Citrix Receiver for iOS 7

Contents

What's new

December 16, 2018

What's new in 7.5.6

When enabling Session Reliability, an alert now appears, saying "You must log in again for this setting to take effect. Citrix Receiver will log you out." You must log back into Citrix Receiver for iOS in order for Session Reliability to function correctly.

What's new in 7.5.5

This release addresses a number of issues that help to improve overall performance and stability.

What's new in 7.5.4

Support for Server Name Indicator (SNI)

Citrix Receiver for iOS now supports NetScaler Gateway with Server Name Indication (SNI) configured so that users can launch desktops and applications successfully. For more information on SNI, see Knowledge Center article CTX125798.

What's new in 7.5.3

This release addresses a number of issues that help to improve overall performance and stability.

What's new in 7.5.2

This release addresses a number of issues that help to improve overall performance and stability.

What's new in 7.5.1

Support for iPhone X

Citrix Receiver for iOS supports the iPhone X.

What's new in 7.5

Enhancement to adaptive transport

In earlier releases, when HDXoverUDP in the ICA file is set to **Preferred**, data transport over EDT is used when possible, with fallback to TCP.

Starting with this release and with session reliability enabled, EDT and TCP are attempted in parallel during initial connection, and during session reliability reconnection. This enhancement reduces connection times when EDT is preferred but TCP needs to be used as is the case when the required underlying UDP transport is unavailable.

By default, after fallback to TCP, adaptive transport continues to seek EDT every five minutes.

New signing certificate

Citrix is changing the signing certificate for Citrix Receiver 7.5 for iOS. This change ensures all Citrix iOS apps are consolidated under one signing certificate and allows improved inter-application communication between all Citrix iOS apps. After upgrading to Citrix Receiver 7.5 for iOS, devices configured to use client certificates or an RSA software token to log on to Citrix Receiver will need to re-import client certificates and RSA software tokens before they can log on to Citrix Receiver for iOS. Devices configured for other authentication methods will not be affected by this change. New installations of Citrix Receiver 7.5 for iOS are also not affected by the signing certificate change. For more information, see Knowledge Center article CTX231419.

Joint Server Certificate Validation policy

Citrix Receiver 7.5 for iOS introduces a new, stricter validation policy for server certificates, which might affect session launches. A Strict Certificate Validation setting has also been added in Advanced Settings. For more information, see Knowledge Center article CTX224709.

TLS versions

A new setting to select TLS versions has been added in Advanced Settings. The option **TLS 1.0, 1.1 (NetScaler Compatibility)** is available in the TLS Versions setting to address the TLS handshake failure when connecting through earlier versions of NetScaler. For more information on the TLS handshake failure, see Knowledge Center article CTX221453. By default, the TLS versions is set to **TLS 1.0, 1.1, 1.2**.

What's new in 7.4

Auto Tablet Mode

Citrix Receiver for iOS supports switching between Tablet Mode and Desktop Mode when using a Windows 10 VDA. On iOS devices, a Windows 10 VDA launches in Tablet Mode when there is no keyboard or mouse attached. When a keyboard or a mouse or both are connected to the session, the VDA starts in Desktop Mode. Detaching or attaching hardware toggles between Tablet Mode and Desktop Mode. XenApp/XenDesktop 7.14 and later and XenServer 7.2 and later are required for this feature.

This option is on by default. To turn it off, users can go to **Settings > Advanced > Auto Tablet Mode**.

> Note:
>
> There is a known limitation in how iOS detects keyboard switching when an app is running and a keyboard is attached to the device. Because of this OS limitation, tablet-to-desktop mode switching does not happen seamlessly when an external keyboard is attached to the device during a session. The mode shifts only after one of the following three user interactions:
>
> - Upon selecting a text area again.
> - Three finger touch on the session.
> - Toggling the keyboard from the toolbar.
>
> However, switching from Desktop Mode to Tablet Mode happens seamlessly when the user detaches a keyboard during a session.

What's new in 7.3.1

Citrix Receiver 7.3.1 for iOS is a maintenance release to address customer reported issues.

What's new in 7.3

Support for iOS 11, including Dock support

Citrix Receiver 7.3 for iOS supports iOS 11, including support for the new Dock. On iPads, Citrix Receiver can be added to the Dock that displays users' favorite apps, or if no favorites are selected, a display of frequently used applications.

> **Important**
>
> Citrix Receiver 7.3 is not supported on Apple devices running iOS 8.x.

What's new in 7.2.5

Citrix Receiver 7.2.5 for iOS is a maintenance release to address an issue that prevents customer ratings.

What's new in 7.2.4

Citrix Receiver 7.2.4 for iOS is a maintenance release to address a customer reported issue.

> **Important**
>
> Support for Apple devices running iOS 8.x has been deprecated from this release.

What's new in 7.2.3

Citrix Receiver 7.2.3 for iOS is a maintenance release to address a customer reported issue.

What's new in 7.2.2

Custom Resolution

Citrix Receiver for iOS now supports custom Retina resolution in sessions and also allows users to set custom session resolutions. Users can go to **Receiver Settings** > **Display Options** > **Custom Resolution** to set the desired resolution. In addition, users can optionally pick an auto-fit mode.

What's new in 7.2.1

Citrix Receiver 7.2.1 for iOS is a maintenance release to address a customer reported issue.

What's new in 7.2

Adaptive transport

Adaptive transport for XenApp and XenDesktop optimizes data transport by applying a new Citrix protocol called Enlightened Data Transport (EDT) in preference to TCP whenever possible. Compared to TCP and UDP, EDT delivers a superior user experience on long-haul WAN and internet connections. EDT dynamically responds to changing network conditions while maintaining high server scalability and efficient use of network capacity. EDT is built on UDP and improves data throughput for all ICA virtual channels, including Thinwire display remoting, file transfer (Client Drive Mapping), printing, multimedia redirection. If UDP is not available, adaptive transport automatically reverts to TCP. For more information, see Adaptive Transport.

Mandatory apps

IT administrators can configure specific applications or desktops as mandatory using StoreFront keywords in the published resource properties. This results in the applications or desktops being automatically subscribed to the user. Users cannot remove these applications or desktops from the Citrix Receiver favorites menu.

What's new in 7.1.3

Citrix Receiver 7.1.3 for iOS is a maintenance release to address the following issue:

- After upgrading an iOS device to iOS 10.2, smart card authentication fails. With this fix, smart card authentication works as intended. The changes required for this fix are isolated to the SmartCard authentication functionality; there are no changes to other Receiver for iOS functions.

What's new in 7.1.2

Support for StoreFront hidden stores

Citrix Receiver for iOS now supports the use of hidden store URLs from StoreFront. Hidden stores may be added by appending "?[store name]" to the URL in the Add New Account dialog.

For more information, see Knowledge Center article CTX214819.

[#665362]

What's new in 7.1.1

Citrix Receiver 7.1.1 for iOS is a maintenance release to address the following issues:

- Receiver for iOS can exit unexpectedly if you attempt to add a new account. This issue occurs only on iOS 8.1.x.
- An SSL handshake Error 183 can occur when you connect to a Receiver session. This issue occurs mainly on iPad 2, 3, and 4.
- When you click the Windows Start menu using an X1 Mouse, the Receiver extended keyboard appears. The extended keyboard bar obscures all or part of the Start menu.
- Configuration of Citrix Receiver for iOS is not possible when using the Citrix Mobile Receiver Setup URL Generator.

What's new in 7.1

iOS 10 support, including Widget support

Citrix Receiver for iOS supports iOS 10, including widgets. The Citrix Receiver widget displays the last application or desktop launched by the user for quicker access to frequently used apps and desktops.

Touch ID support

Touch ID can be used for faster authentication and enhanced user experience.

> **Note:**
>
> Touch ID does not work when launching XenApp/XenDesktop (ICA) sessions > from Worx Home, Safari, or other third-party apps.

New look

The Citrix Receiver icon and background images have been updated to match other Citrix Receiver clients.

X1 Mouse on Citrix Receiver "Ribbon" menu

X1 mouse can be used to pull down the ribbon menu and for selecting options.

Reset Receiver

Clears all user configurations and resets Citrix Receiver to the default settings. This includes associated client certificates.

> **Important**
>
> Citrix Receiver 7.1 is not supported on Apple devices running iOS 7.x

What's new in 7.0.2

Citrix X1 Mouse enhancements

Bluetooth/virtual keyboard and X1 Mouse enhanced to support CTRL+click and SHIFT+click combinations.

Mouse cursor enhancements

X1 Mouse cursor enhanced to support standard Windows mouse cursors.

What's new in 7.0.1

Citrix Receiver 7.0.1 for iOS is a maintenance release that resolves a number of issues.

What's new in 7.0

Session Reliability

This new feature keeps a session active when network connectivity is interrupted.

IPv6 support

Citrix Receiver 7.0 for iOS introduces support for IPv6. This move from IPv4 to IPv6 supports the following scenarios:

- IPv6 end-to-end communication direct to StoreFront
- IPv6 client with IPv4 backend (mixed mode)

HDX SDK

This release provides a software development kit (SDK) that enables customers, independent software vendors (ISVs) and other partners to launch a XenApp or XenDesktop session from within their own native mobile app, without having Citrix Receiver installed on their iOS device. It adds the HDX engine to your enterprise mobile apps, giving them the ability to launch ICA files and support the full HDX user experience. For more information, refer to the HDX SDK blog.

Additional language support

Citrix Receiver 7.0 for iOS provides support for the following languages:

- Portuguese
- Dutch
- Italian
- Swedish
- Danish

> **Important**
>
> Users that have invalid certificates that were successfully connecting previously with Receiver 6.1.5 for iOS and prior will no longer be able to connect when they move to the 7.0 version. For more information, refer to the Citrix Support Knowledge Center.

Fixed issues

October 9, 2018

Fixed issues in 7.5.6

This release also addresses a number of issues that help to improve overall performance and stability.

Fixed issues in 7.5.5

- Apps published on Linux VDAs launch with a gray screen and the session stays active for a few seconds, then closes without displaying any error message. [RFIOS-2665]

Fixed issues in 7.5.4

- The reauthentication prompt might not appear after NetScaler times out during a session. [RFIOS-1469]
- The XenDesktop session might not log off even when you log off manually. [RFIOS-2575]
- The Location Access prompt might appear multiple times during a session. [RFIOS-2576]
- Location access might not be available after upgrading to Citrix Receiver 7.5.3 for iOS. [RFIOS-2578]
- Menus might not appear correctly when using a published application. [RFIOS-2579]
- Sessions might take longer than expected to disconnect when session reliability and ADT are disabled. [RFIOS-2587]

Fixed issues in 7.5.3

- The Auto-fit Screen option might not work correctly on a desktop VDA when using an iPhone X. [RFIOS-2295]

Fixed issues in 7.5.2

- Citrix Receiver for iOS becomes unresponsive after you delete the installed root certificate and then attempt to delete the account. [RFIOS-286]
- When using a smart card on a device running iOS 11, the following error message might appear: "Your smart card does not have a valid certificate." [RFIOS-2039]
- Citrix Receiver for iOS might perform poorly when both session reliability and adaptive transport are disabled. [RFIOS-2464]

Fixed issues in 7.5.1

- Session reliability is unavailable after resetting Citrix Receiver for iOS and tapping **Allow EDT** In the Advanced Settings menu. [RFIOS-2278]
- The extended keyboard options icon does not appear on the virtual keyboard when using an iPhone. [RFIOS-2282]
- Citrix Receiver for iOS might exit unexpectedly when undoing text that contains a blank space. [RFIOS-2285]
- Citrix Receiver for iOS might exit unexpectedly after removing a favorite app on an iPad and then removing the same app on an iPhone with the same account. [RFIOS-2305]
- The Cancel button might disappear on certain screens when adding a store. [RFIOS-2358]
- After waking an iPad, Citrix Receiver for iOS displays an Access Gateway error and becomes unresponsive. [RFIOS-2379]
- Citrix Receiver for iOS might cause high server CPU usage. [RFIOS-2388]
- Sessions might not redraw correctly when you change the session resolution. [RFIOS-2390]

Fixed issues in 7.5

- When connecting to a session using session roaming, Citrix Receiver for iOS exits unexpectedly. [RFIOS-1947]
- The Auto-fit Screen option in Display Settings might not work correctly on an iPhone. [RFIOS-2049]
- The .h264 codec might cause Citrix Receiver for iOS to exit unexpectedly when using an external display. [RFIOS-2224]
- The .h264 codec might cause Citrix Receiver for iOS to exit unexpectedly when launching a session. [RFIOS-2225]

- Citrix Receiver for iOS might exit unexpectedly on certain Thinwire setups. [RFIOS-2250]

Fixed issues in 7.4

- This fix adds overall stability improvements. [RFIOS-2071]
- Tapping the search icon might not make the virtual keyboard appear. [RFIOS-2154]

Fixed issues in 7.3.1

- After updating to 7.2.3, using the keyboard during two-factor authentication might not work. [LC8267]
- When connected to NetScaler, using an email account to set up a Store might fail. [LC8268]
- URLs with an ending backslash might cause an authentication error. [LC8364]

Fixed issues in 7.3

- When selecting more than one cell in Microsoft Excel 2010 and attempting to copy and paste the data, only the text copies over, not any cell formatting. [RFIOS-1781]
- When copying text from the iOS Notes application to an ICA session on a device running iOS 10.3.1, the text copies as HTML text rather than plain text. [RFIOS-1782]
- After Citrix Receiver for iOS disconnects, the error "HdxSdkErrorDomain_Session error 8" might appear and users are unable to launch any applications. [RFIOS-1826]

Fixed issues in 7.2.5

- This fix addresses an issue that prevents customer ratings of Citrix Receiver for iOS in Apple's App Store.

Fixed issues in 7.2.4

- With two-factor authentication enabled, the logon window might move off the screen when attempting to log on. [RFIOS-1850]

Fixed issues in 7.2.2

- The viewer resolution might expand to 100% when you close all the applications on the desktop. [RFIOS-1613]
- XenDesktop sessions might not resume after waking an iOS device from Sleep mode. [RFIOS-1746]
- On an iPad Pro (12.9-inch model), pressing the Tab key to switch input fields in a form might make the keyboard disappear. [RFIOS-1749]

Fixed issues in 7.2

- If the session disconnects while a video is playing, the video might not resume when the session reconnects. [RFIOS-295]
- When using Citrix Receiver for iOS 7.1, users might not be able to connect to published applications. [RFIOS-320]
- Citrix Receiver might exit unexpectedly if .jpg images appear in a session. [RFIOS-333]
- Connecting to an ICA desktop session from an iOS device over ICA Proxy through NetScaler Gateway might work even when the remote gateway's certificates are not installed on the iOS device. [RFIOS-348]
- Citrix Receiver might not connect when the Proxy certification dialog displays. [RFIOS-361]
- The Citrix X1 Mouse might not perform the pinch and zoom function correctly. [RFIOS-491]
- NetScaler might not work as intended when enabling Framehawk. [RFIOS-1492]
- If a user attempts to delete an app or user-added Favorite after logging out of Citrix Receiver, an error occurs. [RFIOS-1489]
- After adding applications to Favorites on a device running iOS 10, Citrix Receiver might exit unexpectedly after rotating the device. [RFIOS-1494]
- If a session starts in mixed IPV6-IPV4 mode, Citrix Receiver might exit unexpectedly. [RFIOS-1499]
- Sessions might disconnect ahead of the configured session timeout if Citrix Receiver for iOS is running in background or the device is locked.

Fixed issues in 7.1.2

- Moving the Citrix X1 mouse causes the Japanese phrase list in the virtual keyboard to disappear after inputting Japanese characters into Outlook. [658983]

- Connecting via Squid proxy server fails to launch published applications or desktops. [651489]
- The wireless trackpad feature does not work on devices with iOS 10 installed. [660963]

Fixed issues in 7.1

- The desktop session displays at a lower resolution than the original session. [653768]

Fixed issues in 7.0.2

- This release resolves a previously reported issue that occurs when an iOS device enters low power mode; as a result, an active session disconnects and an error message (labeled Error 51) appears.
- The keyboard fails to render Japanese characters properly within a session.
- When using the IME keyboard, a performance issue might occasionally appear.

Fixed issues in 7.0.1

- This release resolves an issue when using Citrix Receiver 7.0 for iOS on iOS version 7.x; in some instances, Citrix Receiver may exit unexpectedly. Refer to the Citrix Support Knowledge Center for more information about this issue.
- When an iOS device wakes from sleep, an error message (labeled 'Error 51') may appear if an HDX session was active before the device entered sleep mode.

Known issues

October 9, 2018

Known issues in 7.5.6

No new issues have been observed in this release.

Known issues in 7.5.5

No new issues have been observed in this release.

Known issues in 7.5.4

No new issues have been observed in this release.

Known issues in 7.5.3

No new issues have been observed in this release.

Known issues in 7.5.2

No new issues have been observed in this release.

Known issues in 7.5.1

The following issues have been identified in this release:

- The Windows 7 VDA does not fit the screen when you select Auto-fit Screen on an iPhone X. [RFIOS-2295]
- The keyboard on the iPhone X might shift to the right in Landscape mode, making some buttons unusable. [RFIOS-2451]

Known issues in 7.5

The following issue has been identified in this release:

- When using a smart card, stores might not enumerate correctly when connecting through NetScaler 11.1 56.15.nc. For information on a workaround, see Knowledge Center article CTX231643. [RFIOS-2316]

Known issues in 7.3

The following issue has been identified in this release:

- Smart card authentication might not work on iOS 11 devices. This issue is specific to iOS 11 and there is no workaround. [RFIOS-1810]

Known issues in 7.2.2

The following issues have been identified in this release:

- In Presentation mode, the Citrix X1 Mouse might not open the hidden icons menu in the Windows taskbar. As a workaround, manually disable the keyboard in the Citrix Receiver toolbar. [RFIOS-1759]
- When using a Windows 10 desktop, tapping the touchscreen might not work on an iPad Pro (12.9-inch model) using the Custom Resolution Autofit High setting. As a workaround, use an external mouse or the virtual mouse in the Citrix Receiver toolbar. [RFIOS-1766]

Known issues in 7.1

The following issue has been identified in this release:

- Applications disabled on the Delivery Controller still appear as available on the Apps list. [654514]

Known issues in 7.0.2

The following issues have been identified in this release:

- In some cases, the Apps screen appears black after searching, switching between Favorites/Settings (and back to Apps), and then canceling search results. To resolve this issue, tap Favorites and then Apps to refresh the session screen. [649485]
- In some scenarios, attempts to connect via a Squid proxy server would fail resulting in desktop or published app launches to fail. To resolve this issue disable “Enable HTTP Proxy” from Receiver (Advanced) Settings. [651489]

Known issues in 7.0.1

The following issue has been identified at this release:

- When launching a second app or a desktop from a different server, or when not using the session sharing feature, users may encounter an error message (labeled ‘Error 51’).

Known issues in 7.0

The following issues have been identified in this release:

- On iOS versions 7.x and older, Citrix Receiver may exit unexpectedly when upgrading to Citrix Receiver 7.0 for iOS. Impacted users may either upgrade to iOS 9 or, if not possible due to the device, revert to the R1 version of the app. This version of Citrix Receiver is the 6.1.4 version of Citrix Receiver and is supported for fallback cases only. Search the App Store for "Citrix R1" to install. This version of Citrix Receiver will be a separate install from the current version already installed on the device.
- In some cases, a user may be unable to launch a session when NetScaler is setup to accept LDAP and Cert Policy while the client certificate option is set to Optional (under SSL parameters in the virtual gateway), and the user wants to use LDAP. To resolve this issue, as a NetScaler administrator, create a second virtual gateway and set it to use LDAP as the sole authentication method or mandate client certificates. [594045]
- In some instances, a X1 mouse may experience problems (for example, zooming or pinching) when used with Microsoft Paint that was launched from an iPhone. [590293]
- When playing a video in an active session, bringing up the keyboard from the session toolbar may result in choppy video and audio performance. [622430]
- When an active session encounters a network interruption (for example, loss of a wireless access point), Citrix Receiver fails to display an error message indicating the cause of the disruption; the session reverts back to the Favorites screen. [637957]
- A session may display an error message indicating that an account cannot be added when you attempt to add a StoreFront account directly using a smart card. [639441]
- Audio and video synchronization may fail after disconnecting and reconnecting a network connection. [641012]

System requirements

December 16, 2018

Device requirements

- Citrix Receiver 7.3 and later for iOS supports iOS 9, 10, and 11.
- Citrix Receiver 7.2.4 to 7.2.5 for iOS supports iOS 9 and 10.
- Citrix Receiver 7.1 to 7.2.3 for iOS supports iOS 8, 9, and 10.
- Citrix Receiver 7.0 to 7.0.2 for iOS supports iOS 7, 8, and 9.
- This software update has been validated on the following devices:

  - iPhone 5x models, iPhone 6x models, iPhone 7x models, iPhone 8x models, and iPhone X models, including Plus models.
  - All iPad models (including iPad Pro) except for iPad 1 and iPad 2 which are not supported.
- External display support
  - iPhone - as supported by iOS.
  - iPad - as supported by iOS (does not use the whole screen).

Server requirements

Ensure you install all the latest hotfixes for your servers.

- For connections to virtual desktops and apps, Citrix Receiver supports Citrix StoreFront and Web Interface.

  StoreFront:

  - StoreFront 3.6 or later (recommended). Citrix Receiver 7 for iOS has been validated with the latest version of StoreFront; previous supported versions include StoreFront 2.6 or later.

    Provides direct access to StoreFront stores. Citrix Receiver also supports prior versions of StoreFront.

    Note: With XenApp and XenDesktop 7.8, Citrix introduced support for the Framehawk virtual channel and 3D Pro. This functionality was extended to Citrix Receiver for iOS. For more information, see the XenApp and XenDesktop documentation.

  - StoreFront configured with a Receiver for Web site

    Provides access to StoreFront stores from a Safari web browser. Users must manually open the ICA file using the browser Open in Receiver function. For the limitations of this deployment, see the StoreFront documentation.

  Web Interface:

  - Web Interface 5.4 with Web Interface sites
  - Web Interface 5.4 with XenApp Services sites
  - Web Interface on NetScaler (browser-based access only using Safari)

    You must enable the rewrite policies provided by NetScaler.

- **XenDesktop** and **XenApp** (any of the following products):
  - Citrix XenDesktop 7.x
  - Citrix XenApp 7.5 or later
  - Citrix XenApp 6.5 for Windows Server 2008 R2

Connectivity and authentication

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

	Receiver for Web using browsers	StoreFront Services site (native)	StoreFront XenApp Services site (native)	NetScaler to Receiver for Web (browser)	NetScaler to StoreFront Services site (native)
Anonymous	Yes	Yes			
Domain	Yes	Yes	Yes	Yes*	Yes*
Domain pass-through	Yes	Yes	Yes		
Security token				Yes*	Yes*
Two-factor authentication (domain with security token)				Yes*	Yes*
SMS				Yes*	No
Smart card		Yes		Yes*	Yes*
User certificate				Yes (NetScaler Gateway plug-in)	Yes (NetScaler Gateway plug-in)

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

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

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

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

About secure connections and certificates

Private (self-signed) certificates

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

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

Import root certificates on iPad and iPhone devices

Obtain the root certificate of the certificate issuer and email it to an email 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 iOS supports wildcard certificates.

Intermediate certificates and the NetScaler Gateway

When your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the NetScaler Gateway (or Access Gateway) server certificate. Also, for Access Gateway installations, see the Knowledge Base article that matches your edition:

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

See also:

CTX124937: How to Configure Citrix Access Gateway Enterprise Edition for Use with Citrix Receiver for Mobile Devices

RSA SecurID authentication is supported for Secure Gateway configurations (through the Web Interface only) and all supported Access Gateway configurations.

Citrix Receiver supports all authentication methods supported by Access Gateway.

Smart cards

Citrix Receiver 7 for iOS provides support for SITHS smart cards for in-session connections only.

If you are using FIPS NetScaler devices, configure your systems to deny SSL renegotiations. For details, see How to configure the -denySSLReneg parameter.

The following products and configurations are supported:

- Supported readers:
  - Precise Biometrics Tactivo for iPad Mini Firmware version 3.8.0
  - Precise Biometrics Tactivo for iPad (4th generation) and Tactivo for iPad (3rd generation) and iPad 2 Firmware version 3.8.0
  - BaiMobile® 301MP and 301MP-L Smart Card Readers
    Supported VDA Smart Card Middleware
  - ActiveIdentity
- Supported smartcards:
  - PIV cards
  - Common Access Card (CAC)
- Supported configurations:
  - Smart card authentication to NetScaler Gateway with StoreFront 2.x and XenDesktop 7.x or later or XenApp 6.5 or later

Deploy

December 16, 2018

Provide access information to end users for iOS devices

You must provide users with the Citrix Receiver account information they need to access their hosted their applications, desktops, and data. You can provide this information by:

- Configuring email-based account discovery
- Providing users with a provisioning file
- Providing users with account information to enter manually

Configure email-based account discovery

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

> **Note:**
>
> Email-based account discovery is not supported if Citrix Receiver is connecting to a Web Interface deployment.

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, users simply open the .cr file on the device to configure Citrix Receiver. If you configure Receiver for Web sites, users can also obtain Citrix Receiver provisioning files from those sites.

For more information, see the StoreFront documentation.

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 StoreFront URL or XenApp Services site hosting resources; for example: servername.company.com.
- For access using NetScaler Gateway, provide the NetScaler Gateway address 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, Citrix Receiver attempts to verify the connection. If successful, Citrix Receiver prompts the user to log on to the account.

Session sharing

When users log off from a Citrix Receiver account, if there are still connections to applications or desktops, they have the option to disconnect or log off:

- **Disconnect**: Logs off from the account, but leaves the Windows application or desktop running on the server, and the user can then start another device, launch Citrix Receiver, and reconnect to the last state before disconnecting from the iOS device. This option allows users to reconnect from one device to another device and resume working in running applications.
- **Log off**: Logs off from the account, closes the Windows application, and logs off from the XenApp or XenDesktop server. This option allows users to disconnect from the server and log off the account; when they launch Citrix Receiver again, it opens in the default state.

Provide RSA SecurID authentication for iOS devices

RSA SecurID authentication for Citrix Receiver is supported for Secure Gateway configurations (through the Web Interface only) and all NetScaler Gateway configurations.

URL scheme required for the software token on Citrix Receiver: The RSA SecurID software token used by Citrix Receiver registers the URL scheme com.citrix.securid only.

If users have installed both the Citrix Receiver app and the RSA SecurID app on their iOS device, users must select the URL scheme “com.citrix.securid” to import the RSA SecurID Software Authenticator (software token) to Citrix Receiver on their devices.

To import an RSA SecurID soft token into Citrix Receiver

To use an RSA Soft Token with the Citrix Receiver, have your users follow this procedure.

The policy for PIN length, type of PIN (numeric only, alphanumeric), and limits on PIN reuse are specified on the RSA administration server.

Your users should only need to do this once, after they have successfully authenticated to the RSA server. After your users verify their PINs, they are are also authenticated with the StoreFront server, and it presents available, published applications and desktops.

To use an RSA soft token with Citrix Receiver

1. Import the RSA soft token provided to you by your organization.
2. From the email with your SecurID file attached, select **Open in Receiver** as the import destination. After the soft token is imported, Citrix Receiver opens automatically.
3. If your organization provided a password to complete the import, enter the password provided to you by your organization and click **OK**. After clicking **OK**, you will see a message that the token was successfully imported.
4. Close the import message, and in Citrix Receiver, click the **Add Account**.
5. Enter the URL for the Store provided by your organization and click **Next.**
6. On the Log On screen, enter your credentials: user name, password, and domain. For the Pin field, enter **0000**, unless your organization has provided you with a different default PIN. (The PIN 0000 is an RSA default, but your organization may have changed it to comply with their security policies.)
7. At the top left, click **Log On**. After you click **Log On**, you are prompted to create a new PIN.
8. Enter a PIN from 4 to 8 digits and click **OK**.
9. You are then prompted to verify your new PIN. Re-enter your PIN and click **OK**. After clicking OK, you will be able to access your apps and desktops.

Support for Next Token Mode

If you configure NetScaler Gateway for RSA SecurID authentication, Citrix Receiver supports Next Token Mode. With this feature enabled, if a user enters three (by default) incorrect passwords, the NetScaler Gateway plug-in prompts the user to wait until the next token is active before logging on. The RSA server can be configured to disable a user's account if a user logs on too many times with an incorrect password.

Save Passwords

Using the Citrix Web Interface Management console, you can configure the XenApp authentication method to allow users to save their passwords. When you configure the user account, the encrypted password is saved until the first time the user connects. Consider the following:

- If you enable password saving, Citrix Receiver stores the password on the device for future logons and does not prompt for passwords when users connect to applications.

> **Note:**
>
> The password is stored only if users enter a password when creating an account. If no password is entered for the account, no password is saved, regardless of the server setting.

- If you disable password saving (default setting), Citrix Receiver prompts users to enter passwords every time they connect.

> **Note:**
>
> For StoreFront direct connections, password saving is not available.

To override password saving

If you configure the server to save passwords, users who prefer to require passwords at logon can override password saving:

- When creating the account, leave the password field blank.
- When editing an account, delete the password and save the account.

Using the Save Password feature

Beginning with release 6.1.2, Citrix Receiver introduced a feature that streamlines the connection process by allowing you to save your password, which eliminates the extra step of having to authenticate a session everytime you open Citrix Receiver.

> **Note:**
>
> The save password functionality currently works with the PNA protocol. It does not work with StoreFront *native* mode; however, this functionality works when StoreFront enables PNA *legacy* mode.

Configuring StoreFront PNA legacy mode

To configure StoreFront PNA legacy mode to enable the save password functionality:

1. If you are configuring an existing Store, go to step 3.
2. To configure a new StoreFront deployment, follow the best practices described in Install, setup, and uninstall Citrix StoreFront.
3. Open the Citrix StoreFront management console. Ensure the base URL uses HTTPS and is the same as the common name specified when generating your SSL certificate.

4. Select the Store you want to configure.
5. Click **Configure XenApp Service Support**.
6. Enable **Legacy Support**, and Click **OK**.
7. Navigate to the template configuration file located at c:\\inetpub\wwwroot\Citrix\<store name>\Views\PnaConfig\.
8. Make a backup of Config.aspx.
9. Open the original Config.aspx file.
10. Edit the line <EnableSavePassword>**false**</EnableSavePassword> to change the **false** value to **true**.
11. Save the edited Config.aspx file.
12. On the StoreFront server, run PowerShell with administrative rights.
13. In the PowerShell console:

    a. cd "c:\\Program Files\Citrix\Receiver StoreFront\Scripts"

    b. Type "Set-ExecutionPolicy RemoteSigned"

    c. Type ".\\ImportModules.ps1"

    d. Type "Set-DSDerviceMonitorFeature –ServiceUrl `https://localhost:443/StorefrontMonitor`

14. If you have a StoreFront group, run the same commands on all the members in the group.

Configuring NetScaler to save passwords

> **Note:**
>
> This configuration uses NetScaler load balance servers.

To configure NetScaler to support the save password functionality:

1. Log in to the NetScaler management console.
2. Follow the Citrix best practices to create a certificate for your load balance virtual server(s).
3. On the configuration tab, navigate to Traffic Management -> Load Balancing -> Servers and click **Add**.
4. Enter the server name and IP address of the StoreFront server.
5. Click **Create**. If you have a StoreFront group, repeat step 5 for all the servers in the group.
6. On the configuration tab, navigate to Traffic Management -> Load Balancing -> Monitor and click **Add**.

7. Enter a name for the monitor. Select **STOREFRONT** as the Type. At the bottom of the page, select **Secure** (this is required since the StoreFront server is using HTTPS).
8. Click the **Special Parameters** Tab. Enter the StoreFront name configured earlier, and select the **Check Backed Services** and click **Create**.
9. On the **Configuration** tab navigate to Traffic Management -> Load Balancing -> Service Groups and click **Add**.
10. Enter a name for your Service Group and set the protocol to **SSL**. Click **Ok**.
11. On the right-hand of the screen under Advanced Settings, select **Settings**.
12. Enable Client IP and enter the following for the Header value: **X-Forwarded-For** and click **OK**.
13. On the right-hand of the screen under Advanced Settings, select **Monitors**. Click the arrow to add new monitors.
14. Click the **Add** button and then select the **Select Monitor** drop down; a list of monitors (those configured on NetScaler) appears.
15. Click the radio button beside the monitor(s) you created earlier and click **Select**, then click **Bind**.
16. On the right-hand of the screen (under Advanced Settings), select **Members**. Click the arrow to add new service group members.
17. Click the **Add** button and then select the **Select Member** drop down.
18. Select the **Server Based** radio button; a list of server members (those configured on NetScaler) appears. Click the radio button beside the StoreFront server(s) you created earlier.
19. Enter 443 for the port number and specify a unique number for the Hash ID, then click **Create**, then click **Done**. If everything has been configured properly, the **Effective State** should show a green light, indicating that monitoring is functioning properly.
20. Navigate to Traffic Management -> Load Balancing -> Virtual Servers and click **Add**. Enter a name for the server and select **SSL** as the protocol.
21. Enter the IP address for the StoreFront load-balanced server and click **OK**.
22. Select the **Load Balancing Virtual Server Service Group** binding, click the arrow then add the Service Group created previously. Click **OK** twice.
23. Assign the SSL certificate created for the Load Balance virtual server. Select **No Server Certificate**.
24. Select the Load Balance server certificate from the list and click **Bind**.
25. Add the domain certificate to the Load Balance Server. Click **No CA certificate**.
26. Select the domain certificate and click **Bind**.
27. On the right side of the screen, select **Persistence**.

28. Change the Persistence to **SOURCEIP** and set the time out to **20**. Click **Save,** then click **Done**.
29. On your domain DNS server, add the load balance server (if not already created).
30. Launch Citrix Receiver on your iOS device and enter the full XenApp URL.

Configuration

December 16, 2018

Configure your environment

Citrix Receiver for iOS supports the configuration of Web Interface for your XenApp deployment. There are two types of Web Interface sites: XenApp Services (formerly Program Neighborhood Services) sites and XenApp and XenDesktop Sites. Web Interface sites enable client devices to connect to the server farm. Authentication between Citrix Receiver and a Web Interface site can be handled using various solutions, including Citrix Access Gateway and Citrix Secure Gateway.

Also, you can configure StoreFront to provide authentication and resource delivery services for Citrix Receiver, enabling you to create centralized enterprise stores to deliver desktops, applications, and other resources to users.

For more information about configuring connections, including videos, blogs, and a support forum, see http://community.citrix.com.

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

- When publishing applications on your farms or sites, consider the following options to enhance the experience for users accessing those applications through StoreFront stores.
  - Ensure that you include meaningful descriptions for published applications because these descriptions are visible to users in Citrix Receiver.
  - You can emphasize published applications for your mobile device users by listing the applications in the Featured list of Citrix Receiver. To populate this list on Citrix Receiver, edit the properties of applications published on your servers and append the KEYWORDS:Featured string to the value of the Application description field.
  - To enable the screen-to-fit mode that adjusts the application to the screen size of mobile devices, edit the properties of applications published on your servers and append the KEYWORDS:mobile string to value of the Application description field. This keyword also activates the auto-scroll feature for the application.

  - To automatically subscribe all users of a store to an application, append the KEYWORDS:Auto string to the description you provide when you publish the application in XenApp. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.

- If the Web Interface of your XenApp or XenDesktop deployment does not have a Web site or XenApp and XenDesktop Site, create one. The name of the site and how you create it depends on the version of the Web Interface you have installed.

Configure StoreFront

Important:

- When using StoreFront, Citrix Receiver supports Citrix Access Gateway Enterprise Edition versions from 9.3, and NetScaler Gateway versions through 12.
- Citrix Receiver for iOS supports only XenApp Services sites on Web Interface.
- Citrix Receiver for iOS supports launching sessions from Receiver for Web, as long as the web browser works with Receiver for Web. If launches do not occur, configure your account through Citrix Receiver for iOS directly. Users must manually open the ICA file using the browser Open in Receiver function. For the limitations of this deployment, see the StoreFront documentation.

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

1. Install and configure StoreFront. For details, see StoreFront in the Technologies > StoreFront section of Product Documentation. For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Receiver for iOS.
2. Configure stores for StoreFront as you would for other XenApp and XenDesktop applications. No special configuration is needed for mobile devices. For details, see User Access Options in the StoreFront section of Product Documentation. For mobile devices, use either of these methods:
   - Provisioning files. You can provide users with provisioning files (.cr) containing connection details for their stores. After installation, users open the file on the device to configure Citrix Receiver automatically. By default, Receiver for Web sites offer users a provisioning file for the single store for which the site is configured. Alternatively, you can use the Citrix StoreFront management console to generate provisioning files for single or multiple stores that you can manually distribute to your users.
   - Manual configuration. You can directly inform users of the Access Gateway or store URLs needed to access their desktops and applications. For connections through Access Gateway, users also need to know the product edition and required authentication method. After installation, users type these details into Citrix Receiver, which attempts to verify the connection and, if successful, prompts users to log on.

- Automatic configuration. Tap **Add Account** on the Welcome screen and type the URL of the StoreFront server in the address field. The configuration of the account happens automatically while the account is added.

To configure Access Gateway and NetScaler Gateway

If you have users who connect from outside the internal network (for example, users who connect from the internet of from remote locations), configure authentication through Access Gateway or NetScaler Gateway.

- When using StoreFront, Citrix Receiver supports Citrix Access Gateway Enterprise Edition versions from 9.3, and NetScaler Gateway versions through 12.
- For details, see your version of Access Gateway or NetScaler Gateway in Product Documentation.

To configure Citrix Receiver to access apps

1. If you want to configure Citrix Receiver to automatically access apps when creating an account, in the Address field, type the matching URL of your store, such as storefront.organization.com.
2. Select the Use Smartcard option when you are using a smart card to authenticate.
3. For manual configuration (accessible by tapping Options>Manual Setup), continue by completing the remaining fields and select the Access Gateway (or NetScaler Gateway) authentication method, such as enabling the security token, selecting the type of authentication, and saving the settings.

> **Note:**
>
> Logons to the store are valid for about one hour. After that time, users must log on again to refresh or launch other applications.

Configure client certificate authentication

Important:

- When using StoreFront, Receiver supports Citrix Access Gateway Enterprise Edition versions from 9.3, and NetScaler Gateway versions through 11.
- Client certificate authentication is supported by Receiver for iOS starting with version 5.5.
- Only Access Gateway Enterprise Edition 9.x and 10.x (and subsequent releases) support client certificate authentication.
- Double-source authentication types must be CERT and LDAP.
- Citrix Receiver also supports optional client certificate authentication.

- Only P12 formatted certificates are supported.

Users logging on to an Access Gateway (or NetScaler Gateway) virtual server can also be authenticated based on the attributes of the client certificate that is presented to the virtual server. Client certificate authentication can also be used with another authentication type, LDAP, to provide double-source authentication.

To authenticate users based on the client-side certificate attributes, client authentication should be enabled on the virtual server and the client certificate should be requested. You must bind a root certificate to the virtual server on Access Gateway.

When users log on to the Access Gateway virtual server, after authentication, the user name and domain information is extracted from the specified field of the certificate. This information must be in the certificate's **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** field. It is in the format "username@domain." If the user name and domain are extracted successfully, and the user provides the other required information (for example, a password), then the user is authenticated. If the user does not provide a valid certificate and credentials, or if the username/domain extraction fails, authentication fails.

You can authenticate users based on the client certificate by setting the default authentication type to use the client certificate. You can also create a certificate action that defines what is to be done during the authentication based on a client SSL certificate.

To configure the XenApp Services site

If you do not already have a XenApp Services site created, in the XenApp console or Web Interface console (depending on the version of XenApp you have installed), create a XenApp Services site for mobile devices.

Citrix Receiver for mobile devices uses a XenApp Services site (formerly Program Neighborhood Agent site) to get information about the applications a user has rights to and presents them to the Receiver running on the device. This is similar to the way you use the Web Interface for traditional SSL-based XenApp connections for which an Access Gateway can be configured.

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

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

To configure the Access Gateway appliance

For client certificate authentication, configure the Access Gateway with two-factor authentication using two authentication policies: Cert and LDAP. For details, refer to your version of the Access Gateway Enterprise Edition (9.x only) or Access Gateway 10 in Product Documentation and search for the topic: Configuring Client Certificate Authentication.

1. Create a session policy on the Access Gateway to allow incoming XenApp connections from the Receiver, and specify the location of your newly created XenApp Services site.
    - Create a session policy to identify that the connection is from the Receiver for mobile devices. As you create the session policy, configure the following expression and choose Match All Expressions as the operator for the expression:
      REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
    - In the associated profile configuration for the session policy, on the Security tab, set Default Authorization to Allow.
      On the Published Applications tab, if this is not a global setting (you selected the Override Global check box), ensure that the ICA Proxy field is set to ON.
      In the Web Interface Address field, type the URL including the config.xml for the XenApp Services site that the device users use, such as //XenAppServerName/Citrix/PNAgent/config.xml or /XenAppServerName/CustomPath/config.xml.
    - Bind the session policy to a virtual server.
    - Create authentication policies for Cert and LDAP.
    - Bind the authentication policies to the virtual server.
    - Configure the virtual server to request client certificates in the TLS handshake (on the Certificate tab, open SSL Parameters, and for Client Authentication, set Client Certificate to Mandatory.
      Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), ensure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway documentation.

To configure the mobile device for Citrix Receiver

If client certificate authentication is enabled on Access Gateway, users are authenticated based on certain attributes of the client certificate. After authentication is completed successfully, the user name and domain are extracted from the certificate and any policies specified for that user are applied.

1. From Citrix Receiver, open the Account, and in the Server field, type the matching FQDN of your Access Gateway server, such as GatewayClientCertificateServer.organization.com. Receiver automatically detects that the client certificate is required.

2. Users can either install a new certificate or choose one from the already installed certificate list. For iOS client certificate authentication, the certificate must be downloaded and installed by the Receiver application only.
3. After selecting a valid certificate, the user name and domain fields on the logon screen is pre-populated using the user name information from the certificate, and a user types the remaining details, including the password.
4. If client certificate authentication is set to optional, users can skip the certificate selection by pressing Back on the certificates page. In this case, Receiver proceeds with the connection and provides the user with the logon screen.
5. After users complete the initial log on, they can start applications without providing the certificate again. Receiver stores the certificate for the account and uses it automatically for future logon requests.

Configure Secure Gateway

To configure the XenApp Services site

Important:

- Secure Gateway 3.x is supported by Receiver for iOS using XenApp Services sites.
- Secure Gateway 3.x is supported by Citrix Receiver for iOS using XenApp Web sites.
- Only single-factor authentication is supported on XenApp Services sites, and both single-factor and dual factor are supported on XenApp Web sites.
- You must use the Web Interface 5.4, which is supported by all built-in browsers.

Before beginning this configuration, install and configure the Secure Gateway to work with Web Interface. You can adapt these instructions to fit your specific environment.

If you are using a Secure Gateway connection, do not configure Citrix Access Gateway settings on the Receiver.

The Receiver for mobile devices uses a XenApp Services site (formerly Program Neighborhood Agent site) to get information about the applications a user has rights to and presents them to the Receiver running on the device. This is similar to the way you use the Web Interface for traditional SSL-based XenApp connections for which an Access Gateway can be configured. XenApp Services sites running on the Web Interface 5. x have this configuration ability built in.

Configure the XenApp Services site to support connections from a Secure Gateway connection:

1. In the XenApp Services site, select Manage secure client access > Edit secure client access settings.
2. Change the Access Method to Gateway Direct.
3. Enter the FQDN of the Secure Gateway.

4. Enter the Secure Ticket Authority (STA) information.

> **Note:**
>
> For the Secure Gateway, Citrix recommends using the Citrix default path for this site (//XenAppServerName/Citrix/PNAgent). The default path enables your users to specify the FQDN of the Secure Gateway they are connecting to instead of the full path to the config.xml file that resides on the XenApp Services site (such as //XenAppServerName/CustomPath/config.xml).

To configure the Secure Gateway

1. On the Secure Gateway, use the Secure Gateway Configuration wizard to configure the Secure Gateway to work with the server in the secure network hosting the XenApp Service site. After selecting the Indirect option, enter the FQDN path of your Secure Gateway Server and continue the wizard steps.
2. Test a connection from a user device to verify that the Secure Gateway is configured correctly for networking and certificate allocation.

To configure the mobile device for the Receiver application

1. When adding a Secure Gateway account, enter the matching FQDN of your Secure Gateway server in the **Address** field:
   - If you created the XenApp Services site using the default path (/Citrix/PNAgent), enter the Secure Gateway FQDN: FQDNofSecureGateway.companyName.com
   - If you customized the path of the XenApp Services site, enter the full path of the config.xml file, such as: FQDNofSecureGateway.companyName.com/CustomPath/config.xml
2. If you are manually configuring the account, then turn off the Access Gateway option in the **New Account** dialog.

Configure Web Interface

To configure the Web Interface site

Users with iPhone and iPad devices can launch applications through your Web Interface site and the built-in Safari browser on the mobile device. Configure the Web Interface site the same as you would for other XenApp applications. If no XenApp Services site is configured for the mobile device, Citrix Receiver automatically uses your Web Interface site. No special configuration is needed for mobile devices.

Web Interface 5.x is supported by the built-in Safari browser.

To launch applications on the iOS device

On the mobile device, users can log on to the Web Interface site using their normal logon and password.

Configure mobile devices automatically

In StoreFront, use the Export Multi-Store Provisioning File and Export Provisioning File tasks to generate files containing connection details for stores, including any NetScaler Gateway deployments and beacons configured for the stores. Make these files available to users to enable them to configure Citrix Receiver automatically with details of the stores. Users can also obtain Citrix Receiver provisioning files from Receiver for Web sites.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile. Select the Stores node in the left pane of the Citrix StoreFront management console.
2. To generate a provisioning file containing details for multiple stores, in the Actions pane, click Export Multi-Store Provisioning File and select the stores to include in the file.
3. Click Export and Save the provisioning file with a .cr extension to a suitable location on your network.

Configure accounts manually

In general, when Receiver connects to an Access Gateway, Receiver attempts to locate a XenApp Services site or XenApp Web site after authenticating. If no site is detected, Receiver displays an error. To avoid this situation, you can configure an account manually so Receiver can connect to the Access Gateway.

1. Tap the Accounts icon in the upper right corner and then in the Accounts screen, tap the Plus Sign (+). The New Account screen appears.
2. In the lower left corner of the screen, tap the icon to the left of Options and tap Manual setup. Additional fields appear on the screen.
3. In the Address field, type the secure URL of the site or Access Gateway to which you want to connect (for example, agee.mycompany.com).
4. Select one of the following connection options. The remaining fields on the screen change, depending on your selection.

- Web Interface - Select for Receiver to display a XenApp Web site similar to a Web browser. This is also known as Web View.
- XenApp Services - Select for Receiver to locate a specific XenApp Services site for which authentication through Access Gateway is not configured. In the additional options that appear on this screen, provide site logon credentials.
  - <StoreFront FQDN>: If there are multiple stores, a list will be presented and the user can choose the store to add.
  - <StoreFront FQDN>/citrix/<Store Name>: This will add the StoreFront store <Store Name>.
  - <StoreFront FQDN>/citrix/PnAgent/config.xml: This will add the default legacy PNAgent store.
  - <StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml: This will add the legacy PNAgent store associated with <Store Name>.
- Access Gateway - Select for Receiver to connect to a XenApp Services site through a specific Access Gateway. In the additional options on this screen, select the server edition and its logon credentials, including whether it requires a security token for authentication.

5. For certificate security, use the setting in the Ignore certificate warnings field to determine whether you want to connect to the server even if it has an invalid, self-signed, or expired certificate. The default setting is OFF.
   Important: If you do enable this option, make sure you are connecting to the correct server. Citrix strongly recommends that all servers have a valid certificate to protect user devices from online security attacks. A secure server uses an SSL certificate issued from a certificate authority. Citrix does not support self-signed certificates and does not recommend by-passing the certificate security.
6. Tap Save.
7. Type your user name and password (or token, if you selected two-factor authentication), and then tap Log On. The Citrix Receiver screen appears, in which you can access your desktops and add and open your apps.

Troubleshoot

January 3, 2019

Disconnected sessions

Users can disconnect (but not log off) from a Citrix Receiver session in the following ways:

- While viewing a published app or desktop in session:

  - tap the arrow at the top of the screen to expose the in-session drop down menu.
  - tap the **Home** button to return to the launch pad.
  - notice the white shadow under the icon of one of the published apps that are still in an active session; tap the icon.
  - tap disconnect.
- Close Citrix Receiver:
  - double tap the device's **Home** button.
  - locate Receiver in the iOS app switcher view.
  - tap disconnect in the dialog that appears.
- Pressing the home button on their mobile device.
- Tapping Home or Switch in the app's drop-down menu.

The session remains in a disconnected state. Although the user can reconnect at a later time, you can ensure disconnected sessions are rendered inactive after a specific interval. To do this, configure a session timeout for the ICA-tcp connection in Remote Desktop Session Host Configuration (formerly known as "Terminal Services Configuration"). For more information about configuring Remote Desktop Services (formerly known as "Terminal Services"), refer to the Microsoft Windows Server product documentation.

Issues with numeric keys in applications

If users have issues with numeric keys not working correctly in published applications, they can try disabling the Unicode keyboard in Citrix Receiver. To do this, from the Settings tab, tap **Keyboard Options**, and for Use Unicode Keyboard, toggle the switch to **Off**.

Loss of HDX audio quality from XenDesktop

From XenDesktop, HDX audio to Citrix Receiver for iOS might lose quality when using audio plus video. This issue occurs when the XenDesktop HDX policies cannot handle the amount of audio data with the video data. For suggestions about how to create policies to improve audio quality, see Knowledge Center article CTX123543.

Demonstration accounts available from the Citrix Cloud

Users who do not currently have an account can create a demonstration user account at the Citrix Cloud demo site at http://cloud.citrix.com/.

The Citrix Cloud offers users the ability to experience the power of Citrix solutions without having to set up and configure their own environment. The Citrix Cloud demo environment uses a number of key Citrix solutions including XenServer, XenApp, NetScaler, and Access Gateway.

However, in this demo environment, data is not saved, and when you disconnect, you might not get able to get back to your session.

Expired passwords

Citrix Receiver supports the ability for users to change their expired passwords. Prompts appear for users to enter the required information.

Slow connections

If you experience slow connections to the XenApp Services site, or issues such as missing application icons or "Protocol Driver Error" messages, as a workaround, on the XenApp server and Citrix Secure Gateway or Web Interface server, disable the following Citrix PV Ethernet Adapter Properties for the network interface (all enabled by default):

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

No server restart is needed. This workaround applies to Windows Server 2003 and 2008 32-bit. Windows Server 2008 R2 is not affected by this issue.

Applications might open in different sessions

This server-side issue can occur even when application sharing is enabled. This is an intermittent issue, and there is no workaround.

App Switcher not working

Apps must be published by the IT administrator on the same server. Otherwise, app switching will not work.

Blocking jailbroken devices from running applications from StoreFront

Your users can compromise the security of your deployment by connecting with jailbroken iOS devices. Jailbroken devices are those whose owners have modified them, usually with the effect of bypassing certain security protections.

When Citrix Receiver detects a jailbroken iOS device, Citrix Receiver displays an alert to the user. To further help to secure your environment, you can configure StoreFront or Web Interface to help to prevent detected jailbroken devices from running apps.

Requirements

- Citrix Receiver for iOS 6.1 or later
- StoreFront 3.0 or Web Interface 5.4 or later
- Access to StoreFront or Web Interface through an administrator account

To help to prevent detected jailbroken devices from running apps

1. Log onto your StoreFront or Web Interface server as a user who has administrator privileges.
2. Find the file default.ica, which is in one of the following locations:
    - **C:\inetpub\wwwroot\Citrix***storename***conf** (Microsoft Internet Information Services)
    - **C:\inetpub\wwwroot\Citrix***storename***App_Data** (Microsoft Internet Information Services)
    - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)
3. Under the section **[Application]**, add the following: **AllowJailBrokenDevices=OFF**
4. Save the file and restart your StoreFront or Web Interface server.

After you restart the StoreFront server, users who see the alert about jailbroken devices cannot launch apps from your StoreFront or Web Interface server.

To allow detected jailbroken devices to run apps

If you do not set AllowJailBrokenDevices, the default is to display the alert to users of jailbroken devices but still allow them to launch applications.

If you want to specifically allow your users to run applications on jailbroken devices:

1. Log onto your StoreFront or Web Interface server as a user who has administrator privileges.
2. Find the file default.ica, which is in one of the following locations:
    - **C:\inetpub\wwwroot\Citrix***storename***conf** (Microsoft Internet Information Services)
    - **C:\inetpub\wwwroot\Citrix***storename***App_Data** (Microsoft Internet Information Services)
    - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)
3. Under the section **[Application]** add the following: **AllowJailBrokenDevices=ON**

4. Save the file and restart your StoreFront or Web Interface server.

When you set AllowJailBrokenDevices to ON, your users see the alert about using a jailbroken device, but they can run applications through StoreFront or Web Interface.

Securing Citrix Receiver for iOS communications

To secure the communication between your server farm and Citrix Receiver for iOS, you can integrate your connections to the server farm with a range of security technologies, including Citrix NetScaler Gateway.

> **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 iOS 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 iOS 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 iOS.

> **Note:**
>
> If the remote gateway's certificate cannot be verified upon connection (because the root certificate is not included in the iOS 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 Citrix Receiver for iOS 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 iOS 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

Releases of Citrix Receiver for iOS 7.5 and later introduce a new, stricter, validation policy for server certificates.

> **Important**
>
> Before installing Citrix Receiver for iOS, 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 iOS now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous releases, Citrix Receiver for iOS 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 iOS connections 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 iOS:

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

Then, Citrix Receiver for iOS will check that all these certificates are valid. Citrix Receiver for iOS will also check that it already trusts "Example Root Certificate". If Citrix Receiver for iOS 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:**

Then, Citrix Receiver for iOS 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 iOS needs, but also allows Citrix Receiver for iOS 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 iOS 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 Citrix Receiver for iOS 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 iOS 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 certificates 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.

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

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

If the Secure Gateway Proxy is installed on a server in the secure network, you can use the Secure Gateway Proxy in Relay mode. If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure Citrix Receiver for iOS 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 iOS and servers. Citrix Receiver for iOS supports both SOCKS and secure proxy protocols.

When communicating with the XenApp or XenDesktop server, Citrix Receiver for iOS uses proxy server settings that are configured remotely on the Web Interface server.

When communicating with the Web server, Citrix Receiver for iOS 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 iOS 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 iOS. Citrix Receiver for iOS then connects to the server using the external address and port number.

Connecting using TLS

Citrix Receiver for iOS 7.2.2 and later 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 iOS running on iOS 9 and later 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 iOS supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

> **Note:**
>
> Citrix Receiver for iOS uses platform (iOS) crypto for connections between Citrix Receiver for iOS and StoreFront.

Configuring and enabling Citrix Receiver for iOS 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 iOS and XenApp or XenDesktop, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate.

iOS comes with about 100 commercial root certificates preinstalled, but if you want to use a different 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 iOS keychain.

To add a root certificate to the keychain

1. Send yourself an email with the certificate file.
2. Open the certificate file on the device. This automatically starts the Keychain Access application.
3. Follow the prompts to add the certificate.

4. Starting with iOS 10, verify that the certificate is trusted by going to iOS Settings > About > Certificate Trust Setting. Under Certificate Trust Settings, see the section “ENABLE FULL TRUST FOR ROOT CERTIFICATES.” Make sure that your certificate has been selected for full trust.

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

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States