About Citrix Receiver for Android 3.10

Dec 21, 2016

Citrix Receiver for Android provides on-the-go tablet and phone access to virtual apps and desktops including touch-enabled apps for low intensity use of tablets as alternatives to desktop computers.

Citrix Receiver for Android 3.10 is the current version on Google Play. Users running earlier versions should update to the latest version. The preferred method to update or install Citrix Receiver for Android is from Google Play using an Android device. This allows for automatic updates when new versions are available.

Citrix Receiver for Android is available in English, German, French, Spanish, Japanese, Simplified Chinese, Korean, Italian, Portuguese, Dutch, Swedish, and Danish.

What's new in Citrix Receiver for Android 3.10

This release provides the following new features and enhancements, and resolves a number of previously reported issues to improve the user experience.

- A new customer feedback channel
- Improved process of adding store accounts
- Support for Android immersive window mode (Android 4.4 and onwards)
- Support for Android native mouse cursor (Android 7.0)

Fixed issues

Dec 21, 2016

Issues fixed in 3.10

This release does not fix any customer reported issues.

Known issues

Dec 21, 2016

Known issues in 3.10

The following known issue has been identified in version 3.10:

- If you select **Log Off All** from the **Switch Account** menu, there is a high probability that only the highlighted account is logged off. As a workaround, log off the account from the **Resource** screen. If using the **Switch Account** menu, log off the accounts one by one.

  [RFANDROID-544]

System requirements

Dec 21, 2016

Device requirements

Citrix Receiver for Android 3.10 supports Android 4.0 (Ice Cream Sandwich), 4.1/4.2/4.3 (Jelly Bean), 4.4 (KitKat), 5.0/5.1 (Lollipop), 6.0 (Marshmallow), and 7.0 (Nougat).

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

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.

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

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

Server requirements

StoreFront:

- StoreFront 3.8 (recommended), 3.7, 3.6, 3.5, 3.0 and 2.6
  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.x
- XenApp 6.5 for Windows Server 2008 R2
- XenApp 6 for Windows Server 2008 R2
- XenApp 5 for Windows Server 2008
- Citrix Presentation Server 4.5
- XenDesktop 7.x
- XenDesktop 7
- XenDesktop 5, 5.5, and 5.6

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, 3, 3.5, 3.6, 3.7 or 3.8 (recommended)
- 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 in order to successfully access Citrix resources using Receiver.

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

- BaiMobile 3000MP Bluetooth Smart Card Reader

Supported smartcards:

- PIV cards
- Common Access Cards

Supported configurations:

- Smartcard authentication to NetScaler Gateway with StoreFront 2 or 3 and XenDesktop 5.6 and above or XenApp 6.5 and above
- Smartcard authentication to NetScaler Gateway with Web Interface 5.4.2 and XenDesktop 5.6 and above or XenApp 6.5 or above

> **Note**
>
> Other token-based authentication solutions may be configured using RADIUS. For SafeWord token authentication, search eDocs for "Configuring SafeWord Authentication" and refer to the instructions that match your edition of NetScaler Gateway.

Providing access to virtual apps and desktops

Dec 21, 2016

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.

In this article:

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 and 3.8 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 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

Installing Citrix Receiver on an SD card

Dec 21, 2016

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.

Enabling smart card support

Dec 21, 2016

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. For example, to pair the baiMobile Bluetooth smart card reader with the Android device, see: https://www.biometricassociates.com/downloads/user-guides/baiMobile-3000MP-User-Guide-for-Android-v3.2.pdf.
   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. For details, see http://www.biometricassociates.com/products/smart-card-readers/android-supported-devices/.
   - 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.

Providing RSA SecurID authentication for Android devices

Dec 21, 2016

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 from: ftp://ftp.emc.com/pub/agents/tokenconverter310.zip. 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.

Providing access information to end users for Android

Dec 21, 2016

You must provide users with the 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 Receiver to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Receiver installation and configuration. Receiver determines the 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.

To configure your DNS server to support email-based discovery, see Configuring Email-Based Account Discovery.

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

Provide users with a provisioning file

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

For more information, see the StoreFront documentation.

Provide users with 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 the Access Gateway, provide the Access Gateway address and required authentication method. For more information about configuring NetScaler Gateway, see the NetScaler Gateway or XenApp (for Secure Gateway) documentation.

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

Saving passwords

Dec 21, 2016

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, Receiver stores the password on the device for future logons and does not prompt for passwords when users connect to applications.

> **Tip**
>
> 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), Receiver prompts users to enter passwords every time they connect.

> **Note**
>
> For StoreFront 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.

Changing Citrix Receiver settings on the device

Dec 21, 2016

The following settings can be customized from the Settings tab:

- **Display**
  - Session resolution: Select the in-session resolution. The default is **Fit screen**.
- **Keyboard**
  - Use predictive text: Enable or disable predictive text. The default is **Off**.
  - Extended keyboard: Enable or disable the Extended keyboard. The default is **Off**.
  - Extended keys: Configure special keys, for example Alt and Ctrl, to display as part of the Extended keyboard.
  - Enable client IME: When client-side IME is enabled, users can compose text at the insertion point rather than in a separate window. The default is **Off**.
- **Audio**
  - Audio streaming: Configure in-session audio settings to Audio off, Play, Play and record. The default is **Play**.
- **Advanced**
  - Use device storage: Permission to access device storage. The default is **No access**.
  - Ask before exiting: Configure to ask for confirmation before exiting. The default is **On**.
  - Enable clipboard: Configure to enable or disable use of clipboard. The default is **Off**.
  - Display orientation: Configure to fix display orientation to Landscape mode, Portrait mode, or Automatic (dynamic). The default is **Automatic**.
  - Keep display on: Configure to leave the device display on. The default is **Off**.
- **TLS version supported**: 1.0, 1.1, and 1.2. The actual TLS level that is used is the highest supported by the site.
- **About**: About Citrix Receiver, version and copyright info.

Try the Demonstration Site

Dec 21, 2016

When users launch Citrix Receiver for the first time, the welcome page offers the option to launch a demonstration account in the Citrix Cloud.

Users complete the account registration by entering their names and email addresses (email addresses are prepopulated on some devices). The demonstration site is already configured with published applications so your users can try Citrix Receiver right away.

Users can add, change, and remove their own accounts in Receiver.