Citrix Presentation Server™ Client for Macintosh Administrator's Guide

Citrix Presentation Server™ Client for Macintosh, Version 10.*x*

Document Code: December 6, 2007 (AO)

Contents

Chapter 6 Configuring the User Interface

Chapter 7 Improving Performance

Chapter 8 Integrating the Client with Security Solutions

Before You Begin

Who Should Use this Guide

This guide is for system administrators responsible for installing, configuring, deploying, and maintaining the Client for Macintosh. The guide assumes knowledge of:

- Citrix Presentation Server
- The machine running Presentation Server to which the client connects
- The operating system on the client device (Mac OS X)
- Installation, operation, and maintenance of network and asynchronous communication hardware, including serial ports, modems, and device adapters

To make it easier to read, all the procedures in this guide refer to "you." In some circumstances "you" refers to the administrator of the client, in others to the user of the client, and sometimes to both. The context indicates whether a procedure is primarily an administrator or user activity.

How to Use this Guide

To get the most out of this guide, review the table of contents to familiarize yourself with the topics discussed.

This guide contains the following sections:

Topic	Contents
This section	Introduces the *Client for Macintosh Administrator's Guide*
Introducing the Citrix Presentation Server Client for Macintosh	Gives a detailed list of features and an overview of how the client works
Deploying the Client for Macintosh	Describes how to install and deploy the client

Topic	Contents
Configuring Connections to Servers and Applications	Describes how to configure connection properties and device mappings for the client
Running Applications, Accessing Desktops, and Working in Sessions	Describes how to use connection files to open files in published applications and access remote server desktops
Configuring the User Interface	Describes how to customize the appearance and behavior of client sessions
Improving Performance	Gives recommendations for methods to speed client processing and improve efficiency
Integrating the Client with Security Solutions	Describes how to integrate the client with security technologies such as proxy servers, firewalls, and systems based on Secure Sockets Layer/Transport Layer Security (SSL/TLS)

Accessing Product Documentation

This guide is part of the Presentation Server documentation set and contains conceptual information and installation and configuration steps for the client.

Apple Help is provided for some tasks within the client and Citrix ICA Client Editor. This is shipped with the client software and accessed from the client and ICA Client Editor menu bars, and by using COMMAND+SHIFT+? in the ICA Client Editor.

The documentation for Presentation Server includes online documentation, known issues information, and application Help, as follows:

- Use *Welcome to Citrix Presentation Server* (Read_Me_First.html) to access the complete set of online guides on the Web. Alternatively, to access the documentation at any time, go to http://support.citrix.com. Online documentation is provided as Adobe Portable Document Format (PDF) files.
- Known issues information is included in the product readme, also available on the Web. Use *Welcome to Citrix Presentation Server* (Read_Me_First.html) to access the product readme.
- For information about terminology related to Presentation Server, see the *Citrix Presentation Server Glossary*, available from the Knowledge Center at http://support.citrix.com.
- More information about Citrix documentation, and details about how to obtain further information and support, is included in *Getting Started with*

Citrix Presentation Server, available from the Knowledge Center at http://support.citrix.com.

Note: To provide feedback about the documentation, go to http://www.citrix.com and click **Support > Knowledge Center > Product Documentation**. To access the feedback form, click the **Submit Documentation Feedback** link.

Introducing the Citrix Presentation Server Client for Macintosh

Overview

When connected to a server, the Client for Macintosh provides features that make remote computing just like running applications on a local desktop.

Topics covered in this section include:

- The client architecture
- Features of the Client for Macintosh

You use the client to access remote servers and applications available on those servers, even those running on operating systems other than Macintosh OS X. You can run the applications on the server and see them display locally in a window on your own desktop. The window displays either the remote server desktop, from where you can open any available application, or displays a specific application (called a *published application*) that runs on the remote server.

Architecture

The diagram below shows how the different elements of the client interact with each other and the server in order to display remote applications on the Macintosh screen.

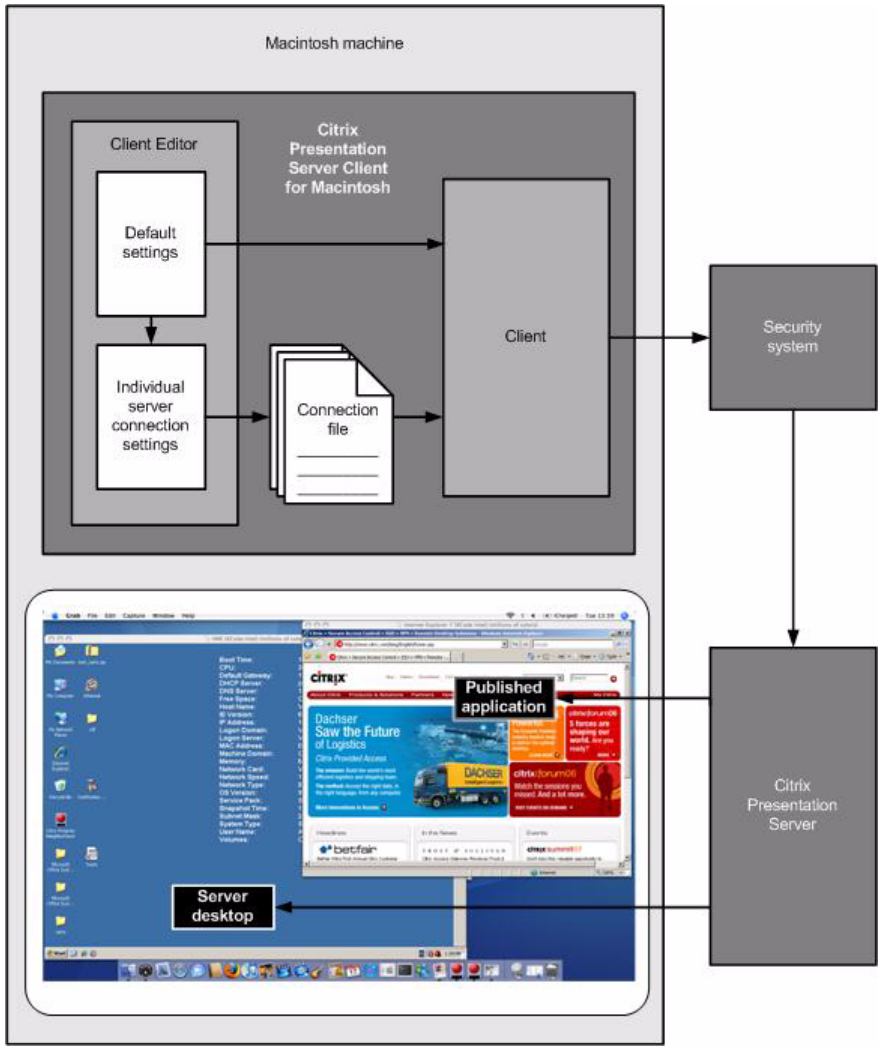

Figure showing the Client for Macintosh's place in a Citrix Presentation Server system

Using the Client

There are two ways of using the client to gain access to Presentation Server applications and content

- You can use the Web Interface to connect through a standard Web browser, or, in the case of Citrix Web Interface for Microsoft Sharepoint, a standard SharePoint environment. Once the client is installed, all the user needs to

do is navigate to a certain page, enter their credentials if required, and click an icon in the list of available resources to start a session.

- You can use the ICA Client Editor to configure a connection to a particular application, server, or group of servers. The ICA Client Editor saves this information as a connection file. You can use the ICA Client Editor to set default values for each connection or build a tailored suite of server desktop and published application connections. If you want to amend any of the settings, use the ICA Client Editor to reconfigure connections.

  When you open the connection file the client connects to the server. This information might go through various security systems such as firewalls and proxy servers before it reaches the server. The server then runs the desktop or published application, but displays it on your client device as though it were an application on your hard disk.

  This document focuses on creating and configuring connection files.

Client for Macintosh Features

Note: SpeedScreen Latency Reduction, audio mapping, time zone support, encryption, automatic reconnection, and support for smart card features are available only when connecting to computers running Presentation Server for Windows and not computers running Presentation Server for UNIX.

New Features at This Release

- **Improved printing.** The user can now use the local Macintosh **Print** dialog box to control output, and use any printer to which they can connect.
- **Kerberos support.** Users can now connect to servers and applications using the Kerberos authentication protocol, and therefore avoid entering their credentials whenever they try to connect.
- **Improved graphics performance.** Using Citrix's SpeedScreen Image Acceleration technology, the connection now uses less bandwidth when displaying graphics.
- **Session reliability.** If the connection to a server is lost, the user can continue to see the session while the client tries to reconnect.
- **Encryption.** This release offers Citrix's SecureICA technology as an alternative means of encryption.

Connection Features

- **Automatic reconnection.** If the client disconnects from a server unexpectedly, it attempts to reconnect automatically. See "Reconnecting to Servers after a Disconnection" on page 40 for more information.
- **Multiple session support.** Users can run multiple connections concurrently.
- **Alternate addresses when connecting to servers across firewalls.** Users can use an alternate address when connecting to a server across a firewall for individual connections. See "Connecting to a Server through a Firewall" on page 62.
- **Per-connection browsing.** Users can specify a server for a particular connection in order to define specific network protocols and servers, or change security settings, for each connection. See "Identifying a Desktop or Application to Connect to" on page 24.
- **File type association.** You can map file extensions to published applications so that ICA sessions are launched automatically using the correct application when a file is opened. See "Opening a File in a Specific Application" on page 33.
- **Local clipboard integration.** Users can cut and paste objects between applications running locally on the client device and applications running remotely in an ICA session.

  Pasted RTF text may not look identical to the text that was copied. If a font is not available on the platform users paste the RTF text to, the application uses a compromise font on that platform.

User Interface Features

- **Dock and menu bar auto-hide.** When a session is running in full screen mode, you can keep the menu bar and Dock out of the way and only show them when you move your mouse to the top of the screen or whichever edge the Dock is located. See "Showing and Hiding the Menu Bar and Dock" on page 46 for more information.
- **Recent items option.** To enable users to find connection files more easily, a list of recently used items is available in both the client and ICA Client Editor File menus.
- **Multi-button mouse support.** The client recognizes three buttons (left, right, and center) on a multi-button mouse. It also recognizes when a wheel is used as a center button and supports all wheel scrolling functions.

Note: The client does not support cursor feedback. This means, for example, that if an administrator is controlling what is happening in the session window, the user might see a menu open, but the cursor on that user's computer would not move to track the administrator's mouse movement.

- **Printing.** Printing uses the Citrix Universal Printer Driver technology so that applications running remotely on the server can print to local printers. For more information, see "Printing" on page 39.
- **PC key mapping.** Users can use special key combinations to mimic PC keys not available on standard Macintosh keyboards and to replicate mouse actions. See "Configuring Hotkeys" on page 47.
- **Time zone support.** Sessions on servers in a different time zone reflect the time zone of the client device, as set in the computer's System Preferences dialog box.

  For example, a user in London logs on to a server in the USA and launches Microsoft Outlook as a published application. Microsoft Outlook stamps emails sent during this session with the user's London time zone information.

  The time zone displayed may be different from the user's actual location because the server uses the first country in the alphabetically ordered list for that time zone. Users in Helsinki will see their time zone reported as Athens because both are GMT +2:00.
- **Seamless windows.** As well as configuring sessions to run in windows of a fixed size, you can choose the *seamless* mode to display applications and desktops in a fully resizeable window.

Security Features

- **Support for smart cards.** You can use smart cards to provide authenticating credentials when logging on to a server. See "Creating a Basic Connection File" on page 23 for more information about using smart cards with the client.

  You may also need to install proprietary software to use smart card readers.
- **Secure proxy server support.** As an alternative to using a SOCKS proxy, the client also supports using a Secure Proxy Server. For more information, see "Configuring the Client to Work with a Proxy Server" on page 57.

- **Secure Sockets Layer (SSL) support.** SSL provides server authentication, encryption of the data stream, and message integrity checks. See "Integrating the Client with the Secure Gateway or SSL Relay" on page 59.
- **Transport Layer Security encryption.** As an alternative to Secure Sockets Layer (SSL) 3.0, the client also supports Transport Layer Security (TLS) 1.0. See "Configuring SSL/TLS" on page 60.
- **NDS support.** When users launch the client, they can log on and be authenticated using their Novell Directory Services (NDS) credentials. Supported NDS credentials are user name (or distinguished name), password, directory tree, and context.
- **Encryption**. The client supports different levels of encryption, including RSA RC5 encryption.

Mapping Features

- **Client device mapping.** The client supports client device and COM port mapping to allow you to access devices attached to the client computer during an ICA session. See "Mapping Client Devices" on page 28 and "Mapping Client COM Ports" on page 30.
- **Client drive mapping.** Client drive mapping allows you to access the local disk drives of the client computer during an ICA session. See "Mapping Client Drives" on page 28.
- **Client audio mapping.** Client audio mapping allows the client computer to play sounds generated by applications running on the server. See "Mapping Client Audio" on page 31.

Performance Improvement Features

- **SpeedScreen Browser Acceleration.** SpeedScreen Browser Acceleration, available to users running Internet Explorer 5.5 or later within a session, increases the rate at which images are downloaded and displayed. SpeedScreen Browser Acceleration must be enabled on the server to be available to the client—it does not work when running Internet Explorer locally. When enabled, SpeedScreen Browser Acceleration operates automatically; you do not need to configure the client.
- **Disk caching.** Disk caching stores locally those graphics that are used regularly, such as icons, fonts, and bitmaps. This avoids retransmitting data. See "Caching Images" on page 51.
- **Data compression.** Data compression reduces the amount of data sent over the communications link to the server. See "Compressing Data" on page 51.

- **SpeedScreen Latency Reduction.** SpeedScreen Latency Reduction accelerates the display of text input on the client computer and provides visual feedback to show that input is being processed. See “Reducing Display Latency” on page 53.
- **Business recovery support.** The client supports multiple server sites with different addresses for the same published application name. See “Configuring Business Recovery and Server Groups” on page 27.

Deploying the Client for Macintosh

Overview

This section describes how to install and deploy the Client for Macintosh. Topics covered in this section include:

- System requirements
- Installing the client
- Uninstalling the client

System Requirements

Users need equipment that meets these minimum requirements to run this release of the client:

- Either an Intel-based Macintosh running Mac OS X Version 10.4 or later, or a PowerPC-based Macintosh running Mac OS X 10.3 or later
- At least 128 MB of RAM
- 12 MB of free disk space
- A working network connection or a working Internet connection to connect to servers

Installing the Client for Macintosh

The client is available as a compressed disk image (**MacICA_OSX.dmg.zip**) on the Citrix Web site.

To install the client from the Citrix Web site

1. Download the file **MacICA_OSX.dmg.zip** and open it. This runs the Disk Utility program, which mounts the file as a disk image accessible from your

Macintosh desktop. This can happen automatically after downloading the **.zip** file, if your browser is set up to do so.

2. Double-click the **Citrix** icon and follow the instructions. (After installation, you might also want to put the client and ICA Client Editor in your Dock so they are easily available.)

Uninstalling the Client for Macintosh

To uninstall the client, delete the folder containing the client and ICA Client Editor.

If you want to remove cache files and any initial settings used by the client, delete the folder at /**Users**/*home*/**Library/Preferences/Citrix ICA Client**, where *home* is the name of the current user's personal Home folder.

Configuring Connections to Servers and Applications

Overview

This section describes how to create and edit connections between the client and server. Topics include:

- Starting the ICA Client Editor
- Creating a basic connection file
- Configuring network protocol and server location
- Changing connection file settings and default settings
- Mapping client drives, COM ports, and printers

About Connection Files

You can create two types of connections to clients: connections to server desktops and connections to published applications.

- A connection to a server desktop lets you access the desktop of a specified server. You can run any applications available on the desktop, in any order.
- A published application is a predefined application and its associated environment. The published application may be available on more than one server.

By using the default settings, you can quickly create a basic connection file (see “Creating a Basic Connection File” on page 23) and customize it in several ways, either when you are creating it or afterwards. The settings you edit can be used either as defaults for all connection files that you create subsequently or you can apply them just to a single file.

If a number of users all need to connect to the same server with the same settings, you can create one standard connection file and install this on each user’s computer.

You can change the following aspects of the client connection:

- The network protocol used to search for servers. See "Identifying a Desktop or Application to Connect to" on page 24.
- The servers the client can connect to. See "Configuring Business Recovery and Server Groups" on page 27.
- Client device mapping, which enables applications running on a server to access devices connected to the client. See "Mapping Client Devices" on page 28 and "Mapping Client COM Ports" on page 30.
- The application to run when the client connects to a server desktop. For details, see "Opening a Specific Application Using a Connection File" on page 38.
- The application used to open a particular file type. See "Opening a Specific Application Using a Connection File" on page 38.
- User interface settings such as the appearance of session windows and quality of sound. See "Configuring the User Interface" on page 45.
- Performance improvement features such as compressing data and reducing display latency. See "Improving Performance" on page 51.
- Security solutions such as connecting through proxy servers. See "Integrating the Client with Security Solutions" on page 57.

Starting the ICA Client Editor

You use the ICA Client Editor to create connection files. You can also place connection files, the client, and the ICA Client Editor in the Dock so they are easily available.

To start the ICA Client Editor

Do one of the following:

- Navigate to the folder where you installed the client and open **Citrix ICA Client Editor**.
- If you have added the ICA Client Editor to the Dock, click on the client icon in the Dock.

Creating a Basic Connection File

To create a connection file

1. In your client installation folder, open **Citrix ICA Client Editor**.

   The ICA Client Editor opens at the **Network Connection** pane.

2. To connect to a desktop, choose **Server**, or to connect to a published application, choose **Published Application**.

3. In the **Connect To** box, type the name or IP address of the server, or the name of the published application or content, or click **Browse** and choose the name from a list.

   Note: If your list of available servers changes, it is because you have access to more than one network and adverse loading conditions mean you are seeing a different set of servers.

   - In order to use Kerberos authentication, choose the **Kerberos Pass-through Authentication** option to connect automatically with the credentials configured in the Macintosh Kerberos application.
   - If you are using a smart card to log on to the server, choose the **Smart Card** option. For information about configuring security policy settings for smart card authentication, see the Presentation Server documentation.
   - Type the user name, the domain (if required), and the password in the appropriate boxes. If you leave these boxes blank, the client prompts for this information each time you make a connection using this file.

4. Click **Save**. Choose a location in which to save the connection file. By default, the **Save** box displays the server or published application name, but you can give the file a different name.

   If you do not save the connection settings, they are lost when you exit the ICA Client Editor or open another connection file. However, you can still make a connection to a server without saving the settings.

5. To start the ICA session immediately, click **Connect**.

6. To exit the ICA Client Editor, click **Quit**. If you did not save the connection details, a dialog box appears prompting you to save them now.

Identifying a Desktop or Application to Connect to

You need to take the following two steps to find the desktop or application you want to use.

1. Identify a server that acts as the master browser. This server contains the list of available desktops and applications and their locations.
2. View the list and choose the desktop or application you want. The master browser then directs the client to the requested desktop or application.

See the Presentation Server documentation for instructions about how to configure a server to act as a master browser.

The way server location works depends on which network protocol is configured:

- For **TCP/IP+HTTP** and **SSL/TLS+HTTPS**, you must set specific server addresses for the servers. The client uses the HTTP or HTTPS protocol to contact these servers. If you choose to use HTTP, the server must be running Presentation Server in interoperability mode.
- For **TCP/IP**, the default setting for server location is **Auto Locate**. The client attempts to contact all of the servers on the network by broadcasting on the User DataGram Protocol (UDP). Alternatively, you can set specific addresses for servers.

To configure a default master browser server for all connections

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.

   The **Default Settings** dialog box opens at the **Making a Connection > Server Location** pane.
2. Choose the network protocol you want to use.

   The network protocol setting lets you control the way the client searches for servers and how it communicates with them.

   The protocols are:

   - **TCP/IP.** The client uses UDP to search for servers. The client communicates with the server using the ICA protocol over TCP/IP.
   - **TCP/IP+HTTP.** The client uses the HTTP protocol to search for servers. The client communicates with the server using the ICA protocol over TCP/IP. This is the default protocol but it can be used

only with servers running Presentation Server in interoperability mode.

- SSL/TLS+HTTPS. The client communicates with the server using the SSL/TLS protocol. This protocol is described in more detail in "Integrating the Client with the Secure Gateway or SSL Relay" on page 59.

3. Click **Add**.

   You can specify groups of servers for each protocol. See "Configuring Business Recovery and Server Groups" on page 27.

4. In the **Server Address** box:

   - If you choose TCP/IP to be the network protocol, choose or type the name of the server.
   - If you choose TCP/IP+HTTP or SLL/TLS+HTTPS to be the network protocol, type the fully qualified domain name (FQDN) of the server and type a port number if different from the default 80.

   For more information about fully qualified domain names, see "The Secure Gateway" on page 59.

5. Click **OK** and then click **Save**. Any changes you make affect all connection files configured to use the default server.

To configure a master browser for an individual connection

1. Do one of the following:

   - From the ICA Client Editor **File** menu, choose **Open** and choose the connection file you want to edit.
   - Drag and drop the connection file onto the ICA Client Editor icon.

2. If you want to connect using a protocol other than the default one, make sure the **Network Protocol > Use Default** check box is cleared.

   The network protocol shown depends on the current connection settings. If you did not change these settings for this connection file, they show the default settings.

   - If the default is set up for secure communications (SSL/TLS), the **Network Protocol > Use Default** check box is selected and the list of protocols displays SSL/TLS+HTTPS

- If the default is set up for normal connections (that is, not using SSL/TLS), the **Network Protocol > Use Default** check box is selected and the list of protocols displays TCP/IP or TCP/IP+HTTP

Choose the protocol you want to use to communicate with the server from the drop-down list. The options are:

- **TCP/IP.** The client uses UDP (User DataGram Protocol)
- **TCP/IP+HTTP.** The client uses the HTTP protocol
- **SSL/TLS+HTTPS.** The client uses the SSL/TLS protocol

3. Make sure the **Server Location > Use Default** check box is cleared.
4. Type the full name of the server. If you chose SSL/TLS+HTTPS as the network protocol, type the fully qualified domain name (FQDN) of the server; for example, `winston.secure.company.com`.

   For more information about fully qualified domain names, see "The Secure Gateway" on page 59.
5. Click **Save**. Any changes you make affect only this specific connection file.

To find the application or desktop to connect to

1. Do one of the following:

   - From the ICA Client Editor **File** menu, choose **Open** and choose the connection file you want to edit.
   - Drag and drop the connection file onto the ICA Client Editor icon.

   The file opens at the **Network Connection** pane.
2. Choose either **Server** or **Published Application**.
3. Click **Browse** to see a list of servers or applications. If you know the name of the server or application you want, you can enter its name in the **Connect To** box without having to browse the list.
4. Choose the server or application from the list and click **Select**.

   The name of the selected server or application appears in the **Connect To** box. When you save the connection file (or click **Connect**), this server or application opens when you start an ICA session.

Configuring Business Recovery and Server Groups

Business recovery provides consistent connections to published applications in the event of a master browser server disruption. You can define up to three groups of servers: a primary and two backups. Each group can contain up to five servers.

When you configure business recovery, the client attempts to contact all the servers within the Primary group simultaneously; the first server to respond acts as the master browser. If none of the servers responds, the client attempts to contact all the servers within the Backup 1 group. If there is still no response, the client attempts to contact all of the servers in the Backup 2 group. When a server responds, the client queries the server for the address of the server on which to run the published application. This process is repeated each time the user attempts to make a connection.

By default, the client uses the TCP/IP+HTTP protocol. You can change the protocol and specify business recovery server addresses. Whichever protocol you choose applies to all connections and cannot be configured for individual servers or groups.

To configure a business recovery server group

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. On the **Making a Connection** > **Server Location** pane, look at the **Server Group > Address List** and choose the server group you want to configure.

   You can specify separate server groups for each protocol.
3. Click **Add** to add a server to the selected group.
4. In the **Server Address** box:
   - For TCP/IP: choose or type the name of the server.
   - For TCP/IP+HTTP and SSL/TLS+HTTPS: type the name of the server and type a port number if different from the default 80.
5. Add more servers as necessary. You can have a maximum of five servers in a group.
6. Click **Save**.

Mapping Client Devices

The client supports client device mapping for connections to servers. Client device mapping allows a remote application running on the server to access devices attached to the local client.

This section includes more information about:

- Mapping client drives
- Mapping client COM ports
- Mapping client audio

For information regarding mapping client printers, see "Printing" on page 39.

Note: Presentation Server for UNIX does not support client audio mapping.

Mapping Client Drives

Because Windows operating systems recognize file paths with drive letters but not Macintosh paths, the client needs to map local Macintosh folders to drive letters for published applications and remote desktop sessions to locate local files.

Client drive mapping allows you to access the local disk drives of the client, including CD-ROM drives, during ICA sessions. When a server is configured to allow client drive mapping, users can access their locally stored files, work with them during their ICA sessions, and then save them either on a local drive or on a drive on the server.

For example, to use the files in the Macintosh HD/MacClientDocs/Docs/MacPDF folder, you can map Macintosh HD/MacClientDocs/Docs to drive M and within a session access the files using the path M:\MacPDF.

In addition, you can configure servers to map their server drives. When server drives are mapped and the drive letters clash with those selected for the user's local drives, the server automatically changes the client drive letters.

To map a folder on the Macintosh hard disk for an ICA session

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Drives and Devices > Drive Mapping** > **Enable Drive Mapping**.

   For each server drive letter, the **Drive Mapping** list shows the disk or path name of the Macintosh folder mapped to the drive. In the **Enabled/Read/**

Write column, icons display each mapped drive that is enabled for use and what type of access users have to the drive. Items that are no longer available do not display a folder icon.

Icons that include a question mark indicate that a drive mapping has "query" permissions. This is a security feature that means when any application tries to read from or write to the folder, a dialog box appears asking whether you want to allow or deny access. If you choose **Deny**, access will be denied for the duration of the connection. In order to remove the deny permission, close or disconnect the session and restart.

Drives A, B, and C are mapped automatically as follows:

Drive:	Mapped to:
A	A Macintosh removable media drive (floppy disk, USB flash drive, or any other item that is removable and can be written to). Where there is more than one removable drive, users can change the one to which drive A is mapped from within an ICA session: From the Drives menu, choose Client A Diskette to display the options and choose the required drive.
B	The Macintosh internal CD or DVD drive, or any other item that is removable and non-writable, such as a disk image .dmg file. Where there is more than one such item, users can change the one to which drive B is mapped from within an ICA session: From the Drives menu, choose Client B CDROM to display the options and choose the required item.
C	Permanently mapped to the user's Home folder on the Macintosh hard disk.

3. Choose an available drive letter.
4. Click **Browse**. Choose the folder on the Macintosh hard disk to map and click **Choose**. The **Drive Mapping** pane now displays the mapped folder. If the drive letter selected is not available on the server, the specified folder is mapped to another free drive letter.
5. Click **Save**.
6. Log off from any open ICA connections and reconnect.

Note: There is no way of ejecting removable media from within the client. To eject a CD or other item, use the standard Macintosh methods.

To turn drive mapping off for a specific connection file

1. In the ICA Client Editor, open the connection file you want to edit.

2. From the **Connection Properties** tab, choose **Turn Drive Mapping Off for this Server**.
3. Click **Save**.

To ensure that client drive mapping works with filenames containing accented characters (for example, é), set the client DOS code page to 1252. You can do this by changing a setting in the server registry.

Caution: Using Registry Editor incorrectly can cause serious problems that require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

Set the registry entry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage\OEMCP

to **1252**.

However, within a console window, you may then need to set the code page back to the original value of the server registry entry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage\OEMCP

You can do this using the **CHCP** command. This ensures that DOS applications can display characters correctly and accept ALT+numeric entries from the keypad.

Mapping Client COM Ports

Client COM port mapping lets you access serial devices connected to the client device. Applications running remotely on the server can use local devices such as modems and serial port printers.

Note: Client COM port mapping is not TAPI compatible. Applications that communicate with devices using TAPI are not supported

---

Macintosh serial ports do not provide all the control signal lines that are used by Windows applications. The DSR (Data Set Ready), DCD (Device Carrier Detect), RI (Ring Indicator), and RTS (Request To Send) lines are not provided. Windows applications that rely on these signals for hardware handshaking and flow control may not work. The Macintosh implementation of serial communications relies on CTS (Clear To Send) and DTR (Data Terminal Ready) lines for input and output hardware handshaking only.

To map a client COM port

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Drives and Devices > COM Port Mapping**.
3. Choose the COM port you want to configure.

   This is a virtual client COM port that is displayed in the ICA session. It does not refer to a physical port on the local machine.
4. Click **Modify** to display the **Select Serial Port** dialog box.
5. Choose the physical port to associate with the selected COM port and click **Select**.
6. Repeat steps 3 through 5 to map other ports as necessary and then click Save to save the new settings.
7. Start the client and log on to a server.
8. To start a command prompt, click **Start > Programs > Accessories > Command Prompt**.
9. 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 (ports 1 through 4 are available).
10. To confirm the mapping, type net use at the prompt. A list displays mapped drives, LPT ports, and mapped COM ports.

You can now use this mapped COM port as you would a COM port on the client.

Mapping Client Audio

Client audio mapping lets applications running on the server play sounds through the client device.

Note: Client audio mapping is not available when you connect to computers running Presentation Server for UNIX.

Three different audio quality settings are available. The higher the audio quality, the more bandwidth is required to transfer the audio data. Higher quality audio also uses more server CPU to process.

You can set the audio quality or turn client audio mapping on or off on the server. You can set the audio quality or turn client audio mapping on or off for each connection file. If the client and server audio quality settings are different, the lower of the two qualities is used.

The audio quality options are:

- **High.** This setting is recommended only for connections where bandwidth is plentiful and sound quality is important. It allows clients to play a sound file at its native data rate. Sounds at the highest quality level require about 1.3 Mbps 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 64 Kbps. This compression results in a moderate decrease in the quality of the sound played on the client. The host CPU utilization decreases compared with the uncompressed version because of the reduction in the amount of data being sent.
- **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 16 Kbps. This compression results in a significant decrease in the quality of the sound. The CPU requirements and benefits of this setting are similar to those of the Medium setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

To turn client audio on or off on a server

From the **ICA Settings** dialog box on the server, administrators can turn client audio on or off by choosing the appropriate option. See the Presentation Server documentation for details.

To turn audio mapping on for a specific connection

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Connection Properties** tab, choose **Enable Sound**.
3. Set **Quality** to **High**, **Medium**, or **Low**, depending on available bandwidth.

Opening a File in a Specific Application

You can assign certain files and file types to specific applications so that the appropriate published application starts automatically when you open a file on your computer. For example, while working on files using a published Windows application on a client, you can work on PC files that you can save to the Macintosh hard disk.

Using file type association, you can open files either by

- Dragging the file icon to the client icon configured to connect to the appropriate published application
- Choosing **File > Open** or double-clicking the file icon to open the published application with your file in it

You need to configure a number of settings on both the server and the client.

Configuring the Server

You need to complete these preliminary tasks for file type association to work:

- Set extended parameter passing, if necessary.
- Identify the server drive letter that is mapped to the client hard disk and tell users so they can map their hard disk or document folder to the correct server drive letter.

Extended Parameter Passing

The server administrator may need to set up the published application to receive and use the file name by appending the parameter "%*" to the command line; for example, **powerpoint "%*"**. Using speech marks ensures that spaces in file names and paths are catered for.

Full details about how to publish applications and set up commands, and information regarding whether or not this parameter is needed for the server you are using, are in the Presentation Server documentation.

Server Drive Mapping

Servers map client drives to drive letters automatically when a client logs on. The server tries to match the client drives to client drive letters, typically A for the first floppy drive, B for the CD or DVD drive, C for the current user's Home folder, and so on. If these letters are already used for drives on the server, the server uses other letters. Machines running Presentation Server start at V and search in ascending order for free drive letters.

Configuring the Client

Client Drive Mapping

For file type association to work, a file must be within a folder that can be accessed through client drive mapping. For example, if client drive mapping is enabled for the C Drive, which is always mapped to the current user's Home directory, file type association will work for all files within the Home directory.

For more information about drive mapping, see "Mapping Client Devices" on page 28.

To view mapped client drives when connected to a server desktop

From within the ICA session, open the **My Computer** window from the desktop to display a list of mapped drives.

Associating the file type

To associate the file type (as identified by its extension) with a published application, you must use the ICA Client Editor to associate the file type with a connection file. This enables you to open a file in a specific application by dragging the file on the client icon. In order to open a file in a specific application by double-clicking on it, or by using the keyboard, you must also use Macintosh functions to associate the file or file type with the client.

To associate a file type with a published application

1. Create a connection file that connects to the published application you want to use. (See "Creating a Basic Connection File" on page 23.)
2. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
3. Choose **Making a Connection > File Type Association** to see a list of current associations.
4. Click **Add** to open the **File Type Association** dialog box.
5. In the **Extension** box, type the file type (extension); for example, **PPTX** for Microsoft PowerPoint files.
6. Click **Browse** to see a list of files, folders, and connection files on your Macintosh.
7. Choose the folder containing the connection file you created in Step 1 above. Choose the connection file and click **Open**. The connection file name appears in the **Map to Connection File** box.

8. Click **OK** to confirm. To remove or change the association, choose the association to make the **Remove** and **Change** buttons active and then click the relevant button.
9. Click **Save** to exit and confirm the association you have just set up.

   You can now open files in an associated application by dragging and dropping them onto the client. If you want to open files in an associated application by double-clicking or using the keyboard, you must perform the following additional steps.
10. Choose a file of the relevant type.
11. From the **Finder** menu bar, choose **File > Get Info > Open with > Other** and choose **Citrix ICA Client**.

    By default, only the selected file opens the associated application. If you want all files of this type to open in the application, choose **Change All**.

Running Applications, Accessing Desktops, and Working in Sessions

Overview

This section describes how to use the client. Topics in this section include:

- Starting an ICA session
- Configuring *file type association* to access published applications
- Opening a specific application using a connection file
- Printing from a published application
- Using the Macintosh keyboard to make PC keystrokes
- What happens when you get disconnected from the server

Starting an ICA Session

After you create one or more connection files (or complete connection details in the ICA Client Editor), you can start an ICA session.

When you start an ICA session, you may see additional messages or warnings displayed on your screen, depending on the requirements of the application you are opening. For example, some applications require read/write access to a directory on your local hard disk (for example, the Home directory) and you may get a dialog box asking you to deny or allow access. If you deny access, you may have trouble using the application if it needs to access local files.

To start an ICA session

Do one of the following:

- Double-click the connection file, or single-click the connection file if it is in the Dock.
- Drag and drop the connection file onto the client icon.

- Open the client. From the **File** menu, choose **Open Connection** and choose the connection file you want to open.
- Open the ICA Client Editor. From the **File** menu, choose **Open** and choose the connection file you want to open. On the **Network Connection** pane, click **Connect**.
- If you configure file type association, you can start an ICA session by dragging the file onto the ICA Client Editor icon. (See "Opening a Specific Application Using a Connection File" on page 38.)
- If you opened connection files in the past, open the ICA Client Editor. From the **File** menu, choose **Open Recent** and choose the connection file you want to open from the list. On the **Network Connection** pane, click **Connect**.

Note: If you cannot connect to a server, you may need to change the Server Location (see "Configuring Business Recovery and Server Groups" on page 27) or proxy server details (see "Configuring the Client to Work with a Proxy Server" on page 57).

Opening a Specific Application Using a Connection File

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

If you specify an application, you cannot run any other application in the ICA session nor access the server desktop.

To specify application properties for a connection file

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Application** tab, specify the path and file name of the application to be executed after connecting to the server.

   For example, to launch Microsoft Word automatically after connecting to the server, type **c:\winword\winword.exe**.
3. If necessary, type the working directory to be used for the application in the **Working Directory** box.

Printing

You can access printers connected to client devices during an ICA session. When a server is configured to allow client printer mapping, applications running remotely on the server can print to any printer that can be used from locally running applications. For information about configuring printer mapping, see the *Citrix Presentation Server Administrator's Guide*.

No special configuration is needed to set up local printers to print during an ICA session. You can choose to print using the dialog box within the session, or use the remote printing dialog box followed by the standard Macintosh printing dialog box and its additional printing options.

Important: A4 pages might not print correctly if the user chooses the **A4** paper size option in the **Page Setup** dialog box (or the Page Layout tab in the case of Microsoft Office 2007 applications). In order to print on A4 paper, the user must either specify it as a default size and use the **A4** paper size option, or choose the **A4 210×297** option if available. To set A4 as the default, from the client menu, choose **File > Default Paper Size > A4**.

All other paper sizes will print correctly if the printer supports that paper size.

You can also turn printing off for a specific connection file.

To print using the Macintosh Print dialog box

From the client menu, choose **File > Enable Print Dialog**.

To turn printing off for a specific connection file

1. Before you make the connection, open the connection file you want to edit in the ICA Client Editor.
2. From the **Connection Properties** tab, choose **Turn Printer Mapping Off for this Server**.
3. Click **Save**.

Note: In some circumstances, when you connect to the server, the Macintosh Printer icon is still present even though you turned printer mapping off. However, if you try to print, you see a Windows error message saying there is a problem when trying to print and printing is not possible.

For information about mapping peripherals other than printers, see "Mapping Client Devices" on page 28.

Reconnecting to Servers after a Disconnection

You can be disconnected from ICA sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the automatic client reconnection feature, the client can detect unintended disconnections and automatically reconnect users to the affected sessions.

When this feature is enabled on a machine running Presentation Server, you do not have to reconnect manually. Instead, a message box appears indicating that automatic reconnection is under way, and the client tries to reconnect until it is successful or the user cancels the reconnection attempts. If you require users to be authenticated again, a dialog box requesting credentials appears during automatic reconnection. Automatic reconnection does not occur if you exit applications without logging off.

Please refer to the Presentation Server documentation for information on how to implement automatic client reconnection.

Session Reliability

With the session reliability feature, users continue to see a published application's window if the connection to the application experiences an interruption, and no message box explaining that the client is trying to reconnect appears for three minutes (at which stage the user can cancel the reconnection attempt). For example, wireless users entering a tunnel may lose their connection when they enter the tunnel and regain it when they come out on the other side. During such interruptions, the session reliability feature enables the session window to remain displayed while the connection is being restored.

To reduce the likelihood that users continue to click links or type text while the connection is being restored, mouse pointers become hourglass icons while the application is unresponsive.

To turn session reliability on for a specific connection

1. In the ICA Client Editor, open the connection file.
2. From the **Connection Properties** tab, under **Session Reliability**, choose **Enable** and enter the port number to which you want to connect. If the session reliability feature is enabled, the default port used for session communication with the server changes from 1494 to 2598. Please refer to the Presentation Server documentation for information on how to change the port used for session reliability.
3. Click **Save**.

Making Keystrokes with Macintosh Keyboards

Remote sessions recognize most Macintosh keyboard combinations for text input, such as Option-G to input the copyright symbol ©. However some keystrokes the user makes during a session do not appear on the remote application or desktop, and instead are interpreted by the Macintosh operating system. This can result in keys triggering Macintosh responses instead (for example, F9 can be configured to run the All Windows feature of Exposé).

The user might also face the problem of wanting to use certain PC keys, such as INSERT, that many Macintosh keyboards do not have.

Keyboards and the ways keys are configured can differ widely between machines. The client therefore offers several choices to ensure that keystrokes can be correctly sent to desktops and applications running within a session. These are listed in the table below.

Conventions used in the table:

- Letter keys are capitalized and do not imply that the Shift key should be pressed simultaneously.
- Hyphens between keystrokes indicate that keys should be pressed together (for example, Control-C); spaces between keystrokes indicate that keys should be pressed and released before pressing the next key (for example, Option-Escape T means the user should press Option and Escape together, and then release the keys and press T).
- *Character keys* are those that create text input and include all letters, numbers, and punctuation marks; *special keys* are those that do not create input by themselves but act as modifiers or controllers. Special keys include Control, Alt, Shift, arrow keys, and function keys.
- Menu instructions relate to the menus in the client session.
- Depending on the the configuration of the machine, some key combinations might not work as expected, and alternative combinations are listed.
- *Fn* refers to the Fn (Function) key on a Macintosh keyboard; *function key* refers to F1 to F12 on either a PC or Macintosh keyboard.

PC key	**Macintosh options**
ALT+character key	Command–Option–character key (e.g. to send ALT-C, use Command-Option-C)
ALT+special key	Option–special key (e.g. Option-Tab) Command–Option–special key (e.g. Command-Option-Tab)

PC key	Macintosh options
CTRL+character key	Command–character key (e.g. Command-C) Control–character key (e.g. Control-C)
CTRL+special key	Control–special key (e.g. Control-F4) Command–Control–special key (e.g. Command-Control-F4
CTRL/ALT/SHIFT combination + function key	Option-Escape Control/Option/Shift–function key Choose **Keyboard > Send Function Key > Control/Alt/ Shift-function key**
CTRL+ALT	Control-Command
CTRL+ALT+DEL	Control–Option–Forward Delete Control-Option-Fn-Delete (on MacBook keyboards)
DELETE	Delete Option-Escape D Choose **Keyboard > Send Special Key > Delete** Fn-Backspace (Fn-Delete on some US keyboards)
END	End Fn-Right Arrow
ESC	Escape Option-Escape E Choose **Keyboard > Send Special Key > Escape**
F1 to F9	F1 to F9 Option-Escape 1 to 9 Choose **Keyboard > Send Function Key > F1 to F9**
F10	F10 Option-Escape 0 (zero) Choose **Keyboard > Send Function Key > F10**
F11	F11 Option-Escape hyphen Choose **Keyboard > Send Function Key > F11**
F12	F12 Option–Escape equal sign Choose **Keyboard > Send Function Key > F12**
HOME	Home Fn–Left Arrow

PC key	Macintosh options
INSERT	Option-Escape I Command-Help Choose **Keyboard > Send Special Key > Insert**
NUM LOCK	Clear Fn-6
PAGE DOWN	Page Down Fn–Down Arrow
PAGE UP	Page Up Fn–Up Arrow
SPACEBAR	Option-Escape S Choose **Keyboard > Send Special Key > Space**
TAB	Option-Escape T Choose **Keyboard > Send Special Key > Tab**

About Client Keyboard Support

The client has two keyboard modes: *Enhanced* keyboard support, for extra options and easier ways to use special keys such as function keys in Windows applications, and *Standard* keyboard support, as used by older client versions. The user selects the preferred keyboard mode using the **Keyboard** menu during a client session.

Enhanced keyboard support comprises a set of three features that can be turned on and off using the client's **Keyboard** menu.

- **Send Special Keys Unchanged** enables the user to send keys to remote sessions without additional keystrokes.
- **Use Command Key for Control Characters** enables the user to send Command-character key combinations as CTRL+character key combinations.
- **Use Command-Option for Alt Characters** enables the user to send Command-Option-key combinations as ALT+key combinations.

Standard keyboard mode enables the following keystrokes to be used.

PC Key or action	Macintosh options
ALT	Command

PC Key or action	Macintosh options
INSERT	0 (zero) on the numeric keypad; Num Lock must be off Option-Help
DELETE	Decimal point on the numeric keypad; Num Lock must be off Clear
F1 to F9	Option 1 to 9 on numeric keypad Option-Escape 1 to 9
F10	Option 0 (zero) on numeric keypad Option-Escape 0
F11	Option minus sign on numeric keypad Option-Escape hyphen
F12	Option plus sign on numeric keypad Option-Escape equal sign
ALT+TAB	Option-Tab (This can be reconfigured by the user—see "Configuring Hotkeys" on page 47)
ALT+SHIFT+TAB	Option-Shift-Tab (This can be reconfigured by the user—see "Configuring Hotkeys" on page 47)

Standard keyboard mode also enables the user to use the **Keyboard** menu to send function keys, send special keys, and enable all the keystrokes that can be used when they select **Use Option-Escape for more Keys**.

Using a Mouse

Citrix recommends using a two button mouse and configuring the right mouse button to be the secondary button. You can also emulate a PC mouse right-click using Option and click.

Configuring the User Interface

Overview

This section discusses the user interface settings you can configure to make connections work according to personal taste and to make them more efficient. It includes the following topics:

- Window properties
- Showing and hiding the Macintosh menu bar and Dock
- Mapping audio and windows alert beeps
- Hotkeys
- Japanese hotkeys and other keyboard settings

Window Properties

You can change the maximum size and color depth of the session window. You can change the default settings or set different dimensions for different connections.

To configure the default window properties

1. From the ICA Client Editor **Options** menu, choose **Default Settings**, or click **Default Settings** in the **ICA Client Editor**.
2. Choose **Connection Properties > Windows and Sounds**.
3. Make your changes:
    - Use the Size pop-up menu to choose a preconfigured window size, choose **Full Screen**, or choose **Custom** and type dimensions at **Width** and **Height**.

      You can also choose **Seamless**, where applications appear in a fully resizable window.

The maximum window size is determined by the server.

- Choose the window color depth to display.

4. Click **Save**.

To specify the window properties for a particular connection

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Window** tab, clear **Use Default** and enter your own settings:
   - For window size, use the size list to choose a preconfigured window size, choose **Full Screen** mode, or choose **Custom** and type your own window size. Choose **Seamless** to display applications in a fully resizable window
   - Choose the window color depth to display.
3. Click **Save**.

Showing and Hiding the Menu Bar and Dock

If your ICA session is running in Full Screen mode, the Macintosh menu bar and Dock might be hidden.

To display the Macintosh menu bar, press Control-Option. The same key combination also hides it again.

Note: If you are not in Full Screen mode, and your window size enables you to see the entire remote desktop, you can use Control-Option to show a standard Macintosh resize control in the bottom right corner of the ICA session window. The same key combination hides the resize box again.

If the window size is too small to show the entire remote desktop, you must use the scroll bars to see the hidden content of the desktop.

To display both the complete window and the Macintosh menu bar, in the client **File** menu, click **Best Window Position**.

You can also configure the client so that it will show the menu bar and Dock only when you move your mouse to the top of the screen or to the edge where the Dock is located.

To display the menu bar and Dock only when the mouse is at the edge of the screen.

Do one of the following:

- In the ICA Client Editor, choose **Default Settings > Connection Properties > Windows and Sounds** and choose the **Display the Macintosh Dock and menu bar automatically**.
- Use the standard Macintosh method from the **Apple** menu by choosing **Dock > Dock Preferences > Automatically hide and show the Dock**.

Configuring Sound Support (Audio Mapping)

You can configure sound support for a connection file using settings on the **Connection Properties** pane of the ICA Client Editor. For details, see "Mapping Client Audio" on page 31.

Playing Windows Alert Beeps

You can set the client to play the default Macintosh beep when an application in the ICA session triggers the default Windows beep.

To configure the default alert beep setting

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Connection Properties > Windows and Sounds**.
3. Choose or clear **Enable Windows Alert Sounds**.
4. Click **Save**.

Configuring Hotkeys

The client offers several means of using a Macintosh keyboard to make the equivalent of PC keystrokes and change the way Macintosh keys are interpreted in Windows desktops and applications running within a session. See "Making Keystrokes with Macintosh Keyboards" on page 41 for information on these features.

The following default key combinations can be changed.

- Option-Tab (to cycle through open applications—equivalent to ALT+TAB on PC)
- Option-Shift-Tab (to cycle through open applications in reverse order—equivalent to ALT+SHIFT+TAB on PC)
- Latency reduction hotkey (to override the selected SpeedScreen mode—see "Reducing Display Latency" on page 53 for more information)

To change the default hotkeys

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Connection Properties > Keyboard** to see the current settings for the hotkeys.
3. Choose the main key for the function, then use the check boxes to choose the additional keystrokes.
4. Click **Save**.

Using Japanese Hotkeys

Choose your input locale in the **Input Menu** from the Macintosh system preferences. Depending on how your hotkeys have been set up, you may be able to use Command-Space Bar to change the input locale; this can be changed using the International options in the Mac OS X System Preferences.

The following Kotoeri hotkeys are supported:

This key combination	Has this effect
Control-Shift-H	Show help
Control-Shift-N	Add word to dictionary
Control-Shift-R	Reconvert
Control-J	Convert to Hiragana
Control-V	Convert to Katakana
Control-L	Convert to full-width alphanumeric
Control–Semi-colon key	Convert to half-width alphanumeric
Control-Shift-J	Hiragana input mode
Control-Shift-K	Katakana input mode

This key combination	Has this effect
Control-Shift-L	Katakana input mode
Control-Shift–Semi-colon	Half-width alphanumeric input mode

There may be a conflict if the remote application uses the same hotkeys as one of the hotkeys listed above.

Note: When you connect to a Japanese server, you may experience difficulty generating Japanese keystrokes using the keyboard. You can use the on-screen buttons of the Input Method Editor (IME) using the mouse. Alternatively, you can set up hotkey mappings that simulate the effect of the IME keys. For example, if you cannot generate the Kanji key normally from the keyboard, you can define Control-Command-5 as the Kanji key.

To map Kotoeri hotkeys

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Connection Properties > Japanese Hotkeys**.
3. Choose **Map Kotoeri Shortcuts**.
4. Click **Save**.

Using Japanese Keyboards

If you use a Japanese keyboard you need to specify the layout and type.

To configure default keyboard layout and type settings

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Connection Properties > Keyboard**.
3. Choose the keyboard layout and keyboard type.
4. Click **Save**.

Solving Japanese Keyboard Problems

If you are using IME version 2000 or later, the Kanji Bango hotkey and the Caps Lock key may not work with the default settings.

If you are using SpeedScreen (Local Text Echo) and your server has two or more input locales, you may experience a problem with 106 key Japanese keyboards with US keyboard layout. See "Reducing Display Latency" on page 53.

Note: Kana input is not supported when using the Apple Extended Keyboard II Japanese with the client. You can still use this keyboard for Roman input.

To enable the Kanji Bango hotkey and Caps Lock key

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Connection Properties > Keyboard**.
3. From the **Keyboard Layout** list, choose **Japanese MS-IME2000**.
4. Click **Save**.

To overcome problems using 106 key Japanese keyboards with US keyboard layout

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the ICA Client Editor.
2. Choose **Connection Properties > Keyboard**.
3. From the **Keyboard Type** list, choose **101 Keyboard (Japanese)**.
4. Click **Save**.

Improving Performance

Overview

This section describes ways you can improve the performance of the client including:

- Compressing data
- Caching images
- Reducing display latency

It also gives tips for improving performance over low-bandwidth connections.

Compressing Data

Data compression reduces the amount of data that needs to be transferred over the connection but requires additional processor resources to compress and decompress the data. In high-bandwidth LAN environments where bandwidth consumption is not a concern, turning data compression off may give better performance because it reduces the demand on the processor.

To turn data compression on or off for a specific connection file

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Connection Properties** tab, choose or clear the **Use Data Compression** check box.
3. Click **Save**.

Caching Images

Disk caching stores commonly used graphical files, such as bitmaps and fonts, in a local cache on the client device. If the connection has limited bandwidth, using disk caching improves performance. If the connection is a high-speed LAN, you do not need disk caching.

Important: Although you can configure default disk cache settings, disk caching does not happen unless you turn it on for a particular connection file.

Note: In addition, the client uses SpeedScreen Browser Acceleration, a feature that also improves performance when you display Web pages containing .jpeg and .gif images in Microsoft Internet Explorer. SpeedScreen Browser Acceleration operates automatically and requires no configuration.

To configure the default settings for disk caching

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. Choose **Connection Properties > Performance**.
3. Change the disk cache settings as required. You can do the following:
   - Use a different disk cache folder (the default directory where the cached data is stored). To do this, click **Folder Location** and choose the folder you want.
   - Change the cache folder size using the **Amount of disk space to use** selector. Choose an amount from 1 MB to 100 MB.
   - For **Minimum size bitmap that will be cached,** specify the size of the smallest bitmap to be cached to disk. This must be a value between 2 and 64 kilobytes.
   - Remove all cached data from the client by clicking **Clear Disk Cache**.
4. Click **Save**.

To turn disk caching on or off for a specific connection file

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Connection Properties** tab, choose or clear the **Use Disk Cache for Bitmaps** check box.
3. Click **Save**.

Reducing Display Latency

Over high latency connections, you might experience significant delays between the time when you type text at the keyboard and when it is displayed on the screen. Similarly, there may be a delay between clicking a mouse button and the screen displaying any visible feedback. This can result in you retyping text or making several unnecessary mouse clicks. The client's SpeedScreen Latency Reduction feature lessens the impact on display of high latency.

Note: SpeedScreen Latency Reduction only works if you enable it on the server. For full details, see the Presentation Server documentation. Note that SpeedScreen Latency Reduction is not available when you connect to computers running Presentation Server for UNIX.

To turn SpeedScreen Latency Reduction on or off for a specific connection file

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Connection Properties** tab, choose the SpeedScreen Latency Reduction settings:

   - **Mouse Click Feedback:** display an hourglass to show the mouse input is being processed.
   - **Local Text Echo:** display text in a generic font (as you type) that gets overwritten with the correct font after the input has been processed by the server. For some applications, such as Microsoft Word, your text might appear in a floating bubble before being displayed in the application you are using.

   For each setting, choose an option:

   - **Auto:** automatically turn the feature on or off depending on the speed of the connection. Choose this option if you are not certain of the connection speed.
   - **On:** choose for slower connections (for example, over a WAN or a dial-up connection).
   - **Off:** choose for faster connections (for example, over a LAN).
3. Click **Save**.

Note: You can override the selected SpeedScreen mode for the current session by using the Latency Reduction hotkey. See "Configuring Hotkeys" on page 47 for details.

Improving Performance Over a Low-Bandwidth Connection

If you have a low-bandwidth connection, such as a modem, there are a number of changes that you can make to improve performance:

- **Change your client configuration.** Changing your client configuration can reduce the bandwidth that the ICA protocol requires. See "Changing Your Client Configuration" on page 54.
- **Change the way you use the client.** See "Changing the Way You Use the Client" on page 55 for ways of reducing the bandwidth required for a high-performance connection by changing working practices.
- **Use the latest client.** Citrix is continually enhancing and improving performance with each release, and many performance features require the latest client and server software.

Changing Your Client Configuration

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

- **Allow maximum data compression.** Compression reduces the size of the data that is transferred over the connection. See "Compressing Data" on page 51.
- **Turn the disk cache on.** Disk caching stores commonly used images and fonts locally on the client computer so that they do not have to be transferred over the connection every time they are needed. See "Caching Images" on page 51.
- **Turn SpeedScreen Latency Reduction on.** SpeedScreen Latency Reduction improves performance over high latency connections by providing instant feedback in response to typed data or mouse clicks. See "Reducing Display Latency" on page 53.

- **Reduce the window size.** Change the window size to the minimum size you can comfortably use. See “Window Properties” on page 45.
- **Turn client audio mapping off.** If you do not need sound, turn client audio mapping off. See “Mapping Client Audio” on page 31.

Changing the Way You Use the Client

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

- **Avoid accessing large files using client drive mapping.** When you access a large file with client drive mapping, the file is transferred over the connection. On slow connections, this may take a long time. Consider opening large file directly from its remote location instead.
- **Avoid printing large documents on local client printers.** When you print a document on a local client printer, the print file is transferred over the connection. On slow connections, this may take a long time. Consider printing large files on a network printer instead.
- **Avoid playing multimedia content.** Playing multimedia content uses a lot of bandwidth and can reduce performance.

Integrating the Client with Security Solutions

Overview

This section describes how you can integrate the client with a range of security technologies, including proxy servers, firewalls, and Secure Sockets Layer/ Transport Layer Security (SSL/TLS) based systems. This section assumes you have a working knowledge of these technologies. It describes:

- Connecting through a proxy server
- Integrating the client with the Secure Gateway or SSL Relay solutions with SSL/TLS protocols
- Connecting to a server using alternate addressing across a firewall

Configuring the Client to Work with a Proxy Server

You can use either a SOCKS proxy or a Secure Proxy Server (also known as Security Proxy Server, HTTPS Proxy Server, or SSL Tunneling Proxy Server). Proxy authentication is also supported. When used with the Secure Gateway, applications can be delivered securely to anywhere in the world by the Web. The client can automatically detect proxy server settings from the network settings in the client computer's Network System Preferences.

To configure the client to work with a proxy server you can specify the default details of your proxy server manually or detect proxy servers automatically. Instructions on how to do this are provided in the following two sections.

Specifying the Proxy Server Manually

If you are specifying the proxy server manually, you need to know its address. You also need to know its port number if it is not set to 1080 for a SOCKS Proxy Server or 8080 for a Secure Proxy Server.

To configure a default SOCKS or Secure Proxy Server

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the ICA Client Editor.
2. On the **Making a Connection** > **Server Location** pane, click **Firewalls** to open the **Firewall Settings** dialog box.
3. Choose the proxy type (or **No Proxy** for a direct connection.)
4. Type the address of the proxy server, and the port number if it is not 1080 (for a SOCKS Proxy Server) or 8080 (for a Secure Proxy Server).
5. Click **OK**, then **Save**.

To specify a SOCKS or Secure Proxy Server for a connection file

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Security** tab, clear the **Proxy > Use Default** check box.
3. Click **Firewall Settings**.
4. Choose the proxy type (or **No Proxy** for a direct connection.)
5. Type the address of the proxy server, and the port number if it is not 1080 (for a SOCKS Proxy Server) or 8080 (for a Secure Proxy Server).
6. Click **OK**.

Note: You can enter only one proxy server address.

Detecting Proxy Details Automatically

If you are deploying the client in an organization with many proxy servers, consider using auto proxy server detection (also called *auto client proxy detection*.) It is also useful if you cannot determine which proxy server will be used when you configure the client. Auto proxy server detection obtains proxy details from the network settings in the client device's Network System Preferences.

To turn auto proxy server detection on by default

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.

2. On the **Making a Connection** > **Server Location** pane, click **Firewalls**.
3. Choose **Use Web browser proxy settings**.
4. Click **OK**, then **Save**.

Integrating the Client with the Secure Gateway or SSL Relay

You can integrate the client with the Citrix Secure Gateway or an SSL Relay service. The client supports both SSL and TLS protocols:

- SSL provides strong encryption to increase the privacy of your connections and certificate-based server authentication to ensure that the server you are connecting to is a genuine server.
- TLS is the latest, standardized, version of the SSL protocol. Because there are only minor technical differences between SSL Version 3.0 and TLS Version 1.0, they are functionally equivalent.

The Secure Gateway

If you are using the server in SSL Relay mode, the Secure Gateway functions as a proxy server. You must configure the client to use both the fully qualified domain name (FQDN) and port number of the Secure Gateway server. (For further details, see the *Secure Gateway for Windows Administrator's Guide*.)

The FQDN of the Secure Gateway server must list the following components in sequence:

- Host name
- Intermediate domain
- Top-level domain

For example, my_computer.my_company.com is an FQDN because it lists, in sequence, a host name (my_computer), an intermediate domain (my_company), and a top-level domain (com). The combination of intermediate and top-level domains (my_company.com) is generally referred to as the *domain name*.

You can configure the Secure Gateway settings only if you already chose SSL/TLS+HTTPS. See "Identifying a Desktop or Application to Connect to" on page 24.

To configure a default Secure Gateway server (Relay mode)

1. Do one of the following:

- From the ICA Client Editor **Options** menu, choose **Default Settings**.
- Click **Default Settings** in the ICA Client Editor.

2. On the **Making a Connection** > **Server Location** pane, click **Firewalls** to open the **Firewalls Settings** dialog box.
3. Type the fully qualified domain name of the Secure Gateway server and the port number, if not 443.
4. Click **OK**, then **Save**.

To specify a Secure Gateway server (Relay mode) for a connection file

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Security** tab, clear the **Proxy > Use Default** check box.
3. Click **Firewall Settings**.
4. Type the fully qualified domain name of the Secure Gateway server and the port number, if not 443.
5. Click **OK**.

SSL Relay

You can use SSL Relay to secure communications between the following:

- An SSL/TLS-enabled client and a server
- Devices running Presentation Server and the Web Interface

For information about configuring and using SSL Relay, see the Presentation Server documentation. For information about configuring Web Interface to use SSL/TLS encryption, see the *Web Interface Administrator's Guide*.

Configuring SSL/TLS

TLS is the standardized form of SSL. Both are cryptographic security protocols designed to ensure the integrity and privacy of data transfers across public networks.

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

There are three main steps involved in setting up SSL/TLS:

1. Set up SSL Relay on the devices running Presentation Server or the Web Interface and obtain and install the necessary server certificate. See the

Presentation Server documentation and SSL Relay documentation for details.

2. Install the equivalent root certificate on the client. See “Configuring SSL/TLS” on page 60.
3. Configure a connection, or all connections, to connect to the server using SSL/TLS. See “Configuring SSL/TLS” on page 60.

Installing Root Certificates on Clients

To use SSL/TLS to secure communications between SSL/TLS-enabled clients and the server, you need a root certificate on the client that can verify the signature of the Certificate Authority on the server certificate. Mac OS X comes with about 100 commercial root certificates already installed, but if you need to install another certificate, follow the guidelines below.

Obtain a root certificate from the Certificate Authority and place it on each client (the certificate will usually have the extension **.crt** or **.cer**). This root certificate is then used and trusted by the client.

Depending on your organization’s policies and procedures, you may want to install the root certificate on each client instead of directing users to install it. The easiest and safest way is to add root certificates to the Mac OS X keychain; alternatively place root certificates in a certificates folder in the folder containing your client.

Important: The following steps assume your organization has a procedure in place for users to check the root certificate before they install it.

To add a root certificate to a keychain

1. Double-click on the file containing the certificate. This will automatically start the Keychain Access application.
2. In the **Add Certificates** dialog box, choose **X509Anchors** (if using Mac OS 10.4 Tiger) or **System** (if using Mac OS 10.5 Leopard) from the **Keychain** pop-up menu. Click **OK**.
3. Type your password in the **Authenticate** dialog box and click **OK**. The root certificate is installed and can be used by SSL-enabled clients and by any other application using SSL.

Configuring the Client to Use SSL/TLS

The following section explains how to configure the client to use SSL/TLS.

To configure the default SSL/TLS settings

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the ICA Client Editor.
2. On the **Making a Connection** > **Server Location** pane, at Network Protocol, choose **SSL/TLS+HTTPS**. The **Address List** changes to show available SSL/TLS-enabled servers.
3. If the address list does not include the server you want, click **Add**. The **Server Address** dialog box appears.
4. Type the fully qualified domain name of the required server, for example `my_computer.my_company.com`.

   For more information about fully qualified domain names, see "Configuring SSL/TLS" on page 60.
5. Type the port number if it is different from the default.
6. Click **OK** to save this server information to the address list.
7. Click **Save**.

Connecting to a Server through a Firewall

If there is a firewall between the client and the server, you must configure the default setting to use the alternate server address returned by the master browser. You need to do this even if you are not using a SOCKS Proxy Server.

If you use the client inside and outside a firewall (at work and at home, for example), you can create two connection files, one with the alternate address setting off (for work) and one with the alternate address setting on (for home.)

To configure the default firewall alternate address setting

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. On the **Making a Connection** > **Server Location** pane, click **Firewalls**.
3. Choose the **Use alternate address for firewall connection** check box and click **OK**.
4. Click **Save**.

To specify the alternate server address setting for a connection file

1. In the **ICA Client Editor**, open the connection file you want to edit.
2. From the **Security** tab, clear the **Proxy > Use Default** check box.
3. Click **Firewall Settings**.
4. Choose the **Use alternate address for firewall connection** check box and click **OK**.
5. Click **Save**.

Using Encryption

Encryption increases the security of your connection. By default, basic encryption is turned on for all connections. This type of security is primarily suited to local networks. If the server you are connecting to supports encryption, you can use it to improve security.

Note: Encryption is not available for connections to servers running Presentation Server for UNIX.

To configure a default encryption level

1. Do one of the following:
   - From the ICA Client Editor **Options** menu, choose **Default Settings**.
   - Click **Default Settings** in the **ICA Client Editor**.
2. On the **Making a Connection** > **Server Location** pane, change the encryption level.
3. Click **Save**.

To change the encryption settings for a specific connection file

1. In the ICA Client Editor, open the connection file you want to edit.
2. From the **Security** tab, clear **Encryption > Use Default** and choose an encryption level supported by the client.

Note: You must configure the server to allow the selected encryption level or greater. See the Presentation Server documentation for more information.

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W