Administrator's Guide

Citrix ICA Win32 Clients

Version 6.20

Citrix Systems, Inc.

Document Code ica32.6.2.acr

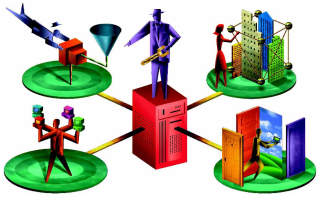
Contents

Chapter 6 Configuring Features Common to the ICA Win32 Clients

Chapter 7 Implementing Security Measures for the ICA Win32 Clients

CHAPTER 1

Before You Begin



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

- The Citrix server to which your ICA Clients connect
- The operating system on the client device (Windows 9x, Windows NT, Windows 2000, Windows Me, or Windows XP)
- 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 Win32 Clients 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, "Before You Begin"	Gives an overview of the documentation.
Chapter 2, "Introduction to the Citrix ICA Win32 Clients"	Gives a detailed list of new and existing features; includes a discussion of deployment methods.
Chapter 3, "Installing and Configuring the ICA Win32 Program Neighborhood Client"	Includes instructions for installing, configuring, and running the ICA Win32 Program Neighborhood Client.
Chapter 4, "Installing and Configuring the ICA Win32 Program Neighborhood Agent"	Includes instructions for installing, configuring, and running the ICA Win32 Program Neighborhood Agent.

Chapter	Contents
Chapter 5, "Installing and Configuring the ICA Win32 Web Client"	Includes instructions for installing, configuring, and running the ICA Win32 Web Client.
Chapter 6, "Configuring Features Common to the ICA Win32 Clients"	Includes instructions for configuring new and existing features common to all of the ICA Win32 Clients, including the Client Auto Update feature.
Chapter 7, "Implementing Security Measures for the ICA Win32 Clients"	Includes information about using SOCKS to direct ICA traffic through firewalls and configuring the ICA Win32 Clients to use SSL encryption.

Document Conventions

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

Convention	Meaning
Boldface	Commands, names of interface items such as text boxes and option buttons, and user input.
Italics	Placeholders for information or parameters that you provide. For example, *filename* in a procedure means you type the actual name of a file. Italics also are used for new terms and the titles of books.
UPPERCASE	Keyboard keys, such as CTRL for the Control key and F2 for the function key that is labeled F2.
`Monospace`	Text displayed at a command prompt or in a text file.
%SystemRoot%	The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or other name specified when Windows is installed.
{ braces }	A series of items, one of which is required in command statements. For example, **{ yes | no }** means you must type **yes** or **no**. Do not type the braces themselves.
[brackets]	Optional items in command statements. For example, [**/ping**] means that you can type **/ping** with the command. Do not type the brackets themselves.
| (vertical bar)	A separator between items in braces or brackets in command statements. For example, **{ /hold | /release | /delete }** means you type **/hold** or **/release** or **/delete**.
… (ellipsis)	You can repeat the previous item or items in command statements. For example, **/route:***devicename*[,…] means you can type additional *devicenames* separated by commas.
▶	Step-by-step procedural instructions.

The Citrix ICA Clients allow users to connect to Citrix servers. When describing a feature or procedure common to all types of MetaFrame XP, 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 ICA Win32 Clients. For additional information, consult 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
- The *Configuration Guide for the ICA Win32 Clients*, available from the Citrix Web site
- The documentation included in your Citrix server package for instructions about installing, configuring, and maintaining your Citrix servers

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 disc
- http://www.citrix.com/download; click the ICA Client platform for which you want information
- http://www.citrix.com/support; click Product Documentation and choose ICA Client

Using the Adobe Acrobat Reader, you can view and search the documentation electronically or print it for easy reference. You can download the Adobe Acrobat Reader for free from the Adobe Web site at http://www.adobe.com.

Important Always consult the Readme files for your Citrix server and the Citrix ICA Client for any last-minute updates, installation instructions, and corrections to the documentation.

Citrix on the World Wide Web

The Citrix Web site, at http://www.citrix.com, offers a variety of information and services for Citrix customers and users. From the Citrix home page, you can access Citrix online Technical Support Services and other information designed to assist MetaFrame administrators, including the following:

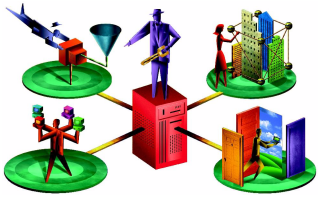
- Downloadable Citrix ICA Clients (at http://www.citrix.com/download)
- Citrix Product Documentation Library, containing the latest documentation for all Citrix products (at http://www.citrix.com/support, select Product Documentation). You can download updated editions of the documentation that ships with Citrix products and supplemental documentation that may only be available from the Citrix Web site.
- Program information about Citrix Preferred Support Services options
- An FTP server containing the latest service packs, hotfixes, utilities, and product literature for download
- An online Solution Knowledge Base containing an extensive collection of application notes, technical articles, troubleshooting tips, and white papers
- Interactive online Solution Forums for discussion of technical issues with other users
- Frequently Asked Questions pages with answers to common technical and troubleshooting questions
- Information about programs and courseware for Citrix training and certifications
- Contact information for Citrix headquarters, including worldwide, European, Asia Pacific, and Japan headquarters
- The Citrix Developer Network (CDN) at http://www.citrix.com/cdn. This open enrollment membership program provides access to developer tool kits, 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.

Reader Comments

We strive to provide accurate, clear, complete, and usable documentation for Citrix products. If you have any comments, corrections, or suggestions for improving our documentation, we want to hear from you.

You can send e-mail to the documentation authors at documentation@citrix.com. Please include the product name and version number, and the title of the document in your message.

CHAPTER 2



Introducing the Citrix ICA Win32 Clients

This chapter introduces the Citrix ICA Win32 Clients. The concepts in this chapter can help you decide which ICA Win32 Clients to use in your computing environment and how to deploy them.

The following topics are covered:

- Overview of the ICA Win32 Clients
- New in this Release
- ICA Win32 Client Features
- Deploying the ICA Win32 Clients

Overview of the ICA Win32 Clients

To choose which ICA Win32 Client or Clients to deploy in your enterprise, decide how your end users will access published applications. If you are using MetaFrame XP in conjunction with Citrix NFuse, you can deliver application sets to users in two ways.

You can use the **ICA Win32 Web Client** with NFuse to publish links to applications into a Web page on your corporate Intranet or the Internet. Users run a standard Web browser to access the Web page that contains the links to their applications. The Web Client includes the engine needed to launch published applications.

For information about installing, configuring, and using the Web Client, see “Installing and Configuring the ICA Win32 Web Client” on page 69.

You can also use the **ICA Win32 Program Neighborhood Agent** with NFuse to “push” links to applications directly to users’ Windows desktops. Because users do not run a Web browser to view a Web page, accessing remote applications is just like accessing local applications.

All client configuration is done at the server level in an XML file. Users connect to the XML file using HTTP or HTTPS to retrieve configuration, enumeration, and launch information. Because the Program Neighborhood Agent uses HTTP to pass the XML data, it is easy to use it with a firewall.

For information about installing, configuring, and using the Program Neighborhood Agent, see "Installing and Configuring the ICA Win32 Program Neighborhood Agent" on page 55 of this guide, and chapter 6 of the *NFuse 1.6 Administrator's Guide*.

If you do not want to deliver applications using NFuse, publish the applications for direct access. To directly access applications published on MetaFrame XP servers, users launch the **ICA Win32 Program Neighborhood Client** to browse for application sets or create custom ICA connections to Citrix servers or published applications.

For information about installing, configuring, and using the Program Neighborhood Client, see "Installing and Configuring the ICA Win32 Program Neighborhood Client" on page 25.

New in this Release

The following new features are supported in Version 6.20 of the ICA Win32 Clients.

For information about enabling and configuring the following new features on MetaFrame XP servers, see the *MetaFrame XP Administrator's Guide* delivered with Feature Release 1 of MetaFrame XP Version 1.0.

Important Features that are marked with this symbol require the MetaFrame XP server to be licensed for Feature Release 1. Features that are not so marked require that Service Pack 1 for MetaFrame XP be installed.

For detailed instructions for enabling and configuring these features on Version 6.20 of the ICA Win32 Clients, see "Configuring Features Common to the ICA Win32 Clients" on page 77 or the chapter on the specific ICA Win32 Client you plan to deploy.

In addition to support for new features, Version 6.20 of the ICA Win32 Clients includes performance enhancements in the following areas:

- ICA display
- Client printer management

Citrix Program Neighborhood Agent

With Citrix Program Neighborhood Agent you can now push links to remote applications directly to your users' Windows desktops. Users are not required to open additional software, such as a Web browser, to launch applications published on MetaFrame XP servers.

With the Program Neighborhood Agent, you place links to NFuse-enabled published applications in the user's Start menu, on the Windows desktop, or in the Windows System Tray. You can integrate remote applications into the Windows desktop so that they appear as locally accessed applications to the user.

You configure Program Neighborhood Agent settings on the NFuse server, allowing you to control connections and application sets from a central location. XML data is passed between the Program Neighborhood Agent and the NFuse server using HTTP or HTTPS and can pass through firewalls using port 80.

The Program Neighborhood Agent supports the following:

- Automatically refreshing application icons
- Pass-through authentication
- Secure Sockets Layer

For information about installing and using the Program Neighborhood Agent, see "Installing and Configuring the ICA Win32 Program Neighborhood Agent" on page 55.

For information about working with the configuration file on the NFuse server, see Chapter 6 of the *NFuse 1.6 Administrator's Guide*.

Secure Sockets Layer Support for ICA

Citrix SSL Relay provides the ability to secure data communications using the Secure Sockets Layer (SSL) protocol. SSL is the security standard for communication across the Internet.

SSL provides server authentication, encryption of the data stream, and message integrity checks. You can now use Citrix SSL Relay to secure communications between an SSL-enabled ICA Win32 Client and a MetaFrame server. Citrix SSL Relay uses Version 3.0 of SSL.

Universal Print Driver Support

The Citrix Universal Print Driver is a standard Windows 2000 or Windows NT print driver that encapsulates print jobs in PCL4 format. A client-based interpreter renders the print job using the client machine's local print driver and printing services. The Universal Print Driver renders print jobs in monochrome at up to 300 dots per inch on a standard set of forms.

Using the Universal Print Driver results in smaller print jobs, which can have a significant impact on printing over WAN or dial-up connections.

Note If the MetaFrame server is configured to automatically create both native driver and Universal Print Driver printers on the client machine, the user must explicitly select a printer to process print jobs. If the print job requires color or advanced printing options such as duplex printing, the user must select the standard printer, which uses the printer's native driver.

Auto Client Reconnect

ICA sessions can be dropped because of unreliable networks, highly variable network latency, or range limitations of wireless devices.

The *auto client reconnect* feature is triggered when the ICA Client detects a disconnected session. When this feature is enabled on a MetaFrame XP server, users do not have to reconnect manually or reenter logon credentials to continue working. Automatic reconnection does not occur if users exit applications without logging off.

Windows Installer Packages for ICA Win32 Clients

The ICA Win32 full Program Neighborhood Client and the Program Neighborhood Agent are now available in Microsoft Windows installer packages (.Msi files), so you can use Windows Installer technology to deploy and install them.

You can distribute the ICA Win32 Client installer package files to users using Microsoft's Systems Management Server or Active Directory.

Published Content Support

Citrix administrators can now "push" content files, including documents, Web pages, video presentations, and sound files, to users. You publish content files on the MetaFrame XP server in the same manner as applications.

Users view or play the published content files with a content viewer or player stored locally on the client device.

Novell Directory Services Support

When users launch ICA Win32 Client software, they can log on and be authenticated using their NDS credentials. Supported NDS credentials are user name (or distinguished name), password, directory tree, and context.

NDS support is integrated into the following:

- Program Neighborhood and Program Neighborhood Agent – If NDS is enabled in the MetaFrame XP farm, NDS users enter their credentials on an NDS tab on the ICA Client logon screen. If users have the Novell Client (Version 4.8) installed, they can browse the NDS tree to choose their context. See chapter 6 of the *NFuse 1.6 Administrator's Guide* for information about configuring the Program Neighborhood Agent for NDS.
- Pass-Through Authentication – If users have the Novell Client (Version 4.8) installed, you can pass their credentials to the MetaFrame XP server, eliminating the need for multiple system and application authentications. To enable pass-through authentication, configure the following policy options in the User Package in ZENworks for Desktops:
  1. Enable the Dynamic Local User policy option.
  2. Set the "Use NetWare Credentials" value to **On.**
- Custom ICA Connections – When users run the Add New ICA Connection wizard, they must enter a distinguished name in the user name field and a password in the password field. Users must leave the domain field blank.
- NFuse Version 1.6 – NDS users enter their credentials on an NFuse NDS logon screen. See chapter 3 of the *NFuse 1.6 Administrator's Guide* for information about how to configure NFuse for NDS.

Note To use NDS logon information with earlier versions of ICA Win32 Clients, enter the NDS tree name in the **Domain** field and a distinguished name in the **User** field on the ICA Win32 Client logon screen.

DNS Name Resolution

You can configure ICA Win32 Clients that use the XML Service to connect to the MetaFrame farm to request a Domain Name System (DNS) name instead of a server's IP address.

Extended Parameter Passing

With extended parameter passing you can associate a file type on a client device with an application published on a Citrix server. When a user double-clicks a locally-saved file, the file is opened in the application associated with it on the MetaFrame XP server.

ICA Win32 Client Features

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 device. You can map the client device to access the following local components when running a remote application:

- Client drives
- Client printers
- Client COM ports

Client Drive Mapping

Client drive mapping allows drive letters on the Citrix server to be redirected to drives that exist on the client device; for example, drive H in a Citrix user session can be mapped to drive C on the local device running the Citrix ICA Client. These mappings are used by the File Manager or Windows 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 device. You can browse for an connect to client printers 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 device as if it were connected to the Citrix server.

Sound Support

ICA Client sound support allows a client device with a compatible sound card to play sound files on the server and present them on the local client device's sound system. Client devices can play 8- or 16-bit mono or stereo Windows Wav files at 8, 11.025, 22.05, and 44.1KHz. You can configure audio support 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.

Per-User Time Zone Support

This MetaFrame XP feature allows the user, when logging on to a Citrix server in a different time zone, to have the ICA session reflect the time zone of the client device.

For example: A user in Los Angeles, which is in the Pacific time zone, logs onto a Citrix server in New York City, which is in the Eastern time zone, and launches Microsoft Outlook as a published application. Microsoft Outlook stamps e-mails sent during this ICA session with the user's Pacific time zone information.

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 device. Users need not manage separate modem entries for their local communications programs.

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

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 device. 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

Note If you use the Windows installer packages to deploy and install the ICA Win32 Program Neighborhood Client or the Program Neighborhood Agent, you cannot use Client Auto Update to update previous versions of the ICA Win32 Client.

Windows Clipboard Integration

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

Low Bandwidth Requirements

The 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 device.

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 is not available when connecting to MetaFrame for UNIX 1.0 and 1.1 servers. The elements of SpeedScreen Latency Reduction are:

Local Text Echo

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

Mouse–Click Feedback

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

Business Recovery

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

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

TCP/IP+HTTP Server Location

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

Configuring the ICA Win32 Clients to use the TCP/IP+HTTP network protocol has several advantages for most server farms:

- The protocol uses XML data encapsulated in HTTP packets and uses TCP port 80 by default. Most firewalls are set to allow the HTTP packets to pass on port 80.
- The protocol does not rely on UDP or broadcasts to locate servers in the server farm.
- The Citrix XML service works in a server farm that contains MetaFrame XP servers alone or in combination with Citrix NFuse, which allows users to connect to application portals with their Web browsers.

Routers pass TCP/IP packets between subnets, allowing client devices to locate servers that are not on the same subnet

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 MetaFrame XP 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. Multiple-monitor support is available only when connecting to MetaFrame 1.8 Feature Release 1 and MetaFrame XP servers.

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 that of your local client desktop. Scaling provides controls that enable you to shrink an ICA session image to fit your desktop.

Note A Win32 Client session window can be reduced to a minimum of 64 pixels in width. However, the Windows operating system may enforce a different limit (greater than 64 pixels) based on the prevailing desktop scheme, which overrides the ICA Client scaling limit.

Deploying the ICA Win32 Clients

You can deliver the ICA Clients to your users and install the software with the following methods:

- Using Microsoft Systems Management Server (SMS) or Active Directory Services in Windows 2000
- Creating an ICA Client download Web site on a Web server
- Copying the ICA Win32 files to a network share point
- Creating installation disks
- Using the ICA Client CD-ROM disc

For a detailed discussion of the latest deployment methods available, see chapter 9 of the *MetaFrame XP Administrator's Guide*. If you are using Citrix NFuse in conjunction with Citrix MetaFrame, see the *NFuse Administrator's Guide* for information about deploying the ICA Clients with Citrix NFuse.

Using Microsoft Systems Management Server or Active Directory Services

The ICA Win32 full Program Neighborhood Client and the Program Neighborhood Agent are both available in Microsoft Windows installer packages (.Msi files), so you can use Windows Installer technology to deploy and install them. You can distribute the ICA Win32 Client installer package files to users using Microsoft Systems Management Server (SMS) or Active Directory Services in Windows 2000.

See your Windows 2000 or Systems Management Server documentation for more information.

The ICA Win32 installer package files are located in the following directories (substitute *language* with the language of the ICA Client software) on the ICA Client CD included in the MetaFrame XP, Feature Release 1 media pack:

Icaweb*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

The installer package for the Program Neighborhood Agent is also located in the directory:

Icainst*language*\ica32\pnagent

Note The Windows Installer service is present by default on computers running the Windows 2000 operating system. If the computer is running Windows NT 4.0 or Windows 9x, you must install Windows Installer Version 1.1 or higher.

Creating an ICA Client Download Web Site on a Web Server

If you are not using Citrix NFuse, Citrix offers an installation method that uses a Web browser on the client device as the interface for downloading the ICA Client. You can create an ICA Client download Web site on a Web server. Users access a setup page containing a link to the ICA Win32 Client setup program.

You can download the elements required to create an ICA Client download Web site and the corresponding documentation from the Citrix Web site at http://www.citrix.com/download, or you can get the required files from the ICA Client CD and the NFuse CD. See chapter 9 of the *MetaFrame XP Administrator's Guide* for more information about using these discs to create an ICA Client download Web site.

Deploying ICA Clients Over a Network

To deploy the ICA Win32 Client software over a network, follow the instructions below.

To deploy ICA Win32 Client software from a network share point

1. Create a share point on a file server that is accessible to your users.
2. Copy the desired ICA Win32 Client executable (ica32.exe for the Program Neighborhood Client; ica32a.exe for the Program Neighborhood Agent; or ica32t.exe for the Web Client) from the ICA Client CD to the share point. These executables are located in the following directory (substitute *language* with the language of your server software):

   Icaweb*language*\ica32

   where *language* is one of:

   - En (English)
   - Fr (French)
   - De (German)
   - Ja (Japanese)
   - Es (Spanish)
3. Supply your users with the path to the executable.
4. Users double-click the executable to begin the installation process.

Creating Client Installation Disks

Use the ICA Client Creator to create client installation disks for the ICA Win32 Program Neighborhood Client. You will need three to four 3.5-inch floppy disks to create the client installation disks.

To create Citrix ICA Client installation disks

1. From a MetaFrame XP server: Click **Start**> **Programs**> **Citrix> MetaFrame XP**> **ICA Client Creator**. The **Make Installation Disk Set** dialog box appears.

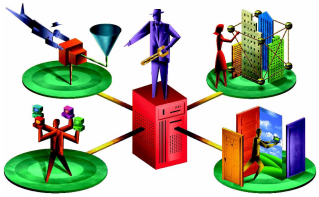
   From a MetaFrame 1.8 server: Click **Start**> **Programs**> **MetaFrame Tools**> **ICA Client Creator**. The **Make Installation Disk Set** dialog box appears.

   From a *WINFRAME* server: In the **Administrative Tools** folder, double-click **ICA Client Creator**. The **Make Installation Disk Set** dialog box appears.
2. 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**.
3. Follow the on-screen instructions.

Using the ICA Client CD-ROM Disc

The ICA Client CD-ROM disc contains setup and installation files for all ICA Clients. You can use the ICA Client CD to directly install ICA Client software on client devices that have CD-ROM drives, or copy the CD image to a network share point on a file server.

CHAPTER 3



Installing and Configuring the ICA Win32 Program Neighborhood Client

This chapter explains how to install and configure the ICA Win32 Program Neighborhood Client. The following topics are covered:

- Overview of the ICA Win32 Program Neighborhood Client
- System Requirements
- Preconfiguring the ICA Win32 Program Neighborhood Client
- Installing the ICA Win32 Program Neighborhood Client
- Starting the ICA Win32 Program Neighborhood Client
- Configuring the ICA Win32 Program Neighborhood Client

Overview of the ICA Win32 Program Neighborhood Client

Use the ICA Win32 Program Neighborhood Client if your users directly access applications published on Citrix servers. With the Program Neighborhood Client, users open the Program Neighborhood user interface to browse for application sets or create custom ICA connections to Citrix servers or published applications.

This ICA Win32 Client can also be used with NFuse and to launch or run applications embedded in a Web browser. If you are planning to use Citrix NFuse, and have not yet deployed the ICA Win32 Client to your users, use the ICA Win32 Program Neighborhood Agent or the ICA Win32 Web Client.

Use the Program Neighborhood Agent to allow users access to published applications from links placed directly on the Windows desktop. Program Neighborhood Agent includes online Help.

Use the Web Client if you want your users to access applications using a Web browser. The ICA Win32 Web Client does not include the Program Neighborhood user interface or online Help files, and is therefore smaller in size and easier to download from a Web page.

The ICA Win32 Program Neighborhood Client provides the following features:

- Program Neighborhood user interface
- SSL support for ICA
- Auto Client Reconnect
- Published content support
- Novell Directory Services support
- DNS name resolution support
- Extended parameter passing
- 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
- Per-user time zone support

System Requirements

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

- Standard PC architecture, 80386 processor or greater as required for the operating system
- Windows 9x, Windows 2000, Windows Me, Windows XP, 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, 32MB or greater for Windows 2000 and Windows Me, and 128MB RAM or greater for Windows XP
- If you are using the ICA Win32 Program Neighborhood Client with a Web browser, the client device must run a standard Web browser; Internet Explorer Version 4.0 or greater, or Netscape Navigator or Communicator Version 4.0 or greater
- Microsoft mouse or 100% compatible pointing device
- VGA or SVGA video adapter with color monitor
- High-density 3.5-inch disk drive (optional) and available hard disk space
- Windows-compatible sound card for sound support (optional)
- For serial (dial-up) 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 connection methods and network transports are:
  - TCP/IP+HTTP
  - SSL+HTTPS
  - TCP/IP
  - NetBIOS
  - IPX
  - SPX

  For information about configuring the ICA Win32 Clients to use SSL to secure communications, see “Using SSL to Encrypt ICA Traffic” on page 113.

Preconfiguring the ICA Win32 Program Neighborhood Client

You can configure numerous settings before you deploy the ICA Win32 Client software to your users. Doing so allows users to install the ICA Client software and begin using it immediately, without having to configure settings.

You can customize many ICA Win32 Client settings, including default application sets, server location, screen display resolution, and encryption level, among others. General instructions for preconfiguring the client are included below. For definitions of parameters in the ICA Win32 Client .Ini files, see the *Configuration Guide for the ICA Win32 Clients* on the Citrix Web site at http://www.citrix.com/support; select **Product Documentation**.

Important You can use any standard compression utility to extract the client files from the packaged executable. However, you must use commercially available software to repackage the client files for distribution to your users.

When the ICA Win32 Program Neighborhood Client is installed on a client device, several of the .Ini files you can modify are copied to the user's profile directory. If you modify settings for a new version of the ICA Win32 Program Neighborhood Client prior to updating with the Client Auto Update feature, your changes are not migrated to the .Ini files under the user's profile directory.

▸ To preconfigure settings for the ICA Win32 Program Neighborhood Client

1. Extract the client file set from ica32.exe, using your preferred compression utility software. These files are located in the following directory (substitute *language* with the language of your server software):

   Icaweb*language*\ica32

   where *language* is one of:

   - En (English)
   - Fr (French)
   - De (German)
   - Ja (Japanese)
   - Es (Spanish)

2. Open the files containing the customizable settings in a text editor. These files are:

   Appsrv.src

   Module.src

   Pn.src

   Wfclient.src

3. Change the parameters to reflect your desired settings.
4. Repackage the client files for distribution to your users.

Installing the ICA Win32 Program Neighborhood Client

You can install the ICA Win32 Program Neighborhood Client with one of the following packages:

- Ica32.msi – a Windows Installer package for use with Windows 2000 Active Directory Services or Microsoft Systems Management Server, approximately 5.2MB in size
- Ica32.exe – a self-extracting executable, approximately 3.7MB in size

---

Note For a discussion of methods for deploying ICA Win32 Client software to users, see "Deploying the ICA Win32 Clients" on page 21 of this guide, and chapter 9 of the *MetaFrame XP Administrator's Guide* delivered with Feature Release 1 of MetaFrame XP 1.0.

Installing the ICA Win32 Program Neighborhood Client with the Windows Installer Packages

The ICA Win32 Program Neighborhood Client is available in a Windows installer package file (ica32.msi). You can distribute the Program Neighborhood Client installer package to your users with Microsoft Systems Management Server or Windows 2000 Active Directory Services.

This package is located in the following directories (substitute *language* with the language of the ICA Client software) on the ICA Client CD included in the MetaFrame XP, Feature Release 1 media pack:

Icaweb*language*\ica32

Icainst*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

Note The Windows Installer service is present by default on computers running the Windows 2000 operating system. If the computer is running Windows NT 4.0 or Windows 9x, you must install Windows Installer Version 1.1 or higher.

To uninstall the ICA Win32 client installed using an installer package, you can either use **Add/Remove Programs** in the Control Panel or you can run the same installer package again.

Updating Previous Versions of the Program Neighborhood Client with the Installer Package

You cannot automatically update previous versions of the ICA Win32 Program Neighborhood Client installed with Windows Installer (.msi) packages. You must redeploy an ICA Win32 Client installer package when a new version of the ICA Client is released.

Configuring the Installer Package for Silent User Installation

You can configure the Program Neighborhood Client installer package for "silent" user installation. Windows Installer informs the user when the ICA Win32 Client software is successfully installed. You must clear the Windows Installer message box.

To configure the Program Neighborhood Client installer package for silent user installation

1. Enter the command line

   msiexec /I <MSI_Package> /qn+ [Key=Value]…

   where <MSI_Package> is the name of the installer package.

2. You can set the following keys:

   INSTALLDIR=<Installation_Path>, where <Installation_Path> is the path to the directory where the ICA Client software is installed. By default, the ICA Client software is installed in the Program Files\Citrix\ICA Client directory.

   CLIENT_UPGRADE=**Yes** or **No**. The default value is **Yes**.

   PROGRAM_FOLDER_NAME=<Start Menu Program Folder Name>, where <Start Menu Program Folder Name> is the name of the Programs folder on the Start menu containing the shortcut to the ICA Client software. The default value is **Citrix ICA Client**.

   ENABLE_SSON=**Yes** or **No**. The default value is **No**. If you enable the SSON property, set the ALLOW_REBOOT property to No to avoid automatic rebooting of the client system.

   ALLOW_REBOOT=**Yes** or **No**. The default value is **Yes**.

Installing the ICA Win32 Program Neighborhood Client with the Self-Extracting Executable

The ICA Win32 Program Neighborhood Client is available in a self-extracting executable (ica32.exe). You can distribute this self-extracting executable to your users for direct installation on client devices.

This executable is located in the following directory (substitute *language* with the language of the ICA Client software) on the ICA Client CD included in the MetaFrame XP, Feature Release 1 media pack:

Icaweb*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

▸ To install the Program Neighborhood Client with the self-extracting executable

1. Make sure the client device 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 of the task bar if it is active) are not running.
2. **If you are installing from disks:** Insert ICA Win32 Client Setup disk number 1 in drive A (or other appropriate drive) of the client device. For Windows 9x, Windows 2000, and Windows NT 4.0 client devices, click **Start** > **Run a:\setup**. For Windows NT 3.5x client devices, on the **File** pull-down menu of Program Manager run **a:\setup**.

   For information about creating ICA Client installation disks, see "Creating Client Installation Disks" on page 23.

   If you are installing from a Citrix server: run setup.exe, located in the following directory on your Citrix server:

   %SystemRoot%\System32\Clients\Ica\Ica32\Disks\Disk1

   If you are installing from the Citrix ICA Client CD: run ica32.exe, located in the following directory (substitute *language* with the language of your server software):

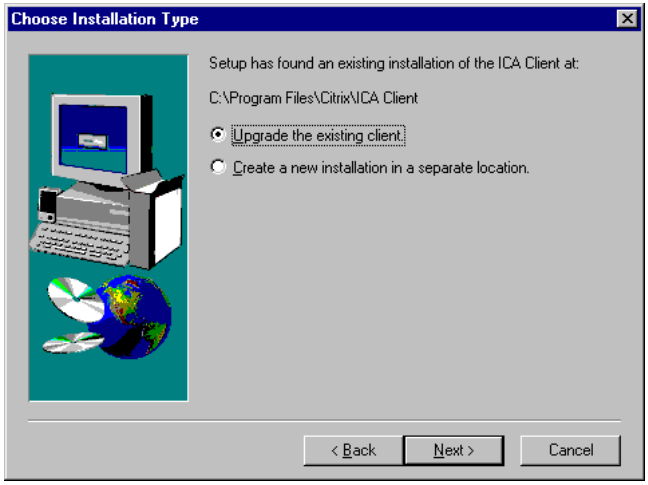
   Icaweb*language*\ica32

   where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

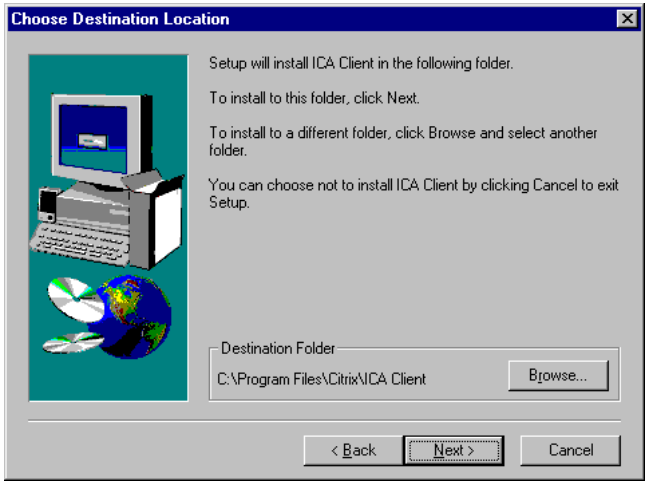
3. The **Welcome** screens appear. Read the information on these screens and click **Next**.
4. The Citrix License Agreement appears. Read the license agreement and click **Next** if you agree to the terms of the agreement.

   The installation program searches your client device for previously installed versions of the ICA Win32 Program Neighborhood Client. If an older version is detected, the screen shown in Step 6 appears. If no older version is detected, the screen shown in Step 7 appears.
5. The **Choose Installation Type** dialog box appears:



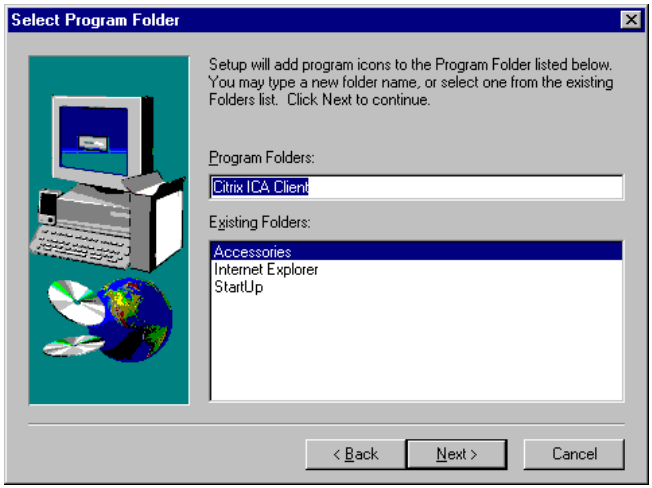
The **Choose Installation Type** dialog box lets you choose either to upgrade the existing client or create a new and separate installation of the ICA Win32 Client in a new location. The default value is **Upgrade the existing client**. Click **Next**.

6. The **Choose Destination Location** dialog box appears:



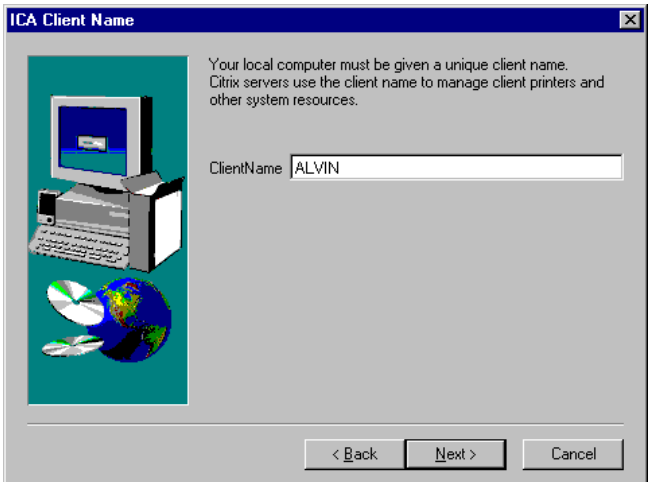
You can change the displayed path if desired by clicking **Browse**. Click **Next** to accept the displayed path and continue installation.

7. The **Select Program Folder** dialog box appears:



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** dialog box appears:



Specify a unique client name for your client device. Citrix servers use the client name to manage client printers and other system resources. If you do not assign a unique machine name to each client device, device mapping and application publishing may not operate correctly. Click **Next** to continue.

9. The **Select Desired Features** screen appears.

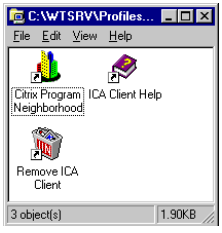
   Select **Yes** to enable the Program Neighborhood Client to access your local Windows user name, password, and domain information. You are not prompted to log on to the Program Neighborhood Client separately.

   A progress window appears, displaying the file names as they are copied to your hard drive.

10. If you are installing from disk, the **Setup Needs the Next Disk** dialog box appears. Remove the first ICA Win32 Client disk from drive A (or other appropriate drive) and insert the second disk. 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 the desktop:



Starting the ICA Win32 Program Neighborhood Client

Users run Program Neighborhood to access applications published on Citrix servers.

To start Program Neighborhood

1. Double-click the Program Neighborhood icon on the desktop to open the **Program Neighborhood** window.
2. If you specified a default application set for this user, this window contains all the applications the user can run. If no default is specified, a list of application sets appears. Select the application set to view and click **Open** from the **File** menu. A logon dialog box appears.
3. Enter a valid user name, domain, and password.

Configuring the ICA Win32 Program Neighborhood Client

This section explains how to configure the Program Neighborhood Client using the Program Neighborhood user interface.

Configuring Network Protocol and Server Location

With the Citrix ICA Win32 Program Neighborhood 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 device. This method uses a serial connection to a Citrix server (custom ICA connections using the Program Neighborhood Client only).
- Over a direct serial cable connection to a Citrix server. This method uses a serial connection to a Citrix server (custom ICA connections using the Program Neighborhood Client only).
- Over the local or wide-area network connection between the client device and the Citrix server. This method uses one of the following network protocols:
  - TCP/IP+HTTP
  - SSL+HTTPS
  - TCP/IP
  - 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 device 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

Specifying the Network Protocol for ICA Browsing

The network protocol setting allows you to control the way the ICA Client searches for Citrix servers and how it communicates with them.

The next section discusses the TCP/IP+HTTP, SSL+HTTPS, and TCP/IP protocols and their implementation in a Citrix server farm. For additional information about configuring MetaFrame XP server farms for ICA browsing, see the *MetaFrame XP Administrator's Guide*.

Using TCP/IP+HTTP Network Protocol for ICA Browsing

If **TCP/IP+HTTP** is specified as the network protocol, the client uses the HTTP protocol to search for Citrix servers. Select this protocol when using the ICA Client over the Internet or through a firewall or proxy server. Select SSL+HTTPS to use SSL-secured communications.

Using the TCP/IP+HTTP protocol for ICA browsing provides the following advantages for most server farms:

- TCP/IP+HTTP uses XML data encapsulated in HTTP packets, which the client sends to port 80 by default. Most firewalls are configured so port 80 is open for HTTP communication.
- TCP/IP+HTTP does not use UDP (User Datagram Protocol) or broadcasts to locate servers in the server farm.
- Routers pass TCP/IP packets between subnets, which allows ICA Clients to locate servers that are not on the same subnet.

If you elect to use TCP/IP+HTTP as the network protocol, specify servers to contact for ICA browsing by entering IP addresses or DNS names of Citrix servers in the **Address List** box in the Program Neighborhood Client.

When **TCP/IP+HTTP** is selected and you specify Citrix servers in the **Address List** box, the ICA Client communicates with the Citrix XML Service on a specified server for ICA browsing.

By default, if no server is specified, the client attempts to resolve the name "ica" to an IP address. This is indicated by the virtual server location "ica" in the **Address List** box. This feature allows the Domain Name System (DNS) or Windows Internet Naming Service (WINS) administrator to configure a host record that maps "ica" to a valid server IP address that can service XML requests from ICA Clients.

With TCP/IP+HTTP selected, Auto-Locate does not use a broadcast to determine the nearest farm server, but rather attempts to resolve the host name "ica" to a Citrix server. Therefore, if Auto-Locate functionality is desired, the TCP/IP+HTTP protocol does not increase network traffic with ICA Client broadcasts.

Tip You can configure the ICA Clients' DNS server to use round-robin DNS to map the name "ica" to a set of servers that can service the XML requests. Use this approach to avoid individually configuring server location addresses on ICA Clients.

To locate an XML Service, the ICA Client makes an HTTP connection to port 80 on the MetaFrame server. If the user is launching a published application, for example, the XML Service then sends to the client the address of a MetaFrame server that has the application published.

When you configure the ICA Client to use TCP/IP+HTTP, communication between the client and XML Service consists of XML-formatted data in HTTP packets.

Communicating with the Citrix XML Service

Citrix XML Service is installed by default on all MetaFrame XP servers. It is also installed with Feature Release 1 for MetaFrame 1.8.

When ICA Clients are configured to use TCP/IP+HTTP for ICA browsing, the XML Service communicates published application information to clients using HTTP protocol and XML data. The XML Service also communicates published application information to NFuse-enabled Web servers.

For example, when a user launches a published application in Program Neighborhood, the ICA Client sends a request for the application. The XML Service responds with the address of a MetaFrame server on which the application is published.

With Citrix NFuse, for example, a user connects to an NFuse Web page using a Web browser. The XML Service provides a list of available applications to the NFuse-enabled Web server. The Web server displays the available applications on the user's personalized application Web page.

Using SSL+HTTPS Network Protocol for ICA Browsing

If **SSL+HTTPS** is specified as the server location network protocol, the client uses the HTTPS protocol to search for a list of Citrix servers. The client communicates with the Citrix server using ICA with SSL (Secure Sockets Layer). SSL+HTTPS provides strong encryption of ICA traffic and Citrix server authentication. Select this option when using the ICA Client over the Internet or via a firewall or proxy server.

When you select SSL+HTTPS as the server location network protocol, you must enter the fully qualified domain name of the server hosting the digital certificate.

Note The TCP/IP+HTTP and SSL+HTTPS protocols can only be used with compatible Citrix servers. See the *MetaFrame Administrator's Guide* for Windows or Unix for information about configuring the MetaFrame server to use SSL.

For information about configuring the ICA Win32 Clients to use SSL to secure communications, see "Using SSL to Encrypt ICA Traffic" on page 113.

Using TCP/IP Network Protocol for ICA Browsing

If **TCP/IP** is specified as the server location network protocol, and **(Auto-Locate)** appears in the **Address List** box in the Program Neighborhood Client, ICA Clients send UDP broadcasts to the ICA Browser service on port 1604 to locate MetaFrame servers and published applications. Select this option if all of the Citrix servers and clients are located on the same network.

By default, MetaFrame XP server farms operating in native mode do not respond to ICA Clients that use UDP broadcasts for ICA browsing. Therefore, if clients are configured to use TCP/IP and to auto-locate servers, they will fail to locate MetaFrame XP servers or published applications in the server farm.

Because UDP broadcast packets do not traverse subnets, using broadcasts for ICA browsing works only if a server that responds to broadcasts is in the same subnet as the clients. When the ICA Client locates a server, it communicates using directed (not broadcast) UDP to port 1604.

Because of broadcast limitations, you might prefer to enter one or more IP addresses or DNS names of MetaFrame XP servers in the **Address List** box in the Program Neighborhood Client. You must do this if the ICA Client is not on the same subnet as a data collector.

Configuring Connections to Citrix Servers and Published Applications

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

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

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 or SSL+HTTPS server location. The ICA Win32 Program Neighborhood Client uses TCP/IP+HTTP as the default network protocol.

▸ **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." 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.

Configuring SSL+HTTPS Server Location

Secure Sockets Layer (SSL) encryption of ICA traffic provides server authentication, encryption of the data stream, and message integrity checks. SSL is the security standard for communications across the Internet.

If you have configured your MetaFrame servers to accept SSL-secured connections, you can enable SSL on the ICA Win32 Client.

To configure SSL+HTTPS server location

1. Select **SSL+HTTPS** from the **Network Protocol** drop-down list.
2. Click **Add** to display the **Add Server Location Address** box.
3. Enter the fully qualified domain name of the MetaFrame server with the digital server certificate and verify that port 80 is listed as the default port.
4. Click **OK**.

Important SSL+HTTPS server location retrieves information only on a per-server farm basis. To retrieve information from more than one server farm, you must configure SSL+HTTPS server location settings for each application set. For custom ICA connections, you must configure 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" on page 43. For more information about using SSL to secure client to server communication, see "Using SSL to Encrypt ICA Traffic" on page 113.

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.

When you choose TCP/IP as the network protocol, the default setting for server location is **(Auto-Locate)**. The auto-locate function works as follows:

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

   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.

   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 and the first server to respond is the one to which you connect. The client broadcasts only if you select **(Auto-locate)** from the address list.

Using Application Sets and Custom ICA Connections

An *application set* is a user's view of the applications published on a given server farm that the user is authorized to access. Applications published in an application set are preconfigured for such session properties as window size and colors and supported level of encryption and audio. 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 device 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 user-defined shortcut to a published application or MetaFrame server. While you can create custom ICA connections to connect to any MetaFrame server or published application, you must use custom ICA connections to connect to:

- An existing Citrix server outside of a server farm scope of management
- An application published prior to the installation of a MetaFrame 1.8 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. 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 you want to configure and click the **Properties** button in the Program Neighborhood toolbar to display the **Properties** dialog box.
3. 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 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 to run the published application.
4. For more information about the options on this tab, click **Help**.

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 Connections Settings**.
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.

4. 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 device 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 device. 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, MetaFrame 1.8 Feature Release 1, and MetaFrame XP.

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 Properties. Specify the number of colors displayed in the application's window in the **Windows Colors** field.

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, deselect this check box and choose new settings.

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

Specify the window size that a published application runs in the **Window Size** field.

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.

Configuring Login Properties

By default, users are required to enter their credentials each time they launch a published application or connect to a MetaFrame server desktop. You can configure Program Neighborhood to reduce the number of times users have to enter credentials using one of the following methods:

- Enabling pass-through authentication
- Caching credentials with application set or custom ICA connection information

You can enable pass-through authentication to pass the user's local Windows desktop credentials to the MetaFrame server. This eliminates the need for multiple authentications.

If you enable pass-through authentication, all existing application sets are automatically configured to use this logon method. However, existing custom ICA connections are automatically configured to have this logon method disabled. You must therefore enable pass-through authentication for each custom ICA connection you want to use this logon method.

Enabling pass-through authentication

To enable pass-through authentication, you must complete the following tasks:

1. Enable the feature at the machine level.
2. Enable the feature at the user level.

Note Because pass-through authentication is disabled by default for existing custom ICA connections, you must enable this feature for each custom connection you want to use this logon method.

Procedures for each of these tasks are outlined below.

▸ **To enable pass-through authentication at the machine level**

1. Log on as an administrator.
2. Start Program Neighborhood.
3. Go to **Tools** > **ICA Settings**.
4. Click the **General** tab and select the **Pass-Through Authentication** option.
5. Click **OK**.

When this feature is turned on at the machine level, each user can enable it at the user level in the following manner.

▸ **To enable pass-through authentication at the user level**

1. Log on as a user.
2. Start Program Neighborhood.
3. Go to **Tools** > **ICA Settings**.

4. Click the **General** tab and select the **Use local user name and password for logon** option.
5. Click **OK**.

Enabling pass-through authentication at the user level makes this the default configuration for all existing and new application sets. However, pass-through authentication is, by default, disabled for custom ICA connections. Follow the instructions below for enabling existing custom ICA connections to use this feature.

▸ **To enable pass-through authentication for existing custom ICA connections**

1. Start Program Neighborhood.
2. Select a custom ICA connection for which you want to enable pass-through authentication.
3. Click **Properties** on the Program Neighborhood toolbar.
4. Click the **Login Information** tab and deselect the **Don't use local user name and password** option.
5. Click **OK**.
6. Repeat Steps 1 through 5 for each ICA connection for which you want to enable pass-through authentication.

Note When creating a new custom ICA connection, enable pass-through authentication by selecting the **Use local user name and password** option in the Add New ICA Connection wizard.

Caching Credentials

Users can choose to cache their password with the application set or custom ICA connection information. If you want to prevent users from caching their password in clear text, see "Preventing Users From Saving Passwords" on page 48.

▸ **To cache credentials**

1. Select the application set or custom ICA connection for which you want to cache credentials.
2. For application sets, click the **Settings** button on the Program Neighborhood toolbar.

   For custom ICA connections, click the **Properties** button on the Program Neighborhood toolbar.
3. Click the **Login Information** tab.
4. Make sure the **Don't use local user name and password** option is selected.

5. Enter the user name and domain information.
6. Select the **Save password** option to enable the password field.
7. Enter the password.
8. Click **OK**. The credentials, including the password, are now cached.

If you want to prevent users from caching their password in clear text, see the section "Preventing Users From Saving Passwords" below.

Preventing Users From Saving Passwords

You can remove the **Save Password** check box from an application set's logon screen and from the **Login Information** tab of the **Settings** dialog box. Removing the check box prevents users from saving their password for application sets or custom ICA connections. You can prevent users from saving their passwords for all application sets or specific application sets.

Use the following table to determine which files you need to edit, then follow the instructions below.

To disable password saving for all application sets	To disable password saving for particular application sets
%User Profile%\Application Data\ICAClient\appsrv.ini	%User Profile%\Application Data\ICAClient\pn.ini

To prevent users from saving their password 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 individual's user-level Appsrv.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
3. Locate the section named [WFClient].
4. Add the following line 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. Repeat Steps 1 through 5 for additional users.
7. Start Program Neighborhood.

Adding this parameter and setting it to **On** prevents this user from saving passwords for any application set. Any existing cached passwords are deleted.

To prevent users from saving their password for *particular* 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 individual's user-level Pn.ini file (default directory: %User Profile%\Application Data\ICAClient) in a text editor.
3. Locate the section name that corresponds to the application set for which you want to disable password saving; for example, [MyAppSet].
4. Add the following line 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. Repeat Steps 1 through 6 for additional users.
8. Start Program Neighborhood.

Adding this parameter and setting it to **On** prevents this user from saving passwords for the specified application set or sets. Any existing cached passwords are deleted.

Configuring General Settings

To configure the general settings

1. Start Program Neighborhood.
2. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. 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 device. 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 device 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 Citrix Terminal product such as *WinFrame* for Terminals and MetaFrame for Terminals, which require 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.

- **Keyboard Layout**. Allows you to specify the keyboard layout of your client device. The Citrix server uses the keyboard layout information to configure the 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 device. 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.
- **Pass-Through Authentication:** If you are logged on as an administrator of the client machine, select this option to enable single sign-on at the machine level. Each user must turn this feature on by selecting the **Use local user name and password for logon** option described below.
- **Use local username and password for logon**: Check this box to enable this feature at the user level in the **Login** dialog boxes. Single sign-on must be enabled at the machine level.

Configuring Bitmap Caching

▸ **To configure bitmap caching**

1. Start Program Neighborhood.
2. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. Click the **Bitmap Cache** tab.

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

   - **Bitmap Cache Size**. Specify the size of the bitmap cache in kilobytes.

- **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.
- **Minimum size bitmap to be cached**. The size of the smallest bitmap to be cached to disk.
- **Clear cache Now**. Click this button to remove all cached data from the directory.

Tip Do not 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. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. Click the **Hotkeys** tab.
4. For each hotkey in the list, select a shift state and a key.
5. 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.

Note 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 hotkey. See your Windows NT documentation for more information about the CTRL-SHIFT-ESC hotkey.
- **Toggle Latency Reduction**. This hotkey turns SpeedScreen Latency Reduction on or off. Latency reduction reduces the time between your keyboard or mouse input and a visible response on the screen. If an application on the MetaFrame XP server is configured to use latency reduction, the ICA Client also uses latency reduction by default. If the latency reduction feature causes problems when running the application, you can turn it off using this hotkey.

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. From the **Tools** menu, click **ICA Settings** to display the **ICA Settings** dialog box.
3. Click the **Event Logging** tab.

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

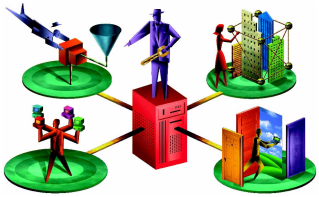
   Event Log File. Enter the name of the file to log Citrix ICA Client events to in the **Name** field.

   - 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. Select the event categories that you want to log from the types listed below. If no events are selected, no logging takes place.

   - **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.

CHAPTER 4



Installing and Configuring the ICA Win32 Program Neighborhood Agent

This chapter explains how to install and configure the ICA Win32 Program Neighborhood Agent. The following topics are covered:

- Overview of the ICA Win32 Program Neighborhood Agent
- System Requirements
- Installing the ICA Win32 Program Neighborhood Agent
- Starting the ICA Win32 Program Neighborhood Agent
- Configuring the ICA Win32 Program Neighborhood Agent

Overview of the ICA Win32 Program Neighborhood Agent

You can use the ICA Win32 Program Neighborhood Agent with Citrix NFuse 1.6 to "push" links to applications directly to users' Windows desktops. You can place links to remote applications in the Start menu, on the desktop, or in the Windows System Tray. Users do not run Web browsers to access a Web page with links to remote applications. Use this ICA Win32 Client if you want to use NFuse in an enterprise that does not permit users to launch browsers.

All client configuration is done at the NFuse server level in an XML file (Config.xml). Users connect to the XML file using HTTP or HTTPS to retrieve configuration, enumeration, and launch information. Because the Program Neighborhood Agent uses HTTP to pass the XML data, it is easy to use it with a firewall.

The Program Neighborhood Agent includes settings that users can configure on the client device, such as server URL, logon mode, and window display. You can allow users to configure Program Neighborhood Agent settings or you can "lock down" the user interface in the Config.xml file to prevent user configuration.

Important For information about working with the configuration file (Config.xml) on the NFuse server to prevent user configuration and to "push" Program Neighborhood settings to the client machine, see Chapter 6 of the *NFuse 1.6 Administrator's Guide*.

The ICA Win32 Program Neighborhood Agent provides the following features:

- Windows desktop integration
- SSL support for ICA
- Auto Client Reconnect
- Published content support
- Novell Directory Services support
- DNS name resolution support
- Seamless windows
- Client device mapping
- Sound support
- Client Auto Update
- Windows clipboard integration
- Low bandwidth requirements
- SpeedScreen Latency Reduction
- Disk caching and data compression
- TCP/IP+HTTP server location
- Wheel mouse support
- Multi-monitor support
- Pass-through authentication
- Panning and scaling
- Per-user time zone support

System Requirements

Computers used with the ICA Win32 Program Neighborhood Agent must meet the following requirements:

- Standard PC architecture, 80386 processor or greater as required for the operating system
- Windows 95 (OSR2 or greater), Windows 98, Windows 2000, Windows Me, Windows XP, 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, 32MB or greater for Windows 2000 and Windows Me, and 128MB RAM for Windows XP
- Microsoft mouse or 100% compatible mouse
- VGA or SVGA video adapter with color monitor
- High-density 3.5-inch disk drive (optional) and available hard disk space
- Windows-compatible sound card for sound support (optional)
- For network connections to the Citrix server, a network interface card (NIC) and the appropriate network transport software are required. Supported connection methods and network transports are:
  - TCP/IP+HTTP
  - SSL+HTTPS

For information about configuring the ICA Win32 Clients to use SSL to secure communications, see “Using SSL to Encrypt ICA Traffic” on page 113.

Installing the ICA Win32 Program Neighborhood Agent

You can install the ICA Win32 Program Neighborhood Agent using one of the following packages:

- Ica32a.msi – a Windows Installer package for use with Windows 2000 Active Directory Services or Microsoft Systems Management Server, approximately 4.4MB in size
- Ica32a.exe – a self-extracting executable, approximately 2.9MB in size

---

Note For a discussion of methods for deploying ICA Win32 Client software to users, see “Deploying the ICA Win32 Clients” on page 21 of this guide, and chapter 9 of the *MetaFrame XP Administrator’s Guide* delivered with Feature Release 1 of MetaFrame XP 1.0.

Installing the ICA Win32 Program Neighborhood Agent with the Windows Installer Package

The ICA Win32 Program Neighborhood Agent is available in a Windows installer package file (Ica32a.msi). You can distribute the Program Neighborhood Agent installer package to your users with Microsoft Systems Management Server or Windows 2000 Active Directory Services.

This package is located in the following directories (substitute *language* with the language of the ICA Client software) on the ICA Client CD included in the MetaFrame XP, Feature Release 1 media pack:

Icaweb*language*\ica32

Icainst*language*\ica32\pnagent

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

Note The Windows Installer service is present by default on computers running the Windows 2000 operating system. If the computer is running Windows NT 4.0 or Windows 9x, you must install Windows Installer Version 1.1 or higher.

To uninstall the Program Neighborhood Agent installed using an installer package, you can either use **Add/Remove Programs** in the Control Panel or you can run the same installer package again.

Updating Previous Versions of the Program Neighborhood Agent with the Installer Package

You cannot automatically update previous versions of the ICA Win32 Client installed with Windows Installer (.msi) packages. You must redeploy an ICA Win32 Client installer package when a new version of the Program Neighborhood Agent is released.

Configuring the Installer Package for Silent User Installation

You can configure the Program Neighborhood Agent installer package for "silent" user installation. Windows Installer informs the user when the ICA Win32 Client software is successfully installed. The user must clear the Windows Installer message box.

To configure the Program Neighborhood Agent installer package for silent user installation

1. Enter the command line

   msiexec /I <MSI_Package> /qn+ [Key=Value]…

   where <MSI_Package> is the name of the installer package.

2. You can set the following keys:

   INSTALLDIR=<Installation_Path>, where <Installation_Path> is the path to the directory where the ICA Client software is installed. The Program Neighborhood Agent software is installed in the directory Program Files\Citrix\PNAgent by default.

   CLIENT_UPGRADE=**Yes** or **No**. The default value is **Yes**.

   PROGRAM_FOLDER_NAME=<Start Menu Program Folder Name>, where <Start Menu Program Folder Name> is the name of the Programs folder on the Start menu containing the shortcut to the Program Neighborhood Agent software. The default value is **Citrix Program Neighborhood Agent**.

   SERVER_LOCATION= NFuse server URL. The default value is **PNAgent**. Enter the URL of the NFuse server hosting the Config.xml file in the format http://<*servername*> or https://<*servername*>.

   Note The Program Neighborhood Agent appends the default path and file name of the config.xml file on the NFuse server to the server URL. If you move the default location of the config.xml file, you must enter the entire new path in the SERVER_LOCATION key.

   ENABLE_SSON=**Yes** or **No**. The default value is **No**. If you enable the SSON (single sign-on) property, set the ALLOW_REBOOT property to **No** to avoid automatic rebooting of the client system.

   ALLOW_REBOOT=**Yes** or **No**. The default value is **Yes**.

Installing the ICA Win32 Program Neighborhood Agent with the Self-Extracting Executable

The ICA Win32 Program Neighborhood Agent is available in a self-extracting executable file (Ica32a.exe). This file is located in the following directories (substitute *language* with the language of the ICA Client software) on the ICA Client CD included in the MetaFrame XP, Feature Release 1 media pack:

Icaweb*language*\ica32

Icainst*language*\ica32\pnagent

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

Configuring the Self-Extracting Executable for Silent User Installation

You can limit user interaction with the self-extracting executable setup program by entering values in the file Install.ini before you deploy the Program Neighborhood Agent to your users.

Important You can use any standard compression utility to extract the client files from the packaged executable. However, you must use commercially available software to repackage the client files for distribution to your users.

▸ **To configure the self-extracting executable for silent user installation**

1. Extract the ICA Client files from Ica32a.exe using your preferred compression utility software or by entering the command line

   ica32a.exe -a -unpack:<Directory Location>

   where <Directory Location> is the directory where you want to extract the client files.

2. Locate the file Install.ini.
3. Open Install.ini in any text editor.

4. You can set the following parameters. When you enter values for these parameters, the setup program dialog boxes do not appear on the user's screen.

   ServerURL=NFuse server URL. The default value is **PNAgent**. Enter the URL of the NFuse server hosting the Config.xml file in the format **http://*servername*** or **https://*servername*** for SSL-secured communications.

   SetMachineNameClientName=Enter **On** to accept the Windows machine name as the client device name.

   Location=Enter the installation location. Use <PROGRAM_FILES> if you want to install the files in a directory in the Program Files folder.

   StartMenu=Enter the Start menu path. The path you enter here will be appended to the Programs folder of the Start menu.

   InstallSingleSignOn=Enter **On** to enable Pass-Through Authentication.

   AcceptClientSideEULA=Enter **On** to accept the end-user license agreement.

5. Save the file and exit the text editor.
6. Repackage the client files for distribution to your users.

▸ To install the Program Neighborhood Agent with the self-extracting executable

1. If you are installing from the Citrix ICA Client CD, run Ica32a.exe, located in the following directory (substitute *language* with the language of your server software):

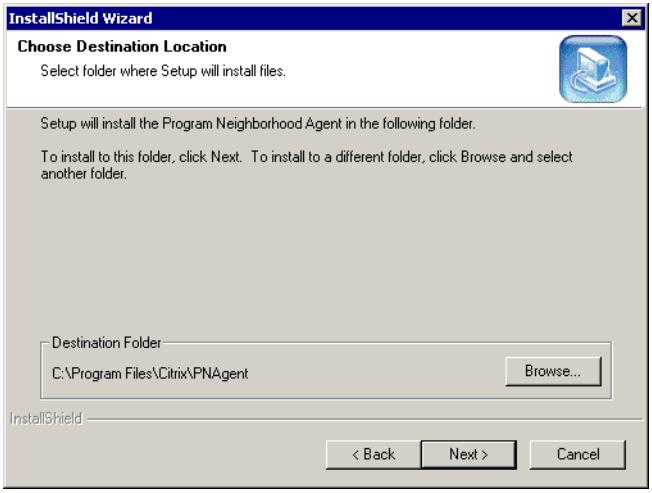
   Icaweb*language*\ica32

   where *language* is one of:

   - En (English)
   - Fr (French)
   - De (German)
   - Ja (Japanese)
   - Es (Spanish)

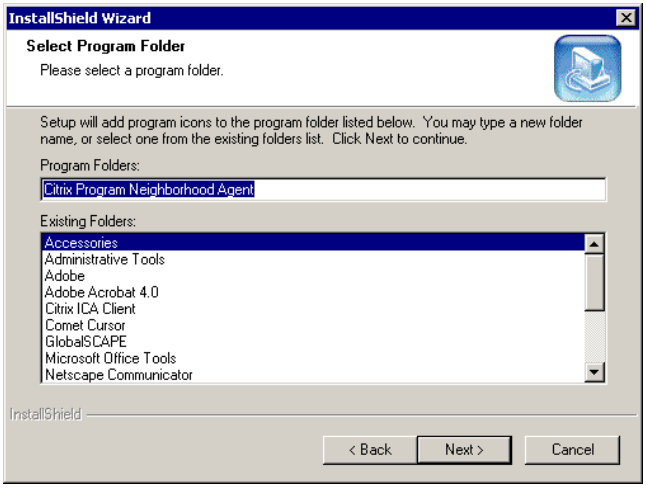
2. The **Welcome** screen appears. Read the information on this screen and click **Next**.
3. The **License Agreement** screen appears. Read the license agreement and click **Next** if you agree to the terms of the agreement.

4. The **Choose Destination Location** dialog box appears:



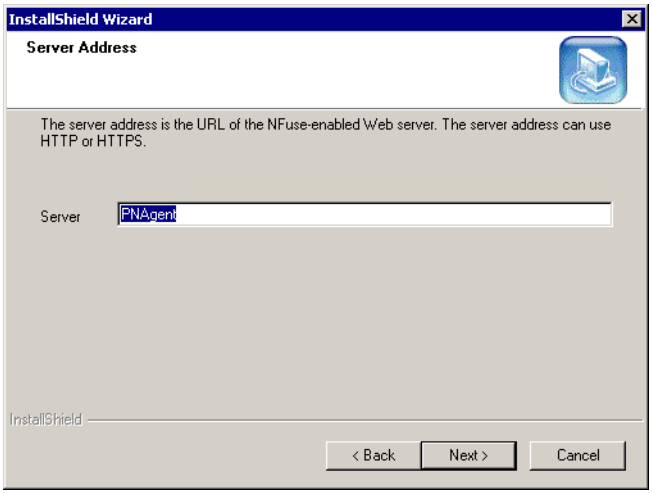
Click **Browse** to select a different installation location. Click **Next** to accept the default path and continue.

5. The **Select Program Folder** dialog box appears:



You can choose to use the default Citrix Program Neighborhood Agent folder, specify the name of a new program folder, or add the Program Neighborhood Agent icon to an existing folder. The program folder you specify is created if it does not already exist. Click **Next** to continue.

6. The **Server Address** dialog box appears.



Enter the URL of the NFuse Web server to connect to in the format http://*servername* or https://*servername*.

Click **Next** to continue.

7. The **Setup Type** dialog box appears.

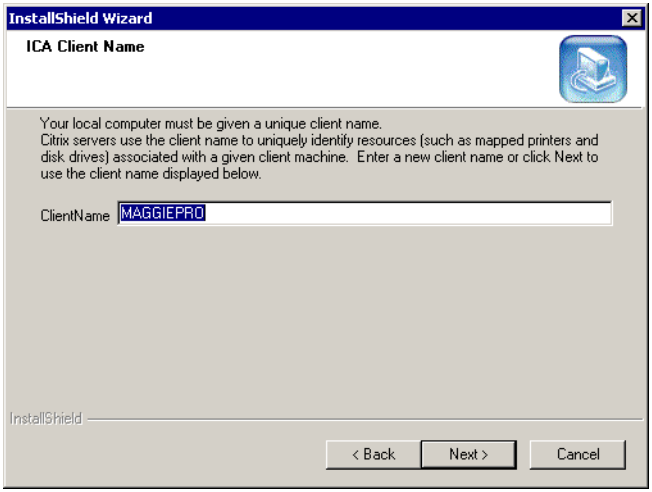
Select **Yes** to enable the Program Neighborhood Agent enable the single sign-on logon method. This feature allows the ICA Client to access the user's local Windows user name, password, and domain information and pass it to the server. Users are not prompted to log on to the Program Neighborhood Agent separately.

You must enable this logon method in the Config.xml file on the NFuse Web server before users can use it from this client. If you want to use the single sign-on logon method, select **Yes** and then select this logon method in the **Properties** dialog box.

Important If you select **No**, you must reinstall the Program Neighborhood Agent if you decide to use the single sign-on logon method at a later time.

Click **Next** to continue.

8. The **ICA Client Name** dialog box appears.



Specify a unique client name for your client device. Citrix servers use the client name to manage client printers and other system resources. If you do not always assign a unique machine name to each client device, device mapping and application publishing may not operate correctly. You can use the client name displayed in the **Client Name** field, or specify a new one.

When you are done, click **Next** to continue. A progress window appears, displaying the file names as they are copied to your hard drive.

9. You are informed that Program Neighborhood Agent was successfully installed on the computer. Click **Finish**.

Starting the ICA Win32 Program Neighborhood Agent

The Program Neighborhood Agent starts when users start client devices. If the logon mode is configured for single sign-on, the Program Neighborhood Agent accesses users' user names, passwords, and domain information when they log on to Windows and passes the information to the Citrix server. Users are not prompted to log on to the Program Neighborhood Agent separately.

To start the Program Neighborhood Agent without rebooting, select **Programs** on the Windows **Start** menu, and then select **Citrix Program Neighborhood Agent**. Select **Program Neighborhood Agent** from the menu that appears.

Note The Program Neighborhood Agent supports both Novell NetWare Directory Services (NDS) and Windows directory services. If your network uses NetWare Directory Services, users log on using the **NDS** logon tab. If your network uses Windows NT, users log on using the **Windows** logon tab.

Configuring the ICA Win32 Program Neighborhood Agent

By default, users can access the Program Neighborhood Agent **Properties** dialog box to configure preferences. You can grant or deny user access to configuration settings in the configuration file (Config.xml) on the NFuse server.

This section presents general information about configuring the Program Neighborhood Agent from the **Properties** dialog box accessed on the client device. For more detailed information, see the online Help for the Program Neighborhood Agent.

Configuring the Server URL

The Program Neighborhood Agent requires the URL of the NFuse server hosting the config.xml file. This XML file contains the URLs for the enumeration and ICA file requests from the client.

If the default setup program is used, you are prompted to enter the server URL during Program Neighborhood Agent installation. You can change the server URL on the Program Neighborhood Agent **Properties** dialog box.

▸ **To configure the server URL**

1. Click the Program Neighborhood Agent icon in the Windows System Tray and choose **Properties** from the menu that appears.
2. The currently configured URL is displayed on the **Server** tab. Click **Change** and enter the server URL on the dialog box that appears. Enter the URL in the format http://<*servername*> or https://<*servername*> to encrypt the configuration data using SSL.

   Important If you are using the Citrix SSL Relay to secure communications between the MetaFrame server and the NFuse server, be sure to specify in the Config.xml file the machine name of the server hosting the SSL certificate. See Chapter 6 of the *NFuse 1.6 Administrator's Guide* for more information.

3. Click **Update** to apply the change and return to the **Server** tab. Click **Cancel** to cancel the operation.
4. Click **OK** to close the Program Neighborhood Agent **Properties** dialog box.

Configuring the Logon Mode

The Program Neighborhood Agent supports both Novell NetWare Directory Services and Windows directory services. If your network uses NetWare Directory Services, users log on using the NDS logon tab. If your network uses Windows NT, users log on using the Windows logon tab.

▸ **To configure a logon mode**

1. Click the Program Neighborhood Agent icon in the Windows System Tray and choose **Properties** from the menu that appears.
2. On the **Server** tab, select one of the following logon modes.

   Prompt User - Users are prompted for a user name, password, and domain when they start the Program Neighborhood Agent. Applications they are authorized to access appear as shortcuts on the desktop or **Start** menu.

   Single Sign-On - The Program Neighborhood Agent accesses users' local Windows user names, passwords, and domain information. Users are not prompted to log on to the Program Neighborhood Agent separately.

   Note If you did not enable the single sign-on feature when you first installed the Program Neighborhood Agent, you must reinstall the software if you decide to use the single sign-on logon method at a later time.

   ---

3. Click **OK** to apply the selections and close the Program Neighborhood Agent **Properties** dialog box.

Configuring Shortcuts to Remote Applications

With the Program Neighborhood Agent, users access remote applications by clicking links you can place on the **Start** menu, Windows desktop, or the **Program Neighborhood Agent** menu in the Windows System Tray.

▸ **To configure shortcuts to remote applications**

1. Click the Program Neighborhood Agent icon in the Windows System Tray and choose **Properties** from the menu that appears.

2. On the **Application Display** tab, choose from the following options:

   Show applications in Start menu – Select this option to place links to remote applications in the Windows **Start** menu. If you want to group the links in a folder, enter the name of the folder in the text box below this option.

   Show this folder in Programs submenu – Select this option to place the customized folder in the Programs submenu of the **Start** menu.

   Show applications in desktop folder – Select this option to place links to remote applications in a folder on the desktop. Enter a name for the folder in the text box below this option.

   Display applications in System Tray – Select this option to place links to remote applications in the **Applications** submenu of the **Program Neighborhood Agent** menu. To access the **Program Neighborhood Agent** menu, click the Program Neighborhood Agent icon in the Windows System Tray.

3. Click **OK** to apply the selections and close the Program Neighborhood Agent **Properties** dialog box.

Configuring Display Options

You can specify the window size, color depth, and audio quality for remote applications.

▸ **To configure display options**

1. Click the Program Neighborhood Agent icon in the Windows System Tray and choose **Properties** from the menu that appears.
2. On the **ICA Options** tab, choose from the following options:

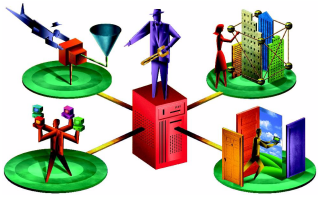
   Window size – When this option is set to **Default**, the window size set in the config.xml file is used. To change the window size, select a specific window size for an ICA session from the drop-down list.

   Color depth – When this option is set to **Default**, the color depth set in the config.xml file is used. To change the color depth, select the number of window colors to use from the drop-down list.

   Audio quality – When this option is set to **Default**, the audio quality set in the config.xml file is used. To change the audio quality, select a different level of audio quality from the drop-down list.

3. Click **OK** to apply the selections and close the Program Neighborhood Agent **Properties** dialog box.

CHAPTER 5



Installing and Configuring the ICA Win32 Web Client

This chapter explains how to install and configure the ICA Win32 Web Client. The following topics are covered:

- Overview of the ICA Win32 Web Client
- System Requirements
- Configuring the ICA Win32 Web Client for Silent User Installation
- Installing the ICA Win32 Web Client
- Using the ICA Win32 Clients with Application Launching and Embedding

Overview of the ICA Win32 Web Client

Use the ICA Win32 Web Client if your users access published applications using a Web browser with Citrix NFuse or through traditional application launching and embedding. The ICA Win32 Web Client is packaged in the file ica32t.exe.

The ica32t.exe file is a self-extracting executable, approximately 1.8MB in size. This package is significantly smaller than the full ICA Win32 Program Neighborhood Client. The smaller size allows quicker downloads and installation. You can configure the ICA Win32 Web Client for silent user installation.

The ICA Win32 Web Client supports the following features:

- SSL support for ICA
- Auto Client Reconnect
- Published content support
- Novell Directory Services support
- DNS name resolution support

- Extended parameter passing
- Seamless windows
- Client device mapping
- Sound support
- TCP/IP+HTTP server location
- Wheel mouse support
- Multi-monitor support
- Panning and scaling
- Per-user time zone support
- Windows clipboard integration
- Low bandwidth requirements
- SpeedScreen Latency Reduction
- Disk caching and data compression

System Requirements

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

- Standard PC architecture, 80386 processor or greater as required for the operating system and Web browser
- Windows 9x, Windows 2000, Windows Me, Windows XP, 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, 32MB or greater for Windows 2000 and Windows Me, and 128MB RAM or greater for Windows XP
- Standard Web browser; Internet Explorer Version 4.0 or greater, or Netscape Navigator or Communicator Version 4.0 or greater
- Microsoft mouse or 100% compatible mouse
- VGA or SVGA video adapter with color monitor
- High-density 3.5-inch disk drive (optional) and available hard disk space
- Windows-compatible sound card for sound support (optional)
- For network connections to the Citrix server, a network interface card (NIC) and the appropriate network transport software are required. The ICA Win32 Web Client supports the TCP/IP network transport only.

Configuring the ICA Win32 Web Client for Silent User Installation

Installing the ICA Win32 Web Client requires minimal user interaction. A typical installation presents the user with the following:

1. An initial prompt informing the user that the Citrix ICA Win32 Web Client is about to be installed. The user clicks **Yes** to continue with setup or **No** to stop setup.
2. A Citrix License Agreement. The user clicks **Yes** to accept the agreement or **No** to reject the agreement. If the user clicks **No**, setup stops.
3. An indication that the setup program is copying files to the client device. The default file location for the ICA Win32 Web Client is Program Files\Citrix\icaweb32.
4. A message box informing the user that the Citrix ICA Web Client was installed successfully. The user must click **OK** to clear the message.
5. If the user is running Netscape Navigator, the user must restart the browser.

You can further limit user interaction with the setup program by suppressing the appearance of the initial user prompt (described in Step 1) and the Citrix License Agreement (described in Step 2). These parameters are contained in the file ctxsetup.ini.

Important You can use any standard compression utility to extract the client files from the packaged executable. However, you must use commercially available software to repackage the client files for distribution to your users.

▸ To configure the ICA Win32 Web Client for silent user installation

1. Extract the ICA Client files from Ica32t.exe using your preferred compression utility software. This executable is located in the following directory (substitute *language* with the language of your server software):

   Icaweb*language*\ica32

   where *language* is one of:

   - En (English)
   - Fr (French)
   - De (German)
   - Ja (Japanese)
   - Es (Spanish)

2. Locate the file Ctxsetup.ini.

3. Open Ctxsetup.ini in any text editor.
4. Locate the **InitialPrompt** parameter. Change the value of the setting from 1 to 0.
5. Locate the **DisplayLicenseDlg** parameter. Change the value of the setting from 1 to 0.
6. Save the file and exit the text editor.
7. Repackage the client files for distribution to your users.

Installing the ICA Win32 Web Client

The instructions below describe how to install the ICA Win32 Web Client using a typical installation.

The ICA Win32 Web Client executable, ica32t.exe, is located on the ICA Client CD in the following directory (substitute *language* with the language of your server software):

Icaweb*language*\ica32

where *language* is one of:

- En (English)
- Fr (French)
- De (German)
- Ja (Japanese)
- Es (Spanish)

If you are using the ICA Win32 Web Client with Citrix NFuse, see the *NFuse Administrator's Guide* for information about deploying this ICA Client with NFuse.

▸ To install the ICA Win32 Web Client

1. Run Ica32t.exe.
2. The initial prompt informs you that the Citrix ICA Win32 Web Client is about to be installed. Click **Yes** to continue with setup or **No** to stop setup.
3. The Citrix License Agreement appears. Click **Yes** to accept the agreement or **No** to reject the agreement. If you click **No**, setup stops.
4. You are informed that the setup program is copying files to the client device. The default file location for the ICA Win32 Web Client is Program Files\Citrix\icaweb32.

5. You are informed that the Citrix ICA Web Client was installed successfully. Click **OK** to clear the message.
6. If you are running Netscape Navigator, you must restart the browser.

Using the ICA Win32 Clients with Application Launching and Embedding

If you are not planning to use Citrix NFuse but still want to deliver applications to your users by a Web-based method, you can use Application Launching and Embedding (ALE) in conjunction with the Web-based ICA Client Installation feature. The ICA Win32 Program Neighborhood and Web Clients can be used with launched and embedded applications.

The ICA Win32 Web Client replaces the ActiveX control and Netscape Plug-In Clients, and is packaged in the file ica32t.exe. This file contains both the ActiveX control and Netscape Plug-In.

The ica32t.exe file is a self-extracting executable, approximately 1.8MB in size. This package is significantly smaller than the full ICA Win32 Program Neighborhood Client. The smaller size allows quicker downloads and installation. You can configure the ICA Win32 Web Client for silent user installation.

Application Launching and Embedding

Application Launching and Embedding allows full-function Windows-based applications to be launched from or embedded into HTML pages without rewriting application code. Using ALE, administrators can provide access to existing applications over Intranets or the Internet. The application looks and feels as if it is running locally, even though it is actually executing on the Citrix server. There are two ways to run an application from a Web page: launching and embedding.

- *Launching* an application from a Web page involves clicking a hyperlink that references an ICA file. Clicking the hyperlink causes the application to start and appear in a separate window on the local desktop. You can then use this application as if it were installed and running on your local computer.
- *Embedding* an application places the window in which the program runs within the Web browser window.

Launched Applications

The Citrix Management Console in MetaFrame XP and the Published Application Manager in MetaFrame 1.8 both include wizards that allow you to create ICA files and HTML pages. The HTML pages are saved on your Web server for users to visit and launch ICA sessions. HTML pages that launch ICA sessions contain a hyperlink to a valid ICA file that is located in a public HTML directory. When clicked, the hyperlink downloads the ICA file to the client device. The client device then passes the ICA file to the ICA Client software installed on the client device. The ICA Client software uses the parameters in the ICA file to launch the application on the user's desktop. If the ICA Client software is not detected on the client device, it is presented to the user to be downloaded and installed.

▸ **To set up a Web page so users can launch an application**

1. Copy the ica32t.exe or ica32.exe file to your Web server. This file is located on the Citrix ICA Client CD in the following directory: \Icaweb\en\Ica32.
2. Publish an application. See the *Administrator's Guide* for the version of MetaFrame you are using or the *WINFRAME Systems Guide* for more information about publishing applications.
3. Use the Create HTML File wizard (using MetaFrame XP) or the Write HTML File wizard (using MetaFrame 1.8) to create an HTML page on your server.You can also create an ICA file. For more information about creating HTML files that contain published applications, see your Citrix server documentation and the online Help for the Citrix Management Console (if you are using MetaFrame XP) or the Published Application Manager (if you are using MetaFrame 1.8).
4. Open the HTML file in a text editor and edit the client type parameter to include the full path to the ica32.exe or ica32t.exe file. This parameter calls the ICA Win32 Client to run the published application.

Embedded Applications

The Citrix ICA Win32 Program Neighborhood and Web Clients allow you to embed applications into Internet Explorer and Netscape Navigator.

Rather than create separate Web pages for Microsoft Internet Explorer and Netscape Navigator users, you can create a single Web page that contains two types of HTML tags to embed applications for Internet Explorer and Netscape Navigator.

Complete the following steps to use one of the ICA Win32 Clients to embed applications into Internet Explorer or Netscape Navigator:

1. Create an ICA Client download Web site using the Web-based ICA Client Installation feature. The elements required for the download Web site are located on the NFuse CD and the ICA Client CD, or can be downloaded from the Download area of the Citrix Web site at http://www.citrix.com/download. Click the "Download Web-based ICA Clients Install Components" link.

   For more information about constructing an ICA Client download Web site using the NFuse CD and the ICA Client CD, see the "Deploying ICA Clients to Your Users" chapter in the *MetaFrame XP Administrator's Guide*.

   For more information about constructing an ICA Client download Web site using the packages downloaded from the Citrix Web site, see the corresponding Readme.htm file located on the same Web page as the packages.

2. Create an HTML page with the appropriate wizard on your Citrix server.
3. Set the **cabLoc** parameter for Internet Explorer users.
4. Set the **Pluginspage** parameter for Netscape Navigator users.

Detailed instructions for Steps 2, 3, and 4 are below.

▸ **To create an HTML page using Citrix server software**

1. If you are using MetaFrame XP, open the Create HTML File wizard on your Citrix server. This wizard is accessed through the Citrix Management Console.

   If you are using MetaFrame 1.8, open the Write HTML File wizard on your Citrix server. This wizard is accessed through the Published Application Manager.

2. Create the HTML file, saving it to your Web server. Follow the on-line help for the appropriate wizard.
3. Open the HTML file in a text editor.

▸ **To set the cabLoc parameter for Internet Explorer users**

1. In the HTML file you created with your Citrix server software, locate the line that begins with the following text: **var cabLoc =**.

   Replace the value after the equal sign (=) with the URL of the appropriate Win32 Client:"http://*Webserver*/*directory*/ica32.exe or ica32t.exe";

   Make sure you include the quotation marks and semicolon.

2. Save the file and make sure it is stored on your Web server with the ICA file for the embedded session. When users visit the HTML page, Internet Explorer automatically downloads and installs the ActiveX control.
3. Keep the HTML file open.

To set the Pluginspage parameter for Netscape Navigator users

1. Locate the line that begins with the following text: **var plugRefLoc =**.

   Replace the value after the equal sign (=) with the full path to the default Web page of the ICA Client download Web site you created with the Web-based ICA Client Installation feature.

   Example: var plugRefloc = "http://*mywebserver*/ica60/setup.htm";

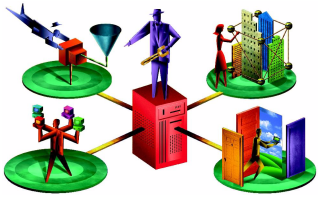
   Make sure you include the quotation marks and semicolon.

2. Save the file and make sure it is stored on your Web server along with the ICA file for the embedded session.

3. Publish a link to the HTML page. When users visit the HTML page, Netscape Navigator refers users who do not have the Plug-In to the appropriate ICA Client download page.

CHAPTER 6

Configuring Features Common to the ICA Win32 Clients



This chapter explains how to configure and use features common to the ICA Win32 Clients. The following topics are covered:

- Configuring New Features on Version 6.20 of the ICA Win32 Clients
- Configuring Existing Features Common to the ICA Win32 Clients
- Configuring Multiple Monitors
- Updating the ICA Clients
- Using Applications Published on MetaFrame for UNIX

Configuring New Features on Version 6.20 of the ICA Win32 Clients

Configure the following new features in the same manner for all of the ICA Win32 Clients.

Auto Client Reconnect

ICA sessions can be dropped because of unreliable networks, highly variable network latency, or range limitations of wireless devices.

The *auto client reconnect* feature is triggered when the ICA Client detects a disconnected session. When this feature is enabled on a MetaFrame server, users do not have to reconnect manually or reenter logon credentials to continue working. Automatic reconnection does not occur if users exit applications without logging off.

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

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

Changing Default ICA Client Reconnection Settings

Auto client reconnect is enabled on the ICA Win32 Clients by default. When the ICA Client detects that its connection to the server is unexpectedly broken, it waits 30 seconds before beginning the reconnection sequence. By default, the ICA Client attempts to reconnect three times and then stops.

No configuration is required on the client devicee to use these default settings. To change the default settings for a particular user, you must add the following entries to the [WFClient] section of the Appsrv.ini file located in the user's %User Profile%\Application Data\ICA Client directory.

TransportReconnectEnabled=0 to disable auto client reconnect.

TransportReconnectDelay=n to configure the number of seconds to wait before attempting to reconnect.

TransportReconnectRetries=n to configure the number of reconnection attempts.

Disabling DNS Name Resolution

You can configure ICA Win32 Clients that use the XML service to connect to the MetaFrame farm to request a Domain Name System (DNS) name instead of a server's IP address.

Important Unless your DNS environment is configured specifically to use this feature, Citrix recommends that you do not enable DNS name resolution in the server farm.

The ICA Win32 Program Neighborhood Client is configured to use TCP/IP+HTTP (the XML service) browsing by default. ICA Clients connecting to remote applications through NFuse also use the XML service to connect. For ICA Clients connecting through NFuse, the NFuse Web server resolves the DNS name on behalf of the client.

DNS name resolution is disabled by default in the MetaFrame farm and enabled by default on the ICA Win32 Clients. When DNS name resolution is disabled in the farm, any client request for a DNS name will return an IP address. There is no need to disable DNS name resolution on the client.

If you are using DNS name resolution in the MetaFrame farm and you are having problems with specific client workstations, you can disable DNS name resolution for each user of those workstations using the following procedure.

▸ **To disable DNS name resolution on the Win32 ICA Clients**

1. Open the user-level Appsrv.ini file. By default, this file is located in the %User Profile%\Application Data\ICA Client directory.
2. Change the line **xmlAddressResolutionType=DNS-Port** to **xmlAddressResolutionType=IPv4-Port**.
3. Save and close the Appsrv.ini file.
4. Repeat Steps 1 through 3 for all users of the client workstation.

Enabling Extended Parameter Passing

With extended parameter passing you can associate a file type on a client device with an application published on a Citrix server. When a user double-clicks a locally-saved file, the file is opened in the application associated with it on the MetaFrame XP server.

For example, if you associate all text-type files on the client device with the application “Notepad” published on the MetaFrame XP server, opening a locally-saved text-type file on the client device causes Notepad to open on the MetaFrame XP server.

Enabling parameter passing requires both server- and client-side configuration. On the server, add the %* (percent and star symbols) tokens to published applications. These tokens act as placeholders for client-passed parameters. For instructions on configuring the MetaFrame XP server to support parameter passing, see the *MetaFrame XP, Feature Release 1 Administrator’s Guide*.

On the client side, you must replace the file type’s **open** command with a command line that passes the file name and path to the Citrix server. You must enable parameter passing on each client device you want to use this feature.

Configuring Extended Parameter Passing

File type association data is stored in the Windows registry. To associate a file type on the client device with the published application, you need to replace the file type's **open** command with a command line that passes the file name and path to the application published on the Citrix server.

The command line you create must include the following elements:

- The file name of the ICA Win32 Client executable used to launch the remote application
- The name of the published application to launch, in the correct syntax
- The parameter passing arguments

The next section explains how to determine which ICA Win32 Client executable to include in the command line.

Determining the ICA Win32 Client Executable

Users can connect to remote applications using the following methods:

- Finding and launching an application in an application set using Program Neighborhood
- Creating and launching a custom ICA connection using Program Neighborhood
- Launching an .Ica file (.Ica files are placed on the client machine when the user connects using NFuse.)

Each of these methods uses a different application launching executable on the client device to launch the published application. The table below lists which executable you need to include in the parameter passing command line based on the user's connection method.

Connection method	ICA Client executable
Applications in application sets (using Program Neighborhood)	pn.exe
Custom ICA connections (using Program Neighborhood)	wfcrun32.exe
Applications identified in ICA files (including connecting using NFuse)	wfica32.exe

The next section explains how to identify the published application with the correct syntax.

Identifying Published Applications

Each ICA Win32 Client executable uses different command line syntax to specify configuration data when launching published applications. When creating your command line, you must use the executable's command line syntax to correctly identify the published application.

Note To view an executable's required command line syntax, start a command prompt, change directories to the ICA Win32 Client's installation directory, and then type the executable's name followed by /? (forward slash question mark).

Command Line Syntax for pn.exe

To use pn.exe to launch a custom ICA connection, specify:

```
C:\Program Files\Citrix\ICA Client\pn.exe /app:"<application
name>"
```

To use pn.exe to launch an application set application that is published in an application set, specify:

```
C:\Program Files\Citrix\ICA Client\pn.exe /pn:"<application set
name>" /app:"<application name>"
```

Note To use pn.exe to launch an application in an application set, the application must exist in the pn.exe application cache.

An application exists in the cache after the user, using Program Neighborhood, logs on to the application set that contains the application. The cache is populated with the names of all applications included in the set when the user logs on. Applications published after the user logs on do not exist in the cache.

To place an application in the pn.exe cache, start pn.exe and log on to the application set containing the application. Confirm that the application appears in the Program Neighborhood interface.

Command Line Syntax for wfcrun32.exe

To use wfcrun32.exe to launch a custom ICA connection, specify:

```
C:\Program Files\Citrix\ICA Client\wfcrun32.exe "<application
name>"
```

Command Line Syntax for wfica32.exe

To use wfica32.exe to launch a published application described in an ICA file, specify:

```
C:\Program Files\Citrix\ICA Client\wfica32.exe <filename>.ica
```

Including Parameter Passing Arguments

When you determine the launching executable and identify the application, you must include the parameter passing arguments `/param:"%1"`.

The sample command line below associates text-type files with the published application "Notepad Text Editor" in the application set "Production Farm."

```
C:\Program Files\Citrix\ICA Client\pn.exe /pn:"Production Farm"
/app:"Notepad Text Editor" /param:"%1"
```

Entering Parameter Passing in the Windows Registry

When you assemble the required elements of the new command line, you must enter the new command in the Windows registry. You can access the **open** command for the file types you want to associate through the **Folder Options** dialog box in Control Panel. For instructions on editing the **open** command for a file type, see the online Help for the Windows operating system of the client device.

The following example command lines combine the required elements into a working ICA Win32 Client command line.

To associate text files with a custom ICA application named "Notepad Text Editor" launched using pn.exe, specify:

```
C:\Program Files\Citrix\ICA Client\pn.exe /app:"Notepad Text
Editor" /param:"%1"
```

To associate text files with an application set application named "Notepad Text Editor" that is published in an application set called "Production Farm," specify:

```
C:\Program Files\Citrix\ICA Client\pn.exe /pn:"Production Farm"
/app:"Notepad Text Editor" /param:"%1"
```

To associate text files with a custom ICA application named "Notepad Text Editor" launched using wfcrun32.exe, specify:

```
C:\Program Files\Citrix\ICA Client\wfcrun32.exe "Notepad Text
Editor" /param:"%1"
```

To associate text files with an application identified in an ICA file named notepad.ica, using wfica32.exe as the launching executable, specify:

```
C:\Program Files\Citrix\ICA Client\wfica32.exe Notepad.ica
/param:"%1"
```

Important The above examples assume that the client devices are connecting to servers that contain remapped server drives. If your Citrix server drives are not remapped, you must add the following text to the argument: `\\client\`; for example: `/param:"\\client\%1".`

Configuring Existing Features Common to the ICA Win32 Clients

This section explains how to configure existing features that are common to the ICA Win32 Clients. For configuration instructions specific to each ICA Win32 Client, see the appropriate chapter about the client you plan to use.

The following topics are discussed is this section:

- Mapping client drives
- Mapping client printers
- Mapping client COM ports
- Mapping client audio
- Configuring multiple monitors

Mapping Client Devices

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

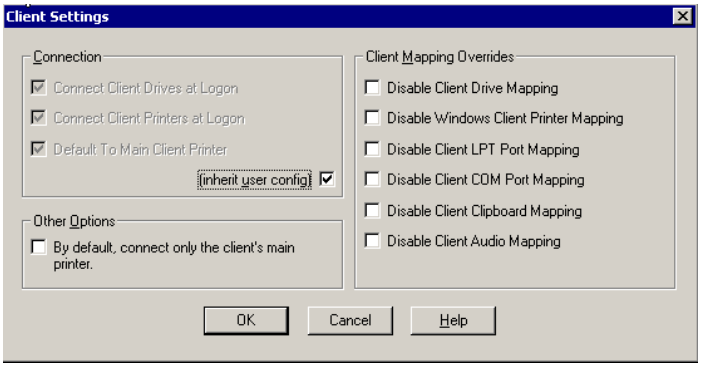
- Transparently access local drives, printers, and COM ports
- Cut and paste between the ICA session and the local Windows clipboard
- Hear audio (system sounds and Wav files) played from the ICA session

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 MetaFrame server, specify client device mapping options in the **Client Settings** dialog box in Citrix 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** options to disable client device connections.

Option	Description
Connect Client Drives at Logon	If this option is checked, the client device's drives are automatically mapped at logon.
Connect Client Printers at Logon	If this option is checked, the client device'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 device.
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 device; for example: drive H in a Citrix user session can be mapped to drive C of the local device 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 drive. (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 devices 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 device connects to a Citrix server, client mappings are reestablished 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 when the user logs off. Each time the user logs on the printer that is already defined is used. If users change the Windows printer settings, they will not automatically be set in this case. If users have custom print settings, you may not want to delete the automatically created printers.

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.

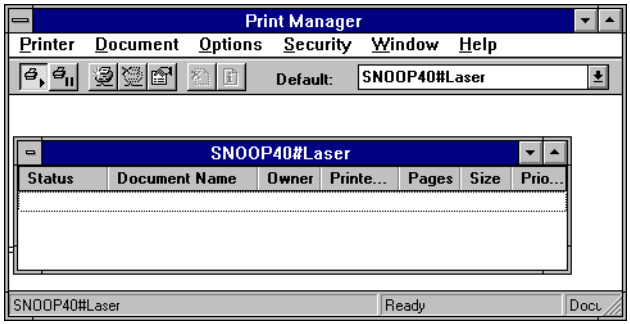
- **To view mapped client printers when connected to a MetaFrame server**

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

  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 device 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** window opens:



  Print Manager 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 device 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.

Mapping Client COM Ports

Client COM port mapping allows devices attached to the client device's COM ports to be used during ICA sessions on a Citrix server. These mappings can be used 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 com*x*: \\client\com*z*:** 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 device.

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

Mapping Client Sound Support

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

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

▸ **To configure ICA Client sound support on a MetaFrame server running on Windows NT 4.0, Terminal Server Edition**

1. Go to **Programs** > **Administrative Tools (Common)** > **Terminal Server Connection Configuration**.
2. Double-click a connection.
3. Click the **ICA Settings** button.
4. Select an option from the **Client Audio Quality** drop-down list.

▸ **To configure ICA Client sound support on a MetaFrame server running on Windows 2000 Server**

1. Go to **Programs** > **Administrative Tools** > **Terminal Services Configuration**.
2. Click **Connections** in the left pane.
3. Double-click a connection in the right pane.
4. Click the **ICA Settings** tab.
5. Select an option from the **Client Audio Quality** drop-down list.

▸ **To configure ICA Client sound support 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 device. 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 device. 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.

Configuring Multiple Monitors

If your client operating system with video hardware and drivers provides multiple monitor support with the Windows taskbar on the primary (left) monitor (Windows 98 and 2000 mode of multiple monitor support), there are restrictions in the level of support when using the client configured with "seamless" windows. Multiple monitors are fully supported when the client is configured in a non-seamless mode and set with the same color depth on all monitors in use.

Note Secondary windows sometimes appear in the primary monitor (uppermost, left).

System Hardware Requirements

To enable multiple monitor support, the system must have the following:

- Multiple PCI video boards, compatible with the Citrix ICA Client on the appropriate Windows platform

  -Or-

- A special multiple monitor video board, such as the Matrox G400, compatible with the Citrix ICA Client on the appropriate Windows platform

The following hardware configurations have been tested with multiple monitor support.

Important It is highly recommended that you test these configurations on your own hardware to ensure that they function properly for your specific machine configuration.

- On Windows 98, Matrox G400 is fully supported as a Windows 98/2000-style multiple monitor
- On Windows 2000, Matrox G400 works in a Windows NT 4.0/Windows 95-style multiple monitor
- Both Windows 98 and Windows 2000 support Matrox G200 PCI (multiple cards installed) as a Windows 98/2000-style multiple monitor
- Windows 98 supports a wide variety of PCI video boards, including many models from ATI and Cirrus Logic

Updating the ICA Clients

Use the Client Auto Update feature to update ICA Client installations with new versions of ICA Client software. As new versions of ICA Clients are released by Citrix, you add them to the Client Update Database. New versions of ICA Clients are released periodically and can be downloaded, along with the updated documentation, from the Citrix Web site at http://www.citrix.com/download.

When users log on to a Citrix server, the server queries the ICA Client to determine the version number. If the version matches the one in the Client Update Database, the logon continues. If the server detects an older version on the client device, the user is informed that a newer version of the ICA Client is available for download. The user can update the client according to the options you set in the database.

Note For users of NFuse Version 1.5: If you have populated the Client Update Database with the ICA Clients from the ICA Client CD included in the MetaFrame XP media, users may receive unnecessary update notifications.

When a user visits an NFuse 1.5 Web site (either a site produced by the NFuse 1.5 Web Site wizard or an example Web site provided by Citrix), the client detection code in the site may incorrectly notify the user that the client device does not have the latest ICA Client installed and prompt the user to update the ICA Client. Select the **Do not show this window at login** option in the update message box to prevent the message from appearing again.

The client detection process was corrected with the release of NFuse Version 1.51, which is included in the MetaFrame XP package. You can also download NFuse from the Citrix Web site at http://www.citrix.com/download.

Client auto update works with all transport types supported by ICA (TCP/IP, IPX, NetBIOS, and asynchronous). Client auto update supports the following features:

- Automatically detects older ICA Client files
- Copies new files over any ICA connection without user intervention

- Provides administrative control of update options for each ICA Client
- Updates ICA Clients from a single database on a network share point
- Safely restores older ICA Client versions when needed

Important You cannot automatically update previous versions of the ICA Win32 Client installed with Windows Installer (.msi) packages. You must redeploy an ICA Win32 Client installer package when a new version of the ICA Client is released.

The ICA Client Update Process

ICA Clients are identified by platform with a product and model number. The version number is assigned when new ICA Clients are released.

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

- If an update is needed, by default, the Citrix server informs the user that a new client is available 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 update process to complete. You can force the client update to complete before allowing the user to continue.
- During the update, new ICA Client files are copied to the user's computer. You 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.
- When the user disconnects from the server and closes all client programs, the ICA Client update process finishes.
- As a safeguard, the existing ICA Client files are saved to a folder named Backup in the Citrix\ICA Client subdirectory of the Program Files directory on the user's local disk.

Configuring the Client Update Database

You can configure a Client Update Database on each Citrix server in a server farm, or configure one database to update the ICA Clients for multiple Citrix servers.

The Client Update Database contains several ICA Clients. As new versions of the ICA Clients are released by Citrix, you add them to the Client Update Database.

Using the Client Update Configuration Utility

Use the Client Update Configuration utility to manage the client update database. From this utility, you can:

- Create a new update database
- Specify a default update database
- Configure the properties of the database
- Configure client update options
- Add new ICA Clients to the database
- Remove outdated or unnecessary ICA Clients
- Change the properties of an ICA Client in the database

The following sections give an overview of the Client Update Configuration utility. For details, see the utility's online help.

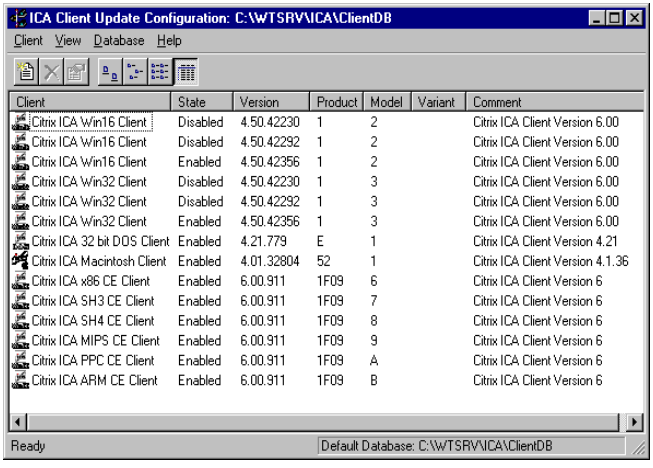
▸ To start the ICA Client Update Configuration utility

1. From a MetaFrame XP server: From the **Start** menu, choose **Programs > Citrix > MetaFrame XP > ICA Client Update Configuration**.

   From a MetaFrame 1.8 server: From the **Start** menu, choose **Programs** > **MetaFrame Tools > 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 status bar shows the location of the current update database, which the Citrix server uses to update ICA Clients. The window shows the ICA Clients in the database.



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 *WINFRAME* server in your server farm.

Creating a New Client Update Database

The ICA Client Distribution wizard creates the Client Update Database in the location %SystemRoot%\Ica\ClientDB. You can create a new update database in any location on a server disk or on a network share point.

▸ **To create a new update database**

1. From the **Database** menu, choose **New**. The **Path for the new Client Update Database** dialog box appears.
2. Enter the path for the new update database and click **Save**. The utility creates a new update database in the specified location and opens the new database.

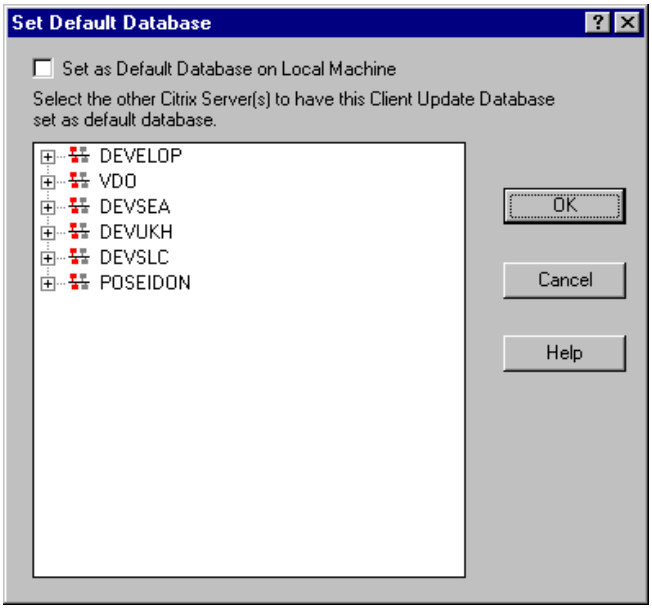
Specifying a Default Client Update Database

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

▸ **To set the default database for Citrix servers**

1. From the **Database** menu, choose **Open**.
2. Specify the path to the default database and click **Open**. The database opens.

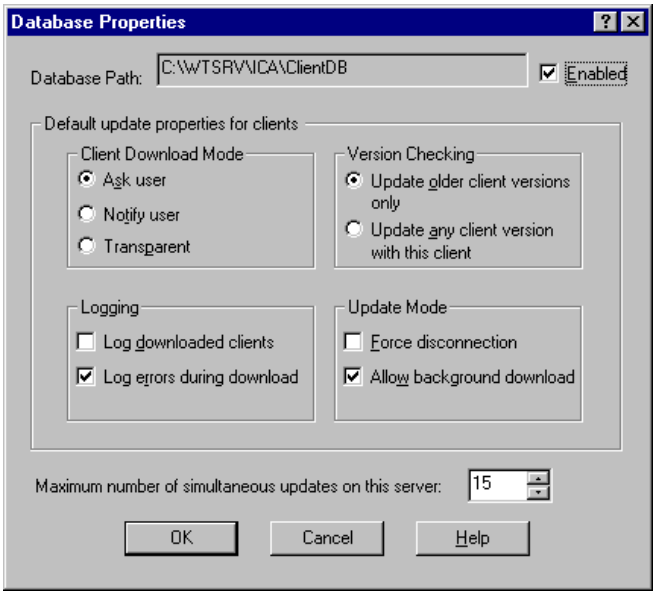
3. On the **Database** menu, click **Set Default**. The **Set Default Database** dialog box opens:



4. Select **Set as Default Database on Local Machine** to make the currently opened database the default database. You can also set other Citrix servers to use the currently open database as the default database.
5. Double-click a domain name to view the servers in that domain. Click a server to set its default database to the currently open database. You can select multiple servers by holding down the CTRL key and clicking each server.
6. Click **OK**.

Configuring Default Client Update Options

Use the **Database Properties** dialog box to configure overall database-wide settings for the current Client Update Database. Choose **Properties** from the **Database** menu to display the dialog box.



- The **Database Path** box displays the path and file name of the database you are configuring.
- For this database to perform ICA Client updates, check **Enabled**.

Tip If the ICA Clients do not need to be updated, disable the database to shorten logon time.

- The options in the **Default update properties for clients** section specify the default behavior for the ICA Clients added to the database. You can also set properties for individual ICA Clients (as described later in this chapter). Individual ICA Client properties override the database properties.
  - Under **Client Download Mode**, select **Ask user** to give the user the choice to accept or postpone the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user's ICA Client software without notifying or asking the user.
  - Under **Version Checking**, select **Update older client versions only** to update only client versions that are older than the new client. Select **Update any client version with this client** to update all client versions to this version; choose this option to force an older client to replace a newer client.

- Under **Logging**, select **Log downloaded clients** to write an event to the event log when a client is updated. By default, errors that occur during a client update are written to the event log. Clear the **Log errors during download** check box to turn this option off.
- Under **Update Mode**, select the **Force disconnection** option to require users to disconnect and complete the update process after downloading the new client. The **Allow background download** option is selected by default to allow users to download new client files in the background and continue working. Clear this check box to force users to wait for all client files to download before continuing.

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

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

Adding ICA Clients to the Client Update Database

When you want to deploy a newer version of the ICA Win32 Client, add it to the Client Update Database. You can download the latest ICA Clients from the Citrix Web site at http://www.citrix.com/download.

Working with the ICA Win32 Client Downloaded from the Citrix Web Site

If you downloaded a new version of the ICA Win32 Program Neighborhood Client, you must first extract the files from the executable ica32.exe before you can add the client to the Client Update Database.

▸ **To extract files from ica32.exe**

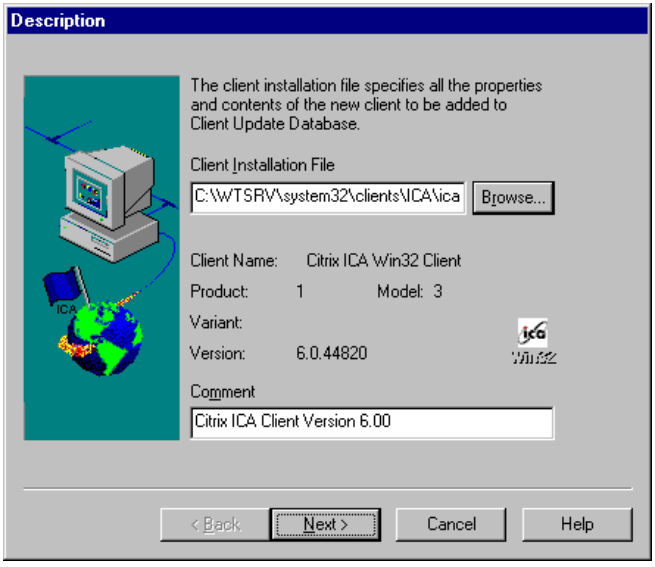
1. Copy ica32.exe to the root of your Citrix server's hard drive.
2. Create a directory to contain the extracted files.
3. At a command prompt, type the following, substituting *samplepath* with the path to the directory you created in Step 2:

   ica32.exe /a /extract /path c:*samplepath*

Note In the above command, the /path command is optional, but recommended. If you do not specify a path, the files are extracted to %SystemRoot%\Ica\Cltimage by default.

To add a Citrix ICA Client to the Client Update Database

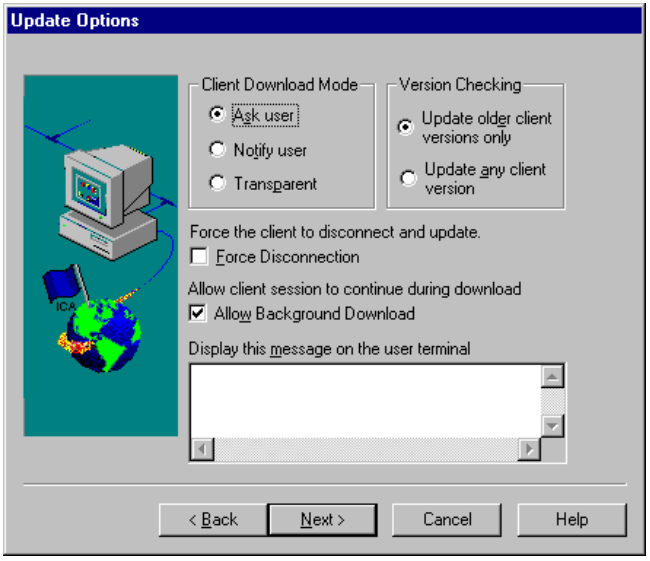
1. From the **Client** menu, click **New** to display the **Description** screen.
2. In the **Client Installation File** box, browse to or enter the path to the client installation file Update.ini. If you ran the ICA Client Distribution Wizard, you can find the Update.ini file in System32\Clients\Ica. You can also find the Update.ini file on the ICA Client CD.



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

   Click **Next** to continue.

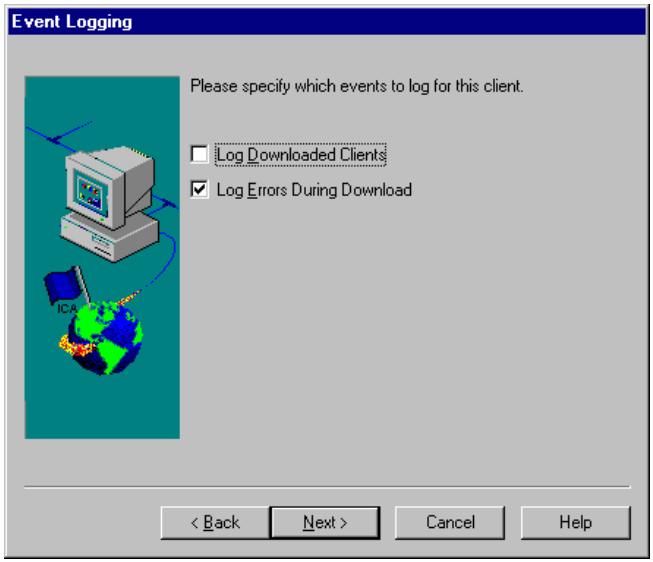
4. The **Update Options** dialog box appears. The options on this dialog box specify how the client update process occurs for this client. The database-wide update options are displayed. You can specify different behavior for individual clients.



The options available in this dialog box are discussed in the online Help for this dialog box.

Click **Next** when you finish configuring the client update options.

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

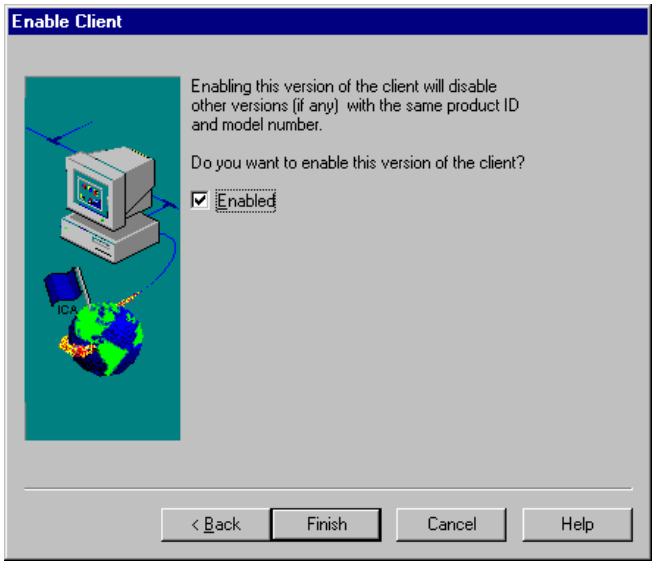


The database-wide logging options are displayed. You can specify different behavior for individual clients.

Select **Log Downloaded Clients** to write an event to the event log when this client is updated. By default, errors that occur during a client update are written to the event log. Clear the **Log Errors During Download** check box to turn this option off.

Click **Next**.

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



The Client Update Database can contain multiple versions of an ICA Client with the same product and model numbers. For example, when Citrix releases a new version of the ICA Win32 Client, you add it to the Client Update Database. However, only one version of the client can be enabled. The enabled client is used for client updating.

Click **Finish** to copy the ICA Client installation files into the Client Update Database.

Removing an ICA Client From the Client Update Database

It is important to delete ICA Clients that are not used from the Client Update Database. A database that contains multiple versions of the same client significantly slows the checking procedure that is carried out each time a user connects to the server.

To remove the ICA Win32 Client from the database

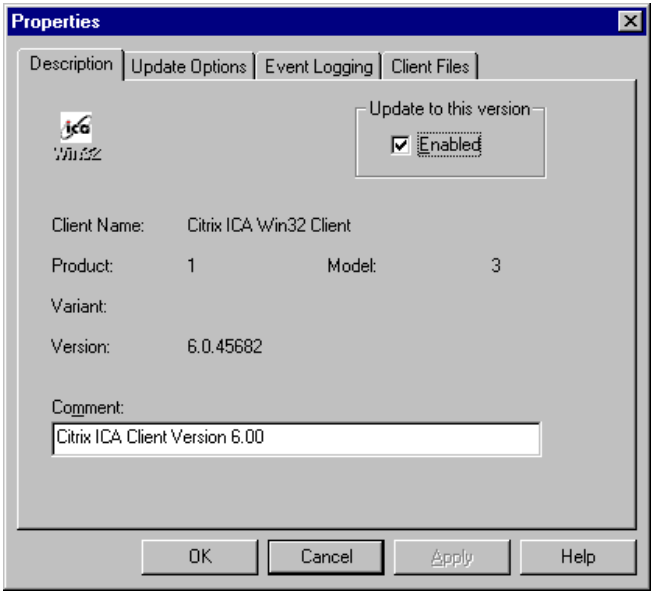
1. Select the Win32 Client you want to remove from the database.
2. From the **Client** menu, choose **Delete**. A message box asks you to confirm the deletion.
3. Click **Yes** to remove the client.

Changing the Properties of the ICA Win32 Client

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

To change the properties of the ICA Win32 Client

1. Select the Win32 Client.
2. On the **Client** menu, choose **Properties**. The **Properties** dialog box appears, containing tabs labeled **Description**, **Update Options**, **Event Logging**, and **Client Files**.

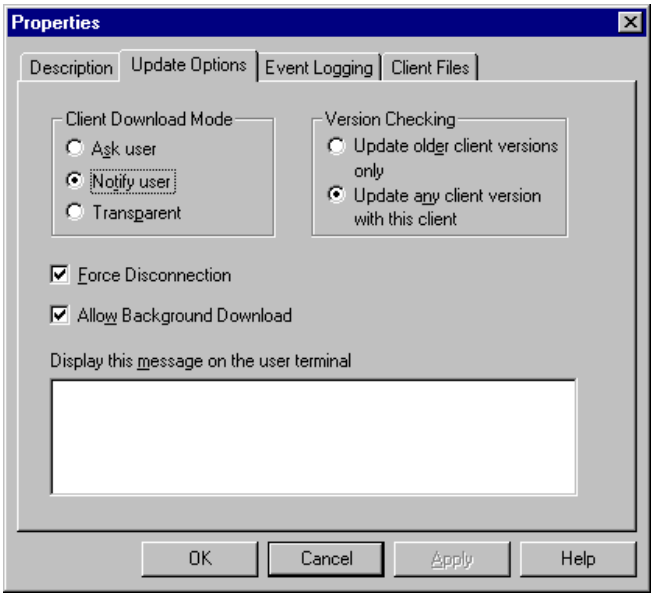


3. The **Description** tab of the **Properties** dialog box lists the client name, product number, model number, and version number.

   Select **Enabled** to update the same platform ICA Client to this version.

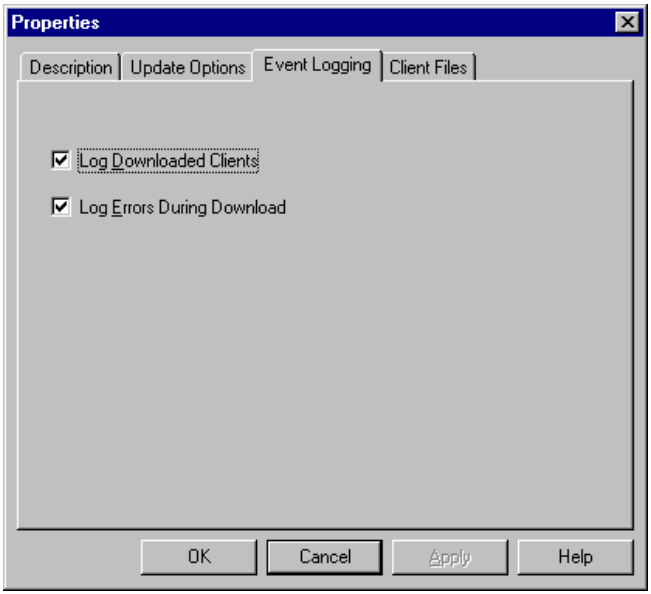
   Optionally, enter a new comment in the **Comment** text box.

4. Use the **Update Options** tab to configure update options for the client.



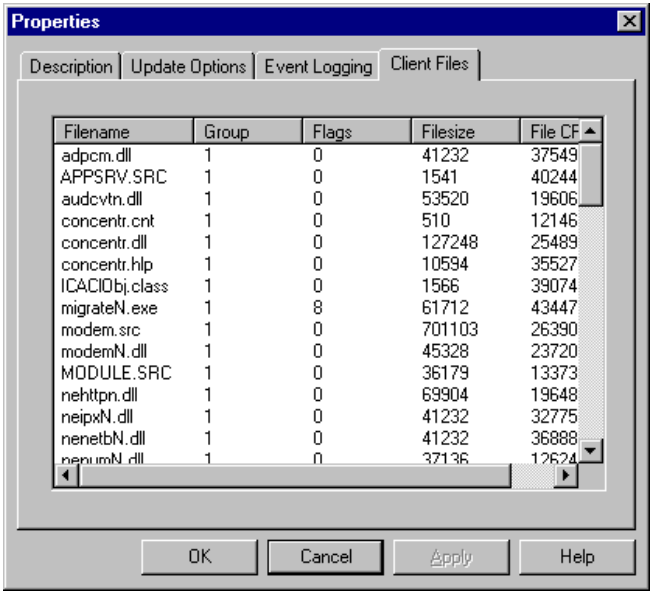
- Under **Client Download Mode**, select **Ask user** to give the user the choice to accept or postpone the update process. Select **Notify user** to notify the user of the update and require the client update. Select **Transparent** to update the user's ICA Client software without notifying or asking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

5. Use the **Event Logging** tab to configure logging settings for this client.



- Select the **Log Downloaded Clients** option to write an event to the event log when a client is updated.
- Select the **Log Errors During Download** option to write errors that occur during a client update to the event log.

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



The Client Update Database stores the following information about each client file: file name, group, flags, file size, and file CRC.

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

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+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.

To	Click	Note
Reposition 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 dialog boxes 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 application in the ICA Window 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**

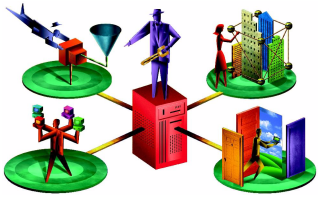
  1. From xv, copy the graphic.
  2. From the **ctxcapture** dialog box, click **From xv** and **To ICA**.
  3. When the transfer is complete, use the appropriate command in the ICA Client window to paste the information.

- **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**.
  3. When the transfer is complete, use the paste command in xv.

CHAPTER 7

Implementing Security Measures for the ICA Win32 Clients



This chapter discusses measures you can take to secure the communication between your Citrix server farm and the ICA Win32 Client. The following topics are covered:

- Using SOCKS to Direct ICA Traffic Through Firewalls
- Using SSL to Encrypt ICA Traffic

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 user name and password authentication.

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

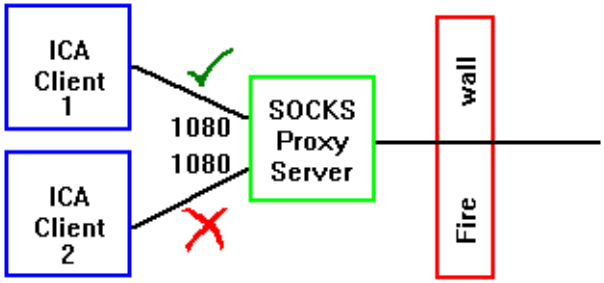
1. Be sure that your firewall is configured and working properly.
2. Install your SOCKS proxy server and test that it works with Web browsers.
3. Configure and deploy the ICA Win32 Client.

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.

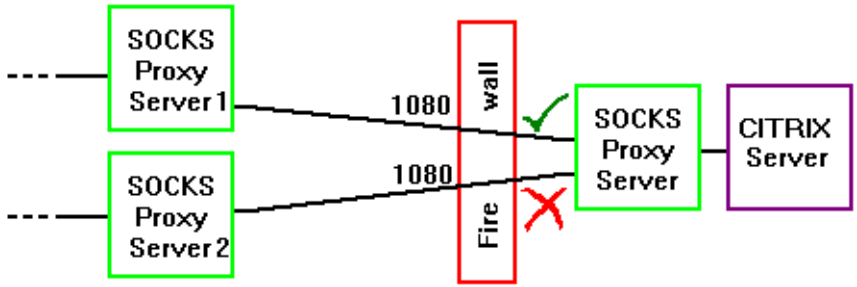


The proxy server uses its authentication features to determine whether ICA Clients can access networks outside the firewall. Configure the firewall to pass only network traffic that comes from the SOCKS proxy server.

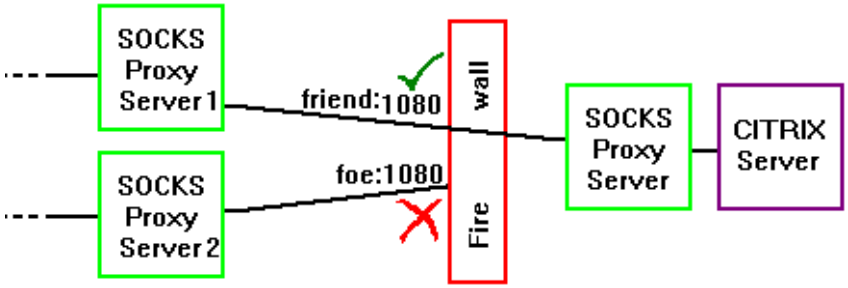
Setting Up a Proxy Between Citrix Servers and a Firewall (for Inbound Connections)

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 network traffic that is directed only to the SOCKS proxy server.



Using SSL to Encrypt ICA Traffic

Secure Sockets Layer (SSL) encryption of ICA traffic provides server authentication, encryption of the data stream, and message integrity checks. SSL is the security standard for communication across the Internet.

Citrix SSL Relay uses TCP port 443 by default to listen for SSL-secured connections. When the SSL Relay receives an SSL connection, it decrypts the data before redirecting it to the MetaFrame server, or, if the user selected SSL+HTTPS browsing, to the Citrix XML Service.

You can use Citrix SSL relay to secure communications:

- Between an SSL-enabled ICA Client and a MetaFrame server. Connections using SSL encryption are marked with a padlock icon in Citrix Connection Center.
- In an NFuse deployment, between the MetaFrame server and the NFuse Web server.

For information about configuring and using SSL Relay to secure your MetaFrame installation, see your Citrix server *Administrator's Guide*. For information about configuring the NFuse Web server to use SSL encryption, see the *NFuse Administrator's Guide*.

System Requirements

In addition to the system requirements listed for each ICA Win32 Client, you also need to ensure that the client device supports 128-bit encryption.

If you have Internet Explorer installed on your system, you can determine the encryption level of your system as follows:

1. Start Internet Explorer.
2. From the **Help** menu, click **About Internet Explorer**.
3. Check the Cipher Strength value. If it is less than 128-bit, you need to obtain and install a high encryption upgrade from the Microsoft Web site. Go to http://www.microsoft.com and search for "128-bit" or "strong encryption."
4. Download and install the upgrade.

If you do not have Internet Explorer installed, or if you are not certain about the encryption level of your system, visit Microsoft's Web site at http://www.microsoft.com to install a service pack that provides 128-bit encryption.

Important All secure systems need to be maintained. Ensure that you apply any service packs or upgrades that Microsoft recommends.

Configuring the ICA Win32 Clients to use SSL

The following section explains how to configure the ICA Win32 Program Neighborhood Client and the Program Neighborhood Agent to use SSL.

Important By default, Citrix SSL Relay uses TCP port 443 on the MetaFrame server for SSL-secured communication. If you configure SSL Relay to listen on a port other than 443, you must change the SSLProxyHost setting to reflect the new port number in the following situations:

- If the user is connecting to a published application accessed through an application set, change the SSLProxyHost setting in the user's local Appsrv.ini and Pn.ini files.
- If the user is connecting to a published application or MetaFrame server using a custom ICA connection, change the SSLProxyHost setting in the user's Appsrv.ini file.

To configure the ICA Win32 Program Neighborhood Client to use SSL

1. Make sure the client machine meets all system requirements outlined on page 27 and page 114 of this guide.
2. Open Program Neighborhood.
3. To configure an application set to use SSL, select the application set and click the **Settings** button on the Program Neighborhood toolbar.

   To configure an individual custom ICA connection to use SSL, select the custom connection in the custom ICA connection window and click the **Properties** button on the Program Neighborhood toolbar.
4. Select **SSL+HTTPS** from the Network Protocol list.
5. Add the fully qualified domain name of the SSL-enabled Citrix server(s) to the Address List.

To configure all custom ICA connections to use SSL

1. Right-click in a blank area of the custom ICA connection window.
2. Choose **Custom Connection Settings** from the menu that appears.
3. Select **HTTP/HTTPS** from the Network Protocol list.
4. Add the fully qualified domain name of the SSL-enabled Citrix server(s) to the Address List.
5. Click **OK** when you are done.

To configure the ICA Win32 Program Neighborhood Agent to use SSL

1. Make sure the client device meets all system requirements outlined on page 57 and page 114 of this guide.
2. To use SSL to encrypt application enumeration and launch data passed between the Program Neighborhood Agent and the NFuse server, configure the appropriate settings in the config.xml file on the NFuse server. The config.xml file must also include the machine name of the Citrix server hosting the SSL certificate. See chapter 6 of the *NFuse 1.6 Administrator's Guide* for more information about configuring the Program Neighborhood Agent to use SSL encryption.
3. To use secure HTTP, or HTTPS, to encrypt the configuration information passed between the Program Neighborhood Agent and the NFuse server, enter the URL of the NFuse server hosting the config.xml file in the format https://<*servername*> on the **Server** tab of the Program Neighborhood Agent **Properties** dialog box.

Installing Root Certificates on the ICA Win32 Clients

To use SSL to secure communications between SSL-enabled ICA Clients and the MetaFrame server, you need a root certificate on the client machine that can verify the signature of the Certificate Authority on the server certificate.

The Citrix ICA Win32 Clients support the Certificate Authorities that are supported by the Windows operating system. The root certificates for these Certificate Authorities are installed with Windows and managed using Windows utilities. They are the same root certificates that are used by Microsoft Internet Explorer.

If you choose to use a different Certificate Authority, you must obtain a root certificate from the Certificate Authority and install it on each client machine. This root certificate is then used and trusted by both Microsoft Internet Explorer and the Citrix ICA Win32 Client.

Depending on your organization's policies and procedures, you may want to install the root certificate on each client machine instead of directing end users to install it. If you are using Windows 2000 with Active Directory on all machines, you can deploy and install root certificates using Windows 2000 Group Profiles. See your Microsoft Windows 2000 documentation for more information.

Otherwise, you may be able to install the root certificate using other administration or deployment methods, such as:

- Using the Microsoft Internet Explorer Administration Kit (IEAK) Configuration Wizard and Profile Manager
- Using third-party deployment tools

Note The procedure outlined below assumes that your organization has a procedure in place for users to check the root certificate as they install it. It is important to verify the authenticity of a root certificate before installing it.

To install a root certificate on the Win32 client machine

1. Double-click on the root certificate file. The root certificate file has the extension .Cer, .Crt, or .Der.
2. Verify that you are installing the correct root certificate.
3. Click **Install Certificate**.
4. The Certificate Import Wizard starts. Click **Next**.
5. Choose the **Place all certificates in the following store** option, and then click **Browse**.
6. On the Select Certificate Store screen select **Show physical stores**.
7. Expand the Trusted Root Certification Authorities store and then select **Local Computer**. Click **OK**.
8. Click **Next** and then click **Finish**. The root certificate is installed in the store you selected.

Index

L

M

N

P

R

S

T

U

W

X