Receiver for Android 3.5.x - 3.4.x

2015-02-22 04:22:27 UTC

Contents

Receiver for Android 3.5.x - 3.4.x

Citrix Receiver enables your users to access PC applications published on XenApp or XenDesktop from their Android devices. You publish applications on XenApp or XenDesktop to make them available to your users. Using Doc Finder through Citrix Receiver, your users can also securely browse and access files stored on the server.

Receiver for Android supports the Mobile SDK for Windows Apps and Citrix deployments, such as XenDesktop 7 and XenApp 6.5 Feature Pack 2, that include built-in mobility features. Mobility features improve the experience of Citrix Receiver users working in supported Windows applications and published server desktops on mobile devices.

In this section

System requirements	Ensure your users have the required hardware and software.
About this release	Review the list of new features and known issues
Manage your connections	Learn how to configure your deployment so your users can access their published applications.
Configure your XenApp server environment	Learn how to configure your deployment so your users can access their published applications.
Provide access information to end users	Ensure users can connect successfully.
Save passwords	Learn about the Receiver's support for configuring the online plug-in to allow users to save their passwords.
Troubleshoot Receiver for Android	Respond to problem reports from your users.

About Receiver for Android 3.5.x - 3.4.x

New in 3.5.x

This update included:

- Android Runtime (ART) support.
- Android 5.0 support. Support for Android 5.0 Lollipop (Android L).

New in 3.5

This release added the following new features:

- SAN Certificate support.
- Android 4.4. support.
- Proxy configuration support.
- Smartcard support.* Receiver for Android now offers support for the following products and configurations.
  - Supported smartcard readers:
    - BaiMobile 3000MP Bluetooth Smart Card Reader
  - Supported smartcards:
    - PIV cards
    - Common Access Card
  - 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.

* Customers using FIPS NetScaler devices should configure their systems to deny SSL renegotiations. See How to configure the -denySSLReneg paramter.

New in 3.4.x

In addition to general usability and performance improvements, this release added these new features:

- HDX Rich Graphics support, which provides the highest frame-rate for the available bandwidth on devices.
- Support for new APIs for Mobile SDK for Windows Apps: photos (and selection of photo attributes), video clips, and audio clips.

About Receiver for Android and Worx Apps

If your users installed Worx Apps through Receiver for Android 3.3.61 and are having problems launching Worx Apps after upgrading to Receiver for Android 3.4.11, upgrading to Receiver for Android 3.4.12 or Receiver for Android 3.5 resolves those issues.

If your users installed Worx Apps through Receiver for Android 3.4.11 and are having problems launching Worx Apps, upgrade to Receiver for Android 3.4.12 or Receiver for Android 3.5 and reinstall the Worx Apps.

Known issues

- Smart card authentication on Web Interface sites is not supported. [#348984]
- 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.
- Multi-touch gestures are not supported on Windows 7.
- 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]
- Receiver does not support Bluetooth Mouse on the Nexus 10 device. [#368795]
- In Receiver for Android 3.5, the Full VPN Tunnel feature is not supported when you use smartcard authentication. [#456657]
- When you add a StoreFront account manually, the full store address is required to successfully add the account. [#455441]
- When you access an app or desktop from a tablet with the keyboard displayed, rotating the tablet 90 degrees and deselecting the keyboard may not result in a full-screen display. If the display does not revert to full-screen after the keyboard is deselected, rotate the tablet 90 degrees to return to full-screen display. [#457589]
- 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]

Issues fixed in 3.5

- When you select the Access Gateway type while changing a site type, the two buttons that appear at the bottom of the device screen may be unresponsive or display only the Edit option, instead of displaying Cancel and Update options. [#450657]

Issues fixed in 3.4.x

- Predictive text is now disabled by default to address reported usability issues. [#403227]
- Korean-specific issue on Samsung devices that prevented Korean characters from being recognized correctly on the Bluetooth keyboard. [#LA2892, 393421]
- The timezone redirection could not redirect exact timezones in an ICA session. [#LA2621]

System requirements for Receiver for Android

Device

- For best results, update Android devices to the latest Android software.
- Mozilla Firefox Browser for Android is the only browser supported by Receiver for Android. Other browsers are not supported.
- Citrix Receiver supports Android versions 2.3.3 or later.
- 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 2.5 (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
- XenDesktop 4

Connectivity

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

For LAN connections:

- StoreFront 2.*x* or 2.5 (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 SSL Certificates

When securing remote connections using SSL, the mobile device verifies the authenticity of the remote gateway's SSL 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 the Citrix Receiver.

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

CTX111872: How to Upload an Intermediate Certificate on Citrix Access Gateway 4.5.x

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. 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.

Availability of Receiver for Android 3.4 features

Some of the features and functionality of Receiver for Android are available only when connecting to newer XenApp and XenDesktop versions and might require the latest hotfixes.

- For XenDesktop 5.6 deployments, HRP01 is required to support File Type Association in the Receiver Docs view (provided by ShareFile integration).
- ShareFile integration with Receiver requires CloudGateway Enterprise.

Manage

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.

Configure your environment for Citrix Receiver for Android

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

- When publishing applications on your farms or sites, consider the following options to enhance the experience for users accessing those applications through StoreFront stores:
  - Ensure that you include meaningful descriptions for published applications, as these descriptions are visible to users in Citrix Receiver.
  - You can emphasize published applications for your mobile device users by listing the applications in Citrix Receiver's Featured list. To populate the Featured list on Citrix Receiver, edit the properties of applications published on your servers and append the string KEYWORDS:Featured to value of the Application description field.
  - To enable the screen-to-fit mode that adjusts the application to the screen size of mobile devices, edit the properties of applications published on your servers and append the string KEYWORDS:mobile to value of the Application description field. This keyword also activates the auto-scroll feature for the application.
  - To automatically subscribe all users of a store to an application, append the string KEYWORDS:Auto to the description you provide when you publish the application in XenApp. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.
  - When publishing the Remote Desktop (RDP) application for the Android, to ensure the shift-key works properly on user devices, append the string KEYWORDS:unikey to the value of the Application description field. This keyword causes Receiver to send keystrokes using an alternate mechanism that allows the Caps Lock key to work.

  For more information see the StoreFront documentation.
- If the Web Interface of your XenApp or XenDesktop deployment does not have a Web site or XenApp Services site, create one. For instructions on how to create one of these sites, see the "Configuring Sites" topics for Web Interface 5.4.
- To enable users to easily browse and access their work files (such as Microsoft Word documents) from a drive space on the server, publish Citrix Doc Finder on the servers your users connect to from their mobile devices.

Installing Receiver on an SD Card

Receiver for mobile devices is optimized to be installed locally 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, users 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 installed locally on their user devices, they can move Receiver to the SD card when needed.

To configure StoreFront for Citrix Receiver for Android

To configure StoreFront

Important:

- Only Citrix Access Gateway Enterprise Edition 9.3 and Access Gateway 5 and 10 are supported by Receiver for Android 3.*x* when using StoreFront.
- Legacy mode is no longer required for StoreFront in any configuration scenario.
- Receiver for Android does not support Receiver for Web.

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, XenApp farms, and App Controller, making these resources available to users.

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

To configure the App Controller

App Controller extends the types of applications that users can access. In addition to providing access to applications published for XenApp and XenDesktop, you can use App Controller, a component of CloudGateway Enterprise, to provide URLs for Web applications and applications on your internal network, including applications that are not Windows-based and internal applications. StoreFront aggregates the applications published through App Controller with the applications published with XenApp or XenDesktop for users to access from Receiver.

If you use StoreFront and App Controller, refer to the App Controller documentation for details about Configuring StoreFront for mobile devices. You must modify the web.config file to register devices.

Use App Controller to configure Web and SaaS apps for users. For details about installing and configuring App Controller, see your App Controller version in eDocs.

To configure Access Gateway

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

- Only Citrix Access Gateway 9.3 Enterprise Edition and Access Gateway 5 and 10 are supported by Receiver for Android 3.*x* using StoreFront.
- For details, see your version of Access Gateway in eDocs.

To configure Receiver to access apps

1. When creating a new account, in the Address field, enter the matching URL of your store, such as `storefront.organization.com`.
2. Continue by completing the remaining fields and select the Access Gateway authentication method, such as enabling the security token, selecting the type of authentication, and saving the settings.

To configure Access Gateway Enterprise Edition for Citrix Receiver for Android

Important:

- Access Gateway Enterprise Edition 9.*x* and 10.*x* are supported by Receiver for Android using XenApp Services sites or Legacy mode on StoreFront servers.
- 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 under that node in eDocs.

Information about the settings required for Receiver for mobile devices are in the following topics:

- 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
- App Preparation Tool for Mobile Apps
- Configuring ShareFile on Receiver for Mobile Devices

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 its sub-topics in Citrix eDocs.

To configure Access Gateway Standard Edition for Citrix Receiver for Android

To configure the XenApp Services site

Important:

- Access Gateway Standard Edition 4.6.*x* is supported by Receiver for Android 3.*x* using XenApp Services sites.
- Access Gateway Standard Edition 4.6.*x* is supported by Receiver for Android 3.*x* using XenApp Web sites.
- Both single-source and double-source authentication are supported on Web Interface sites.
- You must use the Web Interface 5.4, which is supported by all built-in browsers.

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

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

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

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

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

To configure the Access Gateway 4.6.x appliance

1. Configure Authentication realms to authenticate users connecting to the Access Gateway by using the Access Gateway Plug-in.

   Active Directory authentication and RSA SecurID are supported authentication methods for Receiver for Android:

   - If double-source authentication is required (such as Active Directory and RSA SecurID), RSA SecurID authentication must be the primary authentication type. Active Directory authentication must be the secondary authentication type.

   - RSA SecurID can use either RADIUS or an sdconf.rec file to enable token authentication.

   - Active Directory authentication can use either LDAP or RADIUS.

   Test a connection from a user device to verify that the Access Gateway is configured correctly in terms of networking and certificate allocation.

2. To establish communication with XenApp servers and the Web Interface, configure Access Gateway to recognize the servers. You can configure the settings by using group properties on Access Gateway. Configure Access Gateway to allow incoming XenApp connections from the Receiver and specify the location of your newly created XenApp Services site.

   a. In the Administration Tool, click the Access Policy Manager tab.

   b. Right-click a user group and then click Properties.

   c. On the Gateway Portal tab, click Redirect to Web Interface.

   d. If the **Path** field for XenApp Services for Web Interface contains an existing configuration for a Web Interface site for ICA connections on the Access Gateway, do not modify your existing configuration, but make sure that your XenApp Services site is located on the same server that is hosting the Web Interface site. If the Path field is empty, meaning there is no existing configuration for ICA connections, type `/Citrix/PNAgent`.

   e. In Web server, type the IP address or FQDN of the server running the Web Interface.

   f. On the Global Cluster Policies tab, select Enable logon page authentication.

   Note:

   - The check box Single sign-on to the Web Interface is specifically for Web Interface and does not affect connections using the Receiver for mobile devices. If you configured the Access Gateway to use a Web Interface site for other users, continue to maintain and use it for the Web Interface.

   - To enable Citrix XenApp connections on an Access Gateway that has previously been configured to accept connections by using the Access Gateway Plug-in, select Use the multiple logon option page. For more information, see the Access Gateway documentation.

- In the Access Gateway Administration Tool, on the Authentication tab, click the Secure Ticket Authority tab and add the STA details. Make sure the STA information is the same as the XenApp Services site.

Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), make sure that the intermediate certificates are also installed correctly on the Access Gateway. For information about installing certificates, see the Access Gateway documentation.

To configure the mobile device for the Receiver application

1. In Account Settings, in the Address field, enter the matching FQDN of your Access Gateway server:

   If you created the XenApp Services site using the default path (/Citrix/PNAgent), enter the Access Gateway FQDN such as: `GatewayServer.organization.com`.

   If you customized the path for the XenApp Services site, enter the full path to the config.xml file, such as: `FQDNofAccessGateway/CustomPath/config.xml`.

2. Continue by completing the remaining fields and select the Access Gateway authentication method, such as enabling the security token, selecting the type of authentication, and saving the settings. On some mobile devices, Receiver does not include all of those options.

To configure Access Gateway 5.x to use a XenApp Services site

Important:

- Access Gateway 5.x is supported by Receiver for Android 3.*x* by using either XenApp Services sites or XenApp Web sites.
- If using XenApp Web sites, use the steps described in To configure Access Gateway 5.0 for Citrix Receiver. If using XenApp Services, use the steps described in this topic.
- When using XenApp Services sites, only single-factor authentication is supported. When using XenApp Web sites, both single-source and double-source authentication are supported.
- You must use the Web Interface 5.4, which is supported by all built-in browsers.

You can configure Access Gateway 5.*x* to allow users to connect by using Citrix Receiver for mobile devices that work with the XenApp Services site. To do so, you configure the Web Interface to use XenApp Services sites and then on Access Gateway, create a basic logon point and configure it to use the Web Interface for authentication. When users log on, they can start published applications directly from the mobile device. To give users this type of access, the basic steps are:

1. Create a XenApp Services site in the Web Interface, setting the fully qualified domain name (FQDN), Secure Ticket Authority (STA), and the access method.
2. On Access Gateway, create a basic logon point, such as "mobile," and configure it to use the Web Interface for authentication.

   If users log on to the default logon point, they only need to type in the Access Gateway FQDN. If users do not log on to the default logon point, they must enter the FQDN of Access Gateway, plus the full path of the logon point. For example, users would type in `https://<AccessGatewayFQDN>/lp/mobile`.
3. In the basic logon point, set the XenApp Services sites as the home page. When you configure the home page, enter the full path to the config.xml file. For example, `<WI-ServerName>/citrix/pnagent/config.xml`.
4. On Access Gateway, configure the STA and the ICA access control list.

When users log on with the Receiver or online plug-in and enter the Access Gateway FQDN as the server address, the XenApp Services site enumerates applications and the user connection routes through Access Gateway.

Note: You must use Access Gateway 5.*x* to enable this feature.

To configure Access Gateway to connect to the XenApp Services site

1. In the Access Gateway Management Console, click Management.
2. Under Access Control, click Logon Points.
3. In the Logon Points panel, click New.
4. In the Logon Points Properties dialog box, in Name, type a unique name for the logon point, such as "mobile."
5. In Type, select Basic.
6. Select Authenticate with Web Interface.
7. In Web Interface, type the full path to the config.xml file within the XenApp Services site, such as `http://<XenAppServerName>/citrix/pnagent/config.xml`, and then click Save.

To launch Receiver applications on the Android device

1. On the Android device, enter the URL to the server to connect to the logon point that was created for users, such as: `<AccessGatewayFQDN>/lp/mobile/`.
2. Enter your domain credentials normally.

To configure the Web Interface for Citrix Receiver for Android

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

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.

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:

   - Google Play Store
   - The software developer
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 ShareFile Services to Receiver Users

Citrix ShareFile is a cloud-based, secure file sharing service. ShareFile enables users to send large documents by email, securely handle document transfers to third parties, and access a web-based collaboration space from computers or mobile devices.

You can configure Citrix CloudGateway Enterprise to deliver ShareFile Enterprise services, providing users access to document sharing features from the Receiver interface. In the Receiver Docs view, users can view, edit, and share documents. When offline, Receiver users can access documents synced to their desktop computer or mobile device.

To configure App Controller and ShareFile

Prerequisite: To configure a ShareFile account for your organization (and keep users on one subdomain), register for an account for Receiver on ShareFile.com.

Note: If users register for their own ShareFile account, they create multiple subdomains on your server.

General Steps

1. Complete CloudGateway and ShareFile configuration:

   In the App Controller Management Console, configure the ShareFile settings. For more information, see *To configure ShareFile settings* in the App Controller documentation.

   In the StoreFront Management Console, enable data provisioning. For more information, see *To manage the resources made available through stores* in the StoreFront.

2. Optional: Customize the branding and messages that appear in notifications emailed from ShareFile.com when users send or request documents. For more information, see *Customizing Web Portal, Logon Page, and Email Notifications* in the ShareFile documentation.

   If you plan to advertise to users that they can also use the ShareFile Web interface to share files, consider whether to configure custom branding for your ShareFile site. You can customize the ShareFile site at any time.

   Access your ShareFile account at https://*subdomain*.ShareFile.com.

3. Provide your users with the information they need to get started.

   - If your deployment includes CloudGateway Enterprise, ShareFile services are automatically integrated with Receiver. That integration adds the Docs view to the main Receiver window. No user configuration is required. When a user logs on, they can view, edit, and share documents immediately.

- If your deployment does not include CloudGateway Enterprise, or if App Controller has not been configured to integrate ShareFile services with Receiver, instruct users to configure their ShareFile account manually.

Provide RSA SecurID Authentication for Android Devices

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

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

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

Configure email-based account discovery

You can configure 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, or AppController virtual appliance associated with the email address based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access their hosted applications, desktops, and data.

Note: Email-based account discovery is not supported if 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 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

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.

Try the Demonstration Site

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.

Troubleshooting Citrix Receiver for Android

Disconnected sessions

Users can disconnect from a Citrix Receiver session by pressing the Back button on the device.

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

Known issues for configuration with Access Gateway

- For Standard Edition, when configuring authentication realms, these formats are not supported:
  - realm\username
  - user@realm
- For Standard Edition, preauthorization is not supported. You must disable this feature for authentication to be successful.
- On devices running on Android 2.2, the Receiver fails to render the log-on page if the XenApp server is configured with Access Gateway Enterprise Edition. To prevent this issue, configure the Access Gateway for No Authentication so that authentication is handled by the XenApp server.

  Alternatively, install the Mozilla Firefox Web Browser for Android from the Android Market. From the Firefox browser, users can navigate to the Web Interface site and launch Citrix Receiver.

Color depth limitation for sessions

The Android does not support 8-bit color depth in sessions. Make sure that all GPOs requiring Android support are set to a minimum of 16-bit color depth.

Workspace control feature is not supported

If you use Receiver on a mobile device to connect to an application that is already launched from another Receiver, then the session is connected. However, Receiver for Android does not support the option to reconnect to an active session, a feature that is available when using Receivers on desktops.

Connecting with a proxy is not supported

Receiver cannot connect to networks with WiFi or LAN proxies.