Windows CE

2015-04-23 12:40:29 UTC

Contents

Receiver for Windows CE 11.02

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

- Includes Citrix Program Neighborhood to accommodate users who authenticate using a smart card.

In This Section

Under this node, you will find the following resources:

Known Issues for Receiver for Windows CE	Review known issues for this release
System Requirements for Receiver for Windows CE 11	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 Multi-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
Providing Information to Program Neighborhood Users	Ensure users of Program Neighborhood Classic know how to create, configure, and use connections

Known Issues for Receiver for Windows CE 11.02

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

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].

Known Issues for Receiver for Windows CE 11.02

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

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 for Windows CE 11

Device

- Windows CE 6.0 R3
- 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

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

  Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2 (does not support the TCP Browser network protocol)

  Citrix XenApp 6.0 for Microsoft Windows Server 2008 R2 (does not support the TCP Browser network protocol)

  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 Feature Pack 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

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 (not applicable to Program Neighborhood):

- 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 Citrix Program Neighborhood, which is installed with Receiver for Windows CE. For information, see Providing Information to Program Neighborhood Users.

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.

Providing Information to Program Neighborhood Users

Users who authenticate using a smart card must use Citrix Program Neighborhood to create, manage, and establish connections to Citrix XenApp and applications. Program Neighborhood is installed on Windows CE-based terminal devices with Citrix Receiver, which does not support smart card authentication.

To ensure that users can successfully use Program Neighborhood, distribute the following information along with any setting information (such as XenApp server address and port) that users need to configure connections.

About Smart Card Authentication

Program Neighborhood supports smart cards for:

- **Smart card logon authentication**. You can use a smart card to authenticate to Citrix XenApp.
- **Smart card application support**. Published applications that are smart card compatible can access your local smart card device.

Smart card support requires that your smart card devices and published applications are Personal Computer/Smart Card (PC/SC) industry standard compliant.

Important: Smart card data is security-sensitive and must be transmitted over a secure authenticated channel such as SSL/TLS.

Smart card support for XenApp is based on the Microsoft PC/SC standard specifications. XenApp supports only smart cards and smart card devices that are supported by the underlying Windows operating system. Receiver does not control smart card PIN management. PIN management is controlled by the cryptographic service provider for your cards.

Microsoft strongly recommends that you use only the smart card readers tested and approved by the Microsoft Windows Hardware Quality Lab (WHQL) on computers running qualifying Windows operating systems. Visit microsoft.com for additional information about hardware PC/SC compliance.

Creating and Configuring Connections

Your Windows CE-based terminal device has a Connection Manager dialog box that you use to create, configure, and run two types of ICA sessions:

- Server connections: Allows you to connect to a specific computer running Citrix XenApp and then run any of the applications available on the desktop.
- Published applications: Allows you to connection to specific applications set up by an administrator. When you connect to this type of session, the application opens on your desktop.

Your Windows CE-based terminal device also has a Global ICA Client Settings dialog box that you use to configure the settings that apply to all connections on your terminal device and are used as defaults when you create a new connection.

The Connection Manager and the Global ICA Client Settings dialog boxes vary depending on the terminal device you are using. For example, the titles of these dialog boxes and the method for accessing them can differ.

To create a new connection

For flexibility in accessing connection configuration settings, create a connection as described in the following steps and then configure the connection to best suit your needs.

1. According to the instructions for your Windows CE-based terminal device, open the Connection Manager dialog box and then select the option for adding a connection.
2. In the New Connection dialog box, select Citrix ICA Client and then click OK.
3. In the Select a Server or Published Application dialog box, click Server or Published Application to set up a connection. To display an up-to-date list of servers or applications, click Refresh.
4. To define or change server groups, do one of the following:
   - Click Server Location and go to Step 5.
   - Scroll through the displayed list and select the server or published application. Click Next and go to Step 6.
5. In the Server Location dialog box, click Add to enter the XenApp server information and then choose a communication protocol. The default server location protocol is TCP+HTTP browser and the default value entered in the Address List box is ica. Configure these settings as directed by your administrator.
6. Click Server or Published Application to connect and then click OK.
7. In the Select a Title for the ICA Connection dialog box, enter a name for the connection and click Done.

Important: Do not use the following characters in a connection name: ; , [ ]` ! " % ^ & * ( ) { } \ @ ~ # | < > ? /

The connection name appears in the list of connections in the Connection Manager dialog box. To change a connection name, go to the Title tab.

To configure a connection

The settings that you configure in the Connection Manager dialog box override the application settings in Citrix XenApp.

1. In the Connection Manager dialog box, select the option for editing a connection according to the instructions for your Windows-based terminal device.
2. Click the name of the connection that you want to change.
3. Click Edit to display the Edit Connection Details dialog box.
4. Use the tabs to access the settings.

To delete a connection

Select the appropriate option in the Connection Manager dialog box according to the instructions for your Windows CE-based terminal device.

To configure global and default settings

To configure global settings, use the Global ICA Client Settings dialog box, which is usually accessed with other terminal property settings on your terminal device. Refer to the documentation for your Windows CE-based terminal device for the key combination used to display the properties. The key combination is usually a function key such as F2 or a Settings command on the Start menu.

1. Open the Global ICA Client Settings dialog box according to the instructions for your Windows CE-based terminal device.
2. Use the tabs to access the settings.

Opening and Using a Connection

The following procedures require that you have configured smart card authentication as described in "To enable smart card authentication" in Configuring Settings on the Client Device.

To open a connection

1. In the **Connection Manager** dialog box, select the option for connecting to a server according to the instructions for your Windows CE-based terminal device.
2. Click the name of the connection that you want to open.
3. Click **Connect**.
4. Enter your smart card credentials when prompted. After you log on, you are connected to XenApp or the published application configured for the connection. Connections using smart card authentication do not support automatic reconnection when a user moves to a different device.

Using Keyboard Shortcuts

You can use the following default keyboard shortcuts during ICA sessions to control various functions. Some keyboard shortcuts control the behavior of Program Neighborhood while others emulate standard Windows keyboard shortcuts.

Name	Default Value	Description
Connection Status	CTRL+6	Displays a dialog containing information such as the name of the connected server and user, encryption level, ICA session settings, and the incoming/outgoing connection statistics.
Close Session	CTRL+2	Disconnects Program Neighborhood from the server and closes the client window on the local desktop. Using this keyboard shortcut leaves the ICA session running in a disconnected state on the server. If you do not want to leave your session running in a disconnected state, log off instead.
ESC	CTRL+3	Provides the functionality of an ESC key on the terminal device.
CTRL-ALT-DEL	CTRL+4	Displays the Windows Server 2003 dialog box on the server.
CTRL-ESC	CTRL+5	On servers, displays the Windows Start menu.

ALT-TAB	CTRL+7	Cycles the focus through the minimized icons and open windows of applications running in the ICA session. The selected application receives keyboard and mouse focus.
ALT-ESC	CTRL+8	Cycles through all applications in the ICA session. A popup box appears and displays the programs as you cycle through them. The selected application receives keyboard and mouse focus.
ALT-BACKTAB	CTRL+9	Like the ALT+TAB keyboard shortcut, this key sequence cycles through applications that are open in the ICA session, but in the opposite direction. The selected application receives keyboard and mouse focus.

Printing from a Connected Application

If your administrator has configured XenApp to allow printer mapping, you can print to local or networked printers from your connected applications. Configure your Windows CE-based terminal device for printing according to its documentation. Specify a printer driver and the complete path to a network printer, as provided by your administrator.

Configuring Settings on the Client Device

Distribute the following information to end users of Program Neighborhood.

Important: Roaming user reconnect is not supported for connections configured for smart card authentication.

To enable smart card authentication

You must enable smart card authentication before you can log in to Program Neighborhood with a smart card.

1. In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Logon tab.

2. Select the Allow Smart Card logon check box. When you select the check box, text in the Username and Password fields is deleted.

3. Specify the Domain and your PIN for smart card authentication.

To specify an application to run after connecting to XenApp

By default, when you open a connection to XenApp the Windows desktop appears. You can configure a connection so that an application opens instead of the Windows desktop. When you exit the application, the connection closes.

1. In the Connection Manager dialog box, click the name of the server connection that you want to change, click Edit, and then click the Application tab. If the Application tab is not available, the connection you selected is to a published application.

2. In the Command Line box, specify the path and file name of the application to run after connecting to the server. For example, to launch Microsoft Notepad automatically after connecting to a server, type:

   C:\Windows\Notepad.exe

   where C: represents the XenApp server drive.

3. In the Working Directory box, specify the working directory to use with the application. For example: C:\My Documents When you connect to XenApp, the application opens. When you select File > Open from the application, the working directory folder opens.

To view a published application in a seamless window

In seamless window mode, published applications and desktops are not contained within an ICA session window. Each published application and desktop appears in its own resizable window, as if it is physically installed on the client device. Users can switch between published applications and the local desktop.

In non-seamless window mode, published applications and desktops are contained within an ICA session window. This creates the effect of the application appearing in two windows.

1. In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Window tab.
2. Select the View in a separate window (Seamless Window) check box.

Important: The option to view in a seamless window is available only if the connection is to a published application from Windows CE-based terminal devices with desktops configured by the OEM. This check box does not appear if the connection is to a server.

To configure applications for session sharing

1. Ensure that the applications to share a session have the same Server Location list and browser type.
2. Ensure that the applications have Seamless Windows enabled.
3. Ensure that the audio quality and color depth settings of the second application are the same or lower than those of the first application.

To configure keyboard shortcuts

The default keyboard shortcuts (see "Using Keyboard Shortcuts" in Opening and Using a Connection) are mapped to suit Windows servers. You can change the keyboard shortcuts to correspond to different actions in your UNIX Windows Manager.

1. In the Global ICA Client Settings dialog box, click the Keyboard Shortcuts tab.
2. Use the lists of keys to change the default keyboard shortcut sequences. To disable a keyboard shortcut, select Disabled in the appropriate drop-down list.

To configure keyboard pass-through

You can specify when keyboard shortcuts apply to the remote session or your terminal device desktop. This setting applies only to Windows CE-based terminal devices with desktops.

1. To configure a specific connection, open the Connection Manager dialog box. To configure defaults for all connections, open the Global ICA Client Settings dialog box.

2. Navigate to the server settings:

   - In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Options tab.

   - In the Global ICA Client Settings dialog box, click the Preferences tab.
3. Select one of the following values from the Apply Windows key combinations drop-down list:

   - In full screen desktops only. Applies keyboard shortcuts to the remote desktop rather than to the local desktop when the remote session is running in full screen mode. If the session is running in any other window size mode, keyboard shortcuts are applied to the local desktop rather than to the remote desktop.

   - On the remote desktop. Applies keyboard shortcuts to the remote session rather than to the local desktop. For example, pressing ALT+TAB switches between all the windows currently open on the remote desktop, excluding any windows open on the local desktop.

   - On the local desktop. Applies keyboard shortcuts to the local desktop rather than to the remote desktop. For example, pressing ALT+TAB switches between all the windows currently open on the local desktop, including both local and remote windows.

To specify the color depth for a connection

1. To configure a specific connection, open the Connection Manager dialog box. To configure defaults for all connections, open the Global ICA Client Settings dialog box.

2. Navigate to the server settings:

   - In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Window tab.

   - In the Global ICA Client Settings dialog box, click the Preferences tab.
3. Set the color depth. For optimal display, set both the client device and Default Windows Colors to 16-bit color. If the client device is capable of high-color display (more than 256 colors), the options include Thousands and Millions.

To configure sound and microphone use

1. In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Options tab.

2. To enable sound support, select the Enable Sound check box. From the drop-down list, select one of the following sound quality levels:

   - **Low**. Recommended for low-bandwidth connections, including most modem connections. This setting causes any sound sent to the client to compress to a maximum of 16Kbps. This compression results in a significant decrease in the quality of the sound. The CPU requirements and benefits of this setting are similar to those of the Medium setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

   - Medium. Recommended for most LAN-based connections. This setting causes any sound sent to the client to compress to a maximum of 64Kbps. This compression results in a moderate decrease in the quality of the sound played on the client device. The host CPU utilization decreases compared with the uncompressed version because of the reduction in the amount of data being sent across the wire.

   - High. Recommended only for high-bandwidth connections when sound quality is important. This setting allows clients to play a sound file at its native data rate. Sounds at the highest quality level require about 1.3Mbps of bandwidth to play clearly. Transmitting this amount of data can result in increased CPU utilization and network congestion.
3. From the Microphone Input drop-down list, select one of the following values:

   - Disabled. You cannot record sound from a local microphone.

   - Enabled. You can record dictations with applications running on the server using local microphones. For example, when away from the office you can establish a session to record notes. Later in the day, you can retrieve the notes for review or transcription from the desktop device back at the office.

   - Ask before use. When working locally you receive a message asking permission to record from the local microphone.

To configure session reliability

Session reliability ensures that the application window remains visible for a default time of three minutes, after which you can choose when to reconnect to continue working. This feature is available if it is enabled on the XenApp server.

To reduce the likelihood that you click a link or type text while the connection is being restored, the mouse pointer becomes an hourglass icon while the application is unresponsive. Any mouse movements or keyboard inputs are cached and the results are shown when the session is restored.

1. In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Options tab.

2. To continue to see a published application's window if the connection is interrupted, select Enable Session Reliability and enter a port number for session reliability. The default port number is 2598.

To configure server groups

To support business recovery, you can configure server groups to provide consistent connections to published applications and servers in the event of server disruption.

You can define up to three groups of servers: A primary server and two backup servers. Each group can contain from one to five servers.

When you specify a primary server group, Program Neighborhood contacts all servers within that group. When a server responds, you are connected. If all the servers in the primary group fail, Program Neighborhood contacts servers in the first backup group, and then in the second backup group, if necessary.

1. To configure a specific connection, open the Connection Manager dialog box. To configure defaults for all connections, open the Global ICA Client Settings dialog box.

2. Navigate to the server settings:

   - In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, click the Server tab, and then click the Server Location.

   - In the Global ICA Client Settings dialog box, click the Server Location tab.

3. Select the network protocol from the drop-down list at the bottom of the dialog box. The default server location protocol is TCP+HTTP browser. Configure this setting as directed by your administrator.

   - **TCP browser**. Uses the User Datagram Protocol (UDP) to locate servers. Program Neighborhood communicates with XenApp over TCP. Refer to "System Requirements" for server compatibility information.

   - **TCP + HTTP browser**. Uses the HTTP protocol to locate servers. Program Neighborhood communicates with XenApp using the ICA protocol over TCP. Select this option when using Program Neighborhood over the Internet or through a firewall or proxy server. This is the default protocol.

   - **SSL/TLS + HTTPS browser**. Uses the HTTPS protocol to locate servers. Program Neighborhood communicates with the server using ICA with SSL/TLS. SSL/TLS provides strong encryption of ICA traffic and server authentication. Select this option when using the client over the Internet, through a firewall or proxy server, or in a secure environment. When this setting is used, ICA encryption is available.

4. From the Server Group drop-down list, select a group to configure. You can configure your Primary, first backup (Backup 1), or second backup (Backup 2) group. The Address List box lists specific servers in the group you select.

5. To add a server to the selected group, click Add and enter the name or IP address of a computer running XenApp. If you selected the TCP+HTTP or SSL/TLS+HTTPS protocol in the Server Location dialog box, enter the server address and the port number.

6. If you are updating global settings, you can also rename your server groups by clicking Rename Group, which appends the name you enter to Primary, Backup 1, and Backup 2.

Improving Performance

If your Windows CE-based terminal device is using a bandwidth-limited connection, you can improve performance through settings on the Connection Manager Options tab.

Compress Data Stream

Data compression reduces the amount of data transferred during the ICA session. This requires additional processor resources to compress and decompress the data, but can improve performance over bandwidth-limited connections.

Select the option to reduce the amount of data transferred across the connection.

Enable SpeedScreen Multimedia Acceleration

SpeedScreen Multimedia Acceleration optimizes multimedia playback by streaming multimedia content to the client in its original compressed form. This reduces bandwidth consumption and CPU utilization on the server.

This feature has the following requirements:

- Your Windows CE-based terminal device must have the associated codec.
- Your Windows CE-based terminal device must have Windows Media Player 9 or above installed. Citrix recommends that you turn off visualizations when running Windows Media Player, as the visualizations may affect the performance of your client device.

SpeedScreen latency reduction

SpeedScreen latency reduction improves performance over high latency connections by providing instant feedback in response to typed data or mouse clicks.

- If you are not certain of the connection speed, set the SpeedScreen mode to Auto to turn SpeedScreen on or off depending on the latency of the connection.
- For bandwidth-limited connections (for example, if you are connecting over a WAN or a dial-in connection), set the mode to On to decrease the delay between user input and screen display.
- For connections over a high-speed LAN, set the mode to **Off**.

Use Disk Cache

Disk caching stores commonly used graphical objects such as bitmaps in a local cache on Program Neighborhood. For bandwidth-limited connections, using disk caching increases performance. For connections over a high-speed LAN, you do not need disk caching. For dial-in connections, disk caching is enabled by default.

Securing the Connection

To secure communication over your Program Neighborhood connection, you can use a range of security technologies, including:

- A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server, or SSL tunneling proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Program Neighborhood and servers. Program Neighborhood supports SOCKS and secure proxy protocols.

- A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using Program Neighborhood through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

- Encryption. Program Neighborhood supports two encryption protocols: ICA encryption and ICA with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

To configure a proxy server

If your network is using a proxy server, for example to limit access to the computers running Citrix XenApp, configure Program Neighborhood to connect to XenApp through the proxy server.

1. To configure a specific connection, open the Connection Manager dialog box. To configure defaults for all connections, open the Global ICA Client Settings dialog box.

2. Navigate to the server settings:

   - In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Firewall Settings tab.

   - In the Global ICA Client Settings dialog box, click the Firewall Settings tab.

3. Choose the proxy type from the Proxy drop-down list.

   - SOCKS. For connections to XenApp from outside of the firewall over a network that uses a SOCKS proxy server.

     Important: SOCKS is not compatible with UDP browsing.

   - Secure (HTTPS). For connections to XenApp from outside of the firewall over a network that uses a secure proxy server.

     Important: If Program Neighborhood is configured for TCP browsing and secure proxy, specify at least one server on the Server Location tab to enable server and published application browsing.

4. In the Proxy address box, enter the proxy server’s IP address or DNS name. If you do not have this information, contact your help desk.

5. In the Port box, enter the proxy server port number (if different from 1080).

6. If you chose the Secure (HTTPS) proxy type and want to enable SSL/TLS relay, enter the address of the relay and the port number in the appropriate boxes. If you do not have this information, contact your help desk. A message reminds you that you need to use SSL or 128-bit encryption to ensure a secure connection.

To enable automatic proxy detection

You can configure Program Neighborhood to use the proxy server specified in the Web browser settings.

1. To configure the Web browser on your terminal device, open the Internet Options dialog box and then:

   a. Click the Connection tab and select the Access the Internet using a proxy server check box.

   b. In the Address box, enter the default proxy server IP address.
2. In the Global ICA Client Settings dialog box, click the Firewall Settings tab and select the Use Web browser proxy settings check box.

To use alternate address translation

If the firewall uses address remapping, configure Program Neighborhood to use the alternate address returned by the data collector. This is necessary whether or not you are using a SOCKS or secure proxy server.

1. To configure a specific connection, open the Connection Manager dialog box. To configure defaults for all connections, open the Global ICA Client Settings dialog box.

2. Navigate to the server settings:

   · In the Connection Manager dialog box, click the name of the connection that you want to change, click Edit, and then click the Firewall Settings tab.

   · In the Global ICA Client Settings dialog box, click the Firewall Settings tab.
3. Click Use alternate address through firewalls.

To configure encryption

Program Neighborhood supports two levels of encryption:

· ICA encryption: Provides strong encryption to increase the privacy of your ICA connections. Use this encryption level with the TCP and TCP+HTTP network protocols.

· ICA with SSL/TLS: Provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server to which you are connecting is a legitimate server. To use SSL/TLS you must set the Server Location protocol in the Server Location dialog box to SSL/TLS+HTTPS.

1. In the Connection Manager dialog box, select the option for editing a connection according to the instructions for your Windows-based terminal.

2. Click the name of the connection that you want to change and click Edit.

3. Click the Options tab.

4. Select the level of encryption to be used during authentication from the Encryption Level list. The default level is Basic.

   Important: The encryption level specified for Program Neighborhood must be less than the level specified for XenApp. If you do not have this information, contact your help desk.

5. If you choose ICA with SSL/TLS, click the Firewall Settings tab and in the Address of relay box enter the SSL/TLS relay's fully qualified domain name (FQDN). If directed by your administrator, also enter the relay port number.

Troubleshooting Program Neighborhood

Codecs issues

- Compatibility issues may occur between codecs installed on the client device and on the server. If this occurs, investigate using different codecs.
- Playing a file that requires a codec that is available on the client but not on the server can cause Windows Media Player to fail on the server.

Audio and video limitations

- Switching between video clips frequently may cause the client to become unresponsive or close unexpectedly.
- Using the media player slider function frequently, or stopping and starting a video frequently, may cause the video to freeze.
- When playing a playlist, the audio portion of the videos may degrade after the first video on some players. If this occurs use RealOne Player to play the videos.
- Playing videos in Full Mode using Windows Media Player, or with a skin other than the default skin using RealOne Player, when the application is running in seamless mode causes the video to appear on top of everything else on the screen. If this occurs play videos in Skin Mode (Windows Media Player) or with the default skin (RealOne Player).
- On some client devices, covering the video display with another window or pressing CTRL+ALT+DEL can cause the video to freeze in the display.
- On some client devices, the video display stays on top of all other windows after the video has finished.
- Any synchronization issues that occur when playing a video file locally on the client may worsen when playing the file using SpeedScreen Multimedia Acceleration.
- If the volume control does not function correctly, make sure that the client device audio drivers are compatible with the soundcard.

Printing to a network printer

To print from a connected application to a network printer requires an alternate configuration if the printer is on the same side of a firewall as the Windows CE-based terminal device, but the server is on the other side and the printing port is not open. In this case, configure the network printer as if it is local to the terminal device and allow Program Neighborhood itself to print to the printer. This avoids the need for any traffic through the firewall apart from the existing Program Neighborhood connection.

Important: Only the first locally defined network printer is handled in this way, so if you need simultaneous access to network printers on the server side of the firewall as well as on the client side, locally define the client-side network printer first and then any server-side network printers.

Configure the network printer using the terminal device control panel (called “RDP”). When a Program Neighborhood connection is established, this network printer is identified as “LPT4:”, as if it were local to the terminal device. You can then use it within the session as a normal printer.