Receiver for Mac 11.5

2014-12-16 14:16:57 UTC

Contents

Receiver for Mac 11.5

About this Release

About Receiver for Mac

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.

Citrix Receiver for Mac has been enhanced for on-demand access to Windows, Web, and Software as a Service (SaaS) applications. You can use it for web access or configure it for use with Citrix CloudGateway.

What's New

Citrix Receiver for Mac 11.5 provides the following new features and enhancements for customers:

- **CloudGateway Express Interoperability**. Enables existing XenApp and XenDesktop customers to deliver all their Windows apps and desktops to any device using a unified StoreFront with self-service.
- **CloudGateway Enterprise Interoperability**. Enables enterprises to aggregate, control, and deliver all of their Windows, web and software-as-a-service (SaaS) applications to any user on any device.
- **Pass-through authentication to AppController**. When used with Receiver Storefront 1.1, once logged on to Citrix Receiver, users can access Web and SaaS applications through AppController without needing to authenticate again. No Receiver-specific administration is needed to use pass-through authentication support.
- **Flexible installation methods**. You can install Receiver for Mac from Receiver for Web and Web Interface or you can use Electronic Software Distribution (ESD) tools like Casper Suite.
- **Self-service**. Citrix Receiver displays all the resources that you make available to users. Users can browse the list or search for the resources they require and subscribe with a single click. Enabled using one-click configuration and CloudGateway.
- **One-click configuration**. Opening a service record after installing Citrix Receiver activates self-service access to CloudGateway-published resources. You can publish a service record on a web site or email it to multiple users.
- **Auto-provisioned applications**. Receiver automatically adds administrator-designated applications when users first authenticate. Requires CloudGateway StoreFront.

- **Receiver for all devices**. User experience is consistent across Receiver platforms and devices.
- **Follow-me subscriptions**. Users' selected applications follow them across devices. Requires CloudGateway StoreFront.
- **Workspace control**. Provides users with the ability to roam. They can disconnect quickly from all running applications and desktops and reconnect to them. Workspace control enables users to move between user devices and gain access to all of their desktops or open applications when they log on.

Known Issues

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

- Users can stop and start Receiver and then open applications without having to log back in. This occurs because the Authentication Manager process continues running after Receiver closes. If you require users to log back in to Receiver before opening applications, ensure users log out from their Mac OS account to stop the Authentication Manager process, before logging back in and restarting Receiver. [#0286171]
- If your DNS server is set up to redirect users to an error page when a server address cannot be resolved, Receiver treats that error page as a valid beacon point. [# 0299020]

Issues Fixed in this Release

The following issues have been fixed since the previous release of this product:

- Graphics in a shadowed session are corrupted when initiating shadowing from a published Access Management Console. [#0048222]
- UTF8 characters in filenames are missing or displayed incorrectly when viewed using client drive mapping. [# 0008606, # 0010954, # 0035966]
- When session reliability is disabled, sessions take a long period of time (up to 9 minutes) to timeout if the network connection is lost. [# 0031797]
- Sessions disconnect and reconnect intermittently when session reliability is enabled. [#0027128]
- Printing fails due to a printer driver crash. [#0298902]

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
- 62.3 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 products):
  - Citrix XenApp 6.5 for Windows Server 2008 R2
  - 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 products):
  - XenDesktop 5.5
  - XenDesktop 5
  - XenDesktop 4
- Receiver Storefront 1.0
- Receiver for Web 1.0
- Cloud Gateway Enterprise 1.0
- Merchandising Server 2.x

Note: If your user device is running Mac OS X 10.7, Merchandising Server 2.2 is required.

Browser

- Safari Version 5.x
- Mozilla Firefox Versions 3.x through 10.x
- Google Chrome 17.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 with a XenApp Services or XenDesktop Web site
- Receiver for Web sites

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, Receiver verifies the authenticity of the remote gateway's SSL certificate against a local store of trusted root certificate authorities. Receiver 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 user device in order to successfully access Citrix resources using Receiver.

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

Receiver for Mac 11.5, when used with Receiver StoreFront 1.0, supports the following authentication methods:

- Domain
- Security token
- Two-factor (domain plus security token)*

Receiver for Mac 11.5, when used with Web Interface 5.X, supports the following authentication methods:

- Domain
- Security token
- Two-factor (domain plus security token)*

* These authentication methods are available only in deployments that include Access Gateway.

For more information about authentication, including certificate requirements, see the Receiver StoreFront documentation.

Upgrades

Upgrading to Receiver for Mac, Version 11.5 is supported from versions 10.x and 11.x of the Online Plug-in for Mac. You can also upgrade from versions 11.3 and 11.4 of the Receiver for Mac.

Availability of Receiver for Mac 11.5 features

Some of the features and functionality of Receiver are available only when connecting to newer versions of XenApp and XenDesktop and may also require the latest hotfixes for those products.

Installing Receiver for Mac

This release contains a single installation package, CitrixReceiver.dmg, and supports remote access through both Access Gateway and Secure Gateway. Receiver can be installed:

- Automatically from the Web Interface
- By a user
- Using an Electronic Software Distribution (ESD) tool

Upgrading to Receiver for Mac, Version 11.5 is supported from versions 10.x and 11.x of the Online Plug-in for Mac. You can also upgrade from versions 11.3 and 11.4 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.
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.

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 Accounts. 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 Accounts

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

- Automatically, by creating provisioning files and making those files available to users through email or on a Web site.
- Manually, using the **Accounts** pane in Receiver **Preferences**.

If configuring access to accounts 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 Receiver for Web, 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.

Setting up Access to Accounts Automatically

You can use Receiver StoreFront to create provisioning files containing connection details for accounts. You make these files available to your users to enable them to configure Citrix Receiver automatically. If you configure Receiver for Web sites, users can also obtain Citrix Receiver provisioning files from those sites. For more information see the Receiver StoreFront documentation.

Setting up Access to Accounts Manually

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

When a user enters the details for a new account, Receiver attempts to verify the connection. If successful, Receiver prompts the user to log on to the account.

To add a new account

1. Click the gear icon in the Receiver window and choose **Preferences**.
2. Click the **Accounts** tab.
3. Click the **Plus** sign.
4. Enter the information provided by your organization and click **OK**.

To remove an account

1. Click the gear icon in the Receiver window and choose **Preferences**.
2. Click the **Accounts** tab.
3. Select the account you want to remove from the list.
4. 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 an account

1. Click the gear icon in the Receiver window and choose **Preferences**.
2. Click the **Accounts** tab.
3. Select the account that you want to edit from the list and double-click.
4. Edit the details in **Server URL**and the **Description** fields, as required.
5. 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 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
- Providing Continuity for Roaming Users
- Mapping Client Devices
- Changing the Way You Use Receiver

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.

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 XenApp 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.

Providing Continuity for Roaming Users

Workspace control lets desktops and applications follow users as they move between devices. This enables, for example, clinicians in hospitals to move from workstation to workstation without having to restart their desktops and applications on each device.

Policies and client drive mappings change appropriately when you move to a new user device. Policies and mappings are applied according to the user device where you are currently logged on to the session. For example, if a health care worker logs off from a user device in the emergency room of a hospital and then logs on to a workstation in the hospital's X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect for the session as soon as the user logs on to the user device in the X-ray laboratory.

To configure workspace control settings

1. Click the gear icon  in the Receiver window and choose **Preferences**.
2. Click the **General** tab.
3. Choose one of the following:
   - **Reconnect apps when I start Receiver**. Allows users to reconnect to disconnected apps when they start Receiver.
   - **Reconnect apps when I start or refresh apps**. Allows users to reconnect to disconnected apps either when they start apps or when they select **Refresh Apps** from the Citrix Receiver menu.

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.

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

You can improve your users' experience with the following supported features:

- Cleartype font smoothing
- Client-side microphone input
- Windows special keys substitution
- Keystroke forwarding
- Client-side Input Method Editor (IME) and International Keyboard Layout support

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 XenApp and XenDesktop documentation.

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 Mic & Webcam tab in Receiver Preferences:

- **Use my microphone and webcam**
- **Don't use my microphone and webcam**
- **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.

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

Using IME and International Keyboard Layouts

Receiver allows you to use an IME on either the user device or on the server.

When client-side IME is enabled, users can compose text at the insertion point rather than in a separate window.

Receiver also allows users to specify the keyboard layout they wish to use.

To enable client-side IME

1. From the **Citrix Viewer** menu bar, choose **Keyboard** > **International** > **Use Client IME**.
2. Ensure the server-side IME is set to direct input or alphanumeric mode.
3. Use the Mac IME to compose text.

To explicitly indicate the starting point when composing text

- From the **Citrix Viewer** menu bar, choose **Keyboard** > **International** > **Use Composing Mark**.

To use server-side IME

- Ensure the client-side IME is set to alphanumeric mode.

Mapped server-side IME input mode keys

Receiver provides keyboard mappings for server-side Windows IME input mode keys that are not available on Mac keyboards. On Mac keyboards, the Option key is mapped to the following server-side IME input mode keys, depending on the server-side locale:

Server-side system locale	Server-side IME input mode key

Japanese	**Kanji key** (Alt + Hankaku/Zenkaku in Japanese keyboard)
Korean	**Right-Alt key** (Hangul/English toggle on Korean keyboard)

To use international keyboard layouts

- Ensure both client-side and server-side keyboard layouts are set to the same locale as the default server-side input language.

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:

- Access Gateway
- 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
- SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
- A firewall

Connecting with Access Gateway Enterprise Edition

This topic applies only to deployments using the Web Interface.

Configure the XenApp Services site for Receiver to support connections from an Access Gateway connection.

1. In the XenApp Services site, select **Manage secure client access > Edit secure client access settings**.
2. Change the Access Method to **Gateway Direct**.
3. Enter the FQDN of the Access Gateway appliance.
4. Enter the Secure Ticket Authority (STA) information.

To configure the Access Gateway appliance

1. Configure authentication policies to authenticate users connecting to the Access Gateway by using the Access Gateway Plug-in. Bind each authentication policy to a virtual server.

   - If double-source authentication is required (such as RSA SecurID and Active Directory), RSA SecurID authentication must be the primary authentication type. Active Directory authentication must be the secondary authentication type.

   - RSA SecurID uses a RADIUS server to enable token authentication.

   - Active Directory authentication can use either LDAP or RADIUS.

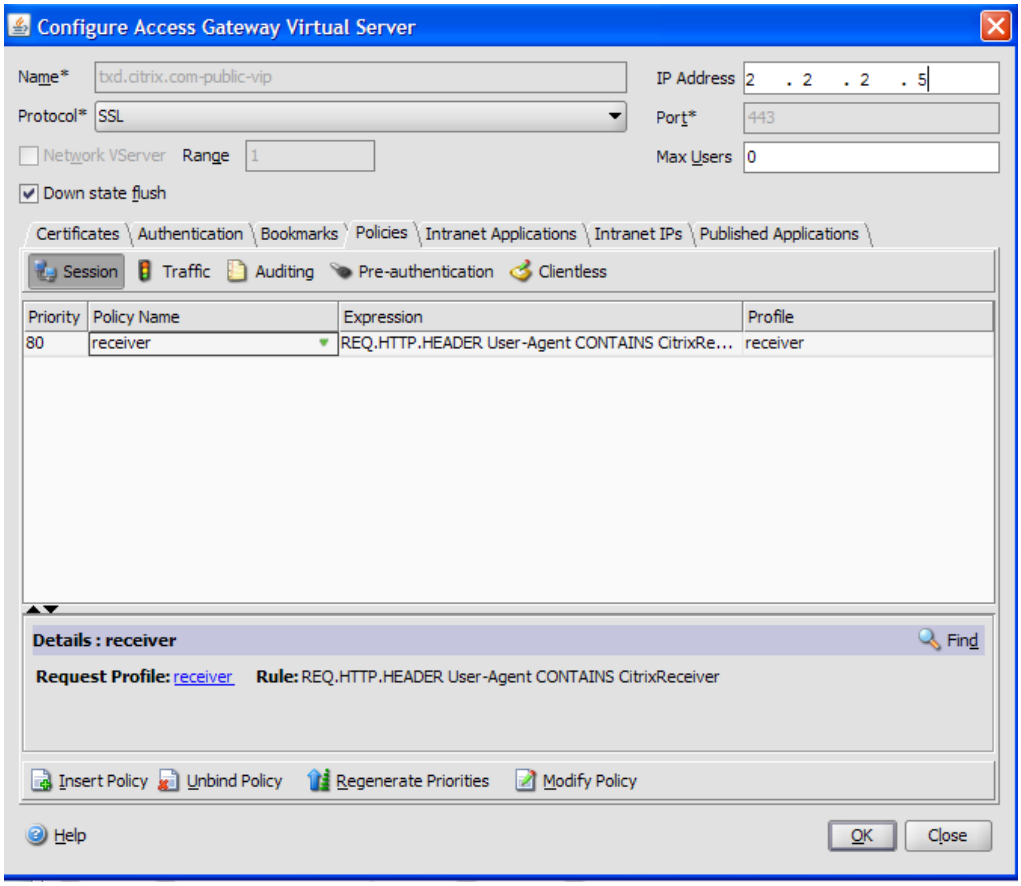
   Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. Create a session policy on the Access Gateway to allow incoming XenApp connections from the Receiver, and specify the location of your newly created XenApp Services site.

   -

   Create a new session policy to identify that the connection is from the Receiver. As you create the session policy, configure the following expression and select **Match All Expressions** as the operator for the expression:

   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver



- In the associated profile configuration for the session policy, on the **Security** tab, set **Default Authorization** to **Allow**.

  On the **Published Applications** tab, if this is not a global setting (you selected the **Override Global** check box), ensure the **ICA Proxy** field is set to **ON**.

  In the **Web Interface Address** field, enter the URL including the config.xml for the XenApp Services site that the device users use, such as http://XenAppServerName/Citrix/PNAgent/config.xml or http://XenAppServerName/CustomPath/config.xml.

- Bind the session policy to a virtual server.

- Create authentication policies for RADIUS and Active Directory.

- Bind the authentication policies to the virtual server.

Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway documentation.

Connecting with Access Gateway 5.0

This topic applies only to deployments using the Web Interface.

Access Gateway setup requires that you configure a basic or a SmartAccess logon point on Access Gateway and use the Web address for the XenApp Services site.

Before you configure a logon point, install the Web Interface and verify that it is communicating with the network. When you configure a logon point, you must also configure at least one Secure Ticket Authority (STA) server and ICA Access Control in Access Gateway. For more information, expand Access Gateway 5.0 in eDocs, and locate the topic *To configure Access Gateway to use the Secure Ticket Authority*.

To configure the Access Gateway 5.0 appliance

1. Configure Authentication profiles to authenticate users connecting to the Access Gateway using the Receiver.

   - If double source authentication is required (such as Active Directory and RSA SecurID), Active Directory authentication must be the primary authentication type. RSA SecurID authentication must be the secondary authentication type.

   - RSA SecurID can use either RADIUS or an sdconf.rec file to enable token authentication.

   - You can configure Active Directory authentication on Access Controller. You can use Active Directory on the Access Gateway appliance by using either an LDAP or RADIUS authentication profile.

   Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. To establish communication with XenApp servers and the Web Interface, configure the Access Gateway with STA servers and the ICA Access Control list on Access Gateway. For more information, see the Access Gateway section of eDocs.

3. Configure logon points on the Access Gateway. Configure the Access Gateway to allow incoming XenApp connections from the Receiver, and specify the location of your Web Interface site.

   a. In the Access Gateway Management Console, click **Management**.

   b. Under **Access Control**, click **Logon Points** > **New**.

   c. In the **Logon Points Properties** dialog box, in **Name**, type a unique name for the logon point.

   d. Select the **Type**:

      For a **Basic** logon point, in the **Web Interface** field, type the fully qualified domain name (FQDN) of the Web Interface, such as `http://xenapp.domain.com/citrix/apps`. You cannot configure a SmartGroup with a basic logon point. Select the authentication type, or click **Authenticate with the Web Interface**.

      If you select **Authenticate with the Web Interface**, when users type the URL to Access Gateway and enter credentials, the credentials are passed to the Web Interface for authentication.

      - For a SmartGroup to use the settings in a **SmartAccess** logon point, you must select the logon point within the SmartGroup. Select the authentication profiles. If you configure a SmartAccess logon point, Access Gateway authenticates users. You cannot configure authentication by using the Web Interface.

        If you select **Single Sign-on to Web Interface**, users do not have to log on to the Web Interface after logging on to the Access Gateway. If not selected, users must log on to both the Access Gateway and Web Interface.

e. Under **Applications and Desktops**, click **Secure Ticket Authority** and add the STA details. Make sure the STA information is the same as the Web Interface site.

f. Finally, under **Applications and Desktops**, click **XenApp or XenDesktop** to add the ICA control list (required for Access Gateway 5.0). For more information, expand Access Gateway 5.0 in eDocs, and locate *To configure ICA Access Control*.

Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway section on *Configuring Intermediate Certificates*.

To configure Access Controller

1. Configure Authentication profiles to authenticate users connecting to the Access Gateway using the Receiver.

   - If double source authentication is required (such as Active Directory and RSA SecurID), Active Directory authentication must be the primary authentication type. RSA SecurID authentication must be the secondary authentication type.

   - RSA SecurID can use either RADIUS or an sdconf.rec file to enable token authentication.

   - You can configure Active Directory authentication on Access Controller. You can use Active Directory on the Access Gateway appliance by using either an LDAP or RADIUS authentication profile.

   Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. To establish communication with XenApp servers and the Web Interface, configure Access Controller to recognize the servers. Configure Access Controller to allow incoming XenApp connections from the Receiver and specify the location of your Web Interface site.

   a. In the Deliver Services Console, expand **Citrix Resources** > **Access Gateway**, and then click the Access Controller on which you want to create the Web resource.

   b. Expand **Resources**, click **Web Resources**, and then under **Common tasks**, click **Create Web resource**. In the wizard, enter a unique name. On the **New Web Address** page, enter the Web address URL of the XenApp Web site.

   c. In **Application type**, select **Citrix Web Interface** and click the **Enable Single Sign-on** check box.

   d. After you click OK, click **Publish for users in their list of resources** , and then in **Home page**, enter the URL of the XenApp Web Site, such as `http://xenapp.domain.com/citrix/apps`, and finish the wizard.

   e. In the navigation pane, click **Logon Points**, click **Create logon point**, and in the wizard, enter a unique name, and select the type:

      For a **Basic** logon point, in the **Web Interface** field, type the fully qualified domain name (FQDN) of the Web Interface, such as `http://xenapp.domain.com/citrix/apps`. Select the Home page, and then select the authentication profile. Leave the remaining options as default values, and click **Enable this logon point** check box at the end of the wizard.

      - For a **SmartAccess** logon point, on **Select Home Page**, select the **Display the Web resource with the highest priority**. Click **Set Display Order**, and move the Web Interface Web resource to the top.

        Select the Authentication Profiles for both authentication and group extraction. Leave the remaining options as default values, and click **Enable this logon point** check box at the end of the wizard.

   f. In the navigation pane, under **Policies** > **Access Policies**, select **Create access policy** and on the **Select Resources** page, expand **Web Resources** to select the

Web Interface web resource.

g. In Configure Policy Settings, select the settings, click **Enable this policy to control this setting**, and select **Extended access, unless denied by another policy**. Add the users allowed to access this resource and finish the wizard.

h. In the navigation pane, under **Access Gateway appliances**, select **Edit Access Gateway appliance properties**, click **Secure Ticket Authority** and add the STA details. Make sure the STA information is the same as the Web Interface site.

i. Finally, click **ICA Access Control** to add the ICA control list (required for Access Gateway 5.0). For more information, expand Access Gateway 5.0 in eDocs, and locate *To configure ICA Access Control* in the Access Controller documentation.

Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway section on *Configuring Intermediate Certificates*.

Connecting with the Secure Gateway

This topic applies only to deployments using the Web Interface.

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*.

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 Secure Sockets Layer Relay

You can integrate Receiver with the 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 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.