Cisco Virtualization Experience Client 2112/2212 ICA Administration Guide for WTOS 7.0_214

July 3, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-215152-01

Cisco Virtualization Experience Client 2112/2212 ICA Administration Guide for WTOS 7.0_214

CONTENTS

Preface

Overview

The Cisco Virtualization Experience Client (VXC) 2112 and 2212 are workstation-class virtualization clients that run WTOS firmware for use with the Independent Computing Architecture (ICA) and the Remote Desktop Protocol (RDP). The ICA and RDP protocols are designed to deliver a user desktop from a centralized host server across standard IP networks, enabling you to use applications and desktop peripherals as if you were using them locally.

The Cisco VXC 2112 and Cisco VXC 2212 are highly optimized zero clients that provide ultra-fast access to applications, files, and network resources available on machines hosted by Citrix infrastructures. WTOS uses the Cisco VXC engine to provide a secure, near-zero management core that requires no local antivirus software or firewall to protect against viruses or malware.

Session and networks services available on enterprise networks may be accessed on enterprise networks, a direct intranet connection, or from a remote location using a secure gateway from Citrix.

Audience

This guide is intended for administrators of Cisco VXC running WTOS. It provides information and detailed system configurations to help you design and manage a WTOS environment.

Organization

This manual is organized as described in the following table.

Chapter	Description
Chapter 1, “Getting Started”	Provides information on getting started
Chapter 2, “Features”	Describes the main features and how to configure them
Chapter 3, “Configuring Connectivity Options”	Describes how to configure the ways to connect the client to the network
Chapter 4, “Configuring Local Settings Options”	Describes how to configure client local options
Chapter 5, “Performing Diagnostics”	Describes how to diagnose client problems

Chapter	Description
Appendix A, "Central Configuration: Automating Updates and Configuration"	Describes methods for automating client configuration and updates
Appendix B, "Remote System Administration"	Describes the remote system administration
Appendix C, "Local System Administration"	Describes client (local) administration
Appendix D, "Setting Up Your HTTPS/SSL Web Server"	Describes how to set up the web server
Appendix E, "Cisco VXC 2112/2212 Power Considerations,"	Describes Power over Ethernet (PoE) support for the Cisco VXC

Related Documentation

For more information, see the documents available at the following URLs:

Cisco Virtualization Experience Client 2000 Series

http://www.cisco.com/en/US/products/ps11499/tsd_products_support_series_home.html

Cisco Virtualization Experience Client Manager

http://www.cisco.com/en/US/products/ps11582/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following convention:

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

CHAPTER 1

Getting Started

WTOS is designed to be centrally managed and configured using INI files, although it can be used in environments without central configuration for basic connectivity needs. In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all Cisco VXC Clients (zero clients) in your WTOS environment.

This chapter includes:

Connecting to a Remote Server

Central Configuration

If you are set up for automatic detection (using INI files—see *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*), your zero client automatically detects and connects to the configured remote services during the boot-up process.

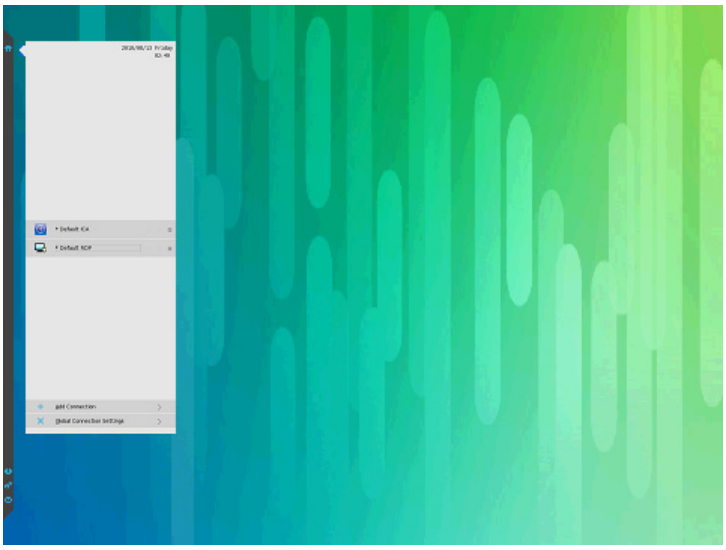
Simply press the power button to turn on your zero client to see the Login dialog box. Enter your username, password, and domain, and then click **Login**. After successful authentication, your available connections are presented for use.

Although the zero client defaults to the Classic Desktop for INI backward compatibility, you can configure the zero client to display the Cisco VXC desktop by using the SysMode=VDI parameter in the INI files or by selecting the desktop option in a dialog box (see Using Your Desktop, page 1-4).

Manual Connection

If you are not yet set up for central configuration, you see the Cisco VXC toolbar, where you can configure the initial server connection you want using the Remote Connections dialog box before you log in. See Manual Connection Procedures, page 1-2.

Figure 1-1 Manual Connection



You need to only complete this manual configuration once (or after reboot to factory defaults). After the zero client knows the location of your server, it automatically connects to the server for login when you start the zero client in the future. After you confirm that your environment is ready for deployment, you can create INI files for central configuration.

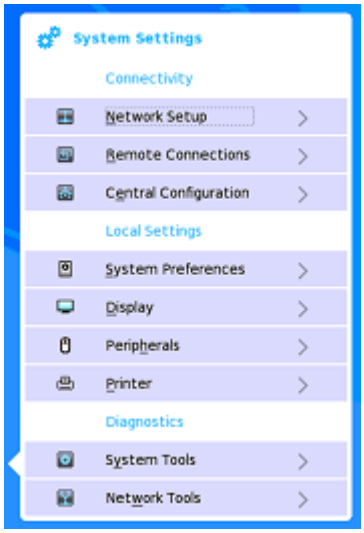
Manual Connection Procedures

Your system administrator will provide the specific steps and information necessary for you to log in to your Cisco VXC client.

One of the standard ways to log in to a Citrix Virtual Machine (VM) is to set up a broker server by clicking **Remote Connections**, selecting **Citrix Xen**, restarting the Cisco VXC client, and then entering login credentials. However, another procedure may be supplied by your system administrator.

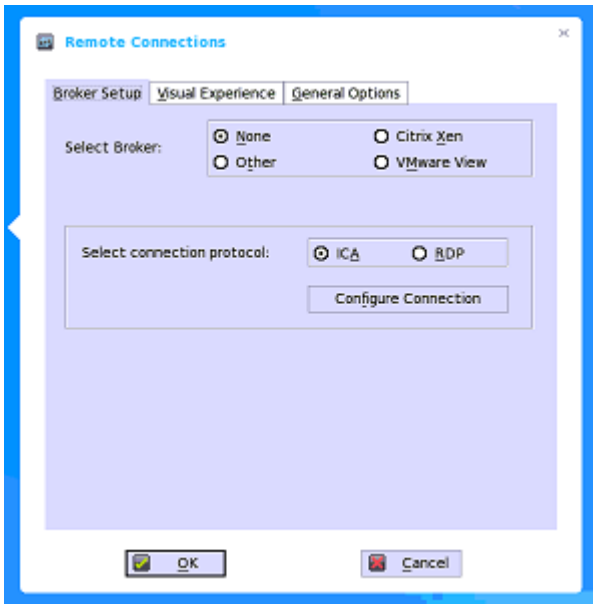
Procedure

Step 1 Click the System Settings icon on the Cisco VXC toolbar to open the System Settings menu, and then click **Remote Connections** to open the Remote Connections dialog box.



Step 2 Use the Broker Setup tab of the Remote Connections dialog box to configure one of the following connections:

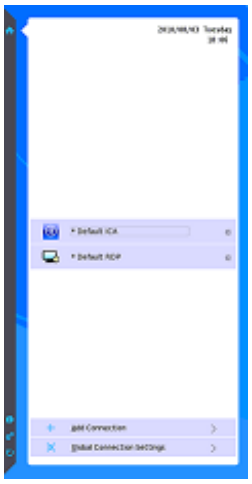
- ICA or RDP connection (select **None**, select **ICA** or **RDP**, click **Configure Connection**, and then follow the wizard)
- A specific broker server connection (select **Other**, **Citrix Xen**, or **VMware View**, and then enter the IP address for the server in the Broker Server field)



Note For more details, see Remote Connections, page 3-7.

Step 3 Click **OK**, and then restart the zero client by clicking the Shutdown icon on the Cisco VXC toolbar to open and use the Shutdown dialog box to restart the zero client.

- (For ICA or RDP Connections) After the zero client restarts, click the Home icon on the Cisco VXC toolbar to open the list of available connections, click the ICA or RDP connection you created, and then log in.



- (For Specific Broker Server Connections) After the zero client restarts, the Login dialog box appears for your server.

Figure 1-2 Login

Step 4 Enter the User Name, Password, and Domain, and click **Login**.

After successful authentication, your Cisco VXC toolbar displays with your assigned connections defined by the broker server.

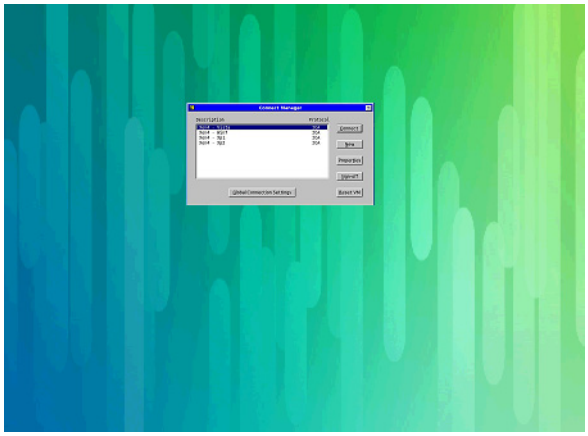
Using Your Desktop

What you see after logging in to the server depends on the administrator configurations.

- Users with a Classic Desktop—See the classic desktop with full task bar, desktop, and Connect Manager. This option is recommended for terminal server environments with published applications.

  For more information on using the Classic Desktop, see Additional Classic Desktop Features, page 2-7.

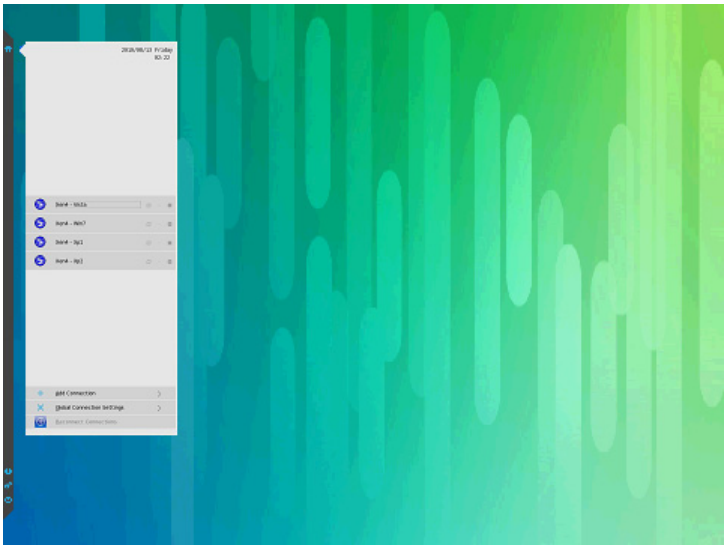
Figure 1-3 Classic Desktop



- Users with a Cisco VXC desktop—See the Cisco VXC desktop with the Cisco VXC toolbar showing the assigned list of connections from which to select. This option is recommended for VDI and any full-screen-only connections.

  For more information on using the Cisco VXC desktop, see Additional Cisco VXC desktop Features, page 2-5.

Figure 1-4 Cisco VXC Desktop

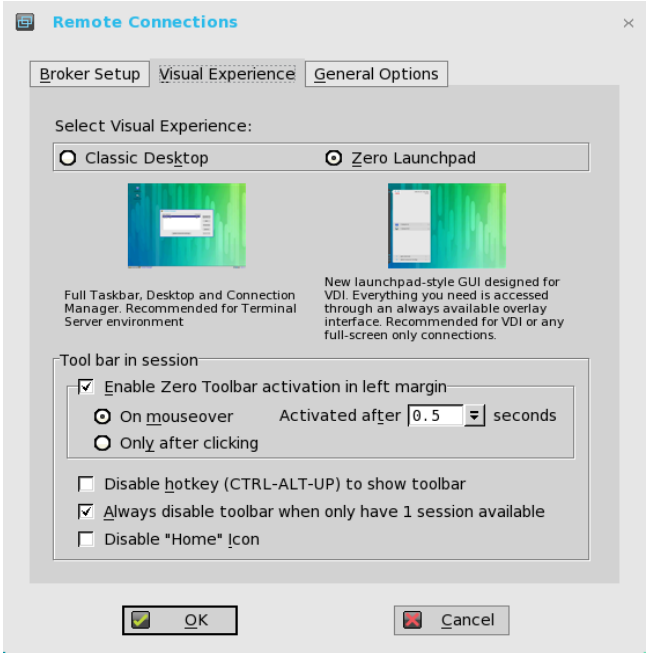


In any desktop case, you can select the desktop option you want (Classic Desktop or Cisco VXC desktop) and create the connections you need using the Remote Connections dialog box (see Remote Connections, page 3-7).

To open the Remote Connections dialog box, do one of the following:

- Classic Desktop—Click **User Name** (User Name is the name of the user who is logged in and the name is displayed at the bottom-left side of the task bar), and then select **System Setup > Remote Connections**.
- Cisco VXC desktop—Click the **System Settings** icon on the Cisco VXC toolbar, and then select **Remote Connections**.

Figure 1-5 Remote Connections



Locking the Zero Client

To help ensure that no one else can access your private information without permission, WTOS allows you to lock your zero client so that credentials are required to unlock and use the zero client after you do one of the following:

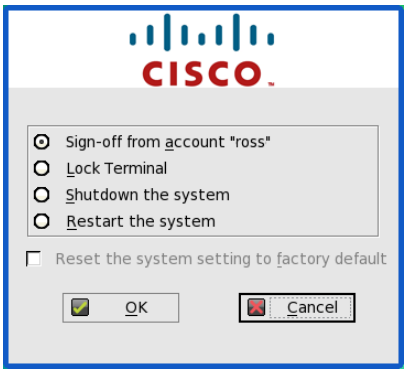
- Use LockTerminal from the shortcut menu and Shutdown dialog box—On the Classic Desktop, click on the desktop and select Lock Terminal, or use the Shutdown dialog box (see Additional Classic Desktop Features, page 2-7). On the Cisco VXC desktop, use the Shutdown dialog box (see Signing Off and Shutting Down, page 1-6). To open the zero client for use, you must use your correct password.
- Use the screen saver—If an administrator has set LockTerminal=2 for the ScreenSaver parameter in the INI files and you use the screen saver, then the zero client will lock. To open the zero client for use, you must use your correct password.

Signing Off and Shutting Down

Use the Shutdown dialog box (Classic Desktop—click **Shutdown** in the Connect Manager or Desktop Menu; Cisco VXC desktop—click the **Shutdown** icon on the Cisco VXC toolbar) to select the available option you want.

Tip You can also configure automatic behavior after all desktop sessions are closed by using the Remote Connections dialog box (see Remote Connections, page 3-7) or the AutoSignoff parameter in a wnos.ini file (see Appendix A, “Central Configuration: Automating Updates and Configuration”).

Figure 1-6 Shutdown



Use the following guidelines (depending on user privilege, some options may not be available for use):

Table 1-1 Shutdown dialog box options

Option	What It Does
Sign-off from account	Allows you to log out from the current open account (the Login dialog box appears and is ready for another user).
Lock Terminal	Locks the zero client from use until you log in again.
Shutdown the system	Turns off the zero client.
Restart the system	Logs out the user account (the Login dialog box appears after the zero client restarts).
Reset the system setting to factory default	Appears for high-privileged users/administrators only. This option allows you to reset the zero client to factory defaults (see Resetting to Factory Defaults Using Shutdown Reset, page C-1).

CHAPTER 2

Features

This chapter includes:

Login Dialog Box Features

While the Login dialog box allows you to log in to the server, it also allows you to obtain system information, configure zero client settings, and shut down the zero client.

Figure 2-1 Login

Use the following guidelines:

- Sys Info—Click the **Sys Info** button to open the System Information dialog box and view the zero client system information such as System Version, IP Address, information on devices connected to your zero client, event logs, and so on (see Accessing System Information, page 2-2).
- Admin Mode—Click the **Admin Mode** button to configure various settings locally on the zero client (not broker desktop configurations). For example, you can choose to manually configure the Citrix Xen Broker Server URL (or override the URL that is centrally defined by file servers) by using the Remote Connections dialog box as described in Remote Connections, page 3-7.

Tip By default there is no password needed for Admin Mode button use. You can password protect the Admin Mode button (to require login credentials) by using the AdminMode parameter in a wnos.ini file (see *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*).

- Shutdown—Click the **Shutdown** button to open and use the Shutdown dialog box to log out, shut down, restart, reset the system setting to factory defaults, and so on (see Signing Off and Shutting Down, page 1-6).

Accessing System Information

Use the System Information dialog box to view the following system information (Classic Desktop—click **System Information** in the Desktop Menu; Cisco VXC desktop—click the **System Information** icon on the Cisco VXC toolbar):

- General Tab—Displays general information such as System Version, Serial Number, Boot From, Memory Size (Total and Free), Terminal Name, IP Address, Net Mask, Gateway, and DHCP Lease.
- Devices Tab—Displays information about devices such as the CPU Speed, ROM Size, Monitor, Parallel Ports, Ethernet Speed, Memory Speed, NAND Size, Resolution, Serial Ports, and the zero client MAC Address.
- Copyright/Patents Tab—Displays the software copyright and patent notices.
- Event Log Tab—Displays the zero client startup steps (normally beginning from System Version to Checking Firmware) or error messages that are helpful for debugging problems.
- Status Tab—Displays status information about TCP performance-related parameters, CPU Busy, System Up Time, Free Memory, and DHCP lease time remaining.

Manually Configuring Global Connection Settings

If you do not use INI files to provide central configuration (global connection settings) to users, you can click **Global Connection Settings** (in the Connect Manager for the Classic Desktop; in the List of Connections for the Cisco VXC desktop) to open and use the Global Connection Settings dialog box to configure settings that affect all of the connections in your list of connections.

Tip For information on configuring the zero client using INI files (recommended), see *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*. For information on configuring the zero client locally using dialog boxes, refer to Configuring Connectivity Options and Configuring Local Settings Options.

Session Tab

Figure 2-2 shows the Session tab.

Figure 2-2 Session

Use the Session tab to select the check boxes you want for the options that are available to all sessions (the Smart Cards check box specifies the default setting for connecting to a smart card reader at startup).

Tip

When using the Disks check box for automatic connection to connected USB sticks, use the following guidelines:

- Support is for VFAT File System only; be sure that the USB stick you use is formatted to FAT16 or FAT32.
- More than one disk can be used at the same time, however, the maximum number of USB sticks (including different subareas) is 12.
- It recommended that you use Windows XP, Windows Server 2003, or Windows Server 2008 for the server.
- Be sure to save all data and sign off from the session mapping the USB stick before removing the USB stick.

ICA Tab

Figure 2-3 shows the ICA tab.

Figure 2-3 ICA

Use the ICA tab to select the check boxes you want for the options that are available to all ICA sessions. Note the following:

- Map to—When a drive is entered, maps a disk under the drive.
- Map all disks under (z:)—When selected, maps all disks under the Z drive.

RDP Tab

Figure 2-4 shows the RDP tab.

Figure 2-4 RDP

Use the RDP tab to enable or disable Network Level Authentication (NLA). The NLA authentication method verifies users before they are allowed to connect with a full Remote Desktop connection.

Additional Cisco VXC desktop Features

This section includes information on:

Cisco VXC Interactive Desktop Guidelines

The Cisco VXC desktop has a Cisco default background with the Cisco VXC toolbar at the left of the screen.

Use the following guidelines:

- If configured to display (by an administrator), the current date and time are shown on the Cisco VXC toolbar.

Tip The zero client is capable of synchronizing its clock to time provided by a Simple Network Time Protocol (SNTP) server.

- Press Ctrl-Alt-Up Arrow to display the Cisco VXC toolbar.
- Press Ctrl-Alt-Down Arrow to open a selection box for toggling between the desktop and currently-active connections.
- Lock the zero client at any time by pressing Ctrl-Alt-Left Arrow or Ctrl-Alt-Right Arrow.
- Keyboard shortcuts are supported. Use the LEFT Alt-UNDERLINED LETTER on the keyboard for keyboard shortcuts (the RIGHT Alt-UNDERLINED LETTER combination is not currently supported).
- Use the Peripherals dialog box to switch the left and right buttons (see Peripherals, page 4-8).
- In addition to the standard two-button mouse, the zero client supports a wheel mouse (used for scrolling). Other similar types of wheel mouse may or may not work.
- Press Print Screen to capture a full desktop or Alt-Print Screen to capture the active window.
- You can copy and paste between application sessions and between sessions and the desktop; however, this function depends on session server configurations.

Cisco VXC toolbar

The Cisco VXC toolbar usually appears at the left edge of the Cisco VXC desktop. However, depending on administrator configurations, the toolbar can be removed or hidden (shown only when a user moves the mouse pointer over the left edge of the desktop screen).

Table 2-1 Toolbar Icons

Icon	What it does
Home 	Opens the list of available connections (see List of Connections, page 2-6).
System Information 	Displays zero client system information (see Accessing System Information, page 2-2).
System Settings 	Opens the System Settings menu to configure zero client system settings and perform diagnostics (see Configuring Connectivity Options, page 3-1, Configuring Local Settings Options, page 4-1, and Appendix A, "Central Configuration: Automating Updates and Configuration").
Shutdown Terminal 	Click the Shutdown Terminal icon to use the Shutdown options available on the zero client (see Signing Off and Shutting Down, page 1-6). Note that the Shutdown Terminal icon does not display on the toolbar when using the Admin Mode button to configure system settings.

Tip Administrators can configure the toolbar settings using either a dialog box (see Remote Connections, page 3-7) or the SysMode parameter in the wnos.ini file (see *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*).

List of Connections

On the Cisco VXC toolbar, you can click the **Home** icon to open your list of assigned connections (in some cases the list may contain only default connections).

Figure 2-5 List of Connections

Use the following options (depending on user privilege level, some options may not be available for use):

Table 2-2 Connection Options

Option	What it does
Name of the connection	Opens the connection you want to use (all open connections display a blue icon to the left of the connection name in the list).
Restart icon 	Restarts the connection (useful when a connection is not functioning properly or you need to reboot the connection).
Quick Disconnect icon 	Closes the connection (the Close icon is dimmed for connections that are not open).
Edit icon 	Opens the Connection Settings dialog box (see Advanced Details on Configuring ICA and RDP Connections, page 3-11) to change the connection options (depending on user privilege level, editing options may not be available for use).
Configuring Global Connection Settings	If you do not use INI files to provide global connection settings, you can click **Global Connection Settings** to open and use the Global Connection Settings dialog box to configure settings that affect all of the connection in the list (see Manually Configuring Global Connection Settings, page 2-2).

Additional Classic Desktop Features

This section includes information on:

- Classic Interactive Desktop Guidelines, page 2-8
- Shortcut Menu, page 2-8
- Desktop Menu, page 2-9

- Connect Manager, page 2-10

Classic Interactive Desktop Guidelines

The Classic Desktop has a Cisco default background with a horizontal task bar at the bottom of the screen. The number of icons that can be displayed on the desktop depends on the desktop resolution and administrator configuration.

Use the following guidelines:

- Icons representing available server connections and published applications are displayed on the background. Hovering the mouse pointer over an icon pops-up information about the connection. Right-clicking (or left-clicking if the mouse buttons are reversed) on an icon opens a Connection Settings dialog box which displays additional information about the connection.
- A server connection/published application can be opened by double-clicking a desktop icon or a user can navigate to the desktop icon they want by using tab key and pressing Enter to initiate the connection.
- The desktop menu may be opened by clicking the mouse button on the desktop background or by clicking on the User Name on the task bar.
- If configured to display (by an administrator), the volume control is displayed in the right corner of the task bar and the current time and date are shown when the cursor is placed on the time.

Tip The zero client is capable of synchronizing its clock to time provided by a Simple Network Time Protocol (SNTP) server.

- Press Ctrl-Alt-Up Arrow to toggle between window display modes.
- Press Ctrl-Alt-Down Arrow to open a selection box for toggling between the desktop, Connect Manager, and currently-active connections.
- Lock the zero client at any time by pressing Ctrl-Alt-Left Arrow or Ctrl-Alt-Right Arrow.
- Keyboard shortcuts are supported. Use the left Alt-Underlined Letter on the keyboard for keyboard shortcuts (the right Alt-Underlined Letter combination is not currently supported).
- Use the System Preference dialog box to switch the left and right buttons (see System Preference, page 4-2).
- In addition to the standard two-button mouse, the zero client supports a Microsoft Wheel Mouse (used for scrolling). Other similar types of a wheel mouse may or may not work.
- You can copy and paste between application sessions and between sessions and the desktop, however, this function depends on session server configurations.

Shortcut Menu

Right-clicking on the desktop provides a shortcut menu with the following options:

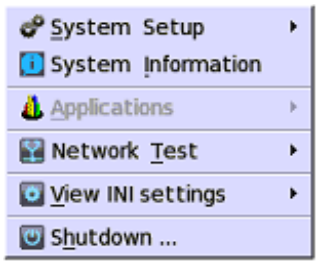
- Administrator Mode—Allows administrators to configure various settings locally on zero client.
- Hide all windows—Brings the full desktop to the foreground.
- Copy to clipboard—Copies an image of the full screen, current window, or event log to the clipboard. The clipboard contents can then be pasted to an ICA or an RDP session.

- Purge clipboard—Discards the contents of the clipboard in order to free up memory.
- Group Sessions—Enables you to open more than three ICA or three RDP or three ICA seamless sessions. The sessions will be displayed as a group on the task bar.
- Lock Terminal—Puts the zero client in a locked state if the user has signed on to the system with a password. The zero client can only be unlocked using the same password.

Desktop Menu

Clicking the User Name (User Name is the name of user who is logged in and the name is displayed at the bottom-left side of the task bar), or clicking on the desktop, opens the desktop menu with the following options (for High-privileged and Low-privileged users only):

Figure 2-6 Desktop Menu



- System Setup—Provides access to the following local system setup dialog boxes:
  - Network Setup—Allows selection of DHCP or manual entry of network settings, as well as entry of locations of servers essential to zero client operation. This menu selection is disabled for low-privileged users. See Network Setup, page 3-2.
  - Remote Connections—Allows you to configure zero client network connections including ICA, RDP, Citrix Xen, and other broker server connections. See Remote Connections, page 3-7.
  - Central Configuration—Allows you to configure zero client central connection settings such as file server and optional VXC Manager server settings. See Central Configuration, page 3-10.
  - WAN Setup—Allows you to configure zero client WAN.
  - System Preference—Allows user selection of zero client parameters that are a matter of personal preference. See System Preference, page 4-2.
  - Display—Allows you to configure the monitor resolution and refresh rate. See Display, page 4-5.
  - Peripherals—Allows you to select the peripherals settings such as keyboard, mouse, volume, and touch screen settings. See Peripherals, page 4-8.
  - Printer—Allows configuration of network printers and local printers that are connected to the zero client. See Printers, page 4-12.
- System Information—Provides zero client system information. See Accessing System Information, page 2-2.
- Applications—Contains a submenu of all locally configured applications and is populated with published applications when a user is signed on using either PNLite or PNAgent.
- Network Test—Opens a submenu from which the Ping and Trace Route tools can be used to check the integrity of the network connection. See Using Ping, page 5-3 and Using Trace Route, page 5-4.

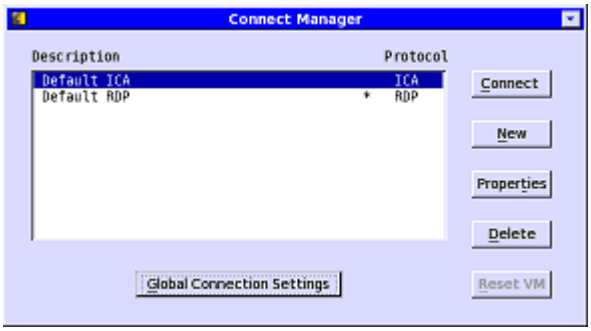
- View INI Settings—Opens a submenu from which the wnos.ini and user.ini windows can be opened to view the contents of the files. See System Tools, page 5-2.
- Shutdown—Opens the Shutdown dialog box. See Signing Off and Shutting Down, page 1-6.

Connect Manager

Clicking Connect Manager on the task bar opens the Connect Manager. The Connect Manager has a list of connection entries and a set of command buttons available for use with the connections.

Tip Non-privileged users cannot view the Connect Manager.

Figure 2-7 Connect Manager



The command buttons available depend on the privileges of the user and administrator configuration; the following default examples are typical:

- High-privileged user—Includes Connect, New, Settings, and Sign-off
- Low-privileged user—Includes Connect, Settings, and Sign-off
- Standalone user—Includes Connect, New, Settings, and Delete

Tip If set by an administrator (enablelocal=yes in the user.ini/wnos.ini file), high-privileged and low-privileged users will have the Delete command button available instead of the Sign-off command button).

The use associated with these command buttons also depends on user privilege. For example, Settings allows a high-privileged user to view and edit connection definitions, while it allows a low-privileged user to only view connection definitions.

Tip Guest-user privileges are determined by an administrator.

The Connect Manager command buttons include:

- Connect—To make a connection, select a connection from the list and click **Connect**.

- New—Clicking New opens the Connection Settings dialog box either directly or through the Connection Protocol menu selection for creating a new connection definition (for more information on the Connection Settings dialog box, refer to Advanced Details on Configuring ICA and RDP Connections, page 3-11). The new locally-defined connections are added to the connection list. Be aware of the following information:
  - High-privileged user—Typically, all locally-defined connection definitions are temporary and are lost when the user logs off and when the zero client restarts or is shut down. However, if configured by an administrator (enablelocal=yes), locally-defined connection definitions can be saved in these cases.
  - Standalone user —Locally defined connections are retained when the zero client restarts or is shut down (there is no individual login). Network configuration settings must be made locally.
- Properties—Clicking Properties opens the Connection Settings dialog box for the selected connection (for more information on the Connection Settings dialog box, refer to Advanced Details on Configuring ICA and RDP Connections, page 3-11). Be aware of the following information:
  - High-privileged user—Can view and edit the definitions for the currently selected connection. Edits are not permanently retained when the user signs-off.
  - Low-privileged user—Cannot create or edit connections, but can view connection definitions.
  - Standalone user—Can permanently modify the persistent connections (except when PNAgent/PNLite services are used).
- Sign-off—To sign-off from the zero client, click **Sign-off**.
- Delete—To delete a connection, select a connection from the list and click **Delete**.
- Reset VM—To reset a virtual connection, select a virtual connection from the list and click **Reset VM**.
- Global Connection Settings—If you do not use INI files to provide global connection settings, you can click Global Connection Settings to open and use the Global Connection Settings dialog box to configure settings that affect all of the connections in the list (see Manually Configuring Global Connection Settings, page 2-2).

CHAPTER 3

Configuring Connectivity Options

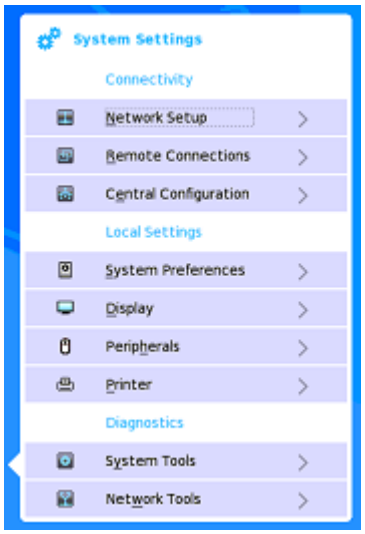
You can configure the following Connectivity options using zero client dialog boxes (depending on user privilege level, some options may not be available for use):

Tip While it is not recommended to use zero client dialog boxes for configuring Connectivity options, they are available in case you want to temporarily override central default configurations or you do not have the option to set up central configuration (smaller environments). In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all zero clients in your WTOS environment (see Appendix A, "Central Configuration: Automating Updates and Configuration").

To access Connectivity options:

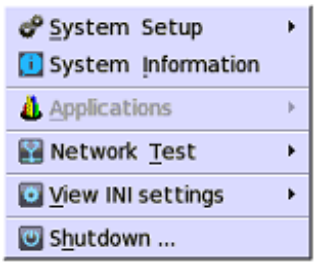
- Cisco VXC desktop—click the **System Settings** icon on the Cisco VXC toolbar (administrators can also click the **Admin Mode** button in the Login dialog box).

Figure 3-1 System Settings



- Classic Desktop—click **User Name** (User Name is the name of the user who is logged in and the name is displayed at the bottom-left side of the task bar), and select **System Setup**.

Figure 3-2 User Name Menu



Network Setup

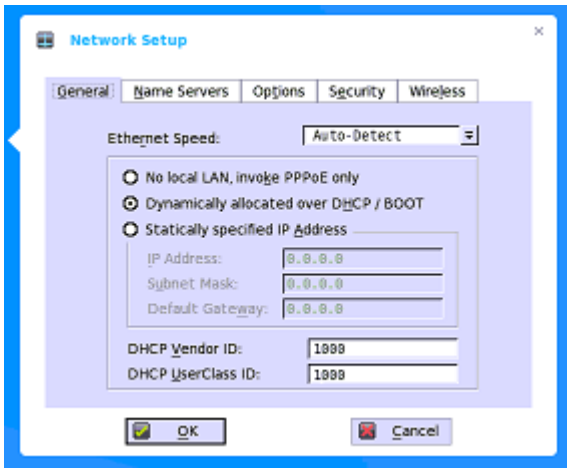
The Network Setup dialog box allows you to configure zero client network settings.

Tip If required by the operating environment, the network administrator may disable access to this dialog box. Specifically, it cannot be accessed by Low-privileged and Non-privileged users (and not until after log-on if using PPPoE access).

General Tab

Figure 3-3 shows the General tab.

Figure 3-3 Network Servers—General



Use the following guidelines for the General tab:

- Ethernet Speed—Normally the default (Auto-Detect) should be selected, but another selection can be made if automatic negotiation is not supported by your network equipment. Selections include Auto-Detect, 10 Mb Half-Duplex, 10 Mb Full-Duplex, 100 Mb Half-Duplex, 100 Mb Full-Duplex.

Tip The 10 Mb Full-Duplex option can be selected locally at the device; however, this mode may need to be negotiated through Auto-Detect.

- No local LAN, invoke PPPoE only—Select this option if the zero client will access a network through a PPPoE connection.
- Dynamically allocated over DHCP/BOOTP—Selecting this option enables the zero client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server (using DHCP options) to provide information. Any value provided by the DHCP server will replace any value entered locally on the Options tab, however, locally entered values will be used if the DHCP server fails to provide replacement values.
- Statically specified IP Address—Select this option to manual enter the IP Address, Subnet Mask, and Default Gateway:
  - IP Address—Must be a valid network address in the server environment. The network administrator must provide this information.
  - Subnet Mask—Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices: same subnet or other subnet. If the location is other subnet, messages sent to that address must be sent through the Default Gateway, whether specified through local configuration or through DHCP. The network administrator must provide this value.
  - Default Gateway—Use of gateways is optional. Gateways are used to interconnect multiple networks (routing or delivering IP packets between them). The default gateway is used for accessing the Internet or an intranet with multiple subnets. If no gateway is specified, the zero client can only address other systems on the same subnet. Enter the address of the router that

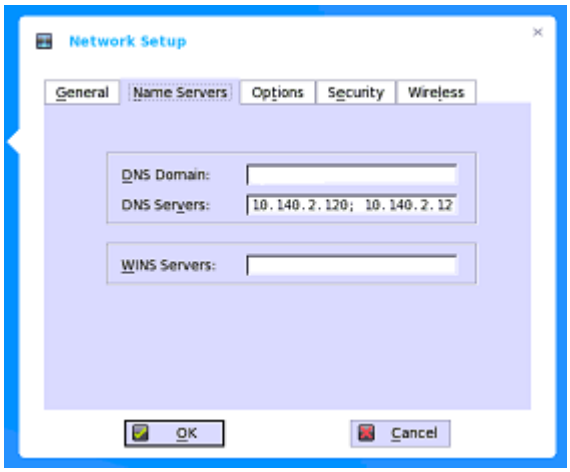
connects the zero client to the Internet. The address must exist on the same subnet as the zero client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.

- DHCP Vendor ID—Shows the DHCP Vendor ID when the Dynamically allocated over DHCP/BOOTP option is selected.
- DHCP UserClass ID—Shows the DHCP UserClass ID when the Dynamically allocated over DHCP/BOOTP option is selected.

Name Servers Tab

Figure 3-4 shows the Name Servers tab.

Figure 3-4 Network Setup—Name Servers



Use the following guidelines for the Name Servers tab:

- DNS Domain and DNS Servers—Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than DNS will be used to make the connection. Enter the DNS Domain and the network address of an available DNS Server. The function of the DNS Domain entry is to provide a default suffix to be used in name resolution. The values for these two boxes may be supplied by a DHCP server. If the DHCP server supplies these values, they will replace any locally configured values. If the DHCP server does not supply these values, the locally configured values will be used.

Tip You may enter two DNS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary DNS server and the second is for a backup DNS server.

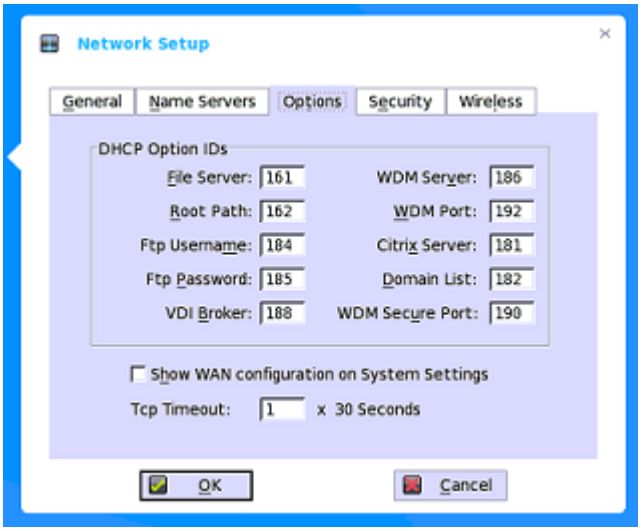
- WINS Servers—Use of WINS is optional. Enter the network address of an available WINS name server. WINS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than WINS will be used to make the connection. These entries can be supplied through DHCP if DHCP is used. DNS and WINS provide essentially the same function, name resolution. If both DNS and WINS are available, the zero client will attempt to resolve the name using DNS first and then WINS.

Tip You may enter two WINS Server addresses (primary and secondary), separated by a semicolon, comma, or space.

Options Tab

Figure 3-5 shows the Options tab.

Figure 3-5 Network Setup—Options



Use the following guidelines for the Options tab:

- DHCP Option IDs—Enter the supported DHCP options (each value can only be used once and must be between 128 and 254). For information on DHCP options, refer to Configuring DHCP (DHCP Options), page A-9.
- Show WAN configuration on System Settings—Allows you to show the WAN configuration on the System Settings submenu.
- Tcp Timeout—Enter the number that is multiplied by 30 seconds for the timeout value of a TCP connection. The value must be between 1 and 255, which means the connection timeout value is from 1 x 30 seconds to 255 x 30 seconds.

Security Tab

Figure 3-6 shows the Security tab.

Figure 3-6 Network Setup—Security

Use the following guidelines for the Security tab:

- Enable IEEE 802.1x authentication—Select this check box to enable this authentication and activate the EAP Type list of options.
- EAP Type—If you have enabled the Enable IEEE 802.1x authentication check box, select the EAP Type option you want (TLS, LEAP, or PEAP).
  - TLS—If you select the TLS option, click **Properties** to open and configure the Authentication Properties dialog box (you can use Browse to find and select the Client Certificate file and Private Key file you want). Note that the CA certificate must be installed on the zero client.
  - LEAP—If you select the LEAP option, click **Properties** to open and configure the Authentication Properties dialog box (be sure to use the correct username and password for authentication). Note that the maximum length for the username or the password is 64 characters.
  - PEAP—If you select the PEAP option, click **Properties** to open and configure the Authentication Properties dialog box (be sure to select either **EAP_GTC** or **EAP_MSCHAPv2**, and then use the correct Username, Password, and Domain, if necessary, for authentication). To configure EAP-GTC, enter the username only, and the password or PIN will be asked when authenticating. To configure EAP-MSCHAPv2, enter the username, password, and domain (domain\username in the username box is supported, but you must leave the domain box blank). Note that the CA certificate must be installed on the zero client (the server certificate is forced to be validated).
- Certificate Management—Opens the Certificates Browser where you can select the Import From option you want to import a certificate (either USB Storage or File Server).
  - USB Storage—If you select the USB Storage option, click **Import** to open and use the Import dialog box to find and select the certificate you want to use. The maximum importing path is limited to 128 characters and the maximum certificate name is limited to 64 characters.
  - File Server—If you select the File Server option, click **Import** to open and use the Import dialog box to enter the detailed path to the certificate you want to use in the File Servers box (if necessary, be sure to use the correct Username and Password). Note that you must enter the

absolute path of the certificate. For example: 10.151.121.100/wnos/cacerts/mycertificate.cer. The maximum importing path is limited to 128 characters and the maximum certificate name is limited to 64 characters.

Remote Connections

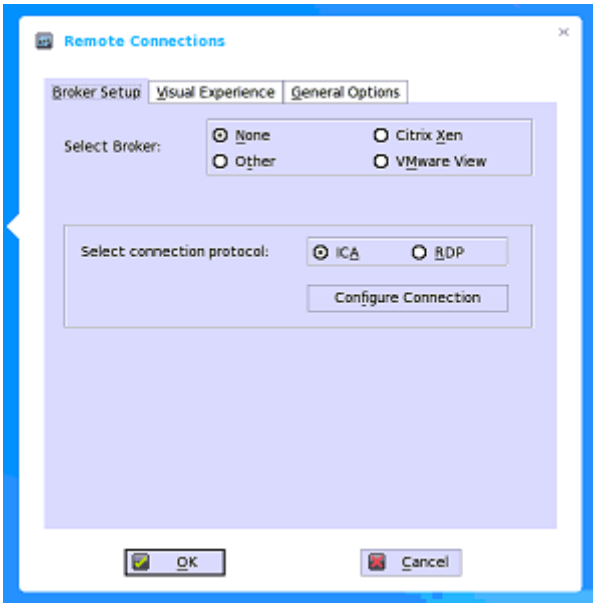
The Remote Connections dialog box allows you to configure zero client remote connections (including ICA, RDP, Citrix XenDesktop, and other broker server connections), visual options, and general connection settings.

Tip In the Classic Desktop option, the Remote Connections dialog box allows you to create default ICA and RDP connections for use. If you want to create several ICA and RDP connections (more than the default connections), use the Connect Manager (see Connect Manager, page 2-10).

Broker Setup Tab

Figure 3-7 shows the Broker Setup tab.

Figure 3-7 Remote Connections—Broker Setup



Use the following guidelines for the Broker Setup tab:

Tip Locations can be supplied through a wnos.ini file if it is used. If DHCP is used, locations can be supplied through DHCP. After creating an entry, be sure to reboot the zero client to have the changes take effect.

- Citrix Xen Connection (Recommended option)—Select **Citrix Xen**, enter the IP address for the server in the Broker Server box, select your options, and then click **OK**.

  Use the following guidelines for the Citrix Xen Broker Server:

  - Enter the IP Address or host name for the server in the **Broker Server** box.
  - Use the **Enable automatic reconnection at logon** and **Enable automatic reconnection from button menu** check boxes and options to further configure the connection for automatic reconnection.
  - After entering the information above, the user must reset the Cisco VXC client for the client to find the broker server for login. When the Cisco VXC client is configured in this way, the system administrator generally does not need to configure any other settings. All other settings have the required defaults.

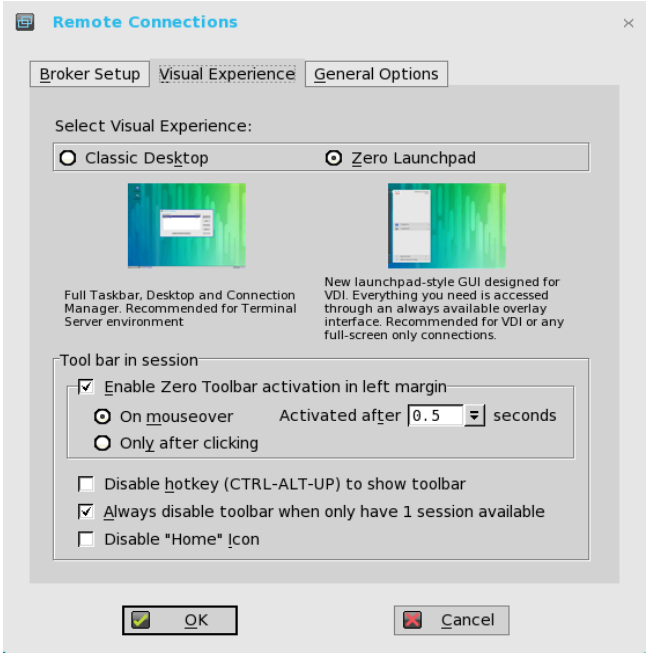
- ICA Connection—Select **None**, select **ICA**, click **Configure Connection**, and then follow the wizard (see Configuring ICA Connections, page 3-11).
- RDP Connection—Select **None**, select **RDP**, click **Configure Connection**, and then follow the wizard (see Configuring RDP Connections, page 3-16).
- Direct Connection—Select **Other**, enter the IP Address for the broker server in the **Broker Server** box, and then click **OK**.
- VMware View Connection—Select **VMware View**, enter the IP Address for the server in the **Broker Server** box, and then click **OK**.

Tip The broker supports both HTTP and HTTPS, and depends on the broker server support. If HTTP or HTTPS is not specified on the broker server, then HTTP is used by default. If HTTPS is specified, the client side must install a corresponding root certificate locally. For detailed instructions on installing a corresponding root certificate locally, see Appendix D, “Setting Up Your HTTPS/SSL Web Server”.

Visual Experience Tab

Figure 3-8 shows the Visual Experience tab.

Figure 3-8 Remote Connections—Visual Experience



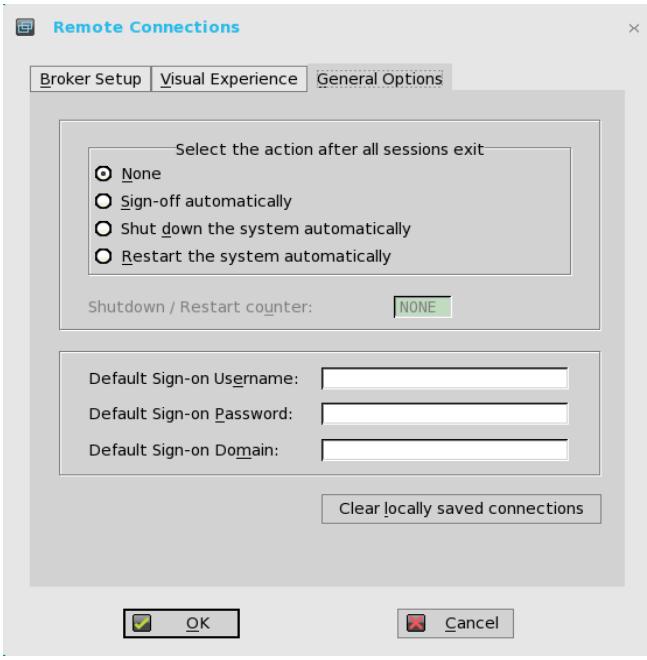
Use the following guidelines for the Visual Experience tab:

- Classic Desktop—Displays the full task bar, desktop, and Connect Manager familiar to WTOS users. This option is recommended for terminal server environment.
- Zero Launchpad—Displays the launchpad-style Cisco VXC desktop GUI designed for VDI use. Functionality is accessed through an always available interface. This option is recommended for VDI and any full-screen-only connections.
- Toolbar, hot key, and connection icon options are also available for configuration.

General Options Tab

Figure 3-9 shows the General Options tab.

Figure 3-9 Remote Connections—General Options

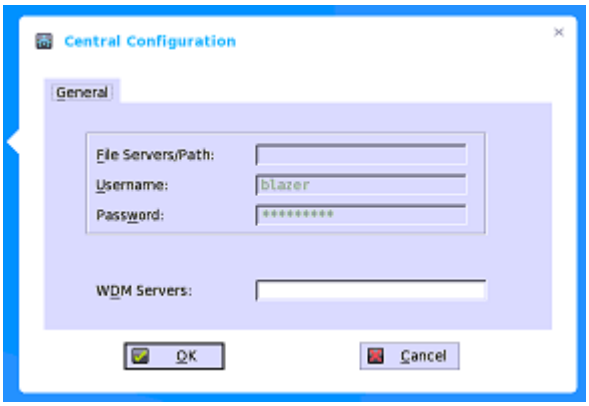


Use the General Options tab options to select the action after you exit all open desktops (by default, the zero client automatically returns to the Login dialog box and is ready for another user), set the default sign-on username and domain, and to clear locally saved connections.

Central Configuration

The Central Configuration dialog box allows you to configure zero client central connection settings such as file server and optional VXC Manager server settings.

Figure 3-10 Central Configuration



Use the following guidelines:

- File Servers/Path, Username, and Password—IP address or host name of the file server that provides the system software and update images. The address can be supplied through DHCP if DHCP is used. Use the following guidelines:
  - File Servers/Path—Allows 128 characters maximum. The data specifies part of the path to be used when the server is accessed. Multiple file servers/paths may be named, as long as all data fits in the length limitation.
  - Username—To log in to the file server. Use 15 characters maximum.
  - Password—To log in to the file server. Use 15 characters maximum.
- WDM Servers—List of IP addresses or host names if the Cisco VXC Manager is used. Locations can be supplied through user profiles if user profiles are used. If DHCP is used, locations can be supplied through DHCP.

Advanced Details on Configuring ICA and RDP Connections

Use the following information when configuring ICA and RDP connections (this information assumes that the zero client does not have a locked down privilege level):

- High-privileged user—The additional functionality provided by the Connection Settings dialog box allows testing of connection definitions before they are entered (by a network administrator) into the user profile files.
- Low-privileged user—The settings for the selected connection can be viewed but cannot be edited, and new connections cannot be defined. Connection definitions are controlled by a network administrator and are accessed by the zero client from the user profiles located on a remote server.
- Standalone user—The Connect Manager is available to Standalone users because connection definitions cannot be accessed from remote user profiles. If user profiles are available on an FTP server but are not accessed because DHCP is not available or is not configured to provide the file server IP address, the file server IP location can be entered manually using the Network Setup dialog box.

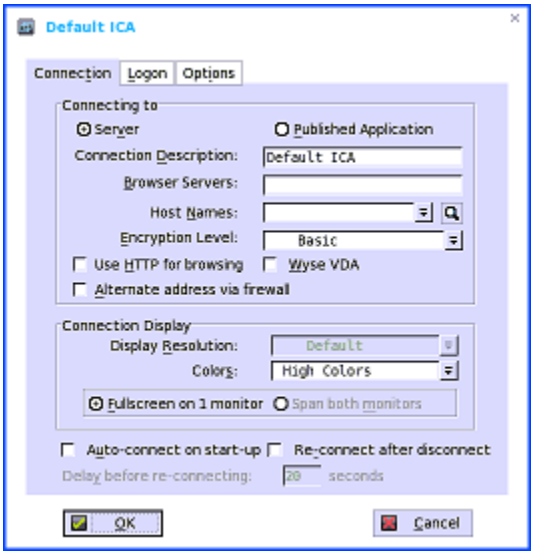
Configuring ICA Connections

The following sections provide information about configuring ICA connections.

Connection Tab

Figure 3-11 shows the Connection tab.

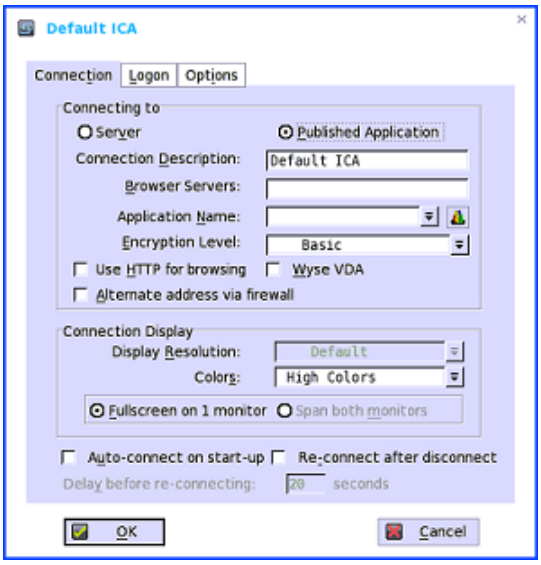
Figure 3-11 Default ICA—Connection (Server Option)



If you select the Server option, the Host Names box is displayed.

If you select the Published Application option, the Application Name box replaces the Host Names box.

Figure 3-12 Default ICA—Connection (Published Application Option)



Use the following guidelines on the Connection tab:

- Server or Published Application—Select the type of connection to which the settings apply.
- Connection Description—Enter the descriptive name that is to appear in the connection list (38 characters maximum).

- Browser Servers IP—Enter a delimited (comma or semicolon) list of IP addresses or DNS-registered names of ICA servers that contains the master browsers list, or that could refer to another server that contains the list. The master browsers list is generated automatically by a browsing program on one of the ICA servers (selected by negotiation between servers). It is used to provide the information displayed in the Server Name or IP box. No entry is needed if the list is on an ICA server in the same network segment as the zero client. No entry is necessary if the connection is to a server, or if the server name or IP contains the IP address of the server.
- Host Name or Application Name (title depends on the Server or Published Application option selected)—You can enter a delimited (semicolon or comma separated) list of server host names or IP addresses, or you can select from the list of ICA servers or published applications (depending on Server or Published Application option selected) obtained from the ICA master browser (you can also use Browse next to the box to make the selection you want). If you enter a delimited list of servers, the zero client attempts to connect to the next server on the list if the previous server attempt failed. If you use the list and the selected connection fails, the zero client attempts to connect to the next one on the list.

Tip The Host Name may be resolved using one of three mechanisms: ICA master browser, DNS, or WINS. Master browser is the only mechanism that can resolve a published application (unless manual entry is made in DNS for the application). DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.

- Encryption Level—Allows you to select the security level of communications between the zero client and the ICA server. Basic (the default option) is the lowest level of security. Basic allows faster communication between the device and the ICA server because it requires less processing than do the higher levels of encryption.

Caution The encryption selection applies to the security of communications between the zero client and the ICA server only. It is independent of the security settings of individual applications on the ICA server. For example, most Web financial transactions require the zero client to use 128-bit encryption. However, transaction information could be exposed to a lower level of security if the zero client encryption is not also set to 128 bits.

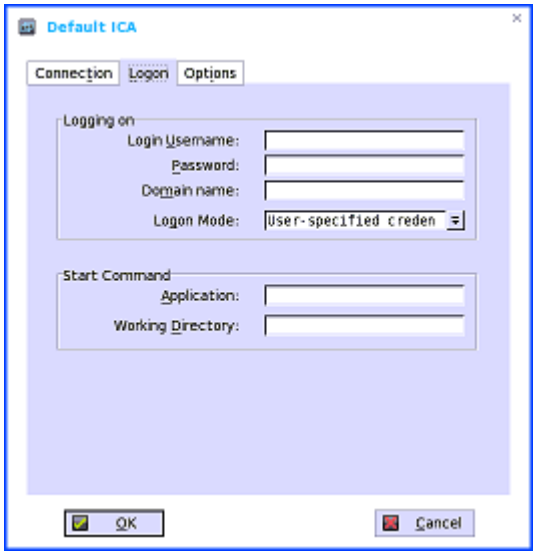
- Use HTTP for browsing—When selected, the zero client, by default, uses http when browsing.
- Alternate address via firewall—When selected, the zero client will use an alternate IP address returned from the ICA master browser to get through firewalls. Used for the Windows log-on when the connection is activated.
- VDA—Not supported on Cisco VXC 2112/2212.
- Display Resolution—Select the display resolution for this connection (if you select the Published Application option, the Connection Display will allow you to select the Seamless Display Resolution option):
  - Default
  - 640 x 480
  - 800 x 600
  - 1024 x 768
  - 1152 x 864
  - 1280 x 720

  - 1280 x 768
  - 1280 x 1024
  - 1360 x 768
  - 1366 x 768
  - 1368 x 768
  - 1440 x 900
  - 1400 x 1050
  - 1600 x 900
  - 1600 x 1200
  - 1680 x 1050
  - 1920 x 1080
  - 1920 x 1200
- Colors—Select the color depth of the ICA session. If High Colors (16bits) or True Colors is selected and the ICA server does not support this color depth, the zero client renegotiates the color depth to the lower value (for example, 256 Colors [8 bits]).
- Window mode and Full screen mode—Select the initial view of the application in a windowed screen or full screen. You can toggle between viewing modes by using Ctrl-Alt-Up Arrow.
- Auto-connect on start-up—When selected, automatically connects the session on start-up.
- Re-connect after disconnect—When selected, causes the zero client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the Delay before re-connecting box (enter the number of seconds 1 to 3600) or the user profile for yes (20 seconds) or seconds. The default is 20 seconds if there is no INI file description of this connection, or is a Standalone user, or simply omitted.

Logon Tab

Figure 3-13 shows the Logon tab.

Figure 3-13 Default ICA—Logon



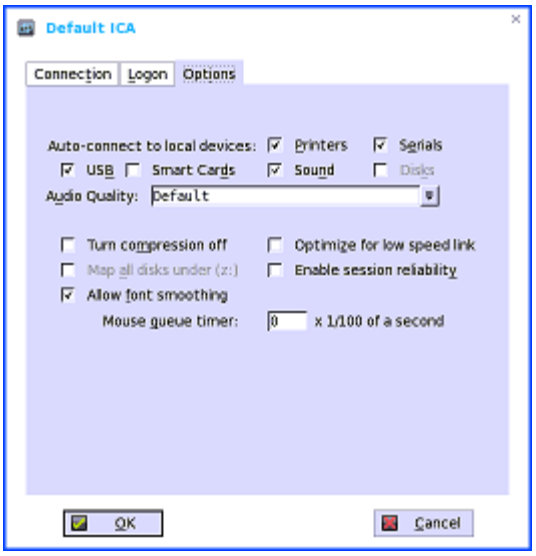
Use the following guidelines on the Logon tab:

- Logging on area—Enter Login Username, Password, Domain name, and Logon Mode (if the Login Username, Password, and Domain name boxes are not populated, you can enter the information manually in the ICA server login screen when the connection is made):
  - Login Username—31 characters maximum.
  - Password—19 characters maximum.
  - Domain Name—31 characters maximum.
  - Logon Mode—Select User-specified credentials, Smart Card, or Local User.
- Start Command area—(Server Connection Option Only—This area is disabled (grayed) for a Published Application option.)
  - Application (127 characters maximum) and Working Directory (63 characters maximum)—Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.

Options Tab

Figure 3-14 shows the Options tab.

Figure 3-14 Default ICA—Options



Use the following guidelines on the Options tab:

- Auto-connect to local devices—Select any options (Printers, Serials, USB, Smart Cards, Sound, and Disks) to have the zero client automatically connect to the devices (an ICA session will not automatically connect to a device through a serial port).
- Turn compression off—When selected, turns compression off (intended for high-speed connections).
- Optimize for low speed link—When selected, allows optimization for low-speed connections, such as reducing audio quality or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dialup.
- Map all disks under (z:)—When selected, maps all disks under the Z drive.
- Enable session reliability—When enabled, session reliability allows a user to momentarily lose connection to the server without having to re-authenticate upon regaining a connection. Instead of a user's connection timing out after X seconds, the session is kept alive on the server and is made available to the client upon regaining connectivity.
- Allow font smoothing—When selected, enables font smoothing (smooth type).
- Mouse queue timer—Specifies the default queue timer of a mouse event in an ICA or RDP session (in 1/100 of a second). It can be used to adjust the bandwidth of a network.

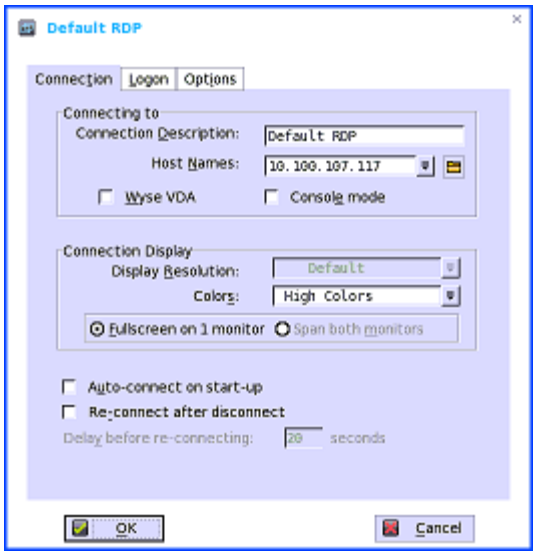
Configuring RDP Connections

In a Virtual Desktop environment, an RDP connection will be assigned by the Virtual Desktop Broker; you do not need to create an RDP connection manually. The Virtual Desktop Broker virtual machine can be reset from the zero client by opening the Connection Settings dialog box of the virtual machine, and then clicking the reset button (appears in the top-right of the dialog box).

Connection Tab

Figure 3-15 shows the Connection tab.

Figure 3-15 Default RDP—Connection



Use the following guidelines on the Connection tab:

- Connection Description—Enter the descriptive name that is to appear in the connection list (38 characters maximum).
- Host Names—Use the list to select the valid DNS server name or the IP address of the server to which the zero client connection is to be made (you can also use Browse next to the box to make the selection you want). For example, a list of WTS servers on the local network from which you can select.

Tip The server name may be resolved using one of two mechanisms: DNS, and WINS. DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.

- VDA—Not supported on Cisco VXC 2112/2212.
- Console mode—Select to set the RDP connection with Windows Console mode.
- Display Resolution—Select the display resolution for this connection:
  - Default
  - 640 x 480
  - 800 x 600
  - 1024 x 768
  - 1152 x 864
  - 1280 x 720
  - 1280 x 768
  - 1280 x 1024

  - 1360 x 768
  - 1368 x 768
  - 1440 x 900
  - 1600 x 900
  - 1600 x 1200
  - 1680 x 1050
  - 1920 x 1080
  - 1920 x 1200
- Colors—Select the color depth of the RDP session. If High Colors (16 bits) or True Colors (32 bits) is selected and the RDP server does not support this color depth, the zero client renegotiates the color depth to the lower value, for example, 256 Colors (8 bits). The highest is 32 bits, if hardware supports it.

Tip For some zero clients versions, only the 256 Colors (8 bits) selection is available for RDP connections. Also, for older versions of the server software (for example, RDP 4.0) the server supports only 8 bit color. This is not detectable in advance but results in use of 8-bit color when the connection is established.

- Window mode and Full screen mode—Select the initial view of the application in a windowed screen or full screen. You can toggle between viewing modes by using Ctrl-Alt-Up Arrow.
- Auto-connect on start-up—When selected, automatically connects the session on start-up.
- Re-connect after disconnect—When selected, causes the zero client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the Delay before re-connecting box (enter the number of seconds 1 to 3600) or the user profile for yes (20 seconds) or seconds. The default is 20 seconds if there is no INI file description of this connection, or is a Standalone user, or is simply omitted.

Tip You can reset the options on the Connection tab of the Connection Settings (RDP) dialog box. To do so, click the **Reset VM** command button. This command button is located in the upper-right of the dialog box. It appears only with a VDM broker connection.

Logon Tab

Figure 3-16 shows the Logon tab.

Figure 3-16 Default RDP—Logon

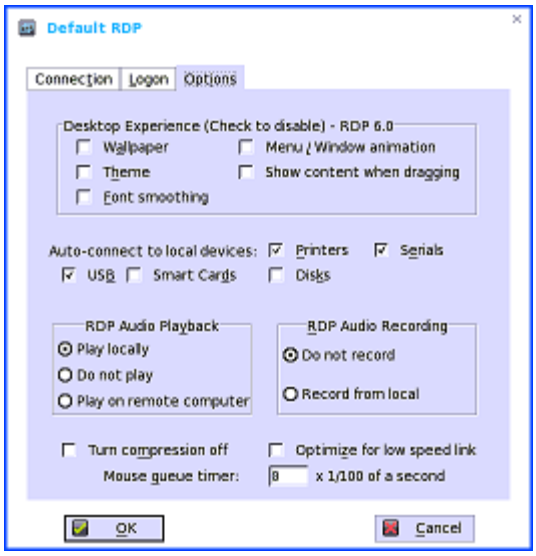
Use the following guidelines on the Logon tab:

- Logging on area—Enter login username, password, and domain name. If these boxes are not populated, you can enter the information manually in the RDP server login screen when the connection is made. Use the following guidelines:
  - Login Username—31 characters maximum.
  - Password—19 characters maximum.
  - Domain Name—31 characters maximum.
- Application (127 characters maximum) and Working Directory (63 characters maximum)—Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.

Options Tab

Figure 3-17 shows the Options tab.

Figure 3-17 Default RDP—Options



Use the following guidelines on the Options tab:

- Wallpaper—When selected, disables the desktop wallpaper.
- Menu / Window animation—When selected, disables the menu or window animation.
- Theme—When selected, disables the desktop themes.
- Show content when dragging—By default, when you "grab" a Window by the title bar and move it around, the contents of the window will move with it. Select this to disable this content view so that only the outline of the window moves when dragging it, until you drop the window. This option can be beneficial, because it uses less processing power.
- Font smoothing—Converts vector text to bitmap for better display.
- Auto-connect to local devices—Select any options (Printers, Serials, USB, Smart Cards, Sound, and Disks) to have the zero client automatically connect to the devices (USB—Redirects locally attached USB devices on the zero client to a Microsoft Windows terminal server. When the user connects to the terminal server, locally attached USB devices on the zero client are accessible).
- RDP Audio Playback and RDP Audio Recording—Select the audio options you want.

Note The RDP Audio options enable the Cisco VXC client to transfer audio information. However, restrictions can still apply from the central server. Users should check with their system administrator to find out if two-way audio is supported in their Cisco VXC architecture.

- Turn compression off—When selected, turns compression off (intended for high-speed connections).
- Optimize for low speed link—When selected, allows optimization for low-speed connections, such as reducing audio quality or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dialup.

Mouse queue timer—Specifies the default queue timer of a mouse event in an ICA or RDP session (in 1/100 of a second). It can be used to adjust the bandwidth of a network

CHAPTER 4

Configuring Local Settings Options

You can configure the following Local Settings options using zero client dialog boxes (depending on user privilege level, some options may not be available for use):

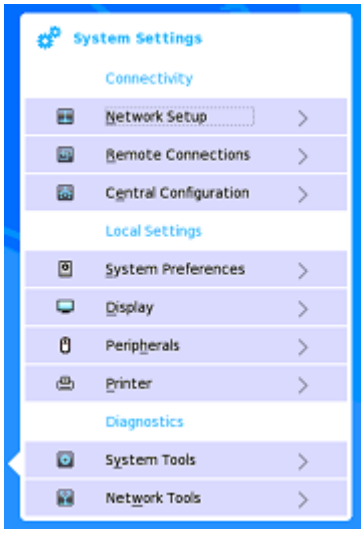
- System Preference, page 4-2
- Display, page 4-5
- Peripherals, page 4-8
- Printers, page 4-12

Tip While it is not recommended to use zero client dialog boxes for configuring Local Settings options, they are available in case you want to temporarily override central default configurations or you do not have the option to set up central configuration (smaller environments). In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all zero clients in your WTOS environment (see Appendix A, "Central Configuration: Automating Updates and Configuration").

To access Local Settings options:

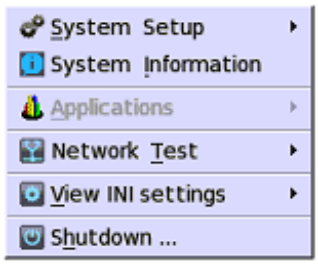
- Cisco VXC desktop—click the **System Settings** icon on the Cisco VXC toolbar (administrators can also click the **Admin Mode** button on the Login dialog box).

Figure 4-1 System Settings



- Classic Desktop—click User Name (User Name is the user who is logged-on and is located at the bottom-left side of the task bar), and select System Setup.

Figure 4-2 Accessing System Settings—Classic Desktop



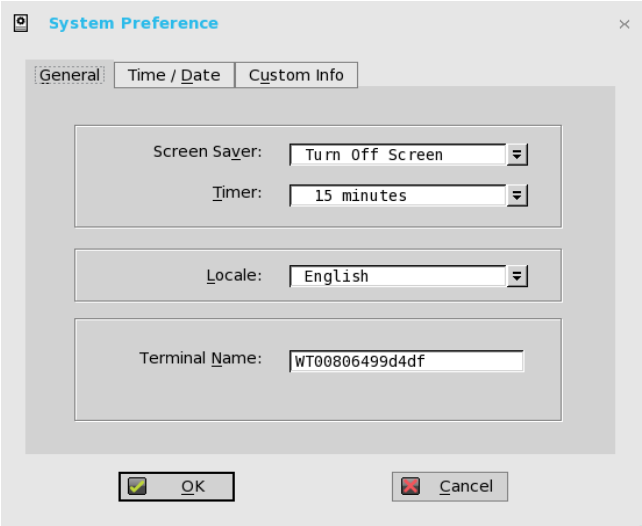
System Preference

The System Preference dialog box allows you to select personal preferences such as screen saver, time/date, and custom information settings.

General Tab

Figure 4-3 shows the General tab.

Figure 4-3 System Preference—General



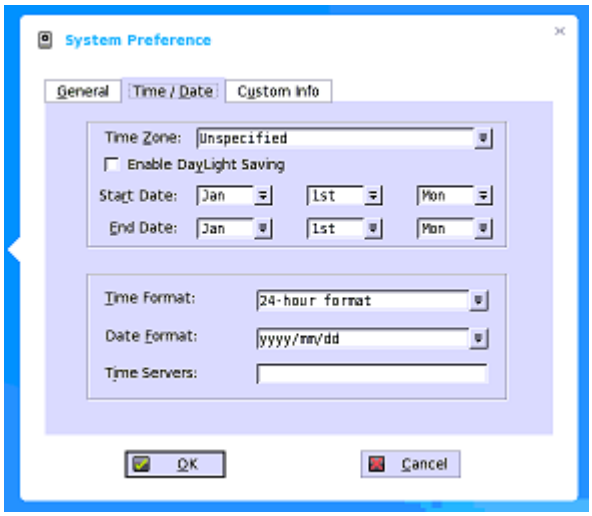
Use the following guidelines for the General tab:

- Screen Saver—Allows you to select the type of screen saver you want. The default is to Turn Off Screen. Other selections available include Flying Bubbles and Moving Image (which are screen savers with the monitor remaining on).
- Timer—Select a time after which the screen saver is to be activated (either 1 minute, 5 minutes, 10 minutes or default is 20 minutes). When the zero client is left idle for the specified idle time, the screen saver is initiated.
- Locale—Allows you to provide minor localization for French and German. While it does not provide full localization (the GUI still displays in English), this option allows the login screen to display username, password, and domain in the desired language (English, French, or German).
- Terminal Name—Allows entry of a name for the zero client. The default is a 14-character string composed of the letters WT followed by the zero client Ethernet MAC address. Some DHCP servers use this value to identify the IP address lease in the DHCP Manager display.

Time/Date Tab

Figure 4-4 shows the Time/Date tab.

Figure 4-4 System Preference—Time/Date



Use the following guidelines for the Time/Date tab:

- Time Zone—Allows you to select a time zone where the zero client operates (default is Unspecified).
- Enable Daylight Saving—Allows you to enable the daylight saving settings. When selected, the six boxes must be properly configured to define the daylight saving starting (month/week/day) and ending (month/week/day) periods. Use the following guidelines:
  - Start Date—Specifies when daylight saving time begins for the time zone you have selected.
  - End Date—Specifies when daylight saving time ends for the time zone you have selected.

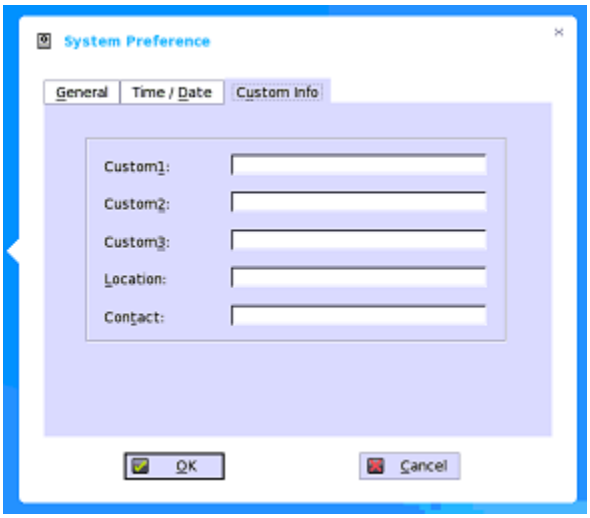
Note If you check the Enable Daylight Saving check box without also properly specifying the Start Date and End Date, the following error appears under Adjust Date and Time in Windows operating systems:
`Your current time zone is not recognized. Please select a valid time zone.`

  - Month—Specifies the month in the year from January through December.
  - Week—Select 1 through 4 for the week in the month. Week Last denotes the last week in the month.
  - Day—Specifies the day of the week from Monday through Sunday.
- Time Format—Allows you to select a 12 or 24 hour time format (default is 24-hour format).
- Date Format—Allows you to select a yyyy/mm/dd (year/month/day) or dd/mm/yyyy (day/month/year) date format (default is yyyy/mm/dd).
- Time Servers—List of IP addresses or host names with optional TCP port number of Time Servers. Each entry with optional port number is specified as Name-or-IP:port, where :port is optional. If not specified, port 80 is used. Locations can be supplied through user profiles if user profiles are used. The Time Servers provide the zero client time based on the settings of time zone and daylight saving information. If DHCP is used, locations can be supplied through DHCP.

Custom Info Tab

Figure 4-5 shows the Custom Info tab.

Figure 4-5 System Preference—Custom Info



Use the Custom Info tab to enter configuration strings for use by Cisco VXC Manager software. The configuration strings can contain information about the location, user, administrator, and so on.

Clicking OK transfers the custom field information you enter in the dialog box to the Windows registry. The information is then available to the Cisco VXC Manager.

For more information on using Cisco VXC for remote administration and upgrading zero client software, see Using Cisco VXC Manager Software For Remote Administration, page B-1.

For details on using Custom Field information, see the *Cisco VXC Manager Administration Guide*.

Display

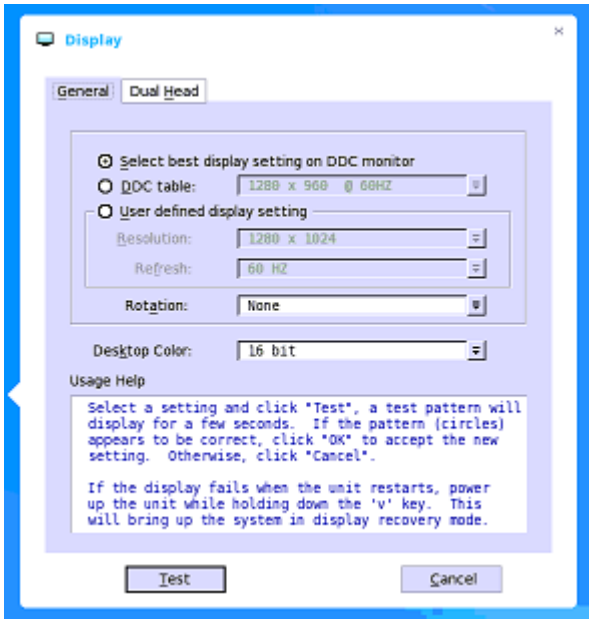
The Display dialog box allows you to select the resolution and refresh rate for the monitor used with the zero client. It also allows you to configure the way two monitors display.

Tip The number of icons that can be displayed on the desktop depends on the desktop resolution and administrator configuration. On zero clients that only support 8 bit color, the 1280 x 1024 resolution will be used to display full screen connections. The 1280 x 1024 resolution will not be used to display the desktop, windowed connections, or seamless connections.

General Tab

Figure 4-6 shows the General tab.

Figure 4-6 Display—General



Use the following guidelines for the General tab:

- Select best display setting on DDC monitor—If the monitor is VESA DDC2B (Display Data Channel) compatible, selection of this option allows the zero client to automatically select the best resolution and refresh rate. If your monitor is not DDC compatible, a Monitor does not support Plug and Play message is displayed (click **OK** to acknowledge the message and remove it from the screen).
- DDC table—If the monitor is VESA DDC2B (Display Data Channel) compatible, selection of this option allows you to select the resolution and refresh rate you want from the list.
- User defined display setting—Select this option and select the resolution and refresh rate supported by your monitor (all combinations are allowed):

  Resolution list selections include:

  - 640 x 480
  - 800 x 600
  - 1024 x 768
  - 1152 x 864
  - 1280 x 720
  - 1280 x 768
  - 1280 x 1024
  - 1360 x 768
  - 1368 x 768
  - 1440 x 900

  - 1600 x 900
  - 1600 x 1200
  - 1680 x 1050
  - 1920 x 1080
  - 1920 x 1200

  Refresh rate list selections include:

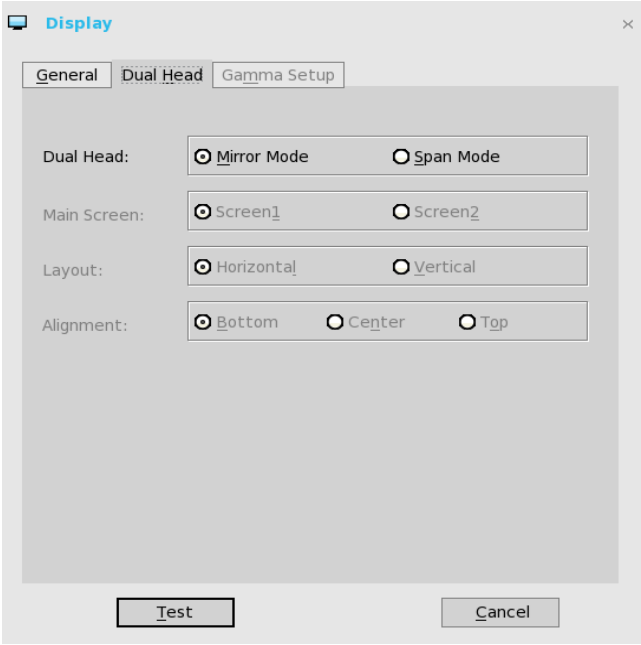
  - 60 Hz (default)
  - 75 Hz
  - 85 Hz

- Rotation—Select a rotation option: None, Left turn (Experimental), or Right turn (Experimental). Note that left or right rotations provide a 90 degree rotation.
- Desktop Color—Select the Desktop Color (either 16 bit or 32 bit).
- Usage Help area—Contains brief instructions for using the Display dialog box and running the test. No operator entry can be made in this box. Make note of the instructions in the area regarding v-key reset usage in case of display failure.

Dual Head Tab

Figure 4-7 shows the Dual Head tab.

Figure 4-7 Display—Dual Head



Use the following guidelines for the Dual Head tab (Supported Dual Monitor Capable Thin Clients Only):

- Dual Head—Select **Mirror Mode** to have the two monitors work in a matching state, or **Span Mode** to have the two monitors work separately (second is extended from first).

- Main Screen—Select which of the two monitors you want to be the main screen (**Screen1** or **Screen2**). The other screen is extended from the main screen.
- Layout—Select how screens are aligned. In horizontal alignment, select **top** for top aligned screens, and **bottom** for bottom aligned screens. In vertical alignment, select **left** for left aligned screens, and right for right aligned screens. In either horizontal or vertical alignment, select **center** for center aligned screens.
- Alignment—Select how you want the two monitors to be oriented to each other (**Horizontal** where you mouse between the monitors from the left and right of the screens or **Vertical** where you mouse between the monitors from the top and bottom of the screens).
- (Classic Desktop Only) Taskbar—Select under which screen you want the Taskbar to appear (**Whole Screen** or **Main Screen**).

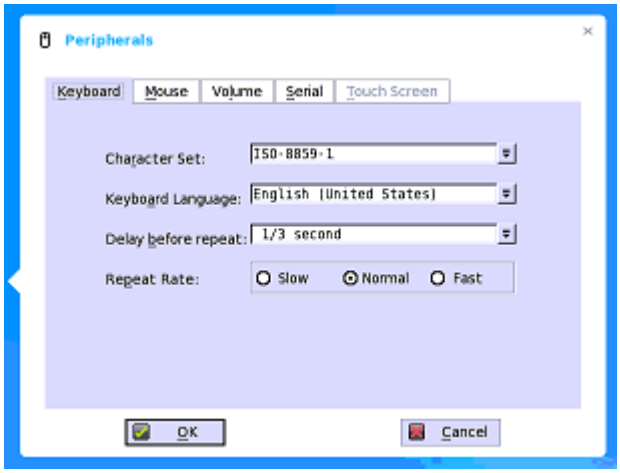
Peripherals

The Peripherals dialog box allows you to select the peripherals settings such as keyboard, mouse, volume, and touch screen settings.

Keyboard Tab

Figure 4-8 shows the Keyboard tab.

Figure 4-8 Peripherals—Keyboard



Use the following guidelines for the Keyboard tab:

- Character Set—Select the character set (Each character is represented by a number. The ASCII character set, for example, uses the numbers 0 through 127 to represent all English characters as well as special control characters. European ISO character sets are similar to ASCII, but they contain additional characters for European languages).

- Keyboard Language—Currently the following keyboard languages are supported. The default is English (United States).

Table 4-1 Supported Keyboard Languages

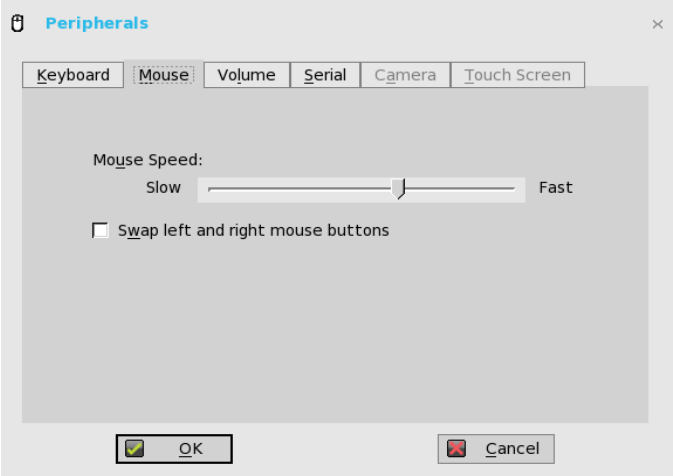
Supported Keyboard Languages		
Arabic (Saudi Arabia)	Arabic (Iraq)	Arabic (Egypt)
Arabic (Libya)	Arabic (Algeria)	Arabic (Morocco)
Arabic (Tunisia)	Arabic (Oman)	Arabic (Yemen)
Arabic (Syria)	Arabic (Jordan)	Arabic (Lebanon)
Arabic (Kuwait)	Arabic (U.A.E.)	Arabic (Bahrain)
Arabic (Qatar)	Brazilian	Canadian (Multilingual)
Chinese (Simplified)	Chinese (Traditional)	Croatian
Czech	Danish	Dutch
Dutch (Belgian)	English (Australian)	English (3270 Australian)
English (New Zealand)	English (United Kingdom)	English (United States)
Finnish	French (Belgian)	French (Canadian)
French (France)	French (Swiss)	German
German (IBM)	German (Swiss)	Greek
Hungarian	Italian	Italian (Swiss)
Japanese	Korean	Norwegian
Polish (214)	Polish Programmers	Portuguese
Portuguese (Brazil)	Romanian	Slovakian
Slovakian (Qwerty)	Slovenian	Spanish
Spanish (Mexican)	Swedish	Turkish
Turkish (QWERTY)	U.S. International	

- Delay before repeat—Repeat parameters for held-down key. Select the Delay before repeat (either 1/5 second, 1/4 second, 1/3 second, 1/2 second, 1 second, 2 seconds, or No Repeat). The default is 1/3 second.
- Repeat Rate—Select Slow, Medium, or Fast. The default is Medium.

Mouse tab

Figure 4-9 shows the Mouse tab.

Figure 4-9 Peripherals—Mouse

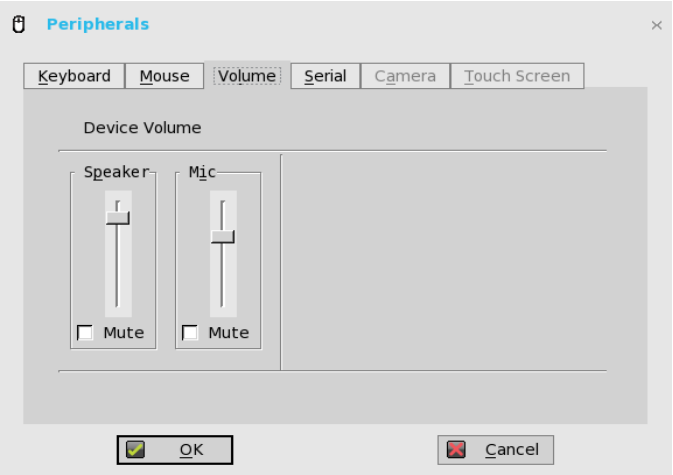


Use the Mouse tab to select the Mouse Speed and mouse orientation (you can swap mouse buttons for left-handed operation by selecting Swap left and right mouse buttons).

Volume Tab

Figure 4-10 shows the Volume tab.

Figure 4-10 Peripherals—Volume

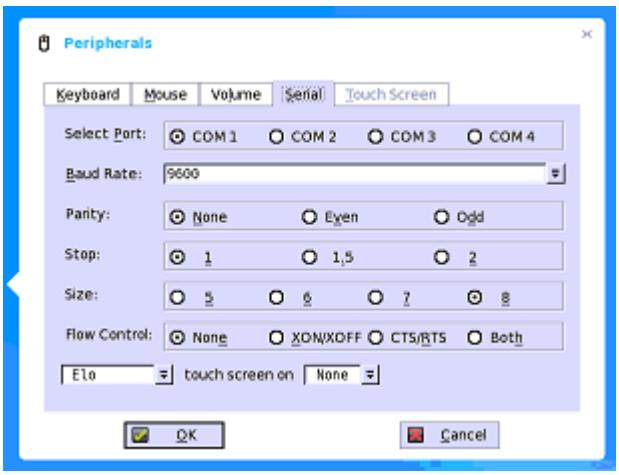


Use the Volume tab to select the volume settings for connected devices.

Serial Tab

Figure 4-11 shows the Serial tab.

Figure 4-11 Peripherals—Serial



Use the following guidelines for the Serial tab:

- Select Port—Select the port to which this setup definition applies. Either COM 1, COM 2, COM 3, or COM 4 can be selected (default is Port COM 1). For Models SX0 and VX0, COM 1 or COM 2 selects from either the USB or serial device.
- Baud Rate—Either 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 baud can be selected (default is 9600).
- Parity—Either None, Even, or Odd can be selected (default is None).
- Stop—Either 1, 1.5, or 2 stop bits can be selected (default is 1).
- Size—Character size 5, 6, 7, or 8 bits can be selected (default is 8).
- Flow Control—Either None, XON/XOFF, CTS/RTS, or Both can be selected (default is None).
- Serial Touch Screen selections—Select the proper touch screen ELO, MicroTouch or FastPoint from the list.
- Touch Screen on—Select the proper serial port (COM port) or None from the list.

Touch Screen Tab

Use the Touch Screen tab to configure touch screens that are connected to the zero client (USB). The tab is available (not grayed out) when the zero client detects that a touch screen is attached through a USB port and the setup (or calibration) has not been performed. The Touch Setup window prompts you to touch two circles on the screen to make the necessary calibration adjustment. After bring calibrated, the adjustment values are saved in the local terminal NVRAM until the system is reset to factory default, or another type of touch monitor is connected.

Printers

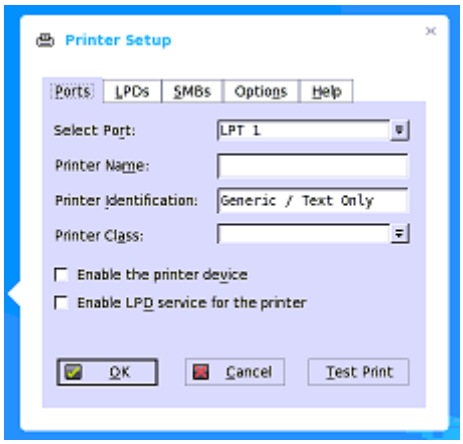
The Printer Setup dialog box allows configuration of network printers and local printers that are connected to the zero client. Through its USB ports, a zero client can support multiple printers. If more than one printer is to be used and another port is not available on your zero client and the port that is to be used must be shared with a USB modem converter, connect a USB hub to the port.

Tip Port LPT1 or LPT2 selects the connection to a USB printer or parallel printer through a USB-to-Parallel converter cable.

Ports Tab

Figure 4-12 shows the Ports tab.

Figure 4-12 Printer Setup—Ports



Use the following guidelines for the Ports tab:

- Select Port—Select the port you want from the list.
- Printer Name—This is a required entry. If Enable LPD service for the printer is selected, the printer name becomes the queue name for other clients using LPR to print to this printer.
- Printer Identification—Enter the type or model of the printer. This name should be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or Generic / Text Only for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).

Tip Most USB direct-connected printers or parallel printers connected through USB-to-parallel cable converters do report their printer identifications. Port LPT1 or LPT2 selects the connection to a USB printer or parallel printer through a USB-to-Parallel cable.

- Printer Class—Select the printer class from the list (PCL5, PS, or TXT).

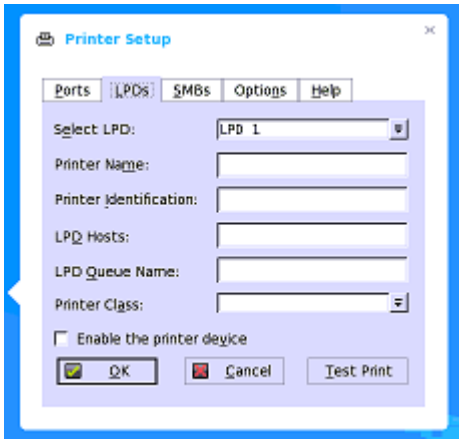
- Enable the printer device—Must be selected to enable the directly-connected printer.
- Enable LPD service for the printer—Select this to make the zero client an LPD (Line Printer Daemon) server for LPD printing requests from the network (see Configuring LPD Services, page 4-16).

Tip If the zero client is to be used as an LPD printer server, DHCP must not be used and a static IP address must be assigned to the zero client (see Network Setup, page 3-2).

LDPs Tab

Figure 4-13 shows the LDPs tab.

Figure 4-13 Printer Setup—LDPs



Use the following guidelines for the LPDs tab:

- Select LPD—Select the port you want from the list.
- Printer Name—Enter the printer name.
- Printer Identification—Enter the type or model of the printer. This name should be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or Generic / Text for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).
- LPD Hosts—The DNS or WINS name of the server for the network printer. An IP address can also be entered.

Tip If the printer is attached to another zero client on your network, the entry in the LPD Hosts box is the name or address of that zero client.

- LPD Queue Name—An LPD host maintains a named queue for each supported printer. Enter the name of the queue associated with the printer to be used.

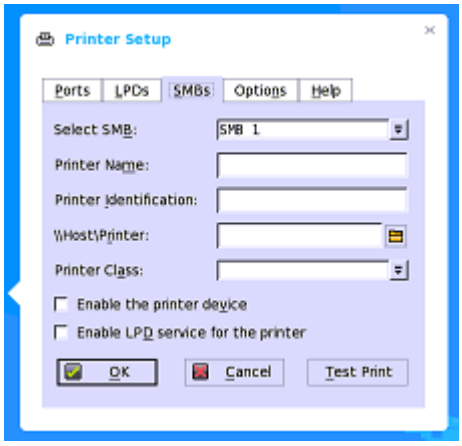
Tip The LPD Queue Name must match the content of the Printer Name box on the zero client with the printer attached.

- Printer Class—Select the printer class from the list.
- Enable the printer device—Must be selected to enable the directly-connected printer.

SMBs Tab

Figure 4-14 shows the SMBs tab.

Figure 4-14 Printer Setup—SMBs



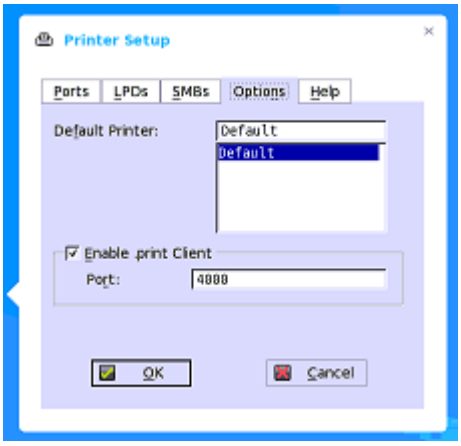
Use the following guidelines for the SMBs tab:

- Select SMB—Select the SMB you want from the list.
- Printer Name—Enter the printer name.
- Printer Identification—Enter the type or model of the printer. This name should be either the device driver name for the printer under the Microsoft Windows system, or a key to map to the device driver. If not specified, the name will be defaulted to the printer-supplied identification for standard direct-connected USB printers or Generic / Text for non-USB connected printers upon connection to Windows hosts. The driver name mapping takes place either through a printer-mapping file read by the system as part of the global profile (wnos.ini) or by MetaFrame servers through the MetaFrame printer configuration file (\winnt\system32\wtsprnt.inf).
- \\Host\Printer—Enter the Host\Printer or use Browse next to the box to make the selection you want.
- Printer Class—Select the printer class from the list.
- Enable the printer device—Must be selected to enable the directly-connected printer.
- Enable LPD service—Select this to make the zero client an LPD (Line Printer Daemon) server for LPD printing requests from the network (see Configuring LPD Services, page 4-16).

Options Tab

Figure 4-15 shows the Options tab.

Figure 4-15 Printer Setup—Options



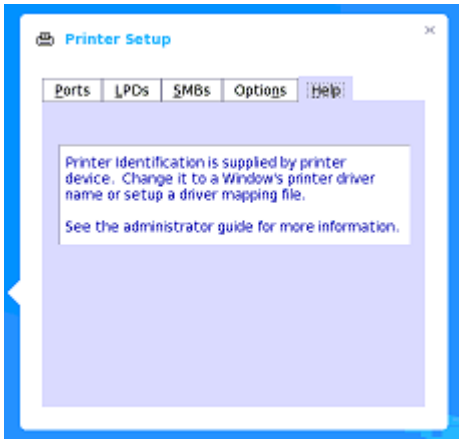
Use the following guidelines for the Options tab:

- Default Printer—Select the printer you want to be the default printer from the list.
- Enable .print Client and Port—If you want to enable .print Client, select Enable .print Client and then enter the Port.

Help Tab

Figure 4-16 shows the Help tab.

Figure 4-16 Printer Setup—Help



The Help tab contains printer help information.

Configuring LPD Services

A zero client can be configured to provide LPD (Line Printer Daemon) services, making the zero client a printer server on the network.

Set-up the zero client that is to provide LPD print services as follows:

Procedure

Step 1 Open the Network Setup dialog box (**Desktop Menu > System Setup > Network**) and enter a static IP address for the zero client.

Step 2 Open the Printer Setup dialog box (**Desktop Menu > System Setup > Printer**) and select any of the listed ports.

Step 3 Name the printer in the **Printer Name** box.

Step 4 Select **Enable LPD service for the printer**.

Step 5 Select **Enable the Printer Device**.

Step 6 Set up the application server as described in either Setting Up Windows NT4 Servers, page 4-16 or Setting Up Windows 2003/2008 Servers, page 4-16.

Setting Up Windows NT4 Servers

Procedure

Step 1 Navigate to **Control Panel > Network > Services** and ensure that the Microsoft TCP/ IP Printing service is installed. If it is not, install it using the Microsoft installation instructions.

Step 2 Add the zero client as the LPD printer by completing the following:

a. Navigate to **Control Panel > Printers > Add Printers > My Computer > Add Port** and double-click **LPR PORT** (if you do not see LPR Port, ensure that the Microsoft TCP/IP Printing service is installed correctly).

b. Type the zero client IP address or DNS name in the Name or address of host providing LPD box.

c. Type the printer name (assigned in Configuring LPD Services, page 4-16) in the **Name of printer on that machine** box.

d. Click **OK**, and then click **NEXT**.

Step 3 After you have selected the printer, you can perform your normal printer setup for the application server. For example, select the manufacturer printer type and printer name.

Setting Up Windows 2003/2008 Servers

Procedure

Step 1 Navigate to **Control Panel > Administrative Tools > Services** and ensure the Microsoft TCP/IP Printing service is installed. If it is not, install it using the Microsoft installation instructions.

Step 2 Add the zero client as the LPD printer by completing the following:

a. Navigate to **Control Panel > Printers > Add Printers > Local Printer > Create a new port** and select **LPR PORT**.

Tip If you do not see LPR Port, ensure that the Microsoft TCP/IP Printing service is installed correctly.

b. Type the zero client IP address or DNS name in the **Name or address of host providing LPD** box.

c. Type the printer name (assigned in Configuring LPD Services, page 4-16) in the **Name of printer on that machine** box.

d. Click **OK**, and then click **NEXT**.

Step 3 After you have selected the printer, you can perform your normal printer setup for the application server. For example, select the manufacturer printer type and printer name.

CHAPTER 5

Performing Diagnostics

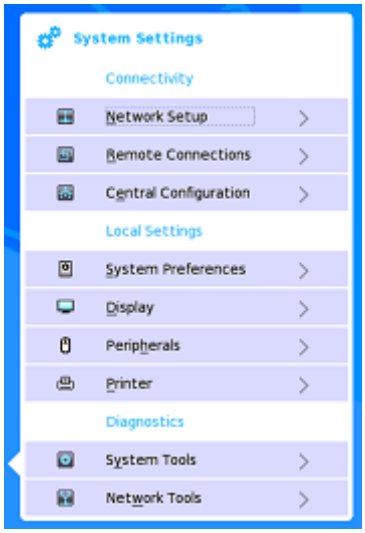
You can use the following diagnostic tools:

- System Tools, page 5-2
- Network Tools, page 5-2

To access Diagnostics options:

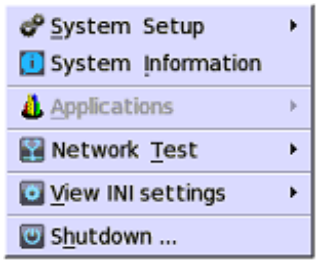
- Cisco VXC desktop—click the **System Settings** icon on the Cisco VXC toolbar (administrators can also click the Admin Mode button on the Login dialog box).

Figure 5-1 System Settings Menu



- Classic Desktop—click User Name (User Name is the user who is logged-on and is located at the bottom-left side of the task bar), and select either **Network Test** (for network tools Ping and Trace Route) or **View INI Settings** (for system tools to configure Trace and Event log settings, and to view INI files).

Figure 5-2 User Name Menu



System Tools

The System Tools dialog box allows you to configure Trace and Event log settings. It also allows you to view wnos.ini and user.ini cached information for troubleshooting purposes.

Figure 5-3 System Tools

Use the Trace and Event log options on the General tab to configure the settings you want.

Use the Global INI tab to view wnos.ini information.

Use the user.ini tab to view user.ini information.

Network Tools

The Network Tools dialog box allows you to use Ping (Packet InterNet Groper) and Trace Route for checking the integrity of the network connection (ping also checks the usability of the network configuration and the availability of all equipment required to communicate between the zero client and the ping destination). Generally, Ping and Trace Route are used for system diagnostics by, or under the direction of, a network administrator.

Using Ping

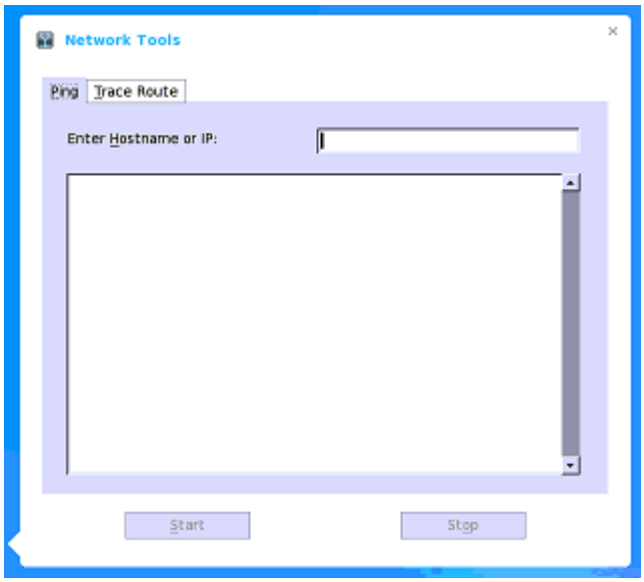
The Ping dialog box executes the ping diagnostic utility and displays response messages. Ping is a diagnostic tool that sends an echo request to a network host. The host parameter is either a valid host name or an IP address. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted (by clicking Stop in the Ping dialog box). The ping utility sends one echo request per second and calculates round trip times and packet loss statistics, and then displays a brief summary upon completion of the calculation.

The ping utility can be used to:

- Determine the status of the network and various foreign hosts
- Track and isolate hardware and software problems
- Test, measure, and manage networks
- Determine the IP address of a host if only the host name is known

Note Not all network equipment will respond to ping packets, because this is a common mechanism used in denial-of-service attacks. Lack of response does not necessarily indicate that the target of the ping is unusable for other purposes. However, a response provides a definite indication that connectivity from the Cisco VXC client to the remote endpoint exists.

Figure 5-4 Ping



Use the following guidelines:

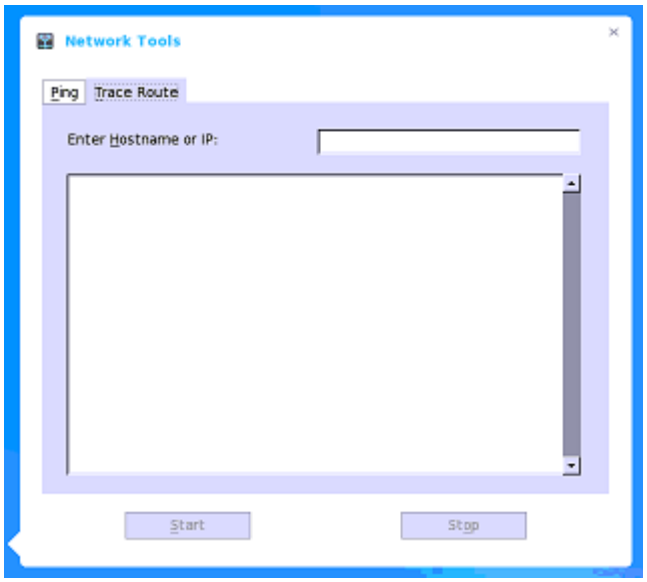
- Enter Hostname or IP—Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be pinged.
- Data area—Displays ping response messages. The ping command sends one echo request per second, calculates round trip times and packet loss statistics, and displays a brief summary upon completing the calculation.
- Start—Executes the ping command. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted by clicking Stop.

- Stop—Terminates the ping request and leaves the Ping dialog box open (so you can read the summary posted in the data area).

Using Trace Route

The Trace Route dialog box executes the tracert diagnostic utility and displays response messages. The tracert utility traces the path from your zero client to a network host. The host parameter is either a valid host name or an IP address. The tracert utility sends out a packet of information three times to each device (routers and computers) in the path and displays the round trip response times and identifying information in the message box.

Figure 5-5 Trace Route



Use the following guidelines:

- Enter Hostname or IP—Enter the IP address, DNS-registered host name, or WINS-registered host name of the target to be traced.
- Data area—Displays round-trip response time and identifying information for each device in the path.
- Start—Executes the tracert command.
- Stop—Terminates the tracert command and leaves the Trace Route dialog box open (so you can read the information posted in the data area).

APPENDIX **A**

Central Configuration: Automating Updates and Configuration

This appendix contains information on the network architecture and enterprise server environment needed to provide network and session services for zero clients running WTOS. It also includes information to help you address important considerations when configuring the services to be provided by the server environment. Use this chapter in conjunction with the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide* to set up and configure your WTOS server environment.

It includes:

Understanding How to Configure Your Network Services

Network services used by the zero client can include DHCP, FTP file services, Virtual Desktop file services, DNS, and so on. How you configure your network services depends on what you have available in your WTOS environment and how you want to design and manage it.

The following topics in this section provide important overview information on the supported service situations you may have when configuring the network services for your WTOS environment (after becoming familiar with your environment requirements, refer to Configuring Network Services, page A-6 for detailed instructions):

Caution If a zero client accesses the enterprise intranet through PPPoE or PPTP VPN and the zero client is locked-down, a non-privileged or low-privileged user attempting to reboot to Standalone user mode will disable the Network Setup dialog box and system reset capabilities. The user will not be able to re-access the enterprise intranet through this path. If this happens, the zero client must be moved to a location

where it can access the enterprise intranet directly (Ethernet cable) and reboot so that an administrator can make any required changes to the zero client operating configurations through the user profiles (for example, set the user profile to unlock the zero client).

DHCP and FTP Servers Available

As a network administrator in an environment where DHCP and FTP servers are available, you can set up both DHCP and FTP network services and create "global" and "user" INI files as described in the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

Tip A zero client is initially (new-zero client or reset zero client to default configurations) configured to obtain its IP address and the location of the FTP server from a DHCP server. DHCP can only be used for the Ethernet Direct access.

A wnos.ini file contains the "global" parameters you want that will affect all zero clients accessing the file server. A {username}.ini file contains the user-specific or "user profile" parameters you want that will comprise the connection profile for an individual user. For information on constructing these INI files, refer to the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

After DHCP and FTP servers are configured and available, simply connect the zero client to the network (directly through a network cable), turn it on, and begin using the zero client. A sign-on name and password may be required for access to the session services. If applications (published by Citrix PNAgent/ PNLite services) are available, a Domain name must be entered or selected from the list. Connections or applications may start automatically if they are configured to automatically start in the INI files.

Tip If session connections or published applications are designated to open automatically on start-up, upon accessing the enterprise server environment you will see a session server log-in or server application window instead of the zero client desktop. Use Ctrl-Alt-Up Arrow to toggle between window display modes. Use Ctrl-Alt-Down Arrow to open a selection box for toggling between the desktop, the Connect Manager, and currently active connections.

If the zero client accesses the enterprise server environment through a manually initiated Dial-up, PPPoE, or PPTP VPN, the automation provided by a DHCP server is not available. In such cases, refer to FTP Server Available (DHCP Server Unavailable), page A-2 and FTP and Virtual Desktop Servers Unavailable (Standalone User or PNAgent/PNLite-only User), page A-5 for configuration information.

Tip If Dial-up, PPPoE, or PPTP VPN are automatically started, FTP server services can be accessed through these connections.

FTP Server Available (DHCP Server Unavailable)

In an environment where a DHCP server is not available but an FTP server is available, the zero client user must locally enter (using the Network Setup dialog box) network information that would otherwise be supplied by the DHCP server.

If the zero client is configured for DHCP (new-zero client or reset zero client to default configurations) but DHCP is not detected on the network, the Network Setup dialog box automatically opens when the zero client is started. You can also open the Network Setup dialog box manually by clicking on the desktop background, selecting System Setup from the desktop menu, and then clicking Network. In the Network Setup dialog box, select the Statically specified IP Address option and configure the dialog box for the following information (any remaining information will be automatically populated from the INI files when the FTP server is contacted):

- Static IP address of the zero client
- Subnet Mask
- Default Gateway
- DNS Domain Name (not necessary if DNS is not used)
- DNS Server Address (not necessary if DNS is not used)
- File Server IP address or DNS name of the FTP server on which the INI files reside and the FTP path on the server to /wnos.
- PNAgent/PNLite Servers list (If PNAgent/PNLite is deployed on the network environment, enter the IP address or Host name with optional TCP port number of one or more PNAgent/PNLite servers that will provide published applications on the network)
- Ethernet Speed
- WINS Server Address (not necessary if WINS is not used)
- Username and Password for login to the FTP server
- Rapport Server Address (not necessary if Rapport server is not used)
- Time Server

Tip A wnos.ini file contains the “global” parameters you want that will affect all zero clients accessing the file server. A {username}.ini file contains the user-specific or “user profile” parameters you want that will comprise the connection profile for an individual user. For information on constructing these INI files, refer to the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

After the network settings are configured, reboot the zero client before using it. A sign-on name and password may be required for access to the session services. If applications (published by Citrix PNAgent/PNLite services) are available, a Domain name must be entered or selected from the list. Connections or applications may start automatically if they are configured to automatically start in the INI files.

DHCP and Virtual Desktop Servers Available

A zero client is initially (new-zero client or reset zero client to default configurations) configured to obtain its IP address and the location of the Virtual Desktop server from a DHCP server. DHCP can only be used for the Ethernet Direct access configuration.

As a network administrator in an environment where DHCP and Virtual Desktop servers are available, you can set up both DHCP and Virtual Desktop network services and create “global” and “user” INI files (in the Virtual Desktop Broker) as described in the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

Tip A zero client is initially (new-zero client or reset zero client to default configurations) configured to obtain its IP address and the location of the Virtual Desktop server from a DHCP server. DHCP can only be used for the Ethernet Direct access configuration.
A wnos.ini file contains the "global" parameters you want that will affect all zero clients accessing the file server. A {username}.ini file contains the user-specific or "user profile" parameters you want that will comprise the connection profile for an individual user. For information on constructing these INI files, refer to the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

After DHCP and Virtual Desktop servers are configured and available, simply connect the zero client to the network (directly through a network cable), turn it on, and begin using the zero client. A sign-on name and password may be required for access to the session services. If applications (published by Citrix PNAgent/PNLite services) are available, a Domain name must be entered or selected from the list. Connections or applications may start automatically if they are configured to automatically start in the INI files.

Tip If session connections or published applications are designated to open automatically on start-up, upon accessing the enterprise server environment you will see a session server log-in or server application window instead of the zero client desktop. Use Ctrl-Alt-Up Arrow to toggle between window display modes. Use Ctrl-Alt-Down Arrow to open a selection box for toggling between the desktop, the Connect Manager, and currently-active connections.

If the zero client accesses the enterprise server environment through a manually initiated Dial-up, PPPoE, or PPTP VPN, the automation provided by a DHCP server is not available. In such cases, refer to Virtual Desktop Server Available (DHCP Server Unavailable), page A-4 for configuration information.

Tip If Dial-up, PPPoE, or PPTP VPN are automatically started, Virtual Desktop server services can be accessed through these connections.

Virtual Desktop Server Available (DHCP Server Unavailable)

In an environment where a DHCP server is not available but a Virtual Desktop server is available, the zero client user must locally enter (using the Network Setup dialog box) network information that would otherwise be supplied by the DHCP server.

If the zero client is configured for DHCP (new-zero client or reset zero client to default configurations) but DHCP is not detected on the network, the Network Setup dialog box automatically opens when the zero client is started. You can also open the Network Setup dialog box manually by clicking on the desktop background, selecting System Setup from the desktop menu, and then clicking Network. In the Network Setup dialog box, select the Statically specified IP Address option and configure the dialog box for the following information (any remaining information will be automatically populated from the INI files when the Virtual Desktop server is contacted):

- Static IP address of the zero client
- Subnet Mask
- Default Gateway
- DNS Domain Name (not necessary if DNS is not used)

- DNS Server Address (not necessary if DNS is not used)
- Ethernet Speed
- WINS Server Address (not necessary if WINS is not used)
- Username and Password for login to the FTP server
- Rapport Server Address (not necessary if Rapport server is not used)
- Time Server
- VDI Server

Tip A wnos.ini file contains the "global" parameters you want that will affect all zero clients accessing the file server. A {username}.ini file contains the user-specific or "user profile" parameters you want that will comprise the connection profile for an individual user. For information on constructing these INI files, refer to the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

After the network settings are configured, reboot the zero client before using it. A sign-on name and password may be required for access to the session services. If applications (published by Citrix PNAgent/PNLite services) are available, a Domain name must be entered or selected from the list. Connections or applications may start automatically if they are configured to automatically start in the INI files.

FTP and Virtual Desktop Servers Unavailable (Standalone User or PNAgent/PNLite-only User)

In an environment where FTP and Virtual Desktop Broker servers are not available (for example, Standalone User or PNAgent/PNLite-only User situations), configuration files are not available and network information must be entered locally at the zero client as follows:

- Standalone User—This user does not access user profiles or PNAgent/PNLite-published applications. New and Settings command buttons appear in the Connect Manager for use (if the Connect Manager does not open automatically, open it from Desktop menu). These command buttons are also available to low-privileged and non-privileged users. Locally entered connection definitions (using these command buttons) are preserved for the next zero client use after the zero client is powered off and restarted (automatic software updates, however, are not available when the zero client is powered on again).
- PNAgent/PNLite-only User—This user does not access user profiles, but applications (published by Citrix PNAgent/PNLite services) are available (the IP address of a PNAgent/PNLite server and Domain are entered into the Network Setup dialog box or available through DHCP options 181 and 182). A login dialog box (similar to the standard login dialog box) opens for logging on to the PNAgent/PNLite server. Applications published by PNAgent/PNLite are listed in the Connect Manager (Published applications that add a shortcut to the client desktop will have an icon on the desktop which you can double-click to open). Locally entered connection definitions are not preserved for the next zero client use after the zero client is powered off and restarted.

Configuring Network Services

Before you use the information in this section to configure your network services, be sure you have read Understanding How to Configure Your Network Services, page A-1, and remember the following important issues:

- Restrictions to Network Services can Exist—Zero client network services reside on the enterprise intranet. When setting up zero client network services, remember that if zero clients are to access the enterprise intranet through Dial-up, PPPoE, or PPTP VPN, restrictions imposed by these access paths must be considered.
- Know How Your Environment Works—Either the FTP server or the Virtual Desktop server (depending on your environment) holds the INI files, while the FTP server (if available) holds the current and upgrade versions of the zero client software.

  The zero client software is acquired from either local flash memory or the FTP server. During the boot process, the local image is transferred to RAM and executed far enough for the zero client to check the image and the INI files on the file servers. Under direction of the INI files and the version of the remote image, the image in RAM can be replaced with the remote image; and separately, the remote image can update the local flash-memory.
- Functionality Depends on You—The WTOS INI files contain the parameters and associated values necessary for the various functionality you want. The INI files (wnos.ini file and {username}.ini file) are constructed and maintained by you and are stored on the file server for use with zero clients running WTOS.

Tip The INI files contain connection definitions and zero client settings. These text-based files must be created and maintained by using an ASCII text editor. If the INI files are omitted or they cannot be accessed because a file server is not used, the zero client user must enter connection definitions locally (or for FTP servers, use what is published by PNAgent/PNLite servers residing on the network).

You can also define connections in the INI files which are to be stored in local NV-RAM and used in cases where the file server fails.

A wnos.ini file contains the “global” parameters you want that will affect all zero clients accessing the file server. A {username}.ini file contains the user-specific or “user profile” parameters you want that will comprise the connection profile for an individual user. The zero client accesses the wnos.ini file upon zero client initialization and accesses any individual {username}.ini file when the user logs on (if user login is required, the {username}.ini file must exist before that user can log in). For information on constructing these INI files, refer to *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

To configure network services, use the information in the following sections:

- Configuring FTP Servers, page A-7
- Configuring Virtual Desktop Infrastructure Servers, page A-9
- Configuring XenDesktop Support, page A-9
- Configuring DHCP (DHCP Options), page A-9
- Configuring DNS, page A-14
- Configuring WINS, page A-14
- Configuring Cisco VXC Manager Servers, page A-14

Configuring FTP Servers

Before you use the information in this section to configure your FTP server, be sure you understand and use the following guidelines:

- General Guideline—When the zero client boots, it accesses the software update images and INI files from the FTP server. The FTP server and path to the software update files are available through DHCP vendor options 161 and 162 (see Configuring DHCP (DHCP Options), page A-9). If these are not specified, the default FTP server is the DHCP server from which the zero client receives its IP address and the default directory (\wnos for Windows FTP servers, or /wnos for Linux FTP servers).

  The FTP server and path to the software update files can also be specified locally on the zero client. DHCP options 184 and 185 can be used to provide the User ID and Password for non-anonymous access to the FTP server in WTOS.

- Non-Anonymous Access Guidelines—You must first create a local account (name the account so that you remember it is a non-anonymous account) on the FTP server defined between the DHCP vendor options 161 and 162 (DHCP server). Then, add DHCP options 184 and 185 to provide the User ID and Password for non-anonymous access to the FTP server. Ensure that option 184 is the account User ID and that option 185 is the account Password, and that you keep consistency with FTP server DHCP vendor options (for example, ensure that the 184 and 185 options are string parameters). Then provide the non-anonymous account with read-only permissions through the entire FTP server path. Be sure to modify these guidelines according to your specific security environment and configuration.

- Windows FTP Server Guideline—You can use the FTP tools available on the Windows server. For WTOS, this support is not necessary because of the User Interface (UI)/DHCP feature to specify the login ID and password.

- Linux FTP Server Guideline—Be aware of the following:

  - The FTP server must be configured to offer FTP services (by adding the following line or equivalent to the /etc/inetd.conf file, if it is not already present):

    ftp stream tcp nowait root /usr/sbin/tcpd in.proftpd

  - The FTP server must be configured to support anonymous FTP. For most FTP servers, this requires establishment of an FTP login account by adding the following line or equivalent to the /etc/password file:

    ftp:x:17:1:Anonymous FTP directory:/home/ftp:/dev/null/ftp-shell

    The shell file /dev/null/ftp-shell need not exist, but some FTP servers require that it be listed in the /etc/shells file to allow FTP connections on this account.

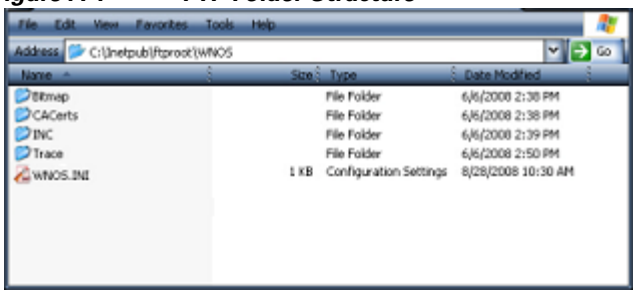
  - Depending on which Linux distribution you are using, additional modifications to a central configuration file for the FTP daemon may be necessary to enable anonymous FTP. You can try man protftp, man wuftpd, or man ftpd to access information applicable to your particular FTP daemon.

  - A Linux server used for FTP must support passive FTP.

- FTP Folder Structure Guidelines—The FTP folder structure that is required by zero clients running WTOS is \wnos and must be placed under the FTP root folder (if DHCP option tag 162 is not used) or under the folder which has been specified by DHCP option 162. For example, if DHCP option tag 162 has been configured with the name ThinClients and DHCP option tag 161 has been configured with IP address 192.168.1.1, then the zero client will check the folder <FTPRoot>\ThinClients\wnos for a wnos.ini and firmware on the FTP server with the IP address (192.168.1.1). The sub-folder \bitmap must be placed under the \wnos folder and can contain

graphical images for icons and background images. The sub-folder \cacerts can be placed under the \wnos folder and can contain your CA certificates. The sub-folder \inc can be placed under the \wnos folder and can contain the mac.ini files (note that the use of the parameter Include=$mac.ini will load "/wnos/inc/mac-address.ini" so that you can use inc in the folder structure and use $MAC.ini). The sub-folder \trace can be placed under the \wnos folder and can contain the trace files that you can capture and play back (be sure to enable the parameter, EnableTrace=yes). Figure A-1 shows an example of the folder structure of an FTP server for WTOS.

Figure A-1 FTP Folder Structure



To configure an FTP server, complete the following procedure.

Procedure

Step 1 Create the following directory structure on your FTP server:

<path from anonymous user FTP root>\wnos\

<path from anonymous user FTP root>\wnos\bitmap\

<path from anonymous user FTP root>\wnos\cacerts\

<path from anonymous user FTP root>\wnos\inc\

<path from anonymous user FTP root>\wnos\trace\

Step 2 If you need to upgrade the firmware for your zero client, place it in the wnos subdirectory of your FTP server.

Step 3 Obtain the Sample User INI files (see the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide* for the example INI files) and copy them into a directory from which they can be examined and modified using an ASCII text editor. These sample files are annotated to allow you to use them as a starter set on your FTP server and can be modified to suit your needs. The sample files include:

- wnos.kiosk—Example wnos.ini file for a kiosk configuration
- wnos.login —Example wnos.ini file to enable multiple user accounts
- user.ini—Template for {username}.ini for individual user profiles

Step 4 Determine whether all the zero clients served by this FTP server will be used as kiosks or will support individual user accounts. You must rename the downloaded files so that there will be one wnos.ini file available to all users globally; and for a multiple user account configuration there will be a unique {username}.ini file for each user. In addition:

- If the kiosk configuration is to be used—Change the name of wnos.kiosk to wnos.ini. Otherwise, for multiple user accounts, change the name of wnos.login to wnos.ini.
- If the individual user account configuration is to be used—Make a copy of the user.ini file for each user name as {username}.ini (where {username} is the name of the user) and place the files in the subdirectory ini of wnos. The files must have read permission enabled, and if users are to be allowed to change their passwords, the files also must have write permission enabled (so that

the zero clients can write the encrypted user passwords to them). For Linux servers, use the chmod command to set the read/write permissions. For Microsoft servers, use the Properties dialog box to set read/write permissions.

Step 5 If desired, you can customize the INI files to match the local environment using the instructions in the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*. If you modify the INI files to include icons and logos, be sure to place the images in the FTP server/wnos/ bitmap subdirectory.

Configuring Virtual Desktop Infrastructure Servers

When the zero client boots, it accesses the INI files from a Virtual Desktop Infrastructure (VDI) server. VDI servers are available through DHCP vendor option 188 (see Configuring DHCP (DHCP Options), page A-9).

The zero client communicates with a Virtual Desktop Broker server by the sysinit, signon, signoff, and shutdown commands. When the zero client boots and successfully connects in a Virtual Desktop environment, it sends the sysinit command to the Virtual Desktop Broker, which then sends back the wnos.ini file (if a broker connection cannot be made, the zero client will attempt to connect to an FTP or PNLite server). After the zero client successfully receives the wnos.ini from the Virtual Desktop Broker, a sign-on window displays, prompting the user for username and password credentials. The zero client then sends the signon command to the Virtual Desktop Broker with the username and password as its parameter. If the sign-on is successful, the Virtual Desktop Broker server will send back the {username}.ini file (if the sign-on is unsuccessful, the user is prompted again for username and password credentials). The signoff command will be sent when a user disconnects from the connection. The shutdown command will be sent when a user turns off the zero client power.

Configuring XenDesktop Support

XenDesktop is supported in WTOS without the need to use a Web browser. To connect to XenDesktop, do not use the VDI Broker parameter. Instead, use the same parameter and configuration that is used when connecting to a PNAgent/Lite server.

Configuring DHCP (DHCP Options)

Before you use the information in this section to configure your DHCP server, be sure you understand and use the following guidelines:

- General Guidelines—The DHCP service provides all zero clients on the network with their IP addresses and related network information when the zero clients boot. DHCP also supplies the IP address and directory path to the zero client software images and user profiles located on the file servers.

  Use of DHCP is recommended. However, if a DHCP server is not available, fixed IP addresses can be assigned (this does, however, reduce the stateless functionality of the zero clients) and the fixed IP addresses must be entered locally for each device using the zero client Network Setup dialog box as described in FTP Server Available (DHCP Server Unavailable), page A-2 and Virtual Desktop Server Available (DHCP Server Unavailable), page A-4).

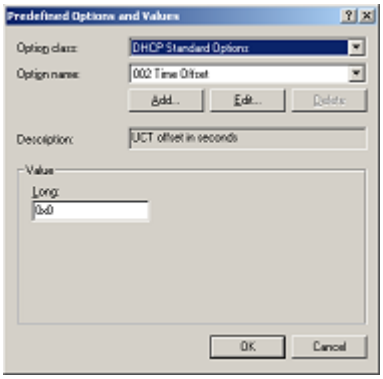
Many DHCP options correspond to places in the network configuration UI where the zero client user can enter information manually. Be aware that wherever there is information in the UI and the zero client receives information about the same function from one or more DHCP options, the information received from the DHCP server will replace the information contained in the UI. However, if the zero client does not receive information from the DHCP server about a particular function, the information manually entered in the UI will remain and will be used.

- LPD Print Server Guideline—If a particular zero client is to function as an LPD print server, it can be assigned a fixed IP address. However, you can also guarantee that an LPD server will always have the same IP address by making a reservation for that zero client in the DHCP server. In that way, you can preserve the stateless nature of the zero client and still guarantee a fixed address for the server. In fact, you can assign a symbolic name to the reservation address so that other zero clients can reference the LPD server by name rather than by static IP address (the symbolic name must be registered with a DNS server before other zero clients will be able to locate this LPD server). The zero client does not dynamically register its name and the DNS registration must be manual.
- Cisco VXC Manager Guidelines—If you use Cisco VXC Manager, the zero client uses port 80 as the default to access a Cisco VXC Manager server. If a port other than 80 is used to access a Cisco VXC server, use option 187 in the list of DHCP options in Table A-1 on page A-11 (option for a Cisco VXC Manager server is option 186 in the list of DHCP options in Table A-1 on page A-11). Cisco VXC Manager options are the only options used by the zero client that are not in text form.
- PNAgent/PNLite Server Guidelines—If you use a a PNAgent/PNLite server, the zero client uses port 80 as the default to access a PNAgent/PNLite server. If a port other than 80 is used to access a PNAgent/PNLite server, the port number must be specified explicitly with the server location in the form IP:port or name:port (option for a PNAgent/PNLite server is option 181 in the list of DHCP options in Table A-1 on page A-11).
- Windows DHCP Server Guidelines—You can use the DHCP tools available on the Windows server.
- Linux DHCP Server Guidelines —For Linux servers, enter DHCP options 161 and 162 (described in Table A-1 on page A-11) in `/etc/dhcpd.conf` (refer to the manual page `man dhcpd.conf` for more information on DHCP and the syntax of this file). For example, if you want the computer to search `ftp://132.237.16.157/pub/serversoftware/wnos`, add the following line to `/etc/dhcpd.conf`:

  ```
  option option-161 132.237.16.157;option option-162 "pub/serversoftware$";
  ```

  As mentioned in Table A-1 on page A-11, the /wnos suffix is automatically appended to the FTP path, so you should not specify it explicitly. In this case, the actual directory searched will be pub/serversoftware/wnos.
- DHCP Options Guidelines—WTOS uses several DHCP option tags. These option tags must be created, activated within the DHCP scope(s), and then added for the zero clients to use them. Figure A-2 shows the Windows DHCP Server Predefined Options and Values dialog box that is displayed when right-clicking the DHCP server and selecting Set Predefined Options. The most commonly used tags are 161 and 186. Depending on the Terminal Server environment, more options can be added using the Predefined Options and Values dialog box.

Figure A-2 Predefined Options and Values



Use the guidelines shown in Table A-1 when creating and adding the DHCP option tags you need for your zero clients.

Tip Ensure that within the DHCP scope these new DHCP option tags you create are activated (this can be done using the Configure Options command), before you add them.

Table A-1 DHCP Options

Option	Description	Notes
1	Subnet Mask	Required only if the zero client must interact with servers on a different subnet (MS DHCP requires a subnet mask and will always send one).
2	Time Offset	Optional.
3	Router	Optional, but recommended. It is not required unless the zero client must interact with servers on a different subnet.
6	Domain Name Server (DNS)	Optional, but recommended.
15	Domain Name	Optional, but recommended. See Option 6.
28	Broadcast Address	Optional.
44	WINS servers IP Address	Optional.
51	Lease Time	Optional, but recommended.
52	Option Overload	Optional.
53	DHCP Message Type	Recommended.
54	DHCP Server IP Address	Recommended.
55	Parameter Request List	Sent by zero client.
57	Maximum DHCP Message Size	Optional (always sent by zero client).
58	T1 (renew) Time	Optional, but recommended.
59	T2 (rebind) Time	Optional, but recommended.
61	Client identifier	Always sent.

Table A-1 DHCP Options (continued)

Option	Description	Notes
161	FTP server list	Optional string. Can be either the name or the IP address of the FTP server. If a name is given, the name must be resolvable by the DNS servers specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to also be the FTP server.
162	Root path to the FTP files	Optional string. If the option provided by the server is blank and the server provides no value for the field, a null string is used. \wnos is automatically appended to the search path. For example, if you enter pub\serversoftware, the path searched will be pub\serversoftware\wnos. **Note** The usage or omission of a leading slash (\) on the path is critical on some servers. Some servers limit access to the root path of the user specified at login. For those servers, the usage of the leading slash is optional. Some UNIX servers can be configured to allow the FTP user access to the entire file system. For those servers, specifying a leading slash specifies that access is to start at the root file system. Proper matching of the file specification to the FTP server in use is critical to ensuring proper operation. A secured Windows server requires the slash be specified in order to complete proper access.
181	PNAgent/PNLite server list	Optional string. The zero client uses the server to authenticate the Windows credentials of the user and to obtain a list of ICA published applications valid for the validated credentials. The user supplies those credentials when logging in to the zero client.

Table A-1 DHCP Options (continued)

Option	Description	Notes
182	NT domain list for PNAgent/PNLite	Optional string. The zero client creates a pull-down list of domains from the information supplied in option 182. This list is presented at zero client login in the order specified in the DHCP option (for example, the first domain specified becomes the default). The selected domain is the one which must authenticate the user ID and password. Only the selected domain is used in the authentication process. If the domain list is incomplete and the user credentials must be verified against a domain not in the list (assuming that the server in option 181 is capable of authenticating against a domain not in the list), the user has the option of not using any of the domains specified in option 182 and typing a different domain name at the time of login.
184	FTP Username	Optional string.
185	FTP Password	Optional string.
186	Cisco VXC Manager server list	Optional binary IP addresses of Cisco VXC Manager. This option can specify up to two Cisco VXC Manager servers. If two are specified, at boot time the zero client will attempt to check-in to the first server. If it cannot contact the first server it will try to check-in to the second server.
187	Cisco VXC Manager server port	Optional number. Byte, word, or two-bytes array. **Note** The value of this option tag, when not embedded in Vendor Class Specific Information option, is interpreted in reverse order when it is sent as 2 bytes (for example, the value of 0x0050 was interpreted as 0x5000).
188	Virtual Desktop Broker port	Optional string.
190	Cisco VXC Manager secure port	Optional number. Word, or two-bytes array. Specifies to use HTTPS to communicate with Cisco VXC Manager instead of HTTP.
192	Cisco VXC Manager server port	Optional number. Word, or two-bytes array. **Note** The value of this option tag represents the same information as option tag 187. The difference is that WTOS interprets the value of this option tag in correct order (for example, the value of 0x0050 is interpreted as 0x0050). If the DHCP server provides both option tag 192 and 187, option tag 192 takes precedence.

Tip The zero client conforms to both RFC-compliant DHCP servers (RFC numbers 2131 and 2132) and RFC-noncompliant Microsoft servers (which NULL terminate strings sent to the zero client). The zero client supports both infinite leases and leases that expire (per RFC 2131 and others).

Tip Not all options in the range 128 to 254 are strings. Options 186, 190, and 192 are employed for all Cisco products that use Cisco VXC Manager. Their format and content are determined by the Cisco VXC Manager product.

Configuring DNS

Zero clients accept valid DNS names registered on a DNS server available to the enterprise intranet. In most cases, DNS is not required but may be used to allow hosts to be accessed by their registered DNS names rather than their IP addresses. Every Windows DNS server in Windows 2000 and later includes Dynamic DNS (DDNS) and every server registers dynamically with the DNS server. There are also DDNS implementations available for UNIX environments. However, the zero client does not perform dynamic registration, and therefore, requires a static or non-variant IP address and manual DNS registration in order to provide LPD support by name (for example, in the case where the zero client is used as an LPD printer server or if DHCP is not available). For DHCP entry of DNS domain and server location information, refer to Configuring DHCP (DHCP Options), page A-9.

Configuring WINS

The zero client does not do dynamic registration and therefore, requires a static or non-variant IP address and manual Windows Internet Naming Service (WINS) registration. Use the network address of an available WINS name server. WINS allows the zero client user to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than WINS will be used to make the connection. These entries are supplied through DHCP, if DHCP is used.

Tip You may use two WINS server addresses, separated by a semicolon, comma, or space. The first address is for the primary WINS server and the second address is for a backup WINS server.

Configuring Cisco VXC Manager Servers

Cisco VXC Manager servers provide network management services to the zero client (complete user-desktop control—with features such as remote shadow, reboot, shutdown, boot, rename, automatic device check-in support, Wake-On-LAN, change device properties, and so on). Use the IP addresses or host names with optional TCP port number for Cisco VXC Manager servers. Each entry with optional port number is specified in the form IP:port or name:port, where :port is optional (if not specified, port 80 is used).

Configuring for Transport Layer Security (TLS) Connections Over a LAN

The IEEE 802.1x standard allows a switch port to remain wired or enabled but not permit traffic to traverse the switch until the identity of the client is confirmed. IEEE 802.1x is a security feature. It defines the process of authenticating a wired client to allow the client to communicate with the network. WTOS supports IEEE 802.1x for zero clients to be authenticated to access an Ethernet network. To enable this connection, you must download certificates from a Certificate Authority (CA), and then install and configure them for the zero client.

To configure the authentication options:

Procedure

Step 1 Open the Network Setup dialog box (click the desktop to open the menu, select **System Setup**, and then click **Network**).

Step 2 Click the **Security** tab.

Step 3 Select the **Enable IEEE802.1x Authentication** check box.

Step 4 In the **EAP Type** drop-down list, select an Extensible Authentication Protocol option.

Tip In Wire mode, only the TLS EAP type is available.

Step 5 Use the following guidelines to configure the EAP Type option you selected:

- TLS—If you select the TLS option, click **Properties** to open and configure the Authentication Properties dialog box (you can use Browse to find and select the Client Certificate file and Private Key file you want). Note that the CA certificate must be installed in the device.

Step 6 In the Network Setup dialog box, select an **Import From** option (either USB Key [the default] or File Server) to configure where a user can import a new certificate, click **Import**, and then use the following guidelines to configure the option you selected:

- USB Key: Select a certificate and click OK to import it to local memory.
- File Server: Enter the path to the certificate, and then enter a username and password.

Configuring Session Services

Before you use the information in this section to configure your ICA and RDP session services, be sure you understand and use the following guidelines:

- General Guidelines—Be aware of the following:
  - The Thin-client session services are made available by servers hosting Citrix ICA and Microsoft RDP software products.
  - A browser must be available through one of the session services to access any on-line help documentation for users.
  - There can be more connections than desktop space to display them.

  - Connections can be defined in persistent memory (with a statement reading enablelocal=yes in the wnos.ini file). These connections can be displayed as desktop icons only in Standalone mode with a Non-privileged user.
  - Only the connections defined in an INI file and containing an icon= clause will be displayed on the desktop (assuming there is adequate desktop space).
  - Connections can be displayed on the desktop without requiring a sign-on (when you define these connections in a wnos.ini file or when the wnos.ini file does not contain a SignOn=yes statement).

- ICA Guidelines—Independent Computing Architecture (ICA) is a three-tier, server-based computing technology that separates the logic of an application from its user interface. The ICA client software installed on the zero client allows the user to interact with the application GUI, while all of the application processes are executed on the server. ICA connects to NT TSE, Windows Server 2003, or Windows Server 2008 Server hosts that have a Citrix MetaFrame server, Citrix Presentation server, or CDS installed. Load balancing is included. ICA browsing or DNS can be used to resolve the server name. For information on configuring ICA, refer to Configuring ICA Session Services, page A-16. For detailed information on the supported parameters (in the INI files) that you can use for ICA connections, refer to the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

Tip The ICA server must be licensed from Citrix Systems, Inc. You must purchase enough client licenses to support the total concurrent zero client load placed on the Citrix server farm. A failure to connect when all client seats are occupied does not represent a failure of Cisco equipment. The ICA client software is installed on the zero client.

- RDP Guideline—Remote Desktop Protocol (RDP), like ICA, is a network protocol that allows a zero client to communicate with the Terminal Server or Windows 2003/2008 Server with Terminal Services over the network. This protocol is based on the T.120 protocol suite, an international standard multi-channel conferencing protocol. For information on configuring RDP, refer to Configuring RDP Session Services, page A-17. For detailed information on the supported parameters (in the INI files) that you can use for RDP connections, refer to the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

Configuring ICA Session Services

Before you use the information in this section to configure your ICA session services, be sure you have read Configuring Session Services, page A-15.

ICA session services can be made available on the network using either Windows 2003/ 2008 Server with Terminal Services and one of the following installed:

- Citrix MetaFrame XP
- Citrix Presentation Server

Tip If PNAgent/PNLite-published application services are to be made available to the zero clients, refer to PNAgent/PNLite Installation Guidelines, page A-17 when installing Citrix MetaFrame XP.

When using the instructions accompanying these products to install them and make sessions and applications available to the zero clients sharing the server environment, be aware of the following:

- If a Windows 2003/2008 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere accessible on the network. The server will grant a temporary (120-day) license on an individual device basis. Beyond the temporary (120-day) license, you must purchase TSCALs and install them on the TSCAL server (you will not be able to make a connection without a temporary or permanent license).
- It is recommended that any ICA connection which traverses a Dial-up or WAN connection have Lowband=yes set in the INI files or the Optimize for low speed link option selected in the Connection Settings (ICA) dialog box.
- If an ICA connection is created using the Connect Manager and the Host Names or Application Name text box is left blank, a message appears prompting the user to enter the IP Address or Server Name of the ICA server to which to connect.
- An audio input port is available (Audio can be recorded).

PNAgent/PNLite Installation Guidelines

PNAgent/PNLite is a component of the Citrix XML publishing service. PNAgent/PNLite is an ICA connection mode that enables the zero client to connect to applications available (published) on an ICA server without having to configure connections for individual published applications.

Use the following guidelines during installation:

- MetaFrame X—Installing MetaFrame XP supports XML publishing services. During installation, a series of prompts appear for you to follow. When you are prompted to install the XML Publishing Service, be aware that clicking Yes to this option allows you to change the default port (80) used by the service.
- Citrix Presentation Serve—Installing Citrix Presentation Server supports XML publishing services. During installation, a series of prompts appear for you to follow.

The port to be used for XML publishing services must be known for making appropriate PNAgent/PNLite server location entries required by the operating mode (for related information, refer to Configuring DHCP (DHCP Options), page A-9 and the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*). The zero client uses port 80 as the default port, but if a port other than 80 is used, the port number must be specified explicitly with the PNAgent/PNLite server location in the form IP:port or name:port, where :port is optional.

Configuring RDP Session Services

Before you use the information in this section to configure your RDP session services, be sure you have read Configuring Session Services, page A-15.

RDP session services can be made available on the network using any of the following:

- Windows 2003/2008 Server with Terminal Services installed
- Windows NT 4.0 Terminal Services (WTS) Edition
- Windows XP

When using the instructions accompanying these products to install them and make sessions and applications available to the zero clients sharing the server environment, be aware of the following:

- If a Windows 2003/2008 Server is used, a Terminal Services Client Access License (TSCAL) server must also reside somewhere accessible on the network. The server will grant a temporary (90-day) license on an individual device basis. Beyond the temporary (90-day) license, you must purchase TSCALs and install them on the TSCAL server (you will not be able to make a connection without a temporary or permanent license).
- It is recommended that any RDP connection which traverses a Dial-up or WAN connection have Lowband=yes set in the INI files or the Optimize for low speed link option selected in the Connection Settings (RDP) dialog box.
- If an RDP connection is created using the Connect Manager and the Host Names or Application Name text box is left blank, a message appears prompting the user to enter the IP Address or Server Name of the RDP server to which to connect.
- WTOS supports an RDP connection with no encryption (found in older versions of Microsoft NT4-TSE servers).
- WTOS supports server browsing over Server Message Block (SMB) when defining an RDP connection. SMB browsing restrictions mean that the server desired may not be listed, in which case the user will need to know either the name or IP address of the target server and enter that information into the text box (as it will not appear in the pull-down list).

APPENDIX **B**

Remote System Administration

This appendix provides remote system administration information to help you perform the routine tasks needed to maintain your WTOS environment.

It includes:

Using Cisco VXC Manager Software For Remote Administration

Cisco VXC Manager servers provide network management services to the zero client (complete user-desktop control, with features such as remote shadow, reboot, shutdown, boot, rename, automatic device check-in support, Wake-On-LAN, change device properties, and so on).

Updating Software

The software version is embedded in both the RAM and flash memory images. This version information is used to compare the images on the FTP server to the currently-loaded flash image on the zero client. A major revision number supersedes a minor revision number when making the comparison. In turn the minor version number takes precedence over the build number. The image names and date-time stamps determine whether or not the update is newer than the version currently installed on the zero client.

Tip The code identifier is split into four parts, the major release identifier, the minor release identifier, the build number identifier, and the sub-build number identifier (if the sub-build number is 0, it will not be displayed). Each part is compared to the current code internal identifier in the same format. If the file identifier is greater, the update is performed. If the file identifier is less, the update is abandoned. If the file identifier is equal, the next term is examined until the build identifiers are found to be equal and the update is abandoned. This comparison process using the build number can be important in cases where you are using a beta release, or in cases where you need to reinstall a release with the same major and minor numbers but with an updated build.

After obtaining software updates from Cisco, you must replace the existing software images in the wnos subdirectory on the FTP server to allow the zero clients to automatically detect and self-install the new software (upon zero client system start). The FTP server address and exact path to these files are specified in DHCP Options 161 and 162 (if DHCP is not used, the path is specified in the Network Setup dialog box on the zero client).

Each time a zero client boots, it checks the software images on the FTP server, and if configured, automatically performs an update if a newer version is detected. Whether or not an update is performed depends on the AutoLoad parameter setting in the wnos.ini file as described in the *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide*.

Be aware that there is a significant distinction between using DHCP and not using DHCP to access the various necessary files as follows:

- If DHCP is used, zero client software automatically inserts the path command /cisco following what it receives from the DHCP server (unless the path is terminated by a $); this is done only if a value is received from DHCP. The dollar sign character ($) acts as a flag that notifies WTOS that the absolute path has been given (that is, where it expects to find WTOS configuration files inside a "wnos" folder) instead of the relative path (where it expects to find the general "cisco" configuration folder).
- If DHCP is not used and the configuration is done manually, the full path up to the wnos component must be inserted; there is no automatic /cisco insertion and no $ processing.
- Note that WTOS software does not recognize a $ terminator as a legal meta-character in a locally entered string.

Tip Citrix ICA Auto-Update does not function for the ICA client installed on the zero client; the ICA client is fully contained in the zero client system and can only be updated by changing that entire system. The RDP client is also not replaceable.

Caution Interrupting power during the update process can corrupt the FLASH on the zero client. Zero clients with corrupted FLASH must be shipped to Cisco for service.

Managing Icons and Logos

Icons and logos specified in the INI files must be placed in the file server /wnos/bitmap subdirectory. Icons are specified in the Icon clause of the connection statement and logos are specified in the FormURL statement. Supported image file types include .ico (icon), .bmp (bitmap), .jpg (JPEG), and .gif(GIF). Color depth for logos can be up to 256 colors. Color depth for icons can be 16 colors. It is recommended that .jpg format not be used for desktop icons.

Use the following guidelines:

- Typical desktop icons are 64 x 48 pixels.
- Typical sign-on logos are 100 x 61 pixels, with transparent background.
- Maximum size for sign-on logos is 352 x 80 pixels (if smaller than this, it will be positioned in the upper-left corner).

Understanding and Using System Lockdown Operations

Lockdown status for a zero client is set or removed using the LockDown clause of the Privilege statement in the INI files. Lockdown establishes the default privilege level following zero client boot and before any privilege statement is read from an INI file.

Access to many facilities is affected by the privilege level.

- Non-Lockdown Operation—For normal operation, Low-privileged and Non-privileged users may access the Network Setup dialog box by temporarily disconnecting the Ethernet cable from the zero client and rebooting to Standalone user mode. The Network Setup dialog box can also be accessed after resetting the zero client to factory defaults by a G-key reset to factory default or using the Reset the system setting to factory defaults check box in the Sign-off/Shutdown window of any user with sufficient privilege to the Sign-off/Shutdown window.
- Lockdown Operation —In most cases, access to the resources available when the system is not locked down is desirable; however, network environments requiring maximum security should not permit uncontrolled changes to zero client network access. Most facilities would include a Privilege with LockDown statement in the wnos.ini file and might override the privilege in a {username}.ini file without modifying the lockdown privilege. Thus, an administrator could log into any unit and have sufficient privilege to modify the configuration of that unit without altering the default privilege at the next reboot.

Caution If the unit is configured for Dial-up access, there must be an RAS server answering the configured telephone number. Otherwise, the unit will require factory attention to recover it.

APPENDIX C

Local System Administration

This appendix provides local (at the zero client) system administration information to help you perform the routine tasks needed to maintain your WTOS environment.

The appendix includes:

Resetting to Factory Defaults Using G-Key Reset

High-privileged or Standalone users can reset the zero client to factory default settings using the G-key reset feature.

To reset the zero client to factory default settings, restart the zero client and continuously tap the G key during the restart process. G-key reset impacts all configuration items, including, but not limited to, both network configuration and connections defined in local NV-RAM.

Tip G-key reset is disabled for Low-privileged and Non-privileged users in Lockdown mode.

Resetting to Factory Defaults Using Shutdown Reset

A High-privileged or Standalone user can reset the zero client to factory default settings from the Sign-off/Shutdown window as follows:

Procedure

Step 1 Select either **Shutdown and Restart the system** or **Shutdown the system**.

Step 2 Select the **Reset the system setting to factory defaults** check box.

Step 3 Click **OK**.

Shutdown reset impacts all configuration items, including, but not limited to, both network configuration and connections defined in local NV-RAM (Terminal name will not change).

Tip Shutdown reset is disabled for Low-privileged and Non-privileged users, regardless of lockdown state.

Resetting Display Settings Using V-Key Reset

If the display settings are inappropriate for the particular monitor that is connected, it is possible that the display will not function properly when the zero client restarts. To correct this, power-on the zero client while continuously tapping the V key. This will restart the zero client with a display resolution of 640 x 480 pixels and a 60 Hz refresh rate.

Accessing Zero Client BIOS Settings

While starting a zero client you will see a Cisco logo for a short period of time. During this start-up you can press **Del** to enter the BIOS of the zero client to make your modifications (enter **Fireport** as the password).

Enabling a Disabled Network Setup Dialog Box

Although there are privileges and user modes associated with user access to zero client resources, access to network setup (using the Network Setup dialog box) depends upon privilege level. A Standalone user either is by default a user with High privilege or has a zero client that is locked down. A Guest user has an implicit privilege of None and all access is governed by that privilege. A PNAgent/PNLite-only user has whatever privilege was set in the wnos.ini file at zero client boot, whatever privilege was locked down at the last access of a wnos.ini file, or High privilege (by default).

If the Privilege parameter is set to Low or None in the INI files, the zero client Network Setup dialog box will be disabled (the user cannot access it). In such a case, there may be occasion to access the Network Setup dialog box without wanting to change the INI files. For example, an occasion when you need to change to another FTP or Virtual Desktop file server or add to the PNAgent/PNLite servers list. To access the Network Setup dialog box in such a case, disconnect the network cable and reboot the zero client to Standalone user mode. The Network Setup dialog box displays after the zero client initializes and you can then make the required entries (be sure to reconnect the network cable and reboot when finished).

Caution If a zero client accesses the enterprise intranet through Dial-up, PPPoE, or PPTP VPN and the zero client is locked-down, a Non-privileged or Low-privileged user attempting to reboot to Standalone User mode will disable the Network Setup dialog box and System Reset capabilities. The user will then be unable to re-access the enterprise intranet through this path. If this happens, the zero client must be moved to a location where it can access the enterprise intranet directly (Ethernet cable) and reboot so that you can make any required changes to the zero client operating configurations (for example, set the INI files to unlock the zero client).

If the zero client is configured for Dial-up access, there must be an RAS server answering the configured telephone number. Otherwise, the zero client will require factory attention to recover it.

Configuring ThinPrint

No ThinPrint-specific configuration is available on the zero clients. Thus to be able to use ThinPrint, users must first set up their printers according to the user documentation, and then configure ThinPrint on the zero client (by clicking on the desktop background, selecting **System Setup** from the menu to open the Network Setup dialog box, and then clicking **Printer** to open and use the printer configurations).

Use the following guidelines:

- Use the Printer Identification field to enter a printer class (you can change the printer name as needed).
- Printer IDs are assigned (depending on the physical port) as follows:
  - COM1 = 1
  - COM2 = 2
  - LPT1 = 3 (USB printers are detected automatically on LPT1)
  - LPT2 = 4
  - LPD0 = 5 (The LPD Queue name is transmitted as the printer name; the Printer Identification as class)
  - LPD1 = 6 (The LPD Queue name is transmitted as the printer name; the Printer Identification as class)
  - LPD2 = 7 (The LPD Queue name is transmitted as the printer name; the Printer Identification as class)
  - LPD3 = 8 (The LPD Queue name is transmitted as the printer name; the Printer Identification as class)
  - SMB1 = 9 (In the form \\host\printershare)
  - SMB2 = 10
  - SMB3 = 11
  - SMB4 = 12

To install the relevant ThinPrint product on the server, use the following guidelines:

- Printer Object(s) Created Manually by the Administrator—After you install .print Engine, create a printer object on the server to use the native driver and ThinPort as a printer port. You can use any protocol (TCP, RDP, or ICA) because WTOS has .print clients for all of the protocols. The printer object needs to observe ThinPrint naming conventions (for example, HPLJ5#_:2, in which case print jobs will be sent to the local printer that has ID number .2) by referring to .print client port ID. If no ID number is present, the .print client sends the print job to the printer set as current.
- Printer Object(s) Created Automatically by ThinPrint AutoConnect—When using ThinPrint AutoConnect, the zero client identifies with the zero client ID number 84 (and thus is recognized as a zero client without a local spooler). You can also set up a template on the server that uses a native driver (for example, HPLJ5) and ThinPort, and then name this template as you want in the form _#AnyName. You can then make sure that the rules (on ThinPrint Autoconnect [1]) have been set to assign the desired local printers to use this server template. The assigned printer will then be shown in the user session using the HPLJ5 driver and ThinPort; it will be named automatically according

to ThinPrint naming convention with the printer name from the client side included. Alternatively, you can also define a template name according to the client printer name (replace .AnyName. with printer name 4. and 5. above [for example, _#HP Laserjet 5]) so that the local printer object .HP Laserjet 5. will be mapped to this template without any rules defined on the ThinPrint Autoconnect.

APPENDIX D

Setting Up Your HTTPS/SSL Web Server

This appendix shows you how to properly configure your HTTPS/SSL web server to manage and upgrade WTOS zero clients.

Creating an Initial Windows 2003 Server or Windows XP SP2 with SSL Capabilities

Use this procedure to create an initial Windows 2003 server or Windows XP SP2 with SSL capabilities. These steps assume you have not set up your web server to use SSL.

Procedure

Step 1 Download the IIS 6.0 Resource Kit.

Step 2 Launch the Installer.

Step 3 During the Installer execution, choose **custom** for install type and **install only the SelfSSL component**.

Step 4 Browse to **Start > Programs > IIS Resources > SelfSSL > SelfSSL**. The DOS shell launches.

Step 5 Type in the following statement, replacing the computer name (CN) with your server name.

selfssl.exe /N:CN=SERVERNAME /K:1024 /V:7 /S:1 /P:443 /T

If the installation is successful, you receive the message “The self-signed certificate was successfully assigned to site 1”.

Step 6 This procedure can reconfigure any existing IIS websites you may have configured, so for advanced options refer to the SelfSSL help by typing:

Selfssl.exe -h

Configuring a Windows 2003 or Windows 2008 Web Server

Prerequisites

You need Windows 2003 Server with IIS and SSL properly configured and Windows 2008 R2.

Configuring the Web Server Mime types

The web server must identify the files types used by Cisco. To identify the files, create two MIME types under IIS. The MIMEs need to be configured on a per site basis.

Procedure

Step 1 On a default IIS installation, launch the IIS administration console.

Step 2 Browse to the **Default Web Site**, right click and select **properties**.

Step 3 Choose the **HTTP Headers** tab and under the MIME Map section choose **File Types** then **New Type**.

Step 4 Add the two MIME types as shown in the following table. Use ".INI" and "." for the associated extension fields.

Table D-1 Mime Type Window Parameters

Associated Extension	Content Type (MIME)
.ini	text/plain
.	text/plain

Step 5 Apply the settings and close the IIS administration console.

Configuring the Web Server Directory Structure

Procedure

Step 1 Installing IIS creates the default directory C:\inetpub\WWWroot. Under this folder create the following directory structure.

C:\inetpub\wwwroot\cisco\wnos\

Step 2 Place the WTOS firmware and .INI files in the \WNOS directory.

Assigning the Client to the HTTPS Server

Use one of the following procedures to assign the WTOS thin computing device to the correct HTTPS server.

Assigning the Client to the HTTPS Server—Method 1

In this method, you manually enter the File Server and Path on the WTOS device.

Procedure

Step 1 Choose **Desktop> System Setup > Network > File Servers/Pat**.

Step 2 Enter the following information.

https://IPADDRESS/cisco

Assigning the Client to the HTTPS Server—Method 2

The second method uses DHCP option tags 161 and 162 to hand the WTOS thin computing device the File Server and Path information.

Set up 161 and 162 tags as described in the Configuring DHCP (DHCP Options), page A-9.

APPENDIX E

Cisco VXC 2112/2212 Power Considerations

You can power the Cisco VXC 2112/2212 using a Cisco PWR-CUBE-4 power adapter or using standard Power over Ethernet (PoE). This appendix describes the Cisco VXC configurations that are supported by the IEEE 802.3af and IEEE 802.3at PoE standards, by Cisco Universal Power Over Ethernet (UPOE), and by the Cisco PWR-CUBE-4 power adapter.

Cisco VXC 2112/2212 USB ports are compliant with USB 2.0 standard specifications to deliver a maximum power level of 2.5 watts.

Available Power on USB Ports

The USB ports on the Cisco VXC 2112/2212 operate at two power levels:

- Low: 0.5 watts
- High: 2.5 watts

USB ports that operate at the low-power level can only power USB devices that consume up to 0.5 watts of power, and USB ports that operate at the high-power level can power USB devices that consume up to 2.5 watts of power.

USB ports on the Cisco VXC 2112/2212 that operate at high power cannot individually power any noncompliant USB accessory that requires more than 2.5 watts of power. To power devices that require between 2.5 and 5 watts of power, you can use a USB Y cable to connect the accessory to USB port 3 and 4 of the client (when these are operating at high power).

In addition, if no device is connected to a port, the Cisco VXC 2112/2212 cannot reallocate the available power from this port to a device on another port. For example, if USB ports 1 and 2 are operating at low power and no device is connected to port 2, the Cisco VXC 2112/2212 cannot redirect the power allocated to port 2 to power a high-power device on port 1. In this case, the maximum power limit on port 1 remains unchanged at 0.5 watts.

Low-power USB devices (0.5 watts or less) are typically keyboards, mice, and joysticks, while high-power USB devices (greater than 0.5 watts) are typically bus-powered cameras, hubs, and some USB Flash drives.

USB Hub Support

USB ports on the Cisco VXC 2112/2212 can power a USB hub provided the hub does not draw more power than is available from the USB port to which it is connected (that is, 0.5 watts on low-power ports or 2.5 watts on high-power ports).

PoE Power Negotiation

The following sections describe the power negotiation process on the Cisco VXC 2112 and Cisco VXC 2212.

Cisco VXC 2112

When the Cisco VXC 2112 is powered using PoE, the firmware performs a one-time negotiation of PoE power requirements at boot time and allocates the available power to the USB ports, power indicators, and monitors, as described in Cisco VXC 2112 Power Support, page E-2. During normal operation, this power allocation does not change.

Cisco VXC 2212

Unlike the Cisco VXC 2112, the Cisco VXC 2212 dynamically negotiates the PoE power allocation from the PoE switch, and allocates the power to the attached devices when they are connected or disconnected. Regardless of the total power that the Cisco VXC 2212 draws, the maximum power available to each USB port is as described in Cisco VXC 2212 Power Support, page E-3.

Cisco VXC 2112 Power Support

Table E-1 describes the power configurations that are supported on the Cisco VXC 2112.

Note

- IEEE 802.3af PoE does not support Cisco VXC 2112 configurations.
- IEEE 802.3at PoE does not support the Cisco VXC 2112 if a Key Expansion Module is attached to a Cisco Unified IP Phone 8961, 9951, or 9971.

Table E-1 Cisco VXC 2112 Power Support

		USB				Monitor		
Cisco VXC 2112 with:	**Power Source**	**Port 1 keyboard**	**Port 2 mouse**	**Port 3 accessories**	**Port 4 accessories**	**DVI Port**	**VGA Port**	**Configuration**
8961	802.3at	Powered (low)	Powered (low)	Powered (low)	Powered (low)	Powered	Powered	Moderate
9951 without camera	802.3at	Powered (low)	Powered (low)	Powered (low)	Powered (low)	Powered	Powered	Moderate
9951 with camera	802.3at	Powered (low)	Powered (low)	Powered (low)	Powered (low)	Powered	Powered	Moderate
9971 without camera	802.3at	Powered (low)	Powered (low)	Powered (low)	Powered (low)	Powered	Powered	Moderate

Table E-1 Cisco VXC 2112 Power Support (continued)

Cisco VXC 2112 with:	Power Source	USB				Monitor		Configuration
		Port 1 keyboard	Port 2 mouse	Port 3 accessories	Port 4 accessories	DVI Port	VGA Port	
9971 with camera	802.3at	Powered (low)	Powered (low)	Unavailable	Unavailable	Powered	Powered	Basic
8961/9951/ 9971 with or without camera	UPOE	Powered (high)	Powered (high)	Powered (high)	Powered (high)	Powered	Powered	Full
	PWR-CUBE-4	Powered (high)	Powered (high)	Powered (high)	Powered (high)	Powered	Powered	Full

As an alternative to PoE, the Cisco PWR-CUBE-4 power adapter can support a Cisco VXC 2112 attached to a Cisco Unified IP Phone 8961, 9951, or 9971 (with or without camera) with up to three Key Expansion Modules in a basic configuration (keyboard, mouse, and two monitors).

If you add one or more Key Expansion Modules to the Cisco Unified IP Phone 8961, 9951, or 9971, these modules may reduce the amount of power available to the Cisco VXC client and may cause additional restrictions for powering Cisco VXC peripheral devices.

Cisco VXC 2212 Power Support

Table E-2 describes the power configurations that are supported on the Cisco VXC 2212.

Note

- The Unified IP Phone PC port can provide the network connectivity for the Cisco VXC 2212; however, it does not provide power for the device. A power adapter is required when you use the Unified IP Phone PC port for network connectivity for the Cisco VXC 2212.
- 802.af PoE can support a Cisco VXC 2212 only in a basic configuration.

Table E-2 Cisco VXC 2212 Power Support

	Power Source	USB				Monitor		Configuration
		Port 1 keyboard	Port 2 mouse	Port 3 accessories	Port 4 accessories	DVI Port	VGA Port	
Cisco VXC 2212	802.3af	Powered (low)	Powered (low)	Unavailable	Unavailable	Powered	Powered	Basic
	802.3at	Powered (high)	Powered (high)	Powered (high)	Powered (high)	Powered	Powered	Full
	UPOE	Powered (high)	Powered (high)	Powered (high)	Powered (high)	Powered	Powered	Full
	PWR-CUBE-4	Powered (high)	Powered (high)	Powered (high)	Powered (high)	Powered	Powered	Full

Cisco VXC 2212 Base LED Behavior

Table E-3 describes the behavior of the base LEDs when you connect power (PoE or Cisco Power Cube 4) to the Cisco VXC 2212.

Table E-3 Cisco VXC 2212 Base LED Behavior

Power source	Client connected to power source (PoE or Power cube)	Press power button for power-on (quick button press - no more than 1/2 second)	Press Power button again for power-off (hold minimum 3 seconds)
IEEE 802.3af PoE	No light	Dim white light	Light turns off
IEEE 802.3at PoE	No light	Dim white light	Light turns off
Cisco UPOE	No light	Dim white light	Light turns off
Cisco Power Cube 4 (plugged in AFTER network cable)	Initial white light flash, then light turns off	Dim white light, which becomes a bright white light after approximately 10 seconds	Light turns off
Cisco Power Cube 4 (plugged in BEFORE network cable)	No light	Dim white light, which becomes a bright white light after approximately 10 seconds	Light turns off

Power Consumption

Table E-4 describes the power consumption on the Cisco VXC 2112/2212.

Table E-4 Power Consumption

Thin Client	Minimum Power Consumption	Maximum Power Consumption
Cisco VXC 2112	12 watts[1]	24 watts[1]
Cisco VXC 2212	12 watts	24 watts

1. The values listed indicate the power consumption for the thin client only. When the Cisco VXC 2112 is attached to a Cisco Unified IP Phone, you must add the phone power consumption to calculate the total power consumption of the system.