

Administrator's Guide

Citrix ICA Win32 Client

Version 6.0

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. 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.

© 1997-2000 Citrix Systems, Inc. All rights reserved.

© 1985-1997 Microsoft Corporation. All rights reserved.

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

Microsoft, MS, MS-DOS, 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.

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

Contents

Before You Begin	1
Who Should Use This Manual	1
How to Use This Guide	1
Conventions	2
Finding More Information	2
Citrix on the World Wide Web	3
Chapter 1 Introduction to the ICA Win32 Client	5
Overview	5
Program Neighborhood	6
TAPI Support	6
Seamless Windows	6
Client Device Mapping	7
Client Drive Mapping	7
Client Printer Mapping	7
Client COM Port Mapping	7
Sound Support	7
Dialing Prefixes	8
Client Auto Update	8
Windows Clipboard Integration	8
Low Bandwidth Requirements	8
Disk Caching and Data Compression	9
SpeedScreen Latency Reduction	9
Business Recovery	9
TCP/IP+HTTP Server Location	9
Wheel Mouse Support	10
Multiple-Monitor Support	10
Pass-Through Authentication	10
Panning and Scaling	10

Chapter 2 Deploying the ICA Win32 Client	11
Overview	11
System Requirements	11
Installation Methods	12
Preconfiguring ICA Client Settings	12
Creating Client Installation Diskettes	12
Installing the Citrix ICA Win32 Client	13
Starting the ICA Win32 Client	16
Understanding Client Auto Update	16
The Citrix ICA Client Update Process	17
Configuring the Client Update Database	18
Chapter 3 Configuring the ICA Win32 Client	25
Overview	25
Mapping Client Devices	25
Turning Off Client Device Mappings	26
Mapping Client Drives	27
Mapping Client Printers	28
Mapping Client COM Ports	30
Mapping Client Audio	31
Connection Types	32
Configuring a SOCKS Proxy Connection	33
Using SOCKS to Direct ICA Traffic Through Firewalls	33
Locating Your Proxy Server	34
Configuring Connections to Citrix Servers and Published Applications	36
Configuring Server Location and Business Recovery	36
Using Application Sets and Custom ICA Connections	39
Adding Application Sets and Custom ICA Connections	39
Configuring Application Sets and Custom ICA Connections	40
Using Applications Published on MetaFrame for UNIX	49
Using the Window Manager	49
Cutting and Pasting Graphics Using ctxgrab and ctxcapture	51
Index	55

Before You Begin

Who Should Use This Manual

This manual is for system administrators responsible for installing, configuring, deploying, and maintaining Citrix ICA Clients for 32-bit Windows (also called the Citrix ICA Win32 Clients). This manual assumes knowledge of:

- The Citrix server to which your ICA Clients connect
- The operating system on the client computer (Windows 95, Windows 98, or Windows NT)
- Installation, operation, and maintenance of network and asynchronous communication hardware, including serial ports, modems, and device adapters

How to Use This Guide

To get the most out of the *Citrix ICA Client Administrator's Guide*, review the table of contents to familiarize yourself with the topics discussed.

This guide contains the following sections:

Chapter	Contents
Chapter 1, "Introduction to the Citrix ICA Win32 Client"	Gives a detailed list of features.
Chapter 2, "Deploying the Citrix ICA Win32 Client"	Describes how to install and update the Citrix ICA Win32 Client.
Chapter 3, "Configuring the Citrix ICA Win32 Client"	Describes how to configure connection properties and device mappings for the Citrix ICA Win32 Client.

Conventions

The following conventional terms, text formats, and symbols are used throughout the printed documentation:

Convention	Meaning
Bold	Indicates boxes and buttons, column headings, command-line commands and options, icons, dialog box titles, lists, menu names, tabs, and menu commands.
<i>Italic</i>	Indicates a placeholder for information or parameters that you must provide. For example, if the procedure asks you to type <i>filename</i> , you must type the actual name of a file. Italic also indicates new terms and the titles of other books.
ALL UPPERCASE	Represents keyboard keys (for example, CTRL, ENTER, F2).
[brackets]	Encloses optional items in syntax statements. For example, [<i>password</i>] indicates that you can choose to type a <i>password</i> with the command. Type only the information within the brackets, not the brackets themselves.
...(ellipsis)	Indicates a command element can be repeated.
Monospace	Represents examples of screen text or entries that you type at the command line or initialization files.
➤	Indicates a procedure with sequential steps.
▪	Indicates a list of related information, not procedural steps.

The Citrix ICA Clients allow users to connect to Citrix servers. When describing a feature or procedure common to all types of MetaFrame and *WINFRAME* servers, this manual uses the term *Citrix server*. When describing a feature unique to a particular MetaFrame or *WINFRAME* server, this manual specifies the appropriate server and version number.

Finding More Information

This manual contains conceptual information and installation and configuration steps for the Citrix ICA Win32 Client. For additional information, see the following:

- The online help for the ICA Client you deploy
- The *Citrix ICA Client Administrator's Guides* for the other ICA Clients you deploy
- For instructions about installing, configuring, and maintaining your Citrix servers, see the documentation included in your Citrix server package

This book and other Citrix documentation is available in Adobe PDF format in the following locations:

- The documentation directory of your Citrix ICA Client CD-ROM
- The documentation directory of your Citrix server CD-ROM
- The product documentation library at <http://www.citrix.com/services/productdocs.asp>.

Using the Adobe Acrobat Reader, you can view and search the documentation electronically or print it for easy reference. To download the Adobe Acrobat Reader for free, please go to Adobe's Web site at <http://www.adobe.com>.

Citrix on the World Wide Web

Citrix offers online Technical Support Services at <http://www.citrix.com> that include the following:

- PDF versions of the documentation
- Downloadable Citrix ICA Clients, available at <http://download.citrix.com>
- A Frequently Asked Questions page with answers to the most common technical issues
- An FTP server containing the latest service packs and hotfixes for download
- An Online Knowledge Base containing an extensive collection of technical articles, troubleshooting tips, and white papers
- Interactive online support forums
- The Citrix Developer Network (CDN) available at <http://www.citrix.com/cdn>.

This new, open enrollment membership program provides access to developer toolkits, technical information, and test programs for software and hardware vendors, system integrators, ICA licensees and corporate IT developers who incorporate Citrix server-based computing solutions into their products.

Introduction to the ICA Win32 Client



Overview

When connected to a Citrix server, the ICA Win32 Client provides additional features that make remote computing just like running applications on a local desktop. The ICA Win32 Client has the following features:

- Program Neighborhood
- TAPI support
- Seamless windows
- Client device mapping
- Sound support
- Dialing prefixes
- Client Auto Update
- Windows clipboard integration
- Low bandwidth requirements
- SpeedScreen latency reduction
- Disk caching and data compression
- Business recovery
- TCP/IP+HTTP server location
- Wheel mouse support
- Multi-monitor support
- Pass-through authentication
- Panning and Scaling

Program Neighborhood

With Program Neighborhood, server-based applications can be pushed to the client, integrated into the local 32-bit Windows desktop, or pushed directly to the client's **Start** menu.

Similar in concept to Windows Network Neighborhood, Program Neighborhood provides complete administrative control over application access and local desktop integration, with no client configuration required.

TAPI Support

The Citrix ICA Win32 Client includes TAPI modem support for dial-up connections to Citrix servers. TAPI support allows the Win32 Client to detect the presence of TAPI Version 1.4 or greater modems on the client computer. Users need not manage separate modem entries for their local communications programs.

When a TAPI modem is detected, the ICA Win32 Client can use the modem installation and configuration utilities built into Windows to manage the modem. If the client computer is not TAPI-capable, the ICA Win32 Client is able to use its own modem installation and configuration utilities.

Seamless Windows

The Citrix ICA Win32 Client supports the seamless integration of local and remote applications on the local desktop. By selecting the Seamless Windows option when configuring a connection, a user no longer needs to access an entire remote desktop to run remote applications. With a single session a user can gain access to multiple applications, have fully functional local keyboard controls (such as ALT+TAB), switch between local and remote applications on the local taskbar, define remote application icons on the local desktop, and even tile and cascade between local and remote applications.

Client Device Mapping

The Citrix ICA Clients support client device mapping. Client device mapping allows a remote application running on the Citrix server to access printers, disk drives, and COM port devices attached to the local client computer. This feature is not available when connecting to MetaFrame for UNIX 1.0 and 1.1 servers.

- Client drive mapping
- Client printer mapping
- Client COM port mapping

Client Drive Mapping

Client drive mapping allows drive letters on the Citrix server to be redirected to drives that exist on the client computer; for example, drive H in a Citrix user session can be mapped to drive C on the local computer running the Citrix ICA Client. These mappings can be used by the File Manager or Explorer and your applications just like any other network mappings. The drive letters used for drive mapping are configurable and long filenames are supported.

Client Printer Mapping

Client printer mapping allows a remote application running on the Citrix server to access printers attached to the client computer. Client printers can be browsed and connected to in the same way as network printers. Users who access a Citrix server with the Citrix ICA Client can transparently access their local printers and disk drives (fixed and removable).

Client COM Port Mapping

The ICA Client COM port redirector gives Citrix ICA Client users access to virtually any peripheral that requires a COM port for operations. COM port mapping is similar to printer and drive mapping, and allows users to access a COM port on the client computer as if it were connected to the Citrix server.

Sound Support

ICA Client sound support allows a client computer with a compatible sound card to play sound files on the server and present them on the local client computer's sound system. Client computers can play 8- or 16-bit mono or stereo Windows .Wav files at 8, 11.025, 2.25, and 44.1KHz. Audio support can be configured to use one of three different sound compression schemes. Each scheme provides different sound quality and bandwidth usage. This feature is not available when connecting to MetaFrame for UNIX 1.0 and 1.1 servers.

Dialing Prefixes

The Citrix ICA Clients support dialing prefixes. Dialing prefixes allow a user to easily add special dialing codes as required by different telephone systems for dialing out and accessing a remote Citrix server.

The most common use of dialing prefixes is defining different dialing methods for different telephone systems. For example, a user with a laptop computer may need to dial 9 to get an outside line at the office and need to dial 1 plus the area code when working on the road or at home. In this case, the user can define a dialing prefix named Office for use when dialing out from the office and a prefix called Remote for use when dialing in from the road or at home.

Client Auto Update

The Client Auto Update feature allows administrators to update ICA Client installations from a central location instead of having to manually install new client versions on each client computer. New versions of Citrix ICA Clients are stored in a central *Client Update Database*. The latest versions of the ICA Client software are downloaded to ICA Client devices when users connect to the Citrix server. MetaFrame for UNIX does not use the Client Update Database. To use the Client Update Database, you must have either a MetaFrame for Windows or *WINFRAME* server in your server farm.

ICA Client Auto Update works with all transport types supported by ICA (TCP/IP, IPX, NetBIOS, and serial).

ICA Client Auto Update supports the following features:

- Automatically detects older client files
- Transparently copies new files over any ICA connection
- 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

Windows Clipboard Integration

Users can cut and paste data between ICA sessions and local applications using the Windows clipboard.

Low Bandwidth Requirements

The highly efficient Citrix ICA protocol typically uses 20K of bandwidth for each session.

Disk Caching and Data Compression

These features 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 computer.

SpeedScreen Latency Reduction

SpeedScreen Latency Reduction is a collective term used to describe functionality that enhances the user's experience on slower network connections. SpeedScreen Latency Reduction functionality includes:

Local Text Echo

This ICA Client option accelerates the display of the input text on the client device.

Mouse Click Feedback

This ICA Client option provides visual feedback for mouse clicks to show that the user's input is being processed.

SpeedScreen latency reduction is not available when connecting to MetaFrame for UNIX 1.0 and 1.1 servers.

Business Recovery

The Citrix ICA Client includes the additional intelligence to support multiple server sites (such as a primary and hot backup) with different addresses for the same published application name.

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

TCP/IP+HTTP Server Location

TCP/IP server location allows you to retrieve Citrix server and published application information across network configurations that restrict broadcast and UDP packets.

Wheel Mouse Support

If you run applications that take advantage of a wheel mouse, the ICA Win32 Client transmits the wheel mouse movements in the same manner that it transmits other mouse data. ICA Win32 Client wheel mouse support requires MetaFrame1.8 Service Pack 1 or later and a local client device that supports wheel mouse functionality.

Multiple-Monitor Support

The Citrix ICA Win32 Client supports multiple monitors connected to a single computer.

Pass-Through Authentication

Pass-through authentication provides the ability to pass the user's desktop password to the server, eliminating the need for multiple system and application authentications.

Panning and Scaling

Panning provides scroll bars that allow you to scroll an ICA session image configured at a higher resolution than your local client desktop. Scaling provides controls that enable you to shrink an ICA session image to fit your desktop.

Deploying the ICA Win32 Client



Overview

This chapter explains how to install and update the Citrix ICA Win32 Client. Topics covered in this chapter include:

- System requirements
- Installation methods
- Creating client installation diskettes
- Installing the Citrix ICA Win32 Client
- Understanding Client Auto Update

System Requirements

Computers used with the ICA Win32 Client must meet the following requirements:

- Standard PC architecture, 80386 processor or greater as required for the operating system
- Windows 9x, Windows 2000, or Windows NT 3.5 or greater
- 8MB RAM or greater for Windows 9x, 16MB RAM or greater for Windows NT 3.51 or 4.0
- Microsoft mouse or 100% compatible mouse
- VGA or SVGA video adapter with color monitor
- High-density 3.5-inch diskette drive and available hard disk space
- Windows-compatible sound card for sound support (optional)
- For serial connections to the Citrix server, an internal modem or serial port and external modem using a 16550 Universal Asynchronous Receiver/Transmitter (UART) is recommended

- For network connections to the Citrix server, a network interface card (NIC) and the appropriate network transport software are required. Supported network transports are:
 - NetBIOS
 - IPX
 - SPX
 - TCP/IP

Installation Methods

You can install the Citrix ICA Win32 Client from:

- The %SystemRoot%\System32\Clients\Ica directory on your Citrix server machine
- Client installation diskettes created with the ICA Client Creator utility
- The Citrix ICA Client CD

For more information, see the “Creating Client Installation Diskettes” and “Installing the Citrix ICA Win32 Client” sections later in this chapter.

Preconfiguring ICA Client Settings

You can create ICA Client installation diskettes with preconfigured client settings. For more information on about creating customized client diskettes, see the Readme.txt file in the Customize directory of your server CD-ROM.

Creating Client Installation Diskettes

Use the ICA Client Creator to create client installation disks.

➤ To create Citrix ICA Client installation disks

1. Have the required number of 3.5-inch disks on hand.
2. From a MetaFrame server: On the **Start** menu, point to **Program**, then point to **MetaFrame Tools**. Click **ICA Client Creator**. The **Make Installation Disk Set** dialog box appears.

From a *WINFRAME* server: In the **Administrative Tools** folder, double-click **ICA Client Creator**. The **Make Installation Disk Set** dialog box appears.

3. In the Network Client or Service list, click the desired Citrix ICA Client. Select the **Format Disks** check box to format the disks when creating the installation media. Click **OK**.
4. Follow the directions on screen.

Installing the Citrix ICA Win32 Client

➤ To install the ICA Win32 Client

1. Make sure the client computer is properly configured and cabled. Make sure any previous installations of the Citrix ICA Client (including the ICA Connection Center, whose icon appears in the system tray in the task bar if it is active) are not running.
2. If you are installing from diskettes, insert ICA Win32 Client Setup diskette #1 in drive A (or other appropriate drive) of the client computer. For Windows 9x, Windows 2000, and Windows NT 4.0 client computers, run **a:setup** using the **Run** option on the **Start** menu. For Windows NT 3.5x client computers, execute a:setup using the Run option on the **File** pull-down menu of Program Manager.

If you are installing from a Citrix server, go to

%SystemRoot%\System32\Clients\Ica\Ica32\disks\disk1, and run **setup.exe**.

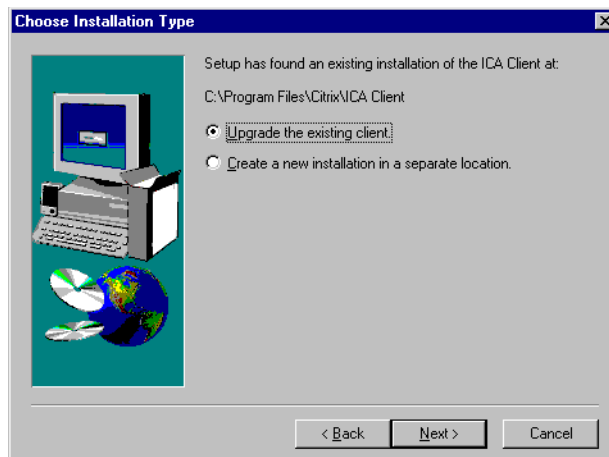
If you are installing from the Citrix ICA Client CD, go to the

\CAINST\language\ICA32\disks\disk1, and run **setup.exe**.

The **Welcome** screen appears. Read the information on this screen and click **Next**.

The installation program searches your client computer for previously installed versions of the ICA Win32 Client. If an older version is detected, the screen in Step 3 appears. If no older version is detected, you will see the screen shown in Step 5.

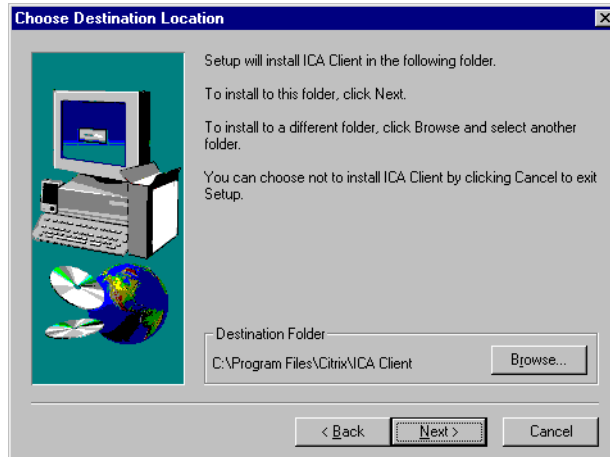
3. The **Choose Installation Type** screen appears:



- The **Choose Installation Type** screen lets you choose to either upgrade the existing client or create a new and separate installation of the ICA Win32 Client in a new location. The default value is **Upgrade the existing client**. Click **Next**.

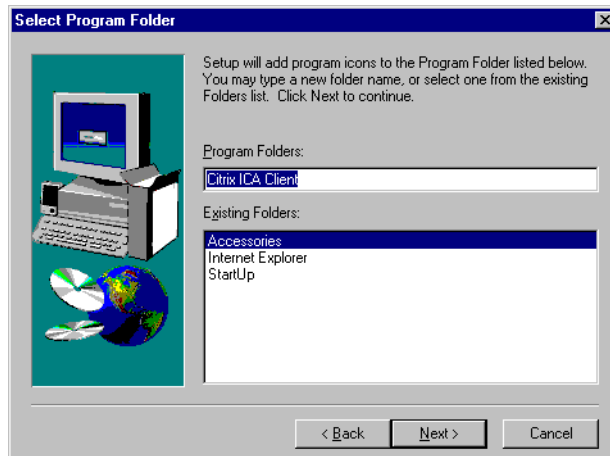
If you choose to create a new installation, go to Step 5. If you choose to upgrade the existing client, go to Step 6.

- The **Choose Destination Location** screen appears:

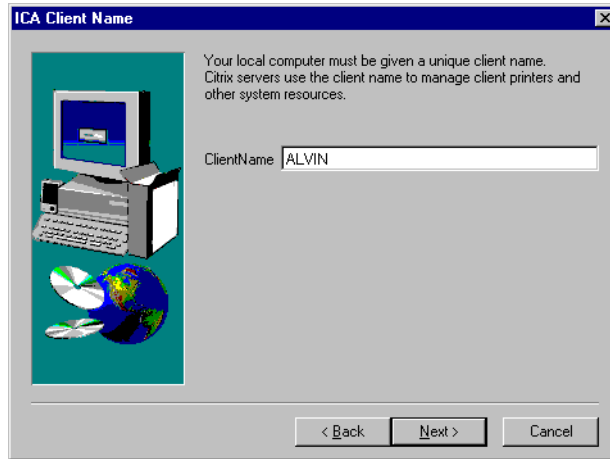


You can change the displayed path if desired by clicking **Browse**. Click **Next** to accept the displayed path and continue installation.

- The **Select Program Folder** appears:



7. You can choose to use the default Citrix ICA Client folder, specify the name of a new program folder, or add the ICA Win32 Client icons to an existing folder. The program folder you specify is created if it does not already exist. Click **Next** to continue.
8. The **ICA Client Name** screen appears:



9. Specify a unique client name for your client computer. Citrix servers use the client name to manage client printers and other system resources. If you do not give your client computers unique client names, device mapping and application publishing may not operate correctly. When you are done, click **Next** to continue. A progress window appears displaying the file names as they are copied to your hard drive.
10. If you are installing from diskette, the **Setup Needs the Next Disk** dialog box appears. Remove the first ICA Win32 Client diskette from drive A (or other appropriate drive) and insert the second diskette. Click **OK**.
11. When the Citrix ICA Client finishes copying the program files, the **Information** dialog box appears. Click **OK** to exit this window.

The Citrix ICA Client program group appears on your desktop:



Starting the ICA Win32 Client

To access applications published on Citrix servers, users must first start Program Neighborhood.

➤ **To start Program Neighborhood:**

1. Double-click the Program Neighborhood icon on your desktop to open the **Program Neighborhood** window.

If you have specified a default application set for your user, this window contains all the applications you can run. If no default is specified, a list of application sets appears. Select the application set to view and, from the **File** menu, click **Open**. A login dialog box appears.

2. Enter a valid user name, domain, and password.

Understanding Client Auto Update

Use the Client Auto Update feature to store new versions of Citrix ICA Clients. The ICA Client software is stored in a client update database and downloaded to ICA Client devices when users connect to the Citrix server.

ICA Client Auto Update works with all transport types supported by ICA (TCP/IP, IPX, NetBIOS, and serial).

ICA Client Auto Update supports the following features:

- Automatically detects older client files
- Transparently copies new files over any ICA connection
- 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

Note Client Auto Update can update client files to newer versions of the same product and model. For example, it can be used to update the Citrix ICA Win32 Client. It cannot be used to update a Citrix ICA Win16 Client to the Citrix ICA Win32 Client.

The Citrix ICA Client Update Process

Each Citrix ICA Client has a product number, model number, and version number. The ICA Client product and model numbers uniquely identify the Citrix ICA Client.

Product/Model number	Platform
1/1	Citrix ICA Client for DOS
1/2	Citrix ICA Client for Win16
1/3	Citrix ICA Client for Win32

The version number is the release number of the Citrix ICA Client.

The process of updating Citrix ICA Clients with new versions uses the standard ICA protocol.

- The Citrix server queries the ICA Client when the user logs on. If the Citrix server detects that the ICA Client is up-to-date, it continues the logon transparently.
- If an update is needed, by default, the Citrix server informs the user of the new client and asks to perform the update. You can specify that the update occurs without informing the user and without allowing the user to cancel the update.
- By default, the user can choose to wait for the client files to finish downloading or to download the files in the background and continue working. Users connecting to the Citrix server with a modem get better performance waiting for the client update to complete. You can force the client update to complete before allowing the user to continue.
- During the client update, new Citrix ICA Client files are copied to the ICA 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 Citrix server again to continue working.
- After disconnecting from the server, the Citrix ICA Client completes the update. All client programs must be closed before the Citrix ICA Client can be updated.
- If the user does not close all client programs before clicking **OK**, a message appears informing the user of the open program. When all programs are closed, the Citrix ICA Client can complete the update.
- In case of a problem, the existing ICA Client files are saved to a folder called Backup in the Citrix ICA Client directory.

Configuring the Client Update Database

During Citrix server setup, a client update database is created that contains the Citrix ICA Win32, Win16, and DOS Clients. By default, the update database is configured to update older client versions.

You can configure a client update database on each Citrix server in a server farm, or a single client update database on a central network share. With a single database, you can configure updates once for all Citrix servers.

Note MetaFrame for UNIX does not use the Client Update Database. To use the Client Update Database, you must have either a MetaFrame for Windows or *WIN-FRAME* server in your server farm.

Use the ICA Client Update Configuration utility to:

- Create a new client update database
- Set a default client update database
- Configure database properties
- Add Citrix ICA Clients to the update database
- Remove Citrix ICA Clients from the update database
- Configure client update options

➤ **To start the ICA Client Update Configuration utility**

1. From a MetaFrame server: Click the **Start** button, point to **Programs**, and then point to **MetaFrame Tools**. Click **ICA Client Update Configuration**.

From a *WINFRAME* server: In the **Administrative Tools** folder, double-click **ICA Client Update Configuration**.

2. The **ICA Client Update Configuration** window appears.

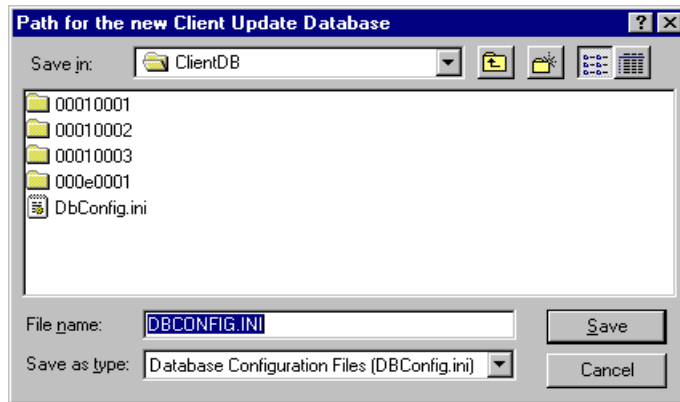
The location of the current client update database is shown in the status bar. This is the database the Citrix server uses to update Citrix ICA Clients. The main window shows the ICA Clients currently configured in the database.

Creating a New Client Update Database

The default location of the client update database is %SystemRoot%\Ica\Clientdb. A new database can be created on the local server hard drive or on a shared network drive. Multiple Citrix servers can be configured to use one shared client update database.

➤ **To create a new client update database**

1. From the **Database** menu, click **New**. The **Path for the new Client Update Database** dialog box appears:



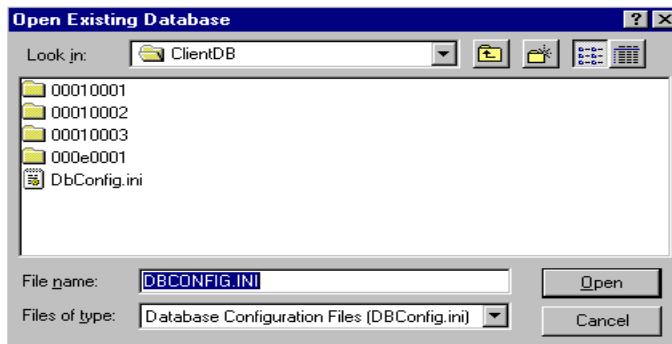
2. Enter a path for the new client update database and click **OK**. A new client update database is created in the specified folder and the new database is opened.

Setting a Default Database

An existing client update database can be used by multiple Citrix servers. If the client update database is on a shared network drive, use the ICA Client Update Configuration utility to configure all Citrix servers to use the shared database.

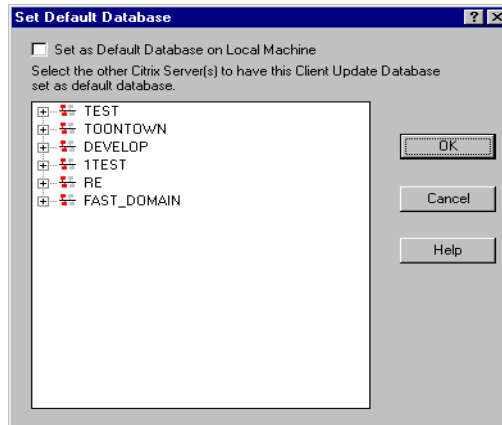
➤ **To specify a new default database for one or more Citrix servers**

1. From the **Database** menu, click **Open**. The **Open Existing Database** dialog box appears:



2. Specify the path to the database that will be used as the default.
3. Click **OK**.

- From the **Database** menu, click **Set Default**. The **Set Default Database** dialog box appears:



Select the **Set as Default Database on Local Machine** check box to make the currently opened database the default database.

Tip You can also set other Citrix servers to use the currently open database as the default database. Double-click on a domain name to view the servers in that domain. Click on a server to set its default database to the currently open database. You can select multiple servers by holding down the CTRL key.

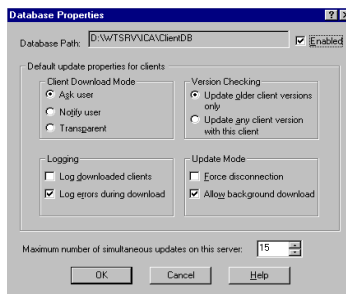
- Click **OK**.

Configuring the Properties of the Client Update Database

Use the **Database Properties** dialog box to configure the current client update database.

- **To configure the properties of the Client Update Database**

On the Database menu, click Properties. The Database Properties dialog box appears:



Clear the **Enabled** check box to disable this client update database. Citrix ICA Clients are not updated if the database is not enabled.

The **Default update properties for clients** options specify the default behavior for Citrix ICA Clients added to the update database. If you change the properties of an individual client in the database, those properties will override the default properties.

- In **Client Download Mode**, click **Ask user** to allow the user to choose to accept or postpone the client update. Click **Notify user** to notify the user of the client update and require the update. Click **Transparent** to update the user's ICA Client without notifying the user.
- In **Version Checking**, select **Update older client versions only** to update 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 of the client. Use this option to force an older client to replace a newer client.
- In **Update Mode**, select the **Force disconnection** check box to require users to disconnect and complete the update. By default, users can choose to disconnect and complete the client update after the new client files are downloaded. Clear the **Allow background download** check box to force users to wait for all client files to download before continuing. By default, users can choose to download new client files in the background and continue working.
- Select the **Log downloaded clients** check box to write an event in the event log when a Citrix ICA 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 off error logging.
- Specify the maximum number of simultaneous updates per Citrix server. When the specified number of client updates is occurring, new client connections are not updated. When the number of client updates drops below the specified maximum, new client connections are updated.

Adding and Removing Citrix ICA Clients

Use the ICA Client Update Configuration utility to add Citrix ICA Clients to and remove them from the database.

➤ To add a new Citrix ICA Client to the client update database

1. From the **Client** menu, click **New** to display the **Description** dialog box.

Enter the path to the client installation file in **Client Installation File** or click **Browse**.

The client installation file, Update.ini, is located in
%SystemRoot%\System32\Clients\Ica\Ica32\disks\disk1.

2. After you specify the client installation file, the **Client Name**, **Product**, **Model**, **Version**, and icon of the selected client appear.

You can also modify the **Comment** used for this client. After making any changes, click **Next** to continue.

3. The **Update Options** dialog box appears.

The **Update Options** dialog box controls how the client update occurs. These options for each client override the settings specified for the database as a whole on the **Database Properties** dialog box.

In **Client Download Mode**, click **Ask user** to give the user the option to accept or postpone the client update. Click **Notify user** to notify the user of the client update and require the update. Click **Transparent** to update the user's ICA Client without notifying the user.

In **Version Checking**, select **Update older client versions only** to update 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 of the client. Use this option to force an older client to replace a newer client.

By default, users can choose to disconnect and complete the client update after the new client files are downloaded. Select the **Force disconnection** check box to require users to disconnect and complete the update.

By default, users can choose to download new client files in the background and continue working. Clear the **Allow background download** check box to force users to wait for all client files to download before continuing.

You can optionally enter a message in **Display this message on the user terminal**. The user can view this message at the start of the client update by clicking **More Info** in the dialog box that appears.

Click **Next** to continue.

4. The **Event Logging** dialog box appears.

Auto Client Update uses the Windows NT event log to report status messages and update errors.

- Select the **Log downloaded clients** check box to write an event in the event log when a Citrix ICA 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 off error logging.

Click **Next** to continue.

5. The **Enable Client** dialog box appears.

The client update database can contain multiple clients with the same product, model and version information. However, only one client of each product, model and version can be enabled. The enabled client is the one used for the auto client update.

Select the **Enable** check box to update Citrix ICA Clients to this client. All other clients of the same product, model, and version are disabled.

6. Click **Finish** to copy the Citrix ICA Client installation files into the client update database.

➤ **To remove a Citrix ICA Client from the database**

1. In **Client Update Configuration**, click on the Citrix ICA Client to remove.
2. From the **Client** menu, click **Delete**. A dialog box displays the selected client information and asks for confirmation. Click **OK** to remove the client.

The Citrix ICA Client is removed from the database.

Changing the Properties of an ICA Client in the Database

Use the **Properties** dialog box to maintain the configuration of a Citrix ICA Client in the client update database. The **Properties** dialog box contains four tabs: the **Description** tab, the **Update Options** tab, the **Event Log** tab, and the **Client Files** tab.

➤ **To modify the properties of a Citrix ICA Client in the database**

1. In **ICA Client Update Configuration**, click on the Citrix ICA Client to modify.
2. From the **Client** menu, click **Properties**. The **Properties** dialog box appears.

- The **Description** tab displays information about the selected client. The **Product**, **Model**, **Version**, and **Client Name** are display-only fields.

Type a new description of the client in **Comment**.

Select the **Enabled** check box to update Citrix ICA Clients to this client. All other clients of the same product, model, and version are disabled.

The client update database can contain multiple clients with the same product, model, and version information. However, only one client of each product, model, and version can be enabled. The enabled client is the one used for the auto client update.

- The **Update Options** tab configures how the client is updated.

In **Client Download Mode**, click **Ask user** to give the user the option to accept or postpone the client update. Click **Notify user** to notify the user of the client update and require the update. Click **Transparent** to update the user's ICA Client without notifying the user.

In **Version Checking**, click **Update older client versions only** to update client versions that are older than the new client. Click **Update any client version with this client** to update all client versions to this version of the client. Use this option to force an older client to replace a newer client.

By default, users can choose to disconnect and complete the client update after the new client files are downloaded. Select the **Force Disconnection** check box to require users to disconnect and complete the update.

By default, users can choose to download new client files in the background and continue working. Clear the **Allow background download** check box to force users to wait for all client files to download before continuing.

You can optionally enter a message in **Display this message on the user terminal**. The user can view this message at the start of the client update by clicking **More Info** in the dialog box that appears.

- The **Event Logging** tab configures the events to log for the client update.

Auto Client Update uses the Windows NT event log to report status messages and update errors.

Select the **Log downloaded clients** check box to write an event in the event log when a Citrix ICA 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 off error logging.

- The **Client Files** tab displays the individual files for the ICA Client

The client update database stores the **File Name**, **Group**, **Flags**, **FileSize**, and **File CRC** for each file of a Citrix ICA Client.

Configuring the ICA Win32 Client



Overview

This chapter describes how to use and configure the ICA Win32 Client. Topics in this chapter include:

- Mapping client devices
- Mapping client drives
- Mapping client printers
- Mapping client COM ports
- Mapping client audio
- Connection types
- Configuring connections to Citrix servers and published applications

Mapping Client Devices

The Citrix ICA Client supports mapping devices on client computers so they are available to the user from within an ICA session. Users can:

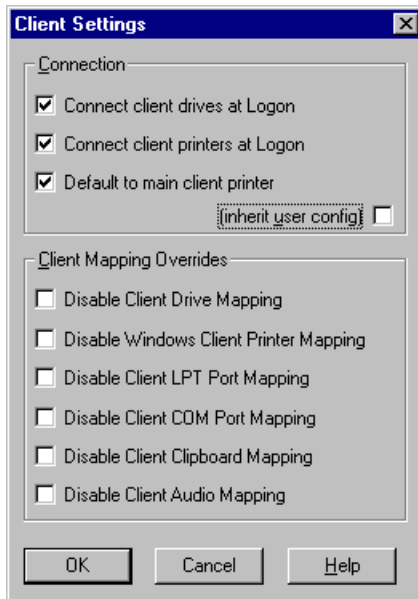
- Transparently access local drives, printers, and COM ports
- Cut and paste between the ICA session and the local Windows clipboard
- Hear audio (system sounds and .Wav files) played from the ICA session

During logon, the ICA Client informs the Citrix server of the available client drives, COM ports, and LPT ports. By default, client drives are mapped to server drive letters and server print queues are created for Windows ICA Client printers so they appear to be directly connected to the Citrix server. These mappings are available only for the current user during the current session. They are deleted when the user logs off and recreated the next time the user logs on.

You can use the net use and change client commands to map client devices not automatically mapped at logon. See your Citrix server documentation for information about the change client command.

Turning Off Client Device Mappings

On a server, specify client device mapping options in the Client Settings dialog box in Terminal Server Connection Configuration. On a *WINFRAME* server, specify client device mapping options in Citrix Connection Configuration.



The Connection options control whether drives and printers are mapped to client drives and printers. If these options are cleared, the devices are still available but must be mapped to drive letters and port names manually.

Use the Client Mapping Overrides to disable client device connections.

Option	Description
Connect client drives at Logon	If this option is checked, the client computer's drives are automatically mapped at logon.
Connect client printers at Logon	If this option is checked, the client computer's printers are automatically mapped at logon. This option applies only to Windows clients and maps only printers already configured in Print Manager on the client computer.
Default to main client printer	If this option is checked, the user's default client printer is configured as the default printer for the ICA session.
(inherit user config)	If this option is checked, the per-user settings in User Manager override these settings.

Mapping Client Drives

Client drive mapping allows drive letters on the Citrix server to be redirected to drives that exist on the client computer; for example: drive H in a Citrix user session can be mapped to drive C of the local computer running the Citrix ICA Client.

Client drive mapping is transparently built into the standard Citrix device redirection facilities. These mappings can be used by the File Manager or Explorer and your applications just like any other network mappings.

Important Client drive mapping is not supported when connecting to MetaFrame for UNIX 1.0 and 1.1 servers.

The Citrix server can be configured during installation to automatically map client drives to a given set of drive letters. The default installation mapping maps drive letters assigned to client drives starting with V and works backwards, assigning a drive letter to each fixed disk and CD-ROM. (Floppy drives are assigned their existing drive letters.) This method yields the following drive mappings in a client session:

Client drive letter	Is accessed by the Citrix server as:
A	A
B	B
C	V
D	U

The Citrix server can be configured so that the server drive letters do not conflict with the client drive letters; in this case the Citrix server drive letters are changed to higher drive letters. For example, changing Citrix server drives C to M and D to N allows client computers to access their C and D drives directly. This method yields the following drive mappings in a client session:

Client drive letter	Is accessed by the Citrix server as:
A	A
B	B
C	C
D	D

The drive letter used to replace the Citrix server drive C is defined during Setup. All other fixed disk and CD-ROM drive letters are replaced with sequential drive letters (for example; C->M, D->N, E->O). These drive letters must not conflict with any existing network drive mappings. If a network drive is mapped to the same drive letter as a Citrix server drive letter, the network drive mapping is not valid.

When an ICA Client computer connects to a Citrix server, client mappings are re-established unless automatic client device mapping is disabled. Automatic client device mapping can be configured for ICA connections and users. In the **Client Settings** dialog box, you can enable or disable automatic client device mapping for an ICA connection. The **User Configuration** dialog box in User Manager for Domains allows you to enable or disable automatic client device mapping for a user.

Mapping Client Printers

The Citrix ICA Win32 Client supports auto-created printers. With *auto-created printers*, users find their local printers mapped to their sessions and ready for use as soon as they connect.

Published applications and ICA server connections configured to run a specified initial program offer users the same access to their local printers. When connected to published applications, users can print to local printers in the same way they would print to a local printer when using locally run applications.

Important For information about how to configure ICA Client printing for MetaFrame for UNIX connections, see the *MetaFrame for UNIX Operating Systems Administrator's Guide*.

If the **Connect Client Printers at Logon** check box is checked in the terminal connection or user profile, the client printers are automatically connected when users log on and are deleted when they log off if the printers do not contain any print jobs. If print jobs are present, the printer (and its associated jobs) is retained.

If users do not want the automatically created printers deleted when they log off, use Print Manager in the ICA session to view the **Properties** dialog box for the client printer. This dialog box contains a **Comment** field (on MetaFrame servers) or a **Description** field (on *WINFRAME* servers) that contains the string **Auto Created Client Printer** for automatically created client printers. If you modify or delete this description, the printer is not deleted at logoff. Subsequent logins will use the printer already defined and not modify it. If users change the Windows printer settings, they will not automatically be set in this case. One reason for not wanting them deleted may be the use of custom print settings.

If your user and terminal connection profile do not specify **Connect Client Printers at Logon**, you can use Print Manager to connect to a client printer. These printers are not automatically deleted when you log off.

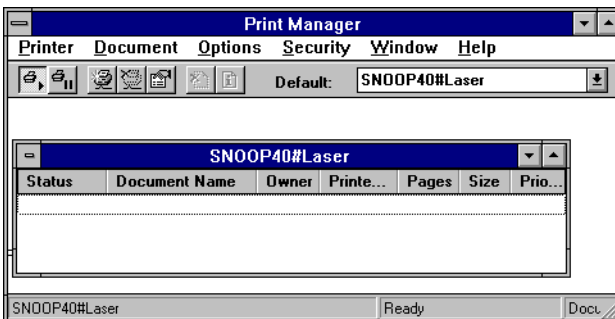
➤ **To view mapped client printers when connected to a MetaFrame server**

While connected to the MetaFrame server, double-click **My Computer** on the remote desktop and then double-click **Printers**. The **Printers** dialog box appears:



The **Printers** screen displays the local printers mapped to the ICA session. The name of the printer takes the form *clientname#printername*, where *clientname* is the unique name given to the client computer during ICA Client Setup and *printername* is the Windows printer name. In this example ICA session, a client machine called “Snoop40” has access to its local printer named “Laser.” This name cannot be changed and is used to locate the specific printer. Because the Windows printer name is used and not the port name (as with DOS Client printing), multiple printers can share a printer port without conflict.

- **To view mapped client printers when connected to a *WINFRAME* server**
While connected to the *WINFRAME* server, double-click **Print Manager** in the **Main** program group. The **Print Manager** appears:



Print Manager displays the local printers mapped to the ICA session. The name of the printer takes the form *clientname#printrname*, where *clientname* is the unique name given to the client computer during ICA Client setup and *printrname* is the Windows printer name. In this example ICA session, a client machine called “Snoop40” has access to its local printer named “Laser.” This name cannot be changed and is used to locate the specific printer. Because the Windows printer name is used and not the port name (as with DOS Client printing), multiple printers can share a printer port without conflict.

Mapping Client COM Ports

Client COM port mapping allows devices attached to the client computer’s COM ports to be used during ICA sessions on a Citrix server. These mappings can be used just like any other network mappings.

Note Client COM port mapping is not supported when connecting to MetaFrame for UNIX 1.0 and 1.1 servers.

- **To map a client COM port**
 1. Start the ICA Client and log on to the Citrix server.
 2. Start a DOS command prompt: on *WINFRAME*, double-click **Command Prompt** in the **Main** program group. On MetaFrame, click **Start**, then click **Programs**, then click **Command Prompt**.
 3. At the prompt, type **net use comx: \\client\comz:** where *x* is the number of the COM port on the server (ports 1 through 9 are available for mapping) and *z* is the number of the client COM port you want to map. Press ENTER.
 4. To confirm the operation, type **net use** at the prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports.

To use this COM port in a session on a Citrix server, install your device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session on the server. Use this mapped COM port as you would a COM port on the client computer.

Note COM port mapping is not TAPI-compatible. TAPI devices cannot be mapped to client COM ports.

Mapping Client Audio

Client audio mapping enables applications running on the Citrix server to play sounds through a Windows-compatible sound device installed on the client computer. You can control the amount of bandwidth used by client audio mapping.

Note Client audio mapping is not supported when connecting to MetaFrame for UNIX 1.0 and 1.1 servers.

- **To configure ICA Client audio on a MetaFrame server**
 1. Click **ICA Settings** in Terminal Server Connection Configuration.
 2. Select an option from the **Client Audio Quality** drop-down list.
- **To configure ICA Client audio on a *WINFRAME* server**
 1. Click **ICA Settings** in Citrix Connection Configuration.
 2. Select an option from the **Client Audio Quality** drop-down list.

Client Audio Mapping can cause excessive load on the Citrix servers and the network. The higher the audio quality, the more bandwidth is required to transfer the audio data. Higher quality audio also uses more server CPU to process. Three different audio quality settings are available, or client audio mapping can be disabled completely.

Important You can set audio quality on a per connection basis, but users can also set it on the client computer. If the client and server audio quality settings are different, the lower of the two qualities is used.

The **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 computer. The host CPU utilization will decrease 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 Moderate setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

Connection Types

Using the Citrix ICA Win32 Client, users can connect to a Citrix server in the following ways:

- By dialing into a Citrix server using the modem installed on the client PC. This method uses a serial connection to a Citrix server (custom ICA connections only).
- Over a direct serial cable connection to a Citrix server. This method uses a serial connection to a Citrix server (custom ICA connections only).
- Over the local or wide-area network connection between the client PC and the Citrix server. This method uses one of the following network protocols:
 - TCP/IP
 - TCP/IP+HTTP
 - IPX
 - SPX
 - NetBIOS

You can also use Microsoft's Remote Access Service (RAS) or Dial-Up Networking (DUN) in combination with the Citrix ICA Client to connect a client PC with a Citrix server.

This type of connection requires:

- The RAS or DUN client software is installed on the client PC
- The RAS server or third-party PPP server is in the same network as the Citrix server

Configuring a SOCKS Proxy Connection

You can configure the ICA Win32 Client to connect to a Citrix server through a SOCKS proxy server. This section describes:

- Why you use a SOCKS proxy server
- Where to locate your SOCKS proxy server

Using SOCKS to Direct ICA Traffic Through Firewalls

To limit access into and out of your Citrix servers, configure a SOCKS proxy server to handle connections between clients and the server. You can place the proxy server on either side of the firewall, or in some situations, on both sides of the firewall.

The benefits of using a SOCKS proxy server include:

- Information hiding, where system names inside the firewall are not made known to systems outside the firewall through DNS (Domain Name System)
- Authentication between an ICA Client and SOCKS proxy servers
- Authentication between two SOCKS proxy servers
- Relaying between two SOCKS proxy servers
- Channeling different TCP connections through one connection
- UDP proxying

Note The ICA Win32 Client supports only clear text username and password authentication.

The general procedure for connecting the ICA Win32 Client through a proxy is:

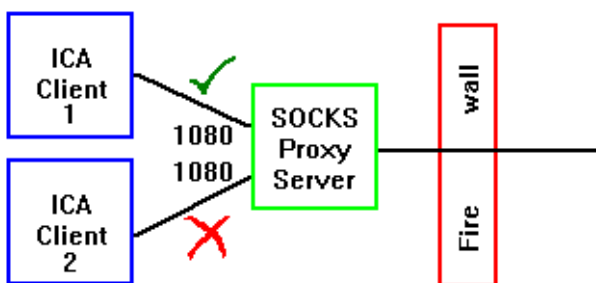
1. Be sure that your firewall is configured and working properly.
2. Install your SOCKS proxy server and test that it works with Web browsers.
3. Configure and deploy the ICA Win32 Client.

Locating Your Proxy Server

You can locate your proxy server on either side of your firewall. In some situations, you may want to locate a proxy server on both sides of the firewall. Typical SOCKS proxy configurations are described below. See your proxy documentation for further details about placement and implementation of your proxy server.

Setting Up a Proxy between Clients and a Firewall (for Outbound Connections)

To restrict clients from connecting directly to servers outside your firewall, install a proxy server between the client systems and the firewall, as shown below.

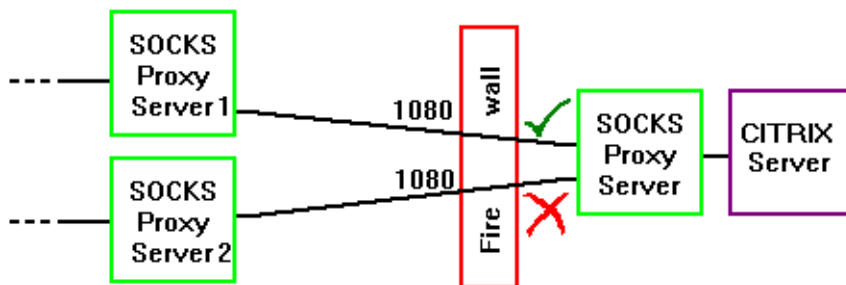


The proxy server uses its authentication features to determine whether ICA Clients can access networks outside the firewall. Configure the firewall to pass only network traffic that comes from the SOCKS proxy server.

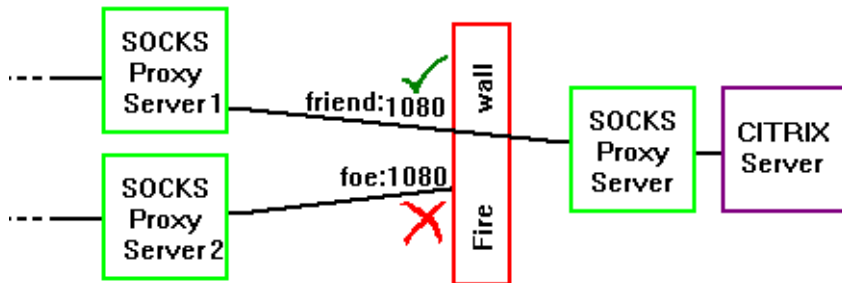
Setting Up a Proxy Between Citrix Servers and a Firewall (for Inbound Connections)

To protect your Citrix servers, install a proxy server between your servers and the firewall. You can configure the firewall in two ways:

Maximize Trust. Configure the firewall to pass only network traffic that is directed to the SOCKS proxy server. The proxy server performs the authentication of the ICA Client.

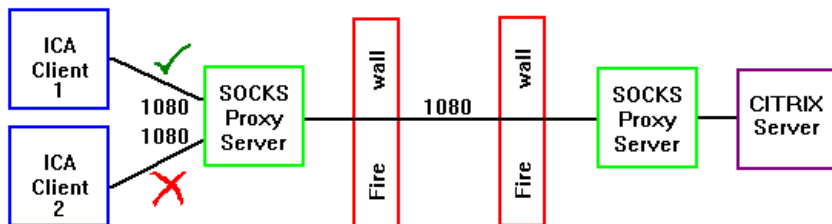


Minimize Risk. Configure the firewall to allow only connections from specific machines in addition to passing only network traffic that is directed to the SOCKS proxy server.



Setting Up a Virtual Private Network Using Two Proxy Servers

You can create a Virtual Private Network (VPN) between two sites by configuring a proxy server inside the firewall at both the client and server sites. Set up the firewalls to allow only directed UDP traffic between the two SOCKS proxy servers and TCP on the SOCKS port. For additional security, configure the SOCKS proxy server on the ICA Client side to authenticate with the SOCKS proxy server on the Citrix server side. To obtain the address of a SOCKS proxy server within an outside firewall, contact the system administrator responsible for configuring that firewall.



For more information about configuring the ICA Win32 Client to use with a SOCKS proxy server, see “Configuring Firewall Settings for Application Sets” and “Configuring Firewall Settings for Custom ICA Connections” later in this chapter.

Configuring Connections to Citrix Servers and Published Applications

This section describes how to configure connections to Citrix servers and published applications. Program Neighborhood offers the user two methods of connection:

- Connecting to Citrix servers and published applications using application sets
- Connecting to Citrix servers and published applications using custom ICA connections

For detailed information about application publishing, see your Citrix server documentation.

Configuring Server Location and Business Recovery

Server location (also called server browsing) provides a method for a user at a network-connected ICA Client to view a list of all Citrix servers on the network that have ICA connections configured for that network protocol, and a list of all published applications. You can specify a separate server location for each network protocol.

The default setting for server location is **(Auto-Locate)**. The auto-locate function works as follows:

4. The ICA Client broadcasts a “Get Nearest Citrix server” packet. The first Citrix server to respond returns the the address of the master ICA Browser, which is used in the next step.
5. The ICA Client sends a request for the server and published application lists to the master ICA Browser.
6. The master ICA Browser responds with a list of all Citrix servers on the network and a list of all published applications.

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 Citrix 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 simultaneously (broadcasting) and the first server to respond is the one to which you connect. The client broadcasts only if you have selected **(Auto-locate)** from the address list. To eliminate broadcasts on your network, or if your network configuration uses routers or gateways, you can set a specific server address for the Citrix server that functions as the master browser.

➤ **To configure server location and business recovery settings:**

On the **Connection** page for both custom ICA connections and application sets, use the following fields to configure server location and business recovery settings:

Network Protocol. Use the **Network Protocol** field to instruct the Citrix ICA Client what low-level network protocol to use to connect to a Citrix server. The protocol that you select must be installed on your local computer and must also be in use on the Citrix server to which you want to connect.

Server Group. Use the **Server Group** field to create lists of specific servers that you want to designate as primary and backup servers for connecting to published applications.

Use this field to designate whether the servers entered in the **Address List** field belong to your Primary, first backup (Backup 1), or second backup (Backup 2) group.

Important Each of these server groups **must** be located on different subnets.

Address List. Use the address list field to:

- Designate servers for your primary and backup server groups
- View and change the list of Citrix servers used in the selected server group.
- Specify an address of a Citrix server that will retrieve server and published application information from the network.

If you have not selected any servers, [**Auto-Locate**] is selected by default.

- Click **Add** to add a Citrix server to your server group's address list. You can use the IP address or name of the Citrix server.

Important All Citrix servers within a server group **must** be located on the same subnet.

- Click **Delete** to remove the selected Citrix server from the Address List.
- If (**Auto-Locate**) is selected, the first server is located automatically.
- **Firewalls.** Click **Firewalls** to display the **Firewall Settings** page. Use this page to configure the ICA Win32 Client to connect to a Citrix server through a SOCKS proxy server, or to use an alternate address to browse for Citrix servers and published applications that are inside a firewall.

➤ **To configure firewall settings**

1. Click **Firewalls** on the **Connection** properties page.
2. Select **Use alternate address for firewalls** to browse for Citrix servers or published applications that are inside a firewall from a client machine that is outside the firewall. The firewall and the Citrix servers must be configured to map the internal network addresses of Citrix servers to external Internet addresses. Enter the external Internet address in the **Address List**.
3. Click the check box next to **Connect via SOCKS proxy**. Enter the SOCKS proxy's IP address in the **Address of proxy to use** box. Enter the port number of the SOCKS proxy server (if different than 1080) in the **Port** box. See the online help for more information.

Note Because you can enter only one SOCKS proxy server address, you cannot configure separate SOCKS settings for primary and backup servers.

Configuring TCP/IP+HTTP Server Location

You can retrieve Citrix server and published application information across a firewall that does not allow UDP broadcasts by using TCP/IP+HTTP server location.

➤ **To configure TCP/IP+HTTP server location**

1. Select **TCP/IP + HTTP** from the **Network Protocol** drop-down list.
2. Click **Add** to display the **Add Server Location Address** box.
3. Enter the name or IP address of a Citrix server and a recognized port number (the default is port 80) and click **OK**.

Note If you do not enter an IP address, you must have a Citrix server on your network mapped to the default name of *ica.domainname*, where *domainname* is a TCP/IP domain name. TCP/IP+HTTP server location does not support the **(Auto-Locate)** function.

4. The specified server responds with a list of all servers and published applications in its server farm.

Important TCP/IP+HTTP server location retrieves information only on a per server farm basis. To retrieve information from more than one server farm, you must configure TCP/IP+HTTP server location settings for each application set. For custom ICA connections, you must configure the TCP/IP+HTTP server location settings for each ICA connection. Do not place addresses from separate farms into the same server location list.

For more information about configuring connections, see “Configuring Connection Properties” later in this chapter.

Using Application Sets and Custom ICA Connections

An *application set* is a user's view of the applications published on a given server farm, which that user is authorized to access. Applications published in an application set are pre-configured for such session properties as window size and colors and supported level of encryption, audio, and video. If these settings are not required to run the published application (such as a required level of encryption), they can be changed on the client machine at the application set level.

Important Application set functionality is not available for applications published on a MetaFrame for UNIX server. To connect to an application published on a MetaFrame for UNIX server, you **must** use a custom ICA connection.

A *custom ICA connection* is a connection to:

- An existing Citrix server outside of a server farm scope of management
- An application published prior to the installation of a MetaFrame or *WINFRAME* 1.8 server that cannot be migrated into a server farm
- An application published on a MetaFrame for UNIX Operating Systems server

Applications published in this way are not enabled for automatic configuration of Program Neighborhood sessions.

Adding Application Sets and Custom ICA Connections

To locate additional application sets that you can access, or to add a custom ICA connection, use the Find a New Application Set and the Add New ICA Connection wizards.

➤ **To find a new application set**

1. Double-click the Find a New Application Set icon in the Program Neighborhood window.
2. Follow the instructions in the Find a New Application Set wizard.

➤ **To add a custom ICA connection**

1. Double-click the **Custom ICA Connections** option to display the Custom ICA Connections window.
2. Double-click the Add ICA Connection icon
3. Follow the instructions in the Add New ICA Connection wizard.

For details about the settings in the Find a New Application Set and Add New ICA Connection wizards, see the wizards' application help.

Configuring Application Sets and Custom ICA Connections

The following procedures describe how to configure the properties and settings of application sets and custom ICA connections.

- Configuring connection properties
- Configuring default options
- Configuring login properties
- Configuring general settings
- Configuring bitmap caching
- Configuring hotkeys
- Configuring event logging

Configuring Connection Properties

➤ **To configure connection properties:**

1. Start Program Neighborhood.
2. Select an application set or a custom ICA connection.
3. In the Program Neighborhood toolbar, click **Properties** to display the **Properties** dialog box.
4. Click the **Connection** tab to display the **Connection** page.

From the **Connection** page, you can configure the following:

Connection Type. Choose a connection type. Select **Local Area Network** to connect to the Citrix server over a local network that covers a confined geographical area (such as an office building or complex). Select **Wide Area Network** to connect to the Citrix server over a network that covers a wide geographical area.

If you are configuring to a custom ICA connection, you can select either **Server** or **Published Application**. When you select the **Server** radio button, this field specifies the Citrix server that will be used to connect and run the published application.

Configuring Default Options

➤ **To configure default options:**

1. Start Program Neighborhood.
2. If you are configuring an application set:

Select the application set and click **Settings** in the Program Neighborhood toolbar.

If you are configuring a custom ICA connection:

Right-click in the custom ICA connection window and select **Custom Connection Properties**.

3. Click the **Default Options** tab to display the **Default Options** page. For custom ICA connections: Any options configured in this dialog box are applied to **all** custom ICA connections. To override these default options on an individual custom ICA connection, select the ICA connection and click **Properties** on the Program Neighborhood toolbar. Select the **Options** tab.

From the **Options** and **Default Options** pages, you can configure the following:

Use data compression. Data compression reduces the amount of data that needs to be transferred but requires additional processor resources to compress and decompress the data. If your connection is bandwidth-limited, enabling data compression increases performance.

Use disk cache for bitmaps. Bitmap caching to disk stores commonly-used graphical objects such as bitmaps in a local cache on the client's hard disk space. If your connection is bandwidth-limited, enabling disk caching increases performance. If your client is on a high-speed LAN, you do not need disk caching. Dial-in connections have disk caching enabled by default.

Queue mouse movements and keystrokes. Queuing causes the client to send mouse and keyboard updates less frequently to the Citrix server. Check this option to reduce the number of network packets sent from the ICA Client to the Citrix server. Leaving this option unchecked makes the session more responsive to keyboard and mouse movements. Checking this option improves performance if you dial in to RAS and then use a network to connect.

Turn off desktop integration for this application set. You can configure Program Neighborhood to create desktop shortcuts and add items to the **Start** menu for published applications. If users do not want published applications sent directly to the desktop, they can select this check box.

Enable sound. Check this box to enable sound support. The client computer must have a compatible sound card installed. Published applications can then play sounds on the client.

Select one of the following values for **Quality**:

- **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 computer. The host CPU utilization will decrease 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 Moderate setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

Encryption Level. Select the level of encryption for the ICA connection. The default level is Basic. Select **RC5 128-bit Login Only** to use encryption during authentication.

The Citrix server must be configured to allow the selected encryption level or greater. To enable encryption levels higher than **Basic**, the Citrix server must support RC5 encryption. This support is included with SecureICA Services and Feature Release 1.

Note Selecting RC5 encryption disables automatic logon to the Citrix server.

SpeedScreen Latency Reduction. SpeedScreen latency reduction is a collective term used to describe the functionality that helps enhance user experience on slower network connections. Latency reduction is available only if you are connecting to a server that is configured and licensed for latency reduction.

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. Choose either **Mouse Click Feedback** or **Local Text Echo**.

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 mode to **Auto** to turn latency reduction on or off depending on the speed of the connection. You can override **Auto** mode using the **Toggle Latency Reduction** hotkey.

Window Size. This field specifies the window size that a published application runs in.

If you are connecting to a published application, you can select **Seamless Windows** to run the application on your local desktop in a separate, seamless window.

Window Colors. This field specifies the number of colors displayed.

Use Server Default (for application sets). To use the server-configured default settings for the properties, make sure this box is checked. To change the settings, de-select this check box and choose new settings.

Use Custom Default (for custom ICA connections). To override the default options, deselect this check box.

Configuring Login Properties

➤ To configure login properties

1. Start Program Neighborhood.
2. Select an application set or custom ICA connection.
3. If you are configuring an application set, select the application set and click **Settings** in the Program Neighborhood toolbar. If you are configuring a custom ICA connection, select the custom ICA connection and click **Properties** in the Program Neighborhood toolbar
4. Click the **Login Information** tab.
5. Enter a valid username, domain, and password for this application set. If the **Use local username and password** box is checked, the user's local desktop credentials are passed to the server.
6. To save your password after you exit Program Neighborhood and close all connections, select **Save password**. If you leave this box unchecked, this password is retained only as long as Program Neighborhood and all current connections are open.

Note The **Save password** option is available only for application sets.

7. Click **OK**.

Preventing Users From Saving Passwords

Program Neighborhood provides administrators with the ability to disable password saving for a single application set or all application sets. By setting a parameter in one of two Program Neighborhood Ini files, you can prevent the **Save Password** check box from appearing in the **Login Information** tab and in the initial logon screen a user sees when authenticating to an application set.

To disable password saving, you must add a parameter and value to one of two Program Neighborhood .Ini files located in the Program Neighborhood installation directory. The file you choose to add the parameter and value to determines which application sets prohibit password saving. Add the parameter and value to:

- Appsrv.ini to prevent all application sets from saving password information
- Pn.ini to prevent individual application sets from saving password information

Note If you add the parameter to both files, the parameter in Appsrv.ini overrides the Pn.ini entry if the Appsrv.ini entry is set to On. If the entry in Appsrv.ini is set to Off or if it does not exist, the entry in Pn.ini is used (if it exists). Setting an entry to Off and leaving it out of the .Ini files results in **Save Password** check boxes appearing in Program Neighborhood.

➤ **To disable password saving for all application sets**

1. Exit Program Neighborhood if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Load the file Appsrv.ini in a text editor.
3. Locate the section named [WFClient].
4. Add the following text to the list of parameters and values in [WFClient]:
NoSavePwordOption=On
If the parameter already exists, make sure its value is set to **On**.
5. Save the file and exit the text editor.
6. Start Program Neighborhood.

Adding this parameter and setting it to **On** prevents users from saving passwords for all application sets. Any existing cached passwords are deleted.

➤ **To disable password saving for individual application sets**

1. Exit Program Neighborhood if it is running. Make sure all Program Neighborhood components, including the Connection Center, are closed.
2. Load the file Pn.ini in a text editor.
3. Locate the section name that corresponds to the application set on which you want to disable password saving; for example, [MyAppSet].
4. Add the following text to the list of parameters in the section:
NoSavePwordOption=On
If the parameter already exists, make sure its value is set to **On**.

5. Add the parameter and value to each application set section as desired.
6. Save the file and exit the text editor.
7. Start Program Neighborhood.

Adding this parameter and setting it to **On** prevents users from saving passwords for the specified application set(s). Any existing cached passwords are deleted.

Configuring General Settings

➤ To configure the general settings for application sets

1. Start Program Neighborhood.
2. Select an application set or custom ICA connection.
3. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
4. Click the **General** tab.

From the **General** page, you can configure the following settings:

- **Client Name.** This field allows you to change the name of the client computer. The Citrix server uses the client name to uniquely identify resources (such as mapped printers and disk drives) associated with a given client PC. The client name must be unique for each computer running the Citrix ICA Client.
- **Serial Number.** This is the serial number of the ICA Client software. This field is necessary only when you are using the Citrix ICA Client with a product such as *WINFRAME* Host/Terminal, which requires each client to have a Citrix *PC Client Pack* serial number to connect to the server. If a serial number is required, you must enter it exactly as it appears on the Serial Number card. The **Serial Number** field is not used by MetaFrame servers.
- **Keyboard Layout.** Allows you to specify the keyboard layout of your client computer. The Citrix server uses the keyboard layout information to configure your user session for your keyboard layout. The default value of **(User Profile)** uses the keyboard layout specified in your user profile.
- **Keyboard Type.** Allows you to specify the keyboard type of your client computer. The Citrix server uses the keyboard type information to configure your user session for your keyboard type. Use the default value of **Default** for most English and European keyboards. When used with a Japanese keyboard, **Default** auto-detects the keyboard type.
- **Display Connect To screen when making Dial-in Connections.** Check this box to display the **Connect To** screen when you make a dial-in connection.

- **Display terminal window when making Dial-in Connections:** Check this box if your dial-in configuration includes third-party products, such as security devices and X.25 PADs, that require an ASCII dialog before connecting to the Citrix server.
- **Allow automatic client updates:** Check this box to allow the Citrix server to update your Citrix ICA Client software when newer versions become available. When the Citrix server detects an outdated client version, it notifies you that a newer version is available and replaces the ICA Client files.
- **Use local username and password for logon:** Check this box to enable this feature in the **Login** dialogs.

Configuring Bitmap Caching

➤ To configure bitmap caching

1. Start Program Neighborhood
2. Select an application set or custom ICA connection.
3. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
4. Click the **Bitmap Cache** tab.

From the **Bitmap Cache** page, you can configure the following settings:

- **Amount of disk space to use.** Use this tool to configure the amount of disk space as a percentage of the partition containing the caching directory.
- **Bitmap cache directory.** The default directory where the cached data is stored is displayed in this field.
- **Change Directory.** If you want to specify a new directory for cached data, click the **Change Directory** button to display the **Change Bitmap Cache Directory** dialog box.
- **Minimum size bitmap to be cached.** The size of the smallest bitmap to be cached to disk.
- **Clear cache.** Click this button to remove all cached data from the directory.

Tip It is not recommended to clear the cache if any ICA connections are open. Before clearing the cache, verify that all ICA connections are closed.

Configuring Hotkeys

➤ **To configure the hotkeys**

1. Start Program Neighborhood.
2. Select an application set or custom ICA connection.
3. From the **Program Neighborhood** menu bar, click **Settings** to display the **Settings** dialog box.
4. Click the **Hotkeys** tab.
5. For each hotkey in the list, select a shift state and a key.
6. You can disable the hotkey by selecting (**none**) for the key.

Hotkeys are used to control the behavior of the Win32 Client, and as substitutes for the standard Windows hotkeys for a published application.

The fields on the **Hotkeys** page are:

- **Task List.** The Task List hotkey displays the Windows Task List for your local Windows NT 3.51 computer or the local Start menu if your local machine is a Windows NT 4.0 or Windows 95/98/2000 computer.
- **Close Remote Application.** The Close Remote Application hotkey disconnects the published application from the Citrix server and closes the Citrix ICA Client window. The behavior of this hotkey is the same as choosing Close from the system menu of the ICA Client window.
- Closing the published application in this manner either leaves the associated application in a disconnected state on the Citrix server, or exits the application on the Citrix server, depending on how the server is configured.
- **Toggle Title Bar.** This hotkey causes the ICA Client window to alternately display and hide its title bar. When the title bar is displayed, the ICA Client window can be moved or closed.

Tip This hotkey must be used to return to a seamless window after accessing the Windows NT Security dialog box using the **CTRL+ALT+DEL** hotkey.

- **CTRL-ALT-DEL.** This hotkey causes the CTRL-ALT-DEL key sequence to be sent to the server that is running the published application. In Windows NT, the CTRL-ALT-DEL key sequence causes a Windows NT session to switch to the Windows NT Security desktop.
- **CTRL-ESC.** This hotkey causes the CTRL-ESC key sequence to be sent to the server that is running the published application. CTRL-ESC is a standard Windows hotkey. See your Windows documentation for more information about the CTRL-ESC hotkey.

- **ALT-ESC.** This hotkey causes the ALT-ESC key sequence to be sent to the server that is running the published application. ALT-ESC is a standard Windows hotkey. See your Windows documentation for more information about the ALT-ESC hotkey.
- **ALT-TAB.** This hotkey causes the ALT-TAB key sequence to be sent to the server that is running the published application. ALT-TAB is a standard Windows hotkey. See your Windows documentation for more information about the ALT-TAB hotkey.
- **ALT-BACKTAB.** This hotkey causes the ALT-SHIFT-TAB key sequence to be sent to the server that is running the published application. ALT-SHIFT-TAB is a standard Windows hotkey. See your Windows documentation for more information about the ALT-SHIFT-TAB hotkey.
- **CTRL-SHIFT-ESC.** This hotkey causes the CTRL-SHIFT-ESC key sequence to be sent to the server that is running the published application. CTRL-SHIFT-ESC is a standard Windows NT 4.0 hotkey. See your Windows NT 4.0 documentation for more information about the CTRL-SHIFT-ESC hotkey.
- **Toggle Latency Reduction.** This hotkey turns SpeedScreen latency reduction on or off. Turning on latency reduction reduces the time between your keyboard or mouse input and a visible response on the screen.

Configuring Event Logging

Use the **Event Logging** page to instruct the Citrix ICA Client whether or not to keep a log of various events that occur while running published applications.

➤ To configure event logging

1. Start Program Neighborhood.
2. Select an application set or custom ICA connection.
3. From the **Program Neighborhood** menu bar, click **ICA Settings** to display the **ICA Settings** dialog box.
4. Click the **Event Logging** tab.

From the **Event Logging** page, you can configure the following settings:

Event Log File. Enter the name of the file to log Citrix ICA Client events to in the **Name** field.

- Select the **Overwrite existing event log** button to cause the event log file to be overwritten with new events when a published application is run.
- Select the **Append to existing event log** button to keep old events and add new ones to the end of the file.

Log Events. Use these buttons to select the event categories that you want to log. If no events are selected, no logging takes place.

Five event categories can be selected for logging:

- **Connections and Disconnections.** Logs an event whenever the Citrix ICA Client connects and disconnects from a Citrix Server. This category is selected by default.
- **Errors.** Logs an event whenever an error is encountered by the Citrix ICA Client. This category is selected by default.
- **Data Transmitted.** Logs an event for each packet of information sent by the Citrix ICA Client to the Citrix server. This is intended primarily for technical support purposes.
- **Data Received.** Logs an event for each packet of information received by the Citrix ICA Client from the Citrix server. This category is intended primarily for technical support purposes.
- **Keyboard and Mouse Data.** Logs an event whenever you press a key on the keyboard or move the mouse. This category is intended for technical support purposes.

Using Applications Published on MetaFrame for UNIX

For connections to applications published on a MetaFrame for UNIX server, two additional utilities provide functionality for configuring session display and cutting and pasting objects between the ICA session and the client device. This section describes how to use these utilities.

Using the Window Manager

If you are connecting to an application published on a MetaFrame for UNIX server, use the Citrix window manager to minimize, resize, position, and close windows, and access seamless “full screen” mode. This section describes how to use the window manager.

About Seamless Windows

Seamless windows are ICA Client session windows containing published applications that are configured to run in seamless mode. In seamless mode, applications running on the MetaFrame server appear to the client as if they are running locally, and each application appears in its own resizable window.

You can also display seamless windows in “full screen” mode, which places the published application in a full-screen sized desktop. This mode lets you access the `ctxwm` menu system.

Accessing Seamless “Full Screen” Mode

- **To switch between seamless and seamless “full screen” modes**






Press SHIFT and F2.

Minimizing, Resizing, Positioning and Closing Windows

When you connect to a published application on a MetaFrame server, buttons to minimize, resize, position, and close windows are provided by the ctxwm window manager.

- **To minimize, resize, position and close window**

Use the left mouse button to click on the following buttons:

To	Click	Note
Minimize published application windows on your desktop		Seamless windows are minimized as buttons on the desktop's taskbar. Non-seamless and seamless “full screen” windows are minimized as icons on the desktop.
Open a minimized window		Click its button on the taskbar or its icon on the desktop
Adjust the size of published application windows		Click and hold down the mouse button, then move the pointer to the edge of the window and drag it in the direction you want to scale it. The window dimensions are displayed in the top left-hand corner. Release the mouse button to apply the resizing. To resize the window proportionately, move the mouse pointer to a corner of the window and drag it.
Re-position published application windows		Click and hold down the mouse button, drag the window to the required position on the desktop, and release the mouse button.
Close and exit a published application		When you close the last application in a session, after 20 seconds the session disconnects automatically.

Using the Citrix Window Manager Menus

In remote desktop and seamless “full screen” windows, you can use the ctxwm menu system to log off, disconnect, and exit from published applications and connection sessions.

➤ To access the ctxwm menu system

1. On a blank area of the remote desktop window, click and hold down the left mouse button. The ctxwm menu is displayed.
2. Drag the mouse pointer over **Shutdown** to display the shutdown options.

➤ To choose an option from the ctxwm menu

Drag the pointer over the required option to highlight it. Release the mouse button to select the option.

To	Choose
Terminate the connection and all running applications	Logoff
Disconnect the session but leave the application running	Disconnect
Disconnect the session and terminate the application	Exit

Note Your Citrix server may be configured to terminate any applications that are running if a session is disconnected.

Cutting and Pasting Graphics Using ctxgrab and ctxcapture

If you are connected to an application published on a MetaFrame for UNIX server, use ctxgrab or ctxcapture to cut and paste graphics between the ICA session and the local desktop. These utilities are configured and deployed from the MetaFrame for UNIX server.

Using ctxgrab

The ctxgrab utility is a simple tool you can use to cut and paste graphics from ICA applications to applications running locally on the client device. This utility is available from the command prompt or, if you are using a published application, from the ctxwm window manager.

- **To access the ctxgrab utility from the window manager**
 1. In seamless mode, right click the **ctxgrab** button in the top, left-hand corner of the screen to display a menu and choose the **screengrab** option.
In full screen mode, left click to display the ctxwm menu and choose the **screengrab** option.
 2. When ctxgrab is started, a dialog box is displayed.
- **To copy from an application in an ICA Client window to a local application**
 1. From the **ctxgrab** dialog box, click **From screen**.
 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, cancel the selection by clicking the right mouse button before releasing the first button.
 3. Use the appropriate command in the local application to paste the object.

Using ctxcapture

The ctxcapture utility is a more fully-featured utility for cutting and pasting graphics between ICA applications and applications running on the client device.

With ctxcapture you can:

- Grab dialogs or screen areas and copy them between an application in an ICA Client window and an application running on the local client device, including non-ICCCM-compliant applications.
- Copy graphics between the ICA Client and the X graphics manipulation utility xvf.

If you are connected to a published desktop, ctxcapture is available from the command prompt. If you are connected to a published application and the Citrix server administrator has made it available, you can access ctxcapture through the ctxwm window manager.

- **To access the ctxcapture utility from the window manager**
 1. Left click to display the **ctxwm** menu and choose the **screengrab** option.
 2. When ctxcapture is started, a dialog box is displayed.

- **To copy from a local application to an application in an ICA Client window**
 1. From the **ctxcapture** dialog box, click **From screen**.
 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, cancel the selection by clicking the right mouse button before releasing the first button.
 3. From the **ctxcapture** dialog box, click **To ICA**. The **xcapture** button changes color to indicate that it is processing the information.
 4. When the transfer is complete, use the appropriate command in the local application to paste the information.
- **To copy from an application in an ICA Client window to a local application**
 1. From the application in the ICA Client window, copy the graphic.
 2. From the **ctxcapture** dialog box, click **From ICA**.
 3. When the transfer is complete, use the appropriate command in the local application to paste the information.
- **To copy from xv to an application in an ICA Client window or local application**
 1. From xv, copy the graphic.
 2. From the **ctxcapture** dialog box, click **From xv** and **To ICA**.
 3. When the transfer is complete, use the appropriate command in the ICA Client window to paste the information.
- **To copy from an application in an ICA Client window to xv**
 1. From the application in the ICA Client window, copy the graphic.
 2. From the **ctxcapture** dialog box, click **From ICA** and **To xv**.
When the transfer is complete, use the paste command in xv.

Index

A

- Adding and Removing Citrix ICA Clients 21
- Adding application sets 39
- Adding custom ICA connections 39
- application publishing
 - using the window manager 49
- application set 39
- authentication 10
- Auto Client Update 16

C

- Changing the Properties of a Citrix ICA Client in the Database 23
- Citrix ICA Client Update Process 17
- Citrix on the World Wide Web 3
- Client Auto Update
 - configuring the MetaFrame server 17
- Configuring bitmap Caching for Application Sets 46
- Configuring Connection Properties for Application Sets 40
- Configuring Connections to Citrix Servers and Published Applications 36
- Configuring Default Options for Application Sets 40
- Configuring Event Logging for Application Sets 48
- Configuring General Settings for Application Sets 45
- Configuring Hotkeys for Application Sets 47
- Configuring the Citrix ICA Win32 Client 25
- Configuring the Client update database 18
- Configuring the Properties of the Client Update Database 20
- Connection Types 32
- Conventions 2
- Creating a New Client Update Database 18
- Creating Client Installation Diskettes 12
- ctxwm, window manager 49, 51
- custom ICA connection 39

D

- Deploying the Citrix ICA Win32 Client 11
- disable password saving 44

E

- event logging 48

F

- Finding Further Information 2
- firewalls 33
- full screen seamless mode 49

H

- How to Use this Guide 1

I

- Installation Methods 12
- Installing the Citrix ICA Win32 Client 13

L

- local text echo 42
- login information 43

M

- Mapping Client Audio 31
- Mapping Client COM Ports 30
- Mapping Client Devices 25
- Mapping Client Drives 27
- Mapping Client Printers 28
- mouse click feedback 42

P

- pass-through authentication 46
- password 43
- Preventing password saving 43
- publishing applications
 - using the window manager 49

R

- remote desktop windows 49

S

Save password 43
seamless windows 49
Setting a Default Database 19
SOCKS proxy connection, configuring 33
Starting the Win32 Client 16
System Requirements 11

T

TCP/IP server location 38
Turning Off Client Device Mappings 26

U

Use local username and password 43
Using Application Sets 39

W

Who Should Use this Manual 1
window manager, published applications 49
windows
 remote desktop 49
 seamless 49