Receiver for Windows CE 11.0

Contents

Receiver for Windows CE 11.0 3
Known Issues 4
System Requirements 6
Configuring Your XenApp Server Environment 8
Configuring Secure Gateway 10
Securing Connections with Certificates 11
Configuring HDX Plug-n-Play Dual-monitor Support 12
Providing Information to Receiver for Windows CE Users 13
Configuring Settings on the Client Device 15

Receiver for Windows CE 11.0

Citrix Receiver for Windows CE enables users to access applications published on XenApp server farms from Windows CE-based terminal devices. Administrators publish applications on a XenApp server to make them available to users.

What's New

- Support for multiple monitors
- HDX WAN optimization

  This optimizes performance by using Citix Branch Repeater to cache bandwidth-intensive data and graphics and deliver them from the most efficient location.

In This Section

Under this node, you will find the following resources:

Known Issues for Receiver for Windows CE 11.0	Review known issues for this release
System Requirements for Receiver 11 for Windows CE	Ensure users have the required hardware, software, and connectivity
Configuring Your XenApp Server Environment for Citrix Receiver for Windows CE	Specify and control user access to Receiver settings
Configuring Secure Gateway for Receiver for Windows CE	Configure the XenApp Services site to support connections from a Secure Gateway connection and configure the Secure Gateway
Securing Connections with Certificates	Review the basics of using SSL certificates
Configuring HDX Plug-n-Play Dual-monitor Support	Learn the requirements and setup required for multiple-monitor support
Providing Information to Receiver for Windows CE Users	Ensure users of Receiver for Windows CE know how to enable Receiver, find applications, and configure settings

Known Issues for Receiver for Windows CE 11.0

The following is a list of known issues in this release.

Changing Window Size in ICA Session Shadowing

Non-desktop Windows CE-based terminal devices can only support full screen mode. If an administrator changes the window size when shadowing an ICA Session with this type of device, this may result in the device's display not including a scroll bar (meaning some icons cannot be accessed), or behaving slowly and erratically.

Do not change the window size during shadowing. [#133800]

Watching Video with HDX Multimedia Acceleration

Playing high bit-rate media files can result in a problem with video playback using the HDX Multimedia Acceleration feature. Temporary loss of video (but not audio) can result. After a period, video is restored but the movie's original color depth is lost. A separate problem can result in a temporarily frozen screen or temporary loss of both video and audio.

If possible, client users should avoid watching high-bit rate media files through HDX Multimedia Acceleration sessions. [#135434, 135329].

Failover between HTTPS and HTTP XenApp Service sites

There are problems using both HTTPS and HTTP XenApp Service sites with the Backup URL Support feature. When adding backup URLs, do not mix HTTPS and HTTP addresses. [#135865]

Launch Desktop task bar partially hidden

Before starting a XenApp or XenDesktop session, enable Auto Hide from the local Windows CE task bar so that the local Windows CE task bar does not partially hide the Launch Desktop task bar. [#240364]

Known Issues for Program Neighborhood Classic

Changing Window Size in ICA Session Shadowing

Non-desktop Windows CE-based terminal devices can only support full screen mode. If an administrator changes the window size when shadowing an ICA Session with this type of device, this may result in the Windows CE-based terminal device's display not including a scroll bar (meaning you cannot access some icons), or behaving slowly and erratically.

Do not change the window size during shadowing [#133800].

Watching Video with SpeedScreen Multimedia Acceleration

Playing high bit-rate media files can result in a problem with video playback using the SpeedScreen Multimedia Acceleration feature. Temporary loss of video (but not audio) can result. After a period, video is restored but the movie's original color depth is lost. A separate issue can result in a temporarily frozen screen or temporary loss of both video and audio.

If possible, users should avoid watching high-bit rate media files through SpeedScreen Multimedia Acceleration sessions. [#135434, 135329].

System Requirements for Receiver 11 for Windows CE

Device

- Windows CE 6.0 FR 3
- An active Internet or wireless connection
- 2.45 megabytes of ROM

  Exact RAM requirement sizing is not possible because of the compression technology used in Windows CE. However, each connection maintains a frame buffer that is the exact size of the image. For example: 1024x768, 256 colors = 768KB

Server

For Receiver for Windows CE

- Web Interface 5.3 for Windows with a XenApp Services site
- XenApp (any of the following products):

  Citrix XenApp 6.0 for Microsoft Windows Server 2008 R2

  Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2003

  Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2008

  Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003

  Citrix XenApp 5.0 for Microsoft Windows Server 2008

  Citrix XenApp 5.0 for Microsoft Windows Server 2003

- Citrix XenDesktop 4

For Program Neighborhood Classic

- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003
- Citrix XenApp 5.0 for Microsoft Windows Server 2008

Connectivity

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

For LAN connections:

- Web Interface 5.3 for Windows with a XenApp Services site

For secure remote connections:

- Citrix Secure Gateway 3.2 (supported only on Microsoft Windows Server 2008 R2)

Configuring Your XenApp Server Environment for Citrix Receiver for Windows CE

Administrators must ensure that the configuration settings on the server running the Web Interface are suitable for Receiver users. The location of Receiver configuration settings and the tool used to update them depend on the version of XenApp you are using.

When a user enables Receiver on the client device and connects to the server URL, Receiver reads the configuration data from the server. If you change the configuration settings, be sure to inform users that they need to disable and then re-enable Receiver so it can use the latest settings.

Note: The configuration settings are global; changing them affects all connected users.

Configuration settings specify the functionality available to users in the **Receiver Properties** dialog box. You can specify whether the following tabs are shown.

- **Server** tab: Allows users to select the server URL to which they want to connect.
- **Application Display** tab: Allows users to choose where they want their list of published resources displayed. This tab is available only to terminals with desktops that have been appropriately configured by the OEM.
- **Session Options** tab: Allows users to select the screen color depth, audio quality, and keyboard shortcut pass-through options for a session.

  The preferences users set for color depth and sound quality affect the amount of bandwidth the ICA session consumes. To limit bandwidth consumption, you can force the server default for some or all of the options on this tab. This removes all settings for the corresponding option, other than Default,from the interface.
- **Reconnect** Options tab: Allows users to specify automatic reconnection settings.

  Active sessions are all sessions currently running on any client device connected to the farm. When you reconnect to active sessions from another client device or devices, the sessions disappear from the original client devices. Disconnected sessions are sessions to which you were connected previously and that are still running on the farm. Sessions run on the farm until you log off.

  Workspace control connects or reconnects all previous active or disconnected sessions regardless of how they were connected. For information about workspace control requirements and server configuration, refer to the XenApp documentation.

Multiple Farm Support

You can use Receiver in Citrix XenApp deployments with more than one farm. When you configure the Web Interface to present users with a combined list of published applications from multiple farms, Receiver automatically supports that configuration as well. It is important to note that you cannot connect to two applications with the same name when connecting to applications published from multiple server farms from the Receiver for Windows CE. For information about configuring the Web Interface, refer to the Web Interface documentation.

Client-to-Server Content Redirection

If your Windows-based terminal supports client-to-server content redirection, you can set up this feature for Receiver users. For more information about client-to-server content redirection, refer to the XenApp documentation.

Worker Group Preference and Failover

A XenApp policy rule enables you to direct user connections to preferred zones and set transparent failover to backup zones when preferred servers are unavailable. When users open applications, the Worker Group Preference and Failover policy rule directs their connections to the server with the highest zone preference and smallest load. Configure this policy on the computer running Citrix XenApp. For more information about the server-side setup, refer to the XenApp documentation.

Configuring Secure Gateway for Receiver for Windows CE

The Secure Gateway works with the Web Interface to facilitate authentication of users attempting to establish connections to a server farm. Authorization occurs when the Secure Gateway confirms that the user is authenticated by the enterprise network. The authorization process is entirely transparent to the user.

To configure the XenApp Services site

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.

Receiver for Windows CE 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.

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 guarantee that the Secure Gateway is configured correctly for networking and certificate allocation.

Securing Connections with Certificates

When securing remote connections using SSL certificates, the client device verifies the authenticity of the remote gateway's SSL certificate against a local store of trusted root certificate authorities. The device automatically recognizes commercially issued certificates (such as VeriSign and Thawte) provided the root certificate for the certificate authority exists in the local keystore.

Private (Self-signed) Certificates

If a private certificate is installed on the remote gateway, install the root certificate for the organization's certificate authority on the device in order to provide access to Citrix resources from Citrix Receiver for Windows CE. For information about installing certificates, refer to the documentation for your client device.

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 appears; however, applications fail to launch.

Configuring HDX Plug-n-Play Dual-monitor Support

Dual monitors are fully supported when the plug-in is configured to connect to seamless applications. Sessions span dual monitors in full screen mode, with multiple monitors shown inside the session; applications snap to monitors as they would locally.

To enable dual-monitor support:

- For the HP t5540: In the **Display Properties** dialog box, select **Dual Monitor Span Mode**. For the setting on other devices, refer to the manufacturer's documentation.

After your monitors are detected:

- **XenDesktop:**Configure the graphics memory limit using the Citrix Machine Policy setting **Display memory limit**.

- **XenApp:**Depending on the version of the XenApp server you have installed:

    - Configure the graphics memory limit using the Citrix Computer Policy setting **Display memory limit**.

    - In the left pane of the Delivery Services Console or Access Management Console, select the farm and in the task pane, select **Modify Server Properties > Modify all properties > Server Default > HDX Broadcast > Display** (or **Modify Server Properties > Modify all properties > Server Default > ICA > Display**) and set the **Maximum memory to use for each session's graphics**.

Ensure the setting is large enough (in kilobytes) to provide a sufficient graphic memory. If this setting is not high enough, the seamless application is restricted to the subset of the monitors that fits within the size specified.

For information about calculating the session's memory graphic requirements, see CTX115637.

Providing Information to Receiver for Windows CE Users

To ensure that users can successfully use Receiver for Windows CE, distribute the following information.

Important: Users who want to authenticate with a smart card must use Receiver for Windows CE 11.02.

Enabling Citrix Receiver for Windows CE

1. Open the **Citrix Receiver Settings** dialog box according to the instructions for the Windows CE-based terminal and then select the **Preferences** tab.
2. Select the **Log On** check box.
3. Enter your logon credentials.

   To use Receiver you specify your user name and password only once at the start of a session. Your credentials are then used for all application connections during the session.

   You can configure Receiver so that users have the option to save their password so they are prompted for it only if the password changes.

Working with Applications

When Citrix Receiver for Windows CE is running, a user's available applications appear in one or more folders, depending on how you or the user configures Receiver.

Start applications from any of these locations:

- The **Start** menu.
- A custom folder on the desktop or in **Start** > **Programs**.

  If the **Citrix Receiver Settings** dialog box includes an **Application Display** tab, the user can specify any of these alternate folder locations for applications, as described in "To specify where to place links to published resources" later in this topic.

Disconnecting from applications accessed from Receiver closes the connection between the client device and the server. The sessions remain active in the server and the user can easily reconnect to them from the same client device or a different one. To disconnect and reconnect applications without closing the server session:

1. Open the **Citrix Receiver Settings** dialog box according to the instructions for the Windows CE-based terminal.

2. Select the **Preferences** tab and then click **Disconnect**.

3. When ready to reopen the disconnected applications, click **Reconnect**.

   For reconnection options, see "To enable automatic reconnection" later in this topic.

To close a session on the server, the user must log off. To log off from all applications:

1. Open the **Citrix Receiver Settings** dialog box according to the instructions for the Windows CE-based terminal.

2. Select the **Preferences** tab and then click **Log Off**.

Configuring Settings on the Client Device

You can configure the client device so that users can change Receiver settings from the **Citrix Receiver Settings** dialog box. Refer users to the instructions for the Windows CE-based terminal for help opening that dialog box. Distribute the following information to users.

To start Citrix Receiver automatically

1. Select the **Preferences** tab.
2. Select the **Force Receiver on Reboot** check box and then click **OK**.

To modify session options

1. Click **Settings**.
2. Select the **Session Options** tab.
3. Make the changes and then click **OK**. Depending on how you configure Receiver on the server, users can set preferences for the screen color depth, sound quality, and keyboard shortcut pass-through options for ICA sessions.

To enable automatic reconnection

A user who connects to an application through Receiver has a session with a XenApp server. In general, if a session disconnects in which a user is running multiple applications, the applications continue to run on the server until the user logs off from the applications. This enables the user to reconnect to a session from another computer and access the applications as if the user never changed computers.

You can configure XenApp so that a session automatically reconnects. You can also give users access to the following reconnect options.

1. Click **Settings**.
2. Select the **Reconnect Options** tab.
3. Select a setting and then click **OK**.

    - **Enable automatic reconnection at logon**: This setting allows the user to reconnect automatically to applications and server sessions when logging on to the server. The user can choose to reconnect to active sessions only or to both active and disconnected sessions.

Active sessions are all sessions currently running on any client device connected to the farm. Disconnected sessions are sessions to which the user was connected previously and that are still running on the farm. Sessions run on the farm until the user logs off.

- **Enable automatic reconnection from Reconnect button**: This setting allows the user to use the **Reconnect** button to reconnect to the server. The user can choose to reconnect to active sessions only or to both active and disconnected sessions.

To specify where to place links to published resources

If the **Application Display** tab is displayed, the user can choose a location for applications.

1. Click **Settings**.
2. Select the **Application Display** tab.
3. Select a setting and then click **OK**.

   - **Show applications in Start menu**: This setting places links to published resources in the Start menu.
   - **Show applications in Programs submenu**: This setting places links to published resources in a Programs submenu in the specified folder name.
   - **Show applications in desktop folder**: This setting places links to published resources in a desktop folder in the specified folder name. To place links directly on the desktop, leave the folder name blank.

To change the server URL

1. Click **Settings**.
2. Select the **Server** tab.
3. Click **Change**, enter the new server URL, and then click **Update**.