Clients for UNIX Administrator's Guide

MetaFrame® Presentation Server Clients for UNIX, Version 8.x
Citrix® MetaFrame® Presentation Server 3.0
Citrix® MetaFrame® Access Suite
Use of the product documented in this guide is subject to your prior acceptance of the End User License Agreement.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. Other than printing one copy for personal use, no part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Citrix Systems, Inc.

© 1994-2004 Citrix Systems, Inc. All rights reserved.


Version 6.30 of the Clients for UNIX and later includes software developed by David Corcoran (corcoran@linuxnet.com) http://linuxnet.com (MUSCLE).

Winscard.h/pcsc lite for smartcard reader communications Copyright © 2000 David Corcoran (corcoran@linuxnet.com). All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by: David Corcoran (corcoran@linuxnet.com)
   http://www.linuxnet.com/ (MUSCLE)

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Citrix, Independent Computing Architecture (ICA), MultiWin, SecureICA, SpeedScreen, Program Neighborhood, MetaFrame, and MetaFrame XP are registered trademarks or trademarks of Citrix Systems, Inc. in the U.S.A. and other countries.

Microsoft, MS, MS-DOS, Outlook, Windows, Windows NT, and BackOffice are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark of The Open Group in the U.S.A. and other countries.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.
All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

HP-UX is a registered trademark of Hewlett-Packard Company.

AIX and RS/6000 are registered trademarks of International Business Machines Corporation.

SGI is a registered trademark of Silicon Graphics, Inc.

SCO is a registered trademark of The Santa Cruz Operation, Inc.

Tru64 is a registered trademark of the Hewlett-Packard Company.

Linux is a registered trademark of Linus Torvalds.

All other Trade Names referred to are the Servicemark, Trademark, or Registered Trademark of the respective manufacturers.

Last Updated: May 20, 2004 (ER)
Contents

Chapter 1 Before You Begin
Who Should Use this Guide ........................................... 11
How to Use this Guide ........................................... 11
Client Overview ..................................................... 12
Accessing Documentation ...................................... 12
  Client for UNIX Documentation ............................. 13

Chapter 2 Introduction to the Clients for UNIX
Overview ............................................................. 15
Features Overview .............................................. 17
  Client Device Mapping ........................................ 17
    Client Drive Mapping ........................................ 17
    Client Printer Mapping ...................................... 17
    COM Port Mapping .......................................... 17
    Client Audio Mapping ...................................... 18
  Disk Caching and Data Compression ...................... 18
  Low Bandwidth Requirements ............................... 18
  Client Auto Update ........................................... 18
  Color Approximation ......................................... 18
  Hotkeys ......................................................... 18
  Transparent Clipboard Access ............................. 19
  Application Publishing Support ........................... 19
  Business Recovery ........................................... 19
New Features Introduced in Version 6.0 .................... 19
  ICA Encryption ................................................ 19
  SpeedScreen Latency Reduction .......................... 20
  Increased Color Support .................................... 20
  Seamless Windows ........................................... 20
  Netscape Plug-in .............................................. 20
New Features Introduced in Version 6.20 .................. 21
  Enhanced Encryption ........................................ 21
  SSL ............................................................. 21
Extended Parameter Passing ........................................... 21
Time Zone Support ..................................................... 21
New Features Introduced in Version 6.30 ............................. 22
  Smart Card Support .................................................. 22
  Auto Client Reconnect ............................................. 22
  Server-Client Content Redirection ................................ 22
  Roaming User Reconnect .......................................... 23
  TLS Encryption ...................................................... 23
  Support for the Secure Gateway .................................. 23
  Enhanced Proxy Support .......................................... 23
  User-to-User Shadowing .......................................... 24
  CDE Integration .................................................... 24
New Features Introduced in Version 7.x ............................. 24
  Program Neighborhood Agent ...................................... 24
  Desktop Integration ............................................... 25
  Universal Printer Driver Support ................................ 25
  Installation and Update of Remote Clients ....................... 25
  SpeedScreen Browser Accelerator ................................ 25
  Non-Rectangular Seamless Windows .............................. 25
  Keyboard Accelerators .......................................... 25
  Other Enhancements .............................................. 25
    Connection Center .............................................. 26
    Browser Support ................................................ 26
New Features Introduced in Version 8.x ............................. 26
  Workspace Control ............................................... 26
  Digital Dictation Support ...................................... 26
  Dynamic Session Reconfiguration ................................ 27
  Zone Preference and Failover ................................... 27
  Improved Logon Look and Feel ................................... 27
  General Performance Improvements .............................. 27
    Better ICA Performance ....................................... 27
    ThinImage ....................................................... 28
  Other Enhancements .............................................. 28
    Middle Button Paste .......................................... 28
    Windows System Tray Emulation Window ....................... 28
    Unicode Support ............................................... 28
    Diagnostic Information ........................................ 28
    xcapture ....................................................... 28
Chapter 3 Deploying the Clients for UNIX

Overview ......................................................... 29
System Requirements ......................................... 29
User Requirements ............................................. 30
Other Factors to Consider before Installation ............. 30
Installing the Client for Linux from the Web .......... 31
Installing the Clients for UNIX ............................. 31
Starting the Clients for UNIX ............................... 33
Updating the Clients for UNIX ............................. 34
About Client Updates ......................................... 34
  Configuring the Client Update Database .............. 34
  Creating a New Client Update Database ............... 35
  Specifying a Default Client Update Database ........ 35
  Configuring the Properties of the Client Update Database ........................ 36
  Adding Clients to the Client Update Database ........ 37
  Removing a Client From the Client Update Database .. 38
  Changing the Properties of a Client ..................... 38
Uninstalling the Clients for UNIX ......................... 39
Using the Client as an “ICA to X Proxy”
(“Server Side ICA”) ............................................ 40
  Server Sizing ............................................... 41
  Supported Features ......................................... 41
  Starting the Clients for UNIX with “Server Side ICA” .... 41
Supporting Faster Browsing ................................ 42

Chapter 4 Configuring the Clients for UNIX

Overview .......................................................... 43
Creating Connection Entries ............................... 44
Viewing Connection Entries ............................... 45
Opening a Connection ........................................ 46
Managing Your Connections ............................... 48
Changing a Connection Entry ............................. 50
  Configuring Network Properties ......................... 50
  Improving Performance over a Low-Bandwidth Connection .... 51
  Changing the Client Configuration ...................... 51
  Changing How the Client Is Used ....................... 54
Configuring Middle Button Paste Functionality ........ 54
Specifying an Application to Run at Connection ....... 54
Changing the Window Properties .............................................. 55
Configuring Logon Properties .................................................. 56
Changing Auto Client Reconnect Settings ................................. 56
Using xcapture ................................................................. 57
Enabling Smart Card Support .................................................. 59
Integrating the Clients for UNIX with Security Solutions ........... 60
Connecting through a Proxy Server ......................................... 60
  Using Auto-Client Proxy Detection ...................................... 61
  Connecting through a SOCKS Proxy Server ........................... 61
  Connecting through a Secure Proxy Server ............................ 62
  Connecting across a Firewall ............................................. 63
  Using the Secure Gateway or Citrix SSL Relay ....................... 64
Mapping Client Devices ....................................................... 68
Mapping COM Ports ............................................................ 68
Mapping Client Drives ........................................................ 69
Mapping Client Printers ........................................................ 72
Mapping Client Printers on MetaFrame Presentation Server for Windows 74
Mapping Client Printers on MetaFrame Presentation Server for UNIX 75
  Setting up Printing .......................................................... 75
  Printing ....................................................................... 76
  Printing from Applications .............................................. 76
Mapping Client Audio .......................................................... 78
Configuring Digital Dictation Support .................................... 79
Changing Default Settings .................................................... 79
  Configuring Keyboard Options, Alert Sounds, Automatic Updates and Digital Dictation Support ........................................ 81
  Configuring Default Window Settings ................................ 81
  Configuring Server Location and Business Recovery ............. 82
  Configuring Hotkeys ....................................................... 83
  Changing Settings for the Disk Cache ................................ 84
  Configuring Auto Client Reconnect ................................... 85
  Configuring Network Protocol ......................................... 86
Integrating the Clients for UNIX with CDE ............................. 86
Integrating the Clients for UNIX with KDE and GNOME ........... 87
Accessing Published Resources with the Program Neighborhood Agent .... 88
  Publishing Content ....................................................... 88
  User Tasks with Program Neighborhood Agent ..................... 89
Before You Begin

Who Should Use this Guide

This guide is for system administrators responsible for installing, configuring, deploying, and maintaining the Clients for the UNIX or Linux platforms. This guide assumes knowledge of:

- Citrix MetaFrame
- The operating system on the client computer (UNIX or Linux)
- Installation, operation, and maintenance of network and asynchronous communication hardware, including serial ports, modems, 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.

**Note**  NFuse Classic has been integrated as a feature in MetaFrame Presentation Server. It is now called the Web Interface for MetaFrame Presentation Server.

How to Use this Guide

To get the most out of this guide, review the table of contents to familiarize yourself with the topics discussed.
This guide contains the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Before You Begin”</td>
<td>Contains background information about the client. Also contains information about the documentation and how to access it.</td>
</tr>
<tr>
<td>Chapter 2, “Introduction to the Clients for UNIX”</td>
<td>Gives a detailed list of features.</td>
</tr>
<tr>
<td>Chapter 3, “Deploying the Clients for UNIX”</td>
<td>Describes how to install and deploy the Citrix ICA Clients for UNIX.</td>
</tr>
<tr>
<td>Chapter 4, “Configuring the Clients for UNIX”</td>
<td>Describes how to configure connection properties and device mappings for the Citrix ICA Clients for UNIX.</td>
</tr>
<tr>
<td>Chapter 5, “Troubleshooting”</td>
<td>Describes common problems you may experience when using the client. It also provides a list of common error messages.</td>
</tr>
</tbody>
</table>

**Client Overview**

The Client for UNIX allows users to connect to computers running MetaFrame Presentation Server.

There are two alternative ways to create and edit connections for the Client for UNIX:

- By using the **Connections** menu, accessed from the main client window, to locally create and edit ICA connections to specific computers running MetaFrame Presentation Server or to published applications.

- By using the Program Neighborhood Agent to obtain pre-defined ICA connection configurations from servers running the Web Interface. This avoids having to manually create and edit separate connections for each application; users can connect to all published applications and content in a server farm through a single URL.

Chapter 3 describes how to create and edit connections using the **Connections** menu. It also contains instructions for configuring and using the Program Neighborhood Agent.

**Accessing Documentation**

This administrator’s guide is part of the MetaFrame Presentation Server documentation set. The documentation set includes guides that correspond to different features of MetaFrame Presentation Server. Documentation is provided in Adobe Portable Document Format (PDF).
Important information about known issues, and last-minute documentation updates and corrections is provided in the Readme. Be sure to read the readme.txt file in the \Documentation directory of the product CD-ROM before you install the client or during troubleshooting.

**Important**  To view, search, and print the PDF documentation, you need to have the Adobe Acrobat Reader 5.0.5 with Search or a later version with Search. You can download Adobe Acrobat Reader for free from Adobe Systems’ Web site at http://www.adobe.com/.

**Client for UNIX Documentation**

The documentation set for the Clients for UNIX comprises:

- **Clients for UNIX Administrator’s Guide** (this guide)—introduces the Clients for UNIX, and explains how to create, configure and manage connections to the computer running MetaFrame Presentation Server

- **Clients for UNIX OEM’S Reference Guide**—outlines how to customize the Clients for UNIX for use with OEM client devices

More information about Citrix documentation, and details about how to obtain further information and support, is included in *Getting Started with MetaFrame Presentation Server*. 
CHAPTER 2

Introduction to the Clients for UNIX

Overview

MetaFrame Presentation Server Clients are the client-side software components of the MetaFrame Presentation Server product family. Combining the ease of use you expect with the security features you require, the clients offer point-and-click, secure access to applications, content, and entire desktops published on computers running MetaFrame Presentation Server.

The Clients for UNIX are developed for several UNIX operating system platforms, and have the following features:

- Client device mapping
  - Client drive mapping
  - Client printer mapping
  - COM port mapping
  - Client audio mapping
- Disk caching and data compression
- Low bandwidth requirements
- Client auto update*
- Color approximation
- Client hotkeys
- Transparent clipboard access
- Application publishing support
- Business recovery
- Encryption
- SpeedScreen latency reduction*
• Increased color support
• Seamless windows support
• SSL support
• Extended parameter passing
• Time zone support*
• Smart card support*
• Auto client reconnect
• Server-client content redirection*
• Roaming user reconnect
• TLS encryption
• Secure Gateway support
• Enhanced proxy support
• User-to-user shadowing
• CDE integration
• Program Neighborhood Agent
• Desktop integration
• Non-privileged user installation and update
• SpeedScreen Browser Accelerator*
• Keyboard accelerators
• Digital dictation support*
• Workspace control
• Dynamic session reconfiguration

Note that some of these features are available only when connecting to servers running:
• MetaFrame Presentation Server for Windows on:
  • Windows NT
    —Or—
  • Windows 2000 Server
• Citrix MetaFrame XP for Windows with Feature Release 3 on:
  • Windows 2000 Server
    —Or—
  • Windows Server 2003
Those features marked with an asterisk (*) are not available when connecting to servers running MetaFrame Presentation Server for UNIX.

Features Overview

The following sections provide a brief introduction to those major features of the client that are common to all versions of the product.

Client Device Mapping

Client device mapping allows a remote application running on the server to access devices such as printers and disk drives attached to the local client device.

Client Drive Mapping

Client drive mapping makes any directory mounted on your UNIX-based computer, including CD-ROMs, available to you during ICA sessions on servers. When a server is configured to allow client drive mapping, you can access your locally stored files, work with them during your ICA sessions, and then save them either on a mounted directory or on a drive on the server.

Client Printer Mapping

Client printer mapping lets users access printers attached to their computers during ICA sessions. Users of the client can print to any spooled printer available from the client device.

COM Port Mapping

Client COM port mapping allows devices attached to the client computer’s serial ports to be used from ICA sessions on a server. This allows local devices like modems, serial printers, and bar-code scanners to be used by applications running on the server.

In Version 3.0, COM port mapping was introduced for the Linux client only. Version 6.0 and later have this feature for more operating systems — Linux, Solaris (SPARC), HP-UX, and AIX.
**Client Audio Mapping**

Client audio mapping allows your client device to play and record sounds generated by applications running on the server.

Audio support in the client includes configurable sound quality levels that allow you to customize sound quality based upon the amount of bandwidth available.

**Disk Caching and Data Compression**

Disk caching and data compression can increase performance over low-speed asynchronous and WAN connections. Disk caching stores commonly used portions of your screen (such as icons and bitmaps) locally, increasing performance by avoiding retransmission of locally cached data. Data compression reduces the amount of data sent over the communications link to the client.

**Low Bandwidth Requirements**

The ICA protocol typically uses 20 KB/s of bandwidth for each session.

**Client Auto Update**

Client auto update allows administrators to update installations of the clients from a central location instead of having to manually install new client versions on each client device. New versions of the clients are stored in a central client update database on the server. The latest versions of the client software are downloaded to client devices when users connect to a server.

**Color Approximation**

Because of differences in the palettes used by the client (and the applications they display) and native UNIX desktops, flashing can occur when switching context on a PseudoColor display. The clients’ color approximation scheme eliminates this flashing by using colors from the local desktop palette to display the ICA sessions.

**Hotkeys**

The client provides hotkeys that can be used to control various functions while in an ICA session. With hotkeys, you can define alternatives to the following combinations because these are reserved for use by X Windows managers: ALT+F1 to ALT+F12, ALT+TAB, ALT+SHIFT+TAB, and Toggle Speedscreen.
Transparent Clipboard Access

You can use the client workstation’s clipboard to cut and paste text and graphics between applications running locally on the client device and applications running remotely in an ICA session.

Access to the local clipboard requires no special configuration or procedures. Using the familiar cut, copy, and paste commands, you can transfer text and graphics back and forth between local and remote applications.

To help the exchange of graphical data between the server clipboard and non-I CCCM-compliant X Windows applications on the X desktop, you can use the xcapture program. See “Using xcapture” on page 57 for more details. Note that not all server platforms support all media types on the clipboard.

Application Publishing Support

You can create a remote application entry that contains all of the information necessary to launch a user session or a published application.

Business Recovery

The client supports multiple server sites (such as primary and backup) with different addresses for the same published application name.

This feature provides consistent connections to published applications in the event of primary server disruption.

New Features Introduced in Version 6.0

The following list outlines the new features introduced in Version 6.0 of the client. These features are also available in all later versions.

ICA Encryption

The client supports encryption using ICA encryption. ICA encryption (SecureICA) is a server extension that adds advanced RSA RC5 encryption to the server and clients. See the MetaFrame Presentation Server Administrator’s Guide for more information.

Note To use advanced encryption, you must install ICA encryption on your server. ICA encryption is included by default in MetaFrame XP, Feature Release 1 and later versions. ICA encryption is not available for servers running UNIX Operating Systems.
**SpeedScreen Latency Reduction**

SpeedScreen latency reduction is a combination of technologies implemented to enhance user experience over high latency connections by providing instant feedback to the user in response to typed data or mouse clicks.

SpeedScreen latency reduction includes Local Text Echo, which accelerates the presentation of input text by changing its display and updating it when details are received from the server. This effectively shields you from experiencing latency on the network. In addition, Mouse Click Feedback is also available, which provides visual feedback of a mouse click by immediately changing the mouse pointer into an hourglass indicator.

**Note** SpeedScreen latency reduction is not available when connecting to servers running Citrix MetaFrame for UNIX Operating Systems Versions 1.0 and 1.1.

**Increased Color Support**

You can configure the client for true color (24-bit) support. Version 6.0 and later of the clients support high color (32 thousand colors) and true color (24-bit) server connections. Support for 16 and 256 colors is included in earlier versions.

**Seamless Windows**

The client supports the seamless integration of local and remote applications on the local desktop. By selecting the seamless windows option when configuring a connection to a server, you do not need to access an entire remote desktop to run remote applications. With a single session, you can gain access to multiple applications and switch between local and remote applications.

**Note** Because the 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.

**Netscape Plug-in**

The client includes a plug-in for Netscape and Mozilla browsers, which allows ICA sessions to be launched from Web pages. It is, therefore, mostly used in conjunction with the Web Interface.
The Netscape plug-in includes MIME type support for ICA files, so that users can launch an associated published application simply by double-clicking a desktop icon while browsing with Netscape. This integration is performed automatically during installation, but you can also configure the browser manually after installation.

You can also embed ICA sessions in Web pages using the plug-in.

The plug-in can also be used to set up auto-client proxy detection, which allows the client to communicate with the local Web browser and discover proxy server details. This is useful if you are in an organization with many proxy servers or if you cannot determine which proxy server will be used when you configure the client.

If Netscape Navigator is already installed on the client, you are prompted to install the plug-in. By default, the plug-in configures Netscape as the default browser.

**New Features Introduced in Version 6.20**

The following list outlines the new features introduced in Version 6.20 of the client. These features are also available in all later versions.

**Enhanced Encryption**

Versions 6.20 and later have enhanced encryption handling capabilities.

**SSL**

The clients support Secure Sockets Layer (SSL) encryption. SSL-level encryption provides server authentication, data stream encryption, and message integrity checks. SSL+HTTPS (secure HTTP) browsing is also supported.

**Extended Parameter Passing**

With extended parameter passing, you can integrate published applications into desktop UNIX environments by associating a file type on a client device with an application published on a server. When you open a locally saved file, the file is opened in the application associated with it.

**Time Zone Support**

This feature allows you, when logging on to a server in a different time zone, to have the ICA session reflect the time zone of the client device.
For example, a user in London, which is in the Greenwich Mean Time zone, logs on to a server in New York City, which is in the Eastern Standard Time zone, and launches Microsoft Outlook as a published application. Microsoft Outlook stamps emails sent during the ICA session with the user’s GMT time zone information.

New Features Introduced in Version 6.30

The following list outlines the new features introduced in Version 6.30 of the client.

**Smart Card Support**

The Clients for UNIX (except the HP-UX client) offer support for a number of smart card readers. If smart card support is enabled on both the server and client sides, you can use smart cards for the following purposes:

- **Smart card logon authentication.** Use smart cards to authenticate users to servers running MetaFrame Presentation Server.
- **Smart card application support.** Allow smart card-aware published applications to access local smart card readers.

Smart card data is security-sensitive and should be transmitted over a secure authenticated channel such as Secure Sockets Layer (SSL). Smart card devices and published applications must comply with the PC/SC industry standard.

**Auto Client Reconnect**

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 a server, you do not have to reconnect manually or reenter logon credentials to continue working. Automatic reconnection does not occur if you exit applications without logging off.

**Server-Client Content Redirection**

Server-client content redirection allows a server administrator 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 allows administrators to allocate resources more efficiently, thereby providing users with better performance.
Roaming User Reconnect

Roaming user reconnect adds roaming capabilities to ICA sessions. Previously, ICA sessions were identified by the name of the client device from which they were initiated, and they were limited to that device. Feature Release 2 of MetaFrame XP identifies sessions by user name. As a result, users can resume their ICA sessions from any ICA-enabled device. This allows users to start a session on one device and resume work on another. Note that roaming user reconnect is effective only when connecting to load-balanced published applications.

Roaming user reconnect does not require client configuration.

Roaming user reconnect passes partial user credentials to the server farm so that the system can identify the user’s session. For this information to be passed to the server farm, the username, and the domain name, must be available in the ICA file, connection file (appsrv.ini) or from the command line.

**Note** Roaming user reconnect is not supported for connections that use smart card authentication, and requires that connections use either the TCP/IP+HTTP or the SSL/TLS+HTTPS protocol.

TLS Encryption

The client supports TLS 1.0, the successor to SSL 3.0, for environments that demand it. TLS (Transport Layer Security) is the standardized form of SSL (Secure Sockets Layer). Both are cryptographic security protocols designed to ensure the integrity and privacy of data transfers across public networks. SSL and TLS are functionally equivalent. Certain organizations have a security policy that requires TLS rather than SSL.

Support for the Secure Gateway

The client provides full support for Version 2.0 and later of the Secure Gateway. The Secure Gateway acts as a secure Internet gateway between SSL/TLS-enabled clients and servers. The Internet portion of ICA traffic between client devices and the Secure Gateway server is SSL/TLS-encrypted. SSL/TLS is the Internet standard 128-bit encryption technology used for client-server authentication; it ensures the integrity and privacy of data transfers across public networks.

Enhanced Proxy Support

As an alternative to SOCKS proxy, the client also supports Secure proxy (also known as Security proxy, HTTPS proxy, and SSL-tunneling). Proxy authentication is also supported. When used with the Secure Gateway for MetaFrame, applications can be delivered securely to anywhere in the world through the Internet.
The clients can auto-detect static proxy server settings from the Web browser and use these for making server connections.

**Note** The use of Proxy Auto Configuration (PAC) files is not supported.

### User-to-User Shadowing

Shadowing is the process of monitoring a user’s session remotely and, optionally, participating in the session using your own keyboard and mouse. Previously reserved for administrators, this feature no longer requires administrative rights. You can now make shadowing available to users, adding powerful collaborative capabilities to a variety of applications, including:

- Help desks, where trained personnel troubleshoot applications
- Training organizations, where students observe instructors and instructors monitor student performance
- Presentation sessions, where multiple remote users attend a presentation hosted by a single user

Shadowing does not require client configuration. This feature is governed by users’ policies set on the server. For information about enabling and configuring this feature, see the *MetaFrame Presentation Server Administrator’s Guide*.

### CDE Integration

The Clients for IBM AIX, HP-UX, and Solaris (SPARC) can now be integrated with the Common Desktop Environment (CDE). CDE integration makes it easy to associate a file type on the client device with an application published on a server.

### New Features Introduced in Version 7.x

The following list outlines the new features introduced in Version 7.x of the client.

#### Program Neighborhood Agent

Program Neighborhood Agent allows the server to capture credentials and launch applications and content that are accessed by users through servers running the Web Interface. The client periodically downloads its configuration data from the server running the Web Interface, and administrators can control the configuration using the Program Neighborhood Agent Admin tool.
Desktop Integration

Desktop integration adds support for the client to the KDE and GNOME desktop environments. Static icons and menu entries are added during installation for the client. When Program Neighborhood Agent is used, icons and system menu entries are added dynamically for published applications and content.

Universal Printer Driver Support

Printing support has been supplemented by an additional software printer description for each of the client printers that are available through ICA. The additional printers are preconfigured with a single (universal) device driver so that they are ready to use without configuration as soon as the user logs on.

Installation and Update of Remote Clients

It is no longer necessary for a user with super-user (root) privileges to install, update, or remove the client software. Non-privileged users can also perform these tasks and use the client auto update feature.

SpeedScreen Browser Accelerator

SpeedScreen Browser Accelerator offers improved performance when displaying pages containing JPEG and GIF images with Microsoft Internet Explorer.

Note
If you are running Linux, this feature requires that the system JPEG library, libjpeg.so is present as part of your installation.

Non-Rectangular Seamless Windows

The client supports the rounded edges of the Luna theme, which is available in Microsoft Windows Server 2003. Other window shapes that can be defined in Windows applications are also supported.

Keyboard Accelerators

Several keyboard accelerators have been added to assist users who prefer or need to use the keyboard, rather than the mouse, when using the client.

Other Enhancements

Version 7.x of the client also provides enhancements in the following areas:
Connection Center

The Connection Center displays the current sessions and seamless windows that are in use. It has been enhanced to allow users and administrators to control sessions more easily, and to view the state and statistics of sessions.

Browser Support

Previous versions of the client supported Netscape 4. Version 7.x supports Mozilla and related browsers such as Netscape 6, Netscape 7, Galeon, and Konqueror.

New Features Introduced in Version 8.x

The following list outlines all the new features in this release.

Workspace Control

Workspace control enables users to quickly switch among client devices and is especially useful to roaming or mobile users.

Administrators can configure the Workspace Control settings available to users of the Presentation Server Console or Web Interface Console using the Program Neighborhood Agent Admin Tool. If the Workspace Control configuration settings of the Presentation Server Console or the Web Interface Console are configured to allow users to override the server settings, users can configure Workspace Control in the Settings options of the Web Interface or the Reconnect page of the Program Neighborhood Agent Properties dialog box. For more information about configuring this feature, see “Configuring Workspace Control” on page 94.

Digital Dictation Support

MetaFrame Presentation Server now supports client-side microphone input. This allows you to publish dictation software for use in client sessions. Using local microphones, users can record dictations from a device in one location and then retrieve them for review or transcription from another device or location.

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. Digital dictation support is available with MetaFrame Presentation Server Advanced and Enterprise Editions.

For users to take and play back digital dictations in client sessions, administrators must enable audio input (for microphones) and output (for speakers) on the server. For information about configuring this feature on the server, see the MetaFrame Presentation Server Administrator’s Guide.
For users to configure digital dictation support for individual connections, audio input support must also be enabled on the client. For information about configuring this feature on the client, see “Configuring Digital Dictation Support” on page 79, and “Configuring Keyboard Options, Alert Sounds, Automatic Updates and Digital Dictation Support” on page 81.

**Dynamic Session Reconfiguration**

This feature creates a smoother experience for users who switch among client devices with varying display capabilities by reconfiguring window appearance appropriately among devices. Users don’t need to reconfigure the color depth and resolution for a session that they reconnect to on a client device with different display capabilities. The existing session’s display automatically adapts to the reconnecting client device’s display capabilities and mode preference.

When connecting to a computer running Metaframe Presentation Server 3.0, this feature enables users to resize non-seamless windows.

**Zone Preference and Failover**

A new policy rule enables you to direct user connections to preferred zones and set transparent failover to backup zones when preferred servers are unavailable. When users open applications, the Zone Preference and Failover policy rule directs their connections to the server with the highest zone preference and lightest load.

The Zone Preference and Failover rule is available if you are using the Enterprise Edition of MetaFrame Presentation Server. For more information about configuring this feature, see the MetaFrame Presentation Server Administrator’s Guide.

**Improved Logon Look and Feel**

The appearance of the Progress dialog has been improved. This dialog now remains visible until the server starts to display the progress of the user’s logon to the session. This enables the user to check that the logon process is continuing satisfactorily.

**General Performance Improvements**

**Better ICA Performance**

New compression technology results in less data being sent over the network. This results in, for example, faster video rendering, file transfer, and printing, and provides a better overall user experience.
ThinImage
The server uses lossy compression for graphics. This reduces bandwidth consumption and provides faster rendering for the entire desktop session.

Note If you are running Linux, this feature requires that the system JPEG library, libjpeg.so, is present as part of your installation.

Other Enhancements
Version 8.x of the client provides enhancements in the following areas:

Middle Button Paste
Version 8.x of the client supports the use of middle button paste when connecting to Windows applications running on a server.

Windows System Tray Emulation Window
Version 8.x of the client provides a Windows SystemTray Emulation Window. If you are running in seamless mode, and using applications that add icons to the Windows System Tray, these will appear in the emulation window instead.

Unicode Support
Version 8.x of the client supports the use of UTF-8 characters in ICA files.

Diagnostic Information
Version 8.x also provides a facility for obtaining diagnostic information about the client. Citrix Support may ask you for this information to help diagnose and rectify any problems you may experience when running the client.

xcapture
To improve usability, you can now run xcapture from the main client window.
Deploying the Clients for UNIX

Overview

This chapter describes how to install, deploy, and remove the Clients for UNIX. Topics covered in this chapter include:

• System requirements
• Installing the client
• Starting the client
• Preparing for client auto update
• Using the client update database
• Removing the client
• Using the client as an “ICA to X proxy” (Server Side ICA)
• Supporting faster browsing

System Requirements

The Clients for UNIX support the following systems and versions.

<table>
<thead>
<tr>
<th>UNIX System</th>
<th>Supported Version of UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compaq Tru64 UNIX</td>
<td>3.2 or above</td>
</tr>
<tr>
<td>HP-UX</td>
<td>10.20 or above</td>
</tr>
<tr>
<td>IBM AIX</td>
<td>4.3.1 or above</td>
</tr>
<tr>
<td>Linux</td>
<td>Red Hat 6.1 or above, and other distributions that include the standard C library, glibc, version 2.1.2 and above.</td>
</tr>
<tr>
<td>SCO</td>
<td>UNIXWare 7, UNIXWare 2.1*, OpenServer 5*</td>
</tr>
<tr>
<td>SGI IRIX</td>
<td>6.3 or above</td>
</tr>
</tbody>
</table>
Systems running the clients require the following:

- 4 MB of free disk space for the installed client and up to 12 MB if you expand the installation package on the disk
- 16 color video display or higher
- TCP/IP networking

**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.

**Other Factors to Consider before Installation**

If you are installing a client on a machine that doesn’t already have a client installed on it, you must install the client manually. See “Installing the Clients for UNIX” on page 31 for details.

If you already have a previous version of the client, you can update it automatically to the latest version by adding this client to the client update database. See “About Client Updates” on page 34 for details.

If you are using the Web Interface in conjunction with Citrix MetaFrame Presentation Server for Windows, see the Web Interface Administrator’s Guide for information about deploying Clients for UNIX with the Web Interface.
Installing the Client for Linux from the Web

An RPM Package Manager (RPM) for the Linux client is available for download and installation from the Citrix Web site. Compared to .tar.gz files, RPM packages assist you in installing, upgrading, and uninstalling UNIX software. However, if you use the RPM package for the Linux client, you cannot:

- Specify the directory where the Linux client is installed
- Enable desktop integration
- Integrate the Netscape browser

If these features are important to you, install the Linux client from a file that is compressed using an alternative, non-RPM, format. You can download both packages for the Linux client (and compressed installation files in other formats) from the support pages of the Citrix Web site (http://www.citrix.com/).

Installing the Clients for UNIX

Before installing the client, ensure that you have at least 12 MB 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>

To install the client

1. (Optional) If you want to enable the desktop and browser integration features, log on as a privileged user (root) at the client workstation. All other features of the client will be installed if you log on as a non-privileged user.

2. Open a command window.

3. If you are installing the client from a CD-ROM, insert the CD-ROM in the drive. Mount the CD-ROM using the appropriate instructions for your workstation. Change to the ICAinst/IcaUNIX directory (ICAclient/IcaUNIX for Version 3.0 installations) on the mounted CD-ROM.

   — Or —

   If you are installing the client from a tar file, uncompress the tar file and extract the contents into a temporary directory.
4. Run the setup program by typing `./setupwfc` and press ENTER.
   — Or —
   If file names on the CD-ROM are displayed in uppercase and are followed by
   other characters (such as ;1), use the command `./SETUPWFC*` and press
   ENTER.
   A menu of options appears.

5. To install the client, type 1 and press ENTER.
   The installation procedure prompts:
   Please enter the directory in which Citrix ICA Client is
to be installed [default /usr/lib/ICAClient] or type
"quit" to abandon the installation:

6. To install in the default location, press ENTER.
   The installation procedure allows you to confirm that you want to proceed.

7. To proceed, type y and press ENTER. To cancel the installation, type n and
   press ENTER.
   The installation procedure displays the Client Software License Agreement and
   then prompts for confirmation to proceed.

8. To proceed, type 1 and press ENTER. To cancel the installation, type 2 and
   press ENTER. If you have Netscape Navigator installed, you are prompted to
   choose installation of the plug-in. If you require the plug-in, press y.

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

The default directory for non-privileged-user installations is $HOME/ICAClient/
platform (for example, $HOME/ICAClient/linuxx86 for the Linux/x86 platform).
Starting the Clients for UNIX

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 the KDE and GNOME desktop environments for Linux.

The client may reside in different menus depending on your Linux distribution. The menu locations for some popular distributions are noted in the following procedure.

KDE

Red Hat and SuSE distributions: On the K menu, click Internet > Citrix ICA Client. The main client window appears.

Mandrake distributions: On the K menu, click Networking > Citrix ICA Client. The main client window appears.

Other distributions: On the K menu, click Applications > Citrix ICA Client. The main client window appears.

GNU

All distributions: On the Citrix menu, click Citrix ICA Client.

Clicking the Citrix ICA Client option on a menu in the KDE or GNOME environment starts the client. The main client window appears.
Updating the Clients for UNIX

The client can be set up so that you can automatically update it from a server when a newer version of the client is available. This means that you can “push” a new version of the client software from the client update database to the workstation instead of installing the client manually at each workstation.

To enable the client software for automatic update

1. On the Tools menu, click Settings.
2. From the drop-down list, choose Preferences to display the Preferences page.
3. Select Allow Automatic Client Updates to allow the client to be automatically updated with a newer version from the server.

About Client Updates

Client auto update allows future versions of clients for your platform to be automatically downloaded when a user connects to a server. The new versions of the clients are downloaded from the client update database.

Client auto update:

• Automatically detects older client files
• Provides full administrative control of client update options for each client
• Updates clients from a single database on a network share point
• Safely restores older client versions when needed

During the client update, new client files are copied to the client device. The administrator can force the user to disconnect and complete the update before continuing the session. The user must log on to the server again to continue working.

In case of a problem, the existing client files are saved in a hidden directory called .bk in /usr/lib/ICAClient.

Configuring the Client Update Database

You can configure a client update database on each server in a server farm or configure one database to update the clients for multiple servers.

The client update database contains several clients. As Citrix releases new versions of the clients, you add them to the client update database.

Use the ICA Client Update Configuration utility to:

• Create a new update database
• Specify a default update database
• Configure the properties of the database
• Configure client update options
• Add new clients to the database
• Remove outdated or unnecessary clients
• Change the properties of a client in the database

To start the ICA Client Update Configuration utility
• On a computer running MetaFrame Presentation Server, from the Start menu, select Citrix > ICA Client Update Configuration.
• From a MetaFrame XP server: From the Start menu, choose Programs > Citrix > MetaFrame XP > ICA Client Update Configuration.
  In the Client Update Configuration window, the status bar shows the location of the current update database that MetaFrame Presentation Server uses to update clients. The window shows the clients in the database.

Creating a New Client Update Database

The ICA Client Distribution wizard creates the Client Update Database in the directory %Program Files%\Citrix\ICA\ClientDB. You can create a new update database in any location on a server drive or on a network share point.

To create a new update database
1. On the Database menu, click New.
2. In the Path for the new Client Update Database dialog box, type the path for the new update database and click Save.
   The utility creates a new update database in the specified location and opens the new database.

Specifying a Default Client Update Database

You can configure one client update database to be used by multiple servers. If the client update database is on a shared network drive, use the ICA Client Update Configuration utility to configure your servers to use the same shared database.

To set the default database
1. On the Database menu, click Open. The Open Existing Database dialog box appears.
2. In the **Open Existing Database** dialog box, type the path to the default database and click **Open**.

3. From the **Database** menu, choose **Set Default**.

4. Select **Set as Default Database on Local Machine** to make the currently opened database the default database. You can also set other servers to use the currently open database as the default database.

5. Expand the node for a domain name to view the servers in that domain. Click a server to set its default database to the currently open database. You can select multiple servers by holding down the CTRL key and clicking each server.

6. Click **OK**.

### Configuring the Properties of the Client Update Database

Use the **Database Properties** dialog box to configure overall database-wide settings for the current client update database.

**To configure database properties**

1. On the **Database** menu, click **Properties**.
   - The **Database Path** box displays the path and file name of the database you are configuring.

2. For this database to perform client updates, select **Enabled**.

   **Tip** If the clients do not need to be updated, disable the database to shorten logon time for your users.

The options in the **Default update properties for clients** section specify the default behavior for the clients added to the database. You can also set properties for individual clients (as described later in this chapter). Individual client properties override the database properties.

- Under **Client Download Mode**, select **Ask user** to give the user the choice to accept or postpone the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user’s client without notifying or asking the user.

- Under **Version Checking**, select **Update older client versions only** to update only client versions that are older than the new client. Select **Update any client version with this client** to update both earlier and later versions of the client to this version; choose this option to force an older client to replace a newer client.
• Under Logging, select Log downloaded clients to write an event to the event log when a client is updated. By default, errors that occur during a client update are written to the event log. Clear the Log errors during download check box to turn this option off.

• Under Update Mode, select the Force disconnection option to require users to disconnect and complete the update process after downloading the new client. The Allow background download option is selected by default to allow users to download new client files in the background while they continue to work. Clear this check box to force users to wait for all client files to download before continuing.

3. Specify the number of simultaneous updates on the server. When the specified number of updates is reached, new client connections are not updated. When the number of client updates is below the specified number, new client connections are updated.

4. Click OK when you finish configuring the database settings.

Adding Clients to the Client Update Database

When you want to deploy a newer version of the client software, add it to the Client Update Database. You can download the latest client software from the Citrix Web site at http://www.citrix.com/download.

To add client software to the Client Update Database

1. On the Client menu, click New to display the Description screen.

2. In the Client Installation File box, browse to or enter the path to the client installation file Update.ini.
   The client installation file, Update.ini, is located in the root of the update packages.

3. The client name, product number, model number, and version number are displayed. The Comment text box displays a description of the new client. You can modify this comment. Click Next to continue.

4. The Update Options dialog box appears. The options in this dialog box specify how the client update process occurs for this client. The database-wide update options are displayed. You can specify different behavior for individual clients. For definitions of the options in this dialog box, see the online help for this dialog box. Click Next when you finish configuring the client update options.
5. The **Event Logging** dialog box appears.
   The database-wide logging options are displayed. You can specify different behavior for individual clients. Select **Log Downloaded Clients** to write an event to the event log when this client is updated. By default, errors that occur during a client update are written to the event log. Clear the **Log Errors During Download** check box to turn this option off. Click **Next** to continue.

6. The **Enable Client** dialog box appears.
   The Client Update Database can contain multiple versions of client software with the same product and model numbers. For example, when Citrix releases a new version of the MetaFrame Presentation Server Clients for UNIX, you add it to the Client Update Database. However, only one version of the client can be enabled. The enabled client is used for client updating.

7. Click **Finish** to copy the client installation files to the Client Update Database.

**Removing a Client From the Client Update Database**

It is important to delete clients that are not used from the client update database. A database with multiple versions of the same client unnecessarily slows the checking procedure that is carried out each time a user connects to the server.

**To remove a client from the database**

1. In the Client Update Configuration window, select the client you want to remove from the database.

2. From the **Client** menu, choose **Delete**. A message box asks you to confirm the deletion.

3. To remove the client, click **Yes**.

**Changing the Properties of a Client**

Use the **Properties** dialog box to set properties for an individual client. Individual client properties override the database properties.

**To change the properties of a Client**

1. In the ICA Client Update Configuration window, select the client whose properties you want to edit.

2. On the **Client** menu, choose **Properties**.
   The **Properties** dialog box contains tabs labeled **Description**, **Update Options**, **Event Logging**, and **Client Files**.
   The **Description** tab of the **Properties** dialog box lists the client name, product number, model number, and version number.
3. To update the same platform client to this version, select **Enabled**.

4. Use the **Update Options** tab to configure update options for the client.
   - Under **Client Download Mode**, select **Ask user** to give the user the choice of accepting or postponing the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user’s client software without notifying or asking the user.
   - Under **Version Checking**, select **Update older client versions only** to update only client versions that are older than the new client. Select **Update any client version with this client** to update all client versions to this version. Select this option to force an older client to replace a newer client.
   - Select the **Force Disconnection** option to require users to disconnect and complete the update process after downloading the new client.
   - Select the **Allow Background Download** option to allow users to download new client files in the background while they continue to work. Clear this check box to force users to wait for all client files to download before continuing.
   - Type a message to be displayed to users when they connect to the server.

5. Use the **Event Logging** tab to configure logging settings for this client.
   - Select the **Log Downloaded Clients** option to write an event to the event log when a client is updated.
   - Select the **Log Errors During Download** option to write errors that occur during a client update to the event log.

6. Use the **Client Files** tab to view the list of files associated with this client.

7. Click **OK** when you finish configuring the settings for the client.

---

**Uninstalling the Clients for UNIX**

To uninstall the client

1. Run the setup program by typing `/usr/lib/ICA/Client/setupwfc` and press ENTER.

2. To remove the client, type **2** and press ENTER.
Using the Client 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 (SPARC) includes 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 Clients for UNIX 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.
Chapter 3  Deploying the Clients for UNIX

Server Sizing

If you want to use a PC running Linux to act as the proxy, the following example is a guide:

- Pentium 166 MMX (no L2 cache), 64MB RAM, Red Hat 6.1, SuSE 6.4, Slackware 7.0, Debian 2.2, and Caldera 2.4
- Linux client Version 6.30
- Sessions directed to an IBM Netstation 100 running as an X terminal

In tests, each ICA session used approximately 2.5 MB of RAM on the Linux proxy device. With six sessions, the running CPU load was 20-25% with each connection running an “average user load” stress test. This indicates that a Pentium II 400 with 128 MB RAM could be expected to comfortably support 40 X11 sessions.

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 will not be 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 Clients for UNIX with “Server Side ICA”

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

1. 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:
   \[ xhost <\text{proxy server name}> \]

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 the command prompt, type:
   \[ \text{wfcmgr } \& \]

**Note** If you get font errors on the local X display when you start the client, start the font server on the proxy server — on Linux just type `xfs &`; on Solaris type `xfs –port fs`.

### 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’s installation includes the `libjpeg.so` JPEG library. This library is built into the Solaris (SPARC) client 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, Microsoft Internet Explorer and other browsers still operate in the absence of this library, but SpeedScreen Browser Accelerator does not function.
Configuring the Clients for UNIX

Overview

This chapter describes how administrators can configure the Clients for UNIX. It also contains procedures that support typical day-to-day 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 normally performed by administrators.

Topics in this chapter include:

- Creating connection entries
- Viewing connection entries
- Opening a connection
- Managing your connections
- Changing a connection entry
- Using xcapture
- Enabling smart card support
- Integrating the client with security solutions
- Mapping client devices
- Changing default settings
- Integrating the client with CDE
- Integrating the client with KDE and GNOME
- Accessing published resources with the Program Neighborhood Agent
- Configuring session options
• Setting up extended parameter passing
• Setting up server-client content redirection

Creating Connection Entries

Users can create two types of connections to servers:

• A connection to a desktop session 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.
2. On the Connections menu, click New.
   The Properties dialog box appears with the Network page displayed.

   **Note** You can copy an existing entry by highlighting the required entry and then choosing Copy from the Connections menu. You can then edit the copied entry as required. This is useful if many of the configuration details are the same for both entries.

3. Click Server or Published Application.
4. For a desktop session, type the name or IP address of the server or select the name from the pop-up menu to the right of the Server field.
   — Or —
   For a published application, type the name of the published application or select the name from the pop-up menu to the right of the Server field.
5. If you type the name of the server or published application, type a unique description for the entry in the Description field. The description is used to identify the connection in the main client window.
   If you select a server or published application from the pop-up menu, a default description is automatically added.
6. Click OK to save the entry or Cancel to exit the Properties dialog box without saving the entry.
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 55.

### Viewing Connection Entries

By default, the main client window displays the Connection view, a list of all the connection entries that users created, including connections to published applications and remote desktop sessions. Immediately after installing the client, this list may be empty.

*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 automatically set up to applications and content published on a server running the Web Interface, they can do so using the PNAgent view.
To view the published resources on a server running the Web Interface

On the View menu, click Go To > PNAgent View. A list of resources on the Web server appears:

![Screen capture of the PNAgent view](image)

*This screen capture shows the PNAgent 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 are displayed.

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 MetaFrame Presentation Server Administrator’s Guide or the Citrix MetaFrame Presentation Server for UNIX Administrator’s Guide.

To view the connections that were created from the client

On the View menu, click Go To > Connection View.

Opening a Connection

Users can connect to published resources on a server in a number of ways:

- From the main client window (the Connection view)
- Using the Program Neighborhood Agent (only for connections to published resources):
  - From the PNAgent view
  - From menu items created by the Program Neighborhood Agent
  - From desktop items created by the Program Neighborhood Agent
  - From a UNIX prompt
• 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. On the Connections menu, click Connect.

To open an application from the PNAgent view
1. In the PNAgent view, select the application to which you want to connect.
2. On the PNAgent menu, click Connect.

To open a connection from the command line
At the command prompt, type:
/usr/lib/ICAClient/wfica -desc "description"
where “description” is the full text from the Description field of the connection entry. If the description contains spaces, enclose them 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 Server Location and Business Recovery” on page 82 and “Connecting through a Proxy Server” on page 60 for details.

To open a connection using a Web browser
If you are using Netscape Navigator, 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 Netscape Navigator 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.)

The .mailcap file modification is:

• In $HOME, create or modify the .mailcap file and add the line:
  • For Version 3.0 clients:
    application/x-ica; /usr/lib/ICAClient/wfica -file %s
  • For Version 6.0 and later clients:
    application/x-ica; /usr/lib/ICAClient/wfica -file %s;
    x-mozilla-flags=plugin:Citrix ICA
The %s indicates that the full filename of the .ica file is passed to the application. The additional text in the Version 6.0 .mailcap file is to make use of the Netscape ICA Client plug-in.

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 allows users to:

- Close applications
- Log off or disconnect from desktop sessions and published applications
- Manage connection windows
- Analyze connection transport statistics for desktop sessions

The Connection Center is a useful productivity tool that allows 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 applications and desktop sessions are listed and a summary of all the connections, showing the total number of servers and applications in use, is presented at the bottom of the Connection Center dialog box.

To manage a connection window

In the Connection Center, select a published application or desktop session from the list and click one of the following buttons:

- **Logoff**: Ends the selected session and closes any open applications.
- **Refresh**: Refreshes the list of sessions and applications with up-to-date information.
- **Properties**: Displays the Connection Center Status dialog box, which contains transport statistics for the selected session.
• **Disconnect**: Cuts the selected connection to the server but any open applications are not closed unless the server is configured to do so on disconnection.

• **Terminate**: Closes the selected application.

• **Iconify**: Minimizes the window used by the selected application or session.

• **Restore**: Displays the window used by the selected application or session.

To analyze the transport statistics for a desktop session

1. On the **Tools** menu, click **Connection Center**.

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

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

**Note**  Transport statistics are available only for desktop sessions, not published applications.
Changing a Connection Entry

This section describes how to change properties for an existing 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 50.
   - 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 51. You also use the Connection page to configure support for middle button paste functionality. See “Configuring Middle Button Paste Functionality” on page 54.
   - The Firewall page, where you can specify proxy server settings. See “Connecting through a Proxy Server” on page 60.
   - 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 54.
   - 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 55.
   - 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 56.
   - The Auto-reconnect page, where you specify settings for auto client reconnection. See “Configuring Auto Client Reconnect” on page 85.

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** field.
   - 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 ICA master browser, click **Network Protocol**. If a firewall restricts UDP messages, select **TCP/IP+HTTP** from the list. In Version 6.20 and later of the client, TCP/IP+HTTP is the default setting. For more information about network protocols, see “Configuring Network Protocol” on page 86

### 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 on page 54, can also reduce the bandwidth required for a high-performance connection

- **Use the latest versions of MetaFrame Presentation Server and Clients for UNIX** — 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 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.

Note 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 84.

Data Compression

Data compression reduces the amount of data transferred across the ICA session. 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.
Chapter 4 Configuring the Clients for UNIX

**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 MetaFrame Presentation Server documentation for more details.

To change SpeedScreen 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 is immediately changed to an hourglass indicator. Select a mode from the drop-down list:
   - 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** hotkey.

**Note**  Local text echo does not support input using an Input Method Editor (IME).

**Reducing the Window Size**

Change the window size to the minimum you can comfortably use. See “Configuring Default Window Settings” on page 81 for more information.

**Modifying Color Depth**

Reducing or increasing color depth can improve performance. See “Configuring Default Window Settings” on page 81 for more information.

The color depth required to achieve optimum performance varies between applications; for example, applications such as Word and Internet Explorer which assemble their screen image off screen, use less bandwidth when color depth is increased.
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 78 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.

Configuring Middle Button Paste Functionality

Use the Connections page in the Properties dialog box to enable middle button paste functionality for users connecting to Windows applications running on a server.

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 Connections to display the Connections page.

4. Select the Enable middle button paste check box.

Specifying an Application to Run at Connection

Use the Application page in the Properties dialog box to specify an application to run 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** field, specify the pathname of an application to be run after connecting to a server.
   - In the **Working Directory** field, 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.

### Changing the Window Properties

The **Window** page controls the window size and number of colors 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** allows 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** 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** allows you to set the number of window colors to **16**, **256**, **32 Thousand**, or **16 Million**. Your display must be capable of displaying the resolution and color depth you select. You can specify only a color depth greater than 256 colors on Version 6.0 and later clients.
• **256 Color Mapping** allows 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 uses 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 81.

### Configuring Logon Properties

The **Login** page allows you to enter logon details of 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**, **Domain** (optional) and **Password** 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 59.

### 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 without logging off.

**Note** Version 8.x of the Clients for UNIX provides new functionality that enables users to disconnect from running applications, reconnect to applications, or log off from running applications, when moving among client devices and starting new sessions. For more information see “Configuring Workspace Control” on page 94.
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.

Auto client reconnect incorporates a re-authentication mechanism based on encrypted user credentials. When a user initially logs on to a server to use an application, MetaFrame Presentation Server encrypts and stores the user credentials in memory and sends the encryption key to the client. For reconnection, the client submits the key to the server. The server decrypts the credentials and submits them to Windows logon for authentication.

When the client detects that its connection to the server is unexpectedly broken, it waits 30 seconds before beginning the reconnection sequence. By default, the client attempts to reconnect four 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 85.

**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**.

**Note**  Auto client reconnect works in the same way regardless of whether a user logged on conventionally or with a smart card. Users who log on to an ICA session using a smart card are automatically reconnected if their session fails and will not have to reenter their PIN number, provided that their smart card remains in the smart card reader.

---

**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 ICA UNIX client).

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 the application in 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 command in the application in the connection window to paste the information.
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.

Enabling Smart Card Support

Version 6.30 and later of the Clients for UNIX (except the HP-UX Client) 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 computers running MetaFrame Presentation Server.

**Smart card application support.** Allow smart card-aware published applications to access local smart card devices.

For more information about configuring smart card support on your servers, see the *MetaFrame Presentation Server 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 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 bypass package, available for download from www.sun.com
To configure smart card support

Note that smart card support is not enabled for the HP-UX Client.

1. In the main client window, click New on the Connections menu to configure a new connection.
   — Or —
   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.

Note  Auto client reconnect works in the same way regardless of whether a user logged on conventionally or with a smart card. Users who log on to a MetaFrame Presentation Server session using a smart card are automatically reconnected if their session fails and will not have to reenter their PIN number, provided that their smart card remains in the smart card reader. However, roaming user reconnect is not supported for connections that use smart card authentication.

Integrating the Clients for UNIX with Security Solutions

You can integrate the client with a range of security technologies, including proxy servers, firewalls, and SSL/TLS-based systems. This section describes:

- Making a connection through a SOCKS proxy server or Secure proxy server (also known as Security proxy server, HTTPS proxy server, or SSL tunneling proxy server)
- Integrating clients with the Secure Gateway or Citrix SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
- Connecting to a server across a firewall using alternate addressing
- Using ICA encryption to help protect data on local networks

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 and, from Version 6.30, the Secure proxy protocol.

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 try 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 only with Netscape for UNIX 4.0 or later, and only if Netscape is statically configured. Auto-client proxy detection is not supported if Netscape is configured to use PAC (Proxy Auto Configuration) files.

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 Netscape settings.
4. Click OK.

To configure auto-client proxy detection for an individual server connection
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 Use Netscape settings.

   **Important** If the list appears dimmed, clear the Use Default check box to stop using the default protocol, and then select Use Netscape 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 UNIX clients, 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 address or IP number in the Proxy Address field and the port number in the Port field for the SOCKS proxy server.
5. 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 address or IP number in the Proxy Address field and the port number in the Port field for the SOCKS proxy server.
6. Click OK.

Connecting through a Secure Proxy Server

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.
4. Type the proxy address or IP number in the Proxy Address field and the port number in the Port field for the SOCKS proxy.
5. 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 SOCKS.

5. Type the address or IP number in the Proxy Address field and the port number in the Port field for the SOCKS proxy server.
6. Click OK.

**Connecting across a Firewall**

Network firewalls can allow or block packets based on the destination address and port. If you are using ICA through a network firewall, use the information provided in this section to configure the firewall settings. You can configure the client to connect to a server through a firewall.

**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 in the Server Location page. See “Configuring Server Location and Business Recovery” on page 82.

**Using ICA Encryption**

Encryption increases the security of your server connection. By default, basic encryption is enabled on all connections. The server must be configured to allow the selected encryption level or greater. To enable encryption levels higher than Basic, the server must support ICA encryption. This support is included with ICA encryption and MetaFrame XP Feature Release 1 or later.
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.

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 Versions 6.20 and later)

Version 6.20 and later of the Clients for UNIX support the SSL protocol, and Version 6.30 also supports 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 MetaFrame installation will also work with TLS. Some organizations, including US government organizations, require the use of TLS to secure data communications.

To specify a Secure Gateway server that is configured to run in Relay mode

To use an ICA file to connect to the Secure Gateway relay server, modify the .ica file as follows:

1. Open the .ica file.
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 relay server to which you want to connect.

3. Save and close the file.

For more information about the Secure Gateway, see the Secure Gateway 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 SSL and TLS are enabled, each time you initiate a connection the client tries to use TLS first, then tries 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:

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Issuing Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class4PCA_G2_v2.crt</td>
<td>VeriSign Trust Network</td>
</tr>
<tr>
<td>Class3PCA_G2_v2.crt</td>
<td>VeriSign Trust Network</td>
</tr>
<tr>
<td>BTCTRoot.crt</td>
<td>Baltimore Cyber Trust Root</td>
</tr>
<tr>
<td>GTECTGlobalRoot.crt</td>
<td>GTE Cyber Trust Global Root</td>
</tr>
<tr>
<td>GTECTRoot.crt</td>
<td>GTE Cyber Trust Root</td>
</tr>
<tr>
<td>Pcs3ss_v4.crt</td>
<td>Class 3 Public Primary Certification Authority</td>
</tr>
<tr>
<td>SecureServer.crt</td>
<td>Secure Server Certification Authority</td>
</tr>
</tbody>
</table>

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.
Important Certificate key lengths of greater than 2048 bits are not supported on the client. Ensure that the bit lengths of Certificate Authority root and intermediate certificates, and of your server certificates, are supported by the client or connection may fail.

To configure the client to use SSL 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 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 from the Network Protocol list.

5. Select the server location.
   • Select the Use Default check box.
     — Or —
   • Enter the fully qualified domain name of the machine to use for server browsing in the Server Location box.
6. If you are connecting to a server, enter the fully qualified domain name of the server in the Server box.
7. Click OK.

To configure the client to use SSL as the default protocol
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 from the Network Protocol list.
   You can specify this protocol for all connections or for individual server groups/servers using the Server Group list and Address List.
4. Click OK.
Chapter 4 Configuring the Clients for UNIX

Note If you attempt to make a non-SSL connection to an SSL server, you will not be connected and a connection failed message will appear.

To configure the client to use TLS on a single connection
1. In the main client window, select the connection entry for which you want to use TLS.
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 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 from the Network Protocol list.

5. Select the server location. Either
   - Select the Use Default check box.
     — Or —
   - Enter the fully qualified domain name of the machine to use for server browsing in the Server Location box.
6. If you are connecting to a server, enter the fully qualified domain name of the server in the Server box.
7. Click OK.

To configure the client to use TLS as the default protocol
1. In the main client window, select Settings from the Tools menu.

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 from the Network Protocol list.
4. You can specify this protocol for all connections or for individual server groups/servers using the Server Group list and Address List.
5. 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 Administrator’s Guide or Citrix SSL Relay service documentation for more information.

Mapping Client Devices

The client supports client device mapping for connections to servers. Client device mapping allows 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 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.

This section includes more information about:

- Mapping COM ports
- Mapping client drives
- Mapping client printers
- Mapping client audio
- Configuring digital dictation support

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 allows a user at the client workstation to use local devices like 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, 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.

You can control drive mapping on the server, in the **Client Settings** dialog box in **Citrix Connection Configuration**. Use the **Connection** settings to specify the devices to automatically map at logon. You can also use the **Client Mapping Overrides** to allow a user to control the device mapping from the client workstation during ICA sessions, in the **Drive Mapping** dialog box. Use this dialog box to specify which folders and drives to map at logon. This applies for all connection sessions.

**To specify the drives and directories to automatically map during logon**

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

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

   For each drive letter, the **Drive Mapping** list shows the disk or pathname of the UNIX directory mapped to the drive. In the **Enable/Read/Write** columns, icons display whether or not 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 field 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 field 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 server, the specified directory is mapped to another free drive letter at logon.
6. Specify the access for the drive by clicking the corresponding read/write icons.
   You can use:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕵️  (Pair of glasses)</td>
<td>Read Access</td>
</tr>
<tr>
<td>🕵️❓ (Pair of glasses, with question mark to the right)</td>
<td>Prompt for read access on first access per session</td>
</tr>
<tr>
<td>🕵️❌ (Pair of glasses, obscured by a cross)</td>
<td>No read access</td>
</tr>
<tr>
<td>✍️   (Pencil)</td>
<td>Write access</td>
</tr>
<tr>
<td>🕵️❓ (Pencil, with a question mark to the left)</td>
<td>Prompt for write access on first access per session</td>
</tr>
<tr>
<td>🕵️❌ (Pencil, obscured by a cross)</td>
<td>No write access</td>
</tr>
</tbody>
</table>

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:

   ![My Computer screenshot](image)

   *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 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.
6. Click Browse.
7. In the Browse For Folder dialog box, expand Client Network.
8. Expand Client, and select the appropriate entry for your UNIX directory from the list of available client drives.
9. If you want to have this drive available to you each time you log on to this server, check Reconnect at Logon.
10. 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 or not 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 mounted 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 mounted 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 for Windows with Feature Release 3 or later provide a simplified printing setup using the universal printer driver. If the client 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 for Windows with Feature Release 3 or later, 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.
Note  Autocreated printers are not used on MetaFrame Presentation Server for UNIX. The client’s default printer is used instead.

This section describes how to set an autocreated printer. The printer used by the system is the default printer set in the configuration file. 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 machine 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.

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 (Auto Created Client printer) is displayed after the default printer.

1. Open a configuration file. Either:
   • Open wfclient.ini, in the $HOME/.ICAClient directory to apply the autocreated printer for a single user
   — Or —
   • Open module.ini, in the $ICAROOT/config directory to apply the autocreated printer to all clients

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 renaming it in the print management utility.
To autocreate non-default printers for a Linux client

1. In /etc/printcap, locate the printers that you want to set as the autocreated printers.
2. Add the following option:
   :wd=drivername\n   where drivername is the name of the driver for the autocreated printer.

---

Important  The Common UNIX Printing System (CUPS), re-creates /etc/printcap at startup. To avoid re-creating 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 the:
   - $HOME/.ICAClient directory to limit the printers for a single user
     — Or —
   - $ICAROOT/config directory to limit the printers for all users of the UNIX clients—all users in this case being those who 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 (:).
3. Save and close the file.

Mapping Client Printers on MetaFrame Presentation Server for Windows

This section describes how to map client printers on MetaFrame Presentation Server for Windows.

To map a local printer on a server

1. From the client, start a server connection and log on to MetaFrame Presentation Server.
2. On the Start menu, click Settings > Printers.
4. Use the wizard to add a network printer from the Client Network, Client domain with a name similar to workstation\printer.

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

**Mapping Client Printers on MetaFrame Presentation Server for UNIX**

Before users can print to a client printer from MetaFrame Presentation Server for UNIX, printing must be enabled by the administrator. This section describes how to enable printing on the server. It describes how users can list available client printers and print files from the command line or from applications.

In a UNIX environment, the application performs the print rendering. The printer driver is specified inside the application or, in the case of a desktop utility, raw text is generated.

**Note** For more information about printing from MetaFrame Presentation Server for UNIX, see the *Citrix MetaFrame Presentation Server for UNIX Administrator’s Guide* and the manual pages.

**Setting up Printing**

**To check if client printing is currently enabled or disabled**

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   ```
   ctxcfg -p list
   ```

   The printing status is displayed.

**To enable or disable client printing**

1. Log on to the server as an administrator.
2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable client printing</td>
<td>ctxcfg -p enable</td>
</tr>
<tr>
<td>Disable client printing</td>
<td>ctxcfg -p disable</td>
</tr>
</tbody>
</table>

**To display mapped client printers**

At a command prompt, type:
ctxprinters

A list of printers configured on the client and mapped for use from the ICA session is displayed. (default) is displayed after the name of the printer that is the default. The following information is shown for each printer:

- Printer name or printer port (for example, lpt1). This can be used in the ctxlpr -P command to specify a printer other than the default.
- Printer driver name. This is for information only.
- Printer connection description. This is for information only.

Printing

To print a file from a client session

1. At a command prompt, type ctxprinters.
2. From the results of ctxprinters, identify the printer or printer port that you want to use. To print to a printer other than the default, note the printer name—the printer name is the first item in the ctxprinters listing.
3. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print the file named filename to the default printer.</td>
<td>ctxlpr filename</td>
</tr>
<tr>
<td>Print a series of files to the default printer. Each file is treated as a separate print job.</td>
<td>ctxlpr filename filename</td>
</tr>
<tr>
<td>Print a file to a printer (or printer port) other than the default. This is the printer name or printer port shown in the first column of the output from ctxprinters.</td>
<td>ctxlpr -P [Printername</td>
</tr>
<tr>
<td>Print a file in the background.</td>
<td>ctxlpr -b filename</td>
</tr>
<tr>
<td>Print a file only if the printer is not in use. Use this option to stop an application waiting while other printer jobs are handled. If the printer is in use, an error message is displayed.</td>
<td>ctxlpr -n filename</td>
</tr>
</tbody>
</table>

Printing from Applications

The exact configuration of how to set up printing from applications depends on the behavior and user interface of the UNIX application.

If the user interface for an application allows you to specify the actual printer command to use when printing, you can configure client printing by replacing the lpr or lp command with the ctxlpr command.
When a user connects to the server and prints from the application in a session, the server redirects the output to the mapped client printer.

Often, in this type of application, you can also specify the command line modifiers on a different line. You can use the same switches for `ctxlpr` as when printing from a command line. For example, use `-P` with a printer name (or printer port) to print to a printer other than the default; use `-b` for background printing, and so on.

**Tip** If the user interface of an application does not allow you to specify the actual printer command to use when printing, determine if the application (or window manager) uses a configuration file where you can replace the `lpr` command functionality with `ctxlpr`.
Mapping Client Audio

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

An administrator can set the audio quality or enable/disable client audio mapping on the server. For more information, see the Metaframe Presentation Server Administrator’s Guide. A user can set the audio quality or enable/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 allows 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 allows reasonable performance for a low-bandwidth connection.

To configure audio mapping for a connection entry

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.

**Note**  Client audio mapping is not supported by Version 3.0 of the client for SGI IRIX, Compaq Tru-64, Sun OS, Solaris (x86), and SCO.
Configuring Digital Dictation Support

MetaFrame Presentation Server now supports client-side microphone input. This allows 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.

Digital dictation support is available with MetaFrame Presentation Server Advanced and Enterprise Editions. For information about configuring this feature on the server, see the *MetaFrame Presentation Server Administrator’s Guide*.

Prerequisites for Configuring Digital Dictation Support

Before configuring digital dictation support for a connection, confirm the following:

- The Enable Sound check box is selected on the Connections page of the Properties dialog box
- 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.

Changing Default Settings

This section describes how to change 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 default setting.

**Note** In Version 7.x and later of the client, 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.
To change the default settings

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

- The Preferences page, where you specify the settings for keyboard options, alert sounds, automatic updates, and digital dictation support that apply to all connection entries. See “Configuring Keyboard Options, Alert Sounds, Automatic Updates and Digital Dictation Support” on page 81.

- The Window page, where you specify the settings to use for all new connection entries. See “Configuring Default Window Settings” on page 81.

- The Server Location page, where you specify the server address for the server that will report the ICA master browser. See “Configuring Server Location and Business Recovery” on page 82.

- The Hotkeys page, where you define alternative key combinations for system hotkeys. See “Configuring Hotkeys” on page 83.

- The Disk Cache page, where you define settings for the disk cache. See “Changing Settings for the Disk Cache” on page 84.

- The Drive Mapping page, where you set up drive mappings. See “Mapping Client Drives” on page 69.

- The COM Ports page, where you configure COM port mapping. See “Mapping COM Ports” on page 68.

- The Firewall settings page, where you configure firewalls and a SOCKS proxy. See “Integrating the Clients for UNIX with Security Solutions” on page 60.

- The Auto Reconnect page, where you specify settings for auto client reconnection. See “Configuring Auto Client Reconnect” on page 85.

- The PNAgent page, where you identify and configure the server running the Web Interface. See “Accessing Published Resources with the Program Neighborhood Agent” on page 88.
Configuring Keyboard Options, Alert Sounds, Automatic Updates 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 field, click the Browse button to select your input locale from the list. Input locale is the language you want to type in.
   • In the Keyboard Type (Client) field, click the Browse button to select your correct workstation keyboard type from the list.
   • In the Keyboard Type (Server) field, click the Browse button 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 Automatic Client Updates to allow the client software at this workstation to be automatically updated when a newer version is available. See “Updating the Clients for UNIX” on page 34 for details.
   • Select Allow Audio Input to enable support for client-side microphone input. See “Configuring Digital Dictation Support” on page 79.

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.

These settings are used as the default for all new connections. If you want to change the window settings for a specific connection, see “Changing the Window Properties” on page 55.

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:

- **Window Size** allows you to select from **Fixed Size**, **Percentage of Screen Size**, or **Full Screen**.

- **Window Colors** allows you to set the number of window colors to 16, 256, 32 Thousand, or 16 Million. Before selecting a new color mode, ensure that it is supported on your machine. You can only specify a color depth of greater than 256 colors on Version 6.0 and later clients.

- **256 Color Mapping** allows 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 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 uses a private colormap.

### Configuring Server Location and Business Recovery

Server location (also called server browsing) provides a method for a user at a network-connected client to view a list of all servers on the network that have server connections configured for that network protocol, or a list of all published applications. You can specify a separate server location for each network protocol. The way in which server location works depends on which network protocol is configured:

**TCP/IP+HTTP and SSL/TLS+HTTPS** — The default server address is ica.domainname, where domainname is a TCP/IP domain name. The client uses the HTTP or HTTPS protocol respectively 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 specific addresses for servers.

Business recovery provides consistent connections to published applications in the event of a master ICA browser server disruption. You can define up to three groups of servers to which you want to connect: a primary and two backups. Each group can contain from one to five servers. When you specify a server group for your client, the client attempts to contact all the servers within that group and the first server to respond passes its master browser address to the client. If the client is unable to contact any of the servers in the primary group, it attempts to contact servers in each of the backup groups in turn.
To configure server location and business recovery

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.

   **Note** 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 a TCP/IP domain name. 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 3 and 4.

8. Click **OK**.

**Configuring Hotkeys**

Hotkeys are used to control the behavior of the client and as substitutes for the standard Windows hotkeys 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 closes the session in X Windows. Hotkey functionality allows 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.

To display the hotkey settings

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

2. From the drop-down list, choose **Hotkeys** to display the **Hotkeys** page.

   On the **Hotkeys** pages, you can define alternative key combinations for the hotkeys <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 <Alt> <Ctrl> <F1> to <ALT> <CTRL> <F12>, ALT +, and ALT - but you can change the definitions by selecting alternative keys from the pop-up menus.
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> <CTRL>). This enables you to turn Speedscreen Local Text Echo on and off within a session.

**Note**  
If you want to use the PC key combination <CTRL> <ALT> <DELETE> during the connection 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 51 for details.

---

### To adjust the settings for the disk cache

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 **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 **Amount of disk space to use** slider to show a percentage of the disk, or typing in the maximum size you want to allow.
   - 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 **Minimum size bitmap that will be cached** slider. The size setting is displayed next to the slider.
• Clear the cache by clicking the **Clear Cache Now** button. Citrix recommend 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 Presentation Server Console. For more information, see the *MetaFrame Presentation Server Administrator’s Guide*.

## Configuring Auto Client Reconnect

Auto client reconnect allows 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, and no configuration is required on the client device to use these default settings.

For more information on 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 56.

### To change the auto client reconnection default settings

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 **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**.

**Note** Auto client reconnect works the same way regardless of whether a user logged on conventionally or with a smart card. Users who log on to an ICA session using a smart card are automatically reconnected if their session fails and will not have to reenter their PIN number, provided that their smart card remains in the smart card reader.
Configuring Network Protocol

The Network Protocol setting allows 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.

   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 your required network protocol from the Network Protocol list.

4. Click OK.

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

Integrating the Clients for UNIX with CDE

During installation, you can choose to integrate the clients for Solaris (SPARC), 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.

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

To set up file type associations

1. In the main client window, select the connection for which you want to set up files associations.

2. On the Connections menu, click Properties.

3. From the drop-down list, choose File Associations to display the File Associations page.
4. Click **Add**.

5. Select the required file type 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**.

---

**Note** The UNIX path where your files are located must be drive-mapped for the server to have access to it. The published application must end in `%*` on the server, which must be running MetaFrame XP 1.0 or later.

---

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

---

### Integrating the Clients for UNIX with KDE and GNOME

During installation, you can choose to integrate the client into the K Desktop Environment (KDE) and 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 and a Citrix menu option from which users can access published applications.

The menu entries and desktop shortcuts are created dynamically by the Program Neighborhood Agent.

---

**Note** For best operation with CDE, set `$ICAROOT` in `$HOME/.profile`, unless the client is installed in the default location.
Accessing Published Resources with the Program Neighborhood Agent

The Program Neighborhood Agent is a sub-component of the client and provides a mechanism for connecting to published resources (that is, published applications and published content) through a server running the Web Interface. The Program Neighborhood Agent creates the menu and desktop items that are used to access published resources. Although you can view published applications and published content, you cannot view connection entries from the PNAgent view.

Customizable options for all users running the Program Neighborhood Agent on your network are defined in a configuration file, `config.xml`, stored on your server running the Web Interface. The client reads the configuration data from the server when a user launches the agent, and updates its settings and the user interface at specified intervals. This arrangement allows the server administrator to easily control the options that users see, and gives users the flexibility to adjust their own desktops if administrators decide that this is appropriate.

To customize users’ Program Neighborhood Agent options, rather than editing `config.xml` manually, administrators should use the Program Neighborhood Agent Admin Tool, which is available in Citrix MetaFrame XP for Windows with Feature Release 3 and later.

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

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 (in the same way that they connect to a published application) from the PNAgent 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 available that supports the file extension 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.
User Tasks with Program Neighborhood Agent

Users control the Program Neighborhood Agent using the PNAgent page that specifies the server running the Web Interface and the desktop environment of the published resources. The Program Neighborhood Agent allows users to:

- Select the server that is used for connections to published resources
- Specify the logon methods to published resources
- Determine how the published resources are added to their desktops and menus
- Set how often the list of published resources is updated on the client
- Specify how they disconnect from, reconnect to, or log off from applications running on the server. This is known as workspace control.
- Specify the window size, color depth and audio quality settings for sessions

Administrator Tasks with Program Neighborhood Agent

Administrator tasks may involve customizing users’ Program Neighborhood Agent options using the Program Neighborhood Agent Admin Tool, which simplifies editing of the configuration file, config.xml. The default location for config.xml on a server is //Inetpub/wwwroot/Citrix/PNAgent.

Important When making changes to config.xml using the Program Neighborhood Agent Admin Tool, Citrix recommends that you make a copy of the file before editing it to assist in reverting any unwanted changes.

To access the Program Neighborhood Agent Admin Tool, connect to http://servername/Citrix/PNAgentAdmin/ on the server running the Web Interface and follow the links to the various pages, each of which allows you to edit a different section of config.xml.

Limiting the Degree of Desktop Customization Available to Users

Depending on the settings that you specify with the Program Neighborhood Agent Admin Tool, you can allow users to customize, from the client, the occurrence and location of menu items and shortcuts for published resources.

Many of the pages in the Program Neighborhood Agent Admin Tool have check boxes that allow you to specify whether users can change settings on the client. If such a check box is unchecked, any changes that the user makes (from the client) to the behavior of the agent are replaced with the behavior specified by config.xml on the Server settings page when the configuration is updated from the server.
Configuration Update Options

After you save any changes to config.xml, the changes are available to the clients that are controlled by the configuration file, but they are not implemented until one of the following events takes place:

- Users restart their clients
- Users click the Refresh Settings button on the PNAgent page
- The next automatic configuration refresh takes place as specified by the Server settings page in the Program Neighborhood Agent Admin Tool

To control customization of the Program Neighborhood Agent

Important To assist in reverting any unwanted changes, Citrix recommends that you make a copy of config.xml using the Program Neighborhood Agent Admin Tool before editing the file.

1. On the User Interface Tab Control page of the Program Neighborhood Agent Admin Tool, specify which pages of the PNAgent dialog box appear or are hidden. The five pages are labeled Server, Application Display, and Application Refresh, Session Options, and Workspace Control (Reconnect).

Note For the Solaris (SPARC) client, the Application Display page is only available if the KDE or GNOME desktop environments are installed.

2. Click Save.

3. On the client, check that your changes were applied by clicking Tools > Settings, selecting the PNAgent page, and clicking Refresh Settings. Other clients on the network are refreshed as described in “Configuration Update Options” on page 90.

Specifying the Server Running the Web Interface

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

Alternatively, you can 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 fix the location of the server

**Important** To assist in reverting any unwanted changes, Citrix recommends that you make a copy of config.xml using the Program Neighborhood Agent Admin Tool before editing the file.

1. On the **Server Settings** page of the Program Neighborhood Agent Admin Tool, ensure that the path of the configuration file in the **Server URL** box is correct.

2. Clear the **Allow users to change the server URL** check box.

3. Click **Save**.

To allow users to change the location of the server

**Prerequisite for Administrator**

In the Program Neighborhood Agent Admin Tool, confirm the following:

- The **Allow users to change the server URL** check box on the **Server Settings** page is selected
- The **Hide the Server tab from users** check box on the **User Interface Tab Control** page is cleared

**Procedure for User**

1. On the **Tools** menu of the main client window, click **Settings**.

2. From the drop-down list, choose **PNAgent** to display the **PNAgent** page.

3. From the drop-down list, choose **Server** to display the **Server** page.

4. On the **Server** page, click **Change**.

5. In the **PNA Configuration** dialog box, enter the URL of the configuration file on the server that you want to use.

  **Tip** You can enter just the server name, not the fully qualified URL, in the PNA Configuration dialog box. The client reads the configuration file on that server.

6. Click **Update**.

7. On the **PNAgent** page, click **OK**.
Specifying a Logon Method

You can define the type of logon method that is available to users when they access published resources. By default, MetaFrame Presentation Server prompts users to provide their credentials each time they connect to a resource, but you can also enable anonymous logons and password saving.

Depending on the logon choices that you enable, users can select a logon method for the resources that they access through the Web Interface.

To specify the logon methods available to users

**Important** To assist in reverting any unwanted changes, Citrix recommends that you make a copy of config.xml using the Program Neighborhood Agent Admin Tool before editing the file.

1. On the Logon Methods page of the Program Neighborhood Agent Admin Tool, select the logon methods that you want to be available to users.
   
   Although all the methods on the page can be selected (and create valid XML in config.xml), only Anonymous logon and Prompt user are supported by the client.

   **Note** Only supported logon methods are displayed in the Logon mode drop-down list offered to the user on the PNAgent page of the client.

2. On the User Interface Tab Control page, clear the Hide the Server tab from users check box.

3. To allow users to save their credentials in the logon dialog box, select the Allow user to save password check box.

4. Click Save. The logon methods that you specified are available on the client when the configuration is updated. For information about how the configuration can be updated, see “Configuration Update Options” on page 90.

To select a logon method for accessing published resources

**Prerequisite for Administrator**

Administrators must decide what logon methods are appropriate for users and specify these using the procedure “To specify the logon methods available to users” on page 92.
Chapter 4   Configuring the Clients for UNIX  93

Procedure for User
1.  On the Tools menu of the main client window, click Settings.
2.  From the drop-down list, choose PNAgent to display the PNAgent 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 are displayed.
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:

• Define a menu used for accessing the resources
• Create desktop shortcuts to the resources
• Specify how their client refreshes the list of resources

Administrators can limit the degree to which users may customize these features by disabling one or more of the five panels of the PNAgent page in the client. For more information about this task, see “To control customization of the Program Neighborhood Agent” on page 90.

To customize the KDE or GNOME desktop
1.  On the Tools menu, click Settings.
2.  From the drop-down list, choose PNAgent to display the PNAgent page. Depending on the content of config.xml, one or more of the five options in the drop-down list on the PNAgent page—Server, Display, Refresh, Reconnect (Workspace Control), and Session—may not be available. By default, only the first two options are displayed.
3.  To display published resources on the KDE or GNOME menu system, on the Application Display page, select Show applications in menu. By default, the resources are displayed in a Citrix menu. To display the resources in a different menu, enter a different name in the box.
4.  To display published resources on the desktop, on the Application Display page, select Put applications in desktop folder. By default, the resources are displayed in a desktop folder called My Program Neighborhood Applications. You can rename this folder by entering a different name in the box. If no name is provided, each resource is displayed as an individual desktop shortcut.
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 PNAgent 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.

Note To configure the display of the five options available from the drop-down list on the PNAgent page, see “To control customization of the Program Neighborhood Agent” on page 90.

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 MetaFrame Presentation Server. 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 the Program Neighborhood Agent.

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 of the Presentation Server Console or Web Interface Console using the Program Neighborhood Agent Admin Tool.
If the workspace control settings of the Presentation Server Console or the Web Interface Console are configured to allow users to override the server settings, users can configure workspace control in the Settings options of the Web Interface or the Reconnect page of the Program Neighborhood Agent Properties 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 *MetaFrame Presentation Server Administrator's Guide* or the *Web Interface Administrator's Guide*.

**Note**  Workspace control is available only to users running Version 8.x of the Clients for UNIX and works only with sessions connected to servers running MetaFrame Presentation Server Version 3.0

### To configure Workspace Control settings

**Important**  To assist in reverting any unwanted changes, Citrix recommends that you make a copy of config.xml using the Program Neighborhood Agent Admin Tool before editing the file.

1. On the **Workspace Control** page of the Program Neighborhood Agent Admin Tool, select the workspace control settings you want to apply to all connections.
2. Clear the **Allow users to override these settings** check boxes.
3. Click **Save**.

### To allow users to configure workspace control settings

**Prerequisite for Administrator**

In the Program Neighborhood Agent Admin Tool, confirm the following:

- The **Allow users to override these settings** check box on the **Workspace Control** page is selected
- The **Hide the Workspace Control tab from users** check box on the **User Interface Tab Control** page is cleared

**Procedure for User**

1. On the **Tools** menu of the main client window, click **Settings**.
2. From the drop-down list, choose **PNAgent** to display the **PNAgent** page.
3. From the drop-down list, choose **Reconnect** 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** allows you to reconnect to disconnected applications, or to both disconnected applications and active applications running on another client device, when you logon
   - **Enable automatic reconnection from Reconnect menu** allows you to reconnect to disconnected applications, or to both disconnected applications and active applications running on another client device using the **Reconnect** menu in the main client window
   - **Customize Log Off button** allows you to configure whether or not 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 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**

---

**Important** To assist in reverting any unwanted changes, Citrix recommends that you make a copy of config.xml using the Program Neighborhood Agent Admin Tool before editing the file.

---

1. Expand **Session Options** on the **Configuration Settings** menu of the Program Neighborhood Agent Admin Tool. Select one of the following pages:

   - **Window Size**
   - **Color Depth**
   - **Audio Quality**
2. Clear the checkbox at the top of the **Window Size**, **Color Depth**, or **Audio Quality** page to prevent users from overriding the session option settings you define on the server.

3. Select the session option settings you want to apply to all connections.

4. Click **Save**.

**To allow users to configure session option settings**

**Prerequisite for Administrator**

In the Program Neighborhood Agent Admin Tool, confirm the following:

- The check boxes at the top of the **Window Size**, **Color Depth** and **Audio Quality** pages are selected

- The **Hide the Session Option tab from users** check box on the **User interface tab control** page is cleared

**Procedure for users**

1. On the **Tools** menu of the main client window, click **Settings**.

2. From the drop-down list, choose **PNAgent**, to display the **PNAgent** page.

3. From the drop-down list, choose **Session**, 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 **Color Depth**
   - Adjust the level of **Audio Quality**

5. Click **OK**.

**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. Command-line parameters from the desktop are passed to the server through the client to start an application session.

The Program Neighborhood Agent creates desktop icons automatically for KDE (Version 2.0 and later) and GNOME (Version 2.0 and later), but administrators of other UNIX desktop systems may need to create such icons manually as outlined in this section. For more information about the Program Neighborhood Agent, see “Integrating the Clients for UNIX with KDE and GNOME” on page 87.
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 *MetaFrame Presentation Server Administrator’s Guide*. 
Setting up Server-Client Content Redirection

Server-client content redirection allows 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 (by default, this is Netscape). Server-client content redirection allows administrators to allocate MetaFrame 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 Netscape and RealPlayer.

Note Real Player 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 if Netscape and RealPlay are not in the UNIX path

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

   Path=
   Command=
   PercentS=

   where Path is the directory where the Netscape 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.

   The default value for PercentS is 3 because the default value for Command is:
   "$ICAROOT/util/nslaunch %s || ${BROWSER:=netscape} %s || mozilla %s."
This setting specifies the following until the content can be displayed successfully:

- The nslaunch utility is run to push the URL into an existing browser window
- A new browser is launched as specified by the $BROWSER environment variable
- Mozilla is used

3. In the [Player] section, modify the following settings:

```
Path=
Command=
PercentS=
```

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

---

**To turn off server-client content redirection from the client**

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

Overview

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

Topics in this chapter include:

• Common Problems
• Common Error Messages
• Sending Diagnostic Information to Citrix Support

Common Problems

This section provides solutions to the most commonly encountered problems when using the client.

I cannot connect to a server using its full Internet name

If you do not have a DNS (Domain Name Server) configured on your network and on your client device, 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 cannot connect properly to a published resource or desktop session

If, when establishing a connection, the client dialog box appears with the message “Connecting to server…” but no subsequent connection window is displayed, you may need to configure the server with a Client Access License (CAL). For more information on licensing, see the MetaFrame Access Suite Licensing Guide.
I experience problems with over-scrolling when using published applications

Users may experience problems with over-scrolling when using certain published applications.

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:
   TWZStopwatchMinimum=100
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.

I experience connection problems using SSL

If you cannot connect using Secure Socket Layer (SSL) even though you selected the SSL/TLS+HTTPS option from the Network Protocol drop-down list on the Server Location page, ensure that you have the required root certificate and any intermediate certificates. These must be located in $ICAROOT/keystore/cacerts.

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 must specify the keyboard type and layout that you are using. For more information about specifying keyboards, see “Configuring Keyboard Options, Alert Sounds, Automatic Updates and Digital Dictation Support” on page 81.

Ghosting occurs when I minimize a window

With some applications (including Microsoft Outlook), ghost windows can be displayed when 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.

When I click on a link in a Windows session, the content is displayed in a local browser

Server-client content redirection may have been 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 100.
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” is displayed, this may be because the environment variable ICAROOT was not defined correctly. This is a requirement if you have installed the client to a non-default location. To overcome this problem, Citrix recommends that you do one of the following. Either:

- Define ICAROOT as the installation directory

  **Note** To check the ICAROOT environment variable was defined correctly try starting the client from a terminal session. If the error message is still displayed, it is likely that the ICAROOT environment variable has not been correctly defined.

—Or—

- Reinstall the client to the default location. For more information about installing the client, see “Installing the Clients for UNIX” on page 31.

  **Note** If the client was previously installed in the default location, remove the /usr/lib/ICAClient or $HOME/ICAClient/linuxx86 directory before reinstalling

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.

**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.

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

Browsers other than 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 launch.asp file.
To configure a non-Netscape 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.

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 have 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_NO_KBD_MAPPING - Cannot find keyboard mapping file "...".

The keyboard mapping file specified on the Preferences page of the Settings dialog box is invalid or cannot be located.

E_CM_WRONG_EXECUTABLE - Unable to perform update: not running $ICAROOT/wfica.

The client cannot update an installation other than its own.

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

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

wfclient.ini Configuration Errors

These errors may occur if you have 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_APPSVR_SECTION_MISSING - Inconsistency in configuration
file: "...
Missing section: "...
The configuration file is corrupt. Create a new configuration file.

E_CSM_DESCRIPTION_NONUNIQUE - This description is already in use.
The Description must be unique.
The Description field on the Network page of the Properties dialog box
must be unique.

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 that the
icon or item refers to.

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.

**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**

On the Help menu of the main client window, click Diagnostic Information.

**Command-Line Parameters**

The table below lists the command-line client command line parameters.

You can use a connection file simply by typing it after `wfica` without any of the
above options.

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

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the connection to use from the Connection file.</td>
<td>-desc description</td>
</tr>
<tr>
<td>Specify the connection to use from the Connection file.</td>
<td>-description description</td>
</tr>
<tr>
<td>Specify a Connection file. This allows the use of an alternative appsrv.ini.</td>
<td>-file connection filename</td>
</tr>
<tr>
<td>Set alternative protocol file. This allows the use of an alternative module.ini.</td>
<td>-protocolfile filename</td>
</tr>
<tr>
<td>Set alternative client configuration file. This allows the use of an alternative wfclient.ini.</td>
<td>-clientfile filename</td>
</tr>
<tr>
<td>Set the location of UNIX client installation files. This is equivalent to setting the ICAROOT environment variable.</td>
<td>-icaroot directory</td>
</tr>
<tr>
<td>Specify a string to be added to a published application.</td>
<td>-param string</td>
</tr>
<tr>
<td>Command</td>
<td>Type</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>Specify the UNIX path to be accessed through Client Drive Mapping by a published application.</td>
<td>-fileparam unixpath</td>
</tr>
<tr>
<td>Specify a username.</td>
<td>-username username</td>
</tr>
<tr>
<td>Specify a password.</td>
<td>-password password</td>
</tr>
<tr>
<td>Specify a clear text password.</td>
<td>-clearpassword clear password</td>
</tr>
<tr>
<td>Specify a domain.</td>
<td>-domain domain</td>
</tr>
<tr>
<td>Specify an initial program.</td>
<td>-program program</td>
</tr>
<tr>
<td>Turn on sound.</td>
<td>-sound</td>
</tr>
<tr>
<td>Turn off sound.</td>
<td>-nosound</td>
</tr>
<tr>
<td>Use private colormap.</td>
<td>-private</td>
</tr>
<tr>
<td>Use shared colormap.</td>
<td>-shared</td>
</tr>
<tr>
<td>Set drive mapping overrides. These are of the form A$=&lt;path&gt;, where &lt;path&gt; can contain an environment variable (for example A$=$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.</td>
<td>-drivemap string</td>
</tr>
<tr>
<td>Show this list of parameters.</td>
<td>-help</td>
</tr>
<tr>
<td>Turn off the splash screen.</td>
<td>-nosplash</td>
</tr>
<tr>
<td>Display version information.</td>
<td>-version</td>
</tr>
<tr>
<td>Suppress connection dialogs.</td>
<td>-quiet</td>
</tr>
<tr>
<td>Set session geometry.</td>
<td>-geometry WxH+X+Y</td>
</tr>
<tr>
<td>Show error numbers.</td>
<td>-ermo</td>
</tr>
<tr>
<td>Display a different name for the client, specified by name, in the Management Console for MetaFrame Presentation Server. The default name is derived from the Sunray device’s MAC address but this is overridden by the ClientName entry in .ICAClient/wfclient.ini, which is itself overridden by issuing the -clientname name command.</td>
<td>-clientname name</td>
</tr>
</tbody>
</table>
Index

A
application publishing
  support for 19
applications
  accessing with Program Neighborhood Agent 88
  printing from 76
  publishing 88
  specifying which to run at connection 54
  troubleshooting applications running locally 102
  working directory for 54
approximate colors 81
audio
  configuring digital dictation support 79
  mapping client audio 78
auto client reconnect
  configuring for individual connections 56
  default settings for 85
  overview of 22

B
bandwidth
  improving performance 51
bitmap caching 52
browser
  supporting faster browsing 42
business recovery 19
  default settings for 82

C
CDE integration 24
changing connection entries 50
Citrix SSL Relay
  configuring client with 64
client
  configuration overview 43, 101
  installing 31
  overview 15
  overview of deployment 43
  redirecting output from 40
  starting 33
  uninstalling 39
client audio
  mapping client audio 78
client auto update 18
client device mapping 68
  overview of 17
client drive mapping 69
  overview of 17
client output
  redirecting 40
client printer mapping 72
  overview of 17
client update database
  configuring 34
  configuring database properties of 36
  creating new client update database 35
  setting default database 35
clipboard 19
  transparent clipboard access 19
colors
  approximate color mapping 81
  color mapping 81
  default windows settings 81
  true color support 20
command line parameters 106
Common Desktop Environment
  integration of client with 24
configuring
  application properties 54
  client with Citrix SSL Relay 64
  client, overview of 43, 101
  default settings for all connections 79
  digital dictation support 79
  extended parameter passing 97
  ICA encryption 63
  logon properties 56
  middle button paste 54
  network properties 50
  security features, overview 60
  server-client content redirection 99
  session options 96
  smart card logons 59
  workspace control 94–95
config.xml 89
connecting
  across a firewall 63
  through a proxy server 60
  through a Secure proxy server 62
  through a SOCKS proxy server 61
  troubleshooting 101
connection entries
  changing 50
  configuring auto client reconnect settings 56
  configuring default settings for 79
creating 44
creating new 44
default settings for 81
default settings for auto client reconnect 85
default settings for hotkeys 83
default settings for network protocol 86
default settings for windows 81
editing 50
running applications 54
content redirection 22
creating connection entries 44
cutting and pasting
  pasting between applications 19
  transparent clipboard access 19
  xcapture 19, 57

D
data compression 52
default settings for all connections
  auto client reconnect settings 85
  hotkey settings 83
  network protocol settings 86
  preferences 81
  windows settings 81
deploying the client
  overview of 43
desktop customization
  limiting 89
desktop integration
  customizing menus and shortcuts 93
  overview of 25
diagnostic information
  overview of 28
digital dictation support 26
  configuring 79
  overview of 26
disconnected sessions
  auto client reconnect 22
disk caching 52
DNS
  troubleshooting 101
dynamic session reconfiguration 27

E
  editing connection entries 50
  encryption
    configuring ICA encryption 63
    forcing TLS connections 68
    ICA encryption 19
    TLS encryption 23
  enhanced proxy support 23
  error messages 104
  extended parameter passing
    configuring 97

G
guest windows
  troubleshooting 102
 GNOME
    integrating client with 87
    graphics
      improving download speed 25
      using xcapture 57

H
hotkeys
  default settings for 83
  overview of 18
HTTPS
  configuring client with 60
HTTPS proxy 23

I
ICA encryption
  configuring 63
ICA performance
  improvements 27
ICA to X proxy 40
improving performance
  data compression 52
  disk caching 52, 84
  low-bandwidth connections 51
  SpeedScreen Browser Accelerator 25
  SpeedScreen latency reduction 53
installation
  as non-privileged user 25
installing client 31
integrating client with CDE 24
integrating client with KDE or GNOME 87
Internet name
troubleshooting 101

K
KDE
  integrating client with 87
keyboard accelerators 25
keyboard problems
  troubleshooting 102
keyboard types
  default settings for 81
keys
  hotkeys 18
  shortcut keys 18

L
latency
  reducing with SpeedScreen latency reduction 20
launch.asp
  troubleshooting 103
limiting desktop customization by users 89
logon
  configuring smart card logons 59
logon methods
  specifying for published resources 92
logon properties
  configuring 56

M
mapping client audio 78
mapping client devices
  general information 68
  overview of 17
mapping client drives
  overview of 17
  procedures 69
mapping client printers
  overview of 17
  procedures 72
mapping COM ports
  procedure 68
mapping default color settings 81
middle button paste
  configuring 54
  overview of 28

N
Netscape
  plug-in for 20
network properties
  configuring 50
network protocol
  default settings for business recovery 86
  specifying 50
non-Netscape browsers
  troubleshooting 103
non-rectangular Seamless Windows 25

O
operating systems
  supported 29
over-scrolling
  troubleshooting 102

P
pass-through mode and seamless windows 20
pasting between applications 19
performance
  improving with SpeedScreen latency reduction 20
performance improvements
  overview of 27
platforms
  supported 29
PNAgent Admin Tool 89
PNAgent page 89
preferences
  default settings for 81
printers
  mapping client printers 72
printing from applications 76
Program Neighborhood Agent
  accessing published resources with 88
  config.xml 89
  limiting desktop customization 89
  menus and desktop shortcuts 93
  PNAgent Admin Tool 89
  refreshing client 90
proxy
  redirecting client output to another device 40
proxy servers
  - connecting across a firewall 63
  - connecting through 60
  - connecting through a Secure proxy server 62
  - support for HTTPS proxy 23
  - support for Security proxy 23
  - support for SSL tunnelling 23
published resources
  - specifying logon methods 92
publishing applications 88
  - server-client content redirection 22
  - support for 19
publishing content 88

R
reconnecting sessions 23
redirecting client 40
redirecting client output 40
refreshing Program Neighborhood Agent configuration 90
remote monitoring 24
removing
  - UNIX client 39
requirements
  - system 29
resolving server names
  - troubleshooting 101
roaming user reconnect
  - overview of 23

S
screen problems
  - troubleshooting 102
screenshots
  - capturing on the clipboard 19
  - using xcapture 57
Seamless Windows
  - non-rectangular 25
seamless windows
  - overview of 20
Secure Gateway
  - configuring client with 64
  - overview of 23
Secure Sockets Layer encryption 23
security
  - configuring client with the Secure Gateway 64
  - configuring ICA encryption 63
  - configuring security features, overview 60
  - forcing TLS connections 68
security features
  - overview of 21
Security proxy protocol
  - configuring client with 60
  - support for 23
server location
  - default settings for 82
  - for Web Interface 90
server name
  - specifying for a connection 50
server side ICA 40
server-client content redirection 22
  - configuring 99
  - troubleshooting 102
session options
  - configuring 96
  - overview of 96
sessions
  - re-establishing with auto client reconnect 22
setting up client 43, 101
shadowing
  - user-to-user 24
shortcut keys 18
smart cards
  - configuring 59
  - configuring logon properties for 56
  - support 22
  - using roaming user reconnect with 23
SOCKS
  - connecting through 61
sound
  - mapping client audio 78
  - Windows alert sounds 81
specifying
  - network protocol for a connection 50
  - published application for a connection 50
  - server name for a connection 50
SpeedScreen Browser Accelerator 25
  - libjpeg.so requirement 42
SpeedScreen latency reduction
  - improving performance with 53
  - overview of 20
SSL
  configuring client with 60
  overview of 64
  SSL in relation to TLS 23
  troubleshooting 102
starting client 33
  troubleshooting 103
system requirements 29
systray emulation window
  overview of 28

T
ThinImage 28
TLS
  configuring client with 60
  overview of 64
TLS encryption 23
transparent clipboard access 19
troubleshooting
  application running locally 102
  color flashing 103
  commonly encountered problems 101
DNS 101
file types 88
ghost windows 102
Internet name 101
keyboard problems 102
launch.asp 103
non-Netscape browsers 103
over-scrolling 102
problems connecting 101
publishing content 88
resolving server names 101
server-client content redirection 102
SSL 102
  starting client 103
ture color support 20

U
Unicode support
  overview of 28
uninstalling client 39
universal printer driver
  overview of 25
UNIX platforms
  supported 29

W
Web Interface
  server location 90
  window settings
    default behavior 81
windows
  default settings for 81
  Non-Rectangular Seamless Windows 25
workspace control 26
  configuring 94–95
  overview of 26

X
xcapture 19, 28, 57
  starting from the command line 58
  starting from the main client window 58
X11 devices
  redirecting client output to 40

Z
zone preference and failover 27
  overview of 27