BlackBerry PlayBook

2015-04-23 12:39:54 UTC

Contents

Receiver for BlackBerry PlayBook 1.0

Citrix Receiver delivers applications and virtual desktops to BlackBerry PlayBook devices.

In This Section

About This Release	Read about the features and known issues in this release.
System Requirements	Ensure your users have the required hardware and software.
Manage Connections	Configure connectivity for Citrix Receiver for BlackBerry PlayBook.
Provide Account Information	Ensure your users can connect to their applications.

About Citrix Receiver for BlackBerry PlayBook 1.0

Citrix Receiver for BlackBerry PlayBook 1.0 is available in the BlackBerry App World.

New Features

Receiver for BlackBerry PlayBook now supports:

- ICA encryption (SecureICA) and SSL, to secure communications between user devices and XenApp and XenDesktop
- Windows Extended keyboard, including keys such as Ctrl, Alt, and Delete
- Pan, pinch, and zoom

  Receiver supports the standard PlayBook gestures, plus a right-click action: Touch with one finger, pause a moment and then release.

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.

Known Issues

- Receiver for BlackBerry PlayBook does not support clipboard functions in application sessions. [158963]
- Receiver for BlackBerry PlayBook can be unresponsive while the PlayBook device attempts to reconnect a dropped wireless network connection during an application or desktop session. [159059]
- Receiver for BlackBerry PlayBook operation requires that the PlayBook device is in landscape mode. [159521]
- The rendering of large numbers of screen updates in 3D and graphics-intensive applications can slow the response of user input over connections using Access Gateway or Secure Gateway. [260624]
- In an application session a user cannot pan an application to bring the area behind the touch screen keyboard into view if the zoom level is set to 100% or less. To pan an application, set the zoom level to greater than 100%. [261686]
- A Receiver user with four or more disconnected application sessions is unable to reconnect all sessions by using the Reconnect button. The Receiver user can reconnect the application sessions individually. [262650]
- Windows function keys (F1 to F12) are not supported by the BlackBerry touch screen keyboard. Use a Bluetooth-enabled keyboard to access Windows function keys. [268635]
- Receiver for BlackBerry PlayBook does not support a Web Interface installation on Java application servers. Use Web Interface installed on Microsoft IIS Services with Receiver for BlackBerry PlayBook. [271177]
- When Receiver for BlackBerry PlayBook is configured with a Web Interface site, the message Unknown Network Error appears after a few minutes of inactivity even if there is no network error. To resume working, click Try Again. [272285]
- A seamless session started in Receiver for BlackBerry PlayBook does not open when the user reconnects from a device running in seamless mode and Web Interface is configured to request a seamless session. To work around this issue, enter Shift-F2 on the other device to switch from seamless to windowed mode. Alternatively, to enable users to roam from Receiver for BlackBerry PlayBook to other devices running in seamless mode, configure Web Interface to request a windowed session. [273277]
- For connections using XenApp 5 Feature Pack 2 for Windows Server 2003, a user who starts a seamless application session using Receiver on a non-PlayBook device and then roams to Receiver for BlackBerry PlayBook is unable to connect to the application. [273278]

Fixed Issues

- Receiver for BlackBerry PlayBook supports the import of self-signed certificates into the PlayBook Web certificate store.
- Control key combinations are now supported on a Bluetooth keyboard during application sessions. [159249]
- After you swipe up from the bottom bezel to minimize an application, the list of application sessions displays correctly. [159006]

About Citrix Receiver for BlackBerry PlayBook 1.0

Citrix Receiver for BlackBerry PlayBook 1.0 is available in the BlackBerry App World.

New Features

Receiver for BlackBerry PlayBook now supports:

- ICA encryption (SecureICA) and SSL, to secure communications between user devices and XenApp and XenDesktop
- Windows Extended keyboard, including keys such as Ctrl, Alt, and Delete
- Pan, pinch, and zoom

  Receiver supports the standard PlayBook gestures, plus a right-click action: Touch with one finger, pause a moment and then release.

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.

Known Issues

- Receiver for BlackBerry PlayBook does not support clipboard functions in application sessions. [158963]
- Receiver for BlackBerry PlayBook can be unresponsive while the PlayBook device attempts to reconnect a dropped wireless network connection during an application or desktop session. [159059]
- Receiver for BlackBerry PlayBook operation requires that the PlayBook device is in landscape mode. [159521]
- The rendering of large numbers of screen updates in 3D and graphics-intensive applications can slow the response of user input over connections using Access Gateway or Secure Gateway. [260624]
- In an application session a user cannot pan an application to bring the area behind the touch screen keyboard into view if the zoom level is set to 100% or less. To pan an application, set the zoom level to greater than 100%. [261686]
- A Receiver user with four or more disconnected application sessions is unable to reconnect all sessions by using the Reconnect button. The Receiver user can reconnect the application sessions individually. [262650]
- Windows function keys (F1 to F12) are not supported by the BlackBerry touch screen keyboard. Use a Bluetooth-enabled keyboard to access Windows function keys. [268635]
- Receiver for BlackBerry PlayBook does not support a Web Interface installation on Java application servers. Use Web Interface installed on Microsoft IIS Services with Receiver for BlackBerry PlayBook. [271177]
- When Receiver for BlackBerry PlayBook is configured with a Web Interface site, the message Unknown Network Error appears after a few minutes of inactivity even if there is no network error. To resume working, click Try Again. [272285]
- A seamless session started in Receiver for BlackBerry PlayBook does not open when the user reconnects from a device running in seamless mode and Web Interface is configured to request a seamless session. To work around this issue, enter Shift-F2 on the other device to switch from seamless to windowed mode. Alternatively, to enable users to roam from Receiver for BlackBerry PlayBook to other devices running in seamless mode, configure Web Interface to request a windowed session. [273277]
- For connections using XenApp 5 Feature Pack 2 for Windows Server 2003, a user who starts a seamless application session using Receiver on a non-PlayBook device and then roams to Receiver for BlackBerry PlayBook is unable to connect to the application. [273278]

Fixed Issues

- Receiver for BlackBerry PlayBook supports the import of self-signed certificates into the PlayBook Web certificate store.
- Control key combinations are now supported on a Bluetooth keyboard during application sessions. [159249]
- After you swipe up from the bottom bezel to minimize an application, the list of application sessions displays correctly. [159006]

System Requirements for Receiver for BlackBerry PlayBook

Device

Citrix Receiver supports BlackBerry PlayBook devices with a firmware version of 1.0.7.2670 or higher.

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

Server

- **Web Interface 5.4, 5.3, 5.2, or 5.1** with a XenApp Services (formerly Program Neighborhood Agent) site
- **XenApp** (any of the following products):
  - Citrix XenApp 6.5 for Windows Server 2008 R2
  - Citrix XenApp 6 for Windows Server 2008 R2
  - Citrix XenApp 5 Feature Pack 2 for Windows Server 2003
- **XenDesktop** (any of the following products):
  - XenDesktop 5.5
  - XenDesktop 5 Service Pack 1
  - XenDesktop 5

Connectivity

Citrix Receiver for BlackBerry PlayBook supports wireless LAN or WAN connections (HTTP, HTTPS, and ICA-over-SSL) to a XenApp server farm through a XenApp Services site.

For secure remote connections, use any of the following products:

- Citrix Access Gateway Enterprise Edition 9.2 or 9.3
- Citrix Secure Gateway 3.x
- A VPN solution supported by the PlayBook device

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 Web certificate store.

Private (Self-signed) Certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization's certificate authority must be installed on the mobile device in order to successfully access Citrix resources using the Citrix Receiver.

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

Importing Root Certificates on PlayBook Devices

For information about importing root certificates, refer to How to import security certificates on the BlackBerry PlayBook.

Wildcard Certificates

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

Intermediate Certificates and the Access Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Access Gateway server certificate. Refer to the Knowledge Base article CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition.

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

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

Authentication

Note: RSA SecurID authentication is not supported for Secure Gateway configurations. To use RSA SecurID, use the Access Gateway.

Receiver for BlackBerry PlayBook supports these authentication methods when used with the Access Gateway:

- Domain Only (RADIUS, LDAP, NTLM)
- RSA SecurID® Only
- Domain + RSA SecurID®

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

Managing Your Connections

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.

Topics in this section describe how to:

- Configure your XenApp deployment
- Configure connections to an enterprise installation of Citrix Access Gateway and Citrix Secure Gateway
- Configure Web Interface
- Provide access information to your users

Configuring Your XenApp Server Environment for Citrix Receiver for BlackBerry PlayBook

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

1. If the Web Interface of your XenApp deployment does not have either a XenApp Services site or XenApp Web 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.

2. To enable users to easily browse and access their work files (such as Microsoft Word documents) from a drive space on the XenApp server, publish Citrix Doc Finder on the servers your users connect to from their mobile devices.

To configure Access Gateway Enterprise Edition for Receiver for mobile devices

To configure the XenApp Services site

Important:

- Access Gateway Enterprise Edition 9.*x* and 10.*x* are supported by Receiver for Android 2.*x* and 3.*x*, Receiver for BlackBerry 2.*x*, Receiver for iOS, and Receiver for BlackBerry PlayBook using XenApp Services sites or Legacy mode on StoreFront servers.
- Access Gateway Enterprise Edition 9.*x* and 10.x are supported by Receiver for Android 2.*x*, Receiver for iPad 4.2.*x*, and Receiver for BlackBerry PlayBook using XenApp Web Sites.
- Receiver for Web is not supported by Receivers for mobile devices.
- Access Gateway Enterprise Edition 9.*x* and 10.*x* are supported by Receiver for Android 3.1 and iOS 5.6 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.

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 integrate Access Gateway and StoreFront

To give users access to Web apps, simply point Access Gateway to AppController.

To give users access to XenApp and XenDesktop published resources, when you configure Access Gateway you must integrate StoreFront. For details, see the Access Gateway 10 section of eDocs and search for *Integrating Access Gateway and Receiver StoreFront*.

To configure the Access Gateway appliance

1. Configure authentication policies to authenticate users connecting to the Access Gateway by using the Receiver. Bind each authentication policy to a virtual server.

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

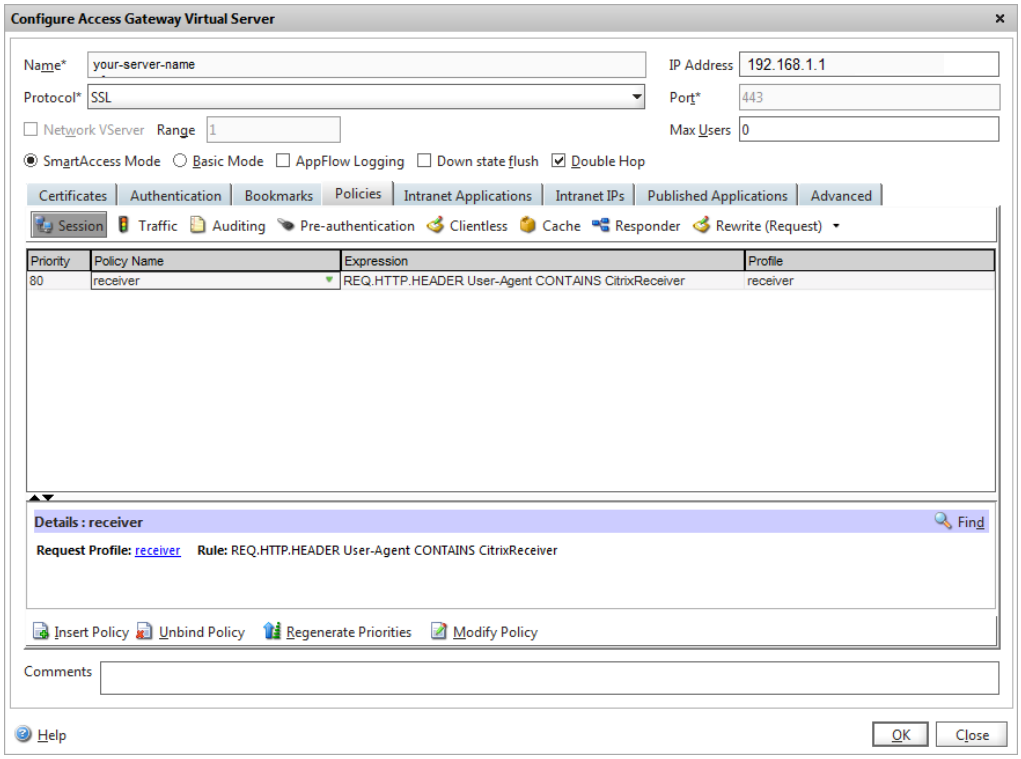
   - If double-source authentication is required (such as RSA SecurID and Active Directory), RSA SecurID authentication must be the primary authentication type. Active Directory authentication must be the secondary authentication type.
   - RSA SecurID uses a RADIUS server to enable token authentication.
   - 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. 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 one of the following settings:

  - 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.

  - Enter the StoreFront address then type in the Store Web address on which remote access is enabled for Access Gateway.

    For example, type https://<StorefrontFQDN>/Citrix/<StoreWebName>/ where <StorefrontFQDN> is the fully qualified domain name (FQDN) of Storefront and StoreWebName is the name of the store.
- Bind the session policy to a virtual server.
- Create authentication policies for RADIUS and Active Directory.
- Bind the authentication policies to the virtual server.

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, such as `GatewayServer.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. On some mobile devices, Receiver does not include all of those options.

To configure the Secure Gateway for Citrix Receiver for mobile devices

To configure the XenApp Services site

Important:

- Secure Gateway 3.*x* is supported by Receiver for Android, Receiver for iOS, and Receiver for BlackBerry PlayBook using XenApp Services sites.
- Secure Gateway 3.*x* is supported by Receiver for Android, Receiver for iOS, and Receiver for BlackBerry PlayBook 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 the Web Interface for Citrix Receiver for mobile devices

To configure the Web Interface site

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

The Receiver supports Web Interface version 5.4 only. In addition, users can launch applications from Web Interface 5.4 using the Firefox mobile browser.

To launch applications on the user device

From the mobile device, users can log into the Web Interface site using their normal logon and password.

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

To configure accounts manually for Citrix Receiver for mobile devices

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

To create an account manually, locate the option to set up the account manually, and follow these general steps:

1. After selecting to set up the account manually, the New Account screen displays additional fields with which to configure the Receiver.

   Note: Options may appear differently for each type of mobile device.

2. Tap one of the following options:

   - Web Interface. This option enables Web View, which allows the Receiver to display a XenApp Web site in the same manner as a Web browser.

   - XenApp Services. This option enables the Receiver to locate a specific XenApp Services site for which authentication through Access Gateway is not configured.

   - Access Gateway. This option enables the Receiver to connect to a XenApp Services site through a specific Access Gateway.

3. In Address, enter the secure URL of the site or Access Gateway to which you want to connect (for example, agee.mycompany.com), provide the remaining details, and tap Next to verify the connection, and then tap Save.

   Important: If you enable the option to Ignore Certificate Errors, you can connect to the server even if the server has an invalid, self-signed, or expired certificate; however, you must make sure that you are connecting to the right 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.

4. Enter your user name and password and tap Log On. The Apps page appears, displaying the desktops you can access.

Providing Account Information to End Users

When users launch Citrix Receiver for the first time, they enter information about the XenApp farm hosting the resources they want to access. To ensure users can connect to the XenApp farm, distribute the following information:

- The location of the XenApp Services site or XenApp Web site hosting resources; for example: `https://servername` (for some Receivers the fully-qualified domain name is required)
- The domain name of the hosting site
- If using Access Gateway, the authentication method

For specific details about configuring the Citrix Access Gateway or Secure Gateway for the Receiver, refer to the configuration topics in this section of eDocs.

Users can turn off authentication by Access Gateway manually by locating the option on the Settings screen. From Accounts, tap Edit and select the account name.

Managing Accounts on User Devices

After creating an account, the user has options to manage the account, including:

- To delete an account, locate the list of accounts and select the option to remove the selected account.
- To synchronize the list of apps with new apps published after the account was created, refresh the list.