CITRIX

Citrix Receiver for Android 3.13

Contents

What's new 3

Fixed issues 7

Known issues 9

Third party notices 11

System requirements 11

Deploy 14

Configuration 17

Enabling Citrix Ready workspace hub 23

Troubleshooting 27

SDK and API 30

What's new

January 10, 2019

What's new in 3.13.9

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

What's new in 3.13.8

File type association support for StoreFront

When you publish applications, you associate them with certain file types present on the server. By doing so, you are redirecting the content from the user device to the server. Devices running Receiver for Android open files of an associated type with a specific published application. For example, when users double-click an email attachment, the attachment opens in the associated application.

For more information, see Accessing files using file type association.

Support to pin on Chromebook

Shortcuts to your favorite apps and desktops are automatically available from the Chrome App Launcher after you add your account to Citrix Receiver for Android running on a Chromebook – not only when you're connecting to StoreFront, but also to XenApp Services Sites (formerly known as PNA accounts).

> **Note:**
>
> This feature is not supported on Web Interface.

What's new in 3.13.7

NetScaler Compatibility Mode

The option **NetScaler Compatibility Mode** is available to address the TLS handshake failure or 41E Error code 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 3.13.6

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

What's new in 3.13.5

Add favorite apps and desktops to Chrome Launcher

After adding your account to Citrix Receiver for Android running on a Chromebook, all your favorite apps and desktops are automatically added to the Chrome Launcher for quick access.

HTTPS support for Citrix Ready workspace hub

HTTPS connections are now supported between Citrix Receiver for Android and Citrix Ready workspace hub.

What's new in 3.13.4

Support for Citrix Ready workspace hub

Built on the Raspberry Pi 3 platform, the Citrix Ready workspace hub provides a secure connection to authorized apps and data. Citrix Receiver for Android supports user authentication to Citrix Ready workspace hubs as an experimental feature.

With this release, Citrix Receiver for Android supports Citrix Casting. Citrix Casting makes it possible for users to securely and seamlessly move virtual app and desktop sessions from a mobile device to a Citrix Ready workspace hub using session roaming and wireless docking. Session roaming enables your phone to authenticate to a Citrix Ready workspace hub and securely roam the user session to the workspace hub. Wireless docking allows users to interact with their phone and cast any app or desktop session to any workspace hub around them.

Dynamic permissions

Previously, Citrix Receiver for Android was asking for all permissions during installation. With this release, running on Android 6.x devices and later, Citrix Receiver dynamically prompts for permissions when needed for SD card access, location, and phone access.

Edit gateways and authentication types

Users can now edit the preferred gateway and the authentication type after adding an account.

> **Note:**
>
> Citrix Receiver populates all authentication types published by StoreFront. Users have to contact their administrator to get the supported authentication types for the selected gateway.

What's new in 3.13.3

Session launch with untrusted certificate

In response to popular request, users can now launch sessions with an untrusted certificate.

> **Note:**
>
> Accepting an untrusted certificate is a risk. Administrators should push trusted certificates by other means (email, download links, existing MDM, etc.) if possible.

Simplified log on

After logging on for the first time, Citrix Receiver for Android autopopulates the user name and domain fields on the logon screen for easier log on.

QR codes for Workspace hub

Citrix Receiver for Android now detects Workspace hub using QR codes.

What's new in 3.13.2

Keyboard layout synchronization

Starting with this release, Citrix Receiver for Android provides dynamic synchronization of the keyboard layout from the client to the VDA in a session. This enables users to switch among preferred keyboard layouts on the client device, providing a consistent user experience when, for example, switching the keyboard layout from English to Spanish. When users switch layouts, they briefly see a message while the synchronization is in progress. They can then continue working with the new keyboard layout.

> **Note:**
>
> This feature works only on soft keyboards on the device, not external keyboards. The "Use Client IME" checkbox in Setting in Citrix Receiver for Android must be checked to enable this feature.

Use the web interface for logging on

Citrix Receiver for Android 3.13.2 allows users to use a web browser to log on rather than the native UI for certain earlier setups.

What's new in 3.13.1

New UI for Citrix Receiver for Android

The Citrix Receiver for Android user interface (UI) has been redesigned based on the extensive feedback provided by the user community, and in accordance with Google's new Material Design guidelines for Android applications.

Some benefits offered by the new user experience are:

- A more streamlined workflow for all tasks. It's now easier to do things users require so they can be more productive.
- Navigational guidelines to get acquainted with the new UI.
- Feedback support now provided within the app to reach out to Citrix with automatic log collection.
- Android Toasts and Snackbars at various places to help identity the operation status as well as Undo operations.

Support for Citrix Ready workspace hub

Built on the Raspberry Pi 3 platform, the Citrix Ready workspace hub provides a secure connection to authorized apps and data. With this release, Citrix Receiver for Android supports user authentication to Citrix Ready workspace hubs as an experimental feature. This allows authenticated users to cast their sessions to a hub. The feature is disabled by default.

> **Note:**
>
> Location permission is required for the Citrix Ready workspace hub experimental feature. You can deny this permission if there are no workspace hubs present.

DTLS Support over Adaptive Transport

DTLS support has been enabled for adaptive transport using NetScaler Gateway. To use DTLS, ensure that EDT is enabled in the Settings menu of Citrix Receiver for Android.

Recommended verification scenarios for DTLS support:

- Use the Store URL to add the store and launch sessions.
- Configure the adaptive transport policy and experience XenApp and XenDesktop sessions through EDT instead of TCP.

For more information on how to configure adaptive transport, see Adaptive Transport.

Automatic configuration

Citrix Receiver for Android 3.13.1 now configures and detects stores for users automatically.

> **Note:**
>
> Manual configuration of stores has been removed.

Fixed issues

August 20, 2018

Fixed issues in 3.13.9

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

Fixed issues in 3.13.8

- After adding an account, the Save Password settings from the Web Interface account might not be reflected in a session. [RFANDROID-570]
- On a VDA running on Version 7.5 Cumulative Update 5, you might not be able to launch text editing applications like notepad in a session. [RFANDROID-2164]

Fixed issues in 3.13.7

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

Fixed issues in 3.13.6

- Citrix Receiver for Android might not launch a session when opening a downloaded ICA file from the browser. [#RFANDROID-2098]

Fixed issues in 3.13.5

- Citrix Receiver for Android might not launch software-as-a-service (SaaS) applications correctly. [#RFANDROID-1963]

Fixed issues in 3.13.4

- With this fix, you can resize Citrix Receiver dynamically when using a Chromebook. [#RFANDROID-1991]

Issues fixed in 3.13.3

- Graphics on published desktops might appear distorted when using a demo account on Android Nougat 7.1.1. [#RFANDROID-1990]
- Stores configured with internal beacons pointing to a redirected location might not connect when on an internal network. [#RFANDROID-1992]

Issues fixed in 3.13.2

- Disconnected sessions fail to launch when you add the account or tap Refresh on the menu. [#RFANDROID-1456]
- Citrix Receiver for Android does not enumerate applications when using XenApp 6.5. [#RFANDROID-1887]
- Citrix Receiver for Android might exit unexpectedly when rendering legacy icons. [#RFANDROID-1958]
- Citrix Receiver for Android might exit unexpectedly when registering a demo account and the user's first or last name contains blank spaces. [#RFANDROID-1960]
- Citrix Receiver for Android might not install on Chromebooks that support Android applications. [#RFANDROID-1968]

Issues fixed in 3.13.1

- Citrix Receiver does not recognize the client name in the default.ica file when it's listed under an application specific entry. [#LC7539]
- The VDI screen flickers when using Citrix Receiver for Android 3.11.1. [#RFANDROID-1642, #LC7800]
- When using only certificates to authenticate a session, Citrix Receiver for Android might not detect the gateway. [#RFANDROID-1882]
- Passwords with a blank space at the beginning or at the end are not honored. [#RFANDROID-1890]
- Citrix Receiver for Android might exit unexpectedly when connecting to stores configured with no authentication. [#RFANDROID-1929]
- StoreFront stores set up with no authentication on NetScaler Gateway might fail to be detected. [#RFANDROID-1936]
- Users might not be able to connect to Web Interface Sites configured behind NetScaler Gateway. [#RFANDROID-1937]
- 16-bit applications might appear graphically distorted on devices running Android Oreo. [#RFANDROID-1938]
- PNA and XenApp stores connection issues are resolved. If you encounter error code 547, please enable option "Allow legacy store access" and try connecting again.

Known issues

July 24, 2018

Known issues in 3.13.9

No new issues have been observed in this release.

Known issues in 3.13.8

If you add the file type assopciation configured Store account on Receiver for Android Version 3.13.7 and lesser and upgrade Receiver to the latest version, Citrix Receiver is not displayed as an option in the 'Open with' dialog when you select a file to launch.

As a workaround, go to **Settings** > select **Refresh**.[RFANDROID-2241]

Known issues in 3.13.7

No new issues have been observed in this release.

Known issues in 3.13.6

No new issues have been observed in this release.

Known issues in 3.13.5

Citrix Receiver for Android might not launch a session when opening a downloaded ICA file from the browser. As a workaround, download a file explorer app from the Google Play Store, locate the file on your device, then open it directly. [#RFANDROID-2098]

Known issues in 3.13.4

No new issues have been observed in this release.

Known issues in 3.13.3

No new issues have been observed in this release.

Known issues in 3.13.2

- The Pin to Phone option for adding applications and desktops to the phone screen does not work. [#RFANDROID-1896]
- This version of Citrix Receiver for Android might not work properly with NetScaler Gateway integrated with the XenApp Services and website.

  As a workaround, do the following:

  1. Tap “Log Off (all)” from Settings.
  2. Tap “Switch Accounts” to go to the “Accounts” page.
  3. Delete the store from the “Accounts” page.
  4. Add the account again. [#RFANDROID-1900]

Known issues in 3.13.1

- Disconnected sessions fail to launch when you add the account or tap Refresh on the menu. [#RFANDROID-1456]
- Applications published on XenApp 6.5 do not launch. [#RFANDROID-1887]
- The Pin to Phone option for adding applications and desktops to the phone screen does not work. [#RFANDROID-1896]
- This version of Citrix Receiver for Android might not work properly with NetScaler Gateway integrated with the XenApp Services and website.

  As a workaround, do the following:

  1. Tap “Log Off (all)” from Settings.
  2. Tap “Switch Accounts” to go to the “Accounts” page.
  3. Delete the store from the “Accounts” page.
  4. Add the account again. [#RFANDROID-1900]

Third party notices

July 24, 2018

Citrix products often include third party code licensed to Citrix for use and redistribution under an open source license. In an effort to better inform its customers, Citrix publicizes open source code included within Citrix products in an open source licensed code list.

You can review the open source list here: https://www.citrix.com/buy/licensing/open-source.html

For additional source info, check here: https://www.citrix.com/downloads/citrix-receiver/receiver-for-android-source/htmlparser.html

System requirements

September 26, 2018

Device requirements

This release of Citrix Receiver for Android and later supports Android 4.4 (KitKat), 5.x (Lollipop), 6.x (Marshmallow), 7.x (Nougat), and 8.x (Oreo).

For best results, update Android devices to the latest Android software.

Citrix Receiver for Android 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 Android directly.

See the Connectivity section for information regarding secure connections to your Citrix environment.

> **Important**
>
> If a Tech Preview version of Citrix Receiver for Android is installed, uninstall it before installing the new version.

Server requirements

StoreFront:

- StoreFront 2.6 or later

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

- StoreFront configured with a Receiver for Web site

  Provides access to StoreFront stores from a web browser. For the limitations of this deployment, see the StoreFront documentation.

Web Interface (not supported for XenDesktop 7 and later deployments):

- Web Interface 5.4 with Web Interface sites
- Web Interface 5.4 with XenApp Services sites

Web Interface on NetScaler:

You must enable the rewrite policies provided by NetScaler.

XenApp and XenDesktop (any of the following products):

- XenApp 7.5 or later
- XenApp 6.5 for Windows Server 2008 R2
- XenDesktop 7.x or later

Connectivity

Citrix Receiver for Android supports HTTP, HTTPS, and ICA-over-TLS connections to a XenApp server farm through any one of the following configurations.

For LAN connections:

- StoreFront 2.6 or later

- Web Interface 5.4
- XenApp Services (formerly Program Neighborhood Agent) site.

For secure remote connections (any of the following products):

- Citrix NetScaler Gateway 10 and 11 (including VPX, MPX, and SDX versions)
- XenMobile is supported only with versions 9 and 10.

About Secure Connections and TLS Certificates

When securing remote connections using TLS, the mobile device verifies the authenticity of the remote gateway's TLS certificate against a local store of trusted root certificate authorities. The device automatically recognizes commercially issued certificates (such as VeriSign and Thawte) provided the root certificate for the certificate authority exists in the local keystore.

Private (Self-signed) Certificates

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

> **Note:**
>
> When 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 selects to continue through the warning, a list of applications is displayed; however, application fails to launch.

Wildcard Certificates

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

Intermediate Certificates and NetScaler Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Access Gateway server certificate. See the Knowledge Center article that matches your edition of the Access Gateway:

CTX114146: How to Install an Intermediate Certificate on NetScaler Gateway

In addition to the configuration topics in this section of Product documentation, see also:

CTX124937: How to Configure NetScaler Gateway for Use with Citrix Receiver for Mobile Devices

Authentication

> **Note:**
>
> RSA SecurID authentication is not supported for Secure Gateway configurations. To use RSA SecurID, use NetScaler Gateway.

Citrix Receiver for Android supports authentication through NetScaler Gateway using the following methods, depending on your edition:

- No authentication (Standard and Enterprise versions only)
- Domain authentication
- RSA SecurID, including software tokens for Wi-Fi and non-Wi-Fi devices
- Domain authentication paired with RSA SecurID
- SMS Passcode (one-time PIN) authentication
- Smartcard authentication

> **Note:**
>
> Smart card authentication on Web Interface sites is not supported.

Citrix Receiver for Android now supports the following products and configurations.

Supported smart card readers:

- BaiMobile 3000MP Bluetooth Smart Card Reader

Supported smart cards:

- PIV cards
- Common Access Cards

Supported configurations:

- Smart card authentication to NetScaler Gateway with StoreFront 2 or 3 and XenDesktop 7.x and later or XenApp 6.5 and later
- Smart card authentication to NetScaler Gateway with Web Interface 5.4.2 and XenDesktop 7.x and later or XenApp 6.5 or later

> **Note:**
>
> Other token-based authentication solutions might be configured using RADIUS. For information about SafeWord token authentication, see Configuring SafeWord Authentication.

Deploy

September 26, 2018

Providing access information to end users for Android devices

You must provide users with the Citrix Receiver account information they need to access their hosted 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 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 Citrix 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 you are 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.

Providing RSA SecurID authentication for Android devices

If you configure the NetScaler Gateway for RSA SecurID authentication, the 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.

For instructions on configuring authentication, see Authentication and Authorization.

> **Tip**
>
> RSA SecurID authentication is not supported for Secure Gateway configurations. To use RSA SecurID, use the NetScaler Gateway.

Installing RSA SecurID Software Tokens

An RSA SecurID Software Authenticator file has an .sdtid file extension. Use the RSA SecurID Software Token Converter to convert the .sdtid file to an XML-format 81-digit numeric string. Obtain the latest software and information from the RSA Web site.

Follow these general steps:

1. On a computer (not a mobile device), download the converter tool here. Follow the instructions on the web site and in the readme included with the converter tool.
2. Paste the converted numeric string into an email and send it to user devices.
3. On the mobile device, make sure that the date and time are correct, which is required for authentication to occur.
4. On the device, open the email and click the string to start the software token import process.

After the software token is installed on the device, a new option appears in the Settings list to manage the token.

> **Note:**
>
> For mobile devices that do not associate the .sdtid file with Receiver, change the file extension to .xml and then import it.

Saving passwords

Using the Citrix Web Interface Management console, you can configure the 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.

- 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.

Configuration

September 26, 2018

Providing access to virtual apps and desktops

Citrix Receiver requires configuration of either Web Interface or StoreFront to deliver apps and desktops from your XenApp or XenDesktop deployment.

Web Interface

There are two types of Web Interface sites: XenApp Services (formerly Program Neighborhood Services) sites and XenApp websites. Web Interface sites enable user devices to connect to the server

farm.

StoreFront

You can configure StoreFront to provide authentication and resource delivery services for Citrix Receiver, enabling you to create centralized enterprise stores to deliver desktops and applications through XenApp and XenDesktop, and Worx Mobile Apps and mobile apps you've prepared for your organization through XenMobile.

Authentication between Citrix Receiver and a Web Interface site or a StoreFront store can be handled using a variety of solutions:

- Users inside your firewall can connect directly to Web Interface or StoreFront.
- Users outside your firewall can connect to StoreFront or the Web Interface through NetScaler Gateway.
- Users outside your firewall can connect through NetScaler Gateway to StoreFront.

Connecting through NetScaler Gateway

NetScaler Gateway 10 and 11 are supported by Citrix Receiver for Android for access to:

- Web Interface 5.4 XenApp Services Sites and XenApp Web Sites
- StoreFront 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 and 3.11 stores

Both single-source and double-source authentication are supported on Web Interface sites and StoreFront.

You can create multiple session policies on the same virtual server depending on the type of connection (such as ICA, CVPN, or VPN) and type of Receiver (Web Receiver or locally installed Citrix Receiver). All of the policies can be achieved from a single virtual server.

When users create accounts on Citrix Receiver, they should enter the account credentials, such as their email address or the matching FQDN of your NetScaler Gateway server. For example, if the connection fails when using the default path, users should enter the full path to the NetScaler Gateway server.

To connect to XenMobile

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

Enabling access to XenMobile 9:

Client Certificate Authentication

Enabling access to XenMobile 10:

NetScaler Gateway and XenMobile

If you deploy XenMobile in your network, allow connections from remote users to AppController by integrating XenMobile and AppController. This deployment allows users to connect to AppController to obtain their web, Software as a Service (SaaS), and mobile apps, and access documents from ShareFile. Users connect through either Citrix Receiver or the NetScaler Gateway Plug-in.

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

To deploy windows and custom apps to your users, you must wrap the apps by using the MDX Toolkit. You can find more information here:

MDX Toolkit

Connecting to StoreFront

Citrix Receiver for Android supports launching sessions from Receiver for Web, provided that the web browser works with Receiver for Web. If launches do not occur, please configure your account through Citrix Receiver for Android directly.

> **Tip**
>
> When Citrix Receiver for Web is used from a browser, sessions are not launched automatically when downloading an .ICA file. The .ICA file must be opened manually shortly after its downloaded for the session to be launched.

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.

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

Configure stores for StoreFront just as you would for other XenApp and XenDesktop applications. No special configuration is needed for mobile devices. 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 NetScaler Gateway or store URLs needed to access their desktops and applications. For connections through NetScaler Gateway, users also need to know the product edition and required authentication method. After installation, users enter these details into Citrix Receiver, which attempts to verify the connection and, if successful, prompts users to log on.

To configure Citrix Receiver to access apps:

When creating a new account, in the Address field, enter the matching URL of your store, such as storefront.organization.com.

Continue by completing the remaining fields and select the NetScaler Gateway authentication method, such as enabling the security token, selecting the type of authentication, and saving the settings.

When adding an account using an automatic configuration you can enter the FQDN of a StoreFront server or NetScaler, or you can alternatively use an email address to create a new account. You are then prompted to enter the user credentials before logging on.

More information:

For more information about configuring access to StoreFront through NetScaler Gateway, see:

Managing Access to StoreFront Through NetScaler Gateway

Integrating StoreFront with NetScaler Gateway

Connecting to Web Interface

Citrix Receiver can launch applications through your Web Interface site. Configure the Web Interface site just as you would for other XenApp and XenDesktop apps and desktops. No special configuration is needed for mobile devices.

Citrix Receiver supports Web Interface version 5.4 only. In addition, users can launch applications from Web Interface 5.4 using the Firefox mobile browser.

To launch applications on the Android device:

From the device, users log into the Web Interface site using their normal logon and password.

For more information about configuring Web Interface sites see:

Configuring Web Interface

Keyboard layout synchronization

To enable keyboard layout synchronization, go to Settings inside Citrix Receiver for Android and check **Enable client IME**.

Notes:

- The VDA must be version 7.16 or later.
- Administrators must enable the Enhanced support for Asian languages feature on the VDA. By default, the feature is enabled. However, on Windows Server 2016 VDA, you must add a new key called DisableKeyboardSync and set the value to 0 in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\IcaIme to enable the feature.
- Administrators must enable the Unicode keyboard layout mapping feature on the VDA. By default, the feature is disabled. To enable it, create the CtxKlMap key under HKEY_LOCAL_MACHINE\SOFTWARE and set DWORD value EnableKlMap = 1 under HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap.

Limitations:

- This feature works only on soft keyboards on the devices, not on external keyboards.
- Certain mobile devices might not fully support keyboard layout synchronization, such as the Nexus 5x
- The keyboard layout can only be synced from the client to the server. When changing the server-side keyboard layout, the client keyboard layout cannot be changed.
- When you change the client keyboard layout to a non-compatible layout, the layout might be synced on the VDA side, but functionality cannot be confirmed.
- Remote applications that run with elevated privileges (for example, applications you run as an administrator) can't be synchronized with the client keyboard layout. To work around this issue, manually change the keyboard layout on the VDA or disable UAC.

Enabling smart card support

Receiver for Android mobile devices provides support for Bluetooth smart card readers with StoreFront, Web Interface-based site, or a PNA site. If smart card support is enabled, you can use smart cards for the following purposes:

- Smart card logon authentication. Use smart cards to authenticate users to Receiver.
- Smart card application support. Enable smart card-aware published applications to access local smart card devices.
- Signing documents and email. Applications such as Microsoft Word and Outlook that are launched in ICA sessions can access smart cards on the mobile device for signing documents and email.

Supported smart cards:

- PIV cards
- Common Access Cards

Configuring smart card support on the device

1. You must pair the smart card with the mobile device. For more information about how to pair smart card readers with the device, refer to the smart card reader specifications.

   Smart card support for Android devices has the following prerequisites and limitations:

   - Receiver supports this feature on all the Android devices listed by the Biometric Associates middleware.
   - Some users might have a global Pin number for smart cards; however, when users log on to a smart card account, they should enter the PIV pin, not the global smart card pin. This is a third-party limitation.
   - Smart card authentication might be slower than password authentication. For example, after disconnecting from a session, wait about 30 seconds before attempting to reconnect. Reconnecting to a disconnected session too quickly might cause Receiver to fail.
   - Smart card authentication is not supported for browser-based access or from a XenApp site.

2. Install Android PC/SC-Lite service on the Android device before adding a smart-card aware account. This service is available in the form of an .apk file in the baiMobile SDK.

   For Android, the PC/SC-Lite .apk file can be downloaded from the Google Play Store.

3. In Receiver, select the Settings icon, and select **Accounts**, select **Add Account**, or edit an existing account.

4. Configure the connection, and turn on the smart card option.

Installing Citrix Receiver on an SD card

Citrix Receiver for Android is optimized for local installation on user devices. However, if devices have insufficient storage, users can install Receiver on an external SD card and mount it on the device to launch published apps on their mobile devices. This support is provided by default and no additional configuration is required.

To launch an app using the SD card, select the app from the list of Receiver apps on the user device, and then select Move to SD card.

If users opt to install Receiver on an external SD card to launch apps, the following issues exist:

- Mounting a USB storage device while the SD card is mounted on the mobile device causes the SD card to become unavailable, and if apps were running, they stop running when the USB device is mounted.
- Some AppWidgets (such as the home screen widgets) are not available when an app is running from the SD card. After unmounting the SD card, users must restart the AppWidgets.

If users install Receiver locally on their user devices, they can move Receiver to the SD card when needed.

Accessing files using file type association

As a prerequisite for this feature to work, go to the Receiver for Android settings and set the **Use device storage** option to **Full Access**.

Receiver for Android reads and applies the settings configured by administrators in Citrix Studio.
To apply FTA in a session, ensure that users connect to the Store server where the FTA is configured.

On the user device, select the file you want to launch File Explorer and click Open. The Android operating system provides an option to launch the file using Receiver for Android (applying the FTA configured by the administrator) or a different application. Depending on your earlier selection, a default application might or might not be set. You can change the default application using the Change default option.

> **Note:**
>
> This feature is available only on StoreFront and requires XenApp and XenDesktop Version is 7 or later.

Limitation

- You can access only MIME file formats supported by Microsoft Office, Adobe Acrobat reader and Notepad applications using the file type association feature.

Enabling Citrix Ready workspace hub

September 25, 2018

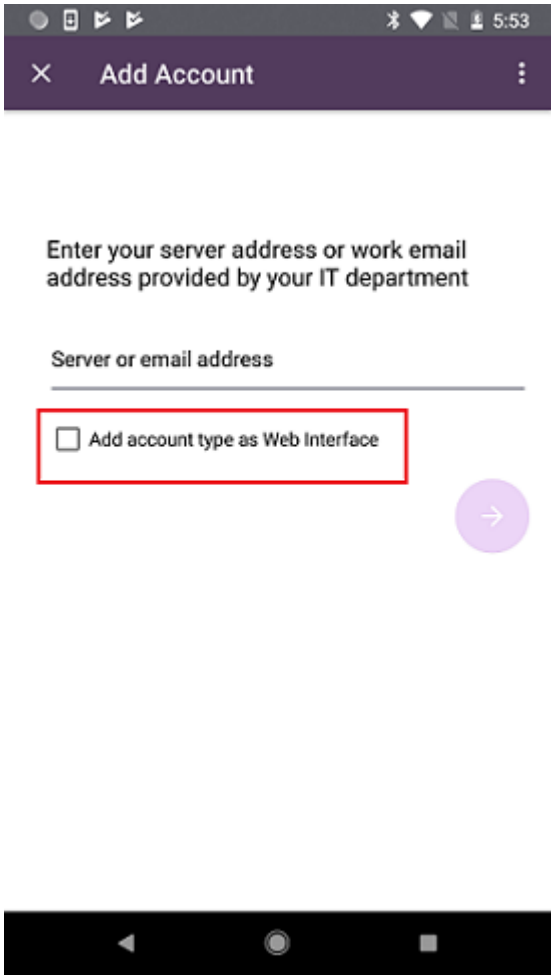
The Citrix Ready workspace hub is disabled by default in Citrix Receiver for Android. To use the hub with an Android device, use the following steps.

Device prerequisites:

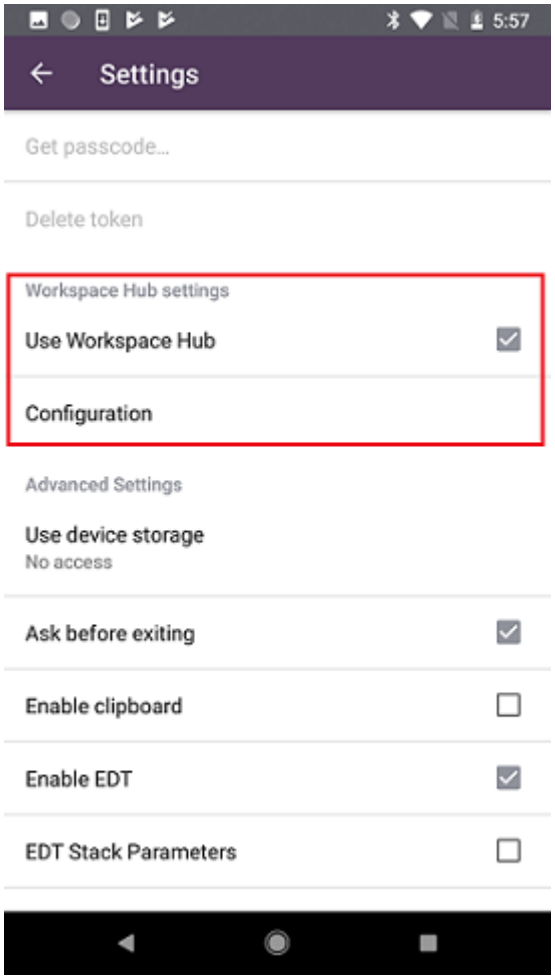
- Citrix Receiver for Android 3.13.5 or later installed
- Bluetooth enabled (for proximity authentication)
- Mobile device and workspace hub using the same Wi-Fi network

Proximity authentication provides a way to authenticate users and launch a session automatically.

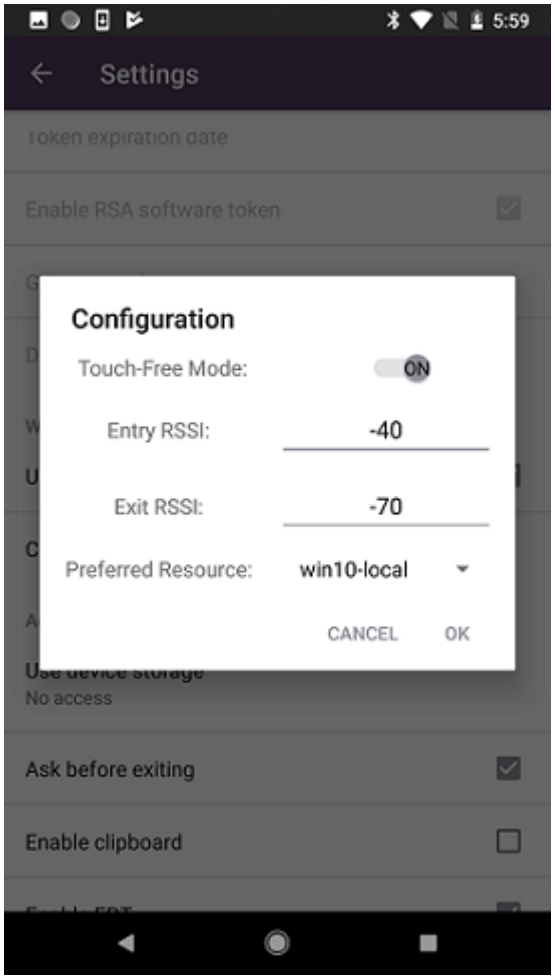
1. To use proximity authentication, enable Bluetooth on the mobile device to ensure that the “Add account type as Web Interface” check box is not selected when setting up the Citrix Receiver account.



2. In Citrix Receiver, go to **Settings** and select **Use Workspace Hub**.



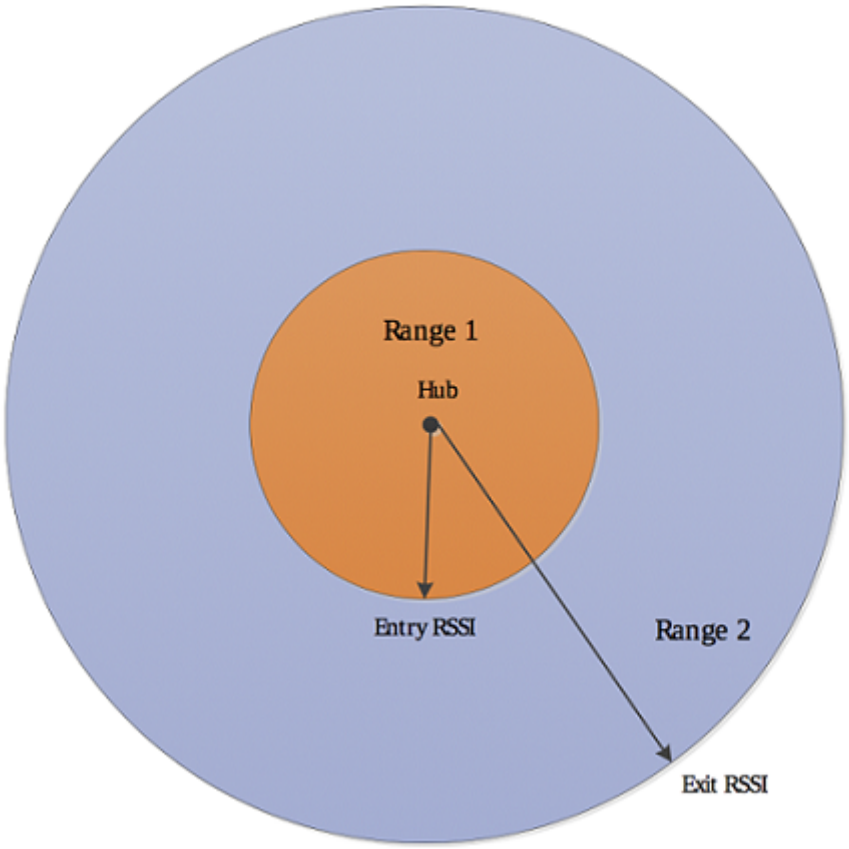
3. Click **Configuration** to bring up the Configuration page.



Touch-Free mode is a switch that lets you enable or disable proximity authentication. When touch-free mode is off, proximity authentication is not available but the other functions of the Citrix Ready workspace hub are. To use touch-free mode, Bluetooth should be enabled on the device.

RSSI represents the Bluetooth signal strength relative to the distance between the mobile device and the hub. Entry RSSI is the range in which the workspace hub beacons are detected. Exit RSSI is the beginning of the range outside of which of the mobile device no longer communicates with the workspace hub. Exit RSSI must be equal to or less than Entry RSSI and values must be negative. The default values are -40 (Entry RSSI) and -70 (Exit RSSI), respectively. You can adjust these values depending on your environment and your range from the workspace hub.

As shown below, when you move your mobile device into Range 1, proximity authentication is triggered and your default desktop or app launches automatically on the workspace hub. As long as the mobile device remains within Range 1 or 2, the default desktop or app keeps running on the workspace hub. When you move the device out of Range 1 and 2, the desktop or app closes automatically.



Preferred Resource is the default desktop or app that launches when the mobile device enters the proximity authentication range. This setting is specific to the account used to log into Citrix Receiver. If you have more than one account, you must set a preferred resource for each. This setting is persistent, which means you need to set your preferred resource only once per account. After you set in, your preferred resource launches every time you enter proximity authentication range until you change the setting.

Troubleshooting

July 24, 2018

Joint Server Certificate Validation Policy

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

> **Important**
>
> Before installing this version of Citrix Receiver for Android, confirm that the certificates at the server or gateway are correctly configured as described here. Connections might 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 Android now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous Citrix Receiver for Android 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 Android's connection to fail.

Suppose that 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 Android:

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

Then, Citrix Receiver for Android will check that all these certificates are valid. Citrix Receiver for Android will also check that it already trusts "Example Root Certificate". If Citrix Receiver for Android 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 Android 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 that a gateway is configured by using these valid certificates. This configuration, omitting the root certificate, is normally recommended:

- “Example Server Certificate”
- “Example Intermediate Certificate”

Then, Citrix Receiver for Android uses 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. This configuration supplies the intermediate certificate that Citrix Receiver for Android needs, but also allows Citrix Receiver for Android to choose any valid, trusted, root certificate.

Now suppose that a gateway is configured by using these certificates:

- “Example Server Certificate”
- “Example Intermediate Certificate”
- “Wrong Root Certificate”

A web browser might ignore the wrong root certificate. However, Citrix Receiver for Android 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 an 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, because it selects 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 by using only the server certificate:

- “Example Server Certificate”

In this case, when Citrix Receiver for Android cannot locate all the intermediate certificates, the connection fails.

SDK and API

July 24, 2018

Citrix Virtual Channel SDK

The Citrix Virtual Channel Software Development Kit (SDK) provides support for writing server-side applications and client-side drivers for additional virtual channels using the ICA protocol. The server-side virtual channel applications are on XenApp or XenDesktop servers. This version of the SDK provides support for writing new virtual channels for Receiver for Android. If you want to write virtual drivers for other client platforms, contact Citrix.

The Virtual Channel SDK provides:

- The Citrix Android Virtual Driver AIDL Interfaces: **IVCService.aidl** and **IVCCallback.aidl**, used with the virtual channel functions in the Citrix Server API SDK (WFAPI SDK) to create new virtual channels.
- A helper class **Marshall.java** designed to make writing your own virtual channels easier.

- Working source code for three virtual channel sample programs that demonstrate programming techniques.

The Virtual Channel SDK requires the WFAPI SDK to write the server side of the virtual channel. For more information on SDK, see Citrix Virtual Channel SDK for Citrix Receiver for Android.

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