Receiver for iOS 5.9.x - 5.8.x

2014-12-07 04:28:47 UTC

Contents

Receiver for iOS 5.9.x - 5.8.x

In this section

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

About Receiver for iOS 5.9.x - 5.8.x

What's new in 5.9.1

- Receiver for iOS now offers support for iOS 8.
- The Workspace Control feature is available in Settings > Advanced > Workspace Control.
- Launched applications can be previewed using the Switch button during a session.
- The ShareFile option in Settings > Advanced is no longer available. To use ShareFile, please download the Citrix ShareFile app from the App Store.

What's new in 5.9

- Receiver now offers smartcard support.* The following products and configurations are supported.
  - Supported readers:
    - Precise Biometrics Tactivo for iPad Mini
    - Precise Biometrics Tactivo for iPad (4th generation) and Tactivo for iPad (3rd generation) and iPad 2
    - BaiMobile® 301MP and 301MP-L Smart Card Readers
  - Supported smartcards:
    - PIV cards
    - Common Access Card (CAC)
  - Supported configurations:
    - Smartcard authentication to NetScaler Gateway with StoreFront 2.x and XenDesktop 5.6 and above or XenApp 6.5 and above.
- iOS 7.1 support.
- SHA2 Certificate support.
- Support for single FQDN access implementation.

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

What's new in 5.8.x

For the 5.8 release, we have made the following improvements on Receiver for your users:

- You can now directly interact with documents on your screen. You can scroll, pan, pinch, and zoom as you would in your host environments. You can also use application-specific gesture.

  This is available in Microsoft Windows 8 and Microsoft Windows Server 2012 environments and Mocrosoft Windows 7.

- You can use the new virtual mouse to perform left-click and right-click tasks, such as font and paragraph formatting and highlighting text in text editing applications. You can also zoom in and out of your entire screen by tapping the base of the mouse.

- Your listening and viewing experience is improved with smoother playback of audio and video clips because of various multimedia enhancements, including the following features:

  - **HDX Mediastream Windows Media Redirection** - When Windows Media Redirection is enabled and you view multimedia videos on the virtual desktop on your iOS user device, the videos are smoother. This is because the files are actually running on your device, rather than on the server. As a result, you do not need as much device bandwidth. Enable this feature on the Settings screen on the device.

  - **HDX H264 encoding support** - Webcam data can now be encoded by H264, which is one of the high-definition codecs. You can now watch videos in formats such as .wmv that were not previously available on an iOS user device.
- To use the features of the new HDX apps, you need to install Citrix Receiver on your device.

Issues fixed in 5.9

The following issues have been fixed since the previous release of this product:

- If you tap the Log On button after typing a password with a length of one character, you are unable to start a published application until you restart Receiver. [#395745]

- When using Receiver on a device running iOS 7, adding an application to the store and launching the application may cause Receiver to crash. [#443642]

- When you use Citrix Receiver on an iPad, opening an RSA token link from an email may result in Receiver crashing after it launches.[#443365]

- When you create a new store from Receiver and import a new client certificate for authentication, entering the certificate URL and selecting the installed certificate may result in the username field populating with the first and last name of the issued user instead of with username@domain. [#444021]

- When you add an account through Receiver, you may be unable to successfully continue past the certificate selection screen to reach the authentication prompt for LDAP. [#443641]

Issues fixed in 5.8.x

The following issues have been fixed since the previous release of this product:

- When working in Microsoft Excel, copying a cell associated with a formula imports the current value, but not the formula. As a workaround, set an ICA policy to disable "Client clipboard redirection" (enabled by default), and the formula is copied with the cell. [#350860]

- When working in a published Microsoft Internet Explorer app, swiping left or right moves the page content in the opposite direction. [#393461]

- On the Receiver for iOS device, when you reconnect to a disconnected session, the published app appears distorted and crunched. [#60990269]

- When session sharing is enabled on Receiver and you type an incorrect password under multiple accounts utilization, Receiver does not prompt with an error. [#61037499]

- When client clipboard mapping is enabled and you copy and paste specially formatted text in a Microsoft Windows Office application, the text is copied, but without the special formatting. [#60750254]

- After you launch a published Windows Internet Explorer app (iexplore.exe) on an iPad running Receiver for iOS 5.7.2, tap Switch in the in-session toolbar. When there is only one app to switch to, â€œ2â€* appears. [#61046027]

Known issues

- On the iPhone only, horizontal scrolling on the home screen is not available for the Store Web account. [#338903]

- On the extended keyboard in Microsoft Excel, tapping Ctrl or Shift does not select multiple spreadsheet cells. As a workaround, tap the current cell and drag your finger across adjacent cells to select them. [#339030]

- When configuring a new user account, there might be a delay in the appearance of the certificate enrollment page. [#339996]

- The RSA software token incorrectly requires that users enter their password and pin (instead of only the pin) every time they log on. [#350169]

- If you change the authentication type in Access Gateway after users have created an account, the new authentication profile is not saved and users might not be able to log on at all. [#350206]

- After you open an app that contains editable data, when you perform a three-finger tap, the virtual keyboard might not appear. As a workaround, on the toolbar, tap Keyboard. [#394204]

- While a streamed audio or video file in a published app on your desktop is running, if you change the Cellular Data setting on the Settings screen from ON to OFF and then ON again, the desktop no longer responds. [#387530]

- When you use both a smartcard store and a non-smartcard store, launching each store consecutively may result in the second launch failing. As a workaround, exit the Receiver app and restart before launching a new store type. [#452347]

- When you log in to your session without using smartcard authentication, you may be unable to use smartcard digital signing within the session. To prevent this issue, log in to your session using smartcard authentication when you plan to use signing within the session. [#457961]

- When you add an account using only the FQDN, the process may fail. To avoid this issue, enter the FQDN in the following format: https://FQDN, where *FQDN* is your FQDN address. [#458569]

- When you launch an app that you have not subscribed to, the session may hang without displaying a logon prompt. To prevent this issue, log on to the store first or subscribe to the app before launching. [#460159]

- If you see distortion or a black screen after starting a VDA or while working with the Control Center or Notification Center, refresh your session by tapping the device screen or by rotating the device. [#406877]

- When you add a store with the smartcard switch turned on, deleting the store and adding it again within 10 minutes may cause NetScaler to return an error message.

  To avoid this issue, wait 10 minutes before adding a deleted store again. [#466490]

- With Windows Media Redirection enabled (on the Settings screen), Citrix has the following suggestions to improve your viewing experience:

- When you play a video on the Windows Media Player on a virtual desktop and tap Home on the iOS device, when Receiver resumes, the video screen could be black. To resume the video, when Receiver resumes, tap the Pause button on the Windows Media Player. Then tap Play.

- Try Demo is not supported when using the keyboard to navigate on devices running iOS 7. To continue and configure the account, tap inside the email field. [#414965]

- To seek a new location in a video running in the Windows Media Player, tap the desired position on the progress bar, rather than dragging the icon to it. If you drag the icon to the new location, on rare occasions, a black screen appears. Tap the progress bar and the video should start playing again.

- For better results, maintain some free storage on the iOS device when you are using Windows Media Redirection. We suggest about 1 GB, depending on the size of the video.

System requirements for Receiver for iOS 5.9.x - 5.8.x

Device

- Citrix Receiver for iOS 5.9.x supports iOS 6.1.*x*, 7 and 8.
- Citrix Receiver 5.8.3 supports iOS 5.1.*x*, 6.1.*x*, and 7.
- Other versions of Citrix Receiver 5.8 support iOS 5.1.*x* and 6.1.*x*.
- This software update is supported on the following devices:
  - iPhone 4, 4S, 5, 5c and 5s. The only versions of receiver supported on iPhone 5c and 5s are Receiver for iOS 5.8.3 and 5.9.x.
  - All iPad models.
  - 5th generation iPod Touch.

Important: For information regarding secure connections to your Citrix environment, see **Connectivity** (below).

Server

Make sure you install all the latest hotfixes for your servers.

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

  StoreFront:

  - StoreFront 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 (browser-based access only)

      You must enable the rewrite policies provided by NetScaler.

- **XenDesktop** and **XenApp** (any of the following products):
    - Citrix XenDesktop 4, 5, 5.5, 5.6, 7, 7.x, and 7.5
    - Citrix XenApp 7.5
    - Citrix XenApp 6.5 for Windows Server 2008 R2
    - Citrix XenApp 6 for Windows Server 2008 R2
    - Citrix XenApp Fundamentals 6.0 for Windows Server 2008 R2
    - Citrix XenApp 5 for Windows Server 2008
    - Citrix XenApp 5 for Windows Server 2003
    - Citrix Presentation Server 4.5
- VDI-in-a-Box 5.2.*x* and 5.3.*x*

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 using StoreFront services

      Single sign-on to Web and SaaS apps published through App Controller requires StoreFront.

    - Web Interface 5.4 for Windows, using Web Interface Sites (not supported for XenDesktop 7 deployments)

  For information about domain-joined and non-domain-joined devices, see the XenDesktop 7 documentation.

- For secure remote connections, any of the following products:
    - Citrix NetScaler Gateway 10
    - Citrix Access Gateway Enterprise Edition 9.*x*, and 10.*x* (CloudGateway is supported only with versions 9.3 and higher)
    - Citrix NetScaler Gateway VPX
    - Citrix Secure Gateway 3.*x* (supported with XenApp Services sites on Web Interface only)

For information about the NetScaler Gateway and Access Gateway versions supported by StoreFront, see the NetScaler Gateway, Access Gateway, and StoreFront documentation in eDocs.

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 device 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, applications fail to start.

Import root certificates on iPad and iPhone devices

Obtain the root certificate of the certificate issuer and email it to an email account configured on your device. When clicking the attachment, you are asked to import the root certificate.

Wildcard certificates

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

Intermediate certificates and the NetScaler Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the NetScaler Gateway (or Access Gateway) server certificate. For information about installing intermediate certificates in the NetScaler Gateway or on the Access Gateway, see the documentation in eDocs. Additionally, for Access Gateway installations, see the Knowledge Base article that matches your edition:

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

See also:

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

Authentication

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

Receiver supports all authentication methods supported by Access Gateway. For information about authentication, see the NetScaler Gateway (or Access Gateway)

documentation and the "Manage" topics in the StoreFront documentation in eDocs. For information about other authentication methods supported by Web Interface, see Configuring Authentication for the Web Interface in the Web Interface documentation.

Availability of Receiver for iOS 5.8 features

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

- XenDesktop 5.6 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 XenApp deployment. There are two types of Web Interface sites: XenApp Services (formerly Program Neighborhood Services) sites and XenApp Web sites. Web Interface sites enable client devices to connect to the server farm. Authentication between Receiver and a Web Interface site can be handled using a variety of solutions, including Citrix Access Gateway and Citrix Secure Gateway.

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 iOS

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

- When publishing applications on your farms or sites, consider the following options to enhance the experience for users accessing those applications through StoreFront stores.
  - Ensure that you include meaningful descriptions for published applications because these descriptions are visible to users in Citrix Receiver.
  - You can emphasize published applications for your mobile device users by listing the applications in the Featured list of Citrix Receiver. To populate this list on Citrix Receiver, edit the properties of applications published on your servers and append the KEYWORDS:Featured string to the value of the Application description field.
  - To enable the screen-to-fit mode that adjusts the application to the screen size of mobile devices, edit the properties of applications published on your servers and append the KEYWORDS:mobile string to value of the Application description field. This keyword also activates the auto-scroll feature for the application.
  - To automatically subscribe all users of a store to an application, append the KEYWORDS:Auto string to the description you provide when you publish the application in XenApp. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.

  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. The name of the site and how you create it depends on the version of the Web Interface you have installed. For instructions on how to create one of these sites, see the "Creating Sites" topic for your version of the Web Interface.

To configure StoreFront for Citrix Receiver for iOS

To configure StoreFront

Important:

- Only Citrix Access Gateway Enterprise Edition 9.3 and 10.0 are supported by Receiver for iOS 5.6 and 5.7 when using StoreFront.
- Receiver for iOS supports only XenApp Services sites on Web Interface.
- Legacy mode is no longer required for StoreFront in any configuration scenario.
- Receiver for iOS 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 iOS.
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, see 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 configuring newer versions of App Controller, see the XenMobile section of eDocs. For older versions of App Controller (such as version 1.2), see the Archive section of 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 and 10.0 Enterprise Edition and Access Gateway 5.0.4 are supported by Receiver for iOS 5.6 or 5.7 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.

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

To configure client certificate authentication for mobile devices

Important:

- Access Gateway Enterprise Edition 9.*x* and 10.*x* are supported by Receiver for iOS 5.5 and 5.6 using XenApp Services sites.
- Client certificate authentication is supported by Receiver for iOS 5.5, 5.6, and 5.7.
- Only Access Gateway Enterprise Edition 9.*x* and 10.*x* support client certificate authentication.
- Double-source authentication types must be CERT and LDAP.
- Receiver also supports optional client certificate authentication.
- Only P12 formatted certificates are supported.

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

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

When users log on to the Access Gateway virtual server, after authentication, the user name information is extracted from the specified field of the certificate. Typically, this field is `Subject:CN`. If the user name is extracted successfully, the user is then authenticated. If the user does not provide a valid certificate during the Secure Sockets Layer (SSL) handshake or if the user name extraction fails, authentication fails.

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

To configure the XenApp Services site

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

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.

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

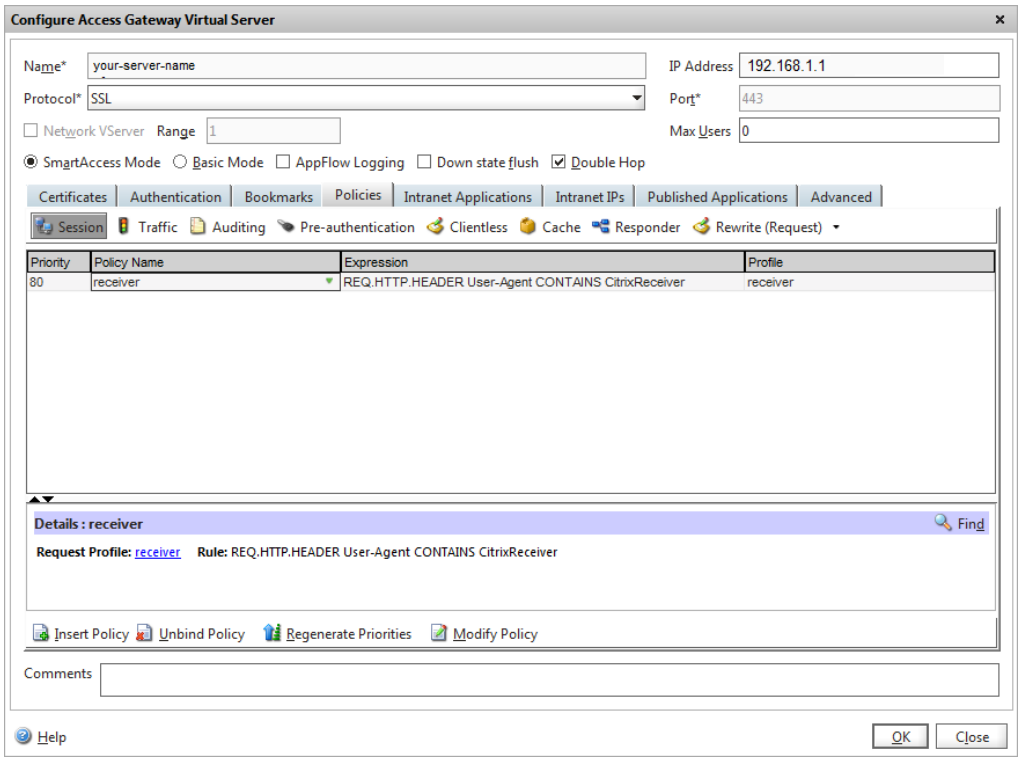
1. In the XenApp Services site, select Manage secure client access > Edit secure client access settings.
2. Change the Access Method to Gateway Direct.
3. Enter the FQDN of the Access Gateway appliance.
4. Enter the Secure Ticket Authority (STA) information.

To configure the Access Gateway appliance

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

1. Create a session policy on the Access Gateway to allow incoming XenApp connections from the Receiver, and specify the location of your newly created XenApp Services site.
   - Create a new session policy to identify that the connection is from the Receiver for mobile devices. As you create the session policy, configure the following expression and select Match All Expressions as the operator for the expression:

     REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver



- In the associated profile configuration for the session policy, on the Security tab, set Default Authorization to Allow.

  On the Published Applications tab, if this is not a global setting (you selected the Override Global check box), ensure the ICA Proxy field is set to ON.

  In the Web Interface Address field, enter the URL including the config.xml for the XenApp Services site that the device users use, such as http://XenAppServerName/Citrix/PNAgent/config.xml or http://XenAppServerName/CustomPath/config.xml.

- Bind the session policy to a virtual server.

- Create authentication policies for Cert and LDAP.

- Bind the authentication policies to the virtual server.

- Configure the virtual server to request client certificates in the SSL handshake (on the Certificate tab, open SSL Parameters, and for Client Authentication, set Client Certificate to Mandatory.

Important: If the server certificate used on the Access Gateway is part of a certificate chain (with an intermediate certificate), 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

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

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

2. Users can either install a new certificate or select one from the already installed certificate list. For iOS client certificate authentication, the certificate must be downloaded and installed by the Receiver application only.

3. After selecting a valid certificate, the user-name field on the logon screen is prepopulated using the user-name information from the certificate, and users enter the remaining details, including password and domain information for domain authentication.

4. If client certificate authentication is set to optional, users can skip the certificate selection by pressing the Back button on the certificates page. In this case, Receiver

proceeds with the connection and provides the user with the logon screen.

5. After users complete the initial logon, they can launch applications without providing the certificate again. Receiver stores the certificate for the account and uses it automatically for future logon requests.

To configure the Secure Gateway for Citrix Receiver for iOS

To configure the XenApp Services site

Important:

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

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

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

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

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

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

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

To configure the Secure Gateway

1. On the Secure Gateway, use the Secure Gateway Configuration wizard to configure the Secure Gateway to work with the server in the secure network hosting the XenApp Service site. After selecting the Indirect option, enter the FQDN path of your Secure Gateway Server and continue the wizard steps.

2. Test a connection from a user device to verify that the Secure Gateway is configured correctly for networking and certificate allocation.

To configure the mobile device for the Receiver application

1. Open Account Settings, and in the Address field, enter the matching FQDN of your Secure Gateway server:

   - If you created the XenApp Services site using the default path (/Citrix/PNAgent), enter the Secure Gateway FQDN: `FQDNofSecureGateway.companyName.com`

   - If you customized the path of the XenApp Services site, enter the full path of the config.xml file, such as: `FQDNofSecureGateway.companyName.com/CustomPath/config.xml`
2. In the Citrix Access Gateway settings, turn off Access Gateway.

To configure Access Gateway Enterprise Edition for Citrix Receiver for iOS

Important:

- Access Gateway Enterprise Edition 9.*x* and 10.*x* are supported by Receiver for iOS using XenApp Services sites or Legacy mode on StoreFront servers.
- Access Gateway Enterprise Edition 9.*x* and 10.*x* are supported by Receiver for iOS using XenApp Web Sites.
- Receiver for Web is not supported by Receivers for iOS.
- Access Gateway Enterprise Edition 9.*x* and 10.*x* are supported by Receiver for iOS 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, see 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
- Configuring Secure Browse in Access Gateway (iOS devices only, not needed for Android devices)
- Allowing Access from Mobile Devices
- MDX Toolkit for Mobile Apps
- Provide ShareFile services to Receiver users

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 4.6.x for Citrix Receiver for iOS

To configure the XenApp Services site

Important:

- Access Gateway Standard Edition 4.6.*x* is supported by Receiver for iOS using XenApp Services sites.
- Access Gateway Standard Edition 4.6.*x* is supported by Receiver for iPad 4.2.*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).

Note: You must use the Citrix default path for the XenApp Services site.

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, SMS authentication (http://smspasscode.com) (iPhone and iPad only), and RSA SecurID are supported authentication methods for Receiver for mobile devices:

   - 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 for Citrix Receiver for iOS

To configure the Web Interface site

Important:

- To use mobile devices with Access Gateway 5.0 through a XenApp Services site, you must update to version 5.0.2 or higher; see To configure Access Gateway 5.x to use a XenApp Services site.
- Access Gateway 5.0 is supported only by Receiver for iPad 4.2 or higher. Also, it is supported only for XenApp Web site configurations.
- You must use the Web Interface 5.4, which is supported by all built-in browsers.

When you configure Access Gateway for mobile devices, you configure a basic or a SmartAccess logon point on Access Gateway and use the Web address for the XenApp Services site.

Before you configure a logon point, install the Web Interface and verify that it is communicating with the network. When you configure a logon point, you must also configure at least one Secure Ticket Authority (STA) server and ICA Access Control in Access Gateway. For more information, expand Access Gateway 5.0 in eDocs, and locate the topic *To configure Access Gateway to use the Secure Ticket Authority*.

Note: Users with mobile devices can launch applications through your Web Interface site and the built-in browser within Receiver or the browser provided by the operating system on the mobile device. Configure the Web Interface site just as you would for other XenApp applications. No special configuration is needed for mobile devices.

To configure the Access Gateway 5.0 appliance

1. Configure Authentication profiles to authenticate users connecting to the Access Gateway using the Receiver.

   Active Directory authentication, SMS authentication (http://smspasscode.com) (iPhone and iPad only), and RSA SecurID are supported authentication methods for Receiver for mobile devices:

   - If double source authentication is required (such as Active Directory and RSA SecurID), Active Directory authentication must be the primary authentication type. RSA SecurID authentication must be the secondary authentication type.
   - RSA SecurID can use either RADIUS or an sdconf.rec file to enable token authentication.
   - You can configure Active Directory authentication on Access Controller. You can use Active Directory on the Access Gateway appliance by using either an LDAP or RADIUS authentication profile.

   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 the Access Gateway with STA servers and the ICA Access Control list on Access Gateway. For more information, see the Access Gateway section of eDocs.

3. Configure logon points on the Access Gateway. Configure the Access Gateway to allow incoming XenApp connections from the Receiver, and specify the location of your Web Interface site.

   a. In the Access Gateway Management Console, click Management.

   b. Under Access Control, click Logon Points > New.

   c. In the Logon Points Properties dialog box, in Name, type a unique name for the logon point.

   d. Select the Type:

      - For a Basic logon point, in the Web Interface field, type the fully qualified domain name (FQDN) of the Web Interface, such as `http://xenapp.domain.com/citrix/mobile`. You cannot configure a SmartGroup with a basic logon point. Select the authentication type, or click Authenticate with the Web Interface.

        If you select Authenticate with the Web Interface, when users type the URL to Access Gateway and enter credentials, the credentials are passed to the Web Interface for authentication.

      - For a SmartGroup to use the settings in a SmartAccess logon point, you must select the logon point within the SmartGroup. Select the authentication profiles. If you configure a SmartAccess logon point, Access Gateway authenticates users. You cannot configure authentication by using the Web Interface.

If you select Single Sign-on to Web Interface, users do not have to log on to the Web Interface after logging on to the Access Gateway. If not selected, users must log on to both the Access Gateway and Web Interface.

e. Under Applications and Desktops, click Secure Ticket Authority and add the STA details. Make sure the STA information is the same as the Web Interface site.

f. Finally, under Applications and Desktops, click XenApp or XenDesktop to add the ICA control list (required for Access Gateway 5.0). For more information, expand Access Gateway 5.0 in eDocs, and locate *To configure ICA Access Control*.

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 section on *Configuring Intermediate Certificates*.

To configure Access Controller

1. Configure Authentication profiles to authenticate users connecting to the Access Gateway using the Receiver.

   Active Directory authentication, SMS authentication (http://smspasscode.com) (iPhone and iPad only), and RSA SecurID are supported authentication methods for Receiver for mobile devices:

   - If double source authentication is required (such as Active Directory and RSA SecurID), Active Directory authentication must be the primary authentication type. RSA SecurID authentication must be the secondary authentication type.
   - RSA SecurID can use either RADIUS or an sdconf.rec file to enable token authentication.
   - You can configure Active Directory authentication on Access Controller. You can use Active Directory on the Access Gateway appliance by using either an LDAP or RADIUS authentication profile.

   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 Controller to recognize the servers. Configure Access Controller to allow incoming XenApp connections from the Receiver and specify the location of your Web Interface site.

   a. In the Deliver Services Console, expand Citrix Resources > Access Gateway, and then click the Access Controller on which you want to create the Web resource.

   b. Expand Resources, click Web Resources, and then under Common tasks, click Create Web resource. In the wizard, enter a unique name. On the New Web Address page, enter the Web address URL of the XenApp Web site.

   c. In **Application type**, select Citrix Web Interface and click the Enable Single Sign-on check box.

   d. After you click OK, click Publish for users in their list of resources , and then in Home page, enter the URL of the XenApp Web Site, such as `http://xenapp.domain.com/citrix/mobile`, and finish the wizard.

   e. In the navigation pane, click Logon Points, click Create logon point, and in the wizard, enter a unique name, and select the type:

      - For a Basic logon point, in the Web Interface field, type the fully qualified domain name (FQDN) of the Web Interface, such as `http://xenapp.domain.com/citrix/mobile`. Select the Home page, and then select the authentication profile. Leave the remaining options as default values, and click Enable this logon point check box at the end of the wizard.
      - For a SmartAccess logon point, on Select Home Page, select the Display the Web resource with the highest priority. Click Set Display Order, and move the Web Interface Web resource to the top.

Select the Authentication Profiles for both authentication and group extraction. Leave the remaining options as default values, and click Enable this logon point check box at the end of the wizard.

f. In the navigation pane, under Policies > Access Policies, select Create access policy and on the Select Resources page, expand Web Resources to select the Web Interface web resource.

g. In Configure Policy Settings, select the settings, click Enable this policy to control this setting, and select Extended access, unless denied by another policy. Add the users allowed to access this resource and finish the wizard.

h. In the navigation pane, under Access Gateway appliances, select Edit Access Gateway appliance properties, click Secure Ticket Authority and add the STA details. Make sure the STA information is the same as the Web Interface site.

i. Finally, click ICA Access Control to add the ICA control list (required for Access Gateway 5.0). For more information, expand Access Gateway 5.0 in eDocs, and locate *To configure ICA Access Control* in the Access Controller documentation.

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 section on *Configuring Intermediate Certificates*.

To launch Receiver applications on the mobile device

1. Install the Receiver application on the device.

2. Launch published applications by using one of the following methods (some mobile devices have slight differences):

   - Launch the Receiver application on the device, and create an account by entering the matching FQDN of your Access Gateway server (including Logon Point, if applicable), and Receiver auto-configures the account to use Receiver's built-in browser to launch applications.

   - Launch the Web browser provided by the operating system of the mobile device, and log on to your organization's Web Interface site to access your applications.

     Note: With this method on iOS devices, users are prompted each time to open the launched application in Citrix. You cannot disable this feature.

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

Important:

- Access Gateway 5.*x* is supported by Receiver for iPad 4.2 and Receiver for iOS 5.0 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.x for Citrix Receiver for iOS. 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 iOS 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 iOS device

1. On the mobile 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 iOS

To configure the Web Interface site

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

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

To launch applications on the iOS device

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

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 AppController 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 AppController Management Console, configure the ShareFile settings. For more information, see *To configure settings for iOS mobile apps* in the AppController documentation.

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

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 *Customize the 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 AppController has not been configured to integrate ShareFile services with Receiver, instruct users to configure their ShareFile account manually.

- For Receiver for iOS 5.6 users only, you must also enable Shared Documents, located in Settings > Advanced.

To configure accounts manually for Citrix Receiver for iOS

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

To configure accounts manually

1. Tap the Accounts icon in the upper right corner and then in the Accounts screen, tap the Plus Sign (+). The New Account screen appears.

2. In the lower left corner of the screen, tap the icon to the left of Options and tap Manual setup. Additional fields appear on the screen.

3. In the Address field, type the secure URL of the site or Access Gateway to which you want to connect (for example, agee.mycompany.com).

4. Select one of the following connection options. The remaining fields on the screen change, depending on your selection.

   - Web Interface - Select for Receiver to display a XenApp Web site similar to a Web browser. This is also known as Web View.

   - XenApp Services - Select for Receiver to locate a specific XenApp Services site for which authentication through Access Gateway is not configured. In the additional options that appear on this screen, provide site logon credentials.

   - Access Gateway - Select for Receiver to connect to a XenApp Services site through a specific Access Gateway. In the additional options on this screen, select the server edition and its logon credentials, including whether it requires a security token for authentication.

5. For certificate security, use the setting in the Ignore certificate warnings field to determine whether you want to connect to the server even if it has an invalid, self-signed, or expired certificate. The default setting is OFF.

   Important: If you do enable this option, make sure you are connecting to the correct server. Citrix strongly recommends that all servers have a valid certificate to protect user devices from online security attacks. A secure server uses an SSL certificate issued from a certificate authority. Citrix does not support self-signed certificates and does not recommend by-passing the certificate security.

6. Tap Save.

7. Type your user name and password (or token, if you selected two-factor authentication), and then tap Log On. The Citrix Receiver screen appears, in which you can access your desktops and add and open your apps.

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

To install RSA SecurID soft tokens

An RSA SecurID soft token 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.

For the iPad only, attach the .sdtid file in an email, open the email on the iPad, and run the file to install the token.

For the iPhone, iPod Touch, or iPad, follow these general steps:

1. On a computer (not a mobile device), download the converter tool from: http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/converter.htm. Follow the instruction
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 soft token is installed on the device, a new option appears in the Settings tab to manage the token.

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

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

Provide access information to end users for iOS devices

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 an auto-generated setup URL
- 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 Configure 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 an auto-generated setup URL

You can use the Setup URL Generator to configure Receiver for mobile devices. After installing Receiver, users simply click on the URL to configure their account and access their resources. Use the utility to configure settings for accounts and email or post that information to all your users at once.

For more information, see To configure mobile devices automatically.

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.

Session sharing

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

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

To configure mobile devices automatically

Use the Citrix Mobile Receiver Setup URL Generator on a PC or Mac to expedite configuring the Citrix Receiver for applicable mobile devices. Use the utility to configure settings for XenApp accounts and email the configurations to many devices at once.

Because the username and password are entered by the user, the configuration requires only the server name, server address, domain name, and Access Gateway information (if applicable).

1. From a PC or Mac, open the Mobile Receiver Setup URL Generator from http://community.citrix.com/MobileReceiverSetupUrlGenerator/.
2. For Account Description, enter the name for the account, such as the group or department, for example, Production or Sales.
3. For Server Address, type the address of your XenApp server farm, for example, gateway.myserverfarm.net.
4. For Domain, type the domain name of the server farm to which you are connecting your users.
5. To enable an Access Gateway configuration, select the Use Gateway check box.
    a. Under Gateway type, choose the Access Gateway edition deployed in server farm to which you are connecting your users. (If you do not know the correct edition, contact your administrator.)
    b. Under Gateway Authentication Type, choose the authentication method used in your infrastructure.
6. Click Generate URL.
7. In Your Result, click configuration link, and copy the generated link.

Use email to send the link directly to mobile devices for users to complete their configuration account for the Receiver on the device.

Important: Some BlackBerry devices require a plain-text formatted email to properly associate the pre-configured URL with the Receiver. Therefore, it is recommended that the URL is always sent as a plain-text formatted email message to BlackBerry users.

Save Passwords

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

- 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.

Troubleshoot Citrix Receiver for iOS

Disconnected sessions

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

- Pressing the home button on their mobile device.
- Tapping Home or Switch in the app's drop-down menu.

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

Issues with numeric keys in applications

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

Loss of HDX audio quality from XenDesktop

From XenDesktop, HDX audio to Receiver for iOS might lose quality when using audio plus video. This issue occurs when the XenDesktop HDX policies cannot handle the amount of audio data with the video data. For suggestions about how to create policies to improve audio quality, see http://support.citrix.com/article/ctx123543.

Demonstration accounts available from the Citrix Cloud

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

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

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

Expired passwords

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

Slow connections

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

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

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

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 iOS 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.

Applications might open in different sessions

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