Citrix Receiver™ for Linux Administrator’s Guide

Citrix Receiver™ for Linux, Version 11.*x*

Copyright and Trademark Notice

Trademark Acknowledgements

Contents

1 **Before You Begin 11**

Who Should Use This Guide 11

New Name for the Client for Linux 11

New Names for Citrix Presentation Server Components. 11

Citrix Receiver for Linux Overview. 12

Finding Documentation. 12

Documentation Conventions 12

Getting Support and Training 13

New Features Introduced in Version 11.x 13

Font Smoothing (ClearType). 13

SpeedScreen Multimedia Acceleration. 14

Multilingual Installation Support 14

Special Folder Redirection 14

User-driven Desktop Restart 14

USB Support 14

Support for Kerberos Authentication 15

Existing ICA Features Supported for Connections to XenDesktop. 15

2 **Deploying the Citrix Receiver for Linux 17**

Overview 17

System Requirements 17

SpeedScreen Multimedia Acceleration. 18

User Requirements 18

Installing the Citrix Receiver for Linux 18

Installing the Citrix Receiver for Linux from the Web. 19

Installing the Citrix Receiver for Linux from a .tar file or CD. 19

Starting the Citrix Receiver for Linux 20

To start the client at a UNIX prompt. 20

To start the client from the Linux desktop 21

Uninstalling the Citrix Receiver for Linux. 21

To uninstall the client 21

Modifying and Repackaging the Citrix Receiver for Linux 21

To modify the client package 22

Using the Citrix Receiver for Linux as an "ICA to X Proxy" ("Server Side ICA") 23

Supported Features 24

Starting the Citrix Receiver for Linux with "Server Side ICA". 24

Supporting Faster Browsing 25

3 Creating and Managing Connections. 27

Overview 27

Creating Connection Entries. 27

To create a connection. 27

Viewing Connection Entries. 28

To view the published resources on a server running the Web Interface. 29

To view the connections that were created from the client 30

Opening a Connection. 30

To open a connection from the main client window. 30

To open an application from the Citrix XenApp view 30

To open a connection from a command line. 31

To open a connection using a Web browser 31

Managing Your Connections 32

To access the Connection Center 32

To manage a connection window 32

To view information about a session. 33

4 Configuring Connections. 35

Overview 35

Customizing the Client Using Configuration Files 36

Configuring Default Connection Settings 37

To change the default settings 37

Configuring Keyboard Options, Alert Sounds, and Digital Dictation Support 38

Configuring Default Window Settings 39

Configuring Network Protocol 39

Configuring ICA Browsing 40

Configuring Keyboard Shortcuts. 41

Changing Settings for the Disk Cache 43

Configuring Auto Client Reconnect 44

Configuring Individual Connection Settings 44

To change the properties for a connection entry. 44

Configuring Network Properties 45

Improving Performance over a Low-Bandwidth Connection 46
Improving Multimedia Performance. 49
Configuring Middle Button Paste Functionality. 50
Configuring Digital Dictation Support 50
Changing the Window Properties 50
Specifying an Application to Run at Connection 52
Configuring Logon Properties. 52
Changing Auto Client Reconnect Settings 53
To change the auto client reconnection settings for a connection entry. 53
Configuring File Type Associations. 54
To configure the client to use static or dynamic file type associations 55
To set up static file type associations 55
Configuring Special Folder Redirection 56
Setting up Extended Parameter Passing 57
Configuring ClearType Font Smoothing 59
Integrating the Clients for UNIX with CDE. 59
Integrating the Citrix Receiver for Linux with KDE and GNOME. 60
Setting up Server-Client Content Redirection 60
To enable server-client content redirection for Version 11.*x* clients if RealPlayer and a browser are not in the UNIX path 61
To enable server-client content redirection for Version 8.*x* clients if RealPlayer and a browser are not in the UNIX path 62
To enable server-client content redirection for Version 6.30 clients if RealPlayer and a browser are not in the UNIX path 63
To turn off server-client content redirection from the client 63
Using xcapture. 63
To start xcapture from the command line 64
To start xcapture from the main client window 64
To copy from the UNIX desktop 64
To copy from xv to an application in a connection window 64
To copy from an application in the connection window to xv .65

5 Mapping Client Devices 67

Overview 67
Mapping COM Ports. 67
To configure COM port mapping 67
Mapping Client Drives 68
To specify drives and directories to automatically map during logon 68
To view mapped client drives when connected to a Windows server 69
To manually map a client drive on a Windows server 70

To configure drive mapping for floppy disks 71
Mapping Client Printers 72
To set an autocreated printer 72
To autocreate non-default printers for the Citrix Receiver for Linux 73
To limit the list of printers configured on the client and mapped for use from an ICA session 73
Mapping Client Printers on XenApp for Windows 74
Mapping Client Printers on XenApp for UNIX 75
Mapping Client Audio 75
To configure audio mapping for a connection entry. 76
To set a non-default audio device 76

6 Configuring Citrix XenApp 77

Overview 77
Publishing Content 78
Customizing Users' Citrix XenApp Options 78
Limiting the Degree of Desktop Customization Available to Users 79
Specifying the Server Running the Web Interface 79
Specifying a Logon Method 80
Customizing Desktop Access to Published Resources 81
To customize the KDE or GNOME desktop on the client 81
Configuring Workspace Control. 82
To configure workspace control settings on the client 83
Configuring Session Options 84
To configure session option settings on the client 84
Supporting NDS Users 85
To use NDS if the tree name is not in DNS 85

7 Securing Client Communication. 87

Overview 87
Connecting through a Proxy Server 87
Using Auto-Client Proxy Detection 88
Connecting through a SOCKS Proxy Server 88
Connecting through a Secure Proxy Server 89
Configuring Automatic Proxy Detection 90
Using the Secure Gateway or Citrix SSL Relay. 91
To specify a default Secure Gateway server 92
To specify a Secure Gateway for a server connection 92
To use configuration files to specify a Secure Gateway server 93

Configuring and Enabling the Client for SSL and TLS 93
Connecting to a Server through a Firewall 95
To connect across an address-translating firewall 95
Using ICA Encryption 96
To change the encryption settings 96
Enabling Smart Card Support 96
To configure smart card support 97

8 Troubleshooting 99
Overview 99
Known Issues 99
Connection Issues 99
Display Issues 101
Browser Issues 106
Other Issues 108
Common Error Messages 112
Connection Configuration Errors 112
wfclient.ini Configuration Errors 112
Drag and Drop Errors 113
PAC File Errors 114
Other Errors 115
Sending Diagnostic Information to Citrix Support 116
To obtain diagnostic information about the client 116

Appendix A Citrix Receiver for Linux Command-Line Parameters 117
Citrix Receiver for Linux Command-Line Parameters 117

Index. 119

Before You Begin

Who Should Use This Guide

This guide is for system administrators responsible for installing, configuring, deploying, and maintaining the Citrix Receiver for Linux. This guide assumes knowledge of the following:

- Citrix XenApp
- Citrix XenDesktop
- The operating system on the client device
- Installation, operation, and maintenance of network and asynchronous communication hardware, including serial ports and device adapters

This guide also contains information and procedures that may assist end users of the clients (referred to as “users” in contrast to “administrators”) in their day-to-day use of the software.

New Name for the Client for Linux

Citrix Receiver for Linux is the new name for the Client for Linux. Throughout the product documentation you may still see references to both the Client for Linux and the Clients for UNIX. These refer to either earlier versions of the client or versions of the client designed for other UNIX operating systems.

New Names for Citrix Presentation Server Components

Citrix XenApp is the new name for Citrix Presentation Server. The following clients and components have been updated to reflect that product name:

- *Citrix XenApp Plugin for Hosted Apps* is the new name for the plugin for server-side virtualization (formerly named Citrix Presentation Server Clients for Windows), which contains the following plugins:
  - *Citrix XenApp*, formerly named the Program Neighborhood Agent

  - *Citrix XenApp Web Plugin*, formerly named the Web Client

- *XenApp Web sites* is the new name for access platform sites
- *XenApp Services sites* is the new name for Program Neighborhood Agent Services sites

Citrix Receiver for Linux Overview

The Citrix Receiver for Linux provide users with access to resources published on XenApp or XenDesktop servers. The clients combine ease of deployment and use, and offer 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.

User 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.

Finding Documentation

Read_Me_First.html and Welcome.html, which are included on the XenApp and XenDesktop installation media respectively, contain links to documents that will help get you started. They also contains links to the most up-to-date product documentation for XenApp/XenDesktop and their components, plus related technologies.

The Citrix Knowledge Center Web site, http://support.citrix.com/, contains links to all product documentation, organized by product. Select the product you want to access and then click the **Documentation** tab from the product information page.

For information about the features supported by the different plugins or clients, refer to the *Client Feature Matrix* at http://support.citrix.com/article/CTX104182.

Information about known issues is included in the product readme.

Documentation Conventions

For consistency, Windows Vista and Windows Server 2008 (64-bit) terminology is used throughout the documentation set; for example, “Documents” rather than “My Documents” and “Computer” rather than “My Computer” are used.

Citrix XenApp and XenDesktop documentation uses the following typographic conventions.

Convention	Meaning
Boldface	Commands, names of interface items such as text boxes, option buttons, and user input.
Italics	Placeholders for information you provide. For example, *filename* means you type the actual name of a file. Italics are also used for new terms and titles of books.
`Monospace`	Text displayed in a text file.
{braces}	In a command, a series of items, one of which is required. For example, {**yes** | **no** } means you must type yes or no. Do not type the braces themselves.
[brackets]	In a command, optional items. For example, [/**ping**] means that you can type /**ping** with the command or you can omit it. Do not type the brackets themselves.
| (vertical bar)	In a command, a separator between items in braces or brackets. For example, { **/hold** | **/release** | **/delete** } means you must type **/hold** or **/release** or **/delete**.
... (ellipsis)	The previous item(s) in the command can be repeated. For example, /route:*devicename*[,…] means you can type additional device names, separated by commas.

Getting Support and Training

The Citrix Knowledge Center (http://support.citrix.com/) offers a variety of technical support services, tools, and developer resources.

For information about Citrix training, see http://www.citrix.com/edu/.

New Features Introduced in Version 11.x

The following new features have been introduced in version 11.x of the Citrix Receiver for Linux.

Font Smoothing (ClearType)

Provides an implementation of sub-pixel font rendering, which improves the quality of displayed fonts, compared to traditional forms of font smoothing or anti-aliasing. Sub-pixel font rendering technology is particularly useful on Liquid Crystal Display (LCD) screens. You can configure this feature through the Citrix Receiver for Linux configuration files. You can turn off this feature for environments that have low network bandwidth.

SpeedScreen Multimedia Acceleration

Overcomes the need for the high bandwidths required to provide multimedia playback on virtual Windows desktops and published applications running on UNIX-based endpoints.

Multilingual Installation Support

Displays the Citrix Receiver for Linux installation scripts in the local language, as defined by the LANG environment variable on the endpoint. English, German, and Japanese are automatically detected; any other languages default to English.

Special Folder Redirection

Enables administrators to specify the locations of a user’s “special folders” on the local file system of the users computer. In this context, the special folders are the user’s Desktop folder and the Documents folder. This feature ensures that users who connect to different XenApp servers, possibly in different server farms, have their special folders redirected consistently.

User-driven Desktop Restart

In the same way that users of physical computers can restart them by pressing the power button, XenDesktop users can restart virtual desktops running on virtual machines (VMs) accessed using the Citrix Receiver for Linux. This feature is available only for virtual desktops running on XenServer, Microsoft Hyper-V, or VMware hypervisors; user-initiated restarting of virtual desktops running on physical servers or blades is not supported.

USB Support

Provided by a separately installable module that enables users to interact with a wide range of USB devices when connected to a XenDesktop session. If enabled, users can plug a USB device into their client endpoint and that device is remoted to their virtual desktop. Devices available for remoting include USB 1.1 and USB 2.0 devices, Flash drives, Smartphones, PDAs, printers, scanners, MP3 players, security devices, tablets, and Bloomberg keyboards.

For a complete list of supported devices and details of how to install and configure this feature, refer to the document *Installing and Configuring USB Support*.

Support for Kerberos Authentication

Integration with Kerberos offers enhanced security for pass-through authentication. Rather than sending user passwords over the network, pass-through authentication uses Kerberos authentication. Kerberos is an industry-standard network authentication protocol.

Existing ICA Features Supported for Connections to XenDesktop

The following standard ICA features are supported for connections to XenDesktop:

- SpeedScreen Image Acceleration
- SpeedScreen Browser Acceleration
- Endpoint device drive, LPT, and COM port mapping
- Printing using the Universal Printer Driver
- SecureICA
- Bi-directional audio, when connecting to Windows XP virtual desktops, but not to Windows Vista virtual desktops

Deploying the Citrix Receiver for Linux

Overview

This chapter describes how to install, deploy, and remove the Citrix Receiver for Linux.

Topics covered in this chapter include:

- “System Requirements” on page 17
- “User Requirements” on page 18
- “Installing the Citrix Receiver for Linux” on page 18
- “Starting the Citrix Receiver for Linux” on page 20
- “Uninstalling the Citrix Receiver for Linux” on page 21
- “Modifying and Repackaging the Citrix Receiver for Linux” on page 21
- “Using the Citrix Receiver for Linux as an “ICA to X Proxy” (“Server Side ICA”)” on page 23
- “Supporting Faster Browsing” on page 25

System Requirements

The Citrix Receiver for Linux supports Red Hat 7.1 or above, and other distributions that include the standard C library, glibc, Version 2.2.2 and above. The client also requires OpenMotif 2.3.1.

Systems running the clients require the following:

- 6MB of free disk space for the installed client and up to 13MB if you expand the installation package on the disk
- Sixteen color video display or higher

- TCP/IP networking

SpeedScreen Multimedia Acceleration

To use the SpeedScreen Multimedia Acceleration feature, you must install GStreamer, an open-source multimedia framework, before you install the client. During installation, you then have the option of specifying that GStreamer is enabled for multimedia acceleration.You can download GStreamer from http://gstreamer.freedesktop.org.

Note: 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.

User Requirements

Although you do not need to log on as a privileged (root) user to install the clients, the desktop integration feature is enabled only if you are logged on as a privileged user when installing and configuring the clients. Installations performed by non-privileged users will, however, enable users to access published resources on the server using the Web Interface through one of the supported browsers.

Installing the Citrix Receiver for Linux

Before installing the client, ensure that you have at least 13MB of free disk space available. Depending on your UNIX platform, you can check the available disk space with one of the following commands:

```
df -k <ENTER>
```

```
df <ENTER>
```

```
bdf <ENTER>
```

Note: If you are using the Web Interface in conjunction with Citrix XenApp, see the *Citrix Web Interface Administrator's Guide* for information about deploying the Citrix Receiver for Linux with the Web Interface.

Installing the Citrix Receiver for Linux from the Web

You can download the Citrix Receiver for Linux in Red Hat Package Manager (RPM) format from the Citrix Web site. RPM packages are generally easier to use than .tar files, but give you no control over the location of the installed files.

If changing the location of the installation is necessary in your environment, install the client from a file that is distributed using an alternative, non-RPM, format as described in the following procedure. You can download both packages for the Citrix Receiver for Linux (and compressed installation files in other formats) from the support pages of the Citrix Web site (http://www.citrix.com/).

Installing the Citrix Receiver for Linux from a .tar file or CD

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).

To install the client

1. (Optional) If you want to enable the desktop integration feature, log on as a privileged user (root) at the client workstation. All other features of the client are installed for your personal use only if you log on as a non-privileged user.

2. Open a command window.

3. Uncompress the .tar file and extract the contents into a temporary directory. For example, for Linux platforms, type:

   tar xvfz *packagename*.tar.gz

   For other platforms, type:

   zcat *packagename*.tar.Z | tar xvf -

4. Do one of the following:

   - Run the setup program by typing **./setupwfc** and press ENTER.

   - If file names on the CD are displayed in uppercase and are followed by other characters (such as ;1), use the command `./setupwfc*` and press ENTER.

   A list of setup options appears.

5. Type **1** (Install Citrix Receiver for Linux 11.x) and press ENTER.

The installation procedure prompts:

```
Please enter the directory in which Citrix Receiver for Linux
is to be installed [default /usr/lib/ICAClient] or type "quit"
to abandon the installation:
```

6. Type the path and name of the required installation directory (and press ENTER) or press ENTER to install in the default location.

   If you do not accept the default, you must also specify the installation directory in the environment variable ICAROOT after installation.

7. When prompted to proceed, type **y** and press ENTER.

   The installation procedure displays the Client Software License Agreement and then prompts you for confirmation.

8. Type **1** 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**.

9. If you have KDE or GNOME installed, you can choose whether to integrate them with the client. To integrate the client with KDE or GNOME, type **y** at the prompt.

10. If you have previously installed GStreamer, you can choose whether to integrate GStreamer with the client and so provide support for SpeedScreen Multimedia Acceleration. To integrate the client with GStreamer, type **y** at the prompt.

11. When the installation is complete, the main installation menu appears again. To exit from the setup program, type **3** and press ENTER.

Required post-installation step

If you did not accept the default installation directory in step 6, you must specify full path and name of the installation directory in the environment variable ICAROOT.

Starting the Citrix Receiver for Linux

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

If the client 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 the client at a UNIX prompt

At the UNIX prompt, type ***/usr/lib/ICAClient/*****wfcmgr** and press ENTER (where */usr/lib/ICAClient* is the directory in which you installed the client).

The main client window appears.

To start the client from the Linux desktop

You can start the client 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 the client from the menu. The client 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 the client. The main client window appears.

Uninstalling the Citrix Receiver for Linux

To uninstall the client

1. Run the setup program by typing ***/usr/lib/ICAClient/*****setupwfc** and press ENTER.
2. To remove the client, type **2** and press ENTER.

Modifying and Repackaging the Citrix Receiver for Linux

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

To modify the client package

1. Expand the client package file into an empty directory. The package file is called *platform-major.minor.build*.tar.gz (for example, linuxx86.11.0.*nnnn*.tar.gz for the Linux/x86 platform).
2. Make the required changes to the client package. For example, you might want to add some connection definitions so that each installation of the client 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 client installation. See “Configuring and Enabling the Client for SSL and TLS” on page 93 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 the client package file, for example:

```
tar czf ../newpackage.tar.gz *
```

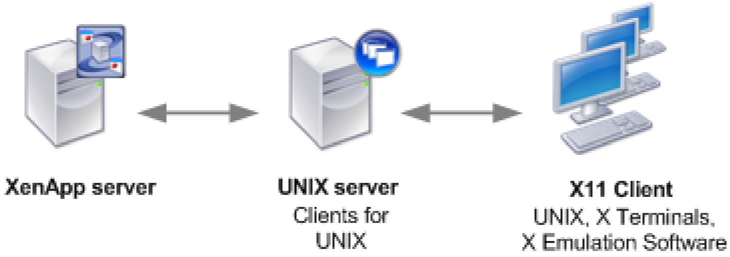
where *newpackage* is the name of the new client package file.

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

You can use a workstation running the client 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 a client is not available. Note that client software is available for many X devices, and installing the software on these devices is the preferred solution in these cases.

Note: The Client for Solaris and the Client for Linux Version 9.*x* and later include support for Sun Ray devices.

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



This graphic shows a system where the Citrix Receiver for Linux are set up as ICA to X proxies.

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

- If you have X terminals already, you can run the client on the UNIX server that usually supplies the X applications to the X terminals.

- If you want to deploy UNIX workstations for which a client is not available, you need an extra UNIX 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.

Starting the Citrix Receiver for Linux with "Server Side ICA"

To start the ICA session from an X terminal or a UNIX workstation

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

   setenv DISPLAY <*local*:0>
3. At a command prompt on the local device, type:

   xhost <*proxy server name*>
4. If the client 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 the client is installed. At a command prompt, type:

wfcmgr &

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

Supporting Faster Browsing

When using Microsoft Internet Explorer with Version 7.*x* or later of the client, this browser's performance with graphically rich pages or large JPEG and GIF images is improved using SpeedScreen Browser Accelerator and ThinImage functionality. For this feature to function correctly, ensure that the client device's installation includes the libjpeg.so JPEG library. This library is built into the Client for Solaris and 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. On the Linux platform, browsers still operate in the absence of this library, but SpeedScreen Browser Accelerator does not function.

Creating and Managing Connections

Overview

This chapter describes how to create and manage connections between the Citrix Receiver for Linux and XenApp servers.

Topics in this chapter include:

- “Creating Connection Entries” on page 27
- “Viewing Connection Entries” on page 28
- “Opening a Connection” on page 30
- “Managing Your Connections” on page 32

Creating Connection Entries

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.
- A connection to a *published application* lets a user access a predefined application and its associated environment. Published applications can be run in seamless mode, where the applications appear to the client as if they are running locally, each application running in its own resizable window.

To create a connection

1. Start the client. See “Starting the Citrix Receiver for Linux” on page 20 for more information about starting the client.
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 main client window.

   If you select a server or published application from the list, a default description is added automatically.

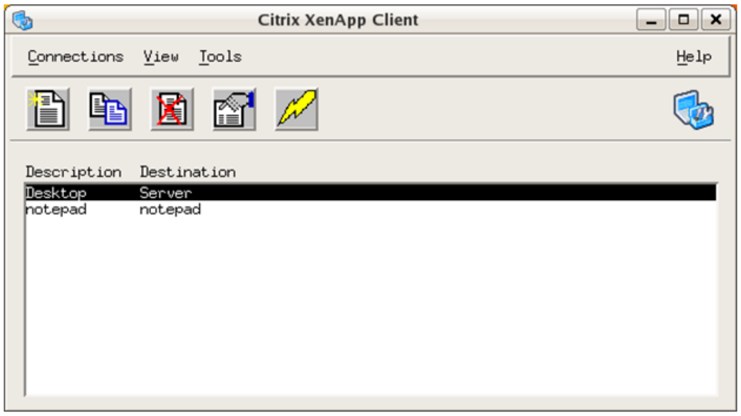
6. Click **OK** to save the entry. Alternatively, to save your changes but retain the current page, click **Apply**.

After you create a connection entry with the appropriate network connection properties set up, the description appears in the main client window.

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 change some of the other properties for a connection; for example, the window size or color settings. See "Changing the Window Properties" on page 50.

Viewing Connection Entries

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



Description	Destination
Desktop	Server
notepad	notepad

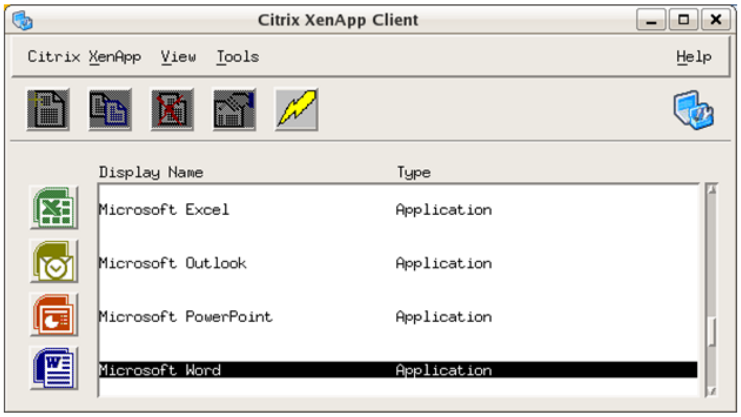
This screen capture shows the Connection view of the main client window, which lists the connection entries users create, by description and server name.

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 the published resources on a server running the Web Interface

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

A list of resources on the server appears:



Display Name	Type
Microsoft Excel	Application
Microsoft Outlook	Application
Microsoft PowerPoint	Application
Microsoft Word	Application

This screen capture shows the Citrix XenApp view of the main client window, which lists the published resources available to the user, by name and type.

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

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

For more information about the publication process, see the *Citrix XenApp for Windows Administrator’s Guide* or the *Citrix XenApp for UNIX Administrator’s Guide*.

To view the connections that were created from the client

On the **View** menu, click **Connection View**.

Opening a Connection

Users can connect to servers in a number of ways:

- From the main client window (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
- From a command line
- From a Web browser

To open a connection from the main client window

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:

/usr/lib/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 UNIX.

Note: If users cannot connect to a server, administrators may need to change the server location or SOCKS proxy details. See "Configuring ICA Browsing" on page 40 and "Connecting through a Proxy Server" on page 87 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 client 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:

   - For Version 6.0 and Version 6.3 clients:

     ```
     application/x-ica; /usr/lib/ICAClient/wfica -file %s; x-
     mozilla-flags=plugin:Citrix ICA
     ```

     The %s indicates that the full file name of the .ica file is passed to the application. The additional text in the .mailcap file is to make use of the Netscape plug-in.

   - For Version 8.*x* and later clients:

     ```
     application/x-ica; /usr/lib/ICAClient/wfica.sh %s;
     x-mozilla-flags=plugin:Citrix ICA
     ```

2. The MIME file modification is:

   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.

4

Configuring Connections

Overview

This chapter describes how administrators can configure connections between the Citrix Receiver for Linux and XenApp servers. It covers both changing the default settings for all connections, and changing the settings for individual connections.

It also contains procedures that support typical tasks performed by users of the clients. 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.

Topics in this chapter include:

- “Customizing the Client Using Configuration Files” on page 36
- “Configuring Default Connection Settings” on page 37
- “Configuring Individual Connection Settings” on page 44
- “Improving Multimedia Performance” on page 49
- “Configuring File Type Associations” on page 54
- “Configuring Special Folder Redirection” on page 56
- “Setting up Extended Parameter Passing” on page 57
- “Configuring ClearType Font Smoothing” on page 59
- “Integrating the Clients for UNIX with CDE” on page 59
- “Integrating the Citrix Receiver for Linux with KDE and GNOME” on page 60
- “Setting up Server-Client Content Redirection” on page 60
- “Using xcapture” on page 63

Customizing the Client Using Configuration Files

You can update many common client settings using the user interface; however, to change more advanced or less common settings, you can modify the client configuration files as described in some of the procedures in this guide. These configuration files are read each time you launch a connection. You can update various different files depending on the effect you want the changes to have.

Important: From Version 10.x of the client, 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 users of the client. If you want the changes to apply to all users of a client installation, modify the module.ini configuration file in the $ICAROOT/config directory.

Applying changes to new users of the client. If you want the changes to apply to all future new users of the client, 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 the client, 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 Default Connection Settings

This section describes how to configure settings that apply to all connection entries on the workstation. These settings are also used as defaults for any new connections that users create. You may want, for example, to customize the default window size if you prefer all new connections to appear in larger or smaller windows than the original setting.

To change the default settings

Note: In Version 7.x and later of the client, you access the **Settings** dialog box from the **Tools** menu in the main client window. In earlier versions, you access this dialog box from the **Option** menu.

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 Keyboard Options, Alert Sounds, and Digital Dictation Support” on page 38.
- The **Window** page, where you specify the window settings to use for all new connection entries. See “Configuring Default Window Settings” on page 39.
- The **Server Location** page, where you specify the server address for the server that will report the data collector. See “Configuring ICA Browsing” on page 40.
- The **Keyboard Shortcuts** page, where you define alternative key combinations for system keyboard shortcuts. See “Configuring Keyboard Shortcuts” on page 41.
- The **Disk Cache** page, where you define settings for the disk cache. See “Changing Settings for the Disk Cache” on page 43.
- The **Drive Mapping** page, where you set up drive mappings. See “Mapping Client Drives” on page 68.

- The **COM Ports** page, where you configure COM port mapping. See "Mapping COM Ports" on page 67.
- The **Firewall** page, where you configure firewalls and a SOCKS proxy. See "Connecting through a Proxy Server" on page 87.
- The **Auto Reconnect** page, where you specify settings for auto client reconnection. See "Configuring Auto Client Reconnect" on page 44.
- The **Citrix XenApp** page, where you identify the server running the XenApp Services site. See "Configuring Citrix XenApp" on page 77.
- The **Secure Gateway** page, where you can specify a Secure Gateway relay server for the client to use when connecting to the server. See "Using the Secure Gateway or Citrix SSL Relay" on page 91.

Configuring Keyboard Options, Alert Sounds, and Digital Dictation Support

To configure the preference settings

1. On the **Tools** menu, click **Settings**.
2. From the drop-down list, choose **Preferences** to display the **Preferences** page.
3. Adjust the settings as required, for example:
   - In the **Keyboard Layout** box, 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.
   - In the **Keyboard Type (Client)** box, 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.

   - In the **Keyboard Type (Server)** box, 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).
   - Select **Enable Windows Alert Sounds** if you want Windows alert sounds to be played using the client device sound system.

- Select **Allow Audio Input** to enable support for client-side microphone input. See “Configuring Digital Dictation Support” on page 50.

Note: You must select **Allow Audio Input** if you want to configure digital dictation support for individual connections.

Configuring Default Window Settings

Use the **Window** page in the **Settings** dialog box to set up the default window settings for all new connection entries. If you want to change the window settings for a specific connection, see “Changing the Window Properties” on page 50.

To configure the default window settings

1. On the **Tools** menu, click **Settings**.
2. From the drop-down list, choose **Window** to display the **Window** page.
3. Adjust the settings as required, for example:
   - **Default Window Size** enables you to select from **Fixed Size**, **Percentage of Screen Size**, or **Full Screen**.
   - **Default Window Colors** enables you to set the number of window colors to **16**, **256**, **32 Thousand**, **16 Million**, or **Automatic**. **Automatic** enables the client to select the best available color depth for the connection. Before selecting a new color mode, ensure that it is supported on your computer. Color settings of greater than 256 colors are available only on Version 6.0 and later clients.
   - **Default 256 Color Mapping** enables you to set up 256 color sessions to use approximate or exact colors. If you select **Private - Exact Colors**, the client will use 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, the client may use a private colormap.

Configuring Network Protocol

The Network Protocol setting enables you to control the way the client searches for servers and how it communicates with them.

To configure a default network protocol

1. In the main client window, select **Settings** from the **Tools** menu.

2. From the drop-down list, choose **Server Location** to display the **ServerLocation** page.
3. Select your required network protocol from the **Network Protocol** list.
4. Click **OK**.

The default protocol for Versions 6.20 or later of the Clients for UNIX is TCP/IP+HTTP. For earlier versions, the default protocol is TCP/IP.

Configuring ICA Browsing

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

TCP/IP+HTTP and SSL/TLS+HTTPS. The default server address is ica. When ICA browsing, the client searches for ica.*domainname*, where *domainname* is one of the default domain names configured for the client. 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 a client sends a request for an application, the data collector responds with the address of a server on which the application is published. The client uses the HTTP or HTTPS protocol to contact servers. TCP/IP+HTTP is supported in Version 6.0 or later; SSL/TLS+HTTPS is supported in Version 6.30 or later.

TCP/IP. The default setting for server location is auto-locate. The client 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 from one to five servers. The client 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** to display the **Server Location** page.
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** to display the **Add Server Location Address** dialog box.
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 the client. 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** and repeat Steps 5 and 6.
8. Click **OK**.

Configuring Keyboard Shortcuts

Alternative keyboard shortcuts are used to control the behavior of the client 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, the client 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.

To configure the keyboard shortcut settings

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: If you are running Linux, it might be necessary to set your client keyboard type to **LINUX** to pass the keyboard shortcuts to remote sessions. See “Configuring Keyboard Options, Alert Sounds, and Digital Dictation Support” on page 38 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. For more information about SpeedScreen settings see “SpeedScreen Latency Reduction” on page 47.

   - 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.

Changing Settings for the Disk Cache

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" on page 46 for details.

To adjust the settings for the disk cache

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.

Note: An administrator can view information about the bitmap cache settings for a server connection using the **Client Cache** tab in the Access Management Console. For more information, see the *Citrix XenApp Administrator's Guide*.

Configuring Auto Client Reconnect

Auto client reconnect enables dropped ICA sessions to be reestablished automatically without users having to reconnect manually or reenter credentials.

Auto client reconnect is enabled on the client by default; no configuration is required on the client device to use these default settings.

For more information about how auto reconnect works and for information about changing the auto reconnect settings for an individual connection, see "Changing Auto Client Reconnect Settings" on page 53.

To change the auto client reconnection default settings

1. On the **Tools** menu, click **Settings**.
2. From the drop-down list, choose **Auto Reconnect** to display the **Auto Reconnect** page.
3. Select the **Enable Auto Reconnect** check box.
4. Enter values for **Maximum Retries** and **Seconds Delay Before Retrying Reconnect**.
5. Click **OK**.

Configuring Individual Connection Settings

This section describes how to change properties for an individual connection entry.

To change the properties for a connection entry

1. In the main client window, 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 "Configuring Network Properties" on page 45.
   - The **Connection** page, where you can control the connection between the server and client; for example, to improve performance by reducing bandwidth. See "Improving Performance over a Low-Bandwidth Connection" on page 46. You can also use the Connection page to configure middle button paste functionality and digital dictation support. See "Configuring Middle Button Paste

Functionality” on page 50 and “Configuring Digital Dictation Support” on page 50.

- The **Firewall** page, where you can specify proxy server settings. See “Connecting through a Proxy Server” on page 87.
- The **Window** page, where you can specify the window size and number of colors used for the ICA session. See “Changing the Window Properties” on page 50.
- The **Application** page, where you can specify an application to run when you connect to the server. See “Specifying an Application to Run at Connection” on page 52.
- 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” on page 52.
- The **Auto Reconnect** page, where you specify settings for auto client reconnection. See “Changing Auto Client Reconnect Settings” on page 53.
- The **Secure Gateway** page, where you can specify a Secure Gateway relay server for the client to use when connecting to the server. See “Using the Secure Gateway or Citrix SSL Relay” on page 91.
- The **File Associations** page, where you can link file types with particular applications. See “Configuring File Type Associations” on page 54.

If you are running Solaris, IBM AIX, or HP-UX, the **File Associations** option is visible by default. If you are running any of the other Clients for UNIX, you have to reconfigure the client to make this option visible. See “Configuring File Type Associations” on page 54 for information about making this option visible.

Configuring Network Properties

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

To change the network properties for a connection entry

1. In the main client window, select the connection entry that you want to change.
2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Network** to display the **Network** page.
4. Adjust the properties as required:

- Enter a description of the connection in the **Description** box.
- To configure a connection to a server, click **Server**. To configure a connection to a 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" on page 40.

Improving Performance over a Low-Bandwidth Connection

If users are using ICA over a low-bandwidth connection, such as a modem or cellular telephone, they can make a number of changes to their client configuration and the way they use the client to improve performance.

- **Change the client configuration.** Changing the configuration of the client, as described below, can reduce the bandwidth that ICA requires and improve performance
- **Change how the client is used.** Changing the way the client is used, described in "Changing How the Client Is Used" on page 49, can also reduce the bandwidth required for a high-performance connection
- **Use the latest versions of XenApp and the Citrix Receiver for Linux.** Citrix continually enhances and improves ICA performance with each release, and many performance features require the latest client and server software

Changing the Client Configuration

On devices with limited processing power or where limited bandwidth is available, there is a trade-off between performance and functionality. The clients provide 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.

Enabling the Disk Cache

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

To enable disk caching

1. In the main client window, select the connection entry that you want to change.

2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Connection** to display the **Connection** page.
4. Select **Use Disk Cache for Bitmaps**.
5. Click **OK**.

You can enable or disable bitmaps for each connection entry so that you can control the connection to each server. Note that only one physical cache is used for all connection sessions that are enabled. See "Changing Settings for the Disk Cache" on page 43.

Data Compression

Data compression reduces the amount of data transferred across the ICA connection. This requires additional processor resources to compress and decompress the data, but it can increase performance over bandwidth-limited connections.

To enable data compression

1. In the main client window, select the connection entry that you want to change.
2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Connection** to display the **Connection** page.
4. Select **Use Data Compression** to reduce the amount of data transferred across the ICA session.

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.

Note: SpeedScreen latency reduction works only if it is available on the server that you are connecting to and only if it is enabled. See the *Citrix XenApp Administrator's Guide* for more details.

To change SpeedScreen latency reduction settings

1. In the main client window, select the connection entry that you want to change.
2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Connection** to display the **Connection** page.

4. In the SpeedScreen section there are two list boxes: **Local Text Echo** and **Mouse Click Feedback**. Local Text Echo accelerates display of the input text, effectively shielding you from experiencing latency on the network. Mouse Click Feedback provides visual feedback of a mouse click, in that the mouse pointer immediately changes to an hourglass indicator. Select a mode for each from the drop-down lists:

   - For slower connections (for example if you are connecting over a WAN or a dial-in connection), set mode to **On** to decrease the delay between user input and screen display.
   - For faster connections (for example, if you are connecting over a LAN), set mode to **Off**.
   - If you are not certain of the connection speed, set the mode to **Auto** to turn SpeedScreen on or off depending on the latency of the connection. You can override Auto mode using the **Toggle SpeedScreen** keyboard shortcut.

Note: Local text echo does not support input using an Input Method Editor.

Reducing the Window Size

Reduce the amount of bandwidth used by changing the window size to the minimum you can comfortably use. See "Configuring Default Window Settings" on page 39 for more information about changing the window size for all connections, or see "Changing the Window Properties" on page 50 for more information about changing the window size for a specific connection.

Modifying Color Depth

Reducing or increasing color depth can improve performance. See "Configuring Default Window Settings" on page 39 for more information about changing the color depth for all connections, or see "Changing the Window Properties" on page 50 for more information about changing the color depth for a specific connection.

The color depth required to achieve optimum performance varies between applications; for example, applications such as Microsoft Word and Internet Explorer that assemble their screen image off screen use less bandwidth when color depth is increased up to a maximum of 32 thousand colors.

Reducing Sound Quality

If you are using sound, reduce the sound quality to the minimum setting or disable client audio mapping. See "Mapping Client Audio" on page 75 for more information.

Changing How the Client Is Used

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

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

SpeedScreen Multimedia Acceleration overcomes the need for the high-bandwidths required to provide multimedia capture and playback on virtual Windows desktops running on UNIX-based endpoints. SpeedScreen Multimedia Acceleration provides a mechanism for playing the media run-time files on the endpoint rather than on the server, thereby reducing the bandwidth requirements for playing multimedia files.

SpeedScreen Multimedia Acceleration 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

To implement this feature, you must install GStreamer, an open-source multimedia framework, on each client that requires multimedia acceleration. Typically, you install GStreamer before you install the client software. This enables you to select the GStreamer option during the installation to ensure that multimedia acceleration is integrated into the client software.

You can download GStreamer from http://gstreamer.freedesktop.org.

Configuring Middle Button Paste Functionality

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

To configure middle button paste functionality

1. In the main client window, 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** to display the **Connection** page.
4. Select the **Enable Middle Button Paste** check box.

Configuring Digital Dictation Support

XenApp supports client-side microphone input. This enables you to publish dictation software for use in client 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 client 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 *Citrix XenApp Administrator’s Guide*.

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.

To configure digital dictation support for a connection entry

1. In the main client window, 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** to display the **Connection** page.
4. Select the **Enable Audio Input** check box and the **Enable Sound** check box.

Changing the Window Properties

You can change the window size, number of colors, and color mapping used for a particular connection.

To configure the window properties

1. In the main client window, select the connection entry you want to change.
2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Window** to display the **Window** page.

- **Window Size** enables you to select from **Fixed Size**, **Percentage of Screen Size**, or **Full Screen**. Select **Fixed Size** or **Percentage** and type the size (in pixels) or percentage in the **Window Size** boxes. If you are connecting to a published application, you can also select **Seamless**. **Seamless** integrates local and remote windows on the desktop. Note that seamless connections to published desktops are not supported.

Note: Because clients support seamless windows natively, it is not necessary to use "pass-through" mode. Pass-through mode is intended to facilitate seamless windows for clients that do not support seamless windows natively, and should only be used from a fixed-size window session on the client device. Note that "seamless within seamless" (that is, seamless windows in pass-through mode) is not a supported configuration.

- **Window Colors** enables you to set the number of window colors to **16**, **256**, **32 Thousand**, **16 Million**, or **Automatic**. **Automatic** enables the client to select the best available color depth for the connection. Your display must be capable of displaying the resolution and color depth you select. Color depths of greater than 256 colors are available only on Version 6.0 and later clients.
- **256 Color Mapping** enables you to set up 256 color sessions to use approximate or exact colors. If you select **Private - Exact Colors**, the client 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**. Note that if other applications allocate all 256 colors, the client may use a private colormap.
- In each case, select **Use Default** to use the default window size or window colors setting. For more information about setting defaults, see "Configuring Default Window Settings" on page 39.

Specifying 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 is closed when you exit the application.

To specify an application to run at connection

1. In the main client window, select the connection entry that you want to change.
2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Application** to display the **Application** page.
   - In the **Application** box, specify the pathname of an application to be run after connecting to a server
   - In the **Working Directory** box, specify the pathname of a directory to be used 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 the logon details for your server connection so that you do not need to type them each time you connect.

To configure logon properties

1. In the main client window, select the connection entry that you want to change.
2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Login** to display the **Login** page.
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 clients, see "Enabling Smart Card Support" on page 96.

Changing Auto Client Reconnect Settings

ICA sessions can be dropped because of unreliable networks, highly variable network latency, or range limitations of wireless devices. Auto client reconnect is triggered when a client detects a disconnected session. When this feature is enabled on servers, users do not have to reconnect manually or reenter logon credentials to continue working. Automatic reconnection does not occur if users exit applications.

When a reconnection sequence begins, the user is informed that the client will reconnect after a set interval. Reconnection requires no action by users, although they can choose to cancel the process or reconnect immediately. Because session drops may be caused by network instability, users must wait a few moments before reconnecting to give the network time to recover from the problem that caused the disconnection.

When the client detects that its connection to the server is unexpectedly broken, it waits for a maximum of 36 seconds before beginning the reconnection sequence. By default, the client attempts to reconnect three times and then, if unsuccessful, it stops. To change the default number of attempts, or other auto client reconnect default settings, see “Configuring Auto Client Reconnect” on page 44.

To change the auto client reconnection settings for a connection entry

1. In the main client window, select the connection entry that you want to change.
2. On the **Connections** menu, click **Properties**.
3. From the drop-down list, choose **Auto Reconnect** to display the **Auto Reconnect** page.
4. Select **Enable Auto Reconnect** and, if required, enter values for **Maximum Retries** and **Seconds Delay Before Retrying Reconnect**.
5. Click **OK**.

Configuring File Type Associations

Drag and drop support enables users to open files without knowing which application is needed. The client uses file type association to determine which application on the server to use with particular file types, and automatically opens the associated application. Version 9.x and later clients enable administrators to set this up from the **File Associations** option in the **Properties** drop-down list as described in this section. Users of earlier versions of the client can manually set up file type associations as described in "Setting up Extended Parameter Passing" on page 57.

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). For information about configuring the client to use dynamic or static file type associations, see "To configure the client to use static or dynamic file type associations" on page 55.

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 the client. These file type associations persist between sessions. For information about setting up static file type associations, see "To set up static file type associations" on page 55.

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

- **Dropping files onto the main client 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 client window, the client makes the connection specified in the file, while if a .pnagent file or a .desktop file is dropped on the client window, the client launches the application specified in the file.
- **Dropping files onto the client manager icon.** If a user drops an .ica file onto the client manager icon, the client makes the connection specified in the file. If other file types are dropped onto the client 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, the client responds only if the icon corresponds to a Citrix published resource. For published application icons, the client always uses dynamic file type associations to check whether the file type is supported by the application. If so, the client 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 the client 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 the client 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 the Client Using Configuration Files" on page 36 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 the client to use static file type associations, and True sets the client to use dynamic file type associations.

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

3. Save and close the file.

To set up static file type associations

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** to display the **File Associations** page. Click **Add**.

Note: If the **File Associations** option is not visible, see "To configure the client to use static or dynamic file type associations" on page 55 for information about displaying this option.

5. 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.

6. Click **OK**.
7. Ensure that the published application and file type are associated for content redirection. See the *Citrix XenApp Administrator's Guide* for more information.

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 is a feature that 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 be used as the users's Documents folder and Desktop folder respectively.

   For example:

   ```
   DesktopFolder = $HOME/.ICACLIENT/desktop
   ```

Guidance

- 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 Extended Parameter Passing

Administrators can integrate published applications into desktop environments by associating a file type on a client device with an application published on a server. Version 9.x and later clients enable administrators to set this up from the **File Associations** option in the **Properties** drop-down list. See “Configuring File Type Associations” on page 54 for more information about this method of setting up file type associations.

Users of earlier versions of the client can set up file type associations manually using extended parameter passing as described in this section. Extended parameter passing involves passing command-line parameters from the desktop through the client to start an application published on the server.

Citrix XenApp creates desktop icons automatically for KDE (Version 2.0 and later) and GNOME (Version 2.0 and later). For more information, see “Integrating the Citrix Receiver for Linux with KDE and GNOME” on page 60. Administrators of other UNIX desktop systems may need to create such icons manually as outlined in this section.

The desktop configuration file must be modified as detailed below for each file type association you require. This type of command line enables users to open an associated published application in an ICA session directly from a file in a file management application or directly from a desktop icon.

To make use of this capability from within your window manager, you need to tell the window manager how and when to start the client. The mechanism for doing this varies for different UNIX desktops. See available documentation for your desktop environment.

Administrators need to set up file associations between desktop file name extensions and the appropriate published applications. The client accepts as command-line arguments:

- The name of an ICA file specifying a connection to be made (`$ICAROOT/wfica` *`connection.ica`*)
- A string to be passed unchanged to a published application (`$ICAROOT/wfica -desc` *`application`* `-param` *`string`*)
- The full path of a file to be passed to a published application (`$ICAROOT/wfica -desc` *`application`* `-fileparam` *`filepath`*)

  Note: The file must be one included in one of the client drive mappings for the server to have access to it. From the full file path, the client determines which mapped directory to use and translates the path accordingly.

If necessary, the **-param** and the **-fileparam** options can be repeated to produce a combined string that is passed to the published application. For example:

```
-param "/C " -fileparam "$HOME/src/file" -param " /L:" -fileparam
/tmp/out.log
```

This might pass the following to the application:

```
/C H:src\file /L:T:out.log
```

Note: For the published application to receive the file name passed from the client, the Published Application Manager must specify a command line containing **"%*"**, for example, **D:\WINNT\system32\notepad.exe "%*"** or **"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"**. Note that quotation marks enclose the executable's path in the second example because the path contains a space. For more information about passing parameters to published applications, see the *Citrix XenApp Administrator's Guide*.

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 the client's bandwidth requirements significantly.

Integrating the Clients for UNIX with CDE

During installation, you can choose to integrate the Client for Solaris, IBM AIX, and HP-UX with the Common Desktop Environment (CDE). Integration creates a "Citrix" group in your CDE Application Manager and adds applications to both the front panel and the Personal Applications subpanel.

CDE integration makes it easy for administrators to associate a file type on the client device with an application published on a server. When users open a file in the CDE File Manager, command-line parameters from the desktop are passed to the server through the client to start an application session. Files are displayed in the File Manager with the icon of their associated application. For more information about setting up file type associations, see "To set up static file type associations" on page 55.

Note: For best operation with CDE, set $ICAROOT in $HOME/.profile, unless the client is installed in the default location.

CDE integration also supports MIME types. This enables users to launch an associated published application by opening a file while browsing a directory with Firefox, Mozilla, or Netscape. Users must ensure, however, that the /tmp directory is drive-mapped.

Integrating the Citrix Receiver for Linux with KDE and GNOME

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

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 the client is installed in the default location.

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 an ICA session opens the required file using the browser on the client 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 the client 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 on the client provided that the UNIX path includes RealPlayer and at least one of Firefox, Mozilla, or Netscape.

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

To enable server-client content redirection for Version 11.*x* clients if RealPlayer and a browser are not in the UNIX 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 until content can be displayed successfully:

   - The nslaunch utility is run to push the URL into an existing browser window
   - Each browser in the list is tried in turn
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 enable server-client content redirection for Version 8.*x* clients if RealPlayer and a browser are not in the UNIX path

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

   ```
   Path=path
   Command=command
   PercentS=percentS
   ```

   where *path* is the directory where the browser executable is located, *command* is the name of the executable used to handle redirected browser URLs, appended with `%s`; for example `netscape %s`, and *percentS* is the number of occurrences of `%s` in the `Command` setting.
3. In the [Player] section, modify the following settings:

   ```
   Path=path
   Command=command
   PercentS=percentS
   ```

   where *path* is the directory where the RealPlayer executable is located, *command* is the name of the executable used to handle the redirected multimedia URLs, appended with `%s`; for example `realplay %s`, and *percentS* is the number of occurrences of `%s` in the `Command` setting.

   The default value for `PercentS` is one because the default value for `Command` is `realplay %s`.
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 enable server-client content redirection for Version 6.30 clients if RealPlayer and a browser are not in the UNIX path

1. Open the configuration file wfclient.ini.
2. Modify the following browser settings:

   ```
   CRBrowserPath=path
   CRBrowserCommand=command
   CRBrowserPercentS=percentS
   ```

   where *path* is the directory where the browser executable is located, *command* is the name of the executable used to handle redirected browser URLs, appended with `%s`; for example `netscape %s`, and *percentS* is the number of occurrences of `%s` in the `Command` setting.
3. Modify the following RealPlayer settings:

   ```
   CRPlayerPath=path
   CRPlayerCommand=command
   CRPlayerPercentS=percentS
   ```

   where *path* is the directory where the RealPlayer executable is located, *command* is the name of the executable used to handle the redirected multimedia URLs, appended with `%s`; for example `realplay %s`, and *percentS* is the number of occurrences of `%s` in the `Command` setting.

   The default value for `PercentS` is one because the default value for `Command` is `realplay %s`.
4. Save and close the file.

To turn off server-client content redirection from the client

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

Using xcapture

The client includes a helper application, xcapture, that can assist 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 UNIX 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 ***/usr/lib/ICAClient/*****util/xcapture** and press ENTER (where */usr/lib/ICAClient* is the directory in which you installed the Client for UNIX).

To start xcapture from the main client window

On the **Tools** menu, click **xcapture**.

To copy from the UNIX desktop

1. From the **xcapture** dialog box, click **From Screen**. The cursor changes to a crosshair.
2. To:
   - **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.

Mapping Client Devices

Overview

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

Note: Client device mapping, except for printers, is not supported when connecting to Citrix MetaFrame for UNIX Operating Systems 1.0 and 1.1. Client printer mapping and, with Hotfix 2, client drive mapping are supported when connecting to Version 1.1, Feature Release 1 and later versions of Citrix XenApp for UNIX.

This topic includes the following sections:

- “Mapping COM Ports” on page 67
- “Mapping Client Drives” on page 68
- “Mapping Client Printers” on page 72
- “Mapping Client Audio” on page 75

Mapping COM Ports

You can perform bidirectional mapping of serial devices on the client device (for example, /dev/ttyS0 on Linux) to COM ports on the server. This enables a user at the client workstation to use local devices such as modems, serial printers, and bar-code scanners seamlessly from the applications running on the server.

To configure COM port mapping

1. On the **Tools** menu, click **Settings**.

Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the Option menu, not the **Tools** menu.

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 makes any directory mounted on a client device, including a CD-ROM or a USB memory stick, available to the user during ICA sessions. When a server is configured to allow client drive mapping, users can access their locally stored files, work with them during their ICA sessions, and then save them again either on a local drive or on a drive on the server. For more information about controlling drive mapping on the server, see the *Citrix XenApp Administrator's Guide*.

To specify drives and directories to automatically map during logon

1. On the **Tools** menu, click **Settings**.

Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the **Option** menu, not the **Tools** menu.

2. Choose **Drive Mapping** from the drop-down menu.

   For each drive letter, the **Drive Mapping** list shows the disk or pathname of the UNIX 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. See the *Citrix XenApp Administrator's Guide* for more information about mapping drives.

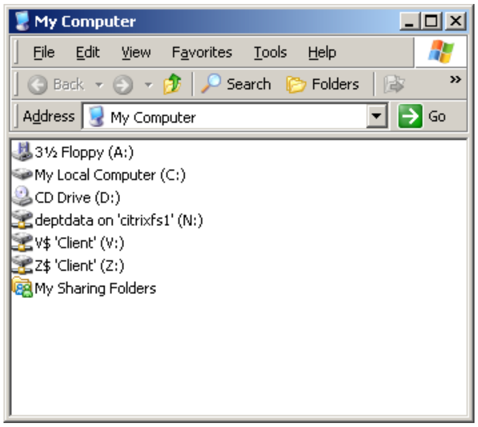
6. Specify the access for the drive by clicking the corresponding read/write icons. You can use:

Icon	**Meaning**
👓 (Pair of glasses)	Read access
👓? (Pair of glasses, with question mark to the right)	Prompt for read access on first access per session
✗ (Pair of glasses, obscured by a cross)	No read access
✏ (Pencil)	Write access
?✏ (Pencil, with a question mark to the left)	Prompt for write access on first access per session
✗ (Pencil, obscured by a cross)	No write access

7. Make sure **Enable Drive Mapping** is selected. 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 view mapped client drives when connected to a Windows server

From the ICA session, double-click My Computer on the remote desktop. The My Computer screen appears:



3½ Floppy (A:)
My Local Computer (C:)
CD Drive (D:)
deptdata on 'citrixfs1' (N:)
V$ 'Client' (V:)
Z$ 'Client' (Z:)
My Sharing Folders

This screen shot shows an example of mapped client drives available when you connect to a Windows server.

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 main client window, 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 UNIX 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 map floppy drives on servers for access within an ICA session. Use the following procedures to manually map floppy drives.

- **SGI IRIX**: DOS formatted floppies mounted automatically by mediad can be accessed in the same way as any other drive. Files can be accessed only through the 8.3 filename convention.
- **Solaris**: On Solaris 2.5.1 or later, DOS formatted floppies mounted on your client device can be accessed either automatically using vold, or by using the volcheck utility. For details about vold and volcheck, and whether your version of Solaris supports them, see your workstation documentation.

  On SunOS 4.1.4 two scripts are provided so DOS formatted floppies mounted on your client device can be accessed. The scripts are located in the client installation directory and are called:

  - mntfloppy - used to mount floppy disks
  - umntfloppy - used to unmount floppy disks

  The scripts are owned by root, but can be run by any user. They use a floppy disk device name of /dev/fd0 and mount the floppy disk to /pcfs. To change these settings, log on as root and edit the script file.

  Long file names are not supported, so save files using the 8.3 file-naming convention.
- **IBM AIX**. DOS formatted floppies on your client device can be accessed using **dosread**, **doswrite**, **dosdir**, **dosformat**, and **dosdel** utilities. For details, see your workstation documentation.
- **HP-UX**. DOS formatted floppies on your client device can be accessed using **doscp**, **dosls**, **dosdf**, **dosmkdir**, **dosrm**, **doschmod**, **dos2ux**, and **ux2dos** utilities. For details, see your workstation documentation.
- **SCO UnixWare or OpenServer**. DOS formatted floppies mounted on your client device can be accessed using the following command:

  ```
  mount -f dosfs /dev/fd0 /floppy
  ```

  Then select the /floppy directory in the **Drive Mapping** dialog box.
- **Linux**. DOS formatted floppies mounted on your client device can be accessed 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

Client printer mapping lets users access spooled printers available to the client device from within ICA sessions. When a server is configured to allow client printer mapping, applications running remotely on the server can print to a spooled printer.

Servers running Citrix MetaFrame XP, Feature Release 3 or more recent versions of XenApp provide a simplified printing setup using the universal printer driver. If the client supports the universal printer driver and is connected to such a server and you can print PostScript output locally, no printer configuration is required.

If you are not connected to a server running Citrix MetaFrame XP, Feature Release 3 or a more recent version of XenApp, you can set a default printer to be available automatically when an ICA session is started; this printer is removed when the session is terminated. This is known as an *autocreated* printer. Published applications often rely on autocreated printers to provide access to a printer because print management utilities may not be available from the application itself.

This section describes how to set an autocreated printer. The printer used by the system is the *default printer* set in the configuration file, although the Citrix Receiver for Linux also allows the autocreation of non-default printers. To ensure that the default printer is available as an autocreated printer, you must specify a Microsoft Windows printer driver for it. If no default printer is set, the UNIX environment variables are searched for default printers; otherwise, the default for the client device print setup is used. The system default printer can be overridden by the LPDEST or PRINTER environment variable in HP-UX, Solaris, and AIX, and the PRINTER environment variable in Linux.

Note: When connecting to servers running Citrix XenApp for UNIX, you do not need to specify a Microsoft Windows printer driver. See the *Citrix XenApp for UNIX Administrator's Guide* for more information.

This section also describes how to limit the number of printers available to clients. This is useful where many printers are available and avoids delays when listing available printers.

To set an autocreated printer

After you define an appropriate printer driver name (as specified by this procedure), the printer configured on the client for autocreation has Auto Created Client printer displayed in its associated comment field on the server.

1. Open a configuration file by doing one of the following:

- Open wfclient.ini, in the $HOME/.ICAClient directory to apply the autocreated printer for a single user
- Open module.ini, in the $ICAROOT/config directory to apply the autocreated printer to all users

2. In the [WFClient] section of the file, edit the following lines:

   ```
   DefaultPrinter=printername (optional)
   ```

   ```
   DefaultPrinterDriver=printerdrivername
   ```

   where *printername* is the name of the chosen UNIX printer and *printerdrivername* is the name of the Microsoft Windows driver for the printer.

3. Save and close the file.

Note: An autocreated printer configuration can be preserved at session termination by changing its comment field in the print management utility before ending the session.

To autocreate non-default printers for the Citrix Receiver for Linux

1. In /etc/printcap, locate the printers that you want to set as the autocreated printers.
2. Add the following option:

   ```
   :wd=drivername\
   ```

   where *drivername* is the name of the driver for the autocreated printer.

Important: The Common UNIX Printing System (CUPS) recreates /etc/printcap at startup. To avoid recreating /etc/printcap at startup, disable this behavior in the CUPS configuration file.

To limit the list of printers configured on the client and mapped for use from an ICA session

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 users of the UNIX clients—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: From Version 10.x of the Clients for UNIX, new entries in wfclient.ini must also be added to the All_Regions.ini configuration file. See "Customizing the Client Using Configuration Files" on page 36 for more information.

3. Save and close the file.

Mapping Client Printers on XenApp for Windows

This section describes how to map client printers on XenApp for Windows. You might need to do this if, for example, the client device's printing software does not support the universal printer driver.

To map a local printer on a server

1. From the client, 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 with a name similar to *printer (from workstation) in session x*.

   Note: When connecting to servers running Presentation Server 3.0 or earlier, or when the server has the Legacy client printers policy rule enabled, the printer name is similar to *workstation#printer*.

See your Windows operating system documentation for more information about adding printers.

Mapping Client Printers on XenApp for UNIX

In a UNIX environment, printer drivers defined by the client are ignored. The printing system on the client 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 about printing from Citrix XenApp for UNIX, see the *Citrix XenApp for UNIX Administrator's Guide* and the man pages.

Mapping Client Audio

Client audio mapping enables applications running on the server to play sounds through a sound device installed on the client device.

On the server, an administrator can set the audio quality and enable or disable client audio mapping. For more information, see the *Citrix XenApp Administrator's Guide*. A user can set the audio quality and enable or disable client audio mapping for an entry from the client device. If the client and server audio quality settings are different, the lower setting is used.

Client Audio Quality options are:

- **High**. This setting is recommended only for connections where bandwidth is plentiful and sound quality is important. This setting enables clients to play a sound file at its native data rate. Sounds at the highest quality level require about 1.3Mbps of bandwidth to play clearly. Transmitting this amount of data can result in increased CPU utilization and network congestion.
- **Medium**. This setting is recommended for most LAN-based connections. This setting causes any sounds sent to the client to be compressed to a maximum of 64Kbps. This compression results in a moderate decrease in the quality of the sound played on the client device. The host CPU utilization decreases compared with the uncompressed version due to the reduction in the amount of data being sent across the wire.
- **Low**. This setting is recommended for low-bandwidth connections, including most modem connections. This setting causes any sounds sent to the client to be compressed to a maximum of 16Kbps. This compression results in a significant decrease in the quality of the sound. The CPU requirements and benefits of this setting are similar to those of the Medium setting; however, the lower data rate enables reasonable performance for a low-bandwidth connection.

To configure audio mapping for a connection entry

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

1. In the main client window, 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 specified as the /dev/dsp file for Linux and the /dev/audio file for Solaris. 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 the Client Using Configuration Files” on page 36 for information about how updates to particular configuration files affect different users.
2. Add the following option, creating the section if necessary:

   ```
   [ClientAudio]
   AudioDevice = /dev/dspN
   ```

   where “dspN” is the entry in /dev that defines the audio device to the operating system.

Note: The HP-UX client uses the **Aserver** daemon; refer to the HP-UX system documentation for the relevant configuration information.

Configuring Citrix XenApp

Overview

This chapter describes how to configure Citrix XenApp (the new name for Program Neighborhood Agent). 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. Although you can view published applications and published content, you cannot view connection entries 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 server running the Web Interface. When a user starts Citrix XenApp, it reads the configuration data from the server. Thereafter, 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.

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

Topics in this chapter include:

- “Publishing Content” on page 78
- “Customizing Users’ Citrix XenApp Options” on page 78
- “Limiting the Degree of Desktop Customization Available to Users” on page 79
- “Specifying the Server Running the Web Interface” on page 79
- “Specifying a Logon Method” on page 80
- “Customizing Desktop Access to Published Resources” on page 81
- “Configuring Workspace Control” on page 82

- “Configuring Session Options” on page 84
- “Supporting NDS Users” on page 85

Publishing Content

Typically, the client connects to applications and desktop sessions. Another use of the client is to 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. Note that published applications and published content (but not connection entries) are together referred to as *published resources*.

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

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

Customizing Users’ Citrix XenApp Options

Use the Web Interface to simplify the customization of users’ Citrix XenApp options through config.xml. For more information, see the *Citrix Web Interface Administrator’s Guide*.

Any changes to config.xml are made available to the clients only after one of the following events takes place:

- A user restarts Citrix XenApp locally.
- A user clicks the **Refresh Settings** button in the **Citrix XenApp** dialog box.
- Configuration refresh takes place automatically, as specified by the server running the Web Interface.

Limiting the Degree of Desktop Customization Available to Users

Depending on the settings that you specify on the server running the Web Interface, you can enable users to customize, from the client, the occurrence and location of menu items and shortcuts for published resources. You can also control which pages of the **Citrix XenApp** dialog box are visible to users, and which are hidden. For information about configuring the options available from the drop-down list in the **CitrixXenApp** dialog box, see the *Citrix Web Interface Administrator's Guide*.

These pages enable users to perform the following tasks:

- The **Server** page enables users to select the server that is used for connections to published resources, and to specify the logon methods to published resources.
- The **Application Display** page enables users to determine how published resources are added to their desktops and menus.

  For the Client for Solaris, this page is available only if the KDE or GNOME desktop environments are installed.
- The **Application Refresh** page enables users to set how often the list of published resources is updated on the client.
- The **Application Reconnection** page enables users to specify how they disconnect from, reconnect to, or log off from applications running on the server. This is known as workspace control.
- The **Session Options** page enables users to specify the window size, color depth, audio quality settings, and how keyboard shortcuts are handled for sessions.

Specifying the Server Running the Web Interface

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

Alternatively, you can use the 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 other servers running the Web Interface.

To change the location of the server on the client

Important: 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 on the server running the Web Interface. For more information about these settings, see the *Citrix Web Interface Administrator’s Guide*.

1. On the **Tools** menu of the main client window, click **Settings**.
2. From the drop-down list, choose **Citrix XenApp** to display the Citrix XenApp page.
3. From the drop-down list, choose **Server** to display the **Server** page.
4. On the **Server** page, click **Change**.
5. 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.

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

Specifying a Logon Method

You can use the 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 the client.

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

To select a logon method for accessing published resources on the client

Important: Before users can choose logon methods, the administrator must decide what logon methods are appropriate and specify these using the 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 server running the Web Interface. For more information about these settings, see the *Citrix Web Interface Administrator's Guide*.

1. On the **Tools** menu of the main client window, click **Settings**.
2. From the drop-down list, choose Citrix XenApp to display the **Citrix XenApp** page.
3. From the drop-down list, choose **Server** to display the **Server** page.
4. Under **Logon mode** on the **Server** page, select the logon method you want to use for all of your connections. Only those supported logon methods that are specified in config.xml appear.
5. Click **OK**.

Customizing Desktop Access to Published Resources

If the server running the Web Interface 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 their client refreshes the list of resources

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

To customize the KDE or GNOME desktop on the client

1. On the **Tools** menu, click **Settings**.
2. From the drop-down list, choose Citrix XenApp to display the Citrix XenApp page. Depending on the content of config.xml, one or more of the five options in the drop-down list on this page—Server, Application

Display, Application Refresh, Application Reconnection, and Session Options—may not be available.

For information about configuring the display the options available from the drop-down list, see the *Citrix Web Interface Administrator's Guide*.

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 the client 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 the client.
   - **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**.

Configuring Workspace Control

Workspace control provides users with the ability to quickly disconnect from all running applications, reconnect to applications, or log off from all running applications. You can move among client 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 a computer running Citrix XenApp. These users can disconnect from multiple applications at one client device and open all the same applications when they reconnect at a different client device.

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

User policies and client drive mappings change appropriately when you move to a new client device. Policies and mappings are applied according to the client device where you are currently logged on to the session. For example, if a health care worker logs off from a client device in the emergency room of a hospital and then logs on to a client device 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.

Administrators can configure the workspace control settings available to users using the Web Interface. If the workspace control settings are configured to enable users to override the server settings, users can configure workspace control using the **Application Reconnection** page in the **Citrix XenApp** dialog box.

If users log on with smart cards, you must set up a trust relationship between the server running the Web Interface and any other server in the farm that the Web Interface accesses for published applications. For more information about workspace control requirements and server configuration, see the *Citrix XenApp Administrator's Guide* or the *Citrix Web Interface Administrator's Guide*.

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

To configure workspace control settings on the client

Important: Before users can change the workspace control settings, the administrator must ensure that the **Application Reconnection** page in the **Citrix XenApp** dialog box is visible, and that the appropriate settings are enabled on the server running the Web Interface. For more information about these settings, see the *Citrix Web Interface Administrator's Guide*.

1. On the **Tools** menu of the main client window, click **Settings**.
2. From the drop-down list, choose **Citrix XenApp** to display the **Citrix XenApp** page.
3. From the drop-down list, choose **Application Reconnection** to display the **Application Reconnection** page.
4. Configure the workspace control settings you want to use for all of your connections.

   The following options are available:

- **Enable automatic reconnection at logon** enables you to reconnect to disconnected applications, or to both disconnected applications and active applications running on another client device, when you log on
- **Enable automatic reconnection from Reconnect menu** enables you to reconnect to disconnected applications, or to both disconnected applications and active applications running on another client device, by clicking **Reconnect Citrix XenApp** on the **Citrix XenApp** menu from the Citrix XenApp view
- **Customize Logoff Button** enables you to configure whether the log off command will include logging you off from applications that are running in the session

5. Click **OK**.

Configuring Session Options

Using the **Session Options** page, you can define the window size, color depth, and sound quality of ICA sessions.

The preferences users set for color depth and sound quality affect the amount of bandwidth the ICA 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 server running the Web Interface are applied to connections from each client.

To configure session option settings on the client

Important: Before users can change the session option settings, the administrator must ensure that the **Session Options** page in the **Citrix XenApp** dialog box is visible, and that the appropriate settings are enabled on the server running the Web Interface. For more information about these settings, see the *Citrix Web Interface Administrator's Guide*.

1. On the **Tools** menu of the main client window, click **Settings**.
2. From the drop-down list, choose **Citrix XenApp**, to display the **Citrix XenApp** page.
3. From the drop-down list, choose **Session Options**, to display the **Session Options** page.
4. 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**

5. 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 client machine. This is provided by the NLDAPsdk package, part of the eDirectory product, and is available from Novell's download page at http://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: From Version 10.*x* of the Clients for UNIX, new entries in wfclient.ini must also be added to the All_Regions.ini configuration file. See "Customizing the Client Using Configuration Files" on page 36 for more information.

3. Save and close the file.

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

Securing Client Communication

Overview

You can integrate the client with a range of security technologies, including proxy servers, firewalls, and SSL/TLS-based systems. This chapter discusses the measures you can take to secure communication between your server farm and the client.

Topics in this chapter include:

- "Connecting through a Proxy Server" on page 87
- "Using the Secure Gateway or Citrix SSL Relay" on page 91
- "Connecting to a Server through a Firewall" on page 95
- "Using ICA Encryption" on page 96
- "Enabling Smart Card Support" on page 96

Connecting through a Proxy Server

Proxy servers are used to limit access to and from your network, and to handle connections between clients and the servers. The client supports the SOCKS protocol, along with the Secure Gateway and Citrix SSL Relay from Version 6.20, the secure proxy protocol from Version 6.30, and Windows NT Challenge/Response (NTLM) authentication from Version 9.x.

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

Using Auto-Client Proxy Detection

If you are deploying clients 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 the client.

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

To configure auto-client proxy detection by default

1. On the **Tools** menu, click **Settings**.

   Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the **Option** menu, not the **Tools** menu.

2. From the drop-down list, choose **Firewall** to display the **Firewall** page.
3. Select **Use Browser settings**.
4. Click **OK**.

To configure auto-client proxy detection for a server connection

1. In the main client window, 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** to display the **Firewall** page.
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 SOCKS Proxy Server

To specify a default SOCKS proxy manually

1. On the **Tools** menu, click **Settings**.

Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the **Option** menu, not the **Tools** menu.

2. From the drop-down list, choose **Firewall** to display the **Firewall** page.
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 main client window, 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** to display the **Firewall** page.
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**.

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 client 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 manually

1. On the **Tools** menu, click **Settings**.

   Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the **Option** menu, not the **Tools** menu.

2. From the drop-down list, choose **Firewall** to display the **Firewall** page.
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 a server connection manually

1. In the main client window, 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** to display the **Firewall** page.
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**.

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 the client to collect it successfully.

To configure automatic proxy detection by default

1. On the **Tools** menu, click **Settings**.

   Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the **Option** menu, not the **Tools** menu.

2. From the drop-down list, choose **Firewall** to display the **Firewall** page.
3. Select **Automatically detect proxy**.
4. Click **OK**.

To configure automatic proxy detection for a server connection

1. In the main client window, 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** to display the **Firewall** page.
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**.

Using the Secure Gateway or Citrix SSL Relay

You can integrate the client with:

- Citrix SSL Relay (Clients for UNIX Version 6.20 and later)
- The Secure Gateway (Clients for UNIX Version 6.20 and later)

Version 6.20 and later of the Clients for UNIX support the SSL protocol. Version 6.30 and later of the Clients for UNIX also support the TLS protocol.

- SSL provides strong encryption to increase the privacy of your server connections and certificate-based server authentication to ensure that the server you are connecting to is genuine.
- TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when they 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 installation will also work with TLS. Some organizations, including US government organizations, require the use of TLS to secure data communications.

You can use the Secure Gateway in either *Normal* mode or *Relay* mode to provide a secure channel for communication between the client and the server. No client configuration is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface. If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure the client to specify the Secure Gateway relay server as described below.

To specify a default Secure Gateway server

Note: These settings are available only on Version 10.x or later of the clients. For earlier versions of the clients, you can use configuration files to specify the Secure Gateway server. See "To use configuration files to specify a Secure Gateway server" on page 93.

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

Note: These settings are available only on Version 10.x or later of the clients. For earlier versions of the clients, you can use configuration files to specify the Secure Gateway server. See "To use configuration files to specify a Secure Gateway server" on page 93.

1. In the main client window, 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 that the **Secure Gateway** option appears dimmed unless the network protocol on the **Network** page is **SSL/TLS + HTTPS server location** for this connection.
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**.

To use configuration files to specify a Secure Gateway server

Note: From Version 10.x of the clients, you can use the main client window to specify a Secure Gateway server. See "To specify a default Secure Gateway server" on page 92 and "To specify a Secure Gateway for a server connection" on page 92.

1. Open appsrv.ini. See "Customizing the Client Using Configuration Files" on page 36 for information about how updates to appsrv.ini in particular locations have different effects.
2. In the [Application] section of the file, create or modify the following entries:

   ```
   SSLProxyHost=csgwy.company.com:443
   SSLEnable=On
   ```

   where `Application` is the section containing published application settings, and the value of `SSLProxyHost` is the Secure Gateway server to which you want to connect.
3. Save and close the file.

For more information about the Secure Gateway, see the *Secure Gateway for Windows Administrator's Guide* or the *Secure Gateway for Solaris Administrator's Guide*.

Configuring and Enabling the Client for SSL and TLS

SSL and TLS are configured in the same way and use the same certificates. When both SSL and TLS are enabled, each time you initiate a connection the client tries to use TLS first, and then SSL. If it cannot connect with SSL, the connection fails and an error message appears.

To use SSL or TLS, you need a root certificate on the client device that can verify the signature of the Certificate Authority on the server certificate. Support for the certificates listed below is built in to Citrix SSL- and TLS-enabled clients:

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 client 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 client 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 the client to use the new certificate, you must restart wfcmgr after adding the certificate.

Important: The client does not support keys of more than 2048 bits. You must ensure that the Certificate Authority root and intermediate certificates, and your server certificates, are less than or equal to 2048 bits long.

To configure the client to use SSL or TLS on a single connection

1. In the main client window, 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** to display the **Network** page.
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**.

To configure a default protocol as SSL or TLS

1. On the **Tools** menu, click **Settings**.

   Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the **Option** menu, not the **Tools** menu.

2. From the drop-down list, choose **Server Location** to display the **Server Location** page.
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 force TLS connections

To force clients to connect only with TLS, you must specify TLS on your Secure Gateway server or SSL Relay service.

See the *Secure Gateway for Windows Administrator's Guide*, the *Secure Gateway for Solaris Administrator's Guide*, or Citrix SSL Relay service documentation for more information.

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 the client through a network firewall that maps the server's internal network IP address to an external Internet address, use the information provided in this section to configure the firewall settings.

To connect across an address-translating firewall

1. On the **Tools** menu, click **Settings**.

Note: In Version 6.30 and earlier of the client, select the **Settings** dialog box from the **Option** menu, not the **Tools** menu.

2. From the drop-down list, choose **Firewall** to display the **Firewall** page.
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. See "Configuring ICA Browsing" on page 40.

Using ICA Encryption

Encryption increases the security of your server connection. By default, basic encryption is enabled on all connections. The client 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 main client window, 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** to display the **Connection** page.
4. From the **Encryption Level** list, choose an encryption level.
5. Click **OK**.

Note: The server can be configured to allow connections only from clients that support basic or advanced encryption. For more information about configuring the server to check encryption levels before allowing connections, see the *Citrix XenApp Administrator's Guide*.

Enabling Smart Card Support

Version 6.30 and later of the Clients for UNIX (except the Client for HP-UX) offer support for a number of smart card readers. If smart card support is enabled on both the server and client, 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 *Citrix XenApp Administrator's Guide*.

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

Note that the Client for HP-UX does not support smart cards.

1. Do one of the following:
   - In the main client window, 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** to display the **Login** page.
3. Click **Allow Smart Card Logon**.
4. Click **OK**.

Troubleshooting

Overview

This chapter describes common problems users may experience when using the Citrix Receiver for Linux, and provides a list of common error messages. It also explains how to provide Citrix Support with diagnostic information.

Topics in this chapter include:

- “Known Issues” on page 99
- “Common Error Messages” on page 112
- “Sending Diagnostic Information to Citrix Support” on page 116

Known Issues

This section lists known issues that can cause problems when using the Citrix Receiver for Linux, along with workarounds where possible.

Connection Issues

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 the Client Using Configuration Files” on page 36 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.

I cannot connect properly to a published resource or desktop session

If, when establishing a connection to a Windows server, the client 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 the *Getting Started with Citrix Licensing Guide*.

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 "Using the Secure Gateway or Citrix SSL Relay" on page 91.

I cannot connect to the Citrix SSL Relay server

If the Citrix SSL Relay server is set to a port other than 443, the Citrix Receiver for Linux cannot connect to a server.

For information about specifying a port for the Citrix SSL Relay, see "Using the Secure Gateway or Citrix SSL Relay" on page 91.

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 the client causes the connection to fail. This is due to a lack of available memory on the server. If the reconnection fails, the client 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 ...;
```

Display Issues

I experience problems with over-scrolling when using published applications

Users may experience problems with over-scrolling when using certain published applications. Note that these problems do not occur when connecting to servers running Citrix Presentation Server 4.5 or later.

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: From Version 10.x of the Clients for UNIX, you must also add the new entries in wfclient.ini to the All_Regions.ini configuration file. See “Customizing the Client Using Configuration Files” on page 36 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 Keyboard Options, Alert Sounds, and Digital Dictation Support” on page 38.

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.

The client 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

The client 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 get graphics corruption when running on AIX in 16 color mode

If you are running AIX Version 4.0 or earlier and are connecting to a server running Citrix XenApp for UNIX in 16 color mode, graphics may be corrupted. To fix this problem, download and install the latest IBM maintenance package from https://techsupport.services.ibm.com/server/aix.fdc.

If you are running AIX Version 4.3.3, this graphics corruption can be fixed by upgrading to Version 4.3.3.0.06.

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: From Version 10.x of the Clients for UNIX, you must add the new entries in wfclient.ini to the All_Regions.ini configuration file. See "Customizing the Client Using Configuration Files" on page 36 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 an ICA 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 main client window, 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, the client buffers rapid palette changes, and updates the real palette only every few seconds.

I have problems entering special characters when running Solaris

Microsoft Windows enables users to enter characters by holding down the left ALT key and entering their encoding value on the numeric keypad. This does not work on Solaris 2.7, 2.8, 2.9, and 2.10 systems, because ALT+0 is used locally by the CDE window manager, dtwm.

To fix this problem, edit the active drwmrc file to comment out the line beginning `Alt<Key>KP_Insert`. On Solaris 2.8, 2.9, and 2.10 systems, you can edit this file from the CDE control panel by selecting **Desktop Controls > Extras > Edit dtwmrc**, then **Reload Actions**. On Solaris 2.7 systems, locate the active dtwmrc file in a subdirectory of $HOME/.dt, edit the file, log off, then restart the session.

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 the Citrix Receiver for Linux.

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

The client uses EUC-JP or UTF-8 character encoding for Japanese characters, while the server uses SJIS character encoding. The client 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 the client when using the GNOME window manager

If you install the client as a non-privileged user, the desktop integration features are not fully enabled. To see the menu entries, install the client 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 the Citrix Receiver for Linux. This can cause problems in the user interface such as missing characters, and the following error message may appear when starting the Citrix Receiver for Linux:

“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 the client startup to run the command xset fp rehash before launching the client or run the xset fp rehash command manually before starting the client. 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 the client.

One workaround is to run the client 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.

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 "To turn off server-client content redirection from the client" on page 63.

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 if you are running Version 8.x or later of the Client for Linux. 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: From Version 10.x of the Clients for UNIX, you must also add the new entries in appsrv.ini to the All_Regions.ini configuration file. See "Customizing the Client Using Configuration Files" on page 36.

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: From Version 10.x of the Clients for UNIX, you must also add the new entries in wfclient.ini to the All_Regions.ini configuration file. See "Customizing the Client Using Configuration Files" on page 36 for more information.

I get excessive memory use when running Microsoft Internet Explorer

Decreasing the size of the SpeedScreen Browser Accelerator cache can fix this issue.

To set the size of the SpeedScreen Browser Accelerator cache

1. Open the wfclient.ini configuration file or the module.ini configuration file.
2. Add the following lines to the [WFClient] section to specify the amount of memory you want to allocate for the cache size:

   ```
   SpeedScreenBADecompressedCacheSize=x
   SpeedScreenBACompressedCacheSize=y
   ```

   These sizes are in kilobytes, and can be adjusted as required.

   Note: From Version 10.x of the Clients for UNIX, you must also add the new entries in wfclient.ini to the All_Regions.ini configuration file. See "Customizing the Client Using Configuration Files" on page 36 for more information.

3. Save and close the file.

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

My configuration file settings no longer work after upgrading the client

From Version 10.x of the Clients for UNIX, 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

From Version 10.x of the Clients for UNIX, 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 the client

If you see an error message such as "/usr/lib/ICAClient/wfcmgr: error while loading shared libraries: libXm.so.3: cannot open shared object file: No such file or directory," this is because the client will not run on distributions that do not include the Motif library or those such as Fedora Core 5 that include only the libXm.so.4 version of the Motif library. The solution is to install libXm.so.3 Version 2.2.3.

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 moving files on DOS floppy disks on Sun computers

If you are running Solaris 5.7 on a Sun computer and want to move files on mounted DOS floppy disks, you have to make a copy on the floppy disk and then delete the original. This requires enough space on the floppy disk to make a copy. The UNIX mv(1) command has the same limitation.

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 the client

If the client 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 the client 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 the client from a terminal session. If the error message still appears, it is likely that the ICAROOT environment variable is not correctly defined.

- Reinstall the client to the default location. For more information about installing the client, see “Installing the Citrix Receiver for Linux” on page 18.

  If the client was previously installed in the default location, remove the /usr/lib/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 European characters, you need to set the server DOS codepage to 1252.

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

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.

Support for Eastern European characters has been added to Version 9.x of the client. Follow the procedure above to set the server DOS codepage to 1250.

My keyboard shortcuts do not function correctly

If your window manager uses the same keyboard shortcut combinations to provide native functionality, your client 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 “Configuring Keyboard Shortcuts” on page 41 for more information about configuring keyboard shortcuts.

I want to use /dev/random with the Client for Solaris

If /dev/random is present, the Client for Solaris can use it to initialize Secure ICA and SSL. /dev/random is a standard feature of Solaris 9 and above, and can be created in previous versions of Solaris by installing the Solaris 8 patches 112438 for the Client for Solaris (SPARC) and 112439 for the Client for Solaris (x86), available from http://www.sunsolve.sun.com/.

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 client device does not have read access to /dev/ttyUSB0, the server cannot access a USB-tethered Pocket PC connected to the client 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 client device and then reconnect it.

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

If you have multiple USB-tethered Pocket PCs connected to your client 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 client device, add the following to the [WFClient] section of the appropriate configuration file:

```
ContinueWithoutPDALockFile=True
```

See “Customizing the Client Using Configuration Files” on page 36 for information about how updates to particular configuration files affect different users.

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

However, if you want the client 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 client executable to match this group, for example by typing:

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

  Set the group id when the client executes by typing:

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

  This enables the client 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 - Error in configuration file: "..." Cannot find section "...".

The configuration file was incorrectly edited or is corrupt.

E_MISSING_INI_ENTRY - Error in configuration file. Section "..." must contain an entry "...".

The configuration file was incorrectly edited or is corrupt.

E_INI_VENDOR_RANGE - Error in configuration file: "..." Bad Vendor Range "..."

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 - A server must be entered.

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

E_CANNOT_WRITE_INI_FILE - Cannot write file: "..."

There was a problem saving the connection database; for example, no disk space.

E_CANNOT_CREATE_INI_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 specified connection.

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

E_CSM_APPSERVERLIST_MISSING - Error in configuration file: "..." Missing section: "..."

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

E_CSM_APPSRV_SECTION_MISSING - Inconsistency in configuration file: "..." Missing section: "..."

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

E_PNAGENT_FILE_UNREADABLE - Cannot read PNAgent file "...": No such file or directory.

— Or — **Cannot read PNAgent file "...": Permission denied.**

You are trying to access a resource through a desktop item or menu, but the PNAgent file for the resource is not available. Refresh the published resources on the client 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 PNAgent file to which the icon or item refers.

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

The **Description** box 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 “...”.

File "..." is not on a drive-mapped file system.

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

No application is associated with the type of file "...".

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.

No file type associations are defined by the server you selected.

Select another server that does have file type associations defined.

The type of file "..." can not be ascertained as it does not have a file extension.

Rename file "..." to have a suitable extension.

File "..." is on a drive-mapped file system which is currently disabled.

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

Client Drive Mapping is currently disabled.

Ensure the **Enable Drive Mapping** check box is selected on the **Drive Mapping** page of the **Settings** dialog box.

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 the client.

Proxy detection failure: JavaScript error.

The PAC file contains invalid JavaScript. Fix the PAC file on the server. Also see "I get a "Proxy detection failure" error message when connecting" on page 100.

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 the client.

An error occurred. The error code is 11 (E_MISSING_INI_SECTION). Please refer to the documentation. Exiting.

When running the client 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 not valid.

Missing argument for option "...".

E_BAD_ARG -The option "..." has an invalid argument: "...".

Invalid argument specified for option "...".

E_INI_KEY_SYNTAX - Error in configuration file: "..." Bad Key "..."

The X Server vendor information in the configuration file is corrupt. Create a new configuration file.

E_INI_VALUE_SYNTAX - Error in configuration file: "..." Bad Value "..."

The X Server vendor information in the configuration file is corrupt. Create a new configuration file.

E_SERVER_NAMELOOKUP_FAILURE - Cannot get address for server "..."

The server name cannot be resolved.

Cannot browse NDS tree: "...".

Refer to Novell documentation for further help with this error.

An error occurred writing to one or more of the files: "...".

Check for disk full issues, or permissions problems. If a problem is found and corrected, retry the operation that prompted the error message.

Connection lost. Some data may be missing from some of the files: "...".

Reconnect and retry the operation that prompted the error.

A server application's attempt to access a PDA device failed because it 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.

An application on the server is requesting access to your local PDA device. This is potentially unsafe. Do you want to grant access?

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 the client, 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 the client

1. On the **Help** menu of the main client 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 client version details, the contents of the client configuration files, and the values of various system variables. Check this file for confidential information before sending it to Citrix Support.

Citrix Receiver for Linux Command-Line Parameters

Citrix Receiver for Linux Command-Line Parameters

The table below lists the Citrix 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*
Set the location of UNIX client installation files. This is equivalent to setting the ICAROOT environment variable.	-icaroot *directory*
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*

To	Type
Specify a clear text password.	-clearpassword *clear password*
Specify a domain.	-domain *domain*
Specify an initial program.	-program *program*
Turn on sound.	-sound
Turn off sound.	-nosound
Use private colormap.	-private
Use shared colormap.	-shared
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*
Show this list of parameters.	-help
Turn off the splash screen.	-nosplash
Display version information.	-version
Suppress connection dialogs.	-quiet
Set session geometry.	-geometry WxH+X+Y
Show error numbers and string.	-errno
Display a different name for the client, specified by *name*, wherever the client name appears. The default client 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*

Index

A

accelerator keys
  troubleshooting IME accelerator keys under KDE 110
accented characters
  troubleshooting in file names 110
All_Regions.ini 36
anti-aliasing 59
applications
  failing due to locked serial ports 109
  publishing 78
  specifying which to run at connection 52
  troubleshooting applications running locally 106
  working directory for 52
approximate colors 39
appsrv.ini 36
Arabic characters
  troubleshooting 105
audio
  configuring digital dictation support 50
  mapping client audio 75
authentication 15
auto client reconnect
  configuring for individual connections 53
  default settings for 44
automatic diagnostics 116
automatic proxy detection
  configuring 90
  troubleshooting 100

B

bandwidth
  improving performance 46
bitmap caching 46
browser
  supporting faster browsing 25

C

canonicalization.ini 36
changing connection entries 44
Citrix documentation set 12
Citrix SSL Relay
  configuring client with 91
  troubleshooting connections to 100
Citrix XenApp
  configuration overview 77
  configuring 77
  limiting desktop customization 79
  menus and desktop shortcuts 81
  publishing content 78
  security of 87
ClearType 59
client
  configuration overview 35, 99
  connections overview 27
  creating connections 27
  modifying 21
  overview of security 87
  redirecting output from 23
  repackaging 21
  starting 20
  uninstalling 21
client audio
  mapping client audio 75
client device mapping 67
client devices
  mapping 67
client drive mapping 68
client printer mapping 72
codecs 18
colors
  approximate color mapping 39
  color mapping 39
  default windows settings 39
  troubleshooting color flashing 103
  troubleshooting graphics corruption in 16-color

mode 102
troubleshooting rapid color changes 103
configuration files
configuring the client using 36
troubleshooting 108
configuring
application properties 52
automatic proxy detection 90
Citrix XenApp, overview of 77
client with Citrix SSL Relay 91
client, overview of 35
default settings for all connections 37
digital dictation support 50
extended parameter passing 57
ICA encryption 96
logon properties 52
middle button paste 50
network properties 45
security features, overview 87
server-client content redirection 60
session options 84
smart card logons 96
workspace control 82–83
configuring the client
overview of 35
configuring, Citrix XenApp 77
connecting
across a firewall 95
client, overview of 27
through a proxy server 87
through a secure proxy server 89
through a SOCKS proxy server 88
troubleshooting 100
Connection Center 32
connection entries
changing 44
configuring auto client reconnect settings 53
configuring default settings for 37
creating 27
default settings for 38
default settings for auto client reconnect 44
default settings for keyboard shortcuts 41
default settings for network protocol 39
default settings for windows 39
editing 44
running applications 52
connections
overview of 27
creating connection entries 27
cursor visibility
troubleshooting 103
cutting and pasting
xcapture 63

D

data compression 47
default settings for all connections
auto client reconnect settings 44
keyboard shortcut settings 41
network protocol settings 39
preferences 38
windows settings 39
desktop customization
limiting 79
desktop integration
customizing menus and shortcuts 81
dev/random
troubleshooting on Solaris 110
diagnostics
automatic 116
digital dictation support
configuring 50
disk caching 46
DNS
troubleshooting 100

E

editing connection entries 44
encryption
configuring ICA encryption 96
forcing TLS connections 95
error messages 112
excessive redrawing
troubleshooting in seamless mode 102
extended parameter passing
configuring 57

F

Fedora
troubleshooting 105, 108
file attributes
troubleshooting changing file attributes 109
troubleshooting setting on floppies 109
file names
troubleshooting accented characters in 110
Firefox
troubleshooting 108
floppies
troubleshooting moving files on DOS floppies 109
troubleshooting setting file attributes 109

folder redirection 56
font smoothing 59

G

ghost windows
- troubleshooting 102

GNOME
- integrating client with 57, 60
- troubleshooting 105
- troubleshooting menu entries 105

graphics
- using xcapture 63

graphics corruption
- troubleshooting in 16-color mode 102

H

HTTPS
- configuring client with 87

I

ICA encryption
- configuring 96

icon compatibility
- troubleshooting 102

IME accelerator keys
- troubleshooting under KDE 110

improving performance
- data compression 47
- disk caching 43, 46
- low-bandwidth connections 46
- SpeedScreen latency reduction 47

integrating client with KDE or GNOME 57, 60
Internet name
- troubleshooting 100

J

Japanese characters
- troubleshooting incorrect display 104

K

KDE
- integrating client with 57, 60
- troubleshooting IME accelerator keys under 110

Kerberos 15
keyboard pass-through
- configuring 41

keyboard problems
- troubleshooting 101

keyboard shortcuts
- default settings for shortcut keys 41
- troubleshooting 110

keyboard types
- default settings for 38

Konqueror
- enabling the ICA plug-in on 106

L

licensing
- troubleshooting on multi-homed hosts 110

limiting desktop customization by users 79
locked serial ports 109
logon
- configuring smart card logons 96

logon methods
- specifying for published resources 80

logon properties
- configuring 52

M

mapping client audio 75
mapping client devices
- general information 67

mapping client drives
- procedures 68

mapping client printers
- procedures 72

mapping COM ports
- procedure 67

mapping default color settings 39
mapping, client devices 67
middle button paste
- configuring 50

modifying client 21
module.ini 36
Mozilla
- troubleshooting launching applications 106

multi-homed hosts
- troubleshooting client licensing on 110

multilingual installation 14
multimedia 18, 20, 49

N

NDS support
- using NDS with Program Neighborhood Agent 85
- using NDS without DNS 85

network properties
- configuring 45

network protocol
- default settings for business recovery 39
- specifying 45

non-Netscape browsers
- troubleshooting 106

Novell Directory Services support
- using NDS with Program Neighborhood Agent 85
- using NDS without DNS 85

NTLM support
- configuring client to use 89

O

operating systems
- supported 17

over-scrolling
- troubleshooting 101

P

PDAs
- troubleshooting access to 111, 116

platforms
- supported 17

Pocket PCs
- troubleshooting access to 111, 116

Polish characters
- troubleshooting on US English keyboards 104

preferences
- default settings for 38

printers
- mapping client printers 72

proxy
- redirecting client output to another device 23

proxy detection failure
- troubleshooting 100

proxy servers
- connecting across a firewall 95
- connecting through 87
- connecting through a secure proxy server 89

published resources
- specifying logon methods 80

publishing applications 78

publishing content 78

R

redirecting client 23

removing
- client 21

repackaging the client 21

requirements
- system 17

resolving server names
- troubleshooting 100

restart 14

S

screen problems
- troubleshooting 101

screenshots
- using xcapture 63

seamless mode
- troubleshooting excessive redrawing in 102
- troubleshooting removing window decorations in 102
- troubleshooting session sharing 99

Secure Gateway
- configuring client with 91

securing the client
- overview of 87

security
- configuring client with the Secure Gateway 91
- configuring ICA encryption 96
- configuring security features, overview 87
- forcing TLS connections 95

Security proxy protocol
- configuring client with 87

serial-port locking 109

server location
- for Web Interface 79

server name
- specifying for a connection 45

server side ICA 23

server-client content redirection
- configuring 60
- troubleshooting 106

servers
- mapping 67

session options
- configuring 84
- overview of 84

session sharing
- troubleshooting seamless connections 99

setting up Citrix XenApp 77

setting up client 27, 35, 99

smart cards 96

smoothing, font 59

SOCKS
- connecting through 88

sound
- mapping client audio 75
- Windows alert sounds 38

special characters
- troubleshooting on Solaris 104

special folder redirection 56

specifying
- network protocol for a connection 45
- published application for a connection 45
- server name for a connection 45

SpeedScreen Browser Accelerator
- libjpeg.so requirement 25

SpeedScreen latency reduction
- improving performance with 47

SpeedScreen Multimedia Acceleration 18, 20, 49

SSL
- configuring client with 87
- overview of 91

starting client 20
- troubleshooting 109

SuSE
- troubleshooting 105

system requirements 17

T

TLS
- configuring client with 87
- overview of 91

troubleshooting
- accented characters in file names 110
- application running locally 106
- Arabic characters 105
- automatic proxy detection 100
- changing file attributes 109
- color flashing 103
- configuration files 108
- connecting to the Citrix SSL Relay server 100
- cursor visibility 103
- DNS 100
- enabling the ICA plug-in on Konqueror 106
- excessive redrawing in seamless mode 102
- Fedora 105, 108
- file types 78
- Firefox 108
- ghost windows 102
- GNOME 105
- GNOME menu entries 105
- graphics corruption in 16-color mode 102
- icon compatibility 102
- IME accelerator keys under KDE 110
- incorrect Japanese character display 104
- Internet name 100
- keyboard problems 101
- keyboard shortcuts 110
- known issues 99
- licensing on multi-homed hosts 110
- moving files on DOS floppies 109
- non-Netscape browsers 106
- over-scrolling 101
- PDA access 111, 116
- Pocket PC access 111, 116
- Polish characters on US English keyboards 104
- problems connecting 100
- proxy detection failure 100
- published applications on Mozilla 106
- publishing content 78
- rapid color changes 103
- removing window decorations in seamless mode

102
- resolving server names 100
- server-client content redirection 106
- session sharing 99
- setting file attributes on floppies 109
- special characters on Solaris 104
- starting client 109
- SuSE 105
- USB synchronization for Pocket PCs 111
- using alternate address for firewall connection 100
- using /dev/random on Solaris 110
- viewing Web site response times 106

TrueColor displays
- troubleshooting rapid color changes in 103

U

uninstalling the client 21

UNIX platforms
- supported 17

USB
- support for 14
- troubleshooting Pocket PC synchronization 111

W

Web Interface
- server location 79

wfclient.ini 36

window settings
- default behavior 39

windows
- default settings for 39

Windows NT challenge/response (NTLM) support
- configuring client to use 89

workspace control
- configuring 82–83

X

X11 devices
- redirecting client output to 23

xcapture 63
- starting from the command line 64
- starting from the main client window 64