About Citrix Receiver for Mac 12

Jun 21, 2016

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.

You can download the latest release from the Citrix Receiver for Mac download page.

What's new in 12.1

Smart card authentication to NetScaler Gateway

This feature enables Citrix Receiver to access apps and desktops through NetScaler Gateway using smart card authentication. See Requirements for smart card authentication for more information about this feature.

El Capitan support for split screen

In the previous release of Citrix Receiver for Mac (12.0), we introduced support for OS X El Capitan. In this release we include full support for El Capitan's split screen feature.

Auto-client reconnect and session reliability improvements

This improvements enable better interoperability with CloudBridge and NetScaler Gateway. A session can reconnect using auto-client reconnect and session reliability regardless of the connection path. The specific improvements for this release are as follows:

Improved connection messages tells your users that the state of their connection and informs them of when they've lost a connection and what do to.

A countdown timer (in minutes/seconds) now illustrates how long before a session times out. A session is terminated when the countdown timer expires. By default, the timeout value is set to 2 minutes. You can change the default value in the **TransportReconnectMaxRetrySeconds** ICA file setting.

> ### Note
>
> This feature provides support for an additional session management setting in XenApp and XenDesktop, **TransportReconnectRetryMaxTimeSeconds**.
>
> **TransportReconnectDelay** and **TransportReconnectRetries** are no longer used. For additional information, see Session Management.

Features introduced in 12.0

When used in conjunction with the centralized customization and branding capabilities of the StoreFront 3.0, users of this Receiver for Mac will receive a centrally managed app and desktop selection experience from StoreFront. This is the same consistent user experience that can be received by the Windows desktop Receivers and HTML5 and Chrome web Receivers when associated with the StoreFront 3.0.

Support for OS X El Capitan (10.11).

Session cookie support: Citrix Receiver for Mac 12.0 supports web session cookies in order to use the new web API required for StoreFront 3.0 and to support load balancing.

Time zone enhancements: Citrix Receiver for Mac 12.0 has better accuracy detecting local and city time zones when used with XenApp Time Zone Redirection. For more information, see: Time zone control policy settings.

Fixed issues in Citrix Receiver for Mac 12

Jun 20, 2016

Fixed issues in Citrix Receiver for Mac 12

This release resolves a number of issues related to smart card integration. Some issues remain and will continue to be investigated.

Other issues fixed in this release:

- An incorrect message was shown on the Credential Dialog Window in Japanese environments （"デモアカウント にログオンしてください", meaning "Please log on to Demo Account"). This message should have read "Please log on to My Virtual Desktop." [#LC2682]
- Mounting multiple Receiver disk images simultaneously could result in the wrong installer being launched. [#551605]
- OS X proxy bypass entries in CIDR notation were ignored. [#564250]
- Only the first 256 characters of the OS X bypass list are used. [#567089]
- An internal beacon false positive check could fail for certain ISPs who have installed DNS error redirection software from Barefruit. [#572456]

Fixed issues in Citrix Receiver for Mac 12.1

- Fixed an issue where if you are using the VPN support built into OS X, Citrix Receiver sometimes wasn't able to connect to a configured account while the VPN was active.
- Fixed an issue in OS X El Capitan, where sessions displayed abnormally when put them in Split View. [582397]
- Fixed an issue where beacon detection failed when you tried to connect externally through an F5 proxy. [582885]
- Fixed an issue where keyboard shortcuts configured in System Preferences weren't applied in the session. [583033]
- Fixed an issue with the '+' keyboard signals in Citrix Receiver for Mac 11.9.15 and 12, which caused the viewer to crash. [586179] [577922]
- Fixed an issue after launching one app Citrix Receiver asks for authentication for another app. [592460]
- Fixed an issue on desktop sessions, where the Ctrl-Q keyboard combination would not pass through correctly. [600601]

Fixed issues in Citrix Receiver for Mac 12.1.100

- Resolved an issue where a session would crash when launching an app or desktop whose name started with an '@' character. [LC4296]
- Fixed a problem where IPV6 connections to NetScaler Gateway would fail. [LC4512]
- Resolved a problem when a Receiver for Mac session failed when connecting through a Cisco ASA 9.32 SSL VPN. [LC3887]
- Fixed an issue where sessions would disconnect resulting in an error message indicating that "The remote SSL peer sent a bad MAC Alert." [LC4367]
- Fixed an issue where attempting to enter a single Japanese or Simplified Chinese character would result in no character being displayed in the session desktop. [603635]

Known issues in Citrix Receiver for Mac 12

Jun 21, 2016

Known issues in Citrix Receiver for Mac 12

The following known issues have been observed in this release:

- On OS X El Capitan (10.11), virtual desktops and apps don't display normally in Split View. [#582397]
- XenDesktop session fails to launch when using smart card authentication. [#550781]
- When using a PIV smart card, Receiver fails to reconnect to a XenDesktop 5.6 session. [#550986]
- If a published Command Prompt is minimized when you disconnect from a session, the Command Prompt might not reappear when reconnected. [#411702]
- SSL SDK might incorrectly flags a certificate chain as “expired” if multiple certificates are installed with some certificates being expired. Deleting expired certificates from the Keychain Access will fix this problem. [#511574]
- Application names viewed on Receiver might not reflect updates on the Broker and StoreFront if the user subscribed to the apps before the updates occurred. Users can delete and resubscribe to the app if this occurs. [#515097]
- Resizing a desktop window when a Windows logon message is displayed might make session inoperative. [#525833]
- When using OS X Mountain Lion (10.8) and upgrading Receiver 11.9 or 11.9.15 to Receiver 12.0, launching Receiver might cause both a new version of Receiver and an older version of Receiver to open. [#552496]
- When using Google Chrome browser for OS X, double clicking the ICA file on the download bar might cause multiple ICA files to launch causing an error message. [#564961]
- Users might not be able to change expired passwords when logging into a WI PNA account. [#568394]
  The lower end of the XenDesktop toolbar button might get cropped out when user go into full-screen mode during a video call session. [#570480]
- Users with computers running OS X Mountain Lion (10.8) might see overlap on the string log on and down icon on the Receiver user interface. Users can click Log on or the user name string instead of the down icon if this occurs. [#504302]
- Changing the viewer to full screen while the DirectX or OpenGL application is running might cause the cursor to disappear. [#510745]
- When server language is set to traditional Chinese, users might not be able to input "[“ or “]" within a session. [#511877]
- Moving the cursor does not change Lync status from Away to Available if the status change was due to the user being idle. Users must manually change the status to Available if this happens. [#512074]
- In a multiple monitor configuration, seamless apps might move to the primary display when any display is reconfigured. [#506532]
- HDX apps might turn black. If this happens, drag applications and close them by clicking where the close button should be located. [#426991]
- In OS X Yosemite (10.10), the upgrade version of Safari might block Receiver as a pop-up window. Enabling pop-ups windows for Apps/Desktops to open will fix the issue.

Known issues in Citrix Receiver for Mac 12.1

The following known issues have been observed in this release:

- Resizing a desktop window while the Windows logon message is displayed can make the session inoperative.
  [525833]
- You might see an error message after launching a virtual desktop from Chrome.
  [564961]
- Viewer is not sending correct keyboard layout to server, which can cause keyboard mapping issues.

[581829]

- When smooth roaming a session to an OS X 10.11 (El Capitan) machine, the session may not reconnect successfully. Use the "Refresh Apps" menu command to reconnect to the session again if it fails the first time.
  [601542]

System requirements for Citrix Receiver for Mac 12

Sep 29, 2016

Supported operating systems for Citrix Receiver for Mac 12.0

- OS X El Capitan (10.11)
- OS X Yosemite (10.10)
- OS X Mavericks (10.9)
- OS X Mountain Lion (10.8)

OS X releases prior to Mountain Lion are not supported.

If you need a version of Citrix Receiver for Mac OS X Lion (10.7) or prior, see Citrix Receiver for Mac 11.9.x.

Hardware Requirements

- 110 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 7.6 for Windows Server 2012 R2
  - Citrix XenApp 7.5 for Windows Server 2012 R2
  - Citrix XenApp 6.5 for Windows Server 2008 R2
- XenDesktop (any of the following products):
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
- Citrix VDI-in-a-Box 5.4 and 5.3
- StoreFront:
  - StoreFront 3.0
  - StoreFront 2.6
  - StoreFront 2.5
  - StoreFront 2.1
- 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 2.1, 2.5 and 2.6
  - Citrix Web Interface 5.4

Supported Browsers

- Safari 6.0 or newer
- Mozilla Firefox 22.x or newer
- Google Chrome 28.x or newer

Connectivity

If your users are running Citrix Receiver for Mac 12 on OS X El Capitan and are having trouble connecting, they may need to upgrade their NetScaler Gateway plugin. For more information, see this article on the Citrix downloads page: NetScaler Gateway Plug-in v3.1.4 for Mac OS X (El Capitan Support).

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

For LAN connections:

- StoreFront using StoreFront services or Receiver for Web site
- Web Interface 5.4 for Windows, using XenApp Services sites

For secure remote or local connections:

- Citrix NetScaler Gateway 11.0 including VPX
- Citrix NetScaler Gateway 10.5 including VPX
- Citrix NetScaler Gateway 10.1 including VPX
- Citrix Access Gateway Enterprise Edition 10.x including VPX
- Citrix Access Gateway Enterprise Edition 9.x including VPX
- Citrix Access Gateway VPX
- 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.

Authentication

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

	Receiver for Web using browsers	**StoreFront Services site (native)**	**StoreFront XenApp Services site (native)**	**NetScaler to Receiver for Web (browser)**	**NetScaler to StoreFront Services site (native)**
Anonymous	Yes	Yes			
Domain	Yes	Yes		Yes*	Yes*
Domain pass-through					
Security token				Yes*	Yes*
Two-factor (domain with security token)				Yes*	Yes*
SMS				Yes*	Yes*

	Receiver for Web using browsers	**StoreFront Services site (native)**	**StoreFront XenApp Services site (native)**	**NetScaler to Receiver for Web (browser)**	**NetScaler to StoreFront Services site (native)**
Smart card**	Yes	Yes		Yes*	Yes*
User certificate				Yes (NetScaler Gateway Plugin)	Yes (NetScaler Gateway Plugin)

*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.

**To use smart cards on OS X 10.10, you must have a least OS X 10.10.2 installed.

For connections to the Web Interface 5.4, Receiver supports the following authentication methods:
Note: Web Interface uses the term Explicit to represent domain and security token authentication.

	Web Interface (browsers)	**Web Interface XenApp Services site**	**NetScaler to Web Interface (browser)**	**NetScaler to Web Interface XenApp Services site**
Anonymous	Yes			
Domain	Yes	Yes	Yes	Yes
Domain pass-through				
Security token			Yes*	Yes
Two-factor (domain with security token)			Yes*	Yes
SMS			Yes*	Yes
Smart card**	Yes	Yes	Yes	Yes
User certificate			Yes (Require NetScaler Gateway Plugin)	Yes (Require NetScaler Gateway Plugin)

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

**Smart card is not supported by OS X 10.10 due to the Apple change in smart card support.

For information about authentication, refer to the NetScaler Gateway or Access Gateway documentation, and the StoreFront documentation, in Citrix Product Documentation. 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 Citrix Product Documentation.

Requirements for smart card authentication

Oct 28, 2015

Receiver for Mac supports smart card authentication in the following configurations:

- Smart card authentication to Receiver for Web/ StoreFront 2.x and XenDesktop 5.6 and above or XenApp 6.5 and above using browser based access.
- Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office, allow users to digitally sign or encrypt documents available in virtual desktop or application sessions.
- With multiple certificates—Receiver for Mac supports using multiple certificates with a single smart card or with multiple smart cards. When your user inserts a smart card into a card reader, the certificates are available to all applications running on the device, including Citrix Receiver.
- In double-hop sessions—if a double-hop is required, a further connection is established between Receiver and your user's virtual desktop.

  Deployments supporting double-hops are described in the XenApp and XenDesktop documentation. For more information, see: Smart card deployments.

About smart card authentication to NetScaler

When using a smart card to authenticate a connection when there are multiple usable certificates on the smart card, Citrix Receiver prompts you to select a certificate. Upon selecting a certificate, Citrix Receiver prompts you to enter the smart card password; once authenticated, the session launches.

If there is only one suitable certificate on the smart card, Citrix Receiver uses that certificate and will not prompt you to select it. However, you must still enter the password associated with the smart card to authenticate the connection and to start the session.

Specifying a PKCS#11 module for smart card authentication

Using advanced configuration options in the Citrix Receiver Preferences window, you can specify the PKCS#11 module for authentication purposes:

1. In Citrix Receiver, select **Preferences**.
2. In the Preferences window, click **Advanced**.
3. In the PKCS#11 field, select the appropriate module; click **Other** to browse to the location of the PKCS#11 module if the desired one is not listed.
4. After selecting the appropriate module, click **Add**.

Supported readers, middleware, and smart card profiles

Receiver for Mac supports most Mac OS X compatible smart card readers and cryptographic middleware. Citrix has validated operation with the following.

Supported readers:

- Common USB connect smart card readers

Supported middleware:

- Clariify
- Activeidentity client version
- Charismathics client version

Supported smart cards:

- PIV cards
- Common Access Card (CAC)

Follow the instructions provided by your vendor's Mac OS X compatible smart card reader and cryptographic middleware for configuring user devices.

Restrictions

- Certificates must be stored on a smart card, not the user device.
- Receiver for Mac does not save the user certificate choice.
- Receiver for Mac does not store or save the user's Smart Card PIN. PIN acquisitions is handled by the OS, which may have its own caching mechanism.
- Receiver for Mac does not reconnect sessions when a smart card is inserted.
- To use VPN tunnels with smart card authentication, users must install the NetScaler Gateway Plug-in and log on through a web page, using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the NetScaler Gateway Plug-in is not available for smart card users.

For more information

See:

- Configuring Citrix XenDesktop 7.6 andNetScaler Gateway 10.5 with PIV SmartCard Authentication (PDF)
- Smart Card Support with Citrix Receiver for Mac 11.9.15 on OS X 10.10.2

Installing, setting up, upgrading, deploying, or removing Citrix Receiver for Mac

Sep 22, 2016

This release of Citrix Receiver for Mac contains a single installation package, CitrixReceiver.dmg, and supports remote access through NetScaler Gateway, Access Gateway, and Secure Gateway.

In this article:

- Installing Receiver for Mac manually
- Upgrading to Receiver for Mac 12.0
- About deploying and configuring Receiver for Mac
- Deploying Receiver from Receiver for Web
- Deploying Receiver from a Web Interface logon screen
- Removing Receiver for Mac

Installation

Receiver can be installed in the following ways:

- 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 NetScaler Gateway or StoreFront server 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 a user 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 the 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 by 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.

Installing 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 username and password of an administrator on the local device.

Upgrading to Receiver for Mac 12.0

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, 11.6,11.7.x, 11.8.x, 11.9.x of Receiver for Mac.

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

About deploying and configuring Receiver for Mac

For deployments with StoreFront:

- A best practice is to configure NetScaler Gateway and StoreFront 2.x as described in the documentation for those products in Citrix Product Documentation. Attach the provisioning file created by StoreFront to an email and inform users how to upgrade and how 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. If you have configured email-based account discovery as described in the StoreFront documentation, tell users to enter 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 then click Activate).

For deployments with Web Interface:

- Upgrade your Web Interface site with Receiver for Mac 11.9 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.

Deploying 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.

Deploying 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.

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 Citrix Receiver for Mac

Oct 28, 2015

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

- Configure your application delivery—Ensure your XenApp environment is configured correctly. Understand your options and provide meaningful application descriptions for your users.
- Configure self-service mode—Configure self-service mode, which allows your users to subscribe to applications from the Receiver user interface.
- Configure StoreFront—Create stores that enumerate and aggregate desktops and applications from XenDesktop sites and XenApp farms, 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.
- 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. For more information see NetScaler Gateway

Configure your application delivery

When delivering applications with XenDesktop or XenApp, consider the following options to enhance the experience for your users when they access their applications:

Web access mode

Without any configuration, Receiver for Mac provides web access mode: browser-based access to applications and desktops. Users simply open a browser to a Receiver for Web or Web Interface site and select and use the applications that they want. In web access mode, no app shortcuts are placed in the App Folder on your user's device.

Self-service mode

By adding a StoreFront account to Receiver or configuring Receiver to point to a StoreFront site, you can configure self-service mode, which enables your users to subscribe to applications through Receiver. This enhanced user experience is similar to that of a mobile app store. In self-service mode you can configure mandatory, auto-provisioned, and featured app keyword settings as needed. When one of your users selects an application, a shortcut to that application is placed in the App Folder on the user device.

When accessing a StoreFront 3.0 site, your users see the Receiver Tech Preview user experience. For more information about the Receiver Tech Preview user experience, see Receiver and StoreFront 3.0 Technology Preview.

When publishing applications on your XenApp farms, to enhance the experience for users accessing those applications through StoreFront stores, ensure that you include meaningful descriptions for published applications. The descriptions are visible to your users through Citrix Receiver.

Configure self-service mode

As mentioned previously, by adding a StoreFront account to Receiver or configuring Receiver to point to a StoreFront site, you can configure self-service mode, which allows users to subscribe to applications from the Receiver user interface. This enhanced user experience is similar to that of a mobile app store.

In self service mode you can configure mandatory, auto-provisioned and featured app keyword settings as needed.

- 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 the need for users to manually subscribe to the application.
- To advertise applications to users or make commonly used applications easier to find by listing them in the Receiver 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 a site. The name of the site and how you create the site depends on the version of the Web Interface you have installed. For more information, see the Web Interface documentation.

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 and XenApp farms, 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.

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 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.

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.example.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.

Optimizing your Citrix Receiver for Mac environment

Oct 28, 2015

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

- Reconnecting users automatically
- Providing HDX Broadcast session reliability
- Providing continuity for roaming users
- Mapping client devices

Reconnecting users

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 and XenDesktop documentation.

Restarting 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.

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 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.

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 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.

Mapping 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.

Mapping 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.

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 mappiAsk me each timengs.

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. At the prompt, type
   net use comx: \\client\comz:

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

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

Improving the user experience in Citrix Receiver for Mac

Oct 28, 2015

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

- ClearType font smoothing
- Client-side microphone input
- Windows special keys
- Windows shortcuts and key combinations
- Use Input Method Editors (IME) and international keyboard layouts
- Using multiple monitors
- Using the Desktop toolbar

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

Windows key or key combination	Mac equivalents
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 key or key combination	**Mac equivalents**
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.

Using multiple monitors

Users can set Receiver for Mac to work in full-screen mode across multiple monitors through the menu option, **Use All Displays In Full Screen**.

Known Limitations

Full-screen mode is only supported on one monitor or all monitors, which is configurable through a menu item.

Using the Desktop toolbar

Users can now access the Desktop Toolbar in both windowed and full-screen mode. Previously, the toolbar was only visible in full-screen mode. Additional toolbar changes include:

- The **Home** button has been removed from the toolbar. This function can be executed by using the following commands:
  - Cmd-Tab to switch to the previous active application.
  - Ctrl-Left Arrow to switch to the previous Space.
  - Using the built-in trackpad or Magic Mouse gestures to switch to a different Space.
  - Moving the cursor to the edge of screen while in full-screen mode will display a Dock where you can choose which applications to make active.
- The **Windowed** button has been removed from the toolbar. Leaving full-screen mode for windowed mode can be executed by the following methods:
  - For OS X 10.10, clicking the green window button on the drop-down menu bar. 🟢 or 🟢
  - For OS X 10.7, 10.8, and 10.9, clicking the blue menu button on the drop-down menu bar. 🟦
  - For all versions of OS X, selecting **Exit Full Screen** from the **View** menu of the drop-down menu bar.
- The toolbar drag behavior is updated to support dragging between windows in full screen with multiple monitors.

Securing Citrix Receiver communications

Feb 16, 2016

In this artcle:

To secure the communication between your server farm and Receiver, you can integrate your Citrix 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). You can use proxy servers to limit access to and from your network and to handle connections between Citrix Receiver and servers. Citrix 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 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.

About certificates

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 mapped to the Access Gateway or NetScaler Gateway server certificate. For information on this task, refer to the NetScaler Gateway documentation. For equivalent information on Access Gateway, refer to the Knowledge Base article that matches your edition of that product:

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

Connecting 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 StoreFront (both components of CloudGateway). The method for enabling access depends on the edition of CloudGateway in your deployment.

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 sectionConfiguring NetScaler Gateway Settings with the Remote Access Wizard. For information on configuring these connections with Access Gateway, refer to the section Integrating Access Gateway with CloudGateway.

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 called Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface, and the topics in that section.

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.

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.example.com is a FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (example), and a top-level domain (com). The combination of intermediate and top-level domain (example.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 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.

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.

Connecting with the Secure Sockets Layer (SSL) Relay

You can integrate Receiver with the Secure Sockets Layer (SSL) Relay service with Receiver for Mac 12.0, which supports TLS 1.0, 1.1 and 1.2 with the following cipher suites for TLS connections between Citrix Receiver and XenApp/XenDesktop:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Transport Layer Security (TLS) 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. 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 Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

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

You can use Citrix SSL Relay to secure communications:

- Between a 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 TLS encryption, see the XenApp and Web Interface documentation.

Configuring and enabling Receiver for TLS

There are two main steps involved in setting up 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 TLS to secure communications between 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 then click OK.

The root certificate is installed and can be used by SSL-enabled clients and by any other application using SSL.

About SSL policies

This section provides information for configuring security policies for ICA sessions over SSL in Citrix Receiver for Mac version 12.0. You can configure certain SSL settings used for ICA connections in Citrix Receiver. These settings are not exposed in the user interface; changing them requires running a command on the device running Receiver.

> ### Note
>
> SSL policies can be managed in other ways, such as when devices are controlled by OS X server or another mobile device management solution.

SSL policies include the following settings:

SecurityComplianceMode. Sets the security compliance mode for the policy. If you don't configure SecurityComplianceMode, FIPS is used as the default value. Applicable values for this setting include:

- **None**. No compliance mode is enforced
- **FIPS**. FIPS cryptographic modules are used
- **SP800-52**. NIST SP800-52r1 compliance is enforced

Setting SecurityComplianceMode to SP800-52:

COPY

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions. This setting specifies the TLS protocol versions that should be accepted during protocol negotiation. This information is represented as an array and any combination of the possible values is supported. When this setting is not configured, the values TLS10, TLS11 and TLS12 are used as the default values. Applicable values for this setting include:

- **TLS10**. Specifies that the TLS 1.0 protocol is allowed.
- **TLS11**. Specifies that the TLS 1.1 protocol is allowed.
- **TLS12**. Specifies that the TLS 1.2 protocol is allowed.

Setting SecurityAllowedTLSVersions to TLS 1.1 and TLS 1.2:

COPY

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy. This feature improves the cryptographic authentication of the Citrix server and improves the overall security of the SSL/TLS connections between a client and a server. This setting governs how a given trusted root certificate authority is treated during an attempt to open a remote session through SSL when using the client for OS X.

When you enable this setting, the client checks whether or not the server's certificate is revoked. There are several levels of certificate revocation list checking. For example, the client can be configured to check only its local certificate list, or to check the local and network certificate lists. In addition, certificate checking can be configured to allow users to log on only if all Certificate Revocation lists are verified.

Certificate Revocation List (CRL) checking is an advanced feature supported by some certificate issuers. It allows an administrator to revoke security certificates (invalidated before their expiry date) in the case of cryptographic compromise of the certificate private key, or simply an unexpected change in DNS name.

Applicable values for this setting include:

- **NoCheck**. No Certificate Revocation List check is performed.
- **CheckWithNoNetworkAccess**. Certificate revocation list check is performed. Only local certificate revocation list stores are used. All distribution points are ignored. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.
- **FullAccessCheck**. Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.
- **FullAccessCheckAndCRLRequired**. Certificate Revocation List check is performed, excluding the root CA. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.
- **FullAccessCheckAndCRLRequiredAll**. Certificate Revocation List check is performed, including the root CA. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.

> ### Note
>
> If you don't set SSLCertificateRevocationCheckPolicy, FullAccessCheck is used as the default value.

Setting SSLCertificateRevocationCheckPolicy to FullAccessCheckAndCRLRequred:

COPY

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

Configuring SSL policies

To configure SSL settings on an unmanaged computer, run the **defaults** command in Terminal.app.

defaults is a command line application that you can use to add, edit, and delete app settings in an OS X preferences plist file.

To change settings:

1. Open Applications > Utilities > Terminal.

2. In Terminal, run the command:

   defaults write com.citrix.receiver.nomas <name> <type> <value>

Where:

<name>: The name of the setting as described above.

<type>: A switch identifying the type of the setting, either -string or -array. If the setting type is a string, this can be omitted.

<value>: The value for the setting. If the value is an array and you are specifying multiple values, the values must be separated by a space.

For example:

COPY

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

Reverting to the default configuration

To reset a setting back to its default:

1. Open Applications > Utilities > Terminal.
2. In Terminal, run the command:

   defaults delete com.citrix.receiver.nomas <name>

Where:

<name>: The name of the setting as described above.

For example:

COPY

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```