 5

Fedora Core 5 ships with Firefox 1.5.0.1, however this version of Firefox does not work with the ICA browser plug-in. To enable the plug-in and get Firefox working correctly, download the latest version of Firefox from the Mozilla Web site at http://www.mozilla.com/firefox.

The installer does not support Mozilla Firefox or other browsers

If you have problems using a specific Web browser such as Mozilla Firefox, set the environment variable BROWSER to specify the local path and name of the required browser before running setupwfc.

Other Issues

The following are known issues of other sorts.

My configuration file settings no longer work after upgrading Receiver

For each entry in appsrv.ini and 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.

My new configuration file settings are not being picked up

For each entry in appsrv.ini and 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 get an error message when trying to run Receiver

If you see an error message such as “/opt/Citrix/ICAClient/wfcmgr: error while loading shared libraries: libXm.so.4: cannot open shared object file: No such file or directory,” this is because Receiver will not run on distributions that do not include the Motif library. The solution is to install libXm.so.4, Version 2.3.1. or above

I cannot set the attributes for files on floppy disks

Changing file attributes on a locally mounted floppy drive fails without giving a warning message, leaving the file properties unchanged.

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 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 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.

I have problems with file names containing accented characters on mapped drives

To ensure the correct operation of client drive mapping with file names containing accented Western or Eastern European characters, you need to set the server DOS codepage to either 1252 (for Western European characters) or 1250 (for Eastern European characters).

To do this, set the server registry entry HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage\OEMCP to either 1252 or 1250.

However, you might then need to set the codepage back to 850 using a console window for DOS applications to display characters correctly, and to accept alt-numeric entries from the keypad.

For the registry setting change to take effect, you need to restart your server.

My keyboard shortcuts do not function correctly

If your window manager uses the same keyboard shortcut combinations to provide native functionality, your keyboard shortcut combinations might not function correctly. For example, the KDE window manager uses CTRL+SHIFT+F1 to CTRL+SHIFT+F4 to switch between desktops 13 to 16. If you experience this problem, choose Direct from the Handling of keyboard shortcuts drop-down list, or reconfigure the window manager to suppress the default keyboard shortcut combinations. See To configure keyboard shortcuts for more information about configuring keyboard shortcuts.

I have problems using IME accelerator keys under KDE

The ATOK-IME accelerator keys on a Windows server and the KDE window manager accelerator keys can conflict. There is an alternative keyboard file for Linux keyboards that maps the left Windows key to be visible as the control key in an ICA session. The left Windows key can then be used when accessing ATOK-IME functions, instead of the CTRL key.

To select the alternative keyboard layout

1. On the Tools menu, click Settings.
2. Select Preferences from the drop-down list to display the Preferences page.
3. Set the Keyboard Type (Client) to LINUX (Japanese KDE) and click OK.

The server does not recognize my Pocket PC

If the user logged on to the user device does not have read access to /dev/ttyUSB0, the server cannot access a USB-tethered Pocket PC connected to the user device. The configuration changes required to enable read access to this file vary for different UNIX systems—see your system documentation for more information.

The server does not recognize my Pocket PC when I reconnect to a session

If you close a session in which the server accessed a USB-tethered Pocket PC, and then reconnect, the server may not recognize the Pocket PC through the new connection. To fix this issue, disconnect the Pocket PC from the user device and then reconnect it.

The server does not recognize a second Pocket PC connected to my user device

If you have multiple USB-tethered Pocket PCs connected to your user device, only one is available to servers. After a server recognizes the first Pocket PC, if a second server tries to access a second Pocket PC, a PDA contention error message appears.

I get an error message when a server connects to my Pocket PC

If the message “You do not have sufficient permission to create lockfiles in directory ...” appears when a session accesses your USB-tethered Pocket PC, this means you cannot create a lockfile to indicate to other programs that your Pocket PC is already in use. There are actions you can take to prevent this message from appearing.

If you never access your Pocket PC from other programs on the user device, add the following to the [WFClient] section of the appropriate configuration file:

```
ContinueWithoutPDALockFile=True
```

See Customizing Receiver Using Configuration Files for information about how updates to particular configuration files affect different users.

The makes Receiver behave as if you answered “Yes” to the message each time. Note that Receiver will still detect contention with other instances of itself.

However, if you want Receiver to detect contention with other programs, such as SynCE, use ls -ld on the directory given in the error message, for example, /var/lock. This probably shows that writing is restricted to members of a group such as uucp or lock, in which case either:

- As root, set the group ownership of the Receiver executable to match this group, for example by typing:

  ```
  chgrp uucp $ICAROOT/wfica
  ```

  Set the group id when Receiver executes by typing:

  ```
  chmod g+s $ICAROOT/wfica
  ```

  This enables Receiver to assume the rights it needs while manipulating the lockfiles. At other times, it will suspend those extra rights.

- Add each user who needs to connect to Pocket PCs to this group (for example, by editing /etc/group as root). This may be particularly appropriate on machines running Gentoo Linux.

Common Error Messages

The following list of errors is not comprehensive. The list is intended to provide descriptions for more commonly occurring error messages.

Connection Configuration Errors

These errors may 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 may occur if you edited wfclient.ini incorrectly.

E_CSM_MUST_SPECIFY_SERVER - You must enter a server.

A server name must be entered on the Network page of the Properties dialog box.

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_CSM_CONNECTLIST_INVALID - Cannot find selected connection.

The configuration file is corrupt. Create a new configuration file.

E_CSM_CONNECTION_NOTFOUND - Cannot find selected connection.

The configuration file is corrupt. Create a new configuration file.

E_CSM_APPSERVERLIST_MISSING - Verify the configuration file "...". Section "..." is missing. Create a new configuration file.

The configuration file is corrupt. Create a new configuration file.

E_CSM_APPSRV_SECTION_MISSING - Verify the configuration file "...". Section "..." is missing. Create a new configuration file.

The configuration file is corrupt. Create a new configuration file.

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.

E_CSM_DESCRIPTION_NONUNIQUE - The Description must be unique. This description is already in use.

The Description text on the Network page of the Properties dialog box must be unique.

Drag and Drop Errors

These errors may occur when using drag and drop to open a file.

Cannot read file "...".

Check the permissions on file “...”.

Cannot open file "...". The file is located on a drive that is not accessible by remote applications.

Check the mappings on the Drive Mapping page of the Settings dialog box.

No file type association. There is no application associated with the file type: "...".

If you are using static file type associations, check these using the File Associations page of the Properties dialog box for each connection that connects to a published application. If you are using dynamic file type associations, either connect to another server that offers an application associated with the type of file “...”, or switch to using static file type associations and set the association up manually.

The server you selected does not have any file type associations defined. Contact your help desk for assistance.

Contact your help desk for assistance.

Cannot find an application for file "..." because it does not have a file extension.

Rename file “...” to have a suitable extension.

Cannot access the file "...". The file is on a drive-mapped file system that is currently disabled. Enable drive mapping to the drive where the file is located.

Check the relevant drive mapping is enabled on the Drive Mapping page of the Settings dialog box.

Client drive aapping is disabled.

Please enable client drive mapping before running applications.

PAC File Errors

These errors may occur when using 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.

Please contact your help desk with the following information: Cannot browse NDS tree: "...".

Contact your help desk, providing details of this error message.

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.

Cannot access this PDA device. This PDA device is currently in use.

If this message appears, a server application failed to access a USB-tethered Pocket PC because it is already being accessed either by a server application in another ICA session or by a local application. You can release the PDA for use by closing any other synchronization agent that is currently running. If this does not fix the problem, contact your system administrator.

Do you want to allow a remote application to access your local PDA device? Allowing a remote application to access your device is potentially unsafe.

If you explicitly connect to a server or to a server application that tries to access your local Pocket PC, either through Citrix XenApp or through the Connection View, access is permitted automatically. However, if you are directed to a server without knowing the server details (for example, using the Web Interface or through an ICA file), this message appears to warn you if an application wants to access the PDA. You then have the option to allow or deny the access.

Sending Diagnostic Information to Citrix Support

If you are experiencing problems using Receiver, you may be asked to provide Citrix Support with diagnostic information. This information assists Citrix Support in trying to diagnose and offer assistance in rectifying the problem.

To obtain diagnostic information about Receiver

1. On the Help menu of the main Receiver window, click Diagnostic Information. The Diagnostic Information dialog box displays the current locations of ICAROOT and wfcmgr.

2. Click Yes to generate a file containing detailed diagnostic information, including version details, the contents of Receiver's configuration files, and the values of various system variables. Check this file for confidential information before sending it to Citrix Support.

Receiver for Linux Command-Line Parameters

The table below lists Receiver for Linux command-line parameters.

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

Note: A list of the parameters can be obtained by typing wfica -?, wfica -help, or wfica -h at a command line.

To	Type
Specify the connection to use from the Connection file.	`-desc` *`description`*
Specify the connection to use from the Connection file.	`-description` *`description`*
Specify a Connection file. This enables the use of an alternative appsrv.ini.	`-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 dialogs.	`-quiet`
Turn off the splash screen.	`-nosplash`
Log connection process.	`-log`

Enable keyword 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 for each drive to be overridden. For the override to work, there must be an existing mapping, though it need not be enabled.	`-drivemap` *`string`*
Associate document with published application.	`-associate`
Only launch the associated published application. Do not open the document.	`-launchapponly`

Tip: All wfica command line options can also be specified in the environment variable WFICA_OPTS, allowing them to be used with wfcmgr and the Web Interface.