About Citrix Receiver for Android 3.7.x

Oct 02, 2015

What's new in Citrix Receiver for Android 3.7.3

Citrix Receiver for Android 3.7.3 is the current version on Google play. Users running prior versions should update to the latest version.

Citrix Receiver for Android 3.7.3 includes support for Android M (6.0).

Issues fixed in 3.7.3

Citrix Receiver for Android 3.7.3 addresses intermittent crashing when Citrix Receiver is used with Nexus 9 Bluetooth.

What's new in Citrix Receiver for Android 3.7

This recent update includes:

- **Fit to display**. When publishing an app with a specific resolution, Receiver now displays the app in a central area and scales the display depending on the aspect ratio; it properly interprets the relationship between the source (app) and the destination (the display).
- **Enhanced support for mirroring the session display**. Receiver for Android enhances the user experience by matching the display characteristics between the screen display and the Android device.
- **Support for Transport Layer Security (TLS)**. Receiver for Android now supports TLS 1.1 and TLS 1.2 protocols. When enabled, TLS provides secure communication between the server and client. This functionality can be configured using the interface or through the **receiverconfig** file.
- Support the hiding of in-session menu bar for devices without touchscreen support.
- Improved keyboard handling of the Korean Hangul alphabet.

Known issues

The following issues and limitations are known at this release of Receiver for Android:

- In the previous release, limited support was provided for mirroring the session display to a second display; a limitation existed where only devices whose resolution matched the display of the Android device were supported. At this release of Receiver for Android, this limitation has been removed - display devices whose resolution differ from the Android device are supported, with the following limitations: [#549471]
  - Session size is determined by the natural resolution of the attached display device; all other settings are ignored because the second display cannot scale the session image. In addition, requests to dynamically adjust the session resolution to match the resolution of an attached display are only partially supported. In such environments, connecting and disconnecting a second display will not allow you to request a resize of the session that observes the normal user settings.
  - Instability may occur when disconnecting a second display, causing Receiver to crash. It is suggested that when using a second display you connect it to your Android device before starting your session.
  - Display performance may be negatively impacted in the attached display; in some cases, the attached display may occasionally experience cosmetic faults, such as faulty display of the mouse pointer and tearing during window moves.
  - Some limitations apply to the user interface as displayed on the primary display of the Android device. For example, the mouse operates to a device's screen dimension, and not to secondary screens. Additionally, no toolbar is displayed

on the device screen when screen mirroring is enabled. [#549471]

- When attaching a secondary display, the screen resolution of the newly attached display is the same resolution as the device. This issue occurs when the connected device is docked after the session is initiated, and when the mouse is not attached to the dock. To resolve this situation, attach the mouse for the second session to return to the correct resolution. This issue applied specifically to the Samsung Galaxy Note II Multimedia Dock. [#541028]
- Removing the mouse from a docked session causes the screen display on the device to rotate 90 degrees clockwise. Session orientation returns to normal after a short period of time. This issue applied specifically to the Samsung Galaxy Note II Multimedia Dock. [#541032]
- When using screen mirroring to an external monitor using an AllCast dongle, no audio is heard when playing media files. This issue appears to be related to the capability of the display device; if a TV with speakers is used, audio output occurs through the TV. If a monitor with no speakers is used, the expectation is that speakers on the Android device would be used, however, this is not the case.[#544330]
- Moving the magnifier to the outer most edge of the session image may cause the magnifier to display part of the unmagnified background image. [#542299]
- On some occasions, closing a session may result in a run time exception. [#523824]
- Maximum 'Pinch Out' level is not maintained after screen rotation. This event may occur after launching a session and using 'Pinch In' to attain the maximum desired view, and then rotating the device 90 degrees; after rotating the device a second time, the previously selected 'Pinch Level' is not maintained. [#538638]
- The extended keyboard is erroneously activated in certain conditions; in some cases, this occurs when screen mirroring is stopped and the device is rotated, in other cases this may occur when the device screen is touched while screen mirroring is enabled. These issues may occur when the Android device is unable to determine whether the soft keyboard is showing; entering mirror mode by connecting another monitor fails to interpret the act of displaying the extended keyboard. [#545231]
- Account creation fails for ASUS Nexus 7 devices running Android version 4.1.1. To prevent this issue, update the device to the latest Android software, such as 4.2.2.
- On some Android devices, the Bluetooth Mouse right-mouse click continues to invoke the Back action, causing the Exit dialog box to appear unintentionally. This issue occurs only on devices with firmware that does not support the right-mouse click. [#331168]
- In Receiver for Android 3.5, the Full VPN Tunnel feature is not supported when you use smartcard authentication. [#456657]
- When you connect to an FIPS NetScaler while the "denysslreneg" policy is set to No or Frontend Client and "Client Authentication" is set to Optional, you may encounter the following error when you log in to Receiver.
  - When you log in to Receiver by entering "Domain\username" in the username field, you may receive a prompt that your username or password was incorrect . This prompt displays Domain\Domain\username in the username field. To resolve this issue, remove one of the domain name entries and log in again using the domain|username format. [#466022]

System requirements for Receiver for Android 3.7.x

Oct 02, 2015

Device

- Citrix Receiver for Android 3.7.3 supports Android versions 4, 5, and 6 (Android M).
- Citrix Receiver for Android 3.7, 3.7.1, and 3.7.2 support Android versions 4 and 5.
- For best results, update Android devices to the latest Android software.
- Receiver for Android supports launching sessions from Receiver for Web, provided that the web browser will work with Receiver for Web. If launches do not occur, please configure your account through Receiver for Android directly.
- If a Technology Preview version of Citrix Receiver is installed, uninstall it before installing the new version.

Important: Refer to the **Connectivity** section (below) for information regarding secure connections to your Citrix environment.

Server

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

- StoreFront 3.0 (recommended)
  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 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 Fundamentals 6.0 for Windows Server 2008 R2
  - XenApp 5 for Windows Server 2008
  - XenApp 5 for Windows Server 2003
  - Citrix Presentation Server 4.5
  - XenDesktop 7.x
  - XenDesktop 7
  - XenDesktop 5, 5.5, and 5.6

Connectivity

Citrix Receiver 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.x or 2.6 (recommended), Web Interface 5.4, or a XenApp Services (formerly Program Neighborhood Agent) site.

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

- Citrix NetScaler Gateway 10 (including VPX, MPX and SDX versions)
- Citrix Access Gateway Enterprise Edition 9.x, and 10.x (including VPX, MPX and SDX versions)
  - CloudGateway is supported only with versions 9.3 and higher

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.

Importing Root Certificates on Android Devices

Android 4.x devices support importing root certificates without gaining root access to the device. Android devices prior to 4.0 do not support automatic import of root certificates.

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 the Access 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 Base article that matches your edition of the Access Gateway:

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

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

CTX124937: How to Configure Citrix Access Gateway Enterprise Edition 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 the Access Gateway.

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

- No authentication (Standard and Enterprise versions only)
- Domain authentication

- RSA SecurID, including software tokens for WiFi and non-WiFi devices
- Domain authentication paired with RSA SecurID
- SMS Passcode (OTP) authentication
- Smartcard authentication*

* Receiver for Android now supports the following products and configurations.
Note: Smart card authentication on Web Interface sites is not supported.
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.x 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 Access Gateway.

Manage

Jun 20, 2013

Receiver requires configuration of Web Interface for your deployment. 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. Authentication between Receiver and a Web Interface site can be handled using a variety of solutions, described in this section.

Additionally, you can configure StoreFront to provide authentication and resource delivery services for 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, refer to http://community.citrix.com.

Installing Receiver on an SD Card

Mar 23, 2015

Receiver for mobile devices 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.

To configure Access Gateway Enterprise Edition for Citrix Receiver for Android

Jan 30, 2015

Important:

- Access Gateway Enterprise Edition 9.x and 10.x are supported by Receiver for Android using XenApp Services sites.
- Access Gateway Enterprise Edition 9.x and 10.x are supported by Receiver for Android using XenApp Web Sites.
- Receiver for Web is not supported by Receivers for Android.
- Access Gateway Enterprise Edition 9.x and 10.x are supported by Receiver for Android to access StoreFront stores.
- Both single-source and double-source authentication are supported on Web Interface sites and StoreFront.
- You must use the Web Interface 5.4, which is supported by all built-in browsers.
- 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 Receivers). All of the policies can be achieved from a single virtual server.
- When users create accounts on Receiver, they should enter the account credentials, such as their email address or the matching FQDN of your Access Gateway server. For example, if the connection fails when using the default path, users should enter the full path to the Access Gateway server.

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

- If you deploy CloudGateway Enterprise in your network, allow connections from remote users to AppController by integrating Access Gateway 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 Access Gateway Plug-in.
- If you deploy CloudGateway Express in your network, allow connections from internal or remote users to StoreFront through Access Gateway by integrating Access Gateway 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.

For information about configuring these connections, refer to "Integrating Access Gateway with CloudGateway" and the other topics in Access Gateway 10 documentation.

For information about the settings required for Receiver for mobile devices see also these topics in the Access Gateway 10 documentation:

- Creating the Session Profile for Receiver for CloudGateway Enterprise
- Creating the Session Profile for Receiver for CloudGateway Express
- Configuring Custom Clientless Access Policies for Receiver
- Allowing Access from Mobile Devices

And the following topic in in the XenMobile documentation:

- App Preparation Tool for Mobile Apps

To enable remote users to connect through Access Gateway to your Web Interface deployment, configure Access

Gateway to work with Web Interface, as described in "Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface" and in the Access Gateway 10 documentation.

To configure the Web Interface for Citrix Receiver for Android

Jun 14, 2013

To configure the Web Interface site

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

The 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 can log into the Web Interface site using their normal logon and password.

To start applications from the Web Interface site when using Receiver for Android, the SD card on the device must be available for the session to launch. If the SD card is not available (for example, if it is either in use or not mounted), the session launch fails.

Enable smart card support

Apr 07, 2015

Receiver for Android mobile devices provides support for Bluetooth smart card readers with 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

To configure 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: http://www.biometricassociates.com/downloads/user-guides/baiMobile-3000MP-User-Guide-for-Android-v2.0.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 3rd 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 PNAgent 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.

Provide RSA SecurID Authentication for Android Devices

Jun 19, 2013

If you configure the Access Gateway for RSA SecurID authentication, the Receiver supports Next Token Mode. With this feature enabled, if a user enters three (by default) incorrect passwords, the Access 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 to configure RSA SecurID authentication, in eDocs, expand your version of the Access Gateway, and locate *— Configuring RSA SecurID Authentication*
.

RSA SecurID authentication is not supported for Secure Gateway configurations. To use RSA SecurID, use the Access 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: http://www.rsa.com/node.aspx?id=2521. 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.

Provide access information to end users for Android

Mar 23, 2015

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 Receiver is connecting to a Web Interface deployment.
To configure your DNS server to support email-based discovery, see Configuring Email-Based Account Discovery in the StoreFront documentation.

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 Access Gateway documentation.

Provide users with a provisioning file

You can use StoreFront to create provisioning files containing connection details for accounts. You make these files available to your users to enable them to configure Receiver automatically. After installing Receiver, users simply open the .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 the Access Gateway or Secure Gateway, see the Access Gateway or XenApp (for Secure Gateway) documentation.

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

Save Passwords

Jun 19, 2013

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.
  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), 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.

Change Citrix Receiver Settings on the device

Mar 23, 2015

The following settings can be customized from the Settings tab in Citrix Receiver for Android:

- **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**.
- **ShareFile**: This feature is no longer supported and will be removed in a future update. Please use the ShareFile app.
- **About**: About Citrix Receiver, version and copyright info.

Try the Demonstration Site

Jun 19, 2013

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.