Receiver for BlackBerry 2.2

2015-04-19 05:21:53 UTC

Contents

Receiver for BlackBerry 2.2

Citrix Receiver delivers applications and virtual desktops to BlackBerry devices running BlackBerry OS 4.6 through 7.1. Publish Citrix Doc Finder in your XenApp deployment so your users can also securely browse and access files stored on the server.

Try the Demonstration Site

When users launch Citrix Receiver on a mobile device 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.

In This Section

About This Release	Read about the new features and known issues in this release.
System Requirements	Ensure your users have the required hardware and software.
Configure Your XenApp Environment	Configure XenApp so your users can connect to their applications.
Manage Connections	Configure connectivity for Citrix Receiver for BlackBerry.
Deploy	Read about considerations for deploying Citrix Receiver and choosing an installation method.
Provide Account Information	Ensure your users can connect to their applications.
Troubleshoot	Respond to problem reports from your users.

About Receiver for BlackBerry 2.2

This topic describes the new features and known issues in Receiver for BlackBerry 2.2.

What's New

- Support for ICA encryption (SecureICA) to secure communications between user devices and XenApp and XenDesktop.
- Support for Web Interface 5.4, enabling users with mobile devices to launch applications through a Program Neighborhood Services site.
- Users can now enter alphanumeric RSA tokens to connect to Citrix Access Gateway.
- User experience enhancements:
  - Streamlined Citrix DemoCloud setup provides immediate access. The user name is the only input needed.
  - For BlackBerry 6.0 and 7.0 devices: Touch the screen or use the trackpad/trackball to change the mode.
  - A self-service network status message keeps users informed about poor network conditions.
  - Support for Windows shortcut keys: Use the Send Windows generic function keys button on the Receiver toolbar for operations such as Copy, Cut, Paste, and Save .
  - Improved error handling and notification to users about expired RSA tokens and more descriptive error messages for connectivity issues.
  - Usability improvements such as improved zoom performance and more accurate cursor movements.

Known Issues

The app list includes published data files, although they cannot be used to launch an application. [#27923]

Using accessibility settings on BlackBerry 6.0 and 7.0 devices can cause Receiver to hang and is not recommended. [#15309]

Before closing an application opened from Receiver, save your work. You cannot save changes to a file when closing the application. [#246837]

Fixed Issues

When working with an application opened from Receiver, zooming to 125% and above slows the keyboard input response. [#14692]

Before upgrading Receiver through a BES push or Blackberry Desktop Software, uninstall the old version of Receiver. [#15204]

A Receiver shortcut on the home screen disappears if you change the account description. [#27927]

System Requirements for Citrix Receiver for BlackBerry

Device

Citrix Receiver supports BlackBerry devices with the following configuration:

- BlackBerry Software 4.6, 4.7, 5.0, 6.0, 7.0, or 7.1
- 128 MB of memory
- High-speed network such as 3G or WiFi

Supported Models

- Torch 9800, 9810, 9850, 9860
- Bold 9000, 9650, 9700, 9780, 9900, 9930
- Style 9670
- Storm2 9520 and 9550
- Tour 9630, 9650, 9670
- Curve 8350i, 8520, 8530, 8900 series, 9300, 9330, 9350, and 9370

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 6.0 for Windows Server 2008 R2
  - Citrix XenApp 5 Feature Pack 3 for Windows Server 2008
  - Citrix XenApp 5 Feature Pack for Windows Server 2008
  - Citrix XenApp 5 for Windows Server 2008
  - Citrix XenApp 5 Feature Pack 3 for Windows Server 2003
  - Citrix XenApp 5 Feature Pack 2 for Windows Server 2003
- **XenDesktop** (any of the following products):
  - Citrix XenDesktop 5
  - Citrix XenDesktop 4

Connectivity

Citrix Receiver supports secure connections to a XenApp server farm using the following products. You can configure Receiver so that users can point to the Citrix Access Gateway or a BlackBerry Enterprise Server.

- Citrix Access Gateway (any of the following products)
  - Access Gateway Advanced Edition 4.5
  - Access Gateway Standard Edition 4.6.3
  - Access Gateway Enterprise Edition 9.2

  Receiver for BlackBerry supports these authentication methods when used with the Access Gateway:
  - Domain Only (RADIUS, LDAP, NTLM)
  - RSA SecurID® Only
  - Domain + RSA SecurID®
  - No authentication (not applicable to the Access Gateway Advanced Edition)
- BlackBerry Enterprise Server (BES) 4.1 or 5.0, with Mobile Data Service (MDS)

  Note: A VPN is not required to use Receiver with BES.

Managing Your Connections

These topics describe how to:

- Configure your XenApp Server environment
- Configure connections to BlackBerry Enterprise Server and Citrix Access Gateway

  Citrix Receiver for BlackBerry supports secure connections to a BlackBerry Enterprise Server (BES) and to an enterprise installation of Citrix Access Gateway. You can configure both BES and a Citrix Access Gateway for Receiver. Receiver users can then connect using the BES or the Access Gateway. Citrix recommends using the Access Gateway to ensure optimum performance.

- Deploy Receiver for BlackBerry to end users and provide access information to them

For more information about configuring connections, including videos, blogs, and a support forum, refer to http://community.citrix.com.

Configuring Your XenApp Server Environment for Citrix Receiver for Mobile Devices

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 Program Neighborhood Services 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.

2. If you want your users to be able to access published content, such as Microsoft Word documents or Excel spreadsheets, publish Citrix Doc Finder on the XenApp servers to which you users connect with their mobile devices.

Configuring Your BES

If you plan to use a BlackBerry Enterprise Server (BES) with Receiver for BlackBerry, Citrix recommends that you install and configure your BES and Mobile Data Service (MDS) according to best practices described in documentation by Research in Motion.

Citrix Receiver requires full network bandwidth to connect to applications hosted on the XenApp server. To avoid network bandwidth error messages, configure the Flow Control setting on the BES to the maximum KB/Connection value of 1024. For instructions, see the following article on the BlackBerry Technical Solution Center: "You have reached the maximum amount of data that can be transferred by the BlackBerry device over a single connection."

You can push Citrix Receiver software to BlackBerry devices from your BES by assigning a software configuration. For instructions, see the following article on the BlackBerry Technical Solution Center: "How to control and remove third-party applications using whitelisting in a software configuration." If your "Optional" Application Control Policy does not enable users to set the Connections, Interactions, and User Data permissions to "Allow", create a custom Application Control Policy for Receiver for BlackBerry.

To configure Access Gateway Standard Edition 4.5.x or 4.6.x for Citrix Receiver for mobile devices

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. 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: For iOS devices (iPad and iPhone) and BlackBerry devices, 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 4.5.x or 4.6.x appliance

1. Configure Authentication realms to authenticate users connecting to the Access Gateway 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.

     Note: For servers prior to Windows Server 2003, Active Directory can use Integrated Windows authentication, also known as NTLM.

   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 to recognize the servers. You can configure the settings using group properties on the Access Gateway. Configure the 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 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 Advanced Edition 4.5 for Citrix Receiver for mobile devices

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. XenApp Services sites running on the Web Interface 5. *x* have this configuration ability built in.

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

Configure the Access Gateway appliance to use the Access Gateway Advanced Edition 4.5 with Hotfix 4 or higher.

1. In the Administration Tool, click the Access Gateway Cluster tab and open the window for the appliance.
2. On the Advanced Options tab, click Advanced Access Control.
3. Continue by configuring the settings for the server running Advanced Access Control.

To configure the server running Advanced Access Control

1. On the server running Advanced Access Control, from your Logon Point, verify that the authentication method you prefer is set up and working. Active Directory authentication, SMS authentication (http://smspasscode.com) (iPhone only), and RSA SecurID are the supported authentication methods for the Receiver for mobile devices. In the Logon Point Properties dialog box, click Authentication, and select a supported authentication method for the mobile device:

   - For single-factor authentication, select Active Directory, LDAP, or RADIUS (which can be used for RSA SecurID or Active Directory authentication).

   - For double-source authentication, under Active Directory, select RSA SecurID, which can be used with either RADIUS or an sdconf.rec file to enable token authentication.

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

2. On the server running Advanced Access Control, create and deploy a Logon point (the default name for the logon point is `iPhone`). You can verify the existence of the logon point by using this address in the Web browser through the Access Gateway, such as `https://FQDNofAccessGateway/CitrixLogonPoint/LogonPointName`.

   Tip: Citrix recommends using`iPhone` as the name for this logon point for any type of mobile device because the Receiver uses this name as the default logon point for the device. If you use any other logon point name, enter the full URL path in the Receiver settings.

   a. Create a Web resource (MobileDevicePNA) for the XenApp Services site of the mobile device.

   b. On the Web Resource Properties page for URL Addresses, set the home page and display order for the device logon point:

      - Ensure your XenApp Service sites are listed under URL, the Application Type is Web Application (not Web Interface), and the Authentication Type is No authentication.

      - Select Publish for users in their list of resources and set Home page to your XenApp Services site URL. Example: `http://webserver.domain.com/Citrix/PNAgent/Config.xml`

   c. Select the new Logon Point and set the following properties:

      - On the Select Home Page tab, select the option to display the home page application and set the display order so that the Web resource home page for the mobile device has the highest priority.

      - On the Authentication tab, select the method to authenticate users connecting to the Access Gateway using the Access Gateway plug-in.

      - On the Session Settings tab, clear the check box for Time to prompt user before password expires.

- On the Visibility tab, select Allow external users access to this logon point.

For more information about creating policies for the Access Gateway and XenApp, see the Access Gateway documentation. Product documentation is available online in Citrix eDocs.

3. In the console under Policies, create a filter applied to this logon point. Right-click Filters, and select Create filter.
   a. In Filter Properties, click the Logon Points tab.
   b. In the Selected logon points list, add the Logon Point name for the mobile device.
4. Create a policy for this Logon Point and set the following Policy Properties:
   a. On the Resources tab, select the check boxes for Web Resources > MobileDevice and for Allow Logon.
   b. On the Settings tab, ensure that the value for Web Resources > Access and Network Resources > Access are set to Allow. This setting allows users to access the Web resource and allows the Logon to this logon point.
   c. On the Filter tab, select the mobile device filter to apply to the policy.

      Note: 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 used `iPhone` as the Logon Point name, enter the FQDN of Access Gateway, such as: `https://GatewayServer.organization.com`.

   If you used anything other than `iPhone` as the Logon Point name, enter the full path in the Address field:
   `https://FQDNofAccessGateway/CitrixLogonPoint/LogonPointName`.

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 Enterprise Edition for Citrix Receiver for mobile devices

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. XenApp Services sites running on the Web Interface 5. *x* have this configuration ability built in.

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

1. Configure authentication policies to authenticate users connecting to the Access Gateway using the Access Gateway Plug-in. Bind each authentication policy to a virtual server.

   Active Directory authentication, TACACS authentication (Android, iPhone, and iPad only), 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 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.

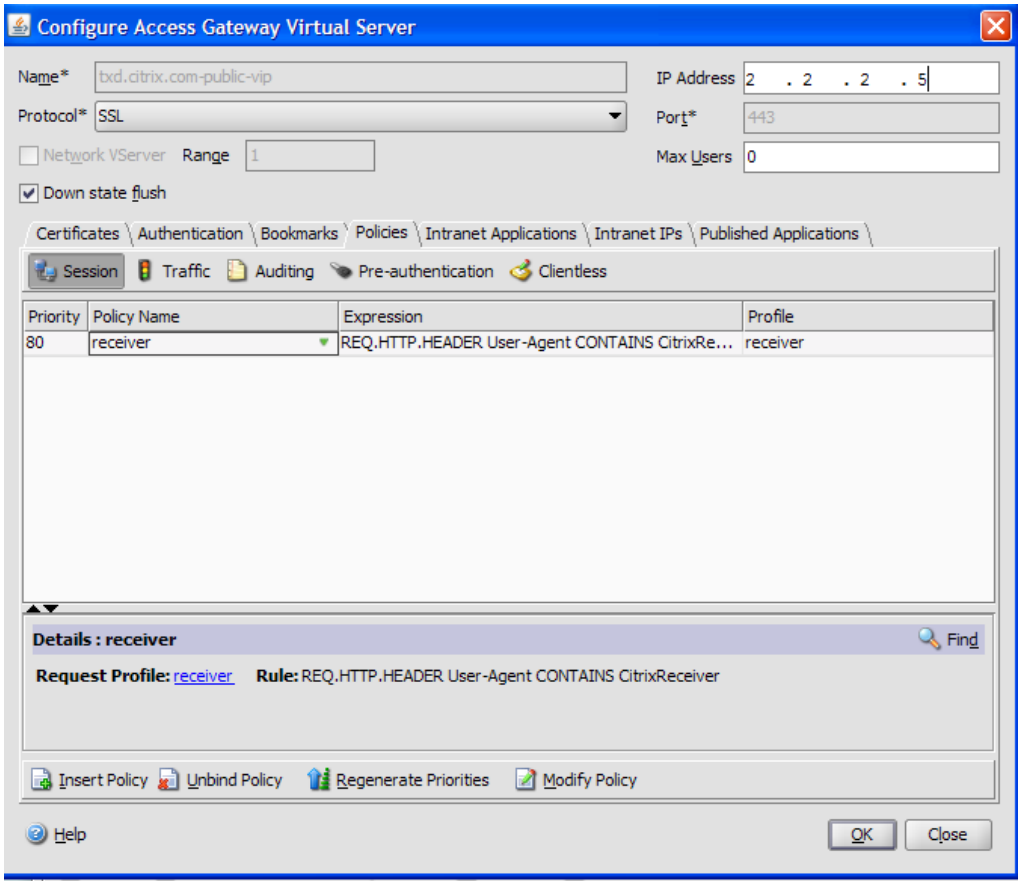
     Note: For servers prior to Windows Server 2003, Active Directory can use Integrated Windows authentication, also known as NTLM.

   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 checked the Override Global check box), ensure the ICA Proxy field is 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 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.

Deploying Citrix Receiver for BlackBerry

To deploy Receiver to your users:

- Depending on your IT configuration, install security certificates on your users' BlackBerry devices to optimize the user experience.
- Identify the preferred software installation method for your organization and, if applicable, the URL for the download.
- Provide installation instructions to your users so they can download Receiver and connect their devices to XenApp and XenDesktop. For more information, see Providing Account Information to End Users.
- Distribute Citrix Receiver for BlackBerry 2.1 User's Guide, a PDF available at http://support.citrix.com/article/CTX129517.

Choose an Installation Method

Deploy Citrix Receiver software to your users through either of the following methods.

- Direct your users to install Receiver from BlackBerry App World, the preferred method.
- Download the Receiver Installation Package and deploy to users by assigning a software configuration on your organization's BlackBerry Enterprise Server (BES).

Get Your Users Connected

After installing Citrix Receiver, users launch it from their BlackBerry devices.

When users start Citrix Receiver for the first time, it displays a welcome page that presents them with the following choices:

- Get Started enables your users to set up their connection to XenApp or XenDesktop configured for your organization.
- Try Demo enables your users to get an account on the Citrix demo site.

Providing Account Information to End Users

When users launch Citrix Receiver for the first time, they are required to enter information about the XenApp farm hosting the resources they want to use (if the connection is through a BlackBerry Enterprise Server) or the Citrix Access Gateway (if the connection is not through a BlackBerry Enterprise Server). To ensure users can connect to XenApp, distribute the following information:

- The location of the XenApp Services site, the Program Neighborhood Services site hosting resources, or the Access Gateway server address; for example: `https://servername`
- The domain name of the hosting site
- For access using the Access Gateway, the product edition and authentication method

  Please note that access using the Access Gateway requires that the BlackBerry device APN settings are configured according to the service provider specification. A BlackBerry device previously configured for a BES might not have the APN settings configured. In that case, a user will need to configure the APN settings provided by the service provider.
- The BlackBerry device requirements for Citrix Receiver
- If applicable, instructions on how to install security certificates on the device

See also To configure mobile devices automatically.

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.

Troubleshooting Citrix Receiver for BlackBerry

Ensuring permissions are correctly set on the BlackBerry device

If your users see the error message "Application has insufficient permissions to run. Please set the required permissions.", advise them to perform the following steps.

1. Depending on your BlackBerry device, open Settings > Options > Advanced Options > Applications > Citrix Receiver, or Settings > Options > Applications > Citrix Receiver.
2. Click the BlackBerry menu key and choose Edit Permissions.
3. Ensure the following are set to Allow:
   - Connections
   - Interactions
   - User Data

Managing disconnected sessions

Users can disconnect from a Citrix Receiver session in such a way that their sessions remain in a disconnected state. Even though the users can reconnect at a later time, you can ensure disconnected sessions are rendered inactive after a specific interval by configuring a session timeout for the ICA-tcp connection in Terminal Services Configuration. For more information about configuring Terminal Services, refer to the Microsoft Windows Server product documentation.

Reaching the maximum amount of data for a single connection

If you are using BlackBerry Enterprise Server (BES) 4.0 or 4.1 for Microsoft Exchange, and your users report that when they connect with Citrix Receiver their BlackBerry devices display an error that they have reached the maximum amount of data that can be transferred over a single connection, increase the flow control on your BES. For more information, see the following article in the BlackBerry Technical Solution Center: You have reached the maximum amount of data that can be transferred by the BlackBerry device over a single connection.

Turning on mobile data services and network connection

If your users report they are getting the error "Mobile data services and network connection must be turned on":

- Ensure your BlackBerry Enterprise Server (BES) is activated (if applicable).
- Ask your users to remove the batteries from their BlackBerry devices for about thirty seconds, then restart.
- Ask your users to verify their BlackBerry devices are connected to a data network or WiFi. From the home page on the BlackBerry device, select Manage Connections.
- Ask your users to verify their BlackBerry devices are enabled and connected to the BES (if applicable):

  1. From the home page on the BlackBerry device, select Manage Connections then Services Status.
  2. In Service Status verify that the description under BlackBerry Enterprise Server reads "Connection: Mobile Network." If it reads "Not connected," re-activate the BlackBerry device on your corporate BES.