



# **Plug-in for Macintosh Administrator's Guide**

## **Copyright and Trademark Notices**

Use of the product documented herein is subject to your prior acceptance of the End User License Agreement. A printable copy of the End User License Agreement is included with your installation media.

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

© 2009 Citrix Systems, Inc. All rights reserved.

Citrix® and ICA® are registered trademarks, and Citrix Presentation Server™, Citrix XenApp™, Citrix XenApp™ for UNIX®, XenDesktop™, Citrix Dazzle™, and SpeedScreen™ are trademarks of Citrix Systems, Inc. in the United States and other countries.

## **Trademark Acknowledgements**

RSA Encryption © 1996–1997 RSA Security Inc. All rights reserved.

FLEXnet Operations and FLEXnet Publisher are trademarks and/or registered trademarks of Aceso Software Inc. and/or InstallShield Co. Inc.

Apple, LaserWriter, Mac, Macintosh, Mac OS, Power Mac, and Safari are trademarks or registered trademarks of Apple Computer Inc.

Microsoft, MS, Windows, Windows Server, Win32, Outlook, ActiveX, Visual J#, ClearType, Excel, SQL Server, Microsoft Access, Windows Vista, .NET, Media Player, and Active Directory are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Firefox is a trademark/registered trademark of the Mozilla Foundation.

Netscape, Netscape Navigator, and Mozilla are trademarks or registered trademarks of Netscape in the United States and other countries.

Novell, Novell Directory Services, NDS, NetWare, Novell Client, and eDirectory are trademarks or registered trademarks of Novell, Inc. in the United States and other countries.

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

All other trademarks and registered trademarks are the property of their respective owners.

Document code: August 5 2009 07:18:58

---

---

# Contents

<b>1</b>	<b>Introduction to the Plug-in for Macintosh.....</b>	<b>5</b>
	How To Use This Documentation.....	6
	Finding Documentation.....	6
	Getting Support and Training.....	6
	New Name for the Client for Macintosh.....	6
	About the Plug-in for Macintosh.....	7
	New Features in This Release.....	7
	Existing Features.....	8
	Custom Connection Files and the ICA Client Editor.....	8
<b>2</b>	<b>Deploying the Plug-in for Macintosh.....</b>	<b>9</b>
	System Requirements.....	10
	Installing the Plug-in.....	10
	To install the plug-in.....	10
	Upgrading the Plug-in.....	10
	Uninstalling the Plug-in.....	11
<b>3</b>	<b>Using Citrix Dazzle.....</b>	<b>13</b>
	Choosing Your Applications and Desktops.....	14
	To subscribe to applications or desktops when installation completes.....	14
	To subscribe to additional applications and desktops.....	14
	Adding an Alias for an Application or Desktop to the Dock.....	14
	To add an alias for an application or desktop to the Dock.....	15
	Launching Applications and Desktops.....	15
	Removing Applications and Desktops.....	15
	To remove applications and desktops using Citrix Dazzle.....	15
	Connecting to a New Server from Citrix Dazzle.....	15
	To connect to a new server from Citrix Dazzle.....	16
<b>4</b>	<b>Configuring the Plug-in for Macintosh.....</b>	<b>17</b>
	Configuring Window Properties.....	18

## Contents

---

To configure window properties.....	18
Showing and Hiding the Menu Bar and Dock.....	18
To show and hide the menu bar and Dock automatically.....	18
Mapping Client Devices.....	19
Mapping Client Drives.....	19
To map client drives.....	19
Mapping Client COM Ports.....	20
To map client COM ports.....	20
Printing.....	21
<b>5 Optimizing the Plug-in Environment.....</b>	<b>23</b>
Improving Performance.....	24
Reconnecting Users Automatically.....	24
Providing Session Reliability.....	24
Reducing Display Latency.....	24
Changing the Way You Use the Plug-in.....	25
Improving the User Experience.....	25
ClearType Font Smoothing in ICA Sessions.....	25
Making Keystrokes with Macintosh Keyboards.....	25
Substituting Windows Special Keys.....	28
Using a Mouse.....	29
<b>6 Securing Plug-in Communication.....</b>	<b>31</b>
Connecting Through a Proxy Server.....	32
Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay.....	32
Connecting with the Secure Gateway.....	32
Configuring the Plug-in for Secure Gateway.....	33
Connecting with Citrix SSL Relay.....	33
Configuring and Enabling the Plug-in for SSL and TLS.....	33
Connecting Through a Firewall.....	34

---

# Chapter 1

## Introduction to the Plug-in for Macintosh

### Topics:

- [\*How To Use This Documentation\*](#)
- [\*New Name for the Client for Macintosh\*](#)
- [\*About the Plug-in for Macintosh\*](#)
- [\*New Features in This Release\*](#)
- [\*Existing Features\*](#)
- [\*Custom Connection Files and the ICA Client Editor\*](#)

Welcome to the Citrix online plug-in for Macintosh. The plug-in provides users with access to resources hosted by XenApp and XenDesktop servers. This section introduces you to the plug-in.

## How To Use This Documentation

This documentation is for system administrators responsible for installing, configuring, deploying, and maintaining the plug-in. This documentation assumes knowledge of:

- ◆ Citrix XenApp and/or Citrix XenDesktop
- ◆ The machine running Citrix XenApp or Citrix XenDesktop to which the plug-in 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 documentation refer to "you." In some circumstances "you" refers to the administrator of the plug-in, in others to the user of the plug-in, and sometimes to both. The context indicates whether a procedure is primarily an administrator or user activity.

## Finding Documentation

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

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

Known issues information is included in the readme.

To provide feedback about the documentation, click the **Article Feedback** link located on the download page for each individual guide.

## Getting Support and Training

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

Information about Citrix training is available at <http://www.citrix.com/edu/>.

## New Name for the Client for Macintosh

Citrix online plug-in for Macintosh is the new name for the software installed on client devices in your deployment (formerly the Citrix Presentation Server Client for Macintosh). You will see the new name used throughout both the product documentation and installed software.

## About the Plug-in for Macintosh

The Citrix online plug-in for Macintosh (*the plug-in*) provides users with access to resources published on XenApp or XenDesktop servers. The plug-in combines ease of deployment and use, and offers quick, secure access to applications and virtual desktops.

After subscribing to published resources, users can access those resources from a familiar Macintosh desktop environment. Users work with published resources the same way they work with local applications and files. Published resources are represented on the local desktop, by icons that behave just like local icons, on the Dock, or in the Citrix Dazzle folder available from the Finder.

Users can also access published resources from within a familiar browser environment, by clicking links on a Web page you publish on your corporate intranet or the Internet.

## New Features in This Release

**Citrix Dazzle.** Provides users with a new interface for selecting the applications and desktops they want to access on XenApp and XenDesktop servers. Icons for those applications can be displayed on the desktop, on the Dock, or in the Dazzle folder available from the Finder.

**Support for Native Launching of Applications.** Provides users with the ability to launch hosted applications and desktops in the same way as local applications.

**Citrix Online Plug-in Preferences.** Provides users with a new interface for editing various plug-in settings. Use the Citrix online plug-in pane in System Preferences to change the appearance of virtual desktops, edit keyboard shortcuts, and map client devices.

**Support for ClearType Font Smoothing.** Provides support for sub-pixel font rendering, which improves the quality of displayed fonts, compared to traditional forms of font smoothing or anti-aliasing. Sub-pixel font rendering technology is particularly useful on Liquid Crystal Display (LCD) screens. The plug-in automatically detects the client device setting for font smoothing and creates a session environment using that setting.

**Enhanced International Keyboard Support.** The plug-in now supports the Latin 2 keyboard layout.

**Integration with Client Detection and Deployment Functionality.** New plugins for Safari and Firefox Web browsers integrate with the client detection and deployment functionality provided by the Web Interface to ensure users always have the most up-to-date version of the plug-in installed on their client device. When users connect to their applications and desktops using a browser, the Web Interface detects the current version of the plug-in installed on a client device and updates it automatically, if required.

## Existing Features

For a full list of existing plug-in features, see the [Plug-in Feature Matrix](#), available on the Citrix Web site.

## Custom Connection Files and the ICA Client Editor

In previous versions of the plug-in, you used the ICA Client Editor to create custom connection files. Those files contained all the settings used by the plug-in when connecting to hosted applications and desktops.

In the current version of the plug-in, both custom connection files and the ICA Client Editor are deprecated and the creation of new custom connection files is no longer supported. You can, however, still use existing custom connection files to connect to hosted applications and desktops.

To configure settings for the current version of the plug-in, use the Citrix online plug-in pane in System Preferences.

---

## Chapter 2

# Deploying the Plug-in for Macintosh

### Topics:

- [System Requirements](#)
- [Installing the Plug-in](#)
- [Upgrading the Plug-in](#)
- [Uninstalling the Plug-in](#)

Installation files for the plug-in are available for download from the Citrix Web site.

This section contains information about installing the plug-in in your environment.

## System Requirements

The plug-in is supported on the following operating systems:

- ◆ Mac OS X Version 10.4 (Intel-based and PowerPC-based Mac computers), 32-bit and 64-bit
- ◆ Mac OS X Version 10.5 (Intel-based and PowerPC-based Mac computers), 32-bit and 64-bit

Requirements:

- ◆ At least 256 MB of RAM
- ◆ 20 MB of free disk space
- ◆ A working network or Internet connection to connect to servers

## Installing the Plug-in

You can download the Citrix online plug-in for Macintosh from the Citrix Web site, at <http://www.citrix.com>.

### To install the plug-in

1. Log on as an administrator.
2. Download the file Citrix online plug-in.dmg from the Citrix Web site and open it. This runs the Disk Utility program, which mounts the file as a disk image accessible from your Macintosh desktop.
3. On the **Introduction** page, click **Continue**.
4. On the **License** page, click **Continue**.
5. Click **Agree** to accept the terms of the License Agreement.
6. On the **Destination Select** page, select the volume where you want to install the plug-in and click **Continue**.
7. On the **Installation Type** page, click **Install**.
8. Enter the administrator account details for the device on which you are installing the plug-in and click **OK**.
9. To subscribe to applications and desktops immediately, click **Open Citrix Dazzle** when prompted.

## Upgrading the Plug-in

You can upgrade to the latest version of the plug-in from previous versions.

---

When you upgrade to version 11.x of the Citrix online plug-in, existing custom connection files are preserved and can be used to connect to remote applications and desktops. The creation of new custom connection files, however, is no longer supported.

## Uninstalling the Plug-in

To uninstall the plug-in, do the following:

- ◆ Delete Citrix Dazzle and the Dazzle folder from the **Applications** folder. Note that deleting the Dazzle folder also deletes any applications you subscribed to using Citrix Dazzle.
- ◆ Delete the Citrix online plug-in and DockApplication from the **/Library/Application Support/Citrix** folder.
- ◆ Delete the Citrix ICA Client folder and com.Citrix.Citrix\_Dazzle.plist file from the Library folder at **/Users/home/Library/Preferences/** where *home* is the name of your personal Home folder.
- ◆ Delete the CitrixICAClientPlugin.plugin file from the **/Library/Internet Plug-ins** folder and the Citrix online plug-in.prefPane file from the **/Library/PreferencePanes** folder on the client device hard disk.



---

## Chapter 3

# Using Citrix Dazzle

### Topics:

- [\*Choosing Your Applications and Desktops\*](#)
- [\*Adding an Alias for an Application or Desktop to the Dock\*](#)
- [\*Launching Applications and Desktops\*](#)
- [\*Removing Applications and Desktops\*](#)
- [\*Connecting to a New Server from Citrix Dazzle\*](#)

Citrix Dazzle provides users with self-service access to the applications and desktops they need to work productively. Icons for those applications and desktops can be presented on the local desktop, on the Dock, or in the Dazzle folder available from the Finder.

The new, easy-to-use interface allows users to subscribe to applications and desktops hosted on XenApp and XenDesktop servers with a single click, replacing the need for individual connection files used by earlier versions of the plug-in.

For more information about connection files, see [Custom Connection Files and the ICA Client Editor](#) on page 8.

## Choosing Your Applications and Desktops

At the end of the plug-in install you are prompted to launch Citrix Dazzle. After launching Citrix Dazzle, you can select the applications and desktops you want to subscribe to and begin working with those applications and desktops immediately.

You can also launch Citrix Dazzle separately, when you want to subscribe to other applications or desktops; for example, when new applications or desktops are added to those already hosted on the server.

### To subscribe to applications or desktops when installation completes

1. Click **Open Citrix Dazzle** when prompted at the end of the plug-in installation process.
2. Enter the address of the server hosting your applications or desktops.
3. Enter the user name and password you use to log on to the server hosting your applications or desktops. If you want to add these details to your keychain, select **Remember this password in my keychain**.
4. Click **OK**.
5. Select the applications and desktops you want to subscribe to and click **Add**. This adds the applications and desktops to your **Dazzle** folder. Alternatively, you can drag the applications or desktops to your local desktop or any folder of your choice. If you do not see the application or desktop you require, you can search for it by typing the name in the search field.

### To subscribe to additional applications and desktops

1. Open **Citrix Dazzle** from the **Applications** folder.
2. Select the applications and desktops you want to subscribe to and click **Add**. This adds the applications and desktops to your **Dazzle** folder. Alternatively, you can drag the applications or desktops to your local desktop or any folder of your choice. If you do not see the application or desktop you require, you can search for it by typing the name in the search field.

## Adding an Alias for an Application or Desktop to the Dock

You can add an alias for a hosted application or virtual desktop to the Dock in the same way as you can for any local application.

## To add an alias for an application or desktop to the Dock

1. In the **Finder**, open the folder containing the application or desktop you want to add to the dock.
2. Drag the application or desktop icon to the Dock.

## Launching Applications and Desktops

Users launch hosted applications and virtual desktops in exactly the same way as local applications. If a user does not add their account information for the Citrix server to the keychain, they are asked to enter that information before the application or desktop launches.

Users can search for applications and desktops to which they have subscribed using Spotlight and can also rename them to more easily distinguish between local and hosted versions.

## Removing Applications and Desktops

You can remove applications and desktops you no longer need access to by dragging them to the **Trash**. Alternatively, you can use Citrix Dazzle to remove applications and desktops.

If you require access to an application or desktop after removing it, use Citrix Dazzle to subscribe to that application or desktop again.

## To remove applications and desktops using Citrix Dazzle

1. Open **Citrix Dazzle** from the **Applications** folder.
2. Select the folder containing the applications and desktops you want to remove.
3. Click **Remove** to remove each application or desktop you no longer require access to.

## Connecting to a New Server from Citrix Dazzle

From time to time, you may need to change the server you connect to from Citrix Dazzle; for example, if your applications and desktops are hosted on more than one server or are migrated from one server to another. You can connect to a new server using the **Change Server** functionality provided with Citrix Dazzle.

Note that when you connect to a new server from Citrix Dazzle, all applications and desktops to which you subscribed previously, on the original server, remain available to you.

## To connect to a new server from Citrix Dazzle

1. Open **Citrix Dazzle** from the **Applications** folder.
2. From the **File** menu, choose **Change Server**.
3. Enter the address of the new server to which you want to connect and click **OK**.  
After you connect to the new server, you can subscribe to applications and desktops hosted on that server in the usual way.

---

## Chapter 4

# Configuring the Plug-in for Macintosh

### Topics:

- *Configuring Window Properties*
- *Showing and Hiding the Menu Bar and Dock*
- *Mapping Client Devices*
- *Printing*

After the plug-in software is installed, you can configure various plug-in settings using the Citrix online plug-in pane in System Preferences.

This section describes how you configure those settings.

## Configuring Window Properties

You can configure the plug-in to display virtual desktops in either fixed size windows or as full screen. Hosted applications are automatically displayed in seamless mode, in fully resizable windows.

### To configure window properties

1. Choose **Apple menu > System Preferences**, and then click **Citrix online plug-in**.
2. Click **Appearance**.
3. Select whether you want to display virtual desktops in **Windowed** or **Full Screen** mode.

## Showing and Hiding the Menu Bar and Dock

When viewing virtual desktops 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 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 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 when connected to a session, from the **Citrix online plug-in** menu, choose **View > Best Window Position**.

You can also configure the plug-in to show the menu bar and Dock automatically, whenever you move your mouse to the top of the screen or to the edge where the Dock is located. If you select this option, the Dock is hidden when you are not using it.

### To show and hide the menu bar and Dock automatically

1. Choose **Apple menu > System Preferences**, and then click **Citrix online plug-in**.
2. Click **Appearance**.
3. Select **Show the Dock and menu bar**.

Alternatively you can use the standard Macintosh method from the Apple menu by choosing **Dock > Dock Preferences > Automatically hide and show the Dock**.

## Mapping Client Devices

You can map local drives and devices so that they are available from within a session. If enabled on the server, client device mapping allows a remote application or desktop running on the server to access devices attached to the local client device. You can:

- ◆ Access local drives, COM ports, and printers
- ◆ Hear audio (system sounds and audio files) played from the session

Note that client audio mapping and client printer mapping do not require any configuration on the client device.

## Mapping Client Drives

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

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.

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

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.

### To map client drives

1. Choose **Apple menu > System Preferences**, and then click **Citrix online plug-in**.
2. Click **Devices**.

The **Mapped Drives** pane lists the disk or path name of every Macintosh folder already mapped to each drive on the server. The Read and Write columns show whether or not you have read and write access.

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).

Drive	Mapped to
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.
C	Permanently mapped to the user's Home folder on the Macintosh hard disk.

3. Click the **Plus** button.
4. Select an available drive letter.
5. Click **Browse**.
6. Select the folder on the Macintosh hard drive that you want to map and click **Browse**.
7. Click **Create**. The **Mapped Drives** pane now displays the mapped folder.
8. Select the level of read and write access for the mapped drive from the **Read** and **Write** pop-up menus.
9. Log out of any open sessions and reconnect to apply the changes.

## Mapping Client COM Ports

Client COM port mapping allows devices attached to the COM ports of the client device to be used during sessions on a server. These mappings can be used like any other network mappings.

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 client COM ports

1. Choose **Apple** menu > **System Preferences**, and then click **Citrix online plug-in**.
2. Click **Devices**.
3. Select the COM port you want to map, from the **Mapped COM Ports** list. This is the virtual COM port that is displayed in the session, not the physical port on the local machine.
4. Select the device to associate with the virtual COM port from the **Device** pop-up menu.
5. Start the plug-in and log on to a server.
6. Run a command prompt.
7. At the prompt, type

```
net use comx: \\client\comz:
```

where *x* is the number of the COM port on the server (ports 1 through 9 are available for mapping) and *z* is the number of the client COM port (ports 1 through 4 are available).

8. To confirm the mapping, type `net use` at the prompt. A list displays mapped drives, LPT ports, and mapped COM ports.

## Printing

You can access printers connected to client devices during a 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.

No special configuration is needed to set up local printers to print during an ICA session. Note, however, that A4 pages might not print correctly if you choose 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 plug-in **File** menu choose **Default Paper Size > A4**. All other paper sizes will print correctly if the printer supports that paper size.



---

## Chapter 5

# Optimizing the Plug-in Environment

### Topics:

- *Improving Performance*
- *Changing the Way You Use the Plug-in*
- *Improving the User Experience*

By optimizing your environment you gain the best performance from the plug-in and provide the best user experience.

## Improving Performance

You can improve the performance of the plug-in software by enabling auto-plug-in reconnections, session reliability, and SpeedScreen Latency Reduction.

### Reconnecting Users Automatically

Users can be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the auto-plug-in reconnection feature, the plug-in can detect unintended disconnections of sessions and reconnect users to the affected sessions automatically.

When this feature is enabled on the server, users do not have to reconnect manually to continue working. The plug-in attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts. If user authentication is required, a dialog box requesting credentials appears to a user during automatic reconnection. Automatic reconnection does not occur if users exit applications without logging off. Users can reconnect only to disconnected sessions.

### Providing 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. For example, wireless users entering a tunnel may lose their connection when they enter the tunnel and regain it when they emerge on the other side. During such interruptions, the session reliability feature enables the session window to remain displayed while the connection is being restored.

You can configure your system to display a warning dialog box to users when the connection is unavailable.

Session reliability is enabled on the server by default.

**Important:** If session reliability is enabled, the default port used for session communication switches from 1494 to 2598.

### 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. SpeedScreen Latency Reduction lessens the impact of high latency connections on your display.

If SpeedScreen Latency Reduction is enabled on the server, you can enable and disable it on the client device by pressing F1.

SpeedScreen Latency reduction is not supported when connecting to Citrix XenApp for UNIX.

## Changing the Way You Use the Plug-in

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, the following tasks can impact performance:

- ♦ **Accessing large files using client drive mapping.** When you access a large file with client drive mapping, the file is transferred over the ICA connection. On slow connections, this may take a long time.
- ♦ **Printing large documents on local client printers.** When you print a document on a local client printer, the print file is transferred over the ICA connection. On slow connections, this may take a long time.
- ♦ **Playing multimedia content.** Playing multimedia content uses a lot of bandwidth and can cause reduced performance.

## Improving the User Experience

The plug-in provides a number of features for improving the user experience, including improved support for ClearType font smoothing and substituting Windows special keys with familiar Mac key combinations within a session.

### ClearType Font Smoothing in ICA Sessions

Citrix XenApp supports ClearType font smoothing with Citrix online plug-in.

If you enable ClearType font smoothing on the XenApp server, you are not forcing client devices to use ClearType font smoothing. You are enabling the server to support ClearType font smoothing on client devices that have it enabled locally and are using the plug-in.

The plug-in automatically detects the client device's font smoothing setting and sends it to the server. The session connects using this setting. When the session is disconnected or terminated, the server's setting reverts to its original setting.

### 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 you make 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.

You 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 plug-in 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.

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).
- ◆ 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, Command, Option, arrow keys, and function keys.
- ◆ Menu instructions relate to the menus in the session.
- ◆ Depending on the configuration of the client device, 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)
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	Choose Keyboard > Send Key > Control/Alt/Shift-function key
CTRL+ALT	Control-Command

PC key	Macintosh options
CTRL+ALT+DEL	CTRL+ALT+DEL Control-Option-Forward Delete Control-Option-Fn-Delete (on MacBook keyboards)
DELETE	Delete Choose Keyboard > Send Key > Delete Fn-Backspace (Fn-Delete on some US keyboards)
END	End Fn-Right Arrow
ESC	Escape Choose Keyboard > Send Key > Escape
F1 to F9	F1 to F9 Choose Keyboard > Send Function Key > F1 to F9
F10	F10 Choose Keyboard > Send Function Key > F10
F11	F11 Choose Keyboard > Send Function Key > F11
F12	F12 Choose Keyboard > Send Function Key > F12
HOME	Home Fn-Left Arrow
INSERT	Command-Help Choose Keyboard > Send Key > Insert
NUM LOCK	Clear Fn-6
PAGE DOWN	Page Down

PC key	Macintosh options
	Fn-Down Arrow
PAGE UP	Page Up Fn-Up Arrow
SPACEBAR	Choose Keyboard > Send Key > Space
TAB	Choose Keyboard > Send Key > Tab

## Substituting Windows Special Keys

The plug-in provides a number of extra options and easier ways to substitute special keys such as function keys in Windows applications with Mac keys. You configure these options using the **Citrix online plug-in** pane in System Preferences. Click on Keyboard and configure the options you want to use, as follows:

- ◆ **Send Control character using** enables you to choose whether or not to send Command-character key combinations as Ctrl+character key combinations within a session. If you select Command or Control from the pop-up menu, you can use familiar Command-character key combinations as Ctrl+character key combinations. If you select Control, you must use Ctrl+character key combinations.
- ◆ **Send Alt character using** enables you to choose how to replicate the Alt key within a session. If you select Command-Option, you can send Command-Option- key combinations as Alt+ key combinations within a session. Alternatively, if you select Command, you can use the Command key as the Alt key.
- ◆ **Send special keys unchanged** enables you to send keys that are normally used by the Mac OS to a session. You may, however, need to use the Command key as part of the key combination. For example, if F9 is assigned to Expose you send the F9 key to a session by pressing Command+F9.

You send function and other special keys to a session using the **Keyboard** menu. You can also use the following keystrokes:

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

PC Key or action	Macintosh options
F1 to F9	Option 1 to 9 on numeric keypad
F10	Option 0 (zero) on numeric keypad
F11	Option minus sign on numeric keypad
F12	Option plus sign on numeric keypad

## 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.



---

## Chapter 6

# Securing Plug-in Communication

### Topics:

- [\*Connecting Through a Proxy Server\*](#)
- [\*Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay\*](#)
- [\*Connecting Through a Firewall\*](#)

This section describes measures you can take to secure the communication between your server farm and the plug-ins. You can integrate your plug-in connections to the server farm with a range of security technologies, including:

- ♦ A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server, or SSL tunneling proxy server)
- ♦ Secure Gateway for Citrix XenApp or SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
- ♦ A firewall

## Connecting Through a Proxy Server

Proxy servers are used to limit access to and from your network, and to handle connections between plug-ins and servers. The plug-in support SOCKS and secure proxy protocols.

When communicating with the server farm, the plug-in uses proxy server settings that are configured remotely on the server running the Web Interface. For information about configuring proxy server settings for the plug-ins, see [Citrix eDocs](#).

In communicating with the Web server, the plug-in uses the proxy server settings that are configured for the default Web browser on the client device. You must configure the proxy server settings for the default Web browser on the client device accordingly.

## Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay

You can integrate the plugins with the Secure Gateway or Secure Sockets Layer (SSL) Relay service. The plugins support both SSL and TLS protocols.

- ◆ SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.
- ◆ TLS (Transport Layer Security) is the latest, standardized version of the SSL protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of SSL as an open standard. TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Because there are only minor technical differences between SSL Version 3.0 and TLS Version 1.0, the certificates you use for SSL in your software installation will also work with TLS. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as FIPS 140 (Federal Information Processing Standard). FIPS 140 is a standard for cryptography.

## Connecting with the Secure Gateway

You can use the Secure Gateway in either *Normal* mode or *Relay* mode to provide a secure channel for communication between the plug-in and the server. No plug-in configuration is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

If the Secure Gateway Proxy is installed on a server in the secure network, you can use the Secure Gateway Proxy in Relay mode. For more information about Relay mode, see [Citrix eDocs](#).

If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure the plug-in to use:

- ◆ The fully qualified domain name (FQDN) of the Secure Gateway server.
- ◆ The port number of the Secure Gateway server. Note that Relay mode is not supported by Secure Gateway Version 2.0.

The FQDN must list, in sequence, the following three components:

- ◆ Host name
- ◆ Intermediate domain
- ◆ Top-level domain

For example, *my\_computer.my\_company.com* is a 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 domain (*my\_company.com*) is generally referred to as the *domain name*.

## Configuring the Plug-in for Secure Gateway

The plug-in uses settings that are configured remotely on the server running the Web Interface to connect to servers running the Secure Gateway.

In communicating with the Web server, the plug-in uses the proxy server settings that are configured for the default Web browser on the client device. You must configure the proxy server settings for the default Web browser on the client device accordingly.

## Connecting with Citrix SSL Relay

By default, Citrix SSL Relay uses TCP port 443 on the Citrix server for SSL/TLS-secured communication. When the SSL Relay receives an SSL/TLS connection, it decrypts the data before redirecting it to the server, or, if the user selects SSL/TLS+HTTPS browsing, to the Citrix XML Service.

You can use Citrix SSL Relay to secure communications:

- ◆ Between an SSL/TLS-enabled client and a server.
- ◆ With a server running the Web Interface, between the XenApp server and the Web server.

For information about configuring and using SSL Relay to secure your installation or configuring the server running the Web Interface to use SSL/TLS encryption, see [Citrix eDocs](#).

## Configuring and Enabling the Plug-in for SSL and TLS

SSL and TLS are configured in the same way, use the same certificates, and are enabled simultaneously.

When SSL and TLS are enabled, each time you initiate a connection the plug-in tries to use TLS first, then tries SSL. If it cannot connect with SSL, the connection fails and an error message appears.

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

1. Set up SSL Relay on the XenApp server and server running the Web Interface and obtain and install the necessary server certificate. For more information, see [Citrix eDocs](#).
2. Install the equivalent root certificate on the client device.

### Installing Root Certificates on Client Devices

To use SSL/TLS to secure communications between SSL/TLS-enabled plug-ins and the server farm, you need a root certificate on the client device 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 want to use another certificate, you can obtain one from the Certificate Authority and install it on each client device.

Depending on your organization's policies and procedures, you may want to install the root certificate on each client device instead of directing users to install it. The easiest and safest way is to add root certificates to the Mac OS X keychain.

#### To add a root certificate to the keychain

1. Double-click the file containing the certificate. This automatically starts the Keychain Access application.
2. In the **Add Certificates** dialog box, choose one of the following from the **Keychain** pop-up menu:
  - **X509Anchors** (if using Mac OS 10.4 Tiger)
  - **System** (if using Mac OS 10.5 Leopard)
3. Click **OK**.
4. 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.

## Connecting Through a Firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using a firewall in your deployment, the plug-in must be able to communicate through the firewall with both the Web server and Citrix server. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 if a secure Web server is in use) for client device to Web server communication. For plug-in to Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

If the firewall is configured for Network Address Translation (NAT), you can use the Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your XenApp server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address to the plug-in. The plug-

in connects to the server using the external address and port number. For more information, see [Citrix eDocs](#).