Receiver for Mac 11.8.x

2015-05-17 05:23:24 UTC

Contents

Receiver for Mac 11.8.x

New in Receiver for Mac 11.8.2

This release of Citrix Receiver improves compatibility with the Mac OS X Mavericks multi-monitor feature and fixes the following issues:

- Gatekeeper settings don't prevent you from uninstalling Receiver.
- Sessions no longer become unresponsive when a font fails to load.
- The desktop toolbar Home button can now show the desktop image, if it's available.
- Displaying tooltips no longer changes the order of stacked windows on your desktop.
- Sessions no longer become unresponsive after opening a folder with a large number of similarly named subfolders.

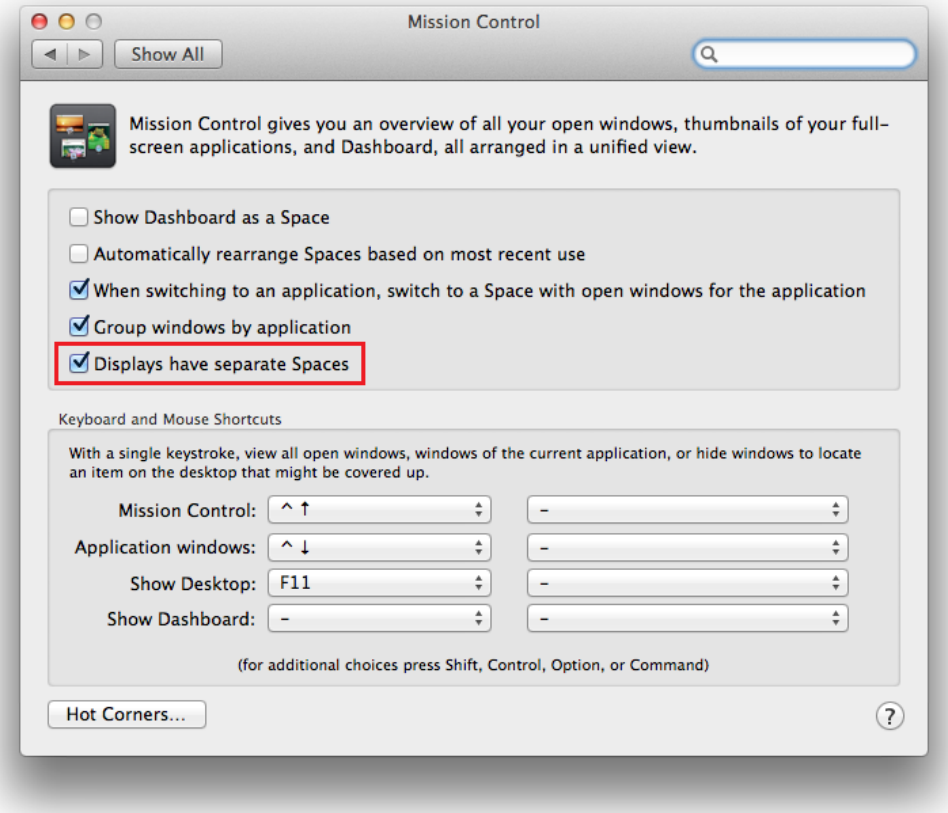
For a complete and more detailed list of issues fixed in this release see CTX138200.

Using multiple monitors on Mac OS X Mavericks

To use Citrix Receiver for Mac 11.8.2 across multiple monitors on Mac OS X Mavericks

1. Open System Preferences.
2. Open Mission Control.

3.



Uncheck Displays have separate Spaces.

4. Log out and log back in.

For more information about Receiver for Mac 11.8.x

About this release	Configure Receiver for Mac
Known issues	Optimize your Receiver environment
System requirements for Receiver for Mac 11.8.x	Improve the user experience
Install, set up, and upgrade Receiver for Mac	Secure Receiver communications

About Receiver for Mac 11.8

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.

Receiver also provides on-demand access to Web and Software as a Service (SaaS) applications. You can use it for Web access or configure it for use with Citrix CloudGateway or XenMobile App Edition.

What's new in the 11.8

The following new features and enhancements are available in this release:

- **XenDesktop 7 support** - Receiver supports the many enhancements provided by XenDesktop 7 including support for IPv6 connections. No configuration of this feature is required.
- **Desktop restart** - Users can restart virtual desktops in Citrix StoreFront if they stall or become corrupted. You configure this feature in XenDesktop.
- **H.264 decoding** - HDX 3D Pro graphics from XenDesktop 7 servers can be displayed. This provides better performance of rich and professional graphics applications on WANs and in public clouds. No configuration of this feature is required.
- **HDX Insight support** - HDX Insight is the integration of EdgeSight network analysis and EdgeSight performance management with Director. With this support now in Receiver, XenDesktop administrators can check performance metrics related to the health of this component. No configuration of this feature is required.
- **Windows shortcuts** - Support for Windows logo key shortcuts is built into the Keyboard menu. This allows Mac users to send Windows shortcuts to their remote desktops and applications.
- **StoreFront 2.0 support** – Receiver supports the many enhancements provided by StoreFront 2.0 including support for IPv6 connections.

Known issues for 11.8.x

The following known issues have been observed in this release.

Printers connected to the user device might not appear in Devices and Printers (a Control Panel item) on a Windows 8 virtual desktop. This occurs because no PostScript printer driver is present on Windows 8. To work around this issue, install a suitable driver on the Windows 8 master image. [#390559]

If you encounter a paywall, and then authenticate to it, pay for services on it, or accept the terms and conditions on it, Receiver does not start. To work around this issue, restart

your wireless network connection. [#381777]

When you connect to a virtual desktop, only a part of it is visible in the Citrix Viewer and, when you move the mouse, desktop items are briefly displayed but then disappear. This issue is only observed in multimonitor arrangements and when the available video memory on the user device is exceeded. To work around the issue, set ConnectionBar to 1 in default.ica for the site on which the desktop is delivered. [#399198]

If, on the user device, the Gatekeeper option Allow applications downloaded from is set to Mac App Store and identified developers, you cannot uninstall Receiver and an error is displayed. To work around this issue, temporarily set this option to Anywhere, uninstall Receiver, and then readjust the option. This issue is fixed in Receiver for Mac 11.8.2. [#400208]

Issues fixed in 11.8

For a list of issues that have been fixed in version 11.8, see CTX138200.

System requirements for Receiver for Mac 11.8.x

Supported operating systems for Receiver for Mac 11.8.2

- Mac OS X Mavericks (version 10.9)
- Mac OS X 10.8
- Mac OS X 10.7
- Mac OS X 10.6

Supported operating systems for Receiver for Mac 11.8

- Mac OS X 10.8
- Mac OS X 10.7
- Mac OS X 10.6

Hardware Requirements

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

Supported Servers

- 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
- XenDesktop (any of the following products):
  - XenDesktop 7.1
  - XenDesktop 7
  - XenDesktop 5.6, Feature Pack 1
  - XenDesktop 5.6
  - XenDesktop 5.5
  - XenDesktop 5
  - XenDesktop 4
- Citrix VDI-in-a-Box 5.2, 5.1, and 5.3
- To manage connections to applications and desktops, Citrix Receiver supports XenMobile App Edition with StoreFront, and CloudGateway with StoreFront or Web Interface.

  XenMobile App Edition:
  - XenMobile App Edition 8.5 or 8.6, with Storefront 2.0, for direct access to StoreFront stores

  CloudGateway:
  - CloudGateway Express, with Storefront 2.0 or 1.2, for direct access to StoreFront stores
  - CloudGateway Express, with StoreFront 2.0, 1.2, 1.1, or 1.0 configured with a Receiver for Web site, for access to StoreFront stores from a Web browser
  - CloudGateway Enterprise 2.0 or 1.0, with Storefront 2.0, 1.2, 1.1, or 1.0, for access to Windows, Web, and Software as a Service (SaaS) applications

  StoreFront:
  - StoreFront 2.0 or 1.2

  Web Interface:
  - Web Interface 5.4 for Windows with XenApp Services (also known as PNAgent Services) sites, for access to applications natively from Receiver rather than from a web browser.

- To deploy Receiver:
  - Citrix Receiver for Web 2.0 or 1.2
  - Citrix Web Interface 5.4

Supported Browsers

- Safari 7.0 and 6.x
- Mozilla Firefox 24.x, 23.x, and 22.x
- Google Chrome 30.x, 29.x, and 28.x

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:
  - StoreFront using StoreFront services or Receiver for Web sites.

    Single sign-on to Web and SaaS applications published through App Controller requires StoreFront 2.0, 1.2, or 1.1.
  - Web Interface 5.4 for Windows, using XenApp Services sites.
- For secure remote or local connections:
  - Citrix NetScaler Gateway 10.1
  - Citrix Access Gateway Enterprise Edition 10.x
  - Citrix Access Gateway Enterprise Edition 9.*x*
  - Citrix Access Gateway VPX
  - Citrix Access Gateway 5.0
  - Citrix Secure Gateway 3.*x* (for use with Web Interface only)

  For information about deploying Access Gateway or NetScaler Gateway with StoreFront, see the Access Gateway or NetScaler Gateway documentation, and the StoreFront documentation, in eDocs.

Authentication

For connections to StoreFront, Receiver supports the following authentication methods:

- Domain
- Security token*

- Two-factor (domain plus security token)*
- SMS*
- User certificate* (the user certificate can be used alone or in combination with other authentication methods)
- Smartcard (smartcard authentication can be used with Receiver for Web [StoreFront 2.5], with or without NetScaler Gateway)

*Available only for Receiver for Web sites and for deployments that include NetScaler Gateway, with or without installing the associated plug-in on the device.

For connections to XenMobile App Controller, Receiver supports the following authentication methods:

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

For connections to Web Interface 5.4, Receiver supports the following authentication methods:

Note: Web Interface uses the term Explicit to represent domain and security token authentication.

- Domain
- Security token*
- Two-factor (domain plus security token)*
- SMS*
- User certificate (user certificate authentication requires NetScaler Gateway plug-ins)

* Available only in deployments that include NetScaler Gateway, with or without installing the associated plug-in on the device.

For information about authentication, refer to the NetScaler Gateway or Access Gateway documentation, and the StoreFront documentation, in eDocs. For information about other authentication methods supported by Web Interface, refer to the topic *Configuring Authentication for the Web Interface* in the Web Interface documentation in eDocs.

Install, set up, and upgrade Receiver for Mac

Installation

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

- By a user from Citrix.com
  - A first-time Receiver user who obtains Receiver from Citrix.com or your own download site can set up an account by entering an email address instead of a server URL. Receiver determines the Access Gateway, StoreFront server, or the App Controller virtual appliance associated with the email address and then prompts the user to log on and continue the installation. This feature is referred to as "email-based account discovery."

    Note: A first-time user is one who does not have Receiver installed on their user device.

  - Email-based account discovery for a first-time user does not apply if Receiver is downloaded from a location other than Citrix.com (such as a Receiver for Web site).

  - If your site requires configuration of Receiver, use an alternate deployment method.
- Automatically from Receiver for Web or from Web Interface
  - A first-time Receiver user can set up an account by entering a server URL or downloading a provisioning file.
- Using an Electronic Software Distribution (ESD) tool
  - A first-time Receiver user must enter a server URL to set up an account.

Setup

For deployments with StoreFront:

- Best practice is to configure NetScaler Gateway and StoreFront 2.0 as described in the documentation for those products in Citrix eDocs. Attach the provisioning file created by StoreFront to an email and inform users how to upgrade and to open the provisioning file after installing Receiver.

- As an alternative to using a provisioning file, tell users to enter either the URL of a NetScaler Gateway or, if you have configured email-based account discovery as described in the StoreFront documentation, their email address.

- Another method is to configure a Receiver for Web site as described in the StoreFront documentation. Inform users how to upgrade Receiver, access the Receiver for Web site, and download the provisioning file from the Receiver for Web interface (click the user name and click Activate).

For deployments with Web Interface

- If you are using App Controller, configure the connectors as described in the App Controller documentation in eDocs.
- Upgrade your Web Interface site with Receiver for Mac 11.8 and let your users know how to upgrade Receiver. You can, for example, provide users with installation captions on their Messages screen to let them know they need to upgrade to the latest version of Receiver.

Upgrade to Receiver for Mac 11.8

Upgrades are supported from versions 10.x and 11.x of the Online Plug-in for Mac. You can also upgrade from versions 11.3, 11.4, 11.5, 11.6, and 11.7.x of the Receiver for Mac.

ShareFile integration is removed from Version 11.8. If you integrated the Receiver with ShareFile, when upgrading you are prompted to download the ShareFile application so that you can continue to access your remote data.

Install 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.

Important: A user must be an administrator for the device on which they want to install or uninstall 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.

Uninstall Receiver for Mac manually

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

Deploy Receiver from Receiver for Web

You can deploy Receiver from Receiver for Web to ensure that users have it installed before they try to connect to an application from a browser. Receiver for Web sites enable users to access StoreFront stores through a Web page. If the Receiver for Web site detects that a user does not have a compatible version of Receiver, the user is prompted to download and install Receiver. For more information, see the StoreFront documentation.

Deploy Receiver from a Web Interface logon screen

You can deploy Receiver from a Web page to ensure that users have it installed before they try to use the Web Interface. The Web Interface provides a client detection and deployment process that detects which Citrix clients can be deployed within the user's environment and then guides them through the deployment procedure.

You can configure the client detection and deployment process to run automatically when users access a XenApp Web site. If the Web Interface detects that a user does not have compatible version of Receiver, the user is prompted to download and install Receiver.

As an alternative, you can provide users with installation captions, which are links that are presented to users on the Messages screen. Users click a link to start the client detection and deployment process. You can also use installation captions to enable users to access the client detection and deployment process to upgrade their Citrix clients to a newer version.

To use the client detection and deployment process, the Receiver installation files must be available on the Web Interface server. By default, the Web Interface assumes that the file names of the Receiver installation files are the same as the files supplied on the XenApp or XenDesktop installation media. If you download Receiver from the Citrix Web site or if you plan to deploy older versions of Receiver, check that the appropriate Receiver installation file names are specified for the ClientIcaMac parameter in the configuration files for your XenApp Web sites.

For more information, see the Web Interface documentation.

Configure Receiver for Mac

After the Receiver software is installed, the following configuration steps allow users to access their hosted applications and desktops:

- Configure your XenApp environment - Ensure your XenApp environment is configured correctly. Set up any Web Interface sites you require and configure NetScaler Gateway, Access Gateway, or Secure Gateway to provide users with secure access to their hosted applications and desktop.
- Configure StoreFront - Create stores that enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and App Controller, making these resources available to users.
- Provide Users with Account Information - Provide users with the information they need to set up access to accounts hosting their applications and desktops. In some environments, users must manually set up access to accounts.

Availability of Receiver for Mac features

Some of the features and functionality of Receiver are available only when connecting to newer XenApp and XenDesktop versions and might require the latest hotfixes for these products and other Citrix components in your deployment.

Configure your XenApp environment

Before your users access applications hosted in your XenApp deployment, configure the following components in your deployment as described here.

- When publishing applications on your XenApp farms, consider the following options to enhance the experience for users accessing those applications through Storefront stores:
  - Ensure that you include meaningful descriptions for published applications, as these descriptions are visible to users in Citrix Receiver.
  - To automatically subscribe all users of a store to an application, append the string KEYWORDS:Auto to the description you provide when you publish the application in XenApp. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.
  - To advertise applications to users or make commonly used applications easier to find by listing them in Citrix Receiver's Featured list, append the string KEYWORDS:Featured to the application description.

  For more information see the StoreFront documentation.
- If the Web Interface of your XenApp deployment does not have a XenApp Services site, create one. The name of the site and how you create it depends on the version of the Web Interface you have installed. For more information, see the Web Interface documentation.

Configure StoreFront

To configure StoreFront

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Receiver. Create stores that enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and App Controller, making these resources available to users.

1. Install and configure StoreFront. For more information, see the StoreFront documentation.

   Note: For administrators who need more control, Citrix provides a template you can use to create a download site for Receiver.

2. Configure stores for CloudGateway just as you would for other XenApp and XenDesktop applications. No special configuration is needed for Receiver. For more information, see *Configuring Stores* in the StoreFront documentation.

To configure the App Controller

In this section, except where specific versions of AppController are mentioned, this component is referred to as App Controller, the new name for AppController.

In addition to providing access to applications published for XenApp and XenDesktop, you can use App Controller, a component of CloudGateway Enterprise, to provide URLs for Web and SaaS apps on your internal network. If you use email-based account discovery, Receiver determines the App Controller associated with a user's email address.

If you do not use email-based account discovery, provide users with a provisioning file that configures Receiver with the settings needed to connect to App Controller. From the AppController 2.5 console, you can email a provisioning file (.cr) to users. Alternatively, if you configure a Receiver for Web site, users can obtain a Receiver provisioning file from that site by clicking Activate in Receiver. For more information, see the App Controller documentation.

To configure NetScaler Gateway or Access Gateway

If you have users who connect from outside the internal network (for example, users who connect from the Internet or from remote locations), configure authentication through NetScaler Gateway or Access Gateway. For more information see the NetScaler Gateway or Access Gateway documentation.

Provide users with account information

After installation, you must provide users with the account information they need to access their hosted applications and desktops. You can provide this information by:

- Configuring email-based account discovery
- Providing users with a provisioning file
- Providing users with an auto-generated setup URL
- Providing users with account information to enter manually

Configure email-based account discovery

You can configure Receiver to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Receiver installation and configuration. Receiver determines the NetScaler Gateway, Access Gateway, or StoreFront server, or the App Controller virtual appliance associated with the email address based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access their hosted applications and desktops.

To configure your DNS server to support email-based discovery, see the topic *Configuring Email-based Account Discovery* in the StoreFront documentation.

To configure NetScaler Gateway or Access Gateway to accept user connections by using an email address to discover the StoreFront, NetScaler Gateway, or Access Gateway URL, see *Connecting to StoreFront by Using Email-Based Discovery* in the NetScaler Gateway or Access Gateway documentation.

Provide users with a provisioning file

You can use StoreFront to create provisioning files containing connection details for accounts. You make these files available to your users to enable them to configure Receiver automatically. After installing Receiver, users simply open the file to configure Receiver. If you configure Receiver for Web sites, users can also obtain Receiver provisioning files from those sites.

For more information, see the StoreFront documentation.

Provide users with an auto-generated setup URL

You can use the Citrix Receiver for Mac Setup URL Generator to create a URL containing account information. After installing Receiver, users simply click on the URL to configure their account and access their resources. Use the utility to configure settings for accounts and email or post that information to all your users at once.

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. Enter the address of the NetScaler Gateway in the Gateway address box.
5. Click Generate URL.
6. In Your Result, copy the generated link.

Use email to send the link directly to users, or post the URL to a Web site that users can access. That allows them to complete the configuration of new accounts on their device.

Provide users with account information to enter manually

If providing users with account details to enter manually, ensure you distribute the following information to enable them to connect to their hosted and desktops successfully:

- The URL for the StoreFront store or XenApp Services site hosting resources; for example: https://servername.company.com
- For access using NetScaler Gateway or Access Gateway: the NetScaler Gateway or Access Gateway address, product edition, and required authentication method

  For more information about configuring NetScaler Gateway or Access Gateway, see the NetScaler Gateway or Access Gateway documentation.

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.

Optimize your Receiver environment

You can optimize your environment to gain the best performance from Receiver, as follows:

- Reconnect users
- Provide HDX Broadcast session reliability
- Provide continuity for roaming users
- Map client devices
- Change the way you use Receiver

Reconnect users

Reconnect 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 and XenDesktop documentation.

Restart desktops

Users can restart a virtual desktop if it fails to start, takes too long to connect to, or becomes corrupted. You configure this feature in XenDesktop.

The contextual menu item Restart is available on all of the desktops that users subscribe to, and on users' App page. The menu item is disabled if restart is not enabled for the desktop. When the user chooses Restart, Receiver shuts down the desktop and then starts it.

Important: Make users aware that restarting desktops can result in data loss.

Provide 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 XenDesktop and XenApp 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.

Provide 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 down arrow 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.

Map client devices

Receiver maps local drives and devices automatically 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.

Map client drives

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

Receiver monitors the directories in which hardware devices such as CD-ROMs, DVDs and USB memory sticks are typically mounted on the user device and automatically maps any new ones that appear during a session to the next available drive letter on the server.

You can configure the level of read and write access for mapped drives using Receiver preferences.

To configure read and write access for mapped drives

1. On the Receiver home page, click the down arrow icon  , and then click Preferences.
2. Click Devices.
3. Select the level of read and write access for mapped drives from the following options:
   - Read and Write
   - Read only
   - No access
   - Ask me each time
4. Log off from any open sessions and reconnect to apply the changes.

Map 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. On the Receiver home page, click the down arrow icon  , and then click Preferences.

2. Click Devices.

3. Select the COM port you want to map, from the Mapped COM Ports list. This is the virtual COM port that is displayed in the session, not the physical port on the local machine.

4. Select the device to associate with the virtual COM port from the Device pop-up menu.

5. Start Receiver and log on to a server.

6. Run a command prompt.

7. 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).

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

Change 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.

Improve 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
- Windows shortcut and key-combination 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.

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” lets you choose whether or not to send Command-character keystroke combinations as Ctrl+character key combinations in a session. If you select “Command or Control” from the pop-up menu, you can send familiar Command-character or Ctrl-character keystroke combinations on the Mac as Ctrl+character key combinations to the PC. If you select Control, you must use Ctrl-character keystroke combinations.

- “Send Alt character using” lets you choose how to replicate the Alt key within a session. If you select Command-Option, you can send Command-Option- keystroke combinations as Alt+ key combinations within a session. Alternatively, if you select Command, you can use the Command key as the Alt key.

- “Send Windows logo key using Command (right)” lets you send the Windows logo key to your remote desktops and applications by pressing the Command key situated on the right side of the keyboard. If this option is disabled, the right Command key has the same behavior as the left Command key according to the above two settings in the preferences panel, but you can still send the Windows logo key using the Keyboard menu; choose Keyboard > Send Windows Shortcut > Start.

- “Send special keys unchanged” lets you disable the conversion of special keys. For example, the combination Option-1 (on the numeric keypad) is equivalent to the special key F1. You can change this behavior and set this special key to represent 1 (the number one on the keypad) in the session by selecting the "Send special keys unchanged" checkbox. By default, this checkbox is not selected so Option-1 is sent to the session as F1.

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	Mac options
INSERT	0 (the number zero) on the numeric keypad. Num Lock must be off; you can turn this on and off using the Clear key. Option-Help
DELETE	Decimal point on the numeric keypad. Num Lock must be off; you can turn this on and off using the Clear key. Clear
F1 to F9	Option-1 to -9 (the numbers one to nine) on the numeric keypad
F10	Option-0 (the number zero) on the numeric keypad

F11	Option-Minus Sign on the numeric keypad
F12	Option-Plus Sign on the numeric keypad

Windows shortcuts and key combinations

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.

You might also want to use certain Windows keys, such as Insert, that many Mac keyboards do not have. Similarly, some Windows 8 keyboard shortcuts display charms and app commands, and snap and switch apps. These shortcuts are not mimicked natively by Mac keyboards but can be sent to the remote desktop or application using the Keyboard menu.

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. The default behavior is described. If you adjust the defaults (using Receiver or other preferences), different keystroke combinations may be forwarded and other behavior may be observed on the remote PC.

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.

Windows key or key combination	Mac equivalents
Alt+character key	Command–Option–character key (for example, to send Alt-C, use Command-Option-C)

Alt+special key	Option–special key (for example, Option-Tab) Command–Option–special key (for example, Command-Option-Tab)
Ctrl+character key	Command–character key (for example, Command-C) Control–character key (for example, Control-C)
Ctrl+special key	Control–special key (for example, Control-F4) Command–special key (for example, Command-F4)
Ctrl/Alt/Shift/Windows logo + function key	Choose Keyboard > Send Function key > Control/Alt/Shift/Command-Function key
Ctrl+Alt	Control-Option-Command
Ctrl+Alt+Delete	Control–Option–Forward Delete Control-Option-Fn-Delete (on MacBook keyboards) Choose Keyboard >Send Ctrl-Alt-Del
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 F12	F1 to F12 Choose Keyboard > Send Function Key > F1 to F12
Home	Home Fn–Left Arrow
Insert	Choose Keyboard > Send Key > Insert
Num Lock	Clear
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

Windows logo	Right Command key (a keyboard preference, enabled by default) Choose Keyboard > Send Windows Shortcut > Start
Key combination to display charms	Choose Keyboard > Send Windows Shortcut > Charms
Key combination to display app commands	Choose Keyboard > Send Windows Shortcut > App Commands
Key combination to snap apps	Choose Keyboard > Send Windows Shortcut > Snap
Key combination to switch apps	Choose Keyboard > Send Windows Shortcut > Switch Apps

Use Input Method Editors (IME) and international keyboard layouts

Receiver allows you to use an Input Method Editor (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 indicate explicitly 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.

Secure Receiver communications

To secure the communication between your server farm and Receiver, you can integrate your Receiver connections to the server farm with a range of security technologies, including:

- Citrix NetScaler Gateway or Citrix Access Gateway. For information about configuring these with Citrix StoreFront, refer to the StoreFront documentation.

  Note: Citrix recommends using NetScaler Gateway to secure communications between StoreFront servers and users' devices.

- A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server, or SSL tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Receiver and servers. Receiver supports SOCKS and secure proxy protocols.

- Secure Gateway. You can use Secure Gateway with the Web Interface to provide a single, secure, encrypted point of access through the Internet to servers on internal corporate networks.

- SSL Relay solutions with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols

- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using Receiver through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

Certificates

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 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 with Access Gateway or NetScaler Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Access Gateway or NetScaler Gateway server certificate. For information on this task, refer to the NetScaler Gateway documentation in eDocs. For equivalent information on Access Gateway, refer to the Knowledge Base article that matches your edition of that product:

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

Connect with NetScaler Gateway or Access Gateway Enterprise Edition

To enable remote users to connect to your CloudGateway deployment through NetScaler Gateway or Access Gateway, you can configure these to work with App Controller or StoreFront (both components of CloudGateway). The method for enabling access depends on the edition of CloudGateway in your deployment:

- If you deploy CloudGateway Enterprise in your network, allow connections from remote users to App Controller by integrating App Controller with NetScaler Gateway or Access Gateway. This deployment allows users to connect to App Controller to obtain their web, Software as a Service (SaaS), and iOS apps. Users connect through either Citrix Receiver, the NetScaler Gateway Plug-in, or Access Gateway Plug-in.

- If you deploy CloudGateway Express in your network, allow connections from internal or remote users to StoreFront through NetScaler Gateway or Access Gateway by integrating NetScaler Gateway or Access Gateway with StoreFront. This deployment allows users to connect to StoreFront to access published applications from XenApp and virtual desktops from XenDesktop. Users connect through Citrix Receiver.

For information on configuring these connections with NetScaler Gateway, refer to the section*Configuring NetScaler Gateway Settings with the Remote Access Wizard* in Citrix eDocs. For information on configuring these connections with Access Gateway, refer to the section *Integrating Access Gateway with CloudGateway* in Citrix eDocs.

To enable remote users to connect through Access Gateway to your Web Interface deployment, configure Access Gateway to work with Web Interface, as described in the section in Citrix eDocs called *Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface*, and the topics in that section.

Connect with Access Gateway 5.0

This topic applies only to deployments using the Web Interface.

When you configure Access Gateway for Receiver, 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*.

Connect 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.

Receiver uses settings that are configured remotely on the Web Interface server to connect to servers running the Secure Gateway. For more information about configuring proxy server settings for Receiver, see the Web Interface documentation.

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*.

Connect 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 Web Interface server. 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.

Connect 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.

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.

Configure and enable 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.

Install 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.

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.

Connect 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.