Receiver for Mac 11.4

2014-12-16 14:18:25 UTC

Contents

Receiver for Mac 11.4

About this Release

Citrix Receiver for Mac provides users with self-service access to resources published on XenApp or XenDesktop servers. Receiver combines ease of deployment and use, and offers quick, secure access to hosted applications and desktops.

Users subscribe to applications and desktops hosted on XenApp and XenDesktop servers with a single click.

After subscribing to published resources, users can access those resources directly from within the Receiver application explorer. Users select the published resources and launch them directly from within Receiver.

Users can also access published resources from a familiar Mac desktop environment, accessing those resources the same way they work with local applications and files, or from within a familiar browser environment, by clicking links on a Web page you publish on your corporate intranet or the Internet.

What's New

Citrix Receiver for Mac 11.4 provides the following new features and enhancements for customers:

- **Support for Mac OS X 10.7 (Lion)**. You can install Receiver for Mac 11.4 on the latest Mac operating system.
- **Secure, remote access through both Access Gateway and Secure Gateway**. Integration with Access Gateway and Secure Gateway provides users with secure access to all of the enterprise applications, virtual desktops, and data they need to be productive.
- **Direct access to applications and desktops when connected on an internal network**. Users can access applications and desktops directly when connected on an internal network.
- **True multi-monitor support**. Allows users to view full-screen desktop sessions from XenDesktop across multiple monitors, with monitor size and position being stored between sessions. Users can also resize existing session windows, by dragging the session window to cover multiple monitors and selecting **Full screen** from the **View** menu.
- **Bi-directional audio support**. Provides support for voice chat using hosted Office Communicator and other audio playback. Enables users to connect audio peripherals such as microphones and dictation hardware at the endpoint device that interact with hosted desktops and applications in the data center. Also includes support for both Speex and Vorbis codecs.
- **Automatic configuration of multiple devices using a Store URL**. The Citrix Receiver for Mac Setup URL Generator utility enables administrators to configure settings for XenApp or XenDesktop resources and email those configurations to multiple users at the

same time. Users can go to the URL and automatically configure Receiver access to specific XenApp and XenDesktop resources.

- **Improved printing support**. Printing improvements enable faster downloading of print files and maintain user interface responsiveness during the print process. Users are now shown a single print dialog when printing, instead of the two print dialogs shown in previous releases. Support is also provided for native server-side print drivers, client-side storage of printer preferences, and printing to client-side TCP printers.

- **Improved HDX video performance**. Receiver utilizes the Mac OS X Core Graphics support to provide significant performance improvement when viewing server-rendered video content.

- **Support for Subject Alternative Name (SAN) certificates.**. Receiver for Mac now provides support for the use of SAN certificates for authentication.

Known Issues

This section contains a list of known issues relating to this release.

- Applications and desktops in the **Applications** folder remain visible after users select **Remove All** to delete them and click Refresh. As a workaround, users should click on another folder and then click the Applications folder again. When the Applications folder reopens, deleted applications and desktops are no longer visible. [#0158663]

- Users are unable to print A3-size documents. A3 printing is not supported by the default Universal printer driver and, therefore, users have to change the Universal printer driver. Changing the Universal printer driver, however, affects client printer mapping and prevents A3 printing. There is no workaround for this issue. [#0005417]

- Multiple **Copy** dialog boxes appear when users attempt to add applications and desktops too quickly. To close these dialog boxes, users should click either **Stop** or **Replace**. [#0046962]

System Requirements

Device

- Mac OS X 10.6 or Mac OS X 10.7, 32-bit or 64-bit
- Intel-based processor
- At least 256 MB of RAM
- 15 MB of free disk space
- A working network or Internet connection to connect to servers

Server

- Web Interface 5.x for Windows with a XenApp Services or XenDesktop Web site
- XenApp (any of the following versions):
  - Citrix XenApp 6.5 for Windows Server 2008
  - Citrix XenApp 6 for Windows Server 2008 R2
  - Citrix XenApp 5 for Windows Server 2008
  - Citrix XenApp 5 for Windows Server 2003
  - Citrix Presentation Server 4.5
- XenDesktop (any of the following versions):
  - XenDesktop 5.5
  - XenDesktop 5
  - XenDesktop 4

Browser

- Safari Version 5.x or later
- Mozilla Firefox Versions 3.x through 5.x

Mouse

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

Connectivity

Receiver for Mac supports HTTP, HTTPS, and ICA-over-SSL connections to XenApp or XenDesktop through any one of the following configurations.

For LAN connections:

- Web Interface 5.x for Windows and a XenApp Services or XenDesktop Web site

For secure remote connections (any of the following products):

- Citrix Access Gateway Enterprise Edition 8.1, 9.x
- Citrix Access Gateway Standard Edition 4.5.8, 4.6.x
- Citrix Access Gateway Advanced Edition 4.5.8 with HF4, or higher
- Citrix Secure Gateway 3.x

About Secure Connections and SSL Certificates

When securing remote connections using SSL, the mobile device verifies the authenticity of the remote gateway's SSL certificate against a local store of trusted root certificate authorities. The device automatically recognizes commercially issued certificates (such as VeriSign and Thawte) provided the root certificate for the certificate authority exists in the local keystore.

Private (Self-signed) Certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the device in order to successfully access Citrix resources using Receiver for Mac.

Note: If the remote gateway's certificate cannot be verified upon connection (because the root certificate is not included in the local keystore), an untrusted certificate warning appears. If a user chooses to continue through the warning, a list of applications is displayed; however, applications fail to launch.

Importing Root Certificates on Receiver for Mac Devices

Obtain the certificate issuer's root certificate and email it to an account configured on your device. When clicking the attachment, you are asked to import the root certificate.

Wildcard Certificates

Wildcard certificates are used in place of individual server certificates for any server within the same domain. Receiver for Mac supports wildcard certificates.

Intermediate Certificates and the Access Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Access Gateway server certificate. Refer to the Knowledge Base article that matches your edition of the Access Gateway:

CTX111872: How to Upload an Intermediate Certificate on Citrix Access Gateway 4.5.x

CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition

Authentication

Note: RSA SecurID authentication is not supported for Secure Gateway configurations. To use RSA SecurID, use the Access Gateway.

Receiver for Mac supports authentication through the Access Gateway using the following methods, depending on your edition:

- No authentication (Standard and Enterprise editions only)
- Domain authentication
- RSA SecurID
- Domain authentication paired with RSA SecurID

Note: Other token-based authentication solutions may be configured using RADIUS. For SafeWord token authentication, search eDocs for "Configuring SafeWord Authentication" and refer to the instructions that match your edition of Access Gateway.

Installing Receiver for Mac

This release contains a single installation package, CitrixReceiver.dmg, that installs the Browser plug-in, Self-service plug-in, and supports remote access through both Access Gateway and Secure Gateway. Receiver can be installed:

- Automatically from Web Interface
- By a user
- Using Merchandising Server and Citrix Receiver (Updater)

Upgrading to Receiver for Mac, Version 11.4 is supported from versions 10.x and 11.x of the Online Plug-in for Mac. You can also upgrade from version 11.3 of the Receiver for Mac.

Important: Before upgrading to the latest version of Receiver, you must remove all applications and desktops to which you subscribed using an earlier version of the software.

Installing and Uninstalling Receiver for Mac Manually

Users can install Receiver from the Web Interface, a network share, or directly on to the user device by downloading the CitrixReceiver.dmg file from the Citrix Web site, at http://www.citrix.com.

To install Receiver for Mac

1. Download the .dmg file for the version of Receiver you want to install 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.
2. On the **Introduction** page, click **Continue.**
3. On the **License** page, click **Continue.**
4. Click **Agree** to accept the terms of the License Agreement.
5. On the **Installation Type** page, click **Install**.
6. Enter the administrator account details for the device on which you are installing Receiver and click **OK**.

Removing Receiver for Mac

You can uninstall Receiver manually by opening the CitrixReceiver.dmg file, selecting **Uninstall Citrix Receiver**, and following the on-screen instructions.

Using Merchandising Server to Deploy Receiver for Mac

You can use the Merchandising Server and Citrix Receiver (Updater) to deploy and update the Receiver for Mac plug-in on a user device.

Citrix Merchandising Server administrator console. With the administrator console, you can upload the plug-in installation and metadata files, create reuseable rules to define the delivery recipients, and create deliveries.

Citrix Receiver (Updater) After users install Receiver (Updater) on their user devices, Receiver (Updater) installs, updates, and starts the plug-in with minimal user interaction.

Users can change their Receiver for Mac plug-in settings using the **Application Delivery** pane in Citrix Receiver preferences.

Upgrading the Receiver for Mac Plug-in using Receiver (Updater)

Updates are, by default, automatically installed on the user device. When an update is available, Receiver (Updater) downloads and installs the updated version of the plug-in automatically.

Uninstalling the Receiver for Mac Plug-in using Receiver (Updater)

Receiver (Updater) upgrades the plug-in when a newer version is available. When users remove Receiver (Updater) manually, the plug-in is also removed. Additionally, the administrator can remove Receiver (Updater) and all of its managed plug-ins through the Merchandising Server Administrator Console.

For more information, see the Merchandising Server documentation.

Configuring Receiver for Mac

After the Receiver software is installed, there are a number of configuration steps to perform to allow users to access their hosted applications and desktops, as follows:

- Configuring Your XenApp or XenDesktop Environment. Ensure your XenApp or XenDesktop environment is configured correctly. Set up any Web Interface sites you require and configure the Access Gateway or Secure Gateway to provide users with secure access to their hosted applications and desktop.

- Configuring Access to Stores. Set up access to the stores hosting users' applications and desktops.

You can also configure Receiver using Merchandising Server. For more information, see the Merchandising Server documentation.

Configuring Your XenApp or XenDesktop Environment

Before your users can access hosted applications and desktops, you must configure your XenApp or XenDesktop deployment.

Configuring the Web Interface

If the Web Interface in your deployment does not have either a XenApp Services site or a XenDesktop Web site, create one. For more information, see the Web Interface documentation.

Configuring the Access Gateway or Secure Gateway

Receiver for Mac supports secure connections to an enterprise installation of the Access Gateway or Secure Gateway.

The process to enable connections from the Receiver for Mac is very similar to configuring the Access Gateway or Secure Gateway to accept Citrix XenApp connections, but with minor differences.

Traditionally, when configuring the Access Gateway or Secure Gateway for XenApp or XenDesktop connections, a Web Interface site provides information about the hosted applications and desktops that a user has rights to and presents them on a Web page with icons to click.

Secure Gateway or Access Gateway connections require a XenApp Services site or a XenDesktop Web site running on Web Interface 5.*x* for all platforms. This site gathers information about hosted application and desktops a user has access to and presents them in the Applications list on Receiver.

Both traditional connections (using Web Interface) and the Receiver for Mac (using XenApp Services or XenDesktop Web sites) can co-exist on the one Access Gateway or Secure Gateway installation.

For more information about configuring connections, including videos, blogs, and a support forum, refer to http://community.citrix.com. See also the Access Gateway or XenApp (for Secure Gateway) documentation.

Configuring Access to Stores

After installation, you must configure Receiver to provide users with access to the stores hosting their applications and desktops. You can configure access to stores:

- Automatically, using the Citrix Receiver for Mac URL Generator.
- Manually, using the **Stores** pane in Receiver **Preferences**.

If configuring access to stores manually, ensure you distribute the following information to users to enable them to connect to their hosted applications and desktops successfully:

- The domain name and location of the XenApp Services or XenDesktop Web site hosting resources; for example: https://servername
- For access using the Access Gateway, the Access Gateway address, product edition, and required authentication method

  For more information about configuring the Access Gateway or Secure Gateway, see the Access Gateway or XenApp (for Secure Gateway) documentation.

Configuring Stores Automatically

You can use the Citrix Receiver for Mac Setup URL Generator on a PC or Mac to configure access to new stores for all your users automatically. Use the utility to configure settings for the stores hosting your XenApp or XenDesktop resources and email that information to all your users at once.

To configure Receiver for Mac automatically

1. From a PC or Mac, open the Citrix Receiver for Mac Setup URL Generator from http://community.citrix.com/MacReceiverSetupUrlGenerator/.
2. For **Description**, enter a name for the account, such as the group or department. For example, Production or Sales.
3. Enter the name of the store to which your users connect in the **Store Address** box.
4. If you are using Access Gateway in your environment, select the edition deployed in the server farm to which your users connect from the **Access Gateway** list.
5. Enter the address of the Access Gateway in the **Gateway address** box.
6. Click **Generate URL**.
7. In **Your Result**, click **configuration link**, and copy the generated link.

Use email to send the link directly to users to complete the configuration of new stores for Receiver on the user device.

Configuring Stores Manually

When users launch Receiver for Mac for the first time, they are required to set up a new store. To do this, they must enter information about the XenApp farm or XenDesktop site hosting the resources they want to access.

When users enter the details for a new store, Receiver attempts to detect the configuration settings for that store automatically. If successful, the details for the store are displayed. If users enter an Access Gateway address, they must also provide details about the type of authentication required for connecting to a store through that Access Gateway.

Users can also enter the details for a new store manually, if required.

Note:

If you installed the Receiver plug-in using Receiver (Updater), you access Receiver preferences from the **Application Delivery** pane in the **Preferences** window.

To add a new store

1. Select **Preferences...** from the drop-down list and then select the **Stores** pane.
2. Click the **Plus** sign.
3. Enter a name for the new store in the **Store Name** field.
4. Enter the address of the new store (server) to which you want to connect in the **Store URL** field and click **OK**.

To connect to a new store

1. Open Citrix Receiver.
2. Choose the new store to which you want to connect from the drop-down list of available stores.
3. If requested, enter the user name and password for the new store and click **OK**.

   Note: If support for saving passwords is configured on the server, you can add these details to your keychain by selecting **Remember this password in my keychain**.

   After you connect to the new store, you can subscribe to applications and desktops hosted by that store.

To remove a store

1. Select **Preferences...** from the drop-down list and then select the **Stores** pane.
2. Select the store you want to remove from the **Stores** list.
3. Click the **Minus** sign, then click **OK** to confirm you want to remove the store from the list.

   Note: You can remove only those stores that you added manually. Stores delivered through Merchandising Server, and denoted by a padlock next to their entry in the **Stores** list, cannot be removed.

To edit the details of a store

1. Select **Preferences...** from the drop-down list and then select the **Stores** pane.
2. Double-click the store you want to edit.
3. Edit the details in **Store Name** and/or **Store URL** fields, as required.
4. Click **OK**.

   Note: You can edit the details only of those stores that you added manually. Stores delivered through Merchandising Server, and denoted by a padlock next to their entry in the **Stores** list, cannot be edited.

Optimizing Your Receiver Environment

You can optimize your environment to gain the best performance from Receiver by:

- Reconnecting Users Automatically
- Providing HDX Broadcast Session Reliability
- Reducing Display Latency
- Changing the Way You Use Receiver
- Improving the User Experience

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 HDX Broadcast auto-client reconnection feature, Receiver can detect unintended disconnections of ICA 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. Receiver 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.

You configure HDX Broadcast auto-client reconnect using policy settings on the server. For more information see the XenApp or XenDesktop documentation.

Providing HDX Broadcast Session Reliability

With the HDX Broadcast Session Reliability feature, users continue to see hosted application and desktop windows if the connection 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.

You configure HDX Broadcast Session Reliability using policy settings on the server. For more information see the XenApp or XenDesktop documentation.

Receiver users cannot override the server settings for HDX Broadcast Session Reliability.

Important: If HDX Broadcast 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. When enabled on the server, SpeedScreen Latency Reduction lessens the impact of high latency connections on your display.

You configure SpeedScreen Latency Reduction on the server, using Speedscreen Latency Reduction Manager. For more information, see your XenApp documentation.

Note: SpeedScreen Latency Reduction is not supported when connecting to XenApp for UNIX or XenDesktop.

Changing the Way You Use Receiver

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

Receiver provides a number of features for improving the user experience, as follows:

- **Cleartype font smoothing**. Also known as Sub-pixel font rendering, improves the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing.
- **Client device mapping**. Allows hosted applications and desktops to access local drives, COM ports, and printers attached to the user device.
- **Windows special keys substitution**. Allows users to substitute Windows special keys, such as function keys used in Windows applications, with keys on the Mac keyboard.
- **Keystroke forwarding**. Ensures that keystrokes made on the Mac keyboard that are normally picked up by the local Mac operating system are sent to the hosted application or desktop.

ClearType Font Smoothing

ClearType font smoothing (also known as Sub-pixel font rendering) improves the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing.

If you enable ClearType font smoothing on the server, you are not forcing user devices to use ClearType font smoothing. You are enabling the server to support ClearType font smoothing on user devices that have it enabled locally and are using Receiver.

Receiver automatically detects the user 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.

Client-Side Microphone Input

Receiver supports multiple client-side microphone input. Locally installed microphones can be used for:

- Real-time activities, such as softphone calls and Web conferences.
- Hosted recording applications, such as dictation programs.
- Video and audio recordings.

Digital dictation support is available with Receiver. For information about configuring this feature, see the administrator's documentation for Citrix XenApp or Citrix XenDesktop.

You can select whether or not to use microphones attached to your user device in sessions by choosing one of the following options from the Microphone tab in Receiver Preferences:

- **Use my microphone**.
- **Don't use my microphone**.
- **Ask me each time**.

If you select **Ask me each time**, a dialog box appears each time you connect to a hosted application or desktop asking whether or not you want to use your microphone in that session.

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 user 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 user device.

Mapping Client Drives

Client drive mapping allows you to access the local disk drives of the user 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, Receiver 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. 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).
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.

2. Click the + (plus) button.
3. Select an available drive letter.
4. Click **Browse.**
5. Select the folder on the Macintosh hard drive that you want to map and click **Browse**.
6. Click **Create**. The **Mapped Drives** pane now displays the mapped folder.
7. Select the level of read and write access for the mapped drive from the **Read** and **Write** pop-up menus.
8. Log off from 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 user device to be used during sessions. 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. Click **Devices**.
2. 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.
3. Select the device to associate with the virtual COM port from the **Device** pop-up menu.
4. Start Receiver and log on to a server.
5. Run a command prompt.
6. At the prompt, type `net use com`*x*`: \\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).
7. To confirm the mapping, type `net use` at the prompt. A list of mapped drives, LPT ports, and mapped COM ports is displayed.

Substituting Windows Special Keys

Receiver provides a number of extra options and easier ways to substitute special keys such as function keys in Windows applications with Mac keys. Use the **Keyboard** tab to 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.

If your keyboard includes a numeric keypad, 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
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

Forwarding Keystrokes made with Mac Keyboards

Remote sessions recognize most Mac keyboard combinations for text input, such as Option-G to input the copyright symbol ©. Some keystrokes you make during a session, however, do not appear on the remote application or desktop and instead are interpreted by the Mac operating system. This can result in keys triggering Mac 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 Mac keyboards do not have.

Keyboards and the ways keys are configured can differ widely between machines. Receiver therefore offers several choices to ensure that keystrokes can be forwarded correctly to hosted applications and desktops. These are listed in the table.

Important: Certain key combinations listed in the table are not available when using newer Mac keyboards. In most of these cases, keyboard input can be sent to the session using the **Keyboard** menu.

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 user device, some key combinations might not work as expected, and alternative combinations are listed.
- Fn refers to the Fn (Function) key on a Mac keyboard; function key refers to F1 to F12 on either a PC or Mac keyboard.

PC key	Mac 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
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 Fn–Down Arrow

PAGE UP	Page Up Fn–Up Arrow
SPACEBAR	Choose Keyboard > Send Key > Space
TAB	Choose Keyboard > Send Key > Tab

Securing Receiver Communications

You can implement a number of measures to secure the communication between your XenApp or XenDesktop servers and Receiver. You can integrate Receiver connections with your XenApp farm or XenDesktop site using 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 Receiver and servers. Receiver supports both SOCKS and secure proxy protocols.

When communicating with the XenApp or XenDesktop server, Receiver uses proxy server settings that are configured remotely on the server running the Web Interface. For information about configuring proxy server settings for Receiver, see the Web Interface documentation.

When communicating with the Web server, Receiver uses the proxy server settings that are configured for the default Web browser on the user device. You must configure the proxy server settings for the default Web browser on the user device accordingly.

Connecting with the Secure Gateway or Citrix Secure Sockets Layer Relay

You can integrate Receiver with the Secure Gateway or Secure Sockets Layer (SSL) Relay service. Receiver 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 Receiver and the server. No configuration of Receiver 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 the XenApp (Secure Gateway) documentation.

If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure Receiver 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 Receiver for Secure Gateway

Receiver uses settings that are configured remotely on the server running the Web Interface to connect to servers running the Secure Gateway.

When communicating with the Web server, Receiver uses the proxy server settings that are configured for the default Web browser on the user device. You must configure the proxy server settings for the default Web browser on the user 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 Receiver 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 your Web Interface server to use SSL/TLS encryption, see the XenApp and Web Interface documentation.

Configuring and Enabling Receiver 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 Receiver 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 your XenApp or XenDesktop server and your Web Interface server and obtain and install the necessary server certificate. For more information, see the XenApp and Web Interface documentation.
2. Install the equivalent root certificate on the user device.

Installing Root Certificates on User Devices

To use SSL/TLS to secure communications between SSL/TLS-enabled Receivers and the server farm, you need a root certificate on the user 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 user device.

Depending on your organization's policies and procedures, you may want to install the root certificate on each user 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:

   - **login** (the certificate applies only to the current user)

   - **System** (the certificate applies to all users of a device)

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, Receiver 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 user device to Web server communication. For Receiver 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 or XenDesktop server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address to Receiver. Receiver then connects to the server using the external address and port number. For more information, see the Web Interface documentation.