# Citrix Receiver for Mac 12.6

Jun 19, 2017

Citrix Receiver for Mac provides users with self-service access to resources published on XenApp or XenDesktop servers. Citrix Receiver for Mac 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.

For information about earlier Citrix Receiver for Mac releases, see the following sections:

Citrix Receiver for Mac 12.5

Citrix Receiver for Mac 12.4

Citrix Receiver for Mac 12.3

Citrix Receiver for Mac 12.2

Citrix Receiver for Mac 12

# What's new

Jun 19, 2017

# What's new in 12.6

**Auto-update**
Auto-update provides automatic updates for Citrix Receiver for Mac and the HDX Real Time Optimization Pack without the need to download updates manually. Auto-update gives you automatic access to the latest version of Citrix Receiver with all the newest features and most up-to-date fixes and security updates.

By default, auto-update is set to enabled and checks for updates daily. When an update is available, Citrix Receiver notifies users to accept the download and install the updates.

You can set auto-update to any of the following options:

- Notify me when updates are available
- Do not notify me when updates are available
- Leave updates up to my administrator

Auto-update can be configured on both Citrix Receiver for Mac and StoreFront. In Citrix Receiver for Mac, configure auto-update by using the **Preferences** dialog.

You can configure auto-update using StoreFront only when you add or refresh a StoreFront account. Citrix Receiver for Mac automatically detects the auto-update client configuration and notifies you.

For information about configuring auto-update in Citrix Receiver for Mac, see Configuring auto-update.

**Thinwire 32-bit cursor support**
Citrix Receiver for Mac now supports 32-bit cursors in Thinwire. In previous versions of Citrix Receiver for Mac, if a 32-bit cursor is used in the VDA, the transparent portion of the cursor appeared as black. With this release of Citrix Receiver for Mac, cursors now work as intended.

**Joint Server Certificate Validation Policy**
Citrix Receiver for Mac 12.5 and later introduced a new, stricter, validation policy for server certificates, which might affect session launches. For more information, see Knowledge Center article CTX224709 and the Secure Communications documentation page.

# Fixed issues

Jun 19, 2017

## Fixed issues in Citrix Receiver for Mac 12.6

Compared to: Citrix Receiver for Mac 12.5

Citrix Receiver for Mac 12.6 contains all fixes that were included in Versions 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, and 12.5 plus the following, new fixes:

- When sharing screens using WebEx, a black window might appear on the shared screen.

  [RFMAC-689, #LC6462]

- After screen sharing is stopped when using WebEx, the application might not appear in the foreground of the desktop.

  [RFMAC-690, #LC6255]

- On macOS Sierra, the Shift-Insert keystroke pair might not work.

  [RFMAC-696]

- After minimizing WebEx, the application might display incorrectly when attempting to view it again.

  [RFMAC-742, #LC6840]

- When launching an application with Citrix Receiver using Google Chrome, the “Starting Application...” window might not appear.

  [RFMAC-744]

- When running a virtual machine, XenDesktop sessions might appear as a black screen.

  [RFMAC-808]

- After an application has launched, the loading popup still appears. Clicking Cancel in the popup causes Citrix Receiver to exit unexpectedly.

  [RFMAC-832, #LC7682]

- When using server-to-client URL redirection, URLs containing a "one-time access token" may launch with the token already expired.

  [RFMAC-856]

- Apps and desktops might not launch when using Safari on macOS Sierra 10.12.6 public beta or macOS High Sierra Developer Preview builds.

[RFMAC-869]

## Fixed issues in Citrix Receiver for Mac 12.5

Compared to: Citrix Receiver for Mac 12.4

Citrix Receiver for Mac 12.5 contains all fixes that were included in Versions 12, 12.1, 12.1.100, 12.2, 12.3 and 12.4 plus the following, new fixes:

- When using smart cards to log on to a Remote Desktop Client, occasionally a “No Certificates found on card” error appears.

  [RFMAC-432, #650298]

- Store detection fails when the server responds by using a non-UTF-8 response.

  [RFMAC-565]

- When starting a SAML application, an “Invalid Request” error might occur.

  [RFMAC-598, #LC6558]

- ReceiverHelper might exit unexpectedly. The issue occurs when CEIPRegistry.json contains an invalid JSON.

  [RFMAC-639]

- Launching a published application from Launchpad or Finder when logged out of Citrix Receiver fails and the following error message appears: “Cannot connect. Unable to communicate with Authentication Manager service.”

  [RFMAC-648]

## Fixed issues in Citrix Receiver for Mac 12.4

Compared to: Citrix Receiver for Mac 12.3

Citrix Receiver for Mac 12.4 contains all fixes that were included in Versions 12, 12.1, 12.1.100, 12.2, and 12.3 plus the following, new fixes:

- Citrix Viewer does not send the correct keyboard layout to the server.

  [#581829]

- When using Citrix Receiver for Mac 12.1, resizing and swapping hosted desktops might not work when using split view.

  [#604943]

- When using multiple displays in a configuration where the primary display is on the bottom, the Citrix Receiver for Mac published application windows may flicker.

[#652254]

- Users might not be able to edit or save a file on a network drive when using published applications.

  [#660657]

- When saving a file on a network drive, the VDA session might get disconnected.

  [#660661]

- When using an external keyboard either in a VDA session or a published application, the Insert key does not work.

  [#660669]

- Printers that are prevented from appearing in a session are still present and available.

  [#667462]

### Fixed issues in Citrix Receiver for Mac 12.3

Compared to: Citrix Receiver for Mac 12.2

Citrix Receiver for Mac 12.3 contains all fixes that were included in Versions 12, 12.1, 12.1.100, and 12.2, plus the following, new fix:

- If Citrix Receiver for Mac is configured to use a proxy server, Secure Socket Layer (SSL) connections can fail.

  [#640652]

### Fixed issues in Citrix Receiver for Mac 12.2

Compared to: Citrix Receiver for Mac 12.1.100

Citrix Receiver for Mac 12.2 contains all fixes that were included in Versions 12, 12.1, and 12.1.100, plus the following, new fixes:

- Fixed an issue on German/Austrian keyboards where the ALT key was not released after typing Alt-l.

  [#LC3796]

- Resolved an issue where server-to-client content redirection would fail if the URL being redirected contained non-ASCII characters.

  [#LC4470]

- This release resolved an issue where an HDX app window could display drawing artifacts after minimizing and maximizing.

  [#LC4668]

- Resolved an issue where smart card pass-through authentication could fail.

  [#LC4907]

- Resolved an issue where audio remoted to the server from a microphone could sound very choppy.

  [#LC5157]

- Resolved an issue where the Ctrl-Tab keyboard combination was not passed to active desktop sessions.

  [#LC5367]

- Fixed an issue where the session keyboard mapping could be incorrect when reconnecting to an existing session.

  [#LC5395]

- Fixed an issue where smart cards were inaccessible to a Microsoft Remote Desktop Client running inside an HDX session.

  [#LC5454]

- This release fixed an issue where sessions would fail to connect if user certificate authentication was configured on NetScaler Gateway.

  [#LC5455]

- Resolved an issue where Receiver for Mac would launch a session in full screen mode if the ScreenPercent parameter was specified in the ICA file.

  [#605353]

- Fixed an issue that caused Receiver for Mac to crash if a session was disconnected while a webcam was remoted to an active session.

  [#612051]

- This release fixed an issue where Receiver or Mac would not use the system proxy configuration when downloading certificate revocation lists.

  [#638176]

### Fixed issues in Citrix Receiver for Mac 12.1.100

Compared to: Citrix Receiver for Mac 12.1

Citrix Receiver for Mac 12.1.100 contains all fixes that were included in Versions 12 and 12.1, plus the following, new fixes:

- Resolved a problem when a Receiver for Mac session failed when connecting through a Cisco ASA 9.32 SSL VPN.

[#LC3887]

- Resolved an issue where a session would crash when launching an app or desktop whose name started with an '@' character.

  [#LC4296]

- 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 a problem where IPV6 connections to NetScaler Gateway would fail.

  [#LC4512]

- 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]

### Fixed issues in Citrix Receiver for Mac 12.1

Compared to: Citrix Receiver for Mac 12

Citrix Receiver for Mac 12.1 contains all fixes that were included in Version 12, plus the following, new fixes:

- 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

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]

# Known issues

Jun 19, 2017

## Known issues in Citrix Receiver for Mac 12.5

The following known issues have been observed in this release:

- When using a proxy connection, communication over EDT fails.

  [#664725, RFMAC-464]

- Citrix Viewer might exit unexpectedly on macOS 10.12 while disconnecting a desktop from the menu bar. The issue also occurs if “Use All Screen In Full Screen” mode is selected while the desktop session is logged off.

  [RFMAC-618]

## Known issues in Citrix Receiver for Mac 12.4

The following known issues have been observed in this release:

- When using a proxy connection, communication over Enlightened Data Transport (EDT) fails.

  [#664725]

- When using NetScaler Gateway configured for EDT with VDA version 7.11 or earlier, the connection to TCP fails because the fallback mechanism to TCP does not work.

  [#665617]

## Known issues in Citrix Receiver for Mac 12.3

The following known issues have been observed in this release:

- When a proxy server is configured on a user device, auto-client reconnection might fail with a VDA for Desktop OS.

  [#659683]

- In an IPV6 environment, attempts to launch a session with Secure Socket Layer (SSL) enabled might fail.

  [#659700]

## Known issues in Citrix Receiver for Mac 12.2

The following known issues have been observed in this release:

- Receiver may hang if multiple, concurrent sessions are running simultaneously while redirecting smart cards.

  [#511140]

- Users may not be able to use the OS X Split View feature with HDX apps windows.

  [#637963]

- When redirecting a USB CD/DVD drive with Generic USB Redirection, the drive may be ejected.

  [#645484]

- Some USB devices may not work in a session if the USB Optimization policy is set to Capture.

  [#649082]

- In some cases, the new USB device notification screen may be incorrectly displayed if a USB device is connected during the auto client reconnection process.

  [#649714]

- Users may be prompted with a keychain prompt when connecting to an account after upgrading to Receiver for Mac 12.2.

  [#649885]

- On systems running Mac OS X 10.9, smart cards may be inaccessible to the Microsoft Remote Desktop Client running inside an HDX session.

  [#650298]

- Keystrokes made during the session reliability reconnection process may not be replayed once the session has reconnected.

  [#652154]

### 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]

### Known issues in Citrix Receiver for Mac 12

The following known issues have been observed in this release:

- If a published Command Prompt is minimized when you disconnect from a session, the Command Prompt might not reappear when reconnected.

  [#411702]

- HDX apps might turn black. If this happens, drag applications and close them by clicking where the close button should be located.

  [#426991]

- 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]

- In a multiple monitor configuration, seamless apps might move to the primary display when any display is reconfigured.

  [#506532]

- Changing the viewer to full screen while the DirectX or OpenGL application is running might cause the cursor to disappear.

  [#510745]

- 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]

- 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]

- 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]

- Sessions fail to launch when using a Gemalto .NET card smart card to authenticate to XenDesktop 5.6.

  [#550781]

- When using a PIV smart card, Receiver fails to reconnect to a XenDesktop 5.6 session.

  [#550986]

- 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]

- On OS X El Capitan (10.11), virtual desktops and apps don't display normally in Split View.

  [#582397]

- 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.

# System requirements

Jun 19, 2017

## Supported Operating Systems

Citrix Receiver for Mac supports the following operating systems:

- macOS Sierra (10.12)
- Mac OS X El Capitan (10.11)
- Mac OS X Yosemite (10.10)

> **Note**
>
> Mac OS X releases prior to Mac OS X Yosemite are not supported.

**Compatible Citrix Products**

Citrix Receiver for Mac is compatible with all currently supported versions of the following Citrix products. For information about the Citrix product lifecycle, and to find out when Citrix stops supporting specific versions of products, see the Citrix Product Lifecycle Matrix.

## Compatible browsers

Citrix Receiver for Mac is compatible with the following browsers:

- Safari 7.0 (and later)
- Mozilla Firefox 22.x (and later)
- Google Chrome 28.x (and later)

**Hardware Requirements**

- 140.7 MB of free disk space
- A working network or Internet connection to connect to servers

- Web Interface:
  - Web Interface 5.4 for Windows with XenApp Services (also known as PNAgent Services) sites, for access to applications natively from Citrix Receiver for Mac rather than from a web browser.
- To deploy Citrix Receiver for Mac:
  - Citrix Receiver for Web 2.1, 2.5 and 2.6
  - Citrix Web Interface 5.4
- StoreFront:
  StoreFront 2.x or higher for access to applications natively from Citrix Receiver for Mac or from web browser.

## Connectivity

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

Citrix Receiver for Mac supports the following connections to XenApp or XenDesktop:

- HTTP
- HTTPS
- ICA-over-TLS

Citrix Receiver for Mac supports the following configurations:

| For LAN connections | For secure remote or local connections |
|---|---|
| • StoreFront using StoreFront services or Citrix Receiver for Mac for Web site<br>• Web Interface 5.4 for Windows, using XenApp Services sites | Citrix NetScaler Gateway:<br>• 11.1 including VPX<br>• 11.0 including VPX<br>• 10.5 including VPX<br>• Enterprise Edition 10.x including VPX<br>• Enterprise Edition 9.x including VPX<br>• VPX<br>Citrix Secure Gateway 3.x (for use with Web Interface only) |

For information about deploying NetScaler Gateway with StoreFront, see the NetScaler Gateway documentation, and the StoreFront documentation.

### Authentication

For connections to StoreFront, Citrix Receiver for Mac 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* |

| | | | | | |
|---|---|---|---|---|---|
| Smart card**<br><br>User certificate | Receiver for Web using browsers | StoreFront Services site (native) | StoreFront XenApp Services site (native) | NetScaler to Receiver for Web (browser)<br>Yes | NetScaler to StoreFront Services site (native)<br>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, Citrix Receiver for Mac 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 | |
| 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.

### Requirements for smart card authentication

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

- Smart card authentication to Receiver for Web/StoreFront 2.x and newer, and XenDesktop 7.1 and newer or XenApp 6.5 and newer 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— Citrix 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 for Mac.
- In double-hop sessions—if a double-hop is required, a further connection is established between Citrix Receiver for Mac and your user's virtual desktop.

**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 for Mac prompts you to select a certificate. Upon selecting a certificate, Citrix Receiver for Mac 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 for Mac 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**

**Note**: Installing PKCS#11 module is not mandatory.

To specify PKCS#11 module for smart card authenticaiton:

1. In Citrix Receiver, select **Preferences**.
2. Click **Security & Privacy**.
3. In the Security & Privacy section, click **Smart Card**.
4. 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.
5. After selecting the appropriate module, click **Add**.

**Supported readers, middleware, ans smart card profiles**

Citrix 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)
- Gemalto .NET cards

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 on the user device.
- Citrix Receiver for Mac does not save the user certificate choice.
- Citrix 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.
- Citrix 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.

**Additional information**

For more information, see:

- Configuring Citrix XenDesktop 7.6 and NetScaler 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

# Requirements for smart card authentication

Mar 22, 2017

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

- Smart card authentication to Receiver for Web/StoreFront 2.x and newer, and XenDesktop 7.1 and newer or XenApp 6.5 and newer 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— Citrix 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 for Mac.
- In double-hop sessions—if a double-hop is required, a further connection is established between Citrix Receiver for Mac and your user's virtual desktop.

**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 for Mac prompts you to select a certificate. Upon selecting a certificate, Citrix Receiver for Mac 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 for Mac 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**

**Note**: Installing PKCS#11 module is not mandatory.

To specify PKCS#11 module for smart card authenticaiton:

1. In Citrix Receiver, select **Preferences**.
2. Click **Security & Privacy**.
3. In the **Security & Privacy** section, click **Smart Card**.
4. 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.
5. After selecting the appropriate module, click **Add**.

## Supported readers, middleware, and smart card profiles

Citrix 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)
- Gemalto .NET cards

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 on the user device.
- Citrix Receiver for Mac does not save the user certificate choice.
- Citrix 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.
- Citrix 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 and NetScaler 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 uninstalling Citrix Receiver for Mac

Jun 19, 2017

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

In this article:


- Installation
- Installing Receiver for Mac manually
- Upgrading to Receiver for Mac 12.2
- 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

Citrix Receiver for Mac can be installed by a user from the Citrix website, automatically from Receiver for Web or from Web Interface, or by using an Electronic Software Distribution (ESD) tool.

**By a user from Citrix.com**:

- A first-time Citrix Receiver for Mac user who obtains Citrix Receiver for Mac from Citrix.com or your own download site can set up an account by entering an email address instead of a server URL. Citrix Receiver for Mac 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 Citrix Receiver for Mac installed on their user device.

- Email-based account discovery for a first-time user does not apply if Citrix Receiver for Mac 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 Citrix Receiver for Mac 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 Citrix Receiver for Mac user must enter a server URL to set up an account.

## Installing Citrix Receiver for Mac manually

Users can install Citrix Receiver for Mac 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 Citrix Receiver for Mac

1. Download the .dmg file for the version of Citrix Receiver for Mac 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 Citrix Receiver for Mac 12.4

Upgrades are supported from versions 11.x of the Online Plug-in for Mac. You can upgrade Citrix Receiver for Mac from any of the previous versions of Citrix Receiver for Mac.

> **Important**
>
> 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 Citrix Receiver for Mac

For deployments with StoreFront:

- A best practice is to configure NetScaler Gateway and StoreFront 3.x as described in the documentation for those products on the Netscaler Gateway and StoreFront 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 Citrix Receiver for Mac.
- 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 Citrix Receiver for Mac, 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 12.4 and let your users know how to upgrade Citrix Receiver for Mac. 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 Citrix Receiver for Mac.

### Deploying Citrix Receiver for Mac from Receiver for Web

You can deploy Citrix Receiver for Mac 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 Citrix Receiver for Mac, the user is prompted to download and install Citrix Receiver for Mac. For more information, see the StoreFront documentation.

### Deploying Citrix Receiver for Mac from a Web Interface logon screen

This feature is available only for XenDesktop and XenApp releases that support Web Interface.

You can deploy Citrix Receiver for Mac 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 website. If the Web Interface detects that a user does not have compatible version of Receiver, the user is prompted to download and install Receiver.

For more information,see Configuring Client Deployment in the Web Interface documentation.

### Uninstalling Citrix Receiver for Mac

You can uninstall Citrix Receiver for Mac manually by opening the CitrixReceiver.dmg file, select **Uninstall Citrix Receiver**, and follow the on-screen instructions.

# Configuring Citrix Receiver for Mac

Jun 19, 2017

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

- Configure USB redirection
- Configure session reliability
- Configure CEIP
- 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 Citrix Receiver for Mac 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.
- Configuring auto-update
- 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 USB redirection

HDX USB device redirection enables redirection of USB devices to and from a user device. For example, a user can connect a flash drive to a local computer and access it remotely from within a virtual desktop or a desktop hosted application. During a session, users can plug and play devices, including Picture Transfer Protocol (PTP) devices such as digital cameras, Media Transfer Protocol (MTP) devices such as digital audio players or portable media players, point-of-sale (POS) devices and other devices such as 3D Space Mice, Scanners, Signature Pads etc.

> ### Note
>
> Double-hop USB is not supported for desktop hosted application sessions.

USB redirection is available for the following Citrix Receiver for Mac:

- Windows
- Linux
- Macintosh

By default, USB redirection is allowed for certain classes of USB devices, and denied for others. You can restrict the types of USB devices made available to a virtual desktop by updating the list of USB devices supported for redirection, as described later in this section.

> ### Tip
>
> In environments where security separation between the user device and server is needed, Citrix recommends that users are

informed about the types of USB devices to avoid.

Optimized virtual channels are available to redirect most popular USB devices, and provide superior performance and bandwidth efficiency over a WAN. Optimized virtual channels are usually the best option, especially in high latency environments.

### Note

For USB redirection purposes, Citrix Receiver for Mac handles a SMART board the same as a mouse.

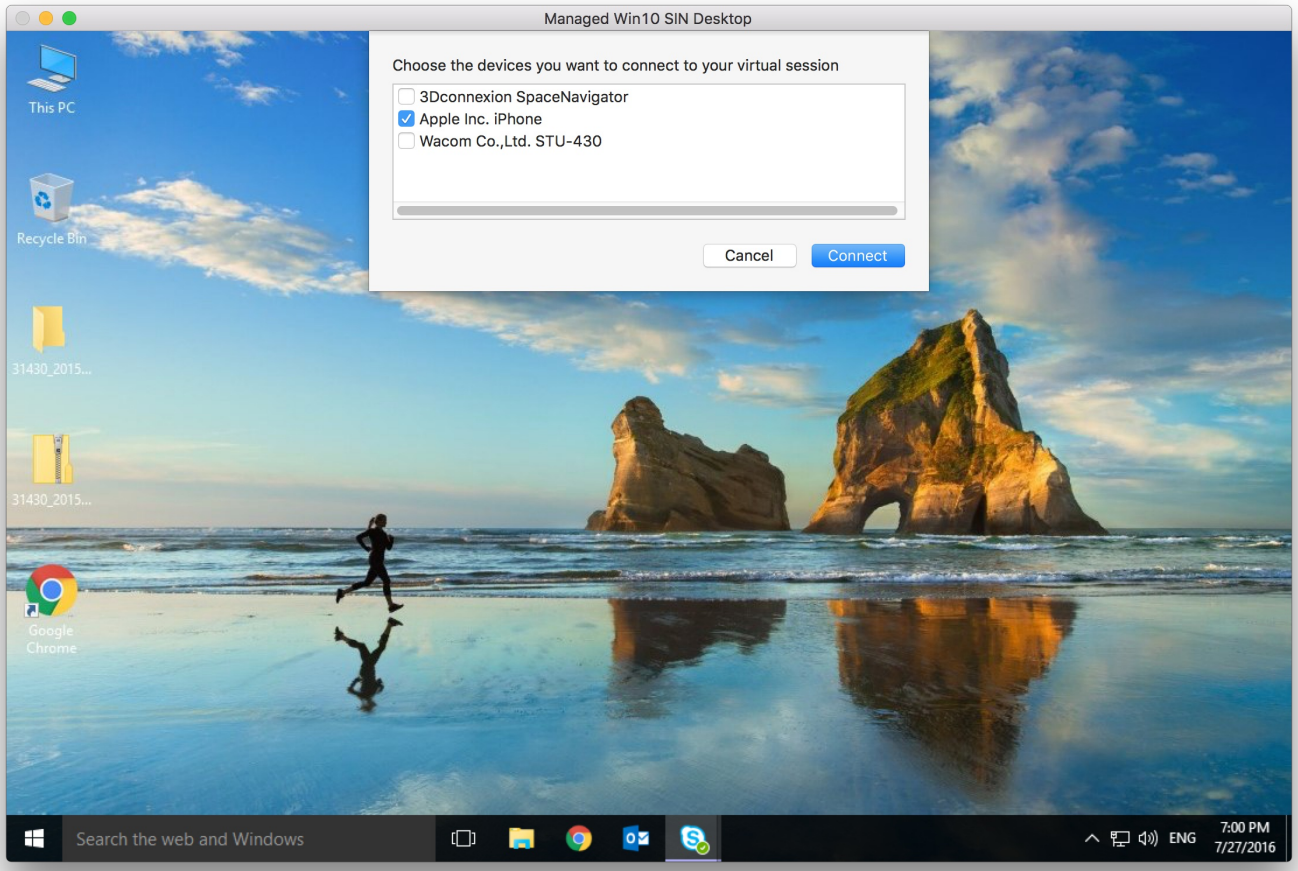
The product supports optimized virtual channels with USB 3.0 devices and USB 3.0 ports, such as a CDM virtual channel used to view files on a camera or to provide audio to a headset). The product also supports Generic USB Redirection of USB 3.0 devices connected to a USB 2.0 port.

Some advanced device-specific features, such as Human Interface Device (HID) buttons on a webcam, may not work as expected with the optimized virtual channel; if this is an issue, use the Generic USB virtual channel.

Certain devices are not redirected by default, and are only available to the local session. For example, it would not be appropriate to redirect a network interface card that is directly attached via internal USB.

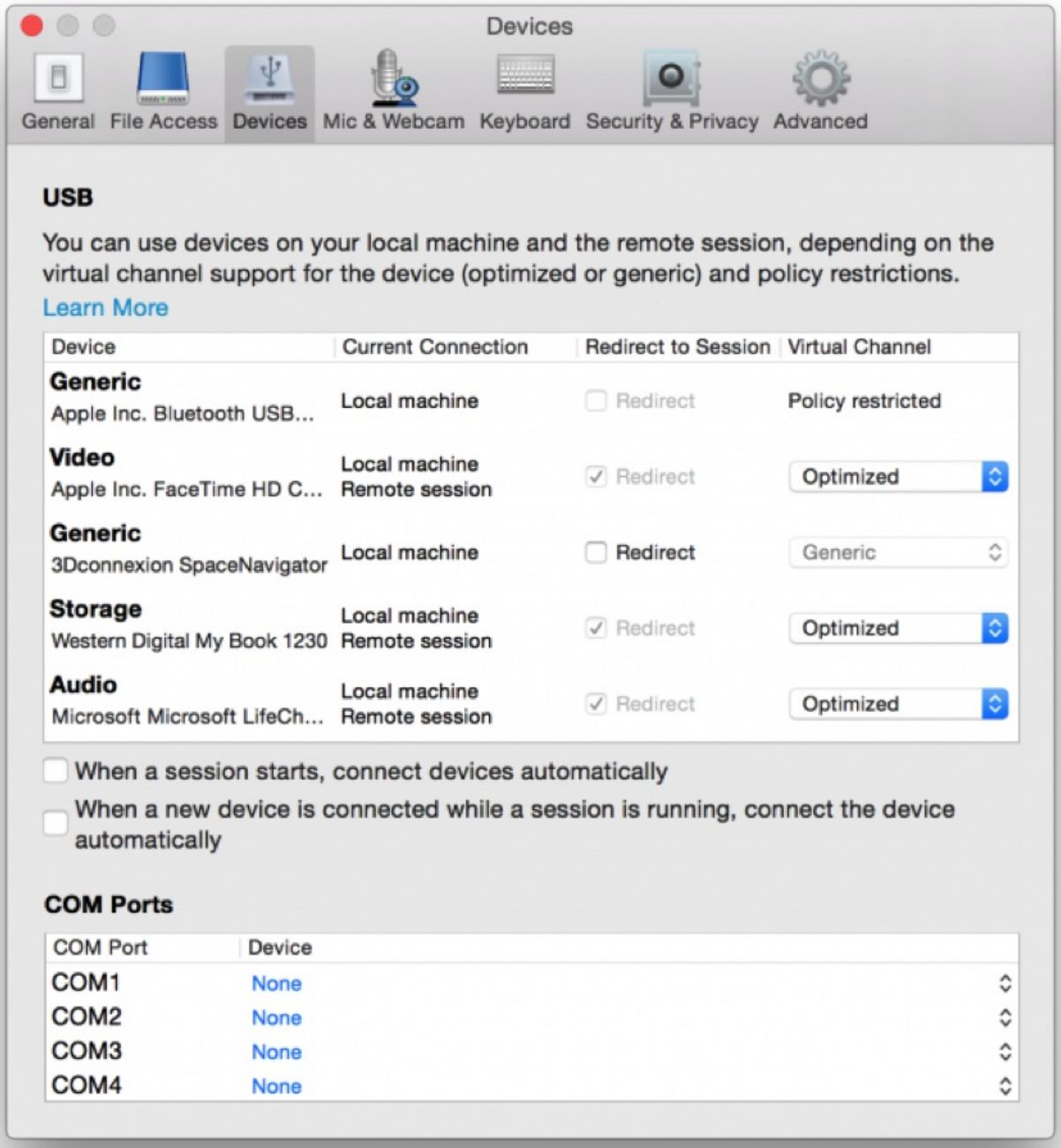
To use USB redirection:

1. Connect the USB device to the device where Receiver is installed.
2. You will be prompted to select the available USB devices on your local system.



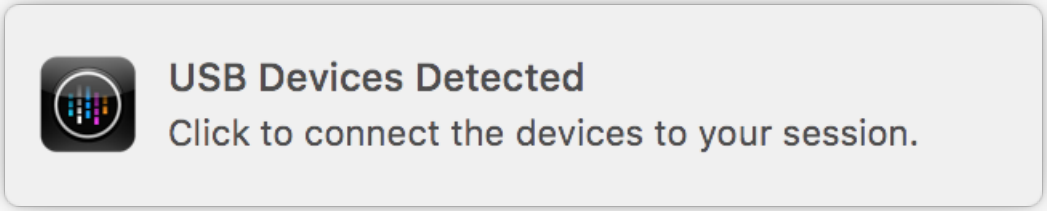

3. Select the device you wish to connect and click **Connect**. If the connection fails, an error message appears.

4. In the **Preferences** window **Devices** tab, the connected USB device is listed in the USB panel:




5. Select the type of virtual channel for the USB device, *Generic* or *Optimized*.

6. A message is displayed. Click to connect the USB device to your session:




**Use and remove USB devices**

Users can connect a USB device before or after starting a virtual session. When using Citrix Receiver for Mac, the following apply:

- Devices connected after a session starts immediately appear in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, sometimes you can resolve the problem by waiting to connect the device until after the virtual session has started.
- To avoid data loss, use the **Windows Safe** removal menu before removing the USB device.

**Configuring Enlightened Data Transport (EDT)**

By default, EDT is enabled in Citrix Receiver for Mac.

Citrix Receiver for Mac reads the EDT settings as set in the default.ica file and applies it accordingly.

To disable EDT, run the following command in a terminal:

defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO

### Configure session reliability and auto client reconnect

Session reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

With session reliability, the session remains active on the server. To indicate that connectivity is lost, the user's display freezes until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session Reliability reconnects users without reauthentication prompts.

> **Important**
>
> Citrix Receiver for Mac users cannot override the server setting.

You can use session reliability with Transport Layer Securuty (TLS).

> **Note**
>
> TLS encrypts only the data sent between the user device and NetScaler Gateway.

### Using session reliability policies

The **session reliability connections** policy setting allows or prevents session reliability.

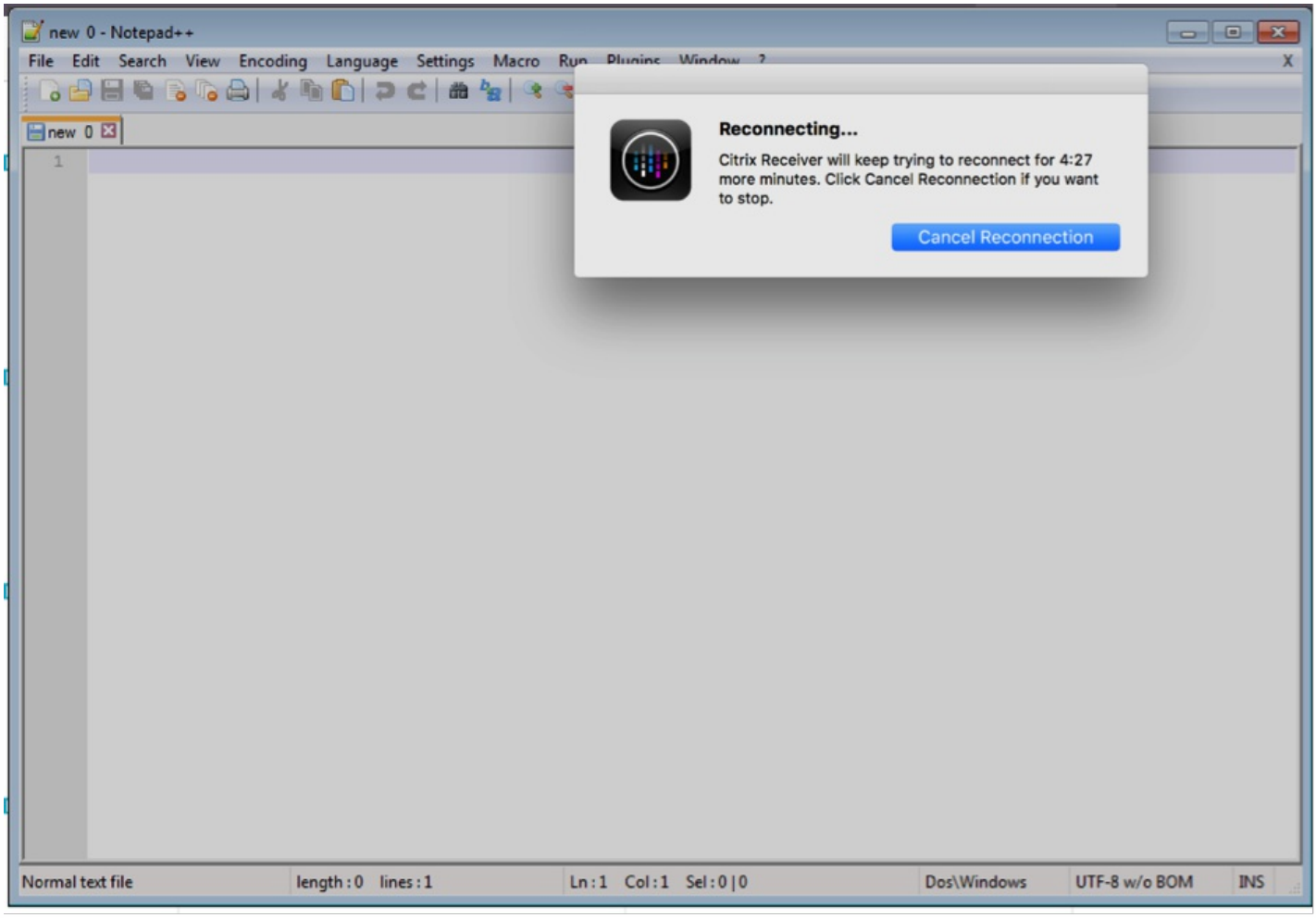
The **session reliability timeout** policy setting has a default of 180 seconds, or three minutes. Though you can extend the amount of time session reliability keeps a session open, this feature is designed to be convenient to the user and it does not, therefore, prompt the user for reauthentication.

> **Tip**
>
> As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.

Incoming session reliability connections use port 2598, unless you change the port number defined in the session reliability port number policy setting.

If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure the Auto client reconnect authentication policy setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both session reliability and auto client reconnect, the two features work in sequence. Session reliability closes, or disconnects, the user session after the amount of time you specify in the Session reliability timeout policy setting. After that, the auto client reconnect policy settings take effect, attempting to reconnect the user to the disconnected session.




## Note

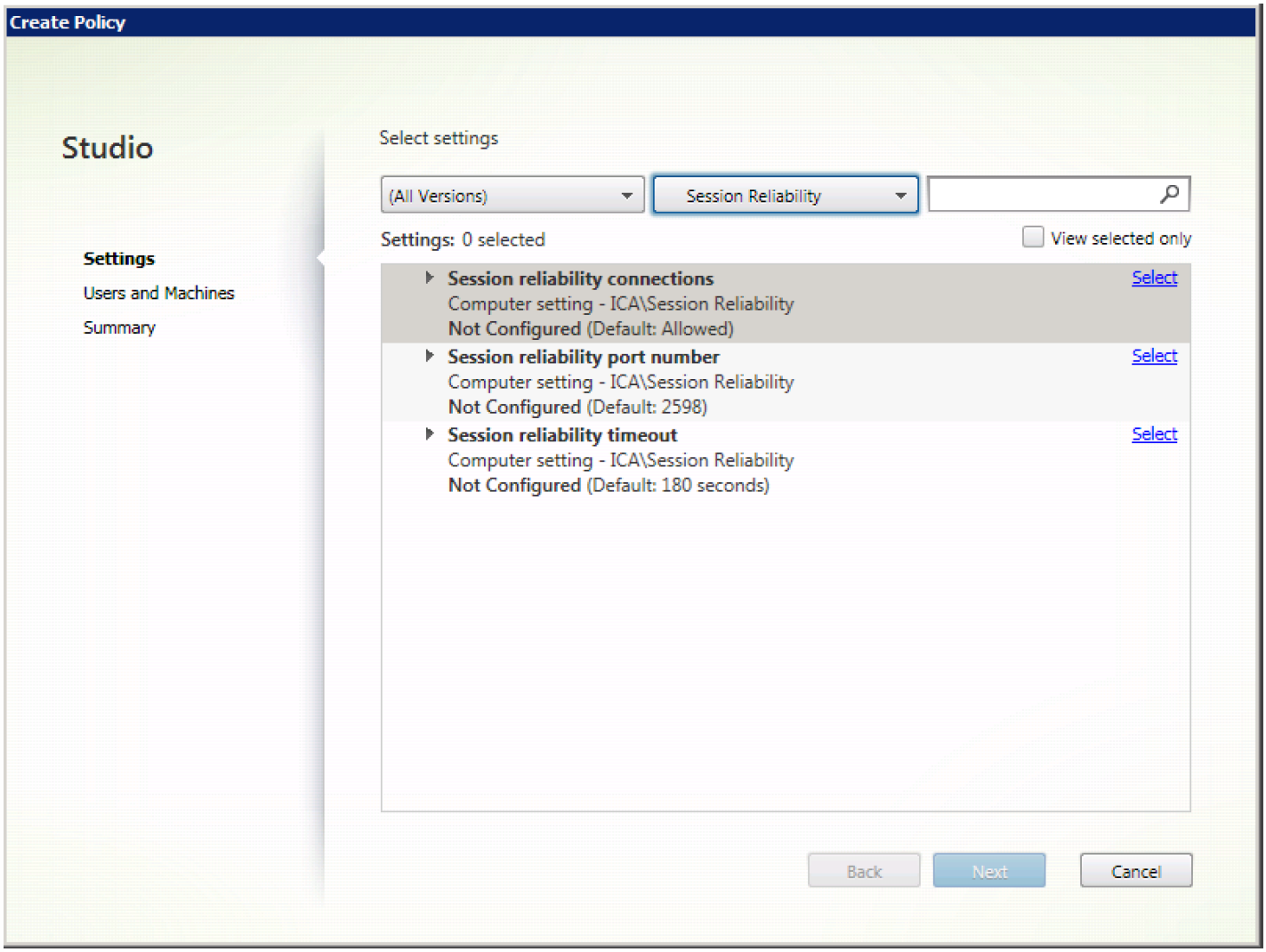
Session reliability is enabled by default at the server. To disable this feature, configure the policy managed by the server.

### Configuring session reliability

By default, session reliability is enabled.

To disable session reliability:

1. Launch Citrix Studio.
2. Open the **Session Reliability connections** policy.
3. Set the policy to **Prohibited**.




**Configuring session reliability timeout**

By default, session reliability timeout is set to 180 seconds.

Note: Session reliability timeout policy can be configured only with XenApp/XenDesktop 7.11 and above.

To modify session reliability timeout:

1. Launch Citrix Studio.
2. Open the **Session reliability timeout** policy.
3. Edit the timeout value.
4. Click **OK**.

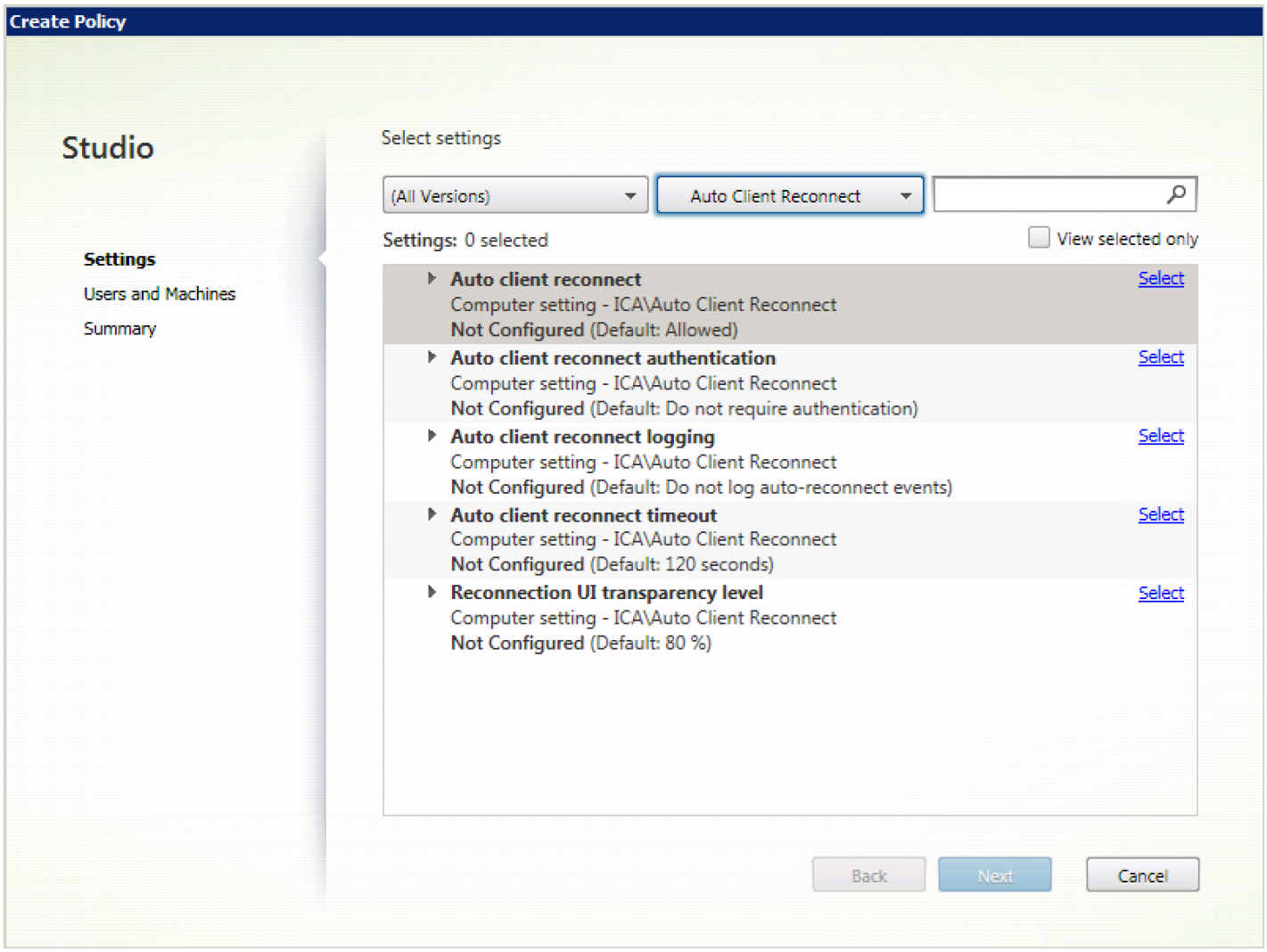
**Configuring auto client reconnection**

By default, auto client reconnection is enabled.

To disable auto client reconnection:

1. Launch Citrix Studio.
2. Open the **Auto client reconnect policy**.

3. Set the policy to **Prohibited**.




**Configuring Auto client reconnection timeout**

By default, Auto client reconnection timeout is set to 120 seconds.

Note: Auto client reconnect timeout policy can be configured only with XenApp/XenDesktop 7.11 and later.

To modify auto client reconnect timeout:

1. Launch Citrix Studio.
2. Open the **Auto client reconnect** policy.
3. Edit the timeout value.
4. Click **OK**.

Limitations:
On a Terminal Server VDA, Citrix Receiver for Mac uses 120 seconds as timeout value irrespective of the user settings.

**Configuring the Reconnect user interface transparency level**

The Session User Interface is displayed during a session reliability and auto client reconnect attempts. The transparency level of the user interface can be modified using Studio policy.

By default, Reconnect UI transparency is set to 80%.

To modify Reconnect user interface transparency level:

1. Launch Citrix Studio.
2. Open the **Reconnect UI transparency level** policy.
3. Edit the value.
4. Click **OK**.

**Auto client reconnect and session reliability interaction**

Mobility challenges associated with switching between various access points, network disruptions and display timeouts related to latency create challenging environments when trying to maintain link integrity for active Citrix Receiver sessions. To resolve this issue, Citrix enhanced session reliability and auto reconnection technologies present in this version of Receiver for Mac.

Auto client reconnection, along with session reliability, allows users to automatically reconnect to their Citrix Receiver sessions after recovering from network disruptions. These features, enabled by policies in Citrix Studio, can be used to vastly improve the user experience.

> **Note**
>
> Auto client reconnection and session reliability timeout values can be modified using the **default.ica** file in StoreFront.

**Auto client reconnection**

Auto client reconnection can be enabled or disabled using Citrix Studio policies. By default, this feature is enabled. For information about modifying this policy, see the auto client reconnection section earlier in this article.

Use the default.ica file in StoreFront to modify the connection timeout for AutoClientReconnect; by default, this timeout is set to 120 seconds (or two minutes ).

| Setting | Example | Default |
|---|---|---|
| TransportReconnectRetryMaxTimeSeconds | TransportReconnectRetryMaxTimeSeconds=60 | 120 |

**Session reliability**

Session reliability can be enabled or disabled using Citrix Studio policies. By default, this feature is enabled.

Use the **default.ica** file in StoreFront to modify the connection timeout for session reliability; by default, this timeout is set to 180 seconds (or three minutes).

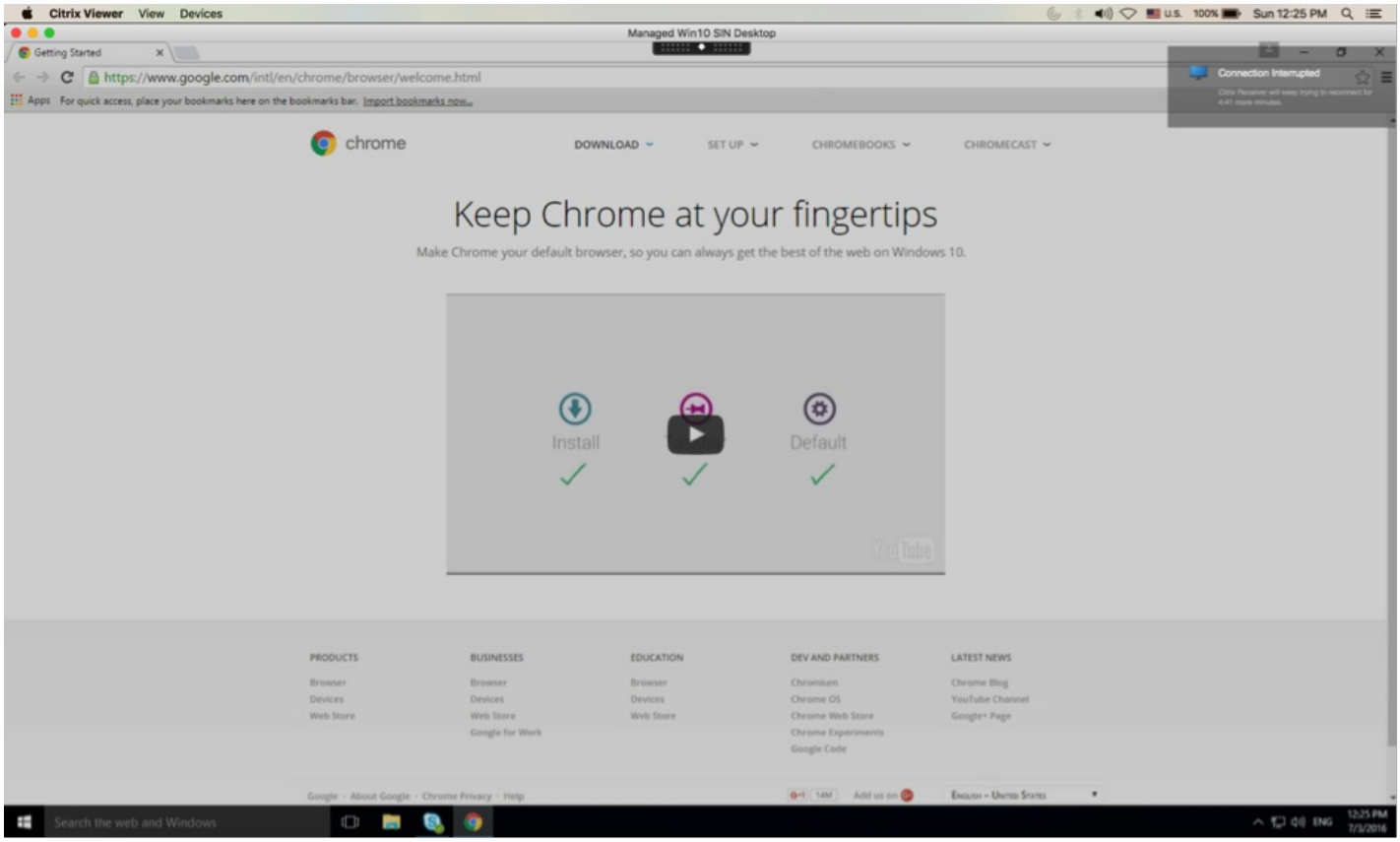
| Setting | Example | Default |
|---|---|---|
| SessionReliabilityTTL | SessionReliabilityTTL=120 | 180 |

**How auto client reconnection and session reliability works**

When auto client reconnection and session reliability are enabled for a Citrix Receiver for Mac, consider the following:

- A session window is greyed out when a reconnection is in progress; a countdown timer displays the amount of time remaining before the session is reconnected. Once a session is timed out, it is disconnected.

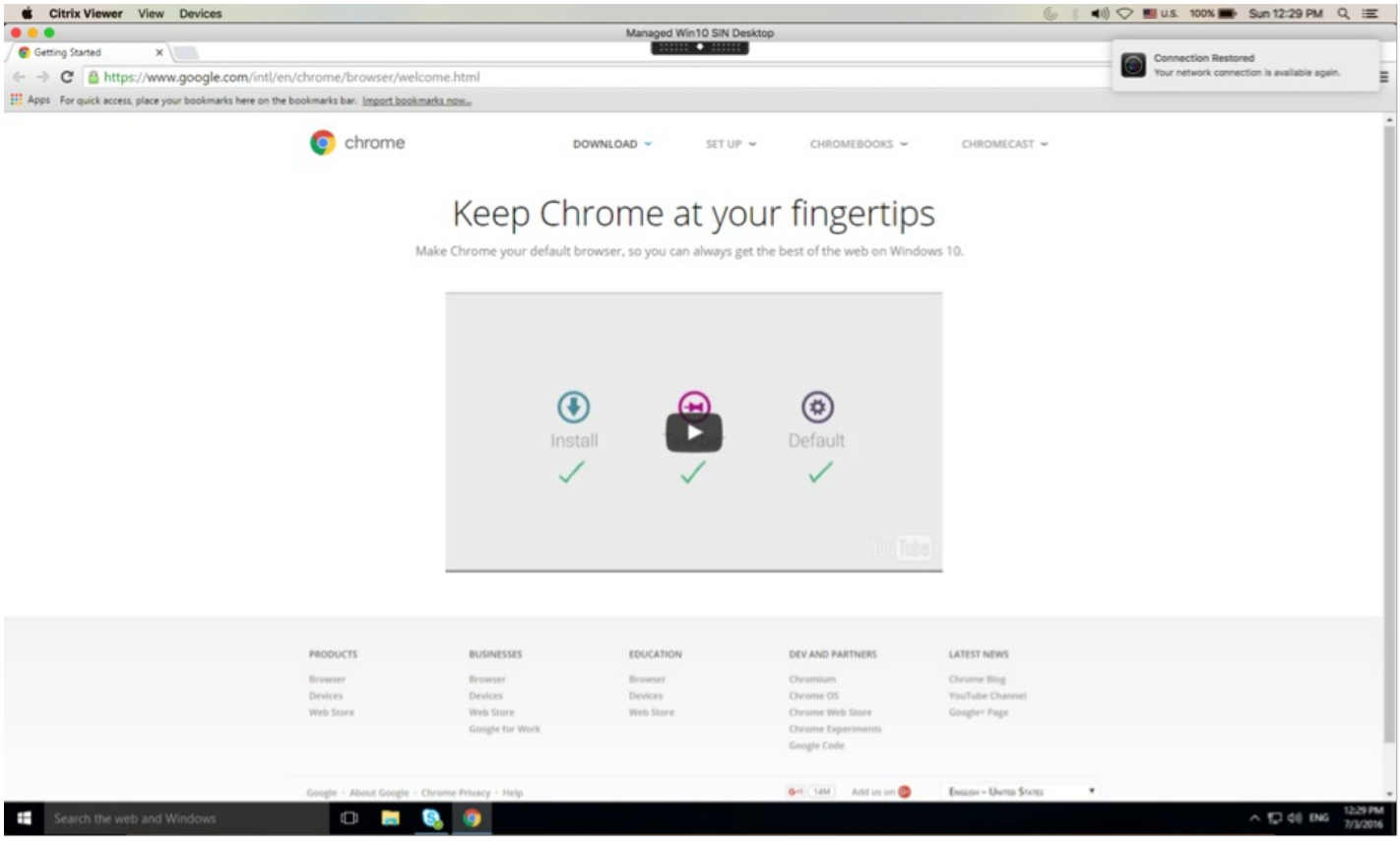
By default, the reconnect countdown timer notification starts at 5 minutes; this time value represents the combined default values for each of the timers (auto client reconnection and session reliability), 2 and 3 minutes respectively. The image below illustrates the countdown timer notification which appears in the upper right portion of the session interface:



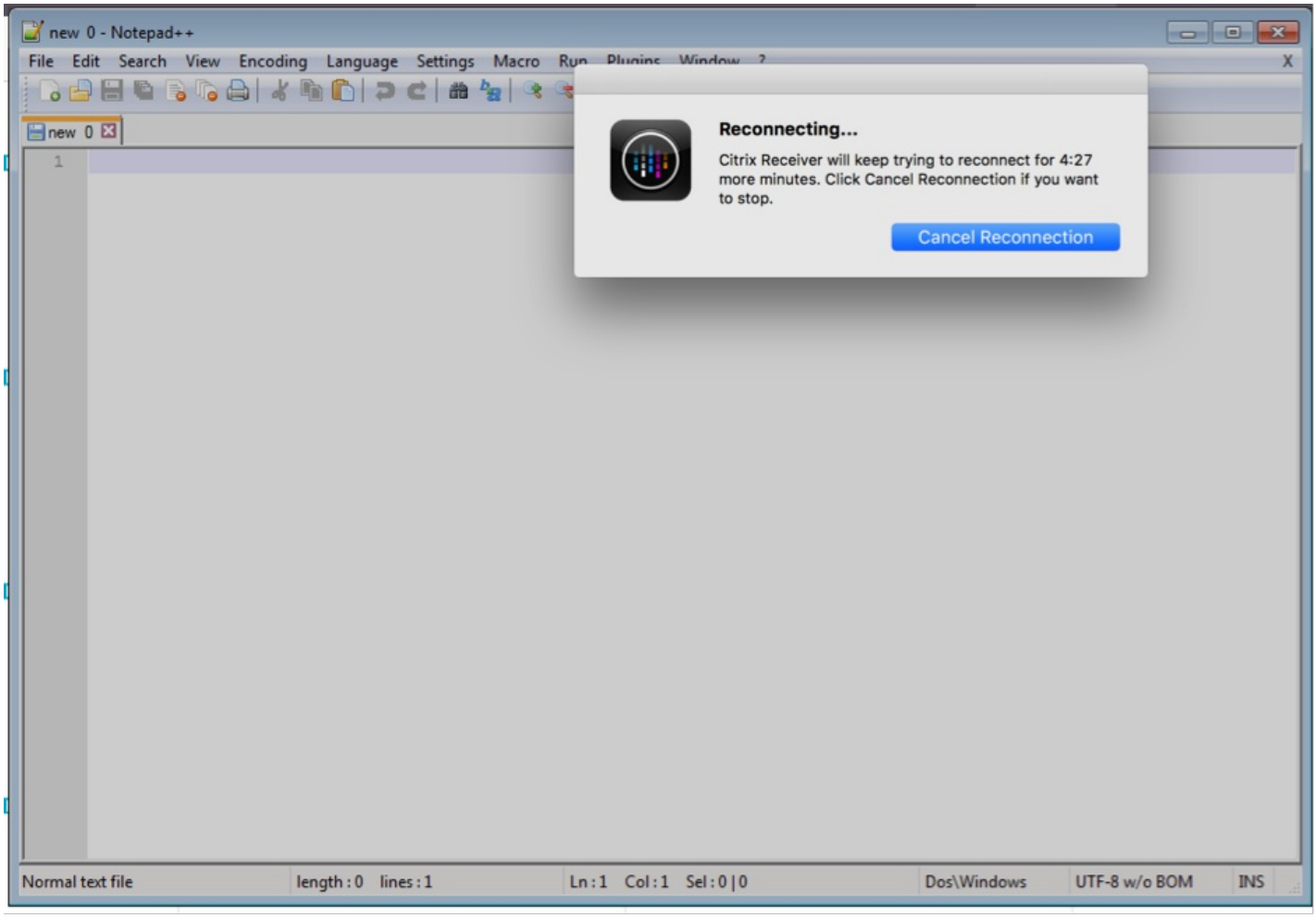

## Tip

You can alter the greyscale brightness used for an inactive session using a command prompt. For example, defaults write com.citrix.receiver.nomas NetDisruptBrightness 80. By default, this value is set to 80. The maximum value cannot exceed 100 (indicates a transparent window) and the minimum value can be set to 0 (a fully blacked out screen).

- Users are notified when a session successfully reconnects (or when a session is disconnected). This notification appears in the upper right portion of the session interface:




- A session window which is under auto client reconnect and session reliability control provides an informational message indicating the state of the session connection. Click **Cancel Reconnection** to move back to an active session.



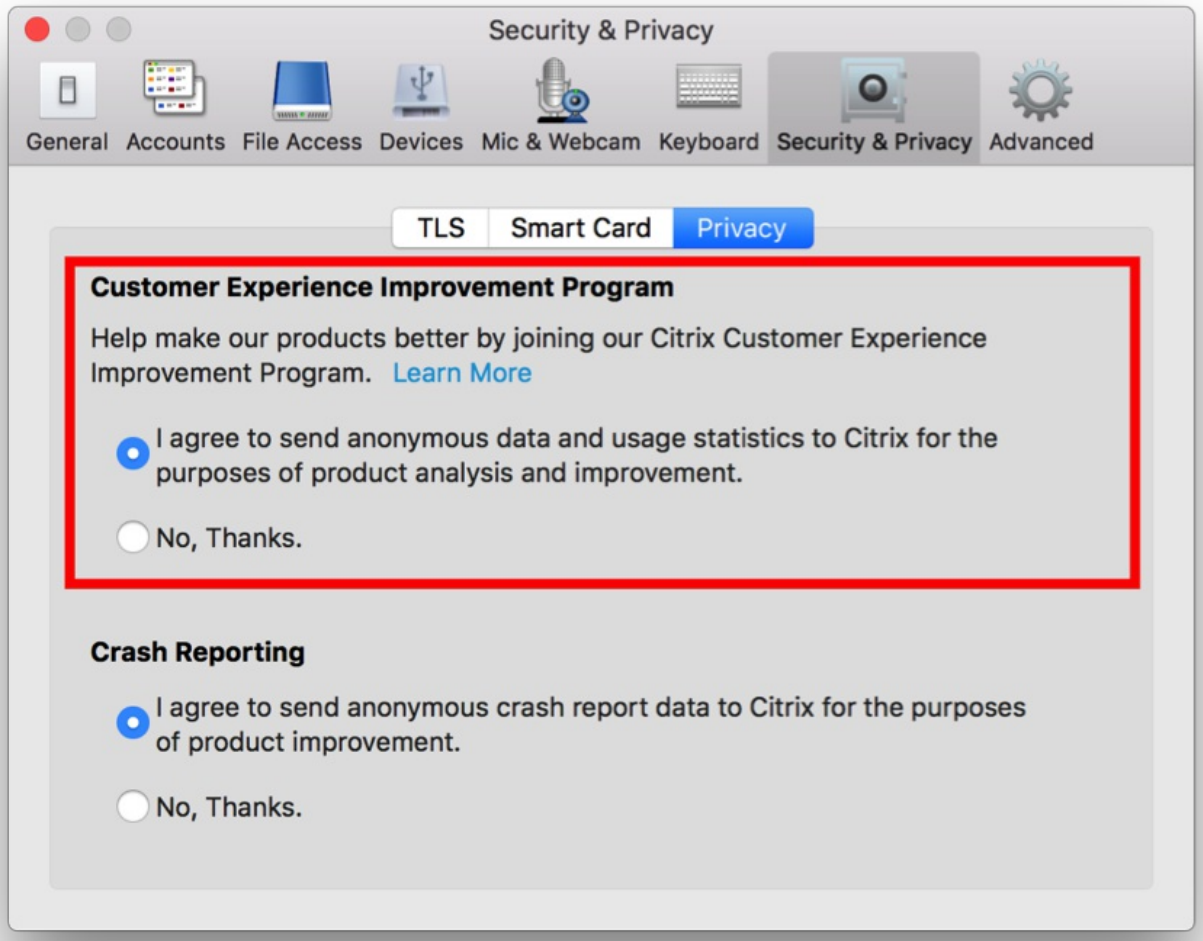

## Configuring CEIP

CEIP is scheduled to collect and securely upload data to Citrix at an interval of 7 days by default. You can change your participation in CEIP anytime using the Citrix Receiver for Mac > **Security > Preferences** screen.

> ### Tip
>
> When CEIP is disabled, minimal information containing only the installed Citrix Receiver for Mac version is uploaded; this happens only once. This minimal information is valuable to Citrix because it provides the distribution of different versions used by customers. This happens only once as soon as CEIP is disabled.

To disable CEIP, or to forego participation:

1. In the **Preferences** window, select **Security and Privacy**.
2. Select the **Privacy** tab.
3. Change the appropriate radio button. For example, to disable CEIP, click "**No, Thanks**."
4. Click **OK**.




## 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, Citrix 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 Citrix Receiver for Mac or configuring Citrix Receiver for Mac to point to a StoreFront site, you can configure self-service mode, which enables your users to subscribe to applications through Citrix Receiver for Mac. 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 Citrix Receiver for MacTech Preview user experience. For more information about the Citrix Receiver for Mac 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 for Mac.

### Configure self-service mode

As mentioned previously, by adding a StoreFront account to Citrix Receiver for Mac or configuring Citrix Receiver for Mac to point to a StoreFront site, you can configure self-service mode, which allows users to subscribe to applications from the Citrix Receiver for Mac 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 Citrix Receiver for Mac 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 for Mac. 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 Citrix Receiver for Mac.
2. Configure stores for CloudGateway just as you would for other XenApp and XenDesktop applications. No special configuration is needed for Citrix Receiver for Mac. 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

## Configuring email-based account discovery

You can configure Citrix Receiver for Mac to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Citrix Receiver for Mac installation and configuration. Citrix Receiver for Mac determines the NetScaler 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 to accept user connections by using an email address to discover the StoreFront, NetScaler Gateway, see
*— Connecting to StoreFront by Using Email-Based Discovery*
in the NetScaler 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 Citrix Receiver for Mac, users simply open the file to configure Citrix Receiver for Mac. If you configure Receiver for Web sites, users can also obtain Citrix Receiver for Mac 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 Citrix Receiver for Mac, 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: the NetScaler Gateway address, product edition, and required authentication method
  For more information about configuring NetScaler Gateway, see the NetScaler Gateway documentation.

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

# Configuring auto-update

### Configuring using the graphical user interface

An individual user can override the auto-update setting using the **Preferences** dialog. This is a per-user configuration and

the settings apply only to the current user.

1. Go to the **Preferences** dialog in Citrix Receiver for Mac.
2. In the **Advanced** pane, click **Auto Update**. The auto-update dialog appears.
3. Select one of the following options:
   - Yes, notify me
   - No, don't notify me
   - Use administrator specified settings
4. Close the dialog box to save the changes.

### Configuring Auto-update using StoreFront

Administrators can configure Auto-update using StoreFront. Citrix Receiver only uses this configuration for users who have selected "Use administrator specified settings." To manually configure it, follow the steps below.

1. Use a text editor to open the web.config file. The default location is C:\inetpub\wwwroot\Citrix\Roaming\web.config
2. Locate the user account element in the file (Store is the account name of your deployment)

   For example: <account id=... name="Store">

   Before the *</account>* tag, navigate to the properties of that user account:

```
<properties>

  <clear />
</properties>
```

3. Add the auto-update tag after *<clear />* tag.

## auto-update-Check

This determines that Citrix Receiver can detect if updates are available.

**Valid values:**

- Auto – Use this option to get notifications when updates are available.
- Manual – Use this option to not get any notification when updates are available. Users need to check manually for updates by selecting **Check for Updates**.
- Disabled – Use this option to disable Auto-update.

## auto-update-DeferUpdate-Count

This determines the number of times the end user will be notified to upgrade before they are forced to update to the latest version of Citrix Receiver. By default, this value is 7.

**Valid values:**

- -1 – The end user will always have the option of getting reminded later when an update is available.

- 0 – End user will be forced to update to the latest version of Citrix Receiver as soon as the update is available.
- Positive integer – End user will be reminded this many number of times before being forced to update. Citrix recommends not to set this value higher than 7.

## auto-update-Rollout-Priority

This determines how quickly a device will see that an update is available.

**Valid values:**

- Auto – The auto-update system will decide when available updates are rolled out to users.
- Fast – Available updates will be rolled out to users on high priority as determined by Citrix Receiver.
- Medium – Available updates will be rolled out to users on medium priority as determined by Citrix Receiver.
- Slow – Available updates will be rolled out to users on low priority as determined by Citrix Receiver.

# Optimizing your Citrix Receiver for Mac environment

Jun 19, 2017

You can optimize your Citrix Receiver for Mac environment as follows:

- Reconnecting users automatically
- Restarting desktops
- Providing session reliability
- Providing continuity for roaming users
- Mapping client devices
- Mapping client drives
- Mapping client COM ports

## Reconnecting users automatically

Users can be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the auto-client reconnection feature, Citrix Receiver for Mac 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. Citrix Receiver for Mac 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 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, Citrix Receiver for Mac shuts down the desktop and then starts it.

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

## Providing session reliability

With the 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 Session Reliability using policy settings on the server. For more information about session reliability and Receiver interaction, refer to this document about ensuring the highest quality of service and reliability.

For additional information specific to policies, see Auto Client Reconnect Policy settings and Session reliability policy settings.

> **Tip**
>
> Citrix Receiver for Mac users cannot override the server settings for Session Reliability.

> **Important**
>
> If 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 Citrix Receiver for Mac window and choose **Preferences**.
2. Click **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

Citrix Receiver for Mac 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**

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.

Citrix Receiver for Mac 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 Citrix Receiver for Mac preferences.

**To configure read and write access for mapped drives**

1. On the Citrix Receiver for Mac 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 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 Citrix Receiver for Mac 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 Citrix Receiver for Mac 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

Jun 19, 2017

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

- Customer Experience Improvement Program (CEIP)
- 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

## Customer Experience Improvement Program (CEIP)

The Citrix Customer Experience Improvement Program (CEIP) gathers anonymous configuration and usage data from Citrix Receiver for Mac and automatically sends the data to Citrix. This data helps Citrix improve the quality, reliability, and performance of Citrix Receiver for Mac. For more information, see Configuring CEIP.

## 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 Citrix Receiver for Mac.

Citrix Receiver for Mac 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

Citrix Receiver for Mac 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 Citrix Receiver for Mac. For information about configuring this feature, see Audio features information on the Product Documentation site.

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 Citrix Receiver for Mac > 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

Citrix Receiver for Mac 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.<br><br>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.<br><br>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 |

| PC key or action | Mac options |
| --- | --- |
| 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. Citrix Receiver for Mac 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 Citrix Receiver for Mac 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)<br>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)<br>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<br>Control-Option-Fn-Delete (on MacBook keyboards)<br>Choose Keyboard >Send Ctrl-Alt-Del |
| Delete | Delete<br>Choose Keyboard > Send Key > Delete<br>Fn-Backspace (Fn-Delete on some US keyboards) |
| End | End<br>Fn-Right Arrow |
| Esc | Escape<br>Choose Keyboard > Send Key > Escape |
| F1 to F12 | F1 to F12<br>Choose Keyboard > Send Function Key > F1 to F12 |
| Home | Home<br>Fn–Left Arrow |
| Insert | Choose Keyboard > Send Key > Insert |
| Num Lock | Clear |
| Page Down | Page Down |

| | |
|---|---|
| | Fn–Down Arrow |
| Page Up | Page Up<br>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)<br>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

Citrix Receiver for Mac 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.

Citrix Receiver for Mac 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 Mar**k.

**To use server-side IME**

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

**Mapped server-side IME input mode keys**

Citrix Receiver for Mac 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 Citrix 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 10.9, 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 for Mac communications

Jun 19, 2017

This section provides information on Secure communication in Citrix Receiver for Mac.


- About certificates
- Connecting with NetScaler Gateway
- Connecting with the Secure Gateway
- Connecting through a proxy server
- Connecting through a firewall
- Connecting with the Transport Layer Security (TLS) Relay
  - About TLS Policies
  - Configuring and enabling Receiver for TLS
  - Installing root certificates on user devices
  - Configuring TLS Policies
- Using the UI to configure security settings


To secure the communication between your server farm and Citrix Receiver for Mac, you can integrate your connections to the server farm with a range of security technologies, including Citrix NetScaler Gateway. For information about configuring this with Citrix StoreFront, see 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 for Mac 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 Citrix Receiver for Mac 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 Citrix Receiver for Mac.

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

**Importing root certificates on Receiver for Mac devices**

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

**Wildcard certificates**

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

**Intermediate certificates with NetScaler Gateway**

If your certificate chain includes an intermediate certificate, the intermediate certificate must be mapped to the NetScaler Gateway server certificate. For information on this task, see NetScaler Gateway documentation. For more information about installing and linking an intermediate certifcate with Primary CA on a NetScaler Gateway appliance, refer to the article How to Install and Link Intermediate Certificate with Primary CA on NetScaler Gateway.

**Joint Server Certificate Validation Policy**

Citrix Receiver for Mac has a stricter validation policy for server certificates.

> ## Important
>
> Before installing this version of Citrix Receiver for Mac, confirm that the certificates at the server or gateway are correctly configured as described here. Connections may fail if:
>
> - the server or gateway configuration includes a wrong root certificate
> - the server or gateway configuration does not include all intermediate certificates
> - the server or gateway configuration includes an expired or otherwise invalid intermediate certificate
> - the server or gateway configuration includes a cross-signed intermediate certificate

When validating a server certificate, Citrix Receiver for Mac now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous Citrix Receiver for Mac releases, it then also checks that the certificates are trusted. If the certificates are not all trusted, the connection fails.

This policy is stricter than the certificate policy in web browsers. Many web browsers include a large set of root certificates that they trust.

The server (or gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Receiver for Mac's connection to fail.

Suppose a gateway is configured with these valid certificates. This configuration is recommended for customers who require stricter validation, by determining exactly which root certificate is used by Citrix Receiver for Mac:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Example Root Certificate"

Then, Citrix Receiver for Mac will check that all these certificates are valid. Citrix Receiver for Mac will also check that it already trusts "Example Root Certificate". If Citrix Receiver for Mac does not trust "Example Root Certificate", the connection fails.

### Important

Some certificate authorities have more than one root certificate. If you require this stricter validation, make sure that your configuration uses the appropriate root certificate. For example, there are currently two certificates ("DigiCert"/"GTE CyberTrust Global Root", and "DigiCert Baltimore Root"/"Baltimore CyberTrust Root") that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available ("DigiCert Baltimore Root"/"Baltimore CyberTrust Root"). If you configure "GTE CyberTrust Global Root" at the gateway, Citrix Receiver for Mac connections on those user devices will fail. Consult the certificate authority's documentation to determine which root certificate should be used. Also note that root certificates eventually expire, as do all certificates.

### Note

Some servers and gateways never send the root certificate, even if configured. Stricter validation is then not possible.

Now suppose a gateway is configured with these valid certificates. This configuration, omitting the root certificate, is normally recommended:

- "Example Server Certificate"
- "Example Intermediate Certificate"

Then, Citrix Receiver for Mac will use these two certificates. It will then search for a root certificate on the user device. If it finds one that validates correctly, and is also trusted (such as "Example Root Certificate"), the connection succeeds. Otherwise, the connection fails. Note that this configuration supplies the intermediate certificate that Citrix Receiver for Mac needs, but also allows Citrix Receiver for Mac to choose any valid, trusted, root certificate.

Now suppose a gateway is configured with these certificates:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- "Wrong Root Certificate"

A web browser may ignore the wrong root certificate. However, Citrix Receiver for Mac will not ignore the wrong root certificate, and the connection will fail.

Some certificate authorities use more than one intermediate certificate. In this case, the gateway is normally configured with all the intermediate certificates (but not the root certificate) such as:

- "Example Server Certificate"
- "Example Intermediate Certificate 1"
- "Example Intermediate Certificate 2"

## Important

Some certificate authorities use a cross-signed intermediate certificate. This is intended for situations there is more than one root certificate, and a earlier root certificate is still in use at the same time as a later root certificate. In this case, there will be at least two intermediate certificates. For example, the earlier root certificate “Class 3 Public Primary Certification Authority” has the corresponding cross-signed intermediate certificate “VeriSign Class 3 Public Primary Certification Authority - G5”. However, a corresponding later root certificate “VeriSign Class 3 Public Primary Certification Authority - G5” is also available, which replaces “Class 3 Public Primary Certification Authority”. The later root certificate does not use a cross-signed intermediate certificate.

## Note

The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To), but the cross-signed intermediate certificate has a different Issuer name (Issued By). This distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such "Example Intermediate Certificate 2").

This configuration, omitting the root certificate and the cross-signed intermediate certificate, is normally recommended:

- "Example Server Certificate"
- "Example Intermediate Certificate"

Avoid configuring the gateway to use the cross-signed intermediate certificate, as it will select the earlier root certificate:

- "Example Server Certificate"
- "Example Intermediate Certificate"
- “Example Cross-signed Intermediate Certificate” [not recommended]

It is not recommended to configure the gateway with only the server certificate:

- "Example Server Certificate"

In this case, if Citrix Receiver for Mac cannot locate all the intermediate certificates, the connection will fail.

### Connecting with NetScaler Gateway

To enable remote users to connect to your XenMobile deployment through NetScaler Gateway, you can configure these to work with StoreFront. The method for enabling access depends on the edition of XenMobile in your deployment.

If you deploy XenMobile in your network, allow connections from internal or remote users to StoreFront through NetScaler Gateway by integrating NetScaler 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, see the Integrating with NetScaler Gateway and NetScaler documentation.

### 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 Citrix Receiver for Mac and the server. No configuration of Citrix Receiver for Mac is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

Citrix Receiver for Mac 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 Citrix Receiver for Mac, 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 and Secure Gateway documentation.

If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure Citrix Receiver for Mac 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 Citrix Receiver for Mac and servers. Citrix Receiver for Mac supports both SOCKS and secure proxy protocols.

When communicating with the XenApp or XenDesktop server, Citrix Receiver for Mac 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, Citrix Receiver for Mac 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, Citrix Receiver for Mac 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 Citrix Receiver for Mac. Citrix Receiver for Mac then connects to the server using the external address and port number. For more information, see the Web Interface documentation.

### Connecting using TLS

Citrix Receiver for Mac 12.3, supports TLS 1.0, 1.1 and 1.2 with the following cipher suites for TLS connections to 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

**Note**: Citrix Receiver for Mac running on Mac OS Sierra does not support the following TLS cipher suites:

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Transport Layer Security (TLS) is the latest, standardized version of the TLS protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of TLS 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.

Citrix Receiver for Mac supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

For information about configuring and using SSL Relay to secure your installation, see the XenDesktop and StoreFront documentation.

> **Note**
>
> Citrix Receiver for Mac uses platform (OS X) crypto for connections between Citrix Receiver for Mac and StoreFront.

## Configuring and enabling Citrix Receiver for Mac 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 Citrix Receiver for Mac 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 TLS-enabled clients and by any other application using TLS.

## About TLS policies

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

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

TLS 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 TLS policies

To configure TLS 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
```

### Using the UI to configure security settings

Numerous security improvements and enhancements were introduced with Citrix Receiver for Mac version 12.3, including:

- improved security configuration user interface. In previous releases, the command line was the preferred method to make security-related changes; configuration settings related to session security are now simple and accessible from the UI, which improves the user experience while creating a seamless method for the adoption of security-related preferences.
- view TLS connections. Citrix Receiver for Mac allows you to verify connections made to servers that are using a specific TLS version, with additional information including the encryption algorithm used for the connection, mode, key size and whether SecureICA is enabled. In addition, you can view the server certificate for TLS connections.

The improved **Security and Privacy** screen includes the following new options in the **TLS** tab:

- set the compliance mode
- configure the crypto module
- select the appropriate TLS version
- select the certificate revocation list
- enable settings for all TLS connections

The image below illustrates the Security and Privacy settings accessible from the UI: