Citrix Receiver for iOS 5.9

Jun 05, 2015

PDF

Receiver for iOS URI for Opening Applications

You can use the Receiver for iOS Uniform Resource Indicator (URI) scheme specified in this document to programmatically open applications published on XenApp, XenDesktop, and StoreFront.

About Citrix Receiver for iOS 5.9.x

Oct 27, 2015

> **Important**
>
> Citrix Receiver for iOS 5.9.x does not support iOS 9. If you have upgraded your device to iOS 9, please upgrade Citrix Receiver to the most recent version.
>
> To upgrade, go to the Citrix download pages: http://www.citrix.com/downloads/citrix-receiver/ios/receiver-for-ios.html.

Receiver for iOS 5.9.6

This release fixes an issue with Bluetooth keyboard interoperability.

Receiver for iOS 5.9.5

What's new

- **X1 Mouse**. You can connect and use the Citrix X1 Mouse within Citrix HDX Sessions. Currently, Receiver only supports one mouse model.
  - To connect and enable the mouse, go to Receiver Settings and toggle **X1 Mouse**.
  - For left-handed users, you can switch the mouse buttons. Go to Receiver Settings and toggle **Left-handed mouse**. Or, from the Windows Control Panel, go to Mouse Properties.

  For details about the Citrix X1 Mouse, see http://www.citrix.com/products/mouse/overview.html.
- **Enhanced external display support**. Receiver for iOS supports external display with iPhone and iPads.
  - To enable external displays, go to Citrix Receiver Settings > Display Options and toggle on **External Display**.
  - External display functionality is available through the following methods:
    - AirPlay
    - Lightning to VGA adapter
    - Lightning Digital AV Adapter

      Note: Lightning Digital AV Adapter has not been tested.
  - External display is not recommended for older iPads (non-Air models) and iPhones (5c and earlier) due to the high processing requirements.
- **Touchpad/Presentation mode – Preview**. You can use an iPad as if it is a keyboard and touchpad when connected with external display, like AppleTV or Lightning to HDMI cable, instead of using a Bluetooth keyboard.
  - To enable presentation mode, go to Citrix Receiver Settings > Display Options and toggle on **External Display** and **Presentation Mode**.
  - Touchpad/Presentation mode is compatible with X1 Mouse.
  - This a preview of Touchpad/Presentation mode and is not for production use.

Fixed issues

- Keyboard states event changes are incorrectly returned for Citrix Mobility Pack. [#522269]
- The session resolution screen is incorrectly sized when using Auto-fit mode on a Citrix Mobility Pack enhanced application. [#545325]
- The session screen cannot be easily scrolled. [#545324]

Receiver for iOS 5.9.4

What's new

- Support for TLS 1.0, 1.1 and 1.2. You can change your environment to use all three. Receiver for iOS uses 1.2 if available, then 1.1, then falls back to TLS 1.0.
- Improved graphics for iPhone 6 Plus and other retina phones.
  - High-resolution sessions can be launched by using the Auto-fit Screen option in Settings > Display Options.

Fixed issues

- Mobility SDK now returns the value **5** for device **orientationFaceUp** and the value **6** for device **orientationFaceDown**.
- A color corruption issue occurs.
- A 3D Pro frame drop issue occurs.
- An iPad black magnifier glass issue occurs.

Receiver for iOS 5.9.3

What's new

- Improved user experience when reconnecting to a session via Worx Home.

Fixed issues

- When using a full-screen, published Remote Desktop Protocol (RDP) session inside an ICA session, no upper-case characters are sent.
- An intermittent issue with on-screen keyboard occurs.
- App Switcher Resolution issues occur.
- Minor graphics corruption occurs when rotating the device.
- An occasional issue occurs with the launch of a desktop through NetScaler.

Receiver for iOS 5.9.2

What's new

- Resolution of "black screen" issues experienced in previous releases.
- Resolution of Mobility SDK-related issues.
- Adds an option to enable keyboard extensions, which is a security update.
- To prevent a new attack, such as POODLE, against the SSLv3 protocol, this version of Receiver for iOS disables its use. For details, see CTX 200238.
  Note: You must ensure that TLS 1.0 is enabled.

Receiver for iOS 5.9.1

What's new

- Support for iOS 8.
- Restored Siri dictation with Citrix Receiver.
- You can access more than one application at a time and can switch between apps with the swipe of a finger. The in-session App Switcher starts automatically when you open a second app in the same Windows session. You can swipe from the edge of the screen to select the next running published app. To use this feature, the apps must be published by the IT administrator on the same server.

- The Workspace Control feature is available in **Settings > Advanced > Workspace Control**.
- Advanced logging is enabled to gather diagnostic data for authentication, store, and connection issues. You can find the logging options in **Settings > Support > Log Options**.
- The ShareFile option in **Settings > Advance** is no longer available. To use ShareFile, download the Citrix ShareFile app from the App Store.

Note: When the "Automatic Keyboard Display" policy is enabled via Citrix policy, you will need two taps on the text (input) area to show the on-screen keyboard.

Receiver for iOS 5.9

What's new

- Receiver offers limited smart card support.
  Note: Customers using FIPS NetScaler devices should configure their systems to deny SSL renegotiations. For details, see How to configure the -denySSLReneg parameter.
  The following products and configurations are supported.
  - Supported readers:
    - Precise Biometrics Tactivo for iPad Mini Firmware version 3.8.0
    - Precise Biometrics Tactivo for iPad (4th generation) and Tactivo for iPad (3rd generation) and iPad 2 Firmware version 3.8.0
    - BaiMobile® 301MP and 301MP-L Smart Card Readers

    Supported VDA Smart Card Middleware
    - ActiveIdentity
  - Supported smartcards:
    - PIV cards
    - Common Access Card (CAC)
  - Supported configurations:
    - Smartcard authentication to NetScaler Gateway with StoreFront 2.x and XenDesktop 5.6 and later or XenApp 6.5 and later.

- iOS 7.1 support
- SHA2 certificate support
- Support for single FQDN access implementation

Issues fixed in 5.9 - 5.9.x

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

- After you open an app that contains editable data, when you perform a three-finger tap, the virtual keyboard might not appear. [#394204]
- 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]
- With Windows Media Redirection enabled (on the Settings screen), Citrix had the following suggestions to improve your viewing experience. In 5.9.x, these workarounds are no longer required:
  - 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.
  - 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.

- If you tap the Log On button after typing a password with a length of one character, you cannot 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 fail. [#443642]
- When you use Citrix Receiver on an iPad, opening an RSA token link from an email may result in Receiver failing 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 continue past the certificate selection screen successfully to reach the authentication prompt for LDAP. [#443641]

Known issues

- When a new password is set, an "Incorrect Credentials" error appears. Although the error message appears, the new password is correctly set. The error message can be ignored. Use the new password at next logon process. [#70576123]
- Performance might degrade when using external displays with a resolution higher than 720 pixels.
- The X1 Mouse might not be able to be paired to another device until using the Forget this device option from iOS Bluetooth settings.
- The X1 Mouse might not interact with application icons on the application launch screen. [#560429]
- Audio might not play to an AirPlay device. [#55671]
- The X1 Mouse might not interact with the session toolbar during a session. [#554469]
- The following issue occurs when connecting to a virtual desktop session of XenDesktop: Connect to the virtual desktop and then open Internet Explorer and navigate to a site with text input forms. The touch keyboard appears as expected; however, when users disconnect and then reconnect to the virtual desktop, the touch keyboard no longer appears automatically. The workaround is to use a three-finger tap on the screen to open the touch keyboard. [#461011]
- 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 NetScaler 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]
- 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 smart card store and a non-smart card 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 smart card 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]
- 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:
  - 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]
  - 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

May 11, 2015

Device

> ### Important
>
> Citrix Receiver for iOS 5.9.x does not support iOS 9. If you have upgraded your device to iOS 9, please upgrade Citrix Receiver to the most recent version.
>
> To upgrade, go to the Citrix download pages: http://www.citrix.com/downloads/citrix-receiver/ios/receiver-for-ios.html.

- Citrix Receiver for iOS 5.9.x supports iOS 6.1.x, 7 and 8.
- This software update is supported on the following devices:
  - iPhone 4, 4S, 5, 5c, 5s, 6 and 6 Plus. The only versions of receiver supported on iPhone 5c and 5s are Receiver for iOS 5.9 and 5.9.x.
  - All iPad models.
  - 5th generation iPod Touch.
- External display support
  - iPhone - none.
  - iPad - as supported by iOS (does not use the whole screen).

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 2.6 (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 Safari web browser. Users must manually open the ICA file using the browser Open in Receiver function. For the limitations of this deployment, see the StoreFront documentation.

  Web Interface:
  - Web Interface 5.4 with Web Interface sites
  - Web Interface 5.4 with XenApp Services sites
  - Web Interface on NetScaler (browser-based access only using Safari)
    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, 7.5, and 7.6
  - Citrix XenApp 7.5 and 7.6
  - 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 and authentication

For connections to StoreFront, Receiver supports the following authentication methods:

	Receiver for Web using browsers	**StoreFront Services site (native)**	**StoreFront XenApp Services site (native)**	**NetScaler to Receiver for Web (browser)**	**NetScaler to StoreFront Services site (native)**
Anonymous	Yes	Yes			
Domain	Yes	Yes	Yes	Yes*	Yes*
Domain pass-through	Yes	Yes	Yes		
Security token				Yes*	Yes*
Two-factor (domain with security token)				Yes*	Yes*
SMS				Yes*	No
Smart card	Yes	Yes		Yes*	Yes*
User certificate				Yes (NetScaler Gateway Plugin)	Yes (NetScaler Gateway Plugin)

*Available only for Receiver for Web sites and for deployments that include NetScaler Gateway, with or without installing the associated plug-in on the device.

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

For connections to the Web Interface 5.4, Receiver supports the following authentication methods:
Note: Web Interface uses the term Explicit to represent domain and security token authentication.

	Web Interface (browsers)	**Web Interface XenApp Services site**	**NetScaler to Web Interface (browser)**	**NetScaler to Web Interface XenApp Services site**
Anonymous	Yes			

Domain Domain pass-through	Yes Yes	Yes	Yes*	
Security token			Yes*	
Two-factor (domain with security token)			Yes*	
SMS			Yes*	
Smart card**	Yes			
User certificate			Yes (Require NetScaler Gateway Plugin)	

About secure connections and certificates

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:

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

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.

Smart Cards

- Receiver offers limited smart card support.
  Note: Customers using FIPS NetScaler devices should configure their systems to deny SSL renegotiations. For details, see How to configure the -denySSLReneg parameter.
  The following products and configurations are supported.
  - Supported readers:
    - Precise Biometrics Tactivo for iPad Mini Firmware version 3.8.0
    - Precise Biometrics Tactivo for iPad (4th generation) and Tactivo for iPad (3rd generation) and iPad 2 Firmware version 3.8.0
    - BaiMobile® 301MP and 301MP-L Smart Card Readers

    Supported VDA Smart Card Middleware
    - ActiveIdentity
  - Supported smartcards:
    - PIV cards
    - Common Access Card (CAC)
  - Supported configurations:
    - Smartcard authentication to NetScaler Gateway with StoreFront 2.x and XenDesktop 5.6 and later or XenApp 6.5 and later.

Configure your environment

Apr 13, 2015

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.

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.

Configure StoreFront

Apr 13, 2015

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.
- Receiver for iOS supports launching sessions from Receiver for Web, provided that the web browser will work with Receiver for Web. If launches do not occur, please configure your account through Receiver for iOS directly. Users must manually open the ICA file using the browser Open in Receiver function. For the limitations of this deployment, see the StoreFront documentation.

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Receiver. Create stores that enumerate and aggregate desktops and applications from XenDesktop sites and XenApp farms, making these resources available to users.

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 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.

Configure client certificate authentication

Apr 13, 2015

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, 5.7, and 5.9.
- 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 TLS 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

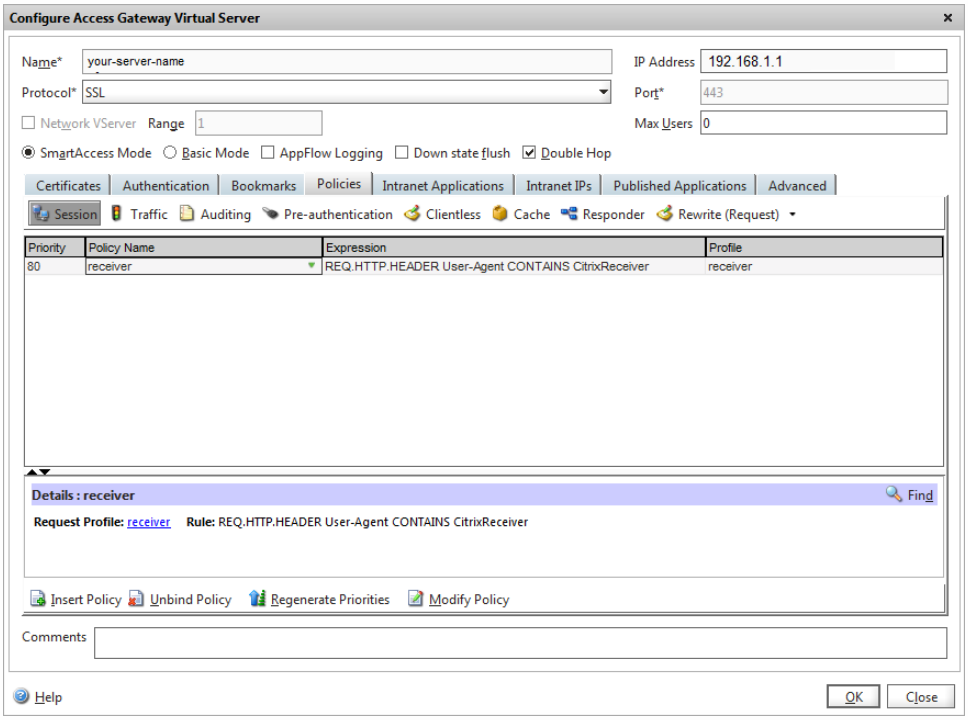
authentication policies: Cert and LDAP. For details, refer to your version of the Access Gateway Enterprise Edition (9.x only) or Access Gateway 10 in eDocs and search for the topic:

— 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 TLS 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.

Configure Secure Gateway

Apr 13, 2015

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.

Configure Access Gateway Enterprise Edition

Apr 13, 2015

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 StoreFront. The method for enabling access depends on the edition of CloudGateway in your deployment:

- 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

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.

Configure Web Interface

Apr 13, 2015

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.

Configure Accounts manually

Apr 13, 2015

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.
     - http://<StoreFront FQDN>: If there are multiple stores, a list will be presented and the user can choose the store to add.
     - http://<StoreFront FQDN>/citrix/<Store Name>: This will add the StoreFront store <Store Name>.
     - http://<StoreFront FQDN>/citrix/PnAgent/config.xml: This will add the default legacy PNAgent store.
     - http://<StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml: This will add the legacy PNAgent store associated with <Store Name>.
   - 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

Aug 12, 2015

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

For instructions to configure RSA SecurID authentication on NetScaler Gateway, see:

- Configuring RSA SecurID Authentication on NetScaler Gateway 11.0
- Configuring RSA SecurID Authentication on NetScaler Gateway 10.5
- Configuring RSA SecurID Authentication on NetScaler Gateway 10.1

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.

To import an RSA SecurID soft token into Citrix Receiver

To use an RSA Soft Token with the Citrix Receiver, have your users follow this procedure.

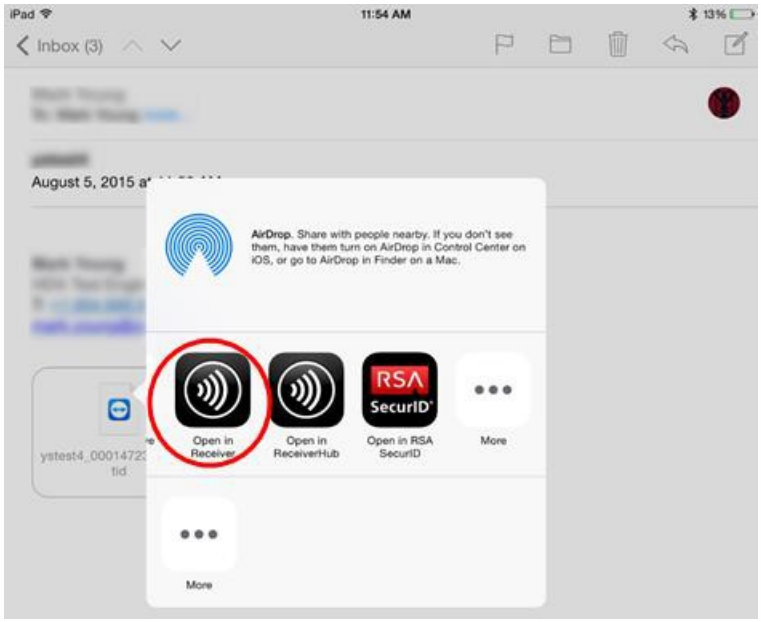
The policy for PIN length, type of PIN (numeric only, alphanumeric), and limits on PIN reuse are specified on the RSA administration server.

Your users should only need to do this once. After your users have successfully authenticated with RSA server. After they verify their PINs, they are are also authenticated with the StoreFront server, and it presents available published applications and desktops.

To use an RSA soft token with Citrix Receiver

1. Import the RSA soft token provided to you by your organization.

From the email with your SecurID file attached, select **Open in Receiver** as the import destination.



After the soft token is imported, Citrix Receiver opens automatically.

2. If your organization provided a password to complete the import, enter the password provided to you by your organization and click **OK**.

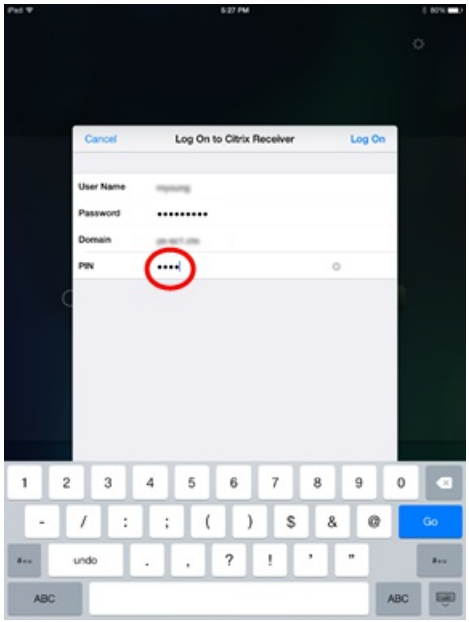
After clicking **OK**, you will see a message that the token was successfully imported.

3. Close the import message, and in Citrix Receiver, click the **Add Account**.

- Enter the URL for the Store provided by your organization.
- Click **Next.**

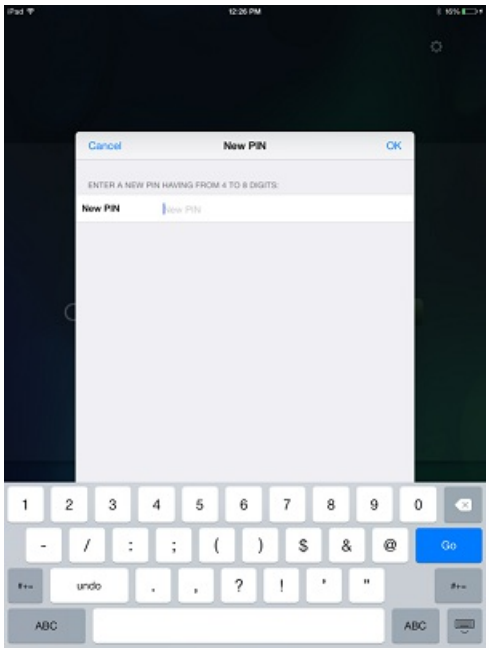
4. In the Log On screen:

- Enter your credentials: user name, password, and domain (such as example.com).
- For the Pin field enter **0000**, unless your organization has provided you with a different default PIN. (The PIN 0000 is an RSA default, but your organization may have changed it to comply with their security policies.)
- At the top left, click **Log On**.



5. After you click the Log On button, you are prompted to create a new PIN.

Enter a PIN from 4 to 8 digits and click **OK**.



6. You are then prompted to verify your new PIN. Re-enter your PIN and click **OK**.

After clicking OK, you will be able to access your apps and desktops.

Support for Next Token Mode

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.

Provide access information to end users for iOS devices

Jun 26, 2013

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.

Configure mobile devices automatically

Apr 13, 2015

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.
    1. 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.)
    2. 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

Mar 22, 2013

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

Oct 30, 2012

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

Dec 08, 2014

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.

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.