HP ThinPro 5.1

Administrator Guide

First Edition: November 2014

Document Part Number: 800032-001

Open source software

This product includes software licensed under an open source software license, such as the GNU General Public License and the GNU Lesser General Public License or other open source license. To the extent HP has an obligation or, in its sole discretion, chooses to make the source code for such software available under the applicable open source software license, source code for the software may be obtained from the ftp: ftp://ftp.hp.com/pub/tcdebian/pool/thinpro51/source/.

About this guide

This guide uses the following styles to distinguish elements of text:

Style	Definition
`<variable>`	Variables or placeholders are enclosed in angle brackets. For example, replace `<pathname>` with the appropriate path, such as `C:\Windows\System`. When typing the actual value for the variable, omit the brackets.
`[optional parameters]`	Optional parameters are enclosed in square brackets. When specifying the parameters, omit the brackets.
`"literal value"`	Command line text that appears inside quotation marks should be typed exactly as shown, including the quotation marks.

Table of contents

1 Welcome 1
Finding more resources 1
Comparison of ThinPro and Smart Zero 1
Document organization 2

2 Getting started 3
Choosing a management service 3
Starting HP ThinPro for the first time 3

3 Navigating the interface 5
Using the taskbar 5
Using the Connection Manager controls 6
Viewing system information 7
Hiding the system information screens 7

4 Control Panel configurations 8
Control Panel overview 9
Client aggregation 12
Configuring client aggregation 13
Configuring the aggregation clients 13
Configuring the aggregation server 14
Display preferences 14
Configuring printers 14
Redirecting USB devices 15
Network settings 15
Wired network settings 16
Wireless network settings 16
DNS settings 17
IPSec rules 18
Configuring VPN settings 18
Configuring HP Velocity 18
Customization Center 18
HP ThinState 19
Managing an HP ThinPro image 19
Capturing an HP ThinPro image to an FTP server 19
Deploying an HP ThinPro image using FTP or HTTP 20

Capturing an HP ThinPro image to a USB flash drive 20
Deploying an HP ThinPro image with a USB flash drive 21
Managing an HP ThinPro profile 21
Saving an HP ThinPro profile to an FTP server 21
Restoring an HP ThinPro profile using FTP or HTTP 21
Saving an HP ThinPro profile to a USB flash drive 22
Restoring an HP ThinPro profile from a USB flash drive 22
VNC Shadowing 22
Certificates 23
Certificate Manager 23
SCEP Manager 23
DHCP options 24

5 Common connection configurations 25
Common connection settings 25
Kiosk Mode 26

6 Citrix connections 27
Citrix connection management features 27
Citrix Receiver features 27
HDX MediaStream 28
Citrix connection support matrix 29
Citrix general settings 29
Citrix connection-specific settings 32

7 RDP connections 34
RDP features 34
RDP general settings 34
RDP connection-specific settings 34
Using RemoteFX with RDP 37
Using multi-monitor sessions with RDP 38
Using multimedia redirection with RDP 38
Using device redirection with RDP 39
Using USB redirection with RDP 39
Using mass storage redirection with RDP 39
Using printer redirection with RDP 40
Using audio redirection with RDP 40
Using smart card redirection with RDP 41

8 VMware Horizon View connections 42
VMware Horizon View settings 42
Using multi-monitor sessions with VMware Horizon View 45
Using keyboard shortcuts with VMware Horizon View 45
Using Multimedia Redirection with VMware Horizon View 45
Using device redirection with VMware Horizon View 46
Using USB redirection with VMware Horizon View 46
Using mass storage redirection with VMware Horizon View 46
Using printer redirection with VMware Horizon View 46
Using audio redirection with VMware Horizon View 46
Using smart card redirection with VMware Horizon View 47
Using webcam redirection with VMware Horizon View 47
Changing the VMware Horizon View protocol type 47
VMware Horizon View HTTPS and certificate management requirements 48

9 Web Browser connections 50
Web Browser general settings 50
Web Browser connection-specific settings 50

10 Additional connection types (ThinPro configuration only) 51
TeemTalk connection settings 51
XDMCP connection settings 53
SSH connection settings 53
Telnet connection settings 55
Custom connection settings 55

11 HP Smart Client Services 56
Supported operating systems 56
Prerequisites for HP Smart Client Services 56
Obtaining HP Smart Client Services 57
Viewing the Automatic Update website 57
Creating an Automatic Update profile 57
Updating clients 57
Using the broadcast update method 57
Using the DHCP tag update method 58
Example of performing DHCP tagging 58
Using the DNS alias update method 58
Using the manual update method 59
Performing a manual update 59

12 Using the Profile Editor 60
Accessing the Profile Editor 60
Loading a client profile 60
Modifying a client profile 60
Selecting the platform of a client profile 61
Selecting the connection type of a client profile 61
Modifying the registry settings of a client profile 61
Enabling or disabling menu items on clients 61
Enabling or disabling user configurations on clients 62
Adding files to a client profile 62
Adding a configuration file to a client profile 62
Adding certificates to a client profile 62
Adding a symbolic link to a client profile 63
Saving the client profile 63
Configuring a serial or parallel printer 63
Obtaining the printer settings 64
Setting up printer ports 64
Installing printers on the server 64

13 Troubleshooting 66
Troubleshooting network connectivity 66
Troubleshooting firmware corruption 66
Reimaging client device firmware 67
Troubleshooting Citrix password expiration 67
Using system diagnostics to troubleshoot 67
Saving system diagnostic data 67
Uncompressing the system diagnostic files 67
Uncompressing the system diagnostic files on Windows-based systems 67
Uncompressing the system diagnostic files in Linux- or Unix-based systems . . 68
Viewing the system diagnostic files 68
Viewing files in the Commands folder 68
Viewing files in the /var/log folder 68
Viewing files in the /etc folder 68

Appendix A USB updates 69

Appendix B BIOS tools 70
BIOS settings tool 70
BIOS flashing tool 70

Appendix C Resizing the flash drive partition 71

Appendix D Customizing the Smart Zero login screen 72

Customizing the screen background 72

Common attributes 72

Elements 74

Image 76

Text 77

Appendix E Registry keys 80

root > Audio 81

root > CertMgr 81

root > ConnectionManager 82

root > ConnectionType 82

root > ConnectionType > custom 82

root > ConnectionType > firefox 85

root > ConnectionType > freerdp 89

root > ConnectionType > ssh 96

root > ConnectionType > teemtalk 101

root > ConnectionType > telnet 103

root > ConnectionType > view 107

root > ConnectionType > xdmcp 114

root > ConnectionType > xen 118

root > DHCP 128

root > Dashboard 128

root > Display 129

root > Network 131

root > SCIM 135

root > Serial 136

root > SystemInfo 136

root > TaskMgr 136

root > USB 137

root > auto-update 137

root > background 139

root > config-wizard 140

root > desktop 140

root > entries 140

root > keyboard 141

root > logging 142

root > mouse 142

root > screensaver 142
root > security 143
root > sshd 143
root > time 143
root > touchscreen 144
root > translation 145
root > usb-update 145
root > users 145
root > vncserver 148

Index 150

1 Welcome

This guide is intended for administrators of HP thin client models that are based on the HP ThinPro operating system. It is assumed that you are using the latest image provided by HP and that you log on as an administrator when making configurations or accessing administration utilities.

Finding more resources

Resource	Contents
HP support website http://www.hp.com/support	Image updates and add-ons Documentation for HP software not covered in detail in this guide **TIP:** If your search results cannot locate the software you are looking for, search for the thin client model instead.
Microsoft support website http://support.microsoft.com	Documentation for Microsoft software not covered in detail in this guide
Citrix support website http://www.citrix.com/support	Documentation for Citrix software not covered in detail in this guide
VMware support website http://www.vmware.com/support	Documentation for VMware software not covered in detail in this guide

Comparison of ThinPro and Smart Zero

Beginning with HP ThinPro 5.0, ThinPro and Smart Zero are two different configurations of the same operating system image. You can easily switch between the two configurations using an option in the Control Panel. See the following table for a comparison of ThinPro and Smart Zero.

	ThinPro	Smart Zero
Default available connection types **NOTE:** You can change which connection types are available using the registry key `priorityInConnectionLists` for each connection type. See root > ConnectionType on page 82 for more information.	• Citrix • RDP • VMware Horizon View • Web Browser (Firefox) • TeemTalk • XDMCP • SSH • Telnet • Custom	• Citrix • RDP • VMware Horizon View • Web Browser (Firefox)
Number of connections supported at a time	Multiple	One
Kiosk Mode default setting	Disabled	Enabled

Document organization

This guide is divided into the following chapters and appendixes:

- Getting started on page 3—Describes the basic steps to deploy a thin client running HP ThinPro.
- Navigating the interface on page 5—Provides an overview of the different components of the interface.
- Control Panel configurations on page 8—Describes the connection-related settings and configurations in the Control Panel and details some of the more advanced configurations.
- Common connection configurations on page 25—Describes settings that are common to all connection types and configuring a client for Kiosk Mode.
- Citrix connections on page 27—Describes the settings and configurations for the Citrix connection type.
- RDP connections on page 34—Describes the settings and configurations for the RDP connection type.
- VMware Horizon View connections on page 42—Describes the settings and configurations for the VMware Horizon View connection type.
- Web Browser connections on page 50—Describes the settings for the Web Browser connection type.
- Additional connection types (ThinPro configuration only) on page 51—Describes the settings for the TeemTalk, XDMCP, SSH, Telnet, and Custom connection types.
- HP Smart Client Services on page 56—Describes how to use HP Smart Client Services to remotely manage large numbers of thin clients using Automatic Update.
- Using the Profile Editor on page 60—Describes using the Profile Editor to set up and edit client profiles, which contain connection information, settings, and files used in the self-configuration process.
- Troubleshooting on page 66—Describes common troubleshooting issues and solutions.
- USB updates on page 69—Describes how to install add-ons and profile updates from a USB flash drive.
- BIOS tools on page 70—Describes how to view and update BIOS settings and flash a new BIOS version.
- Resizing the flash drive partition on page 71—Describes how to increase the size of the flash drive partition.
- Customizing the Smart Zero login screen on page 72—Describes the common attributes and elements used in customizing the client login screen background.
- Registry keys on page 80—Lists the paths, functions, and options for the HP ThinPro registry keys.

2 Getting started

Choosing a management service

Thin clients running HP ThinPro can be managed by either HP Smart Client Services or HP Device Manager (HPDM). You can use whichever management service is best for your deployment.

HP Smart Client Services is optimized for use with Smart Zero. This option allows for zero management.

HPDM is ideal for large environments that contain thin clients with a variety of different operating systems. This option provides more visibility to thin clients and a greater variety of management options.

Starting HP ThinPro for the first time

When you first turn on a new thin client running HP ThinPro, a setup utility runs.

First, the setup utility checks for a network connection. If specific network settings are required, click the **Network Settings** button to open the Network Manager (see Network settings on page 15 for more information).

The setup utility then checks to see if the thin client is being managed by either HP Smart Client Services or HP Device Manager (HPDM). If the thin client is being managed by either program, the setup utility exits and the management program performs predefined configurations to the thin client.

NOTE: For more information about HP Smart Client Services, see HP Smart Client Services on page 56. For more information about HPDM, go to http://www.hp.com/go/hpdm.

If the thin client is not being managed by either HP Smart Client Services or HPDM, the utility checks whether there is an image update available from HP. If there is, click **Install now** on the **Software Update** tab to update the image.

TIP: If you want to maintain your own internal site for image updates, you can customize where the operating system looks for updates by changing the following registry key:

`root/config-wizard/FirmwareUpdate/firmwareUpdateURL`

If you want to verify whether service packs or package updates are available, click **Easy Update** to launch HP Easy Tools.

If you need to manually configure the HPDM Agent or the Automatic Update settings for HP Smart Client Services, click the **Device Management** tab of the setup utility and choose the appropriate option.

TIP: If you want to check for software updates every time the thin client starts up, enable the **Check for software updates every boot** option.

If you want to preserve your thin client configuration when you upgrade your image version, enable the **Preserve Thin Client Configuration** option.

After you close the setup utility, if no connections are configured, you are prompted to configure a connection.

NOTE: This initial connection wizard offers a quicker setup process than the standard Connection Manager wizard.

If you plan to configure a single thin client and then copy and deploy its configurations to other thin clients using HP ThinState (see HP ThinState on page 19), use the Control Panel to make all of the desired configurations first. See Navigating the interface on page 5 and Control Panel configurations on page 8 for more information.

3 Navigating the interface

This chapter discusses the following topics:

- Using the taskbar
- Using the Connection Manager controls
- Viewing system information

Using the taskbar

Table 3-1 Taskbar components

1	**Connection Manager**—Use to start, stop, add, edit, and delete remote connections. See Using the Connection Manager controls on page 6 for more information.
2	**Control Panel**—Use to configure the client, switch between Administrator Mode and User Mode, and check for software updates. See Control Panel overview on page 9 for more information.
3	**System Information**—Use to view system, network, and software information about the client. See Viewing system information on page 7 for more information.
4	**Application area**—Displays the icons for the currently open applications. **TIP:** You can hold down Ctrl+Alt and then press Tab repeatedly to select an application to bring to the foreground.
5	**System tray**—Provides quick access to or provides information about certain utilities, applications, and functions. Items in the system tray can include the following, but some items might not appear depending on the system configuration: • Audio mixer • Virtual keyboard • Network status • Automatic Update status—A green icon with a checkmark indicates that Automatic Update finished successfully. A yellow icon with an exclamation point indicates that the Automatic Update server was not found or that there are some problems with the server-side settings. A red icon with an X indicates that Automatic Update failed, such as when a package or profile is invalid. A blue icon with a spinning arrow indicates that Automatic Update is currently checking for updates. • Smart Common Input Method (SCIM) controls • Citrix applications
6	**Date and time**—Displays the current date and time. Click to access the date and time settings.
7	**Power button**—Use to log out of, reboot, or power off the client.

Using the Connection Manager controls

1	**Start**—Starts the selected connection.
2	**Stop**—Stops the selected connection.
3	**Edit**—Opens a Connection Manager specific to the selected connection type (such as the Citrix Connection Manager), allowing you to edit settings that are specific to the selected connection only.
4	**Delete**—Deletes the selected connection.
5	**Add**—Allows you to add a new connection. **NOTE:** See Comparison of ThinPro and Smart Zero on page 1 for a list of the available connection types.
6	**Settings**—Allows you to edit general settings for Citrix, RDP, or Web Browser connections. These settings apply to all connections of that type.

For more information about configuring connections, see the following:

- Common connection configurations on page 25
- Citrix connections on page 27
- RDP connections on page 34
- VMware Horizon View connections on page 42
- Web Browser connections on page 50
- Additional connection types (ThinPro configuration only) on page 51

Viewing system information

Click the **System Information** button on the taskbar to view system, network, and software information about the client. The following table describes the information that is displayed on each tab.

Table 3-2 System Information tabs

Tab	Description
General	Displays information about the BIOS, operating system, CPU, and memory.
Network	Displays information about the network interface, gateway, and DNS settings.
Net Tools	Provides the following tools for monitoring and troubleshooting purposes: • **Ping**—Specify an IP address of another device on the network to attempt to establish contact. • **DNS Lookup**—Use this tool to resolve a domain name into an IP address. • **Trace Route**—Use this tool to track the path that a network packet takes from one device to another.
Software Information	Displays a list of installed add-ons on the **Service Packs** tab and software version information on the **Software Installed** tab. **TIP:** You can also access the Administrator Guide (this document) from this screen.
System Logs	Displays the following logs: • Network Manager • Smart Zero Client Service • DHCP Wired Leases • DHCP Wireless Leases • Kernel • X Server • Connection Manager Check **Enable Debug Mode** to display additional information that might be requested by HP support for troubleshooting purposes. Click **Diagnostic** to save a diagnostic file. For more information, see Using system diagnostics to troubleshoot on page 67.

Hiding the system information screens

See root > SystemInfo on page 136 for information about registry keys that can be used to hide the System Information screens.

4 Control Panel configurations

This chapter includes the topics as follows:

- Control Panel overview
- Client aggregation
- Display preferences
- Configuring printers
- Redirecting USB devices
- Network settings
- Customization Center
- HP ThinState
- VNC Shadowing
- Certificates
- DHCP options

Control Panel overview

The Control Panel provides access to utilities for configuring the client. All of the utilities are accessible in Administrator Mode. When in User Mode, only the utilities that are enabled by the administrator for use by users are accessible.

To switch between Administrator Mode and User Mode:

▲ Select **Administrator/User Mode Switch** in the Control Panel.

The first time you switch to Administrator Mode, you will be prompted to set up an administrator password. The administrator password must be entered to switch to Administrator Mode every subsequent time.

TIP: When in Administrator Mode, the screen is surrounded by a red border.

The following tables describe the Control Panel utilities available in each of the menu categories.

TIP: To specify which utilities standard users have access to, select **Setup > Customization Center** in the Control Panel and select or deselect utilities in the **Applications** list.

Table 4-1 Control Panel > Peripherals

Menu option	Description
Client Aggregation	Lets you configure client aggregation settings, allowing you to combine thin clients to create additional screen real estate. For more information, see Client aggregation on page 12.
Display Preferences	Lets you configure and test options for both a primary and secondary display. For more information, see Display preferences on page 14.
Keyboard Layout	Lets you change the keyboard layout to accommodate the language used by the keyboard.
Sound	Lets you control the playback and input audio levels.
Mouse	Lets you configure the mouse speed and whether mouse input is right-handed or left-handed.
Printers	Lets you set up local and network printers. Local printers can be shared across the network. For more information, see Configuring printers on page 14.
Touch Screen	Lets you configure touch screen options.
USB Manager	Lets you configure the redirection options for USB devices. For more information, see Redirecting USB devices on page 15.
SCIM Input Method Setup	Allows you to configure the Smart Common Input Method (SCIM) for Chinese, Japanese, and Korean input. For more information on this open source program, go to http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page.

Table 4-2 Control Panel > Setup

Menu option	Description
Background Manager	Lets you configure the background theme.
Date and Time	Lets you configure the time zone and the date and time options.
Language	Lets you display the client interface in a different language.
Network	Lets you configure network settings. For more information, see Network settings on page 15.
Screensaver	Lets you configure a screensaver.
Security	Lets you set up or change system passwords for the client administrator and user.
Customization Center	Lets you do the following: • Switch between the ThinPro and Smart Zero configurations • Configure desktop and taskbar options • Select which connection types and control panel utilities standard users have access to For more information, see Customization Center on page 18.

Table 4-3 Control Panel > Management

Menu option	Description
AD/DDNS Manager	Lets you add the client to an organizational unit of the Active Directory server and enable automatic Dynamic DNS updates of the client's name and IP address association. **NOTE:** This utility does not enable authentication against the Active Directory database.
HPDM Agent	Lets you configure the HP Device Manager (HPDM) Agent. For more information about HP Device Manager, see the *HP Device Manager Administrator Guide*.
Automatic Update	Lets you configure the Automatic Update server manually. For more information, see HP Smart Client Services on page 56.
Easy Update	Opens the Easy Update wizard. Easy Update is a component of HP Easy Tools that lets you install the latest software updates for the client. **TIP:** Selecting **Preserve Thin Client Configuration** when performing an image update preserves all previously configured settings. For more information about HP Easy Tools, see the *HP Easy Tools Administrator Guide*.
Snapshots	Lets you restore the client to a previous state or to its default factory configuration.

Table 4-3 Control Panel > Management (continued)

Menu option	Description
SSHD Manager	Enables access through a secure shell.
ThinState	HP ThinState lets you make a copy of or restore the entire operating system image or just its configuration settings. For more information, see HP ThinState on page 19.
VNC Shadow	Lets you configure VNC Shadowing options. For more information, see VNC Shadowing on page 22.

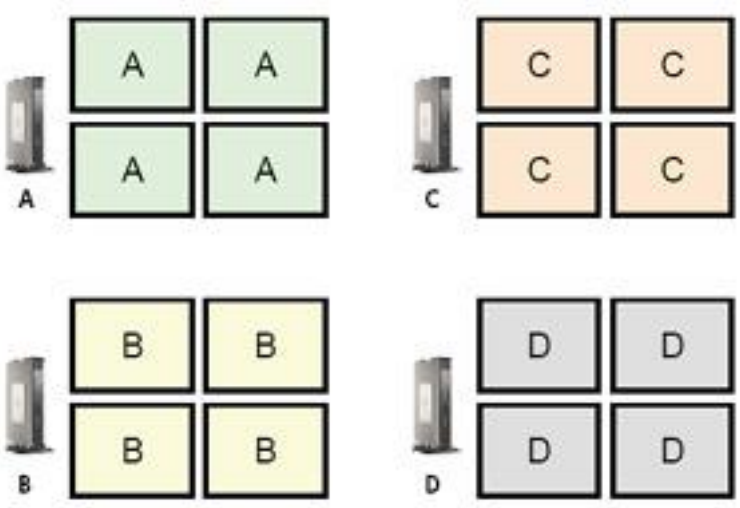
Table 4-4 Control Panel > Advanced

Menu option	Description
Certificates	Opens the Certificate Manager, which lets you easily import, view, or remove certificates. For more information, see Certificate Manager on page 23.
CPU Manager	Lets you choose between **Balanced** and **High Performance** CPU performance.
DHCP Options	Lets you configure DHCP options. For more information, see DHCP options on page 24.
SCEP Manager	Allows for network-based certificate management.
Serial Manager	Lets you configure serial devices.
Keyboard Shortcuts	Lets you create, modify, and delete keyboard shortcuts.
Task Manager	Lets you monitor the CPU usage and the CPU usage history for the client.
Text Editor	Opens a basic text editor for viewing and editing text files.
X Terminal	Lets you execute Linux commands.

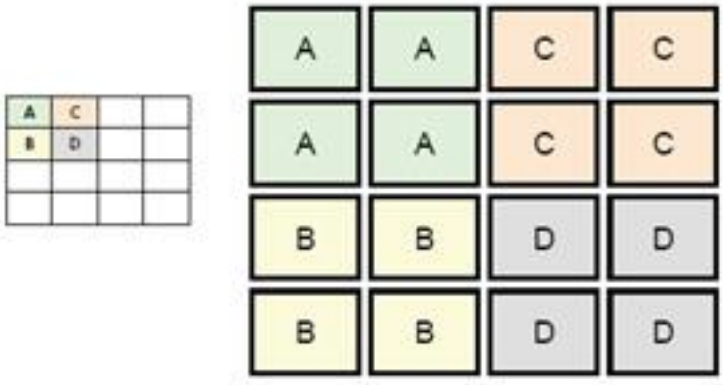
Client aggregation

Clients running HP ThinPro support up to four monitors, depending on the hardware model. If you need additional screen real estate, client aggregation allows up to four clients to be combined together making it possible to have a total of 16 monitors controlled by a single keyboard and mouse, without the need for additional hardware or software.

Assume that you have four clients, each with four monitors configured as a 2x2 array as shown below.

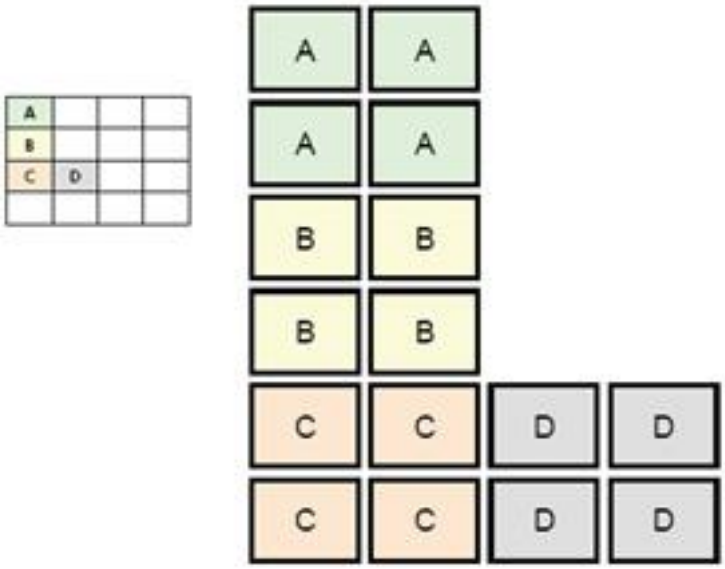


Client aggregation allows you to arrange the four clients on a 4x4 grid. The following illustration shows one possible arrangement.



When moving the mouse pointer off the right side of the thin client A monitors, for example, the pointer will appear on the left side of the thin client C monitors. Likewise, keyboard input will be redirected from thin client A to thin client C.

The following illustration shows another possible arrangement.



In this configuration, moving the mouse pointer off the right side of the thin client A monitors will cause it to appear on the upper 1/3 of the left side of the thin client D monitors. Similarly, moving the mouse pointer off the right side of the thin client B monitors will cause it to appear in the middle 1/3 of the left side of the thin client D monitors. Finally, moving the mouse pointer off the right side of the thin client C monitors will cause it to appear in the lower 1/3 of the left side of the thin client D monitors.

NOTE: Desktop windows cannot span or be moved between clients. Typically, each client will create windows based on its connection to an associated remote computer, and there won't be a need to move windows between clients.

The client physically connected to the keyboard and mouse is referred to as the aggregation server. The other clients are referred to as aggregation clients. When the mouse pointer is on one of the aggregation clients, the mouse and keyboard inputs (from the aggregation server) are encrypted and sent over the network to that aggregation client. The aggregation client decrypts the mouse and keyboard inputs and passes the inputs to the local desktop of the aggregation client.

Client aggregation is based on an open source software package called Synergy, with encryption provided by a package called stunnel.

Configuring client aggregation

Client aggregation configuration is a two-step process:

1. Configuring the aggregation clients on page 13
2. Configuring the aggregation server on page 14

Configuring the aggregation clients

Perform this procedure on each aggregation client:

1. Select **Peripherals > Client Aggregation** in the Control Panel.
2. Click **Client**.
3. Type the server hostname or IP address of the aggregation server in the field.
4. Click **Apply**.

Configuring the aggregation server

To configure the aggregation server:

1. Select **Peripherals > Client Aggregation** in the Control Panel.
2. Click **Server**.
3. The aggregation server is displayed in a blue box that contains its hostname. Click and drag the aggregation server to the desired location in the 4x4 grid.
4. Click the location in the 4x4 grid where you want to place the first aggregation client, type its hostname or IP address, and then press Enter. The aggregation client is displayed in a green box.
5. Add up to two additional aggregation clients in the 4x4 grid, if desired.

   Placement of the aggregation server and the aggregation clients in the 4x4 grid can be modified at any time by clicking and dragging a client computer to a new location.

Once the aggregation clients and the aggregation server have been configured, they automatically attempt to establish encrypted communications with each other. Click **Status** to view the connection status between computers.

Display preferences

HP ThinPro allows you to create profiles for display preferences and apply different profiles to different monitors. A profile includes resolution, refresh rate, bit depth, and orientation.

To configure display profiles:

1. Select **Peripherals > Display Preferences** in the Control Panel.
2. Configure the options as necessary, and then click **Apply**.

NOTE: The options may differ depending on the hardware model.

See the following tips about when customizing display profiles would be useful:

- Some applications might require a specific resolution or bit depth to function properly.
- Some applications might require the display to be rotated.
- Using a 16-bit color depth should improve Citrix and RDP connection performance because less data has to be transmitted over the network or sent to the graphics chip.
- AMD-based platforms (t520, t610, t620) offer only 32-bit color depth. The t505 and t510 offer either 16-bit or 32-bit color depth. In all cases, 32-bit color depth actually uses 24 bits.
- An administrator might want to standardize on one display profile, even though there are many different monitors across the organization.

Configuring printers

To configure a printer:

1. Select **Peripherals > Printers** in the Control Panel.
2. In the **Printing** dialog, click **Add** .
3. In the **New Printer** dialog, select the printer to configure, and then click **Forward**.

NOTE: If you select a serial printer, be sure to input the correct settings on the right side of the dialog, or the printer might not function correctly.

4. Select the make of the printer. If you are unsure, select the **Generic (recommended)** option, and then click **Forward**.
5. Select the model of and driver for the printer, and then click **Forward**.

NOTE: If you are unsure of the printer model or which driver to use, or if the model of your printer is not listed, click **Back** and try using the **Generic (recommended)** option for the make of the printer.

If using the **Generic (recommended)** make, be sure to select **text-only (recommended)** for the model and **Generic text-only printer [en] (recommended)** for the driver.

6. Fill in optional information about the printer, such as its name and location.

NOTE: HP recommends that you enter in the correct driver name into the **Windows Driver** box. Without a driver to map to when connecting to a remote session, Windows might not use the correct driver and printing might not work. The driver must also be installed on the Windows server for the printer to work properly.

7. Click **Apply**, and then print a test page if desired.

Repeat this process to configure additional printers if necessary.

TIP: The most common problem is that the wrong driver is being used for the printer. To change the driver, right-click the printer and select **Properties**, and then change the make and model.

Redirecting USB devices

To redirect USB devices:

1. Select **Peripherals > USB Manager** in the Control Panel.
2. On the **Protocol** page, select a remote protocol.

   If the setting is **Local**, you can also specify the options **allow devices to be mounted** and **mount devices read-only**.
3. On the **Devices** page, you can change the redirection options for individual devices if necessary. To do this, click the box to the left of the device name to switch between the following redirection options:
   - **Use Defaults**
   - **Redirect**
   - **Do Not Redirect**
4. When finished, click **OK**.

Network settings

Network settings can be configured using the Network Manager. To open the Network Manager:

▲ Select **Setup > Network** in the Control Panel.

See the following sections for more information about the different tabs in the Network Manager:

- Wired network settings

- Wireless network settings
- DNS settings
- IPSec rules
- Configuring VPN settings
- Configuring HP Velocity

Wired network settings

The following table describes the options available in the **Wired** tab of the Network Manager.

Option	Description
Enable IPv6	Enables IPv6. IPv4 is used by default, and they cannot be used at the same time.
Ethernet Speed	Lets you set the Ethernet Speed. If your switch or hub does not have a special requirement, leave this at the default setting of **Automatic**.
Connection Method	Lets you choose between **Automatic** and **Static**. If your network environment is using DHCP, then the **Automatic** option should work without any further configurations needed. If **Static** is selected, the **Static Address Configuration** settings will become available. Be sure to input these values according to whether you are using IPv4 or IPv6.
MTU	Allows you to enter the maximum transmission unit (in bytes).
Security Settings	Lets you set the authentication setting to one of the following: • None • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS Note the following about TTLS and PEAP: • The **Inner Authentication** option should be set to whatever your server supports. • The **CA Certificate** setting should point to the server's certificate on the local client. • The **Username** and **Password** are the user's credentials. Note the following about TLS: • The **CA Certificate** setting should point to the server's certificate on the local client. • If your **Private Key** file is .p12 or .pfx, then the **User Certificate** setting can be left blank. • The **Identity** setting should be the username that corresponds to the user certificate. • The **Private Key Password** setting is the password of the user's private key file.

Wireless network settings

The following table describes the options available in the **Wireless** tab of the Network Manager.

NOTE: This tab is available only if the client has a wireless adapter.

Option	Description
Scan AP	Scans for available wireless networks.

Option	Description
SSID	Use this box to manually enter the SSID of the wireless network if it is not found by the scan.
SSID Hidden	Enable this option if the SSID of the wireless network is set to be hidden (not broadcasting).
Enable IPv6	Enables IPv6. IPv4 is used by default, and they cannot be used at the same time.
Enable Power Management	Enables the power management feature for the wireless adapter.
Connection Method	Lets you select between **Automatic** and **Static**. If your network environment is using DHCP, then the **Automatic** option should work without any further configurations. If **Static** is selected, the **Static Address Configuration** settings will become available. Be sure to input these values according to whether you are using IPv4 or IPv6.
Security Settings	Lets you set the authentication setting to one of the following: • None • WEP • WPA/WPA2-PSK • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS • EAP FAST For WEP and WPA/WPA2-PSK, you just need to enter the network key and click **OK**. For EAP-FAST, set **Anonymous Identity**, **Username**, **Password**, and **Provisioning Method**. You do not need to change the PAC file settings. See Wired network settings on page 16 for more information about TTLS, PEAP, and TLS.

DNS settings

The following table describes the options available in the **DNS** tab of the Network Manager.

Option	Description
Hostname	This is generated automatically according to the MAC address of the thin client. You can alternatively set a custom hostname.
DNS Servers	Use this box to set custom DNS server information.
Search Domains	Use this box to restrict the domains that are searched.
HTTP Proxy FTP Proxy HTTPs Proxy	Use these boxes to set proxy server information using the following format: `http://<ProxyServer>:<Port>` HP recommends using the `http://` prefix for all three proxy settings because it is supported better. **NOTE:** The proxy settings are set to the **http_proxy**, **ftp_proxy**, and **https_proxy** environmental variables for the system.

IPSec rules

Use this tab to add, edit, and delete IPSec rules. An IPSec rule should be the same for each system that uses IPSec to communicate.

When configuring an IPSec rule, use the **General** tab to set the rule's information, addresses, and authentication method. The **Source Address** is the IP address of the thin client, and the Destination Address is the IP address of the system that the client is going to communicate with.

NOTE: Only the **PSK** and **Certificate** authentication types are supported. Kerberos authentication is not supported.

Use the **Tunnel** tab to configure settings for tunnel mode.

Use the **Phase I** and **Phase II** tabs to configure advanced security settings. The settings should be the same for all peer systems that communicate with each other.

NOTE: An IPSec rule can also be used to communicate with a computer running Windows.

Configuring VPN settings

HP ThinPro supports two types of VPN:

- Cisco
- PPTP

Enable the **Auto Start** option to start the VPN automatically.

Note the following about creating a VPN using Cisco:

- The **Gateway** is the gateway's IP address or hostname.
- The **Group name** and **Group password** are the IPSec ID and IPSec password.
- The **Domain** setting is optional.
- The **User name** and **User password** are the user credentials that have rights to create a VPN connection on the server side.
- The **Security Type** should be set the same as it is on the server side.

Note the following about creating a VPN using PPTP:

- The **Gateway** is the gateway's IP address or hostname.
- The **NT Domain** setting is optional.
- The **User name** and **User password** are the user credentials that have rights to create a VPN connection on the server side.

Configuring HP Velocity

Use the **HP Velocity** tab to configure HP Velocity settings. Go to http://www.hp.com/go/velocity for more information about the HP Velocity modes.

Customization Center

To open the Customization Center:

▲ Select **Setup > Customization Center** in the Control Panel.

The button at the top of the **Desktop** page can be used to switch between the ThinPro and Smart Zero configurations. See Comparison of ThinPro and Smart Zero on page 1 for more information about the differences between the two configurations.

NOTE: When switching from ThinPro to Smart Zero, if you have configured a single connection, that connection is used automatically as the Smart Zero connection. If you have configured multiple connections, you are prompted to select the connection to use.

The following table describes the rest of the options available on the **Desktop** page.

Option	Description
Launch the Connection Manager at start up	When enabled, the Connection Manager launches automatically at system startup.
Enable/disable right click	Disable this option to disable the context menu that appears when you right-click the desktop
Allow user to switch to admin mode	Disable this option to remove the **Administrator/User Mode Switch** option from the Control Panel in User Mode.
Enable X host access control security	When enabled, only the systems listed in the **XHost Access Control List** area are allowed to remotely control the thin client.
Enable USB Update	Enables updates to be installed from a USB flash drive. See USB updates on page 69 for more information.
Authenticate USB Update	Disable this option to allow standard users to install updates via USB.

Use the **Connections** and **Applications** pages to select which connection types and Control Panel applications are available in User Mode.

Use the **Taskbar** page to configure the taskbar.

HP ThinState

HP ThinState allows you to capture and deploy an HP ThinPro image or configuration (profile) to another client of compatible model and hardware.

Managing an HP ThinPro image

Capturing an HP ThinPro image to an FTP server

To capture an HP ThinPro image to an FTP server:

IMPORTANT: The directory on the FTP server where you intend to save the captured image must already exist before initiating the capture.

1. Select **Management > ThinState** in the Control Panel.
2. Select **the HP ThinPro image**, and then click **Next**.
3. Select **make a copy of the HP ThinPro image**, and then click **Next**.
4. Select **a FTP server**, and then click **Next**.
5. Enter the FTP server information in the fields.

NOTE: The name of the image file is set by default to be the client's hostname.

Select **Compress the image** if you want to compress the captured image.

NOTE: The HP ThinPro image file is a simple disk dump. The uncompressed size is about 1 GB, and a compressed image without add-ons is approximately 500 MB.

6. Click **Finish**.

   When the image capture begins, all applications stop and a new window appears showing the progress. If a problem occurs, click **Details** for information. The desktop reappears after the capture is complete.

Deploying an HP ThinPro image using FTP or HTTP

IMPORTANT: If you abort a deployment, the previous image will not be restored and the contents of the client's flash drive will be corrupted.

To deploy an HP ThinPro image using FTP or HTTP:

1. Select **Management > ThinState** in the Control Panel.
2. Select **the HP ThinPro image**, and then click **Next**.
3. Select **restore an HP ThinPro image**, and then click **Next**.
4. Select either the FTP or HTTP protocol, and then enter the server information in the fields.

   NOTE: The **Username** and **Password** fields are not required if you are using the HTTP protocol.

5. Select **Retain HP ThinPro Configuration** if you want to preserve all previously configured settings.
6. Click **Finish**.

   When the image deployment begins, all applications stop and a new window appears showing the progress. If a problem occurs, click **Details** for information. The desktop reappears after the deployment is complete.

NOTE: An MD5sum check is done only if the MD5 file exists on the server.

Capturing an HP ThinPro image to a USB flash drive

To capture an HP ThinPro image to USB flash drive:

IMPORTANT: Back up any data on the USB flash drive before you begin. HP ThinState automatically formats the flash drive to create a bootable USB flash drive. This process will erase all data currently on the flash drive.

1. Insert a USB flash drive into a USB port on the client.
2. Select **Management > ThinState** in the Control Panel.
3. Select **the HP ThinPro image**, and then click **Next**.
4. Select **make a copy of the HP ThinPro image**, and then click **Next**.

5. Select **create a bootable USB flash drive**, and then click **Next**.
6. Select the USB flash drive, and then click **Finish**.

   When the image capture begins, all applications stop and a new window appears showing the progress. If a problem occurs, click **Details** for information. The desktop reappears after the capture is complete.

Deploying an HP ThinPro image with a USB flash drive

To deploy an HP ThinPro image with a USB flash drive:

IMPORTANT: If you abort a deployment, the previous image will not be restored and the contents of the client's flash drive will be corrupted.

1. Turn off the target client.
2. Insert the USB flash drive.
3. Turn on the client.

NOTE: The screen remains black for 10-15 seconds while the client detects and boots from the USB flash drive. If the client fails to boot from the USB flash drive, try unplugging all other USB devices and repeat the procedure.

Managing an HP ThinPro profile

An HP ThinPro profile contains the connections, settings, and customizations that were configured using the Connection Manager and various Control Panel utilities. A profile is saved in a configuration file that is specific to the version of HP ThinPro in which it was created.

NOTE: A profile can also be preconfigured and deployed using the Profile Editor and Automatic Update (see Using the Profile Editor on page 60 and HP Smart Client Services on page 56 for more information).

Saving an HP ThinPro profile to an FTP server

To save an HP ThinPro profile to an FTP server:

IMPORTANT: The directory on the FTP server where you intend to save the profile must already exist before initiating the save.

1. Select **Management > ThinState** in the Control Panel.
2. Select **the HP ThinPro configuration**, and then click **Next**.
3. Select **save the configuration**, and then click **Next**.
4. Select **on a FTP server**, and then click **Next**.
5. Enter the FTP server information in the fields.
6. Click **Finish**.

Restoring an HP ThinPro profile using FTP or HTTP

To restore an HP ThinPro profile using FTP or HTTP:

1. Select **Management > ThinState** in the Control Panel.
2. Select **the HP ThinPro configuration**, and then click **Next**.

3. Select **restore a configuration**, and then click **Next**.
4. Select **on a remote server**, and then click **Next**.
5. Select either the FTP or HTTP protocol, and then type the server information in the fields.

NOTE: The **Username** and **Password** fields are not required if you are using the HTTP protocol.

6. Click **Finish**.

Saving an HP ThinPro profile to a USB flash drive

To save an HP ThinPro profile to a USB flash drive:

1. Insert a USB flash drive into a USB port on the client.
2. Select **Management > ThinState** in the Control Panel.
3. Select **the HP ThinPro configuration**, and then click **Next**.
4. Select **save the configuration**, and then click **Next**.
5. Select **on a USB key**, and then click **Next**.
6. Select the USB flash drive.
7. Click **Browse**.
8. Navigate to the desired location on the USB flash drive and assign a file name to the profile.
9. Click **Save**.
10. Click **Finish**.

Restoring an HP ThinPro profile from a USB flash drive

To restore an HP ThinPro profile from a USB flash drive:

1. Insert the USB flash drive containing the profile into a USB port on the target client.
2. Select **Management > ThinState** in the Control Panel.
3. Select **the HP ThinPro configuration**, and then click **Next**.
4. Select **restore a configuration**, and then click **Next**.
5. Select **on a USB key**, and then click **Next**.
6. Select the USB key.
7. Click **Browse**.
8. Double-click the desired configuration file on the USB key.
9. Click **Finish**.

VNC Shadowing

Virtual Network Computing (VNC) is a remote desktop program that allows you to see the desktop of a remote computer and control it with your local mouse and keyboard.

To access the VNC Shadow utility:

▲ Select **Management > VNC Shadow** in the Control Panel.

NOTE: You must restart the client before any changes to the VNC Shadowing options will take effect.

The following table describes the options available in the VNC Shadow utility.

Option	Description
Enable VNC Shadow	Enables VNC Shadowing.
VNC Read Only	Makes the VNC session read-only.
VNC Use Password	Makes a password required when accessing the client using VNC. Click **Set Password** to set the password.
VNC Notify User to Allow Refuse	Enables a notification dialog on the remote system that informs the remote user when someone is attempting to connect using VNC. The user can refuse either allow or refuse access.
VNC Show Timeout for Notification	Sets the length of time in seconds that the remote notification dialog is displayed.
User Notification Message	Allows you to display a message in the notification dialog to the remote user.
Refuse connections in default	If enabled, the VNC connection will be refused by default when the timer expires.
Re-set VNC server right now	Resets the VNC server after applying the new settings.

Certificates

NOTE: For more information about using certificates in Linux, go to http://www.openssl.org/docs/apps/x509.html.

Certificate Manager

To open the Certificate Manager:

▲ Select **Advanced > Certificates** in the Control Panel.

Use the Certificate Manager to manually install a certificate from a certificate authority (CA). This action copies the certificate to the user's local certificate store (/usr/local/share/ca-certificates) and configures OpenSSL to use the certificate for connection verification.

If desired, use the Profile Editor to attach the certificate to a profile, as described in Adding certificates to a client profile on page 62.

NOTE: Generally, a self-signed certificate will work as long as it is valid according to specification and can be verified by OpenSSL.

SCEP Manager

To open the SCEP Manager:

▲ Select **Advanced > SCEP Manager** in the Control Panel.

Use the SCEP Manager when you need to enroll or renew client-side certificates from a CA.

During an enrollment or renewal, the SCEP Manager generates the client's private key and certificate request, and then it sends the request to the CA on the SCEP server. When the CA issues the

certificate, the certificate is returned and placed in the client's certificate store. OpenSSL uses the certificate for connection verification.

NOTE: Before enrollment, make sure that the SCEP server is configured properly.

Use the **Identifying** tab of the SCEP Manager to enter information about the user, if desired.

NOTE: The **Common Name** is required and is the client's Fully Qualified Domain Name (FQDN) by default. The other information is all optional. The **Country or Region** is entered as two letters, such as US for the United States and CN for China.

Use the **Servers** tab of the SCEP Manager to add SCEP servers and enroll or renew certificates.

TIP: When entering a new SCEP server, save the server information first, and then use the **Settings** button to go back and do an enrollment.

DHCP options

To open the DHCP Option Manager:

- Select **Advanced > DHCP Options** in the Control Panel.

The DHCP Option Manager displays details of the DHCP options that are requested by the client.

TIP: The drop-down list in the lower-left corner of the DHCP Option Manager allows you to filter which DHCP tags are displayed.

To direct the client to request or ignore specific DHCP options:

- Select or deselect the checkboxes in the **Requested** column.

If a pencil is shown in the **DHCP Code** column, the code number can be changed in case there is a conflict on your DHCP server over a particular code number.

To change a DHCP code:

- Double-click the DHCP code and type a new number.

NOTE: Changeable DHCP codes can only be changed while that DHCP option is enabled in the **Requested** column.

To learn more about how a DHCP option is used on the client and on the DHCP server:

- Click the icon in the **Info** column of that option.

5 Common connection configurations

This chapter discusses configurations that are common to all connection types.

- Common connection settings
- Kiosk Mode

Common connection settings

The following table describes the settings that are available on the final page of the Connection Manager wizard for each connection type. These settings are connection-specific and apply to only the connection you are currently configuring.

Table 5-1 Common connection settings

Option	Description
Fallback Connection	Specifies the fallback connection. If the connection fails to start, the fallback connection will attempt to start instead. **NOTE:** This option is not available for the VMware Horizon View connection type.
Auto start priority	Determines the order that connections will auto-start. **0** means auto-start is disabled. The other values determine the startup order, with **1** being the highest priority.
Share credentials with screensaver	Enables users to unlock the local screensaver using their credentials for that connection. **NOTE:** This option is only available for the Citrix, RDP, and VMware Horizon View connection types.
Auto reconnect	If enabled, this connection will attempt to auto-reconnect if the connection is dropped. **NOTE:** Stopping a connection via the Connection Manager will prevent an auto-reconnection.
Wait for network before connecting	Disable this option if your connection doesn't need the network to start or if you don't want to wait for network to start the connection.
Show icon on desktop	If enabled, a desktop icon will be created for this connection.
Allow the user to launch this connection	If enabled, this connection can be launched by a standard user.
Allow the user to edit this connection	If enabled, this connection can be modified by a standard user.
Login dialog options	Enable or disable these options to configure the login dialog for the connection. **NOTE:** This option is only available for the Citrix, RDP, and VMware Horizon View connection types. The following options are available: • **Show username field** • **Show password field** • **Show domain field**

Table 5-1 Common connection settings (continued)

Option	Description
	• **Show smartcard checkbox** • **Show 'remember me' checkbox** **NOTE:** This option saves the user name and domain, but the password still needs to be entered each time. • **Show 'show password' button**

Kiosk Mode

When a thin client is configured for Kiosk Mode, it performs an automatic login to the default connection on startup using predefined user credentials. If the connection is ever lost due to a logout, disconnect, or network failure, it reconnects automatically as soon as it can be restored.

TIP: The remote host can be configured to auto-start applications on login, making the Kiosk Mode experience seamless.

The easiest way to configure a thin client for Kiosk Mode is to switch it to the Smart Zero configuration (see Customization Center on page 18) and configure a connection. When this is done, the following settings are set automatically:

- The taskbar auto-hides.
- The connection auto-starts.
- The connection auto-reconnects.
- The connection shares the user credentials with the local screensaver.
- The desktop theme is set to that connection type's default theme.
- The USB redirection protocol in the USB Manager is set to that connection type's protocol.

If you want to configure a thin client for Kiosk Mode in the ThinPro configuration (for example, if you want to use a connection type available only with ThinPro), you need to configure the following settings manually for the desired connection:

- In the Customization Center, set the taskbar to **Auto hide**.
- In the Connection Manager for the connection, do the following:
  - Set the **Auto start priority** to **1**.
  - Enable **Auto reconnect**.
  - Enable **Share credentials with screensaver**, if available.
  - For a Web Browser connection only, select the **Enable kiosk mode** option.
- In the USB Manager, set the proper USB redirection protocol, if necessary.

TIP: When in Kiosk Mode, to minimize the connection and return to the local desktop, press Ctrl+Alt +End.

6 Citrix connections

- Citrix connection management features
- Citrix Receiver features
- Citrix connection support matrix
- Citrix general settings
- Citrix connection-specific settings

Citrix connection management features

When using a Citrix connection, you can configure the client to automatically perform the following functions:

- Launch resources when only a single resource is published
- Launch a specified resource
- Launch a published desktop
- Reconnect sessions on connection startup
- Log off the connection after a specified timeout period
- Launch published resources use the following configurable shortcuts:
  - Desktop icons
  - Start menu icons
  - Taskbar icons

Citrix Receiver features

Citrix Receiver features include the following:

- Window size and depth settings
- Seamless window support
- Sound quality settings
- Static drive mapping
- Dynamic drive mapping
- USB redirection for XenDesktop and VDI-in-a-Box

NOTE: Based on internal testing and validation, HP has found that a webcam connected through a Citrix connection using basic USB Redirection performs poorly. HP does not recommend using this configuration and suggests that customers who require this function test using Citrix HDX technology to ensure satisfactory levels of performance.

- Smart card virtual channel enablement

NOTE: This feature is equivalent to a smart card login/authentication when using direct, non-PNAgent connections. With a PNAgent connection, smart card virtual channel enablement enables or disables the smart card virtual channel but does not provide for initial connection authentication. For a smart card authentication to XenApp and XenDesktop, use the provided Web Browser connection instead of the Citrix connection and be sure to enable web access.

- Printer mapping
- Serial port mapping
- HDX MediaStream (hardware-accelerated on most models)

NOTE: See HDX MediaStream on page 28 for more information.

- HDX Flash Redirection (x86-only)
- HDX Webcam Compression

NOTE: HDX Webcam Compression works best on x86 units. HP has found the performance of webcams on ARM units to be poor and does not recommend using ARM units for webcam redirection.

- HDX RealTime (MS Lync Optimization) (x86-only)

NOTE: This is only available on Lync 2010.

- Authentication to Citrix Access Gateway 5.0 and NetScaler Gateway 9.x/10.x using ICA Proxy mode

NOTE: Only CA-issued SHA-1 based certificates are supported. Self-signed and SHA-2 based certificates are not supported.

HDX MediaStream

Whenever possible, HDX MediaStream leverages the processing power of the thin client to render the multimedia content. On the datacenter side, the compressed multimedia information is sent directly to the thin client in its native format. The experience will vary based on the processing power and multimedia capability of the thin client.

NOTE: Certain video types might not perform well on low-end units. High-end units are recommended for HDX media redirection.

Table 6-1 HDX MediaStream support matrix

Feature	Support
Frame rate	• 24 fps
Resolution	• 1080p • 720p
Video containers	• WMV • AVI • MPG • MPEG • MOV • MP4

Table 6-1 HDX MediaStream support matrix (continued)

Feature	Support
Video codecs	• WMV2 • WMV3 / VC-1 • H.264 / AVC / MPEG-4 Part 10 • MPEG-4 Part 2 • H.263 • DivX • Xvid • MPEG1
Audio codecs	• MP3 • WMA • AAC • PCM • mpeg-audio • MLAW / ULAW

Citrix connection support matrix

The following table describes the supported Citrix backends.

Table 6-2 Citrix connection support matrix

		Backend		
		XenApp	XenDesktop	VDI-in-a-Box
Access type	Direct (legacy)	4.5 / 5 / 6 / 6.5		
	PNAgent (legacy)	4.5 / 5 / 6 / 6.5 / 7.X	4.5 / 5.5 / 5.6.5 / 7.X	5.x
	Web browser	4.5 / 5 / 6 / 6.5 / 7.X	4.5 / 5.5 / 5.6.5 / 7.X	5.x
	StoreFront	4.5 / 5 / 6 / 6.5 / 7.X	4.5 / 5.5 / 5.6.5 / 7.X	5.x

Citrix general settings

The following tables describe the settings available in the XEN Connection General Settings Manager. These settings are universal and apply to all Citrix connections.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 6-3 XEN Connection General Settings Manager > Options

Option	Description
Enable HDX MediaStream	Enables HDX MediaStream.

Table 6-3 XEN Connection General Settings Manager > Options (continued)

Option	Description
	IMPORTANT: For HDX MediaStream to be enabled, both this setting and the **Enable MultiMedia** setting must be enabled. Both settings can be found on the same page in the XEN Connection General Settings Manager.
Enable Windows Alert Sound	Enable the Windows alert sound.
ICA Acceleration (LAN Only)	Enable ICA Acceleration.
Disable Info Box Before Connecting	Do not display the information box displayed before a connection is completed.
Use Asynchronous COM-port Polling	Use asynchronous polling of the COM port.
Allow Smart Card Logon	Use a client-connected Smart Card for logon authentication.
Enable Auto Reconnect	Enable automatic reconnection of dropped connections.
Enable MultiMedia	Enables HDX MediaStream. **IMPORTANT:** For HDX MediaStream to be enabled, both this setting and the **Enable HDX MediaStream** setting must be enabled. Both settings can be found on the same page in the XEN Connection General Settings Manager. **NOTE:** This option might need to be disabled to support Lync RTME.
Use Data Compression	Use data compression for this connection.
Enable H264 Compression	Enables H264 compression. See Citrix documentation to determine if this method of data compression is best for your use cases.
Enable Middle Button Paste	Enables a middle mouse button click to perform a paste operation.
User Agent String	Specify a User Agent string to be used for requests sent to the Citrix server. This option is useful for Netscaler configuration.
HDX Flash Redirection	Enables HDX Flash redirection to play flash content locally.
HDX Flash Server Side Content Fetch	Allows the server to fetch the flash content for redirection.
Sound	Specifies the sound quality to be used. Valid options are: **High Quality**, **Med Quality**, and **Low Quality**.
Speed Screen	Valid options are: **Auto**, **On**, and **Off**.
Local Text Echo	Controls keyboard latency reduction. The recommended setting is **Auto**.
Encryption Level	Specifies the encryption level of an ICA session.

Table 6-4 XEN Connection General Settings Manager > Local Resources

Option	Description
Printers	Select **Printer Mapping**, **USBR**, or **Disable**.
Webcam/Audio-Input	Select **HDX Compression**, **USBR**, or **Disable**.
USB Drive	Select **Dynamic Mapping**, **USBR**, or **Disable**.
Enable Static Drive Mapping (Legacy)	Allows you to specify drive mappings to local paths.

Table 6-5 XEN Connection General Settings Manager > Window

Option	Description
TWI Mode	Allows you to display a single window on the local ThinPro desktop as if it were a native application.
Default Window Size	Establish the default window size. Options are: **Full Screen**, **Fixed Size**, **Percentage of Screen Size**.
Default Window Colors	Establish the default window colors. Options are: **16**, **256**, **16-bit**, **24-bit**, **Automatic**.
Default 256 Color Mapping	This option is only enabled if **Default Window Colors** is set to **256**. Options are: **Shared - Approximate Colors** and **Private - Exact Colors**.

Table 6-6 XEN Connection General Settings Manager > Firewall

Option	Description
Proxy Type	Options are: **None - direct**, **SOCKS**, **Secure - HTTPS**, **Use browser settings**, **Automatically detect proxy**.
Proxy Address	The IP address of the proxy server.
Proxy Port	The port for connection to the proxy server.
Username	The username to use for connection to the proxy server.
Password	The password to use for connection to the proxy server.
Use Alternate Address for Firewall Connection	The Citrix ICA Client will request the alternate address defined for the server when contacting servers inside the firewall. The alternate address must be specified for each server in a server farm.

Table 6-7 XEN Connection General Settings Manager > Keyboard Shortcuts

Option	Description
Enable UseLocalIM	Uses the local input method to interpret keyboard input. This is supported only for European languages.
Use EUKS Number	Controls use of Extended Unicode Keyboard Support on Windows servers: 0=no EUKS 1=EUKS used as fallback 2=use EUKS whenever possible
Handling of keyboard shortcuts	Specifies how function keys should be handled. Options are: **Translated**, **Direct in full screen desktops only**, and **Direct**.
Stop Direct key handling	Not enabled when the option **Handling of keyboard shortcuts** is set to **Translated**.
<List of keyboard shortcuts>	Only enabled when **Handling of keyboard shortcuts** is **Translated** or **Direct in full screen desktops only**.

Table 6-8 XEN Connection General Settings Manager > Session

Option	Description
Auto Logout Delay Before App Launch	When using a Citrix server with multiple published resources, this specifies the number of seconds to allow a user to launch an app after login before the system automatically logs out and returns to the initial login screen.
Auto Logout Delay After App Close	When using a Citrix server with multiple published resources, this specifies the number of seconds between the closing of the last Xen published resource and when the user is automatically logged out and returned to the initial login screen.
Server Check Timeout	To perform a basic connectivity check to the selected server and port, set this option to a value other than the default **–1**.
TIP: Setting any of these values to less than 0 will disable auto-logout.	
NOTE: Citrix processing delays might increase the auto-logout time.	

Citrix connection-specific settings

The following table describes the settings available in the Citrix Connection Manager. These settings are connection-specific and apply to only the Citrix connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 6-9 Citrix Connection Manager > Configuration

Option	Description
Name	The connection name.
Service URL	The Citrix server hostname or IP address. If you are configuring a connection to a server on an HTTPS site, enter the FQDN for the site and the local root certificate in the Citrix certificate store.
Connection Mode	Select **PNAgent**, **StoreFront**, or **Direct**.
Username	The username to use for the connection.
Password	The password to use for the connection.
Domain	The domain to use for the connection.
Auto Start Resource	The name of an autostart resource.
Auto Start Desktop	Automatically launches a desktop type resource if available.
Auto Start Single Application	If there is a single application or desktop published, it is automatically started when enabled.
Show applications on desktop	Shows remote resources on the local desktop.
Show applications on taskbar	Shows remote resources on the local taskbar.
Auto Reconnect Applications on Login	If not using SmoothRoaming, disable this option to increase your connection speed.

Table 6-10 Citrix Connection Manager > Security

Ignore Certificate Check	If enabled, certificates are not checked and the connection is insecure.
Force HTTPS Connection	If enabled, the connection is forced to use the HTTPS protocol, helping to ensure a secure connection.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the Citrix Connection Manager.

7 RDP connections

- RDP features
- RDP general settings
- RDP connection-specific settings
- Using RemoteFX with RDP
- Using multi-monitor sessions with RDP
- Using multimedia redirection with RDP
- Using device redirection with RDP

RDP features

The RDP client is based on FreeRDP 1.1 and meets the following requirements for RDP 7.1:

- Hardware-accelerated RemoteFX
- MMR supported when connecting to Windows hosts with the Desktop Experience feature enabled (Windows 7 or Windows Server 2008 R2)
- USBR supported when connecting to Windows 7 Remote Desktop Virtual Hosts
- Bidirectional audio
- True multi-monitor support
- Gateway and brokered connection support

RDP general settings

The following table describes the settings available in the RDP Connection General Settings Manager. These settings are universal and apply to all RDP connections.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 7-1 RDP Connection General Settings Manager

Option	Description
Send hostname as	Specifies whether to send the client's hostname or MAC address as the hostname specified to the remote system.
Enable Multimedia Redirection	Enables multimedia redirection.

RDP connection-specific settings

The following tables describe the settings available in the RDP Connection Manager. These settings are connection-specific and apply to only the RDP connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 7-2 RDP Connection Manager > Network

Option	Description
Name	A custom name for this connection
Address	The IP address or server name for this connection
Port	The connection port (3389 by default)
Username	The username for this connection
Password	The password for this connection
Domain	The domain name for this connection (optional)
Allow Smartcard Login	Enables smart card authentication
Enable RD Gateway	Enables additional RD Gateway options, such as the gateway address, port, and credentials

Table 7-3 RDP Connection Manager > Window

Option	Modes	Description
Hide Window Decoration	Standard Desktop	This setting makes sure that screen elements such as the menu bar, minimize and close options, and borders of the window pane are not displayed.
Window Size	Standard Desktop Alternate Shell	Sets the window size to **full**, **fixed**, or **percent**.
Percentage Size	Standard Desktop Alternate Shell	If **Window Size** is set to **percent**, this option sets the percentage of the screen that a desktop window occupies. NOTE: The resulting sizes might be rounded. NOTE: RemoteFX supports only a fixed list of resolutions.
Fixed Size	Standard Desktop Alternate Shell	If **Window Size** is set to **fixed**, this option sets the width and height in pixels that the desktop window occupies.
Application	Remote Application	Specifies the path of the application to run. If using RDP Seamless Windows mode, type the path of `seamlessrdpshell.exe` on your server, followed by a space and then the path of the application to run. See the following example: `c:\seamless\seamlessrdpshell.exe c:\Program Files\Microsoft\Word.exe`
Command	Alternate Shell	Specifies the application that will run in **Alternate Shell** mode. Enter the command that executes the application. For example, to run Microsoft Word, type `Word.exe`.
Directory	Alternate Shell	Enter the server's working directory path for the application's program files. For example, the working directory for Microsoft Word is `C:\Program Files\Microsoft`.

Table 7-4 RDP Connection Manager > Options

Option	Description
Enable motion events	If enabled, mouse motions are continuously relayed to the RDP server.
Enable data compression	Enables bulk compression of data between the RDP server and client.
Enable deprecated RDP encryption	Enables last-generation RDP encryption when NLA is not available.
Enable offscreen cache	If enabled, off-screen memory is used to cache bitmaps.
Attach to admin console	Attaches the connection to the administrator console port.
Cross-session copy/paste	If enabled, copy and paste are enabled between different RDP sessions.
Certificate Verification Policy	Select one of the following: • **Accept all RDP server certificates** • **Use remembered hosts; warn if unknown or invalid certificate** • **Skip remembered hosts; warn if unknown or invalid certificate** • **Connect only to pre-approved RDP servers**
Hostname to send	Normally, the client's hostname is used for Client Access Licenses. This field allows a different value to be sent.
Load Balance Info	Use this option with a brokered RDP connection. Enter the URL found in any of the .desktop files of the Web Interface.

Table 7-5 RDP Connection Manager > Local Resources

Option	Description
Audio Devices	Determines whether audio devices are redirected by high-level RDP audio redirection, low-level USB redirection, or disabled for this connection.
Printers	Determines whether printers are redirected by high-level printer redirection (which requires them to be set up via the Printers utility in the Control Panel), low-level USB redirection, or disabled for this connection.
Serial/Parallel Ports	Determines whether serial and parallel ports are redirected or disabled for this connection.
USB Storage	Determines whether USB storage devices such as flash drives and optical drives are redirected by high-level storage redirection, low-level USB redirection, or disabled for this connection.
Local Partitions	Determines whether local partitions of the thin client's flash drive are redirected or disabled for this connection.
Other USB Devices	Determines whether other classes of USB devices (such as webcams and tablets) are redirected by low-level USB redirection or disabled for this connection.

Table 7-6 RDP Connection Manager > Experience

Option	Description
Choose your connection speed to optimize performance	Selecting a connection speed (**LAN**, **Broadband**, or **Modem**) will enable or disable the following options to optimize performance: • **Desktop background**

Table 7-6 RDP Connection Manager > Experience (continued)

Option	Description
	• **Font smoothing** • **Desktop composition** • **Show contents of window while dragging** • **Menu and window animation** • **Themes** Selecting **Client Preferred Settings** allows the client to choose which options to use to provide the best RDP experience. You can also select your own custom combination of options.
End-to-End Connection Health Monitoring	Select to enable the timeout options.
Warning Timeout	Specifies the amount of time in seconds after receiving the last network traffic from the server before the user is warned of a lost connection. This function can be disabled by clearing the option or setting the time to zero. **TIP:** HP recommends increasing the timeout value for networks that experience frequent busy periods or momentary outages.
Recovery Timeout	Specifies the amount of time in seconds after receiving the last network traffic from the server that the client waits for the connection to recover without taking any special action. At the end of this period, the client attempts a quick reconnection with the session.
Error Timeout	Specifies the amount of time in seconds after receiving the last network traffic from the server that the client waits before stopping attempts to reconnect with that server.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the RDP Connection Manager.

Using RemoteFX with RDP

RemoteFX (RFX) is an advanced graphics display protocol that is designed to replace the graphics component of the traditional RDP protocol. It uses the hardware acceleration capabilities of the server GPU to encode the screen contents via the RFX codec and send screen updates to the client. RFX uses advanced pipelining technologies and adaptive graphics to make sure that it delivers the best possible experience based on content type, CPU and network bandwidth availability, and rendering speed.

RFX is enabled by default. The administrator or user does not have to change any settings to enable it. The client negotiates with any RDP server it contacts, and if RFX is available, it will be used.

To disable RFX, set the following registry key to 0:

`root/ConnectionType/freerdp/connections/<UUID>/remoteFx`

TIP: For simplified management, HP recommends that you enable or disable RFX on the remote host.

NOTE: Some Windows RDP servers will not send RemoteFX content to clients enabled for RDP 7.1 without a change to Group Policy. Check the setting of the following policy:

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment > Enable RemoteFX encoding for RemoteFX clients designed for Windows Server 2008 R2 SP1

In addition, Windows Server 2012 and Windows Server 2012 R2 require the following setting to be set to **32-bit**:

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment > Limit maximum color depth

Using multi-monitor sessions with RDP

True multi-monitor support does not require special configuration. The RDP client automatically identifies which monitor is specified as the primary monitor in the local settings and places the taskbar and desktop icons on that monitor. When a window is maximized within the remote session, the window will only cover the monitor it was maximized on.

Display preferences and monitor resolutions can be viewed but not modified within the remote session. To modify the session resolution, log out of the session and change the resolution on the local client.

By default, all RDP sessions will be full-screen and cover all monitors to enhance the virtualization experience. Additional window options are available in the RDP Connection Manager.

NOTE: Remote Desktop Virtualization Host (RDVH) sessions with graphics card support might only support certain resolutions and counts of monitors. The limits are specified when the RemoteFX virtual graphics device is configured for the RDVH virtual machine.

Using multimedia redirection with RDP

Multimedia redirection (MMR) is a technology that integrates with Windows Media Player on the remote host and streams the encoded media to the client instead of playing it on the remote host and re-encoding it via RDP. This technology reduces the server load and network traffic, and greatly improves the multimedia experience, supporting 24 fps playback of 1080p videos with automatic audio syncing. MMR is enabled by default. A client will negotiate with any RDP server it contacts, and if MMR is available, it will be used.

MMR also uses an advanced codec detection scheme that identifies whether the client supports the codec being requested by the remote host before attempting to redirect it. The result is that only supported codecs will be redirected and all unsupported codecs fall back to server-side rendering.

To disable MMR on the client for all RDP connections, set the following registry key to 0:

`root/ConnectionType/freerdp/general/enableMMR`

Because RemoteFX already delivers acceptable multimedia performance, you can disable MMR with RFX by setting the following registry key to 1:

`root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX`

TIP: For simplified management, HP recommends that MMR be enabled or disabled on the remote host.

Using device redirection with RDP

Device redirection makes sure that when a user plugs a device into the client, the device is automatically detected and accessible in the remote session. RDP supports redirection of many different types of devices.

Using USB redirection with RDP

USB redirection works by transmitting low-level USB protocol calls over the network to the remote host. Any USB device plugged into the local host appears within the remote host as a native USB device, as if it were plugged in locally. Standard Windows drivers support the device in the remote session, and all device types are supported without requiring additional drivers on the client.

Not all devices default to USB redirection. For example, USB keyboards, mice, and other input devices usually are not set to be redirected, as the remote session expects input to come from the client. Some devices such as mass storage, printers, and audio devices might use additional options for redirection.

Note the following additional information about USB redirection with RDP:

- The server must support USB redirection for it to be available to the client. General-purpose USB redirection is supported with RDVH servers with RemoteFX, Windows 8, and Windows Server 2012.
- The protocol in the USB Manager in the Control Panel must be set to RDP.
- For RDP connections, the controls in the USB Manager determine if a USB device is redirected. The settings for the individual connection determine how a USB device is redirected.

Using mass storage redirection with RDP

By default, the RDP session redirects all mass storage devices to the remote host using high-level drive redirection. When a device such as a USB flash drive, USB DVD-ROM drive, or USB external HDD is plugged into the system, the client detects and mounts the drive on the local file system. RDP then detects a mounted drive and redirects it to the remote host. Within the remote host, it will appear as a new disk drive in Windows Explorer, with the name `<device label> on <client hostname>`; for example, `Bill_USB on HP04ab598100ff`.

There are three restrictions to this type of redirection.

- The device will not appear in the taskbar on the remote host with an icon to eject the device. Because of this, make sure to give the device a sufficient amount of time to sync data after a copy before removing the device to be sure that the device does not corrupt. Typically, less than one second is required after the file copy dialog finishes, but up to 10 seconds might be required depending on the device write speed and network latency.
- Only file systems supported by the client will be mounted. The supported file systems are FAT32, NTFS, ISO9660 (CD-ROMs), UDF (DVD-ROMs), and ext3.
- The device will be treated as a directory; common drive tasks like formatting and modification of the disk label will not be available.

USB redirection of storage devices can be disabled in an individual connection's settings. If desired, you can disable mass storage redirection altogether. To do this, turn off USB redirection, and then change the registry keys as described in the following table.

Table 7-7 Disabling USB redirection

Registry entry	Value to set	Description
root/USB/root/holdProtocolStatic	1	Makes sure that the USBR type will not be automatically changed when a connection is set or unset
root/USB/root/protocol	local	Makes sure that the RDP connection does not attempt to redirect any devices to the remote session

To completely disable local mounting of USB mass storage devices or to disable the redirection of USB mass storage devices but still allow other devices to redirect, in the client file system, delete the udev rule `/etc/udev/rules.d/010_usbdrive.rules`.

Using printer redirection with RDP

By default, RDP has two methods of printer redirection enabled:

- **USB redirection**—Any USB printer plugged into the device will show up as a local printer in the remote session. The standard printer installation process must happen in the remote session if the printer is not already installed on that remote host. There are no settings to manage locally.
- **High-level redirection**—If either USB redirection is unavailable on the remote host or the printer is a parallel or serial printer, use high-level redirection. Configure the printer to use a local printer spooler, and the RDP client automatically sets up a remote printer that sends print spooling commands through a virtual channel from the remote host to the client.

  This method requires both that the printer be configured on the client and a Windows driver be specified on the client because the RDP client needs to specify to the remote host which driver to use for the remote printer. This Windows driver must match the driver that the printer would use when locally attached to a Windows operating system. This information is usually found under the **Model** in the printer properties.

NOTE: See Configuring a serial or parallel printer on page 63 for more information.

Using audio redirection with RDP

By default, high-level audio redirection will redirect audio from the remote host to the client. Basic voice control might need to be set up, and RDP 7.1 contains a number of advanced audio redirection features that might require additional configuration.

See the following notes about using audio redirection with RDP:

- RDP delivers the highest quality audio as the network bandwidth allows. RDP reduces audio quality to play on low-bandwidth connections.
- No native audio or video syncing mechanisms are available in standard RDP. Longer videos might not sync with audio. MMR or RemoteFX can resolve this issue.
- HP recommends high-level audio redirection, but USB redirection of audio devices is possible if additional functionality is present, such as a digital volume control. Only high-level redirection is available for analog devices.
- Microphone redirection is enabled by default. The default microphone volume might need to be adjusted on the client. Older Windows RDP servers must have their settings modified to enable audio input.
- Both the local and remote volume settings will affect the final volume. HP recommends setting the local volume to a maximum and adjusting the volume within the remote host.

Using smart card redirection with RDP

By default, smart cards will be redirected using high-level redirection, allowing them to be used to log in to the session and other remote applications.

To enable smart card login for an RDP connection:

▲ Select **Allow Smartcard Login** in the RDP Connection Manager.

This will allow the user to connect without first specifying credentials. The RDP client will start the RDP session, and the user will be prompted to authenticate by smart card.

This technology requires drivers for the smart card reader driver to be installed on the client. By default, the CCID and Gemalto drivers are installed, which adds support for the majority of smart card readers available. Additional drivers can be installed by adding them to `/usr/lib/pkcs11/`.

NOTE: When smart card login is enabled, Network Level Authentication is not supported and is automatically disabled.

8 VMware Horizon View connections

- VMware Horizon View settings
- Using multi-monitor sessions with VMware Horizon View
- Using keyboard shortcuts with VMware Horizon View
- Using Multimedia Redirection with VMware Horizon View
- Using device redirection with VMware Horizon View
- Changing the VMware Horizon View protocol type
- VMware Horizon View HTTPS and certificate management requirements

VMware Horizon View settings

The following tables describe the settings available in the VMware Horizon View Connection Manager. These settings are connection-specific and apply to only the VMware Horizon View connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 8-1 VMware Horizon View Connection Manager > Network

Option	Description
Name	Enter a name for this connection.
Server	Enter the hostname or IP address of a VMware Horizon View server.
Username	Enter the username to use for the connection.
Password	Enter the password to use for the connection.
Domain	Enter the domain to use for the connection.
Desktop	Specify the optional desktop pool to automatically connect to.

Table 8-2 VMware Horizon View Connection Manager > General

Option	Description
Automatic login	When enabled, the user is automatically logged in when the connection is established. **NOTE:** HP recommends enabling this option.
Allow Smartcard login	Enables smart card login. **NOTE:** For more information on smart cards, see Using smart card redirection with VMware Horizon View on page 47.
Don't start application maximized	If enabled, applications do not start in maximized windows.
Application Size	Select **All Monitors**, **Full Screen**, **Large Window**, or **Small Window**.

Table 8-2 VMware Horizon View Connection Manager > General (continued)

Option	Description
Desktop Size	Select **All Monitors**, **Full Screen**, **Large Window**, or **Small Window**.
Command Line Arguments	Enter any desired command line arguments to be used for the connection. For more help on using advanced command line arguments, do one of the following: • On the command line, enter `vmware-view--help`. • See the Linux Horizon View client documentation provided by VMware at http://www.vmware.com. **NOTE:** This option does not apply to the Teradici-accelerated PCoIP client.

Table 8-3 VMware Horizon View Connection Manager > Security

Option	Description
Close After Disconnect	Makes the VMware Horizon View client close automatically after users log out of their desktops or the session terminates with an error. This option is a security feature designed so that a user does not need to take an additional step to fully log out after they are finished with their desktop session. This option is enabled by default for security purposes but can be disabled if users find that they are often switching to a new desktop pool after logging out of a session and do not want to fully log in again.
Hide top Menu bar	Makes the top menu bar invisible for users. This option enabled by default. Disable it if users prefer to access options for window size or desktop pool selection in a VMware Horizon View session.
Prevent users from changing server address	If enabled, standard users cannot change the server address.
Connection Security Level	Use the **Connection Security Level** to adjust the security level that the VMware Horizon View client uses when connecting to the server. **NOTE:** For more information, see VMware Horizon View HTTPS and certificate management requirements on page 48 for details on how connection security levels behave.

Table 8-4 VMware Horizon View Connection Manager > RDP Options

Option	Description
Enable motion events	Enables motion events for this connection.
Enable data compression	Uses data compression for this connection.
Enable deprecated RDP encryption	Enables encryption for this connection.
Enable offscreen cache	If enabled, off-screen memory is used to cache bitmaps.
Attach to admin console	Attaches the connection to the administrator console port.
Certificate Verification Policy	Select one of the following: • **Accept all RDP server certificates** • **Use remembered hosts; warn if unknown or invalid certificate**

Table 8-4 VMware Horizon View Connection Manager > RDP Options (continued)

Option	Description
	• **Skip remembered hosts; warn if unknown or invalid certificate** • **Connect only to pre-approved RDP servers**
Hostname to send	Sends the hostname to the remote system for this connection.
Load Balance Info	Use this option with a brokered RDP connection. Enter the URL found in any of the .desktop files of the Web Interface.
Remote computer sound	Specifies where the remote computer's sound should be played (remotely or locally) or if it should not be played at all.
Enable port mapping	Maps the client's serial and parallel ports to the remote session.
Enable printer mapping	Maps the local print queue to the remote session. Use this option if either USB redirection is unavailable on the remote host or the printer is a parallel or serial printer. Configure the printer to use a local printer spooler, and the RDP client automatically sets up a remote printer that sends print spooling commands through a virtual channel from the remote host to the client. This method requires both that the printer be configured on the client and a Windows driver be specified on the client because the RDP client needs to specify to the remote host which driver to use for the remote printer. This Windows driver must match the driver that the printer would use when locally attached to a Windows operating system. This information is usually found under the **Model** in the printer properties.
Shared folders	**Add**, **Remove**, or **Edit** shared folders.

Table 8-5 VMware Horizon View Connection Manager > RDP Experience

Option	Description
Enable MMR	Enables multimedia redirection.
Choose your connection speed to optimize performance	Selecting a connection speed (**LAN**, **Broadband**, or **Modem**) will enable or disable the following options to optimize performance: • **Desktop background** • **Font smoothing** • **Desktop composition** • **Show contents of window while dragging** • **Menu and window animation** • **Themes** Selecting **Client Preferred Settings** will allow the client to choose which options to use. You can also select your own custom combination of options.
End-to-End Connection Health Monitoring	Select to enable the timeout options.
Warning Timeout	Specifies the amount of time in seconds after receiving the last network traffic from the server before the user is warned of a lost connection. This function can be disabled by clearing the option or setting the time to zero.

Table 8-5 VMware Horizon View Connection Manager > RDP Experience (continued)

Option	Description
	TIP: HP recommends increasing the timeout value for networks that experience frequent busy periods or momentary outages.
Error Timeout	Specifies the amount of time in seconds after receiving the last network traffic from the server that the client waits before stopping attempts to reconnect with that server.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the VMware Horizon View Connection Manager.

Using multi-monitor sessions with VMware Horizon View

VMware Horizon View supports multi-monitor sessions. To enhance the virtualization experience, the default VMware Horizon View sessions use full-screen and span all monitors. To choose a different window size, select **Full Screen – All Monitors** under the protocol type of the desktop pool for the connection and then choose another option from the window size list. The next time you connect to a session the window will open in the selected size.

Using keyboard shortcuts with VMware Horizon View

Windows keyboard shortcuts

To help administer Windows systems, VMware Horizon View supports Windows keyboard shortcuts. For example, when Ctrl+Alt+Del is used, VMware Horizon View displays a message that provides the following options:

- Send a **Ctrl+Alt+Del** command.
- Disconnect the session—Use this when you have no other way of ending the session.

Windows keyboard shortcuts will be forwarded to the remote desktop session. The result is that local keyboard shortcuts, such as Ctrl+Alt+Tab and Ctrl+Alt+F4, will not function while inside the remote session.

TIP: To be able to switch sessions, disable the **Hide top Menu bar** option in the VMware Horizon View Connection Manager or via the registry key `root/ConnectionType/view/connections/<UUID>/hideMenuBar`.

Media keys

VMware Horizon View uses media keys to control options such as volume, play/pause, and mute during a remote desktop session. This supports multimedia programs such as Windows Media Player.

Using Multimedia Redirection with VMware Horizon View

VMware Horizon View connections support MMR functionality when used with the Microsoft RDP protocol.

For more information, see Using multimedia redirection with RDP on page 38.

Using device redirection with VMware Horizon View

Using USB redirection with VMware Horizon View

To enable USBR for VMware Horizon View connections, select **VMware Horizon View** as the remote protocol in the USB Manager.

For more information on USBR, including device- and class-specific redirection, see Using USB redirection with RDP on page 39.

Using mass storage redirection with VMware Horizon View

You must use the RDP connection protocol to use mass storage redirection with a VMware Horizon View connection.

To perform drive redirection of a USB drive or internal SATA drive:

▲ Add – `xfreerdpoptions='/drive:$foldname,shared folder path, share device'` in the command-line arguments option.

For example, `–xfreerdpoptions='/drive:myfolder,/home/user,/dev/sda2'` shares the `/home/user` on the `/dev/sda2` drive as `myfolder` in a VMware Horizon View connection.

For more details, see Using mass storage redirection with RDP on page 39.

Using printer redirection with VMware Horizon View

For connections made with the PCoIP protocol on x86 units, printers can be shared using VMware Horizon View's high-level printer redirection or USBR. PCoIP connections on ARM units support only USBR printer redirection. For connections made with the RDP protocol, see Using printer redirection with RDP on page 40 for more information.

Using audio redirection with VMware Horizon View

If you do not need the audio recording capability, use high-level audio redirection. Audio will play out of the 3.5 mm jack or, by default, a USB headset if it is plugged in. Use the local audio manager to adjust the input/output level, select playback, and capture devices.

The VMware Horizon View client supports high-level audio-record redirection only via the PCoIP connection type on x86 units when connecting to a server running VMware Horizon View 5.2 Feature Pack 2 or higher. If you need audio-recording support and are using a different configuration, use one of the following methods:

- If your system uses VMware Horizon View Client 1.7 or higher, use the RDP protocol to allow for high-level audio redirection through either the 3.5 mm jack or a USB headset.

NOTE: To use high-level audio-record redirection through the RDP protocol, the server must support it and be configured to allow audio recording over a remote session. The server must be running Windows 7 or greater. You also must make sure the `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\fDisableAudioCapture` registry key is set to `0`.

- If you have a USB headset with a microphone, you can use USBR. Set the USB headset to be redirected into the session. The headset will show up as an audio device. By default, USB audio devices are not redirected and the view client uses high-level audio redirection. To redirect the USB headset, use the client's USB Manager and select the USB headset to be redirected. Make sure that **VMware Horizon View** is selected as the USBR protocol and make sure that the headset is checked under the **Devices** to be redirected.

NOTE: VMware and HP do not recommend using USBR for headsets. A large amount network bandwidth is required to stream audio data over the USBR protocol. Also, you might experience poor audio quality with this method.

Using smart card redirection with VMware Horizon View

To use a smart card to log in to the VMware Horizon View server:

1. Be sure smart card login is enabled in the VMware Horizon View Connection Manager.

   After starting the connection, the VMware Horizon View client will display a list of server credentials.

2. To unlock the credentials and access the VMware Horizon View Manager server, type the appropriate PIN for the server.

NOTE: After you supply the correct PIN, the user's credentials will be used to log in to the VMware Horizon View Manager server. Please see the VMware Horizon View documentation for details on configuring the server to support smart card login. As long as the server is configured to allow smart card login, the user's credentials will pass through and they will be logged in to the desktop without having to enter their PIN again.

NOTE: To log in to the VMware Horizon View Manager administrator server with a smart card, the local smart card driver must be installed on the client. See Using smart card redirection with RDP on page 41 for more information on smart card driver installation. Once logged in to the remote host, the smart card will be passed to the remote host using a virtual channel, not USBR This virtual channel redirection makes sure that the smart card can be used for tasks such as email signing, screen locking, and so on, but might cause the smart card to not show as a smart card device in the Windows Device Manager.

NOTE: The remote host must have the proper smart card drivers installed.

Using webcam redirection with VMware Horizon View

The VMware Horizon View client supports high-level webcam redirection only through RTAV using x86 units connected to a back-end server running VMware Horizon View 5.2 Feature Pack 2 or higher. Other connection methods do not support high-level webcam redirection and can redirect webcams only using USBR. Based on internal testing and validation, HP has found that the performance of a webcam connected through basic USBR performs poorly. HP does not recommend the use of this configuration and suggests that customers who require this function test using x86 units with RTAV technology to ensure satisfactory levels of performance. With USBR, the webcam might perform poorly or not at all. See Using USB redirection with RDP on page 39 for more information.

Changing the VMware Horizon View protocol type

The VMware Horizon View client connects to desktops using one of the following protocol types:

- PCoIP protocol
- RDP protocol

To change the connection type:

1. In the VMware Horizon View client, select a pool that supports one of the following protocols:

- PCoIP
- RDP

2. Under the **Connection** menu, select **Settings**.
3. Change the protocol by using the drop-down box next to **Connect Via**.

NOTE: Use the VMware Horizon View Manager to configure which connection protocol should be used for each desktop pool.

TIP: HP recommends using the PCoIP protocol to enhance the desktop experience. However, the RDP protocol provides more options for customization and might work better on slower connections.

VMware Horizon View HTTPS and certificate management requirements

VMware Horizon View Client 1.5 and VMware Horizon View Server 5.0 and later require HTTPS. By default, the VMware Horizon View client warns about untrusted server certificates, such as self-signed (like the VMware Horizon View Manager default certificate) or expired certificates. If a certificate is signed by a Certificate Authority (CA) and the CA is untrusted, the connection will return an error and the user will not be allowed to connect.

HP recommends that a signed certificate verified by a standard trusted root CA be used on the VMware Horizon View Manager server. This makes sure that users will be able to connect to the server without being prompted or required to do any configuration. If using an internal CA, the VMware Horizon View client connection returns an error until you complete one of the following tasks:

- Use the Certificate Manager to import the certificate from a file or URL.
- Use a remote profile update to import a certificate.
- In the VMware Horizon View Connection Manager, set **Connection Security Level** to **Allow all connections**.

Table 8-6 VMware Horizon View certificate security levels

		Security level		
		Refuse insecure connections	**Warn**	**Allow all connections**
Certificate trust	**Trusted**	Trusted	Trusted	Trusted
	Self-signed	Error	Warning	Untrusted
	Expired	Error	Warning	Untrusted
	Untrusted	Error	Error	Untrusted

Table 8-7 Certificate security level definitions

Level	Description
Trusted	Connects without a certificate warning dialog and displays a green lock icon
Untrusted	Connects without a certificate warning dialog and displays a red unlock icon

Table 8-7 Certificate security level definitions (continued)

Level	Description
Warning	Connects with a certificate warning dialog and displays a red unlock icon
Error	Does not allow the connection

9 Web Browser connections

- Web Browser general settings
- Web Browser connection-specific settings

Web Browser general settings

The following table describes the settings available in the Web Browser Connection General Settings Manager. These settings are universal and apply to all Web Browser connections.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 9-1 Web Browser Connection General Settings Manager

Option	Description
Web Browser preferences	Opens the Firefox Preferences dialog.
Allow connections to manage their own settings	When enabled, Firefox settings are saved for each Web Browser connection. Otherwise, the settings are reset each time the connection is launched.

Web Browser connection-specific settings

The following table describes the settings available in the Web Browser Connection Manager. These settings are connection-specific and apply to only the Web Browser connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 9-2 Web Browser Connection Manager > Configuration

Option	Description
Name	The connection name.
URL	The URL for the connection.
Enable kiosk mode	Enables Kiosk Mode.
Enable full screen	Uses full screen mode for the connection.
Enable print dialog	Enables the print dialog box.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the Web Browser Connection Manager.

10 Additional connection types (ThinPro configuration only)

The connection types listed in this chapter are available only when the client is set to the ThinPro configuration. For more information, see Comparison of ThinPro and Smart Zero on page 1.

- TeemTalk connection settings
- XDMCP connection settings
- SSH connection settings
- Telnet connection settings
- Custom connection settings

TeemTalk connection settings

TIP: For more information on HP TeemTalk, see the *HP TeemTalk Terminal Emulator User Guide*.

The following table describes the settings available in the TeemTalk Connection Manager. These settings are connection-specific and apply to only the TeemTalk connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 10-1 TeemTalk Connection Manager > Configuration

Option	Description
Name	The connection name.
TeemTalk creation wizard	Opens the TeemTalk Session Wizard. See the other tables in this section for more information.
System beep	Enables the system beep sound.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the TeemTalk Connection Manager.

The following tables describe the settings available in the TeemTalk Session Wizard, which is a component of the TeemTalk Connection Manager. These settings are connection-specific and apply to only the TeemTalk connection you are currently configuring.

NOTE: For information about how to locate these settings, see Table 10-1 TeemTalk Connection Manager > Configuration on page 51.

Table 10-2 TeemTalk Session Wizard > Page 1

Option	Description
Session Name	The name of the session.

Table 10-2 TeemTalk Session Wizard > Page 1 (continued)

Option	Description
Transport	The network transport to use for the connection. Valid transports are: **TCP/IP**, **Serial**, **SSH2**, and **SSL**.
Connection	The connection method to be used. Advanced connection options can be configured via the button.
Emulation	Emulation types are: **hp70092**, **IBM 3151**, **IBM3270 Display**, **IBM3270 Printer**, **IBM5250 Display**, **IBM5250 Printer**, **MD Prism**, **TA6530**, **VT Series**, and **Wyse**.

Table 10-3 TeemTalk Session Wizard > Page 2

Option	Description
Emulation Printer	The HP TeemTalk emulation printer settings.
Auto Logon	The HP TeemTalk auto login settings.
Key Macros	The HP TeemTalk key macros settings.
Mouse Actions	The HP TeemTalk mouse actions settings.
Soft Buttons	The HP TeemTalk soft buttons settings.
Attributes	The HP TeemTalk attributes settings.
Auxiliary Ports	The HP TeemTalk auxiliary ports settings.
Hotspots	The HP TeemTalk hotspots settings.

Table 10-4 TeemTalk Session Wizard > Page 3

Option	Description
Preferences	Displays the preferences shown in Table 10-5 TeemTalk Session Wizard > Page 3 > Preferences on page 52.
Start session connected	Starts the session connected.
Show Status Bar	Displays the status bar for this connection.

Table 10-5 TeemTalk Session Wizard > Page 3 > Preferences

Option	Description
Show Configuration Bar	Displays the Configuration Bar.
Save Current Window Position	Saves current window's size and position when you click **Save Preferences**. It will be restored on the next system launch. **NOTE:** Click **Save Preferences** each time you change the window size or position to save the new values.
Run in Full Screen Mode	Select to make the window full screen and remove the frame, soft buttons, menu, and configuration bars. **NOTE:** This option does not become effective until the next system launch and overrides the **Show Configuration Bar** and **Save Current Window Position** options.

Table 10-5 TeemTalk Session Wizard > Page 3 > Preferences (continued)

Option	Description
Browser Command	In the box, type the command that runs your web browser, such as: `/ display html links Firefox`
Command Line Start Up Options	Use to specify an alternate location for the startup options. **NOTE:** For specific information on HP TeemTalk Command Line Startup Options, see the *HP TeemTalk Terminal Emulator User Guide*.

Table 10-6 TeemTalk Session Wizard > Page 4

Component	Description
Summary Session Information	Displays a summary of the session that is to be created.

XDMCP connection settings

XDMCP is a way to connect directly to remote X servers. X servers are used to display graphics on most UNIX-like operating systems, such as Linux, Berkeley Software Distribution (BSD), and Hewlett Packard UniX (HP-UX).

The following table describes the settings available in the XDMCP Connection Manager. These settings are connection-specific and apply to only the XDMCP connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 10-7 XDMCP Connection Manager > Configuration

Option	Description
Name	The connection name.
Type	The XDMCP connection type. Valid options are: **chooser**, **query**, and **broadcast**.
Address	This value is required if the **Type** value is set to **query**.
Use font server	Use a remote X font server instead of locally installed fonts.
Font server	Font server is not enabled unless the **Use font server** option is checked.
Configure display	Click to set the display configuration for the connection. If you do not set this configuration, the default configuration will be used.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the XDMCP Connection Manager.

SSH connection settings

Secure Shell (SSH) is the most common way to gain remote command line access to UNIX-like operating systems, such as Linux, BSD, and HP-UX. SSH is also encrypted.

The following table describes the settings available in the Secure Shell Connection Manager. These settings are connection-specific and apply to only the SSH connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 10-8 Secure Shell Connection Manager > Configuration

Option	Description
Name	The connection name.
Address	The IP address of the remote system.
Port	The remote port to use for the connection.
User name	The username to use for the connection.
Run application	The application to run to make the connection.
Compression	Select this option if you want to compress the data sent between the server and thin client.
X11 connection forwarding	If the server has an X server on it, select this option to allow the user to open user interfaces from the SSH session and display them locally on the thin client.
Force TTY allocation	Select this option and specify a command to initiate a temporary session to run the command. Once the command has completed, the session will terminate. If no command is specified, then the session will run normally as if the option were not selected.
Foreground color	The default color of the text in the SSH session.
Background color	The default color of the background in the SSH session.
Font	Valid options are: **7X14**, **5X7**, **5X8**, **6X9**, **6X12**, **7X13**, **8X13**, **8X16**, **9X15**, **10X20**, and **12X24**.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the SSH Connection Manager.

Telnet connection settings

Telnet is an older method of gaining remote command line access. It is not encrypted.

The following table describes the settings available in the Telnet Connection Manager. These settings are connection-specific and apply to only the Telnet connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 10-9 Telnet Connection Manager > Configuration

Option	Description
Name	The name of the connection.
Address	The IP address of the remote system.
Port	The port to use on the remote system.
Foreground color	The foreground color.
Background color	The background color.
Font	Valid options are: **7X14**, **5X7**, **5X8**, **6X9**, **6X12**, **6X13**, **7X13**, **8X13**, **8X16**, **9X15**, **10X20**, and **12X24**.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the Telnet Connection Manager.

Custom connection settings

If you would like to install a custom Linux application, you can use the Custom connection to allow you to open this application through the connection manager.

The following table describes the settings available in the Custom Connection Manager. These settings are connection-specific and apply to only the Custom connection you are currently configuring.

NOTE: For information about how to locate these settings, see Using the Connection Manager controls on page 6.

Table 10-10 Custom Connection Manager > Configuration

Option	Description
Name	The connection name.
Enter command to run	The command to run to make the remote connection.

NOTE: See Common connection settings on page 25 for information about the settings available on the final page of the Custom Connection Manager.

11 HP Smart Client Services

HP Smart Client Services is a set of server-side tools that enable you to configure client profiles that can be distributed to large numbers of thin clients. This function is called Automatic Update.

Clients detect an Automatic Update server upon startup and configure themselves accordingly. This simplifies device installation and maintenance.

- Supported operating systems
- Prerequisites for HP Smart Client Services
- Obtaining HP Smart Client Services
- Viewing the Automatic Update website
- Creating an Automatic Update profile
- Updating clients

Supported operating systems

HP Smart Client Services supports the following operating systems:

- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2003
- Windows Vista
- Windows XP

NOTE: The installer is 32-bit only, although it is supported on both the 32-bit and 64-bit versions of the Windows operating system.

Prerequisites for HP Smart Client Services

Before installing HP Smart Client Services, verify the configuration and installation status of the following components:

- **Internet Information Services (IIS)**
- **.NET Framework 3.5**

For information about installing or enabling these components on the operating system that you are using for the server, go to http://www.microsoft.com.

Obtaining HP Smart Client Services

To obtain HP Smart Client Services:

1. Go to http://www.hp.com/support.
2. Search for the thin client model. HP Smart Client Services can be found under the **Software - System Management** category of the **Drivers, Software & Firmware** page.

Viewing the Automatic Update website

1. On the server desktop, select **Start > Control Panel**, and then click **Administrative Tools**.
2. Double-click **Internet Information Services (IIS) Manager**.
3. In the left pane of the IIS Manager, expand the following items:

   "Server name" > Sites > HP Automatic Update > auto-update

NOTE: The physical location where the Automatic Update files are stored is as follows:

```
C:\Program Files (x86)\Hewlett-Packard\HP Smart Client Service\auto-update
```

Creating an Automatic Update profile

This section describes how to create an Automatic Update profile for a single MAC address.

1. Obtain the MAC address of the client using the system info. For example, the following steps use the MAC address `00fcab8522ac`.
2. Use the Profile Editor to create or modify a client profile (see Using the Profile Editor on page 60) until you are ready to save the client profile.
3. In the **Profile Editor**, click the **Finish** link in the left-hand pane to access the **Current profile** pane.
4. Click **Save profile as** to save the client profile as the following:

   ```
   C:\Program Files (x86) Hewlett-Packard\HP Smart Client Service\auto-update\PersistentProfile\MAC\00fcab8522ac.xml
   ```

5. Click the **Finish** button in the **Current profile** pane to exit the Profile Editor.
6. Reboot the client that uses the specified MAC address to initiate the Automatic Update process.

Updating clients

- Using the broadcast update method
- Using the DHCP tag update method
- Using the DNS alias update method
- Using the manual update method

Using the broadcast update method

To do a broadcast update, plug the client into the same network as the update server. A broadcast update relies on HP Smart Client Services, which works with IIS to automatically push updates to the client.

NOTE: Broadcast updates work only if the client is on the same subnet as the server.

TIP: To verify that the broadcast updates are working, run the Profile Editor and make some changes. Connect the thin client and verify that it has downloaded the new profile. If it has not, see Troubleshooting on page 66.

Using the DHCP tag update method

On the Windows Server 2003 and Windows Server 2008 systems, DHCP tagging enables a client to update. Use this method to update specific clients; however, if you have only one or two clients to update, consider using the manual update method instead. Otherwise, HP recommends the broadcast update method.

Example of performing DHCP tagging

The example in this section shows how to perform DHCP tagging on a Windows 2008 R2 Server.

NOTE: To use DHCP tagging, see your DHCP server documentation.

1. On the server desktop, select **Start > Administrative Tools > DHCP**.
2. In the left pane of the **DHCP** screen, click the domain where the clients are connected.
3. In the right pane of the **DHCP** screen, expand and right-click **IPv4**, and then click **Set Predefined Options**.
4. In the **Predefined Options and Values** dialog, click **Add**.
5. In the **Option Type** box, configure the options as described in the following table.

Table 11-1 Example DHCP tagging options

Field	Entry
Name	Type `auto-update`.
Data Type	Select **String**.
Code	Type `137`.
Description	Type `HP Automatic Update`.

6. Click **OK**.
7. In the **Predefined Options and Values** dialog, under **Value > String**, type the update server address in the format of the following example:

   `http://auto-update.dominio.com:18287/auto-update`

8. To complete the setup, click **OK**. DHCP tagging is now ready to update specific clients.

Using the DNS alias update method

During system startup, Automatic Update attempts to resolve the DNS alias **auto-update**. If that host name resolves, it attempts to check for updates at **http://auto-update:18287**. This update method enables clients to access a single update server across the entire domain, thus simplifying management for deployments with many subnets and DHCP servers.

To configure the DNS alias update method:

- Change the hostname of the server hosting HP Smart Client Services to **auto-update** or create a DNS alias of **auto-update** for that server.

Using the manual update method

Use the manual update method to connect a client to a specific server for an update. Also, use this method if you want to test an update on a single client before pushing the update to many clients, or if you have specific updates to be installed on only one or two clients.

NOTE: Be sure you specify the hostname of the manual server in the profile that you are updating to. Otherwise the settings reset to automatic when downloading the profile. Use the **Profile Editor** to modify these settings at root/auto-update.

NOTE: If multiple clients require specific updates, use the DHCP tagging method.

If no update segregation is required, use the broadcast update method.

Performing a manual update

1. Select **Management > Automatic Update** in the Control Panel.
2. Select **Enable manual configuration**.
3. Set the **Protocol** as **http**.
4. In the **Server** field, type the update server hostname and port in this format: `<hostname>:18287`
5. In the **Path** field, type the following: `auto-update`
6. Select **Preserve Thin Client Configuration** if you want to preserve all previously configured settings.
7. Click **OK**, and then the client will pull the updates.

12 Using the Profile Editor

HP Smart Client Services contains the Profile Editor, which allows administrators to create client profiles and upload them to the Automatic Update server.

TIP: In addition to creating a new client profile, you can edit an existing profile that was exported using HP ThinState.

An HP ThinPro profile contains the connections, settings, and customizations that were configured using the Connection Manager and various Control Panel utilities. A profile is saved in a configuration file that is specific to the version of HP ThinPro in which it was created.

This section includes the following topics:

- Accessing the Profile Editor
- Loading a client profile
- Modifying a client profile
- Configuring a serial or parallel printer

NOTE: See Registry keys on page 80 for a comprehensive list and description of registry keys.

Accessing the Profile Editor

▲ Click **Start > All Programs > Hewlett-Packard > HP Automatic Update Server > Profile Editor**.

Loading a client profile

The Profile Editor will automatically load the default profile that was created during the HP Smart Client Services installation process. This is indicated by the `Profile.xml` link in the **Profile Editor** pane.

To load a profile:

1. In the **Profile Editor** pane, click **Profile.xml**.
2. Select the desired profile, and then click **Open**.

Modifying a client profile

Use the various screens in the Profile Editor to modify a client profile as discussed in the following topics:

- Selecting the platform of a client profile
- Selecting the connection type of a client profile
- Modifying the registry settings of a client profile
- Adding files to a client profile
- Saving the client profile

Selecting the platform of a client profile

Use the **Platform** link in the Profile Editor to access the **Platform** pane, which can be used to configure the following settings:

- Client software versions compatible with your hardware
- Optional client kits that provide additional registry settings

To set up the client profile platform:

1. In the **Platform** pane, under **Smart Zero Client versions > OS Build ID**, select an OS Build ID.

TIP: Be sure to create a different profile for each hardware type.

NOTE: If a client kit is installed, the additional registry settings are automatically displayed in the client kit box and the Registry pane.

2. Set the configuration to either **Standard** (ThinPro) or **Zero** (Smart Zero).

NOTE: For older image versions, this setting is greyed out and set to Zero automatically.

3. When complete, click **Next**.

Selecting the connection type of a client profile

Use the **Connection** link in the Profile Editor to access the **Remote Connection Server** pane, which can be used to set up a connection type for the client profile using the following procedure:

1. In the **Remote Connection Server** pane, under **Type**, choose the desired **Connection Type**.
2. Under **Server**, type the name or IP address of the server to be configured.
3. When complete, click **Next**.

Modifying the registry settings of a client profile

Use the **Registry** link in the Profile Editor to access the **Registry Editor**, which can be used to change default values in client profile settings using the following procedure:

1. Expand the folders in the **Registry settings** tree to locate the option to be changed.
2. Click the option, and then change the default value in the **Value** field.

Enabling or disabling menu items on clients

1. In the **Registry settings** tree, navigate to **root > zero-login > controls**.
2. Expand the folder for the menu item to be either enabled or disabled and click on the **authorized** setting.
3. Type the appropriate number in the **Value** field:
   - 0 (disable)
   - 1 (enable)

Enabling or disabling user configurations on clients

1. In the **Registry settings** tree, navigate to **root > users > user > apps**.
2. Expand the folder for the menu item to be either enabled or disabled and click on the **authorized** setting.
3. Type the appropriate number in the **Value** field:
   - 0 (disable)
   - 1 (enable)

Adding files to a client profile

Use the **Files** link in the Profile Editor to access the **Additional Configuration Files** pane, which can be used to add configuration files to be automatically installed on the client when the profile is installed. This is typically used for the following reasons:

- To add certificates
- To modify device settings when a registry setting for the change is unavailable
- To modify the behavior of the system by inserting custom scripts or modifying existing scripts

You can also specify a symbolic link that points to a file already installed on the client. Use this when the file needs to be accessed from more than one directory.

Adding a configuration file to a client profile

1. In the **Additional Configuration Files** pane, click **Add a file**.
2. Click **Import File**, locate the file to be imported, and then click **Open**.

   NOTE: Files can also be exported using the **Export File** button, if further details about the file are required.

3. In the **Path** field, set the path where the file will be installed on the client.
4. In the **File details** pane, set the **Owner**, **Group**, and **Permissions** fields to the appropriate values.

   NOTE: Typically, setting the owner and group as **root** and the permissions as **644** is satisfactory. If a special owner, group, or permissions are required, refer to standard Unix file permissions for guidelines on changing the file details.

5. Click **Save** to finish adding the configuration file to the client profile.

NOTE: A file installed as part of a profile will automatically overwrite any existing file on the file system at the destination path. Additionally, a second profile without the file attached will not revert previously attached files. All files that have been installed through profile attachment are permanent and must be reverted manually or through a factory reset.

Adding certificates to a client profile

Client profiles automatically include certificates that are imported to a standard client certificate store for the following applications:

- VMware Horizon View, Citrix, RDP
- Automatic Update

- HP Smart Client Services
- Web browser stores

To import other certificates to a client profile:

1. In the **Additional Configuration Files** pane, click **Add a file**.
2. Click **Import File**, locate the certificate, and then click **Open**.

   NOTE: The certificate should be formatted as a `.pem` or `.crt` file.

3. In the **Path** field, set the path to the following:

   `/usr/local/share/ca-certificates`

4. Click **Save** to finish adding the certificate to the client profile.
5. After installing the client profile, use the **Certificate Manager** to confirm that the certificate was properly imported.

Adding a symbolic link to a client profile

1. In the **Additional Configuration Files** pane, click **Add a file**.
2. In the **Type** drop-down list, select **Link**.
3. In the **Symbolic link details** pane, set the **Link** field to the path of the desired file already installed on the client.
4. Click **Save** to finish adding the symbolic link.

Saving the client profile

1. In the **Profile Editor**, click the **Finish** link in the left-hand pane to access the **Current profile** pane.
2. Click **Save Profile** to save to the current client profile, or click **Save Profile As** to save as a new client profile.

   NOTE: If **Save Profile** is disabled, your client profile has not changed since the last time it was saved.

3. Click the **Finish** button in the **Current profile** pane to exit the Profile Editor.

Configuring a serial or parallel printer

Use the Profile Editor to set up the serial or parallel printer ports. A USB printer automatically maps when plugged in.

This section includes the following topics:

- Obtaining the printer settings
- Setting up printer ports
- Installing printers on the server

Obtaining the printer settings

Before configuring printer ports, obtain the printer's settings. If available, check the printer's documentation before going further. If it is not available, follow these steps:

1. For most printers, press and hold the **Feed** button while turning the device on.
2. After a few seconds, release the **Feed** button. This allows the printer to enter a test mode and print the required information.

TIP: You might need to turn the printer off to cancel the Test mode or press **Feed** again to print a diagnostic page.

Setting up printer ports

1. In the **Profile Editor**, select **Registry**, and then enable the **Show all settings** checkbox.
2. Enable printer port mapping for your connection type:
   - Citrix—No action is required.
   - RDP—Navigate to **root > ConnectionType > freerdp**. Right-click on the **connections** folder, select **New connection**, and then click **OK**. Set the **portMapping** registry key to `1` to enable printer port mapping.
   - VMware Horizon View—Navigate to **root > ConnectionType > view**. Right-click on the **connections** folder, select **New connection**, and then click **OK**. Under the **xfreerdpOptions** folder, set the **portMapping** registry key to `1` to enable printer port mapping.
3. Navigate to **root > Serial**. Right-click the **Serial** folder, select **New UUID**, and then click **OK**.
4. Under the new directory, set the **baud**, **dataBits**, **flow**, and **parity** values to the ones obtained in Obtaining the printer settings on page 64.

   Set the **device** value to the port the printer will be plugged into. For example, the first serial port would be `/dev/ttyS0`, the second serial port would be `/dev/ttyS1`, and so on. For USB serial printers, use the format `/dev/ttyUSB#`, where `#` is the number of the port, starting with 0.

Installing printers on the server

1. On the Windows desktop, select **Start > Printers and Faxes**.
2. Select **Add Printer**, and then click **Next**.
3. Select **Local Printer attached to this Computer** and, if required, deselect **Automatically detect and install my Plug and Play printer**.
4. When completed, click **Next**.
5. In the menu, select a port.

NOTE: The port you need is in the section of ports labeled **TS###**, where ### is a number between 000–009, 033–044. The appropriate port depends on your hostname and the printer you want to install. For example, with a hostname of ZTAHENAKOS and a serial printer, select the port with **(ZTAHENAKOS:COM1)**. For a parallel printer, select **(ZTAHENAKOS:LPT1)**. The **TS###** is assigned by the server, so it will not be the same every time.

6. Select the manufacturer and driver for your printer.

TIP: If desired, use the driver disc **Windows Update** to install the driver.

NOTE: For basic or test printing, the **Generic Manufacturer** or **Generic/Text Only** printer usually works.

7. If prompted to keep the existing driver and it is known to work, keep it, and then click **Next**.
8. Assign a name to the printer. To use it as the default printer, select **Yes**, and then click **Next**.
9. To share the printer, select **Share name** and assign it a share name. Otherwise, click **Next**.
10. On the next page, you may request a test print. HP recommends this because it will verify the printer setup is correct. If it is not set up properly, review the settings and try again.

NOTE: If the client disconnects from the server, the printer will need to be set up again the next time the client connects.

13 Troubleshooting

This chapter discusses the following topics:

- Troubleshooting network connectivity
- Troubleshooting firmware corruption
- Troubleshooting Citrix password expiration
- Using system diagnostics to troubleshoot

Troubleshooting network connectivity

1. Ping the client server by doing the following:
   a. Click the System Information button on the taskbar, and then click on the **Net Tools** tab.
   b. Under **Select Tool**, select **Ping**.
   c. In the **Target Host** box, type the server address, and then click **Start Process**.

   If the ping is successful, the system will display the following output:

   ```
   PING 10.30.8.52 (10.30.8.52) 56(84) bytes of data.

   64 bytes from 10.30.8.52: icmp_seq-1 ttl=64 time=0.81 5 ms 64 bytes
   from 10.30.8.52: icmp_seq=2 ttl=64 time=0.735 ms
   ```

   If the ping is unsuccessful, the client might be disconnected from the network and experience a long delay with no system output.
2. If the client does not respond to the ping, do the following:
   a. Check the network cable and check the network settings in the Control Panel.
   b. Try pinging other servers or clients.
   c. If you can reach other network clients, verify that you typed the correct server address.
   d. Ping the server using the IP address instead of the domain name or vice-versa.
3. Check the system logs by doing the following:
   a. Click the System Information button on the taskbar, and then click on the **System Logs** tab.
   b. Check for any errors in the logs.
   c. If there is an error, then the **Server is not set up** notification appears. Verify that the server is set up properly and that HP Smart Client Services is running.

Troubleshooting firmware corruption

If the client beeps two times after it is powered on or does not appear to boot, then the device firmware may be corrupt. It is possible to resolve this by downloading the client image from http://www.hp.com, copying the image to a removable USB flash drive, and then booting the client from that flash drive.

Reimaging client device firmware

1. Download the image from http://www.hp.com.
2. Unpack the image to the path **C:\USBBoot**.
3. Format a USB flash drive.
4. Copy all the files from **C:\USBBoot** to the root of the USB flash drive.
5. Power off the client.
6. Insert the USB flash drive into the client.
7. Power on the client. The client will boot to the USB flash drive.
8. Follow the on-screen instructions to reimage the client.
9. When the reimage process completes, remove the USB flash drive and press Enter.

Troubleshooting Citrix password expiration

If users are not being prompted to change expired Citrix passwords, then make sure the XenApp Services site (PNAgent site) has the **Prompt** authentication method set to allow users to change expired passwords. If you allow users to change their passwords by connecting directly to the domain controller, then make sure the time of the client is in sync with the domain controller and use the full domain name (for example, `domain_name.com`) when entering the Citrix login credentials. For more information, see Citrix documentation.

Using system diagnostics to troubleshoot

System diagnostics take a snapshot of the client that can be used to help solve issues without physical access to the client. This snapshot contains log files from the BIOS information and the processes active at the time the system diagnostics were run.

TIP: Check the **Enable Debug Mode** box in the **System Logs** tab of the **About this client** screen to generate more information in the diagnostic report. This information may be requested by HP for troubleshooting. Because the system resets log files when it reboots, be sure to capture logs before a reboot.

Saving system diagnostic data

1. Insert a USB flash drive into the client.
2. Click the System Information button on the taskbar, and then click the **System Logs** tab.
3. Click **Diagnostic**, and then save the compressed diagnostic file **Diagnostic.tgz** to the USB flash drive.

Uncompressing the system diagnostic files

The system diagnostic file **Diagnostic.tgz** is compressed and will need to be uncompressed before you can view the diagnostic files.

Uncompressing the system diagnostic files on Windows-based systems

1. Download and install a copy of the Windows version of **7-Zip**.

NOTE: You may obtain a free copy of 7-Zip for Windows at http://www.7-zip.org/download.html.

2. Insert the USB flash drive that contains the saved system diagnostic file, and then copy **Diagnostic.tgz** to the desktop.
3. Right-click **Diagnostic.tgz** and select **7-zip > Extract files**.
4. Open the newly created folder named **Diagnostic** and repeat step 3 on **Diagnostic.tar**.

Uncompressing the system diagnostic files in Linux- or Unix-based systems

1. Insert the USB flash drive that contains the saved system diagnostic file, and then copy **Diagnostic.tgz** to the home directory.
2. Open a terminal and browse to the home directory.
3. On the command line, enter `tar xvfz Diagnostic.tgz`.

Viewing the system diagnostic files

The system diagnostic files are divided into the **Commands**, **/var/log**, and **/etc** folders.

Viewing files in the Commands folder

This table describes the files to look for in the **Commands** folder.

Table 13-1 Commands folder files

File	Description
demidecode.txt	This file contains information on the system BIOS and graphics.
dpkg_--list.txt	This file lists the packages installed at the time system diagnostics were run.
ps_-ef.txt	This file lists the active processes at the time system diagnostics were run.

Viewing files in the /var/log folder

The useful file in the **/var/log** folder is **Xorg.0.log**.

Viewing files in the /etc folder

The **/etc** folder contains the file system at the time the system diagnostics were run.

A USB updates

When USB updates are enabled (see Customization Center on page 18), you can use a USB flash drive to simultaneously install multiple add-ons and certificates, as well as deploy a profile.

To perform USB updates:

1. Place the desired files onto a USB flash drive.

   NOTE: The files can be placed in the root directory or in subfolders.

2. Connect the USB flash drive to the thin client.

   Updates are detected automatically and displayed in the **USB Update** dialog, in which you can search and view details about the detected updates.

3. Select the checkboxes next to the updates you want to install, and then click **Install**.

4. After installation, restart the thin client if prompted.

B BIOS tools

There are two kinds of BIOS tools for HP ThinPro:

- BIOS settings tool—Used to retrieve or modify BIOS settings
- BIOS flashing tool—Used to update the BIOS

BIOS settings tool

The following table describes the syntax for the BIOS settings tool.

Syntax	Description
`hptc-bios-cfg -G [options] [filename]`	Retrieves the current BIOS settings and saves them to the specified file so they can be viewed or modified (CPQSETUP.TXT by default).
`hptc-bios-cfg -S [options] [filename]`	Writes the BIOS settings from the specified file (CPQSETUP.TXT by default) to the BIOS.
`hptc-bios-cfg -h`	Displays a list of options.

BIOS flashing tool

The following table describes the syntax for the BIOS flashing tool.

Syntax	Description
`hptc-bios-flash [options] <ImageName>`	Flashes the BIOS with the specified BIOS image.
`hptc-bios-flash -h`	Displays a list of options.

C Resizing the flash drive partition

When a thin client running HP ThinPro is shipped from the factory, the image flashed on it has a size of 1 GB, regardless of the total size of the flash drive. This makes it easier to customize the image and deploy it to other clients that might have a smaller flash drive.

To use the entire space of the flash drive, you have to modify the partition size and expand the file system to take up that additional space. This can be accomplished using the `resize-image` script.

NOTE: When an image is deployed via HPDM, HP ThinState, or Automatic Update, the file system is automatically resized to use all available space on the flash drive.

The following table describes the syntax for the `resize-image` script.

Syntax	Description
`resize-image`	When called with no parameters, the script displays the current size of the partition and the amount of available space on the flash drive. The script prompts you to enter the target partition size and then confirm the change. The change takes effect after the next thin client restart. **NOTE:** It is not possible to decrease the partition size. The entered value must be larger than the current partition size.
`resize-image--size <size>`	Using this syntax, you can provide directly the target partition size as a parameter, and then confirm the change.

`resize-image--no-prompt`
—or—
`resize-image--no-prompt--size <size>`
	Using this syntax, the script runs automatically with no user interaction required.
	If no specific size is given as a parameter simultaneously, the partition size is increased to the maximum size.
	TIP: This non-interactive mode is useful for scripting and performing this operation from a remote administration tool like HP Device Manager.

D Customizing the Smart Zero login screen

Customizing the screen background

This section describes the common attributes and elements used in customizing the client login screen background.

There is one directory per connection type—plus a default style—that specifies the style elements of the connection's background image and login window style.

In a style directory, the file **bgConfig.rtf** specifies the elements in the desktop's background window. The syntax of the **bgConfig.rtf** file is in a stylesheet-like format with some or all of the elements described below. Each element begins with an element type and then a set of attributes surrounded by braces, such as in the following example:

```
global {

color: 666666; # Dark gray

padding: 20; # 20 pixels }
```

Any number of image or text elements can be specified. If any gradients are specified, only the last of them is used to color the desktop's background; otherwise, the color specified in the global section is used. Any line that begins with a number sign "#" is considered a comment and is ignored, as are blank lines. Text following a semicolon that begins with a "#" is also treated as a comment, such as the previous example.

Each element is assigned a set of attributes such as size, color, and position. Each attribute is specified by the attribute name, followed by a colon, followed by its values, followed by a semicolon, all on a single line. Some of these attributes are common to many element types.

The elements include:

- Common attributes
- Elements
- Image
- Text

Common attributes

Table D-1 Login Screen > Common Attributes > Name

Type	Description
Parameter	A string
Example	name: ItemName;
Default	
Use	Specifies a string to associate with the element. It is used only in debugging output, such as when a syntax or value error is found in attribute parsing.

Table D-2 Login Screen > Common Attributes > padding

Type	Description
Parameter	An absolute (pixel) or percentage value
Example	padding: 20;
Default	
Use	An object will be positioned on the screen as if the screen were smaller on all sides by the padding value. For example, if an element would normally be placed at 0,0 with a padding of 20, it would be placed at 20,20 instead. If specified in the global element, it will apply to all subsequent elements, leaving an empty gutter around the screen edge, unless those elements override the padding with their own padding value.

Table D-3 Login Screen > Common Attributes > color

Type	Description
Parameter	RRGGBB 6-digit hex value or rrr,ggg,bbb 0–255,0–255,0–255 form
Example	color: ff8800;
Default	255,255,255 (white)
Use	Specifies the color of the element

Table D-4 Login Screen > Common Attributes > alpha

Type	Description
Parameter	0–255 integer
Example	alpha: 127;
Default	255 (fully opaque)
Use	Specifies the opacity of the element. 255 is fully opaque; 0 is fully transparent. Elements are layered over the background in the order they are defined.

Table D-5 Login Screen > Common Attributes > size

Type	Description
Parameter	WWxHH, where WW is the width in absolute pixels or in a percentage of screen width and HH is the height in absolute pixels or in a percentage of the screen height.
Example	size: 256x128;
Default	The natural size of the element; for example, the pixel size of an image.
Use	Specifies the size of the element. Elements will be scaled to match the specified size.

Table D-6 Login Screen > Common Attributes > position

Type	Description
Parameter	XX,YY where XX and YY are positions in absolute pixels or in percentages of the screen width and height.
Example	position: 50%, 90%;
Default	0,0 (the upper left)
Use	Specifies the position of the element. See the **alignment** table as well.

Table D-7 Login Screen > Common Attributes > alignment

Type	Description
Parameter	[left I hcenter I right] [top I vcenterlbottom]
Example	alignment: left bottom;
Default	hcenter vcenter—the element is centered at the given position.
Use	The combination of position and alignment specify both an anchor point for the element and how the element is aligned relative to that anchor point. For example, with a position of 90%,70% and an alignment of right bottom, the element is positioned so that its right edge is at 90% of the width of the screen and its bottom edge is at 70% of the height of the screen.

Table D-8 Login Screen > Common Attributes > context

Type	Description
Parameter	[login I desktop I all]
Example	context: login;
Default	all
Use	Specifies whether the element should be shown only on the login screen for the protocol, on the desktop screen for the protocol (if any), or on both. Only some protocols (for example, Citrix XenDesktop) have a desktop screen.

Elements

Table D-9 Login Screen > Elements > Custom > Global

Type	Description
Use	Specifies the global background or padding values.
Common attributes recognized	**name, color, padding** • **color**—specifies the solid background color of the screen, if no gradients are specified

Table D-9 Login Screen > Elements > Custom > Global (continued)

Type	Description
	• **padding**—specifies the default padding for all subsequent elements

Table D-10 Login Screen > Elements > Custom > Gradient

Type	Description
Use	Specifies a full-screen gradient for use in the background.
Common attributes recognized	**name, context**

Table D-11 Login Screen > Elements > Custom > Type

Type	Description
Parameter	Specifies a full-screen gradient for use in the background.
Example	Type: linear;
Default	linear
Use	Linear gradients can be either horizontally oriented or vertically oriented; coordinates given in colors are a fraction of the width or height. Radial gradients are centered on the screen center; coordinates are a fraction of the distance to the screen edge (top and bottom or left and right).

Table D-12 Login Screen > Elements > Custom > Axis

Type	Description
Parameter	[height I width]
Example	axis: width;
Default	height
Use	For linear gradients, the axis specifies the direction of the gradient (top-to-bottom or left-to-right). For radial gradients, the axis specifies whether the radius of the gradient is half-screen height or half-screen width.

Table D-13 Login Screen > Elements > Custom > Metric

Type	Description
Parameter	[linear I squared]
Example	metric: linear;
Default	squared
Use	For radial gradients, the metric specifies whether the color interpolation between points is done with a dx2+dy2 distance

Table D-13 Login Screen > Elements > Custom > Metric (continued)

Type	Description
	calculation (squared) or the square root of number (linear). Squared interpolation is somewhat quicker to draw.

Table D-14 Login Screen > Elements > Custom > colors

Type	Description
Parameter	A space-separated list of [value,color] pairs, where the value is a 0.0–1.0 floating point fraction of the axis of measurement (for example, the width of the screen in a linear width-axis gradient) and the color is the color of the gradient at that point. The value runs top-to-bottom for vertical linear gradients; left-to-right for horizontal linear gradients; and center-to-edge for radial gradients. Colors are specified as either six-digit hex or three 0–255 comma-separated values.
Example	colors: 0.0,000000 0.5,996600 0.9,255,255,255;
Default	Not applicable
Use	Colors are interpolated along the linear or radial axis between the points and colors specified. If no values are given, the colors are assumed to be evenly spaced on the axis between 0.0 and 1.0. If the first fractional value is greater than 0.0, the first color will be used in the space between the screen edge and the first value. Likewise, if the last value is less than 1.0, the last color will be used between the last value and the screen edge. Values must be in increasing sorted values, though a value can be repeated for a sharp transition. For example, “0.0, CCCCCC 0.5,EEEEEE 0.5,660000 1.0,330000” in a vertical linear gradient would specify a gradient between light grays on the upper half and dark reds on the lower half.

Table D-15 Login Screen > Elements > Custom > dithered

Type	Description
Parameter	[true | false]
Example	dithered: true;
Default	false
Use	If a gradient shows signs of color banding, dithering will eliminate this visual artifact. Dithering is not supported for radial gradients with the squared metric.

Image

Table D-16 Login screen > Image

Type	Description
Use	Specifies an image to overlay a portion of the background.

Table D-16 Login screen > Image (continued)

Type	Description
Common attributes recognized	name, size, alpha, position, alignment, context
Common attributes	See the tables following.

Table D-17 Login screen > Custom Attributes > Source

Type	Description
Parameter	File path
Example	source: /writable/misc/Company_logo.png;
Default	Not applicable
Use	Specifies the absolute pathname to the image file. Many formats are supported; for example, png, jpg,and gif. The image may have transparent regions.

Table D-18 Login screen > Custom Attributes > Proportional

Type	Description
Parameter	[true | false]
Example	proportional: false;
Default	true
Use	When true, if the image needs to be scaled, its aspect ratio will be maintained to fit within the rectangle specified. When false, non-proportional scaling is done to make the image exactly fit the specified size.

Text

Table D-19 Login screen > Text

Type	Description
Use	Specifies a string of text to lay over the background
Common attributes recognized	name, size, color, alpha, position, alignment, context
Common attributes	See the tables below.

Table D-20 Login screen > Text > text-locale

Type	Description
Parameter	Localized text
Example	text-de_DE: Dieser Text is in Deutsch.;

Table D-20 Login screen > Text > text-locale (continued)

Type	Description
Default	Not applicable
Use	When in the matching locale, this text will be used for the string. The supported text strings are as follows: • de_DE (German) • en_US (English) • es_ES (Spanish) • fr_FR (French) • ja_JP (Japanese) • zh_CN (Simplified Chinese) NOTE: The file encoding is UTF-8.

Table D-21 Login screen > Text > text

Type	Description
Parameter	Default text text:
Example	This will be shown on the screen.;
Default	Not Applicable
Use	If no matching localized text is specified, this text string will be used instead. NOTE: The text rendering engine does not support HTML-style markup.

Table D-22 Login screen > Text > font-locale

Type	Description
Parameter	locale-specific fontName
Example	font-ja_JP: kochi-gothic;
Default	Not applicable
Use	When in the matching locale, this font will be used when the string is rendered. See the description for text-locale previous. The name must match one of the fonts under **/usr/share/fonts/ truetype**. For Japanese text, it might be necessary to select kochi-gothic; for Simplified Chinese text, u mi ng.

Table D-23 Login screen > Text > font

Type	Description
Parameter	fontName
Example	font: DejaVuSerif-Bold

Table D-23 Login screen > Text > font (continued)

Type	Description
Default	; DejaVuSerif
Use	If no matching localized font is specified, this font will be used instead. The name must match one of the fonts under **/usr/share/fonts/truetype**.

Table D-24 Login screen > Text > font-size

Type	Description
Parameter	Pixels (for example, 20) or percentage of the screen height (for example, 5%) or points (for example, 12pt)
Example	font-size: 12pt;
Default	Not applicable
Use	Specifies the default size of the font. The text may be further scaled if size, max-width, and/or max-height are specified.

Table D-25 Login screen > Text > max-width

Type	Description
Parameter	Size in pixels or in a percentage of the screen width
Example	max-width: 90%;
Default	Not applicable
Use	If the string would otherwise turn out to be wider than the size given, it is scaled down to fit within the width specified.

Table D-26 Login screen > Text > max-height

Type	Description
Parameter	Size in pixels or in a percentage of screen height.
Example	max-height: 64;
Default	Not applicable
Use	If the text would otherwise turn out to be taller than the size given, it is scaled down to fit the height specified.

E Registry keys

The tables in this appendix describe the paths, functions, and options for the registry keys of HP ThinPro.

The values of these registry keys can be modified in several different ways:

- Using a **_File and Registry** task in HPDM
- Using the Registry Editor component of the Profile Editor and then deploying the new profile
- Using the Registry Editor in the client user interface, which is available by typing `regeditor` in the X Terminal.

NOTE: Some registry keys might apply to the ThinPro or Smart Zero configuration only.

Registry keys are organized into the following high-level folders:

- root > Audio
- root > CertMgr
- root > ConnectionManager
- root > ConnectionType
- root > DHCP
- root > Dashboard
- root > Display
- root > Network
- root > SCIM
- root > Serial
- root > SystemInfo
- root > TaskMgr
- root > USB
- root > auto-update
- root > background
- root > config-wizard
- root > desktop
- root > entries
- root > keyboard
- root > logging
- root > mouse
- root > screensaver

- root > security
- root > sshd
- root > time
- root > touchscreen
- root > translation
- root > usb-update
- root > users
- root > vncserver

root > Audio

Table E-1 root > Audio

Registry key	Description
root/Audio/AdjustSoundPath	Sets the full path to the sound played when the playback volume is changed via the volume controls.
root/Audio/OutputMute	If set to 1, the internal speaker and headphone jack are muted.
root/Audio/OutputScale	Sets the volume scale for the internal speaker and headphone jack, ranging from 1 to 400.
root/Audio/OutputScaleAuto	If set to 1, the OutputScale value will be set automatically based on the thin client model.
root/Audio/OutputVolume	Sets the volume for the internal speaker and headphone jack, ranging from 1 to 100.
root/Audio/PlaybackDevice	Sets the device to use for playback.
root/Audio/RecordDevice	Sets the device to use for capture.
root/Audio/RecordMute	If set to 1, the microphone jack is muted.
root/Audio/RecordScale	Sets the volume scale for the microphone jack, ranging from 1 to 400.
root/Audio/RecordScaleAuto	If set to 1, the RecordScale value will be set automatically based on the thin client model.
root/Audio/RecordVolume	Sets the volume for the microphone jack, ranging from 1 to 100.
root/Audio/VisibleInSystray	If set to 1, a speaker icon is visible in the system tray.

root > CertMgr

This registry category is used internally and does not have any user-defined entries.

root > ConnectionManager

Table E-2 root > ConnectionManager

Registry key	Description
root/ConnectionManager/customLogoPath	
root/ConnectionManager/defaultConnection	To properly launch a connection on startup, this must be set to a valid connection using the format <type>:<label> like in the following example: xen:Default Connection
root/ConnectionManager/minHeight	
root/ConnectionManager/minWidth	
root/ConnectionManager/splashLogoPath	Sets the full path to the image displayed while a connection is loading.
root/ConnectionManager/useKioskMode	
root/ConnectionManager/useSplashOnConnectionStartup	If set to 1, the image set by splashLogoPath is enabled. By default, this is enabled for ThinPro and disabled for Smart Zero.

root > ConnectionType

root > ConnectionType > custom

Table E-3 root > ConnectionType > custom

Registry key	Description
root/ConnectionType/custom/authorizations/user/add	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/custom/authorizations/user/general	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/custom/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/custom/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/custom/connections/<UUID>/authorizations/user/edit	If set to 1, a standard user has permission to modify the connection settings for this connection.
root/ConnectionType/custom/connections/<UUID>/authorizations/user/execution	If set to 1, a standard user has permission to execute this connection.
root/ConnectionType/custom/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/custom/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when autoReconnect is set to 1.

Table E-3 root > ConnectionType > custom (continued)

Registry key	Description
root/ConnectionType/custom/connections/<UUID>/autostart	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/custom/connections/<UUID>/autostartDelay	Sets the amount of time in seconds to wait before starting the connection after the system boots. The default of 0 will cause the connection to start immediately. This setting only takes effect when autostart is set to 1.
root/ConnectionType/custom/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/custom/connections/<UUID>/command	Sets the main command for the custom connection to execute.
root/ConnectionType/custom/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/custom/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/custom/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/custom/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to Default Connection and does not display in the UI.
root/ConnectionType/custom/connections/<UUID>/startMode	If set to the default focus and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/custom/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/custom/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.

Table E-3 root > ConnectionType > custom (continued)

Registry key	Description
root/ConnectionType/custom/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/custom/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/custom/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/custom/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/custom/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/custom/coreSettings/serverRequired	Sets whether a server name or address is `unused`, `optional`, or `required` for this connection type.
root/ConnectionType/custom/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/custom/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by `appName`. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/custom/gui/CustomManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/gui/CustomManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/gui/CustomManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect	Controls the state of the **Auto reconnect** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/autostart	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

Table E-3 root > ConnectionType > custom (continued)

Registry key	Description
root/ConnectionType/custom/gui/CustomManager/widgets/command	Controls the state of the **Enter command to run** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/fallBackConnection	Controls the state of the **Fallback Connection** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/hasDesktopIcon	Controls the state of the **Show icon on desktop** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/label	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/waitForNetwork	Controls the state of the **Wait for network before connecting** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.

root > ConnectionType > firefox

Table E-4 root > ConnectionType > firefox

Registry key	Description
root/ConnectionType/firefox/authorizations/user/add	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/firefox/authorizations/user/general	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/address	Sets the URL or IP address to connect to.
root/ConnectionType/firefox/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/firefox/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/edit	If set to 1, a standard user has permission to modify the connection settings for this connection.

Table E-4 root > ConnectionType > firefox (continued)

Registry key	Description
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/execution	If set to 1, a standard user has permission to execute this connection.
root/ConnectionType/firefox/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/firefox/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when autoReconnect is set to 1.
root/ConnectionType/firefox/connections/<UUID>/autostart	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/firefox/connections/<UUID>/autostartDelay	Sets the amount of time in seconds to wait before starting the connection after the system boots. The default of 0 will cause the connection to start immediately. This setting only takes effect when autostart is set to 1.
root/ConnectionType/firefox/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/firefox/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/connections/<UUID>/enablePrintDialog	If set to 1, the Print dialog in the web browser can be used.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/firefox/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/firefox/connections/<UUID>/fullscreen	If set to 1, the web browser will start in full screen. If kioskMode is disabled, the browser UI is accessible in full screen mode.
root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/kioskMode	If set to 1, the web browser will launch in Kiosk Mode, meaning that the web browser will start in full screen (even if fullscreen is set to 0) and the browser UI is inaccessible.
root/ConnectionType/firefox/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to Default Connection and does not display in the UI.
root/ConnectionType/firefox/connections/<UUID>/startMode	If set to the default focus and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.

Table E-4 root > ConnectionType > firefox (continued)

Registry key	Description
root/ConnectionType/firefox/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/firefox/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/firefox/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/firefox/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/firefox/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/firefox/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/firefox/coreSettings/restartIdleTime	Sets the time in minutes before the web browser restarts when the system is not receiving user input. If set to 0, restart is disabled.
root/ConnectionType/firefox/coreSettings/serverRequired	Sets whether a server name or address is `unused`, `optional`, or `required` for this connection type.
root/ConnectionType/firefox/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/firefox/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/firefox/general/enableUserChanges	If set to 1, the settings configured in the Firefox Preferences dialog will be saved after each session.

Table E-4 root > ConnectionType > firefox (continued)

Registry key	Description
root/ConnectionType/firefox/gui/FirefoxManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/gui/FirefoxManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/gui/FirefoxManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Controls the state of the **URL** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Controls the state of the **Auto reconnect** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog	Controls the state of the **Enable print dialog** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection	Controls the state of the **Fallback Connection** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon	Controls the state of the **Show icon on desktop** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/kioskMode	Controls the state of the **Enable kiosk mode** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/label	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

Table E-4 root > ConnectionType > firefox (continued)

Registry key	Description
root/ConnectionType/firefox/gui/FirefoxManager/widgets/startMode	Controls the state of the **Enable full screen** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/waitForNetwork	Controls the state of the **Wait for network before connecting** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.

root > ConnectionType > freerdp

Table E-5 root > ConnectionType > freerdp

Registry key	Description
root/ConnectionType/freerdp/authorizations/user/add	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/freerdp/authorizations/user/general	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/ExtraArgs	Specifies extra arguments for the xfreerdp client. Run xfreerdp --help from an X terminal to see all available arguments.
root/ConnectionType/freerdp/connections/<UUID>/SingleSignOn	
root/ConnectionType/freerdp/connections/<UUID>/address	Sets the hostname or IP address to connect to.
root/ConnectionType/freerdp/connections/<UUID>/application	Specifies an alternate shell or application to run.
root/ConnectionType/freerdp/connections/<UUID>/attachToConsole	
root/ConnectionType/freerdp/connections/<UUID>/audioLatency	Sets the average milliseconds of offset between the audio stream and the display of corresponding video frames after decoding.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/edit	If set to 1, a standard user has permission to modify the connection settings for this connection.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/execution	If set to 1, a standard user has permission to execute this connection.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the

Table E-5 root > ConnectionType > freerdp (continued)

Registry key	Description
	connection to reconnect immediately. This setting only takes effect when `autoReconnect` is set to 1.
`root/ConnectionType/freerdp/connections/<UUID>/autostart`	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
`root/ConnectionType/freerdp/connections/<UUID>/autostartDelay`	Sets the amount of time in seconds to wait before starting the connection after the system boots. The default of 0 will cause the connection to start immediately. This setting only takes effect when `autostart` is set to 1.
`root/ConnectionType/freerdp/connections/<UUID>/certificateCheck`	If set to 1, certificate checks are enabled. The certificate of the RDP server is checked for validity and for name-matching between the server name provided and the server name stored in the certificate.
`root/ConnectionType/freerdp/connections/<UUID>/clipboardExtension`	If set to 1, clipboard functionality is enabled between different RDP sessions and between RDP sessions and the local system.
`root/ConnectionType/freerdp/connections/<UUID>/compression`	If set to 1, compression of RDP data sent between the client and the server is enabled.
`root/ConnectionType/freerdp/connections/<UUID>/dependConnectionId`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/freerdp/connections/<UUID>/directory`	Specifies the startup directory where an alternate shell application is executed.
`root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX`	If set to 1, multimedia redirection is disabled if a valid RemoteFX session is established.
`root/ConnectionType/freerdp/connections/<UUID>/domain`	Sets the default domain to supply to the remote host during login. If a domain is not specified, the default domain for the remote host will be used.
`root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/key`	Sets the name of an extra environment variable for use with the connection.
`root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/value`	Sets the value of an extra environment variable for use with the connection.
`root/ConnectionType/freerdp/connections/<UUID>/fallBackConnection`	Sets the fallback connection via its UUID.
`root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount`	Sets the number of video frames the server can push without waiting for acknowledgement from the client. Lower numbers result in a more responsive desktop but lower frame rate. If set to 0, frame acknowledgement is not used in the client-server interactions.
`root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress`	Sets the RD Gateway server name or address.
`root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain`	Sets the default domain to supply to the RD Gateway during login. Usually, this setting is used with kiosk-style applications where a generic user name is used to login. If `gatewayUsesSameCredentials` is to 1, this value is disabled.
`root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled`	If set to 1, RD Gateway is expected to be used.

Table E-5 root > ConnectionType > freerdp (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword	Sets the default password to supply to the RD Gateway during login. This value is usually encrypted. Usually, this setting is used with kiosk-style applications where a generic user name is used to login. If gatewayUsesSameCredentials is to 1, this value is disabled.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPort	Sets the port number to use when contacting the RDP server. This value can be left empty. The most common value is 443.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUser	Sets the default user name to supply to the RD Gateway during login. Usually, this setting is used with kiosk-style applications where a generic user name is used to login. If gatewayUsesSameCredentials is to 1, this value is disabled.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUsesSameCredentials	If set to 1, the same credentials that are used to connect to the final server are used to connect to the RD Gateway.
root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to Default Connection and does not display in the UI.
root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo	This value is the load balancing cookie sent for brokering purposes to the server upon connection and corresponds to the loadbalanceinfo field in the .rdp file. By default, the value is empty.
root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection	If set to 1, the local non-USB storage partitions are redirected to the remote host via the Storage extension. If set to 0, the extension is disabled for non-USB storage partitions that are not used by HP ThinPro.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/domain	Shows the **Domain** field in the login dialog for the connection.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/password	Shows the **Password** field in the login dialog for the connection.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/rememberme	Shows the **Remember me** checkbox in the login dialog for the connection.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/showpassword	Shows the **Show password** button in the login dialog for the connection.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/smartcard	Shows the **Smart card login** checkbox in the login dialog for the connection. This checkbox might not appear if no smart card is detected, even if this option is enabled.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/username	Shows the **User Name** field in the login dialog for the connection.
root/ConnectionType/freerdp/connections/<UUID>/mouseMotionEvents	If set to 0, mouse motion events are not sent to the server. This can prevent some user feedback such as tooltips from functioning properly.
root/ConnectionType/freerdp/connections/<UUID>/offScreenBitmaps	If set to 0, off-screen bitmaps are disabled. This can increase performance slightly but will cause blocks of the screen to

Table E-5 root > ConnectionType > freerdp (continued)

Registry key	Description
	update asynchronously, causing screen transitions to update non-uniformly.
root/ConnectionType/freerdp/connections/<UUID>/password	Sets the default password to supply to the remote host during login. This value will be encrypted. Generally, this setting is used for kiosk-style applications where a generic password is used for login.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagDesktopComposition	If set to 1, desktop composition (such as translucent borders) is allowed if supported by the server. Turning off desktop composition can improve performance for low-bandwidth connections. Generally, this only affects RemoteFX. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagFontSmoothing	If set to 1, font smoothing is allowed if supported by the server and enabled. Turning off font smoothing can improve performance on low-bandwidth connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorSettings	If set to 1, cursor blinking is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorShadow	If set to 1, mouse cursor shadows are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoMenuAnimations	If set to 1, menu animations are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoTheming	If set to 1, user interface themes are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWallpaper	If set to 1, the desktop wallpaper is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWindowDrag	If set to 1, full-content window dragging is disabled, which can improve performance on low-bandwidth RDP connections. The window outline is used instead. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/port	Sets the port number to use when contacting the RDP server. This can be left empty. The most common value is 3389.
root/ConnectionType/freerdp/connections/<UUID>/portMapping	If set to 1, all serial and parallel ports are redirected to the remote host via the `Ports` extension. If set to 0, the extension is disabled.
root/ConnectionType/freerdp/connections/<UUID>/printerMapping	If set to 1, all printers defined locally via CUPS are redirected to the remote host via the `Printers` extension. If set to 0, the extension is disabled. If set to 2, the USB printers are redirected as configured in the USB Manager.
root/ConnectionType/freerdp/connections/<UUID>/rdpEncryption	If set to 1, standard RDP encryption is used to encrypt all data between the client and the server.

Table E-5 root > ConnectionType > freerdp (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/remoteApp	Sets the name of an available application to run in Remote Application Integrated Locally (RAIL) mode.
root/ConnectionType/freerdp/connections/<UUID>/remoteFx	If set to 1, RemoteFX is used if available.
root/ConnectionType/freerdp/connections/<UUID>/seamlessWindow	If set to 1, window decorations are disabled. This can be desirable in a multi-monitor configuration to allow the connection to be set to the size of the primary monitor.
root/ConnectionType/freerdp/connections/<UUID>/securityLevel	Sets the certificate security level. If set to 0, all connections are allowed. If set to 1, remembered hosts are checked and a warning dialog is shown if verification is not passed. If set to 2, remembered hosts are not checked and a warning dialog is shown if verification is not passed. If set to 3, all insecure connections are refused.
root/ConnectionType/freerdp/connections/<UUID>/sendHostname	Sets the client hostname that is sent to the remote host. If left blank, the system hostname is sent. The registry key root/ConnectionType/freerdp/general/sendHostname must be set to hostname for this key to be used.
root/ConnectionType/freerdp/connections/<UUID>/smartcard	If set to 1, local smartcard authentication to the remote host is allowed. Currently, this will disable Network Level Authentication (NLA).
root/ConnectionType/freerdp/connections/<UUID>/sound	If set to 1, the playback and recording devices are redirected to the remote host via the Audio extension. If set to 0, the extension is disabled. If set to 2, the USB audio devices are redirected as configured in the USB Manager. Generally, HP recommends setting this value to 1 so that high-level audio redirection is used. This will improve audio quality and ensure that client audio redirected via other extensions (such as Multimedia Redirection) matches local audio settings.
root/ConnectionType/freerdp/connections/<UUID>/startMode	If set to the default focus and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/freerdp/connections/<UUID>/timeoutError	Sets the number of milliseconds to wait after losing the connection before giving up on reconnecting with the server. If set to 0, reconnection is attempted forever.
root/ConnectionType/freerdp/connections/<UUID>/timeoutRecovery	Sets the number of milliseconds to wait after losing the connection for networking to recover without trying a forced reconnect.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarning	Sets the number of milliseconds to wait after losing the connection before warning the user that the connection has been lost.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarningDialog	If set to 1, when an end-to-end connection drop is detected, a dialog is displayed and the screen will turn grayscale. Otherwise, messages are written to the connection log and the session freezes.
root/ConnectionType/freerdp/connections/<UUID>/timeoutsEnabled	If set to 1, end-to-end connection health checks are done.

Table E-5 root > ConnectionType > freerdp (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/usbMiscRedirection	If set to 0, redirection is disabled for all other USB devices except those handled by sound, printerMapping, portMapping, usbStorageRedirection, and localPartitionRedirection. If set to 2, all other USB devices are redirected to the remote host as configured in the USB Manager.
root/ConnectionType/freerdp/connections/<UUID>/usbStorageRedirection	If set to 1, USB storage devices are redirected to the remote host via the Storage extension. If set to 0, the extension is disabled. If set to 2, USB storage devices are redirected as configured in the USB Manager.
root/ConnectionType/freerdp/connections/<UUID>/username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.
root/ConnectionType/freerdp/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/freerdp/connections/<UUID>/windowMode	If set to Remote Application, RDP will run in Remote Application Integrated Locally (RAIL) mode. This requires that the remote app server allows a nominated application to run as a remote application. The application will be displayed in a separate window within the desktop environment, making it look as the application is part of the local system. Also see the remoteApp registry key. If set to Alternate Shell, a non-standard shell is invoked. Also see the application and directory registry keys.
root/ConnectionType/freerdp/connections/<UUID>/windowSizeHeight	
root/ConnectionType/freerdp/connections/<UUID>/windowSizePercentage	
root/ConnectionType/freerdp/connections/<UUID>/windowSizeWidth	
root/ConnectionType/freerdp/connections/<UUID>/windowType	
root/ConnectionType/freerdp/connections/<UUID>/xkbLayoutId	Sets an XKB layout ID for bypassing the system keyboard. To see the list of available IDs, enter the following command in an X terminal: xfreerdp --kbd-list.
root/ConnectionType/freerdp/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning	If set to 1, the operating system does not generate a dialog indicating that networking is down because the connection protocol handles such situations.
root/ConnectionType/freerdp/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.

Table E-5 root > ConnectionType > freerdp (continued)

Registry key	Description
root/ConnectionType/freerdp/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/freerdp/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/freerdp/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	Sets the number of seconds to wait for an initial response from the RDP server before giving up.
root/ConnectionType/freerdp/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/freerdp/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/freerdp/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by `appName`. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/freerdp/general/autoReconnectDialogTimeout	If `autoReconnect` is enabled, this key sets the number of seconds before timing out any error dialogs for the connection. If set to 0, the dialogs wait indefinitely for user interaction.
root/ConnectionType/freerdp/general/disablePasswordChange	When a remote login fails due to bad credentials, the user is presented with a button that brings up a dialog for updating their password. If this key is set is 1, that button and dialog are not displayed.
root/ConnectionType/freerdp/general/enableMMR	If set to 1, the `Multimedia Redirection` plugin is enabled, causing supported codecs played through Windows Media Player to be redirected to the client. This will greatly improve full screen and high definition video playback for codecs such as WMV9, VC1, and MPEG4.
root/ConnectionType/freerdp/general/preferredAudio	Sets the default audio backend for high-level audio redirection (both in and out).

Table E-5 root > ConnectionType > freerdp (continued)

Registry key	Description
root/ConnectionType/freerdp/general/sendHostname	If set to hostname, the system hostname is sent to the remote host. This is typically used to identify the client machine associated with a particular RDP session. The sent hostname can be overridden using sendHostname in the connection-specific settings. If set to mac, the MAC address of the first available network adapter is sent instead of the hostname.
root/ConnectionType/freerdp/general/serialPortsDriver	This setting ensures a better compatibility with the expected underlying Windows driver SerCx2.sys, SerCx.sys, or Serial.sys.
root/ConnectionType/freerdp/general/serialPortsPermissive	If set to 1, errors for unsupported features will be ignored.

root > ConnectionType > ssh

Table E-6 root > ConnectionType > ssh

Registry key	Description
root/ConnectionType/ssh/authorizations/user/add	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/ssh/authorizations/user/general	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/ssh/connections/<UUID>/address	Sets the hostname or IP address to connect to.
root/ConnectionType/ssh/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/ssh/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/ssh/connections/<UUID>/application	Specifies the application to run.
root/ConnectionType/ssh/connections/<UUID>/authorizations/user/edit	If set to 1, a standard user has permission to modify the connection settings for this connection.
root/ConnectionType/ssh/connections/<UUID>/authorizations/user/execution	If set to 1, a standard user has permission to execute this connection.
root/ConnectionType/ssh/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/ssh/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when autoReconnect is set to 1.
root/ConnectionType/ssh/connections/<UUID>/autostart	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/ssh/connections/<UUID>/autostartDelay	Sets the amount of time in seconds to wait before starting the connection after the system boots. The default of 0 will

Table E-6 root > ConnectionType > ssh (continued)

Registry key	Description
	cause the connection to start immediately. This setting only takes effect when `autostart` is set to 1.
`root/ConnectionType/ssh/connections/<UUID>/backgroundColor`	Sets the background color for the connection.
`root/ConnectionType/ssh/connections/<UUID>/beforeStartingCommand`	Sets the command to execute before the connection starts.
`root/ConnectionType/ssh/connections/<UUID>/compression`	Enables compression for an SSH connection.
`root/ConnectionType/ssh/connections/<UUID>/connectionEndAction`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/ssh/connections/<UUID>/coord`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/ssh/connections/<UUID>/dependConnectionId`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/key`	Sets the name of an extra environment variable for use with the connection.
`root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/value`	Sets the value of an extra environment variable for use with the connection.
`root/ConnectionType/ssh/connections/<UUID>/fallBackConnection`	Sets the fallback connection via its UUID.
`root/ConnectionType/ssh/connections/<UUID>/font`	Sets the font size for the connection.
`root/ConnectionType/ssh/connections/<UUID>/foregroundColor`	Sets the foreground color for the connection.
`root/ConnectionType/ssh/connections/<UUID>/fork`	If set to 1, the **Fork into background** option is enabled for the connection.
`root/ConnectionType/ssh/connections/<UUID>/hasDesktopIcon`	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
`root/ConnectionType/ssh/connections/<UUID>/isInMenu`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/ssh/connections/<UUID>/label`	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to `Default Connection` and does not display in the UI.
`root/ConnectionType/ssh/connections/<UUID>/port`	Sets the port number to use when contacting the SSH server. The default is 22.
`root/ConnectionType/ssh/connections/<UUID>/startMode`	If set to the default `focus` and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
`root/ConnectionType/ssh/connections/<UUID>/tty`	If set to 1, the **Force TTY allocation** option is enabled for the connection.
`root/ConnectionType/ssh/connections/<UUID>/username`	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.

Table E-6 root > ConnectionType > ssh (continued)

Registry key	Description
root/ConnectionType/ssh/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/ssh/connections/<UUID>/x11	If set to 1, the **X11 connection forwarding** option is enabled for the connection.
root/ConnectionType/ssh/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/ssh/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/ssh/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/ssh/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/ssh/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/ssh/coreSettings/serverRequired	Sets whether a server name or address is `unused`, `optional`, or `required` for this connection type.
root/ConnectionType/ssh/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/ssh/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by `appName`. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/ssh/gui/SshManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/gui/SshManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.

Table E-6 root > ConnectionType > ssh (continued)

Registry key	Description
root/ConnectionType/ssh/gui/SshManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/gui/SshManager/widgets/address	Controls the state of the **Address** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/application	Controls the state of the **Run application** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Controls the state of the **Auto reconnect** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/autostart	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor	Controls the state of the **Background color** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/compression	Controls the state of the **Compression** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection	Controls the state of the **Fallback Connection** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/font	Controls the state of the **Font** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/foregroundColor	Controls the state of the **Foreground color** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If

Table E-6 root > ConnectionType > ssh (continued)

Registry key	Description
	set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/fork`	Controls the state of the **Fork into background** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/hasDesktopIcon`	Controls the state of the **Show icon on desktop** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/isInMenu`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/ssh/gui/SshManager/widgets/label`	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/port`	Controls the state of the **Port** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/tty`	Controls the state of the **Force TTY allocation** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/username`	Controls the state of the **User name** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/waitForNetwork`	Controls the state of the **Wait for network before connecting** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/ssh/gui/SshManager/widgets/x11`	Controls the state of the **X11 connection forwarding** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

root > ConnectionType > teemtalk

Table E-7 root > ConnectionType > teemtalk

Registry key	Description
root/ConnectionType/teemtalk/authorizations/user/add	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/teemtalk/authorizations/user/general	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/teemtalk/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/teemtalk/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/edit	If set to 1, a standard user has permission to modify the connection settings for this connection.
root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/execution	If set to 1, a standard user has permission to execute this connection.
root/ConnectionType/teemtalk/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/teemtalk/connections/<UUID>/autostart	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/teemtalk/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/teemtalk/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/teemtalk/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/teemtalk/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/teemtalk/connections/<UUID>/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to `Default Connection` and does not display in the UI.
root/ConnectionType/teemtalk/connections/<UUID>/startMode	If set to the default `focus` and the connection is already started, the connection will be given focus. Otherwise, an

Table E-7 root > ConnectionType > teemtalk (continued)

Registry key	Description
	error will be returned stating that the connection is already started.
root/ConnectionType/teemtalk/connections/<UUID>/systembeep	If set to 1, system beep is enabled for the connection.
root/ConnectionType/teemtalk/connections/<UUID>/ttsName	Sets the TeemTalk profile name.
root/ConnectionType/teemtalk/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/teemtalk/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/teemtalk/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/teemtalk/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/teemtalk/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/teemtalk/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/teemtalk/coreSettings/serverRequired	Sets whether a server name or address is `unused`, `optional`, or `required` for this connection type.
root/ConnectionType/teemtalk/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/teemtalk/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.

Table E-7 root > ConnectionType > teemtalk (continued)

Registry key	Description
root/ConnectionType/teemtalk/gui/TeemtalkManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/gui/TeemtalkManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/gui/TeemtalkManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autoReconnect	Controls the state of the **Auto reconnect** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autostart	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/hasDesktopIcon	Controls the state of the **Show icon on desktop** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/label	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/waitForNetwork	Controls the state of the **Wait for network before connecting** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

root > ConnectionType > telnet

Table E-8 root > ConnectionType > telnet

Registry key	Description
root/ConnectionType/telnet/authorizations/user/add	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/telnet/authorizations/user/general	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.

Table E-8 root > ConnectionType > telnet (continued)

Registry key	Description
root/ConnectionType/telnet/connections/<UUID>/address	Sets the hostname or IP address to connect to.
root/ConnectionType/telnet/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/telnet/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/telnet/connections/<UUID>/authorizations/user/edit	If set to 1, a standard user has permission to modify the connection settings for this connection.
root/ConnectionType/telnet/connections/<UUID>/authorizations/user/execution	If set to 1, a standard user has permission to execute this connection.
root/ConnectionType/telnet/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/telnet/connections/<UUID>/autostart	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/telnet/connections/<UUID>/backgroundColor	Sets the background color for the connection.
root/ConnectionType/telnet/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/telnet/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/telnet/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/telnet/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/telnet/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/telnet/connections/<UUID>/font	Sets the font size for the connection.
root/ConnectionType/telnet/connections/<UUID>/foregroundColor	Sets the foreground color for the connection.
root/ConnectionType/telnet/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/telnet/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to `Default Connection` and does not display in the UI.
root/ConnectionType/telnet/connections/<UUID>/locale	Sets the locale of the connection.
root/ConnectionType/telnet/connections/<UUID>/port	Sets the port number to use when contacting the server. The default is 23.

Table E-8 root > ConnectionType > telnet (continued)

Registry key	Description
root/ConnectionType/telnet/connections/<UUID>/startMode	If set to the default focus and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/telnet/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/telnet/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/telnet/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/telnet/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/telnet/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/telnet/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/telnet/coreSettings/serverRequired	Sets whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/telnet/coreSettings/stopProcess	Sets the behavior that should occur when connection-mgr stop is called on this connection. By default this is close, which will send a standard kill signal to the process. When set to kill, the process specified by appName will be forcefully killed. When set to custom, a custom execution script specified by wrapperScript will be executed with the argument stop to terminate the process gracefully.
root/ConnectionType/telnet/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/telnet/gui/TelnetManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.

Table E-8 root > ConnectionType > telnet (continued)

Registry key	Description
root/ConnectionType/telnet/gui/TelnetManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/telnet/gui/TelnetManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/telnet/gui/TelnetManager/widgets/address	Controls the state of the **Address** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/autoReconnect	Controls the state of the **Auto reconnect** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor	Controls the state of the **Background color** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection	Controls the state of the **Fallback Connection** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor	Controls the state of the **Foreground color** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon	Controls the state of the **Show icon on desktop** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/label	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/port	Controls the state of the **Port** widget in the Connection Manager for this connection type. If set to `active`, the

Table E-8 root > ConnectionType > telnet (continued)

Registry key	Description
	widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork`	Controls the state of the **Wait for network before connecting** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

root > ConnectionType > view

Table E-9 root > ConnectionType > view

Registry key	Description
`root/ConnectionType/view/authorizations/user/add`	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
`root/ConnectionType/view/authorizations/user/general`	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
`root/ConnectionType/view/connections/<UUID>/ExtraArgs`	Specifies extra arguments for the VMware Horizon View client. Run `view_client --help` or `vmware-view --help` from an X terminal to see all available arguments.
`root/ConnectionType/view/connections/<UUID>/SingleSignOn`	
`root/ConnectionType/view/connections/<UUID>/afterStartedCommand`	Sets the command to execute after the connection has been started.
`root/ConnectionType/view/connections/<UUID>/afterStoppedCommand`	Sets the command to execute after the connection has been stopped.
`root/ConnectionType/view/connections/<UUID>/appInMenu`	If set to 1, all applications for this connection will be displayed in the taskbar menu.
`root/ConnectionType/view/connections/<UUID>/appOnDesktop`	If set to 1, all applications for this connection will be displayed on the desktop.
`root/ConnectionType/view/connections/<UUID>/applicationSize`	Sets the size in which the VMware Horizon View client will launch applications.
`root/ConnectionType/view/connections/<UUID>/attachToConsole`	
`root/ConnectionType/view/connections/<UUID>/authorizations/user/edit`	If set to 1, a standard user has permission to modify the connection settings for this connection.
`root/ConnectionType/view/connections/<UUID>/authorizations/user/execution`	If set to 1, a standard user has permission to execute this connection.
`root/ConnectionType/view/connections/<UUID>/autoReconnect`	If set to 1, the connection will be restarted when it is closed or disconnected.
`root/ConnectionType/view/connections/<UUID>/autoReconnectDelay`	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the

Table E-9 root > ConnectionType > view (continued)

Registry key	Description
	connection to reconnect immediately. This setting only takes effect when `autoReconnect` is set to 1.
`root/ConnectionType/view/connections/<UUID>/automaticLogin`	If set to 1, the VMware Horizon View client will attempt to log in automatically if all fields are provided. If set to 0, users have to click **Connect** manually in the VMware Horizon View client, log in, and select a desktop.
`root/ConnectionType/view/connections/<UUID>/autostart`	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
`root/ConnectionType/view/connections/<UUID>/autostartDelay`	Sets the amount of time in seconds to wait before starting the connection after the system boots. The default of 0 will cause the connection to start immediately. This setting only takes effect when `autostart` is set to 1.
`root/ConnectionType/view/connections/<UUID>/beforeStartingCommand`	Sets the command to execute before the connection starts.
`root/ConnectionType/view/connections/<UUID>/closeAfterDisconnect`	If set to 1, the connection is ended after the first desktop is closed. If set to 0, the VMware Horizon View client returns to the desktop selection screen. This is enabled by default to prevent users from accidentally leaving the connection at the desktop selection screen after logging off.
`root/ConnectionType/view/connections/<UUID>/coord`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/view/connections/<UUID>/dependConnectionId`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/view/connections/<UUID>/desktop`	If specified, the named desktop will launch automatically upon login. By default, if there is only one desktop available, it will launch automatically without needing to be specified.
`root/ConnectionType/view/connections/<UUID>/desktopSize`	Sets the size in which the VMware Horizon View client will launch the desktop.
`root/ConnectionType/view/connections/<UUID>/directory`	
`root/ConnectionType/view/connections/<UUID>/disableMaximizedApp`	If set to 1, window size settings for maximized applications are disabled.
`root/ConnectionType/view/connections/<UUID>/domain`	Sets the domain to provide to View Connection Server. If no domain is specified, the default domain for the server is used.
`root/ConnectionType/view/connections/<UUID>/enableSingleMode`	
`root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/key`	Sets the name of an extra environment variable for use with the connection.
`root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/value`	Sets the value of an extra environment variable for use with the connection.
`root/ConnectionType/view/connections/<UUID>/fallBackConnection`	Sets the fallback connection via its UUID.
`root/ConnectionType/view/connections/<UUID>/fullscreen`	If set to 1, the VMware Horizon View client launches in full screen mode when started.

Table E-9 root > ConnectionType > view (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/view/connections/<UUID>/hideMenuBar	If set to 1, the top menu bar within the desktop is hidden. This bar is used to manage remote devices and start other desktops.
root/ConnectionType/view/connections/<UUID>/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to `Default Connection` and does not display in the UI.
root/ConnectionType/view/connections/<UUID>/lockServer	If set to 1, standard users are prevented from changing the server address.
root/ConnectionType/view/connections/<UUID>/loginfields/domain	Shows the **Domain** field in the login dialog for the connection.
root/ConnectionType/view/connections/<UUID>/loginfields/password	Shows the **Password** field in the login dialog for the connection.
root/ConnectionType/view/connections/<UUID>/loginfields/rememberme	Shows the **Remember me** checkbox in the login dialog for the connection.
root/ConnectionType/view/connections/<UUID>/loginfields/showpassword	Shows the **Show password** button in the login dialog for the connection.
root/ConnectionType/view/connections/<UUID>/loginfields/smartcard	Shows the **Smart card login** checkbox in the login dialog for the connection. This checkbox might not appear if no smart card is detected, even if this option is enabled.
root/ConnectionType/view/connections/<UUID>/loginfields/username	Shows the **User Name** field in the login dialog for the connection.
root/ConnectionType/view/connections/<UUID>/password	Sets the default password to supply to the remote host during login. This value will be encrypted. Generally, this setting is used for kiosk-style applications where a generic password is used for login.
root/ConnectionType/view/connections/<UUID>/saveCredentials	
root/ConnectionType/view/connections/<UUID>/server	Sets the address of the remote host to connect to. This is typically a URL such as `http://server.domain.com`.
root/ConnectionType/view/connections/<UUID>/sessionEndAction	
root/ConnectionType/view/connections/<UUID>/singleDesktop	
root/ConnectionType/view/connections/<UUID>/smartcard	If set to 1, locally-attached smart cards are forwarded to the remote host, allowing them to be used by applications on the remote host. This only enables smart card login for the remote host, not for View Connection Server.
root/ConnectionType/view/connections/<UUID>/startMode	If set to the default `focus` and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.

Table E-9 root > ConnectionType > view (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.
root/ConnectionType/view/connections/<UUID>/viewSecurityLevel	If set to Refuse insecure connections, the VMware Horizon View client will not allow a user to connect to View Connection Server if the server's SSL certificate is invalid. If set to Warn, the VMware Horizon View client will display a warning if the server's certificate is not able to be verified, and if the certificate is self-signed or expired, the user still will not be allowed to connect. If set to Allow all connections, the server certificate will not be verified and connections to any server will be allowed.
root/ConnectionType/view/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/attachToConsole	
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/audioLatency	Sets the average milliseconds of offset between the audio stream and the display of corresponding video frames after decoding.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/colorDepth	This setting is deprecated. It is used to reduce the color depth of the connection below that of the native desktop resolution. Frequently, this has been used to reduce network bandwidth. Reducing color depth to a level not supported by the video driver can cause screen corruption or launch failures.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/compression	If set to 1, compression of RDP data sent between the client and the server is enabled.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/disableMMRwithRFX	If set to 1, multimedia redirection is disabled if a valid RemoteFX session is established.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/frameAcknowledgeCount	Sets the number of video frames the server can push without waiting for acknowledgement from the client. Lower numbers result in a more responsive desktop but lower frame rate. If set to 0, frame acknowledgement is not used in the client-server interactions.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/enableMMR	If set to 1, the Multimedia Redirection plugin is enabled, causing supported codecs played through Windows Media Player to be redirected to the client. This will greatly improve full screen and high definition video playback for codecs such as WMV9, VC1, and MPEG4.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname	If set to hostname, the system hostname is sent to the remote host. This is typically used to identify the client machine associated with a particular RDP session. The sent hostname can be overridden using sendHostname in the connection-specific settings. If set to mac, the MAC address of the first available network adapter is sent instead of the hostname.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo	This value is the load balancing cookie sent for brokering purposes to the server upon connection and corresponds to the loadbalanceinfo field in the .rdp file. By default, the value is empty.

Table E-9 root > ConnectionType > view (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents	If set to 0, mouse motion events are not sent to the server. This can prevent some user feedback such as tooltips from functioning properly.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/offScreenBitmaps	If set to 0, off-screen bitmaps are disabled. This can increase performance slightly but will cause blocks of the screen to update asynchronously, causing screen transitions to update non-uniformly.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagDesktopComposition	If set to 1, desktop composition (such as translucent borders) is allowed if supported by the server. Turning off desktop composition can improve performance for low-bandwidth connections. Generally, this only affects RemoteFX. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagFontSmoothing	If set to 1, font smoothing is allowed if supported by the server and enabled. Turning off font smoothing can improve performance on low-bandwidth connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorSettings	If set to 1, cursor blinking is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorShadow	If set to 1, mouse cursor shadows are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoMenuAnimations	If set to 1, menu animations are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoTheming	If set to 1, user interface themes are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWallpaper	If set to 1, the desktop wallpaper is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWindowDrag	If set to 1, full-content window dragging is disabled, which can improve performance on low-bandwidth RDP connections. The window outline is used instead. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/portMapping	If set to 1, the following serial and parallel ports are redirected to the remote host: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/printerMapping	If set to 1, all printers defined locally via CUPS are redirected to the remote host.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/rdpEncryption	If set to 1, standard RDP encryption is used to encrypt all data between the client and the server.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/remoteFx	If set to 1, RemoteFX is used if available.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/securityLevel	Sets the certificate security level. If set to 0, all connections are allowed. If set to 1, remembered hosts are checked and

Table E-9 root > ConnectionType > view (continued)

Registry key	Description
	a warning dialog is shown if verification is not passed. If set to 2, remembered hosts are not checked and a warning dialog is shown if verification is not passed. If set to 3, all insecure connections are refused.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sendHostname	Sets the client hostname that is sent to the remote host. If left blank, the system hostname is sent. The registry key root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname must be set to hostname for this key to be used.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sound	If set to Bring to this computer, sound is redirected from the remote host to the client using a standard virtual channel. If set to Leave at remote computer, sound is left at the remote host. This can be useful when using a redirected USB audio device. If set to any other value, audio is disabled. Generally, HP recommends setting this value to Bring to this computer and not redirecting USB playback devices to the remote host. This will improve audio quality and ensure that client audio redirected via other virtual channels (such as Multimedia Redirection) matches local audio settings.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutError	Sets the number of milliseconds to wait after losing the connection before giving up on reconnecting with the server. If set to 0, reconnection is attempted forever.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutRecovery	Sets the number of milliseconds to wait after losing the connection for networking to recover without trying a forced reconnect.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarning	Sets the number of milliseconds to wait after losing the connection before warning the user that the connection has been lost.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarningDialog	If set to 1, when an end-to-end connection drop is detected, a dialog is displayed and the screen will turn grayscale. Otherwise, messages are written to the connection log and the session freezes.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutsEnabled	If set to 1, end-to-end connection health checks are done.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/xkbLayoutId	Sets an XKB layout ID for bypassing the system keyboard. To see the list of available IDs, enter the following command in an X terminal: xfreerdp --kbd-list.
root/ConnectionType/view/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/view/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/view/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/view/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/view/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.

Table E-9 root > ConnectionType > view (continued)

Registry key	Description
root/ConnectionType/view/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/view/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/view/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/view/coreSettings/serverRequired	Sets whether a server name or address is `unused`, `optional`, or `required` for this connection type.
root/ConnectionType/view/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/view/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by `appName`. This key should not need to be modified.
root/ConnectionType/view/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/view/general/rdpOptions	Options specified here will be forwarded directly to the RDP client if RDP is used as the display protocol for the VMware Horizon View connection. To see a full list of options, enter the following command in an X terminal: `rdesktop --help`
root/ConnectionType/view/gui/viewManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/gui/viewManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/gui/viewManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/gui/viewManager/widgets/autostart	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection	Controls the state of the **Fallback Connection** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/view/gui/viewManager/widgets/label	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to `active`, the

Table E-9 root > ConnectionType > view (continued)

Registry key	Description
	widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

root > ConnectionType > xdmcp

Table E-10 root > ConnectionType > xdmcp

Registry key	Description
`root/ConnectionType/xdmcp/authorizations/user/add`	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
`root/ConnectionType/xdmcp/authorizations/user/general`	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
`root/ConnectionType/xdmcp/connections/<UUID>/address`	Sets the hostname or IP address to connect to.
`root/ConnectionType/xdmcp/connections/<UUID>/afterStartedCommand`	Sets the command to execute after the connection has been started.
`root/ConnectionType/xdmcp/connections/<UUID>/afterStoppedCommand`	Sets the command to execute after the connection has been stopped.
`root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/edit`	If set to 1, a standard user has permission to modify the connection settings for this connection.
`root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/execution`	If set to 1, a standard user has permission to execute this connection.
`root/ConnectionType/xdmcp/connections/<UUID>/autoReconnect`	If set to 1, the connection will be restarted when it is closed or disconnected.
`root/ConnectionType/xdmcp/connections/<UUID>/autostart`	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
`root/ConnectionType/xdmcp/connections/<UUID>/beforeStartingCommand`	Sets the command to execute before the connection starts.
`root/ConnectionType/xdmcp/connections/<UUID>/color`	Sets the color depth of the display for the connection.
`root/ConnectionType/xdmcp/connections/<UUID>/connectionEndAction`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/xdmcp/connections/<UUID>/coord`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/xdmcp/connections/<UUID>/dependConnectionId`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/key`	Sets the name of an extra environment variable for use with the connection.
`root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/value`	Sets the value of an extra environment variable for use with the connection.

Table E-10 root > ConnectionType > xdmcp (continued)

Registry key	Description
root/ConnectionType/xdmcp/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/xdmcp/connections/<UUID>/fontServer	Sets the address of the font server to use. The registry key useFontServer must also be set to 1.
root/ConnectionType/xdmcp/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to Default Connection and does not display in the UI.
root/ConnectionType/xdmcp/connections/<UUID>/refreshRate	Sets the refresh rate of the display for the connection.
root/ConnectionType/xdmcp/connections/<UUID>/startMode	If set to the default focus and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/xdmcp/connections/<UUID>/type	Sets the XDMCP connection type. If set to chooser, all available hosts are listed and the user can select which one to connect to. If set to query, an XDMCP request is sent to the specified host directly. If set to broadcast, all available hosts are listed and the first one is connected to automatically.
root/ConnectionType/xdmcp/connections/<UUID>/useFontServer	If set to 1, the font server is enabled. If set to 0, the local font is used.
root/ConnectionType/xdmcp/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/xdmcp/connections/<UUID>/windowSize	Sets the window size of the connection.
root/ConnectionType/xdmcp/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/audio	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/desktopButton	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.

Table E-10 root > ConnectionType > xdmcp (continued)

Registry key	Description
root/ConnectionType/xdmcp/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/xdmcp/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/xdmcp/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/xdmcp/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/xdmcp/coreSettings/serverRequired	Sets whether a server name or address is `unused`, `optional`, or `required` for this connection type.
root/ConnectionType/xdmcp/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/xdmcp/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by `appName`. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/xdmcp/gui/XdmcpManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/gui/XdmcpManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/gui/XdmcpManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/address	Controls the state of the **Address** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect	Controls the state of the **Auto reconnect** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autostart	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If

Table E-10 root > ConnectionType > xdmcp (continued)

Registry key	Description
	set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/color`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/fontServer`	Controls the state of the **Font server** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/hasDesktopIcon`	Controls the state of the **Show icon on desktop** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/isInMenu`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/label`	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/refreshRate`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/type`	Controls the state of the **Type** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/useFontServer`	Controls the state of the **Use font server** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/waitForNetwork`	Controls the state of the **Wait for network before connecting** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/windowSize`	This registry key is either used internally or reserved for future use. The value should not be changed.

root > ConnectionType > xen

Table E-11 root > ConnectionType > xen

Registry key	Description
root/ConnectionType/xen/authorizations/user/add	If set to 1, a standard user has permission to add a new connection of this type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/xen/authorizations/user/general	If set to 1, a standard user has permission to modify the general settings for this connection type using the Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/xen/connections/<UUID>/SingleSignOn	
root/ConnectionType/xen/connections/<UUID>/address	Sets the address of the remote host to connect to. This is typically a URL such as http://server.domain.com.
root/ConnectionType/xen/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/xen/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/xen/connections/<UUID>/anonymousLogin	If set to 1, anonymous login is allowed for PNAgent and direct connections.
root/ConnectionType/xen/connections/<UUID>/appInMenu	If set to 1, all applications for the connection will be displayed in the taskbar menu.
root/ConnectionType/xen/connections/<UUID>/appOnDashboard	If set to 1, all applications for the connection will be displayed on the taskbar.
root/ConnectionType/xen/connections/<UUID>/appOnDesktop	If set to 1, all applications for the connection will be displayed on the desktop.
root/ConnectionType/xen/connections/<UUID>/authorizations/user/edit	If set to 1, a standard user has permission to modify the connection settings for this connection.
root/ConnectionType/xen/connections/<UUID>/authorizations/user/execution	If set to 1, a standard user has permission to execute this connection.
root/ConnectionType/xen/connections/<UUID>/autoLaunchSingleApp	If set to 1, and if only a single published application or desktop is returned by the Citrix server, that resource will be launched automatically.
root/ConnectionType/xen/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/xen/connections/<UUID>/autoReconnectAppsOnLogin	If set to 1, the system will attempt to reconnect any active or disconnected Citrix sessions upon initial login.
root/ConnectionType/xen/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when autoReconnect is set to 1.
root/ConnectionType/xen/connections/<UUID>/autoStartDesktop	If set to 1, the first desktop to become available when the connection is started will be launched automatically.
root/ConnectionType/xen/connections/<UUID>/autoStartResource	Sets the name of the desktop or application to start automatically when the connection is launched.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/connections/<UUID>/autostart	If set to a value of 1–5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/xen/connections/<UUID>/autostartDelay	Sets the amount of time in seconds to wait before starting the connection after the system boots. The default of 0 will cause the connection to start immediately. This setting only takes effect when autostart is set to 1.
root/ConnectionType/xen/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/xen/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/connections/<UUID>/connectionMode	Sets the Citrix connection mode for the connection as follows: store=StoreFront, pnagent=Web Interface, direct=Direct Connection.
root/ConnectionType/xen/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/connections/<UUID>/disableSaveCredentials	
root/ConnectionType/xen/connections/<UUID>/domain	Sets the domain to provide to the XenDesktop server. If no domain is specified, the default domain for the server is used.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/xen/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/xen/connections/<UUID>/folder	
root/ConnectionType/xen/connections/<UUID>/forceHttps	If set to 1, only HTTPS connections are allowed.
root/ConnectionType/xen/connections/<UUID>/fullscreen	If set to 1, the Citrix client launches in full screen mode when started.
root/ConnectionType/xen/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/xen/connections/<UUID>/ignoreCertCheck	If set to 1, certificate checks are ignored for the connection.
root/ConnectionType/xen/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to Default Connection and does not display in the UI.
root/ConnectionType/xen/connections/<UUID>/logOnMethod	

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/connections/<UUID>/loginfields/domain	Shows the **Domain** field in the login dialog for the connection.
root/ConnectionType/xen/connections/<UUID>/loginfields/password	Shows the **Password** field in the login dialog for the connection.
root/ConnectionType/xen/connections/<UUID>/loginfields/rememberme	Shows the **Remember me** checkbox in the login dialog for the connection.
root/ConnectionType/xen/connections/<UUID>/loginfields/showpassword	Shows the **Show password** button in the login dialog for the connection.
root/ConnectionType/xen/connections/<UUID>/loginfields/smartcard	Shows the **Smart card login** checkbox in the login dialog for the connection. This checkbox might not appear if no smart card is detected, even if this option is enabled.
root/ConnectionType/xen/connections/<UUID>/loginfields/username	Shows the **User Name** field in the login dialog for the connection.
root/ConnectionType/xen/connections/<UUID>/password	Sets the default password to supply to the remote host during login. This value will be encrypted. Generally, this setting is used for kiosk-style applications where a generic password is used for login.
root/ConnectionType/xen/connections/<UUID>/requireCredentialsDirectConnect	If set to 0, credentials are not needed to initiate a direct connection. However, credentials are needed to launch an application.
root/ConnectionType/xen/connections/<UUID>/savePassword	
root/ConnectionType/xen/connections/<UUID>/startMode	If set to the default `focus` and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/xen/connections/<UUID>/username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.
root/ConnectionType/xen/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/xen/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch	This setting applies to Citrix servers with multiple published resources. If less than 0, no auto-logout is performed. Otherwise, this setting dictates the number of seconds between the closing of the last Xen published resource and when the user is logged out automatically and returned to the initial login screen. Citrix process delays might extend the auto-logout time.
root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch	This setting applies to Citrix servers with multiple published resources. If less than 0, no auto-logout is performed. Otherwise, this setting dictates the number of seconds allowed to pass while no applications are launched before the user is logged out automatically and returned to the initial login screen. Citrix process delays might extend the auto-logout time.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/editor	Sets the internal application name to use when the Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/icon16Path	Sets the path to the 16x16 pixel icon for this application.
root/ConnectionType/xen/coreSettings/icon32Path	Sets the path to the 32x32 pixel icon for this application.
root/ConnectionType/xen/coreSettings/icon48Path	Sets the path to the 48x48 pixel icon for this application.
root/ConnectionType/xen/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/xen/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in the Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/xen/coreSettings/serverRequired	Sets whether a server name or address is `unused`, `optional`, or `required` for this connection type.
root/ConnectionType/xen/coreSettings/stopProcess	Sets the behavior that should occur when `connection-mgr stop` is called on this connection. By default this is `close`, which will send a standard kill signal to the process. When set to `kill`, the process specified by `appName` will be forcefully killed. When set to `custom`, a custom execution script specified by `wrapperScript` will be executed with the argument `stop` to terminate the process gracefully.
root/ConnectionType/xen/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by `appName`. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/xen/general/TWIMode	Controls seamless mode for published applications. This setting directly maps to the Citrix .ini file setting `TWIMode`.
root/ConnectionType/xen/general/TWIModeResizeType	This setting directly maps to the Citrix .ini file setting `TWIMoveResizeType`.
root/ConnectionType/xen/general/allowReadOn<AthruZ>	If set to 1, a user can read the mapped drive.
root/ConnectionType/xen/general/allowWriteOn<AthruZ>	If set to 1, a user can write to the mapped drive.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/general/async	If set to 1, asynchronous polling is enabled. This setting directly maps to the Citrix .ini file setting CommPollSize.
root/ConnectionType/xen/general/autoReconnect	If set to 1, automatic session reconnection is enabled. This is not the same as the connection-specific auto-reconnect. This occurs internally within the Citrix client without restarting the connection. This setting directly maps to the Citrix .ini file setting TransportReconnectEnabled.
root/ConnectionType/xen/general/ bitmapCacheSize	Sets the minimum size for bitmap caching. This setting directly maps to the Citrix .ini file setting PersistentCacheMinBitmap.
root/ConnectionType/xen/general/colorDepth	Forces a specific color depth for all connections. This is usually done only in specialized environments where the automatic depth selection fails or in very slow networks to reduce congestion.
root/ConnectionType/xen/general/colorMapping	If set to Shared - Approximate Colors, approximate colors from the default colormap are used. If set to Private - Exact Colors, precise colors are used. This setting directly maps to the Citrix .ini file setting ApproximateColors.
root/ConnectionType/xen/general/ contentRedirection	If set to 1, links from web content are sent from the server to the client so that the client can try to open them locally.
root/ConnectionType/xen/general/ defaultBrowserProtocol	Controls the protocol used to locate the host for the connection. If not specified, the default value from the [WFClient] section of wfclient.ini is used. This setting directly maps to the Citrix .ini file setting BrowserProtocol.
root/ConnectionType/xen/general/ drivePathMappedOn<AthruZ>	Sets the local filesystem directory to map to the remote host. Typically this is set to /media to allow all connected USB drives to be mapped to the remote host via a single drive letter.
root/ConnectionType/xen/general/ enableAlertSound	If set to 1, Windows alert sounds are enabled. This setting indirectly maps to the Citrix .ini file setting DisableSound.
root/ConnectionType/xen/general/ enableAudioInput	If set to 1, audio input is enabled. This will set both the AllowAudioInput and EnableAudioInput settings to 1 in wfclient.ini and appsrv.ini respectively. If set to 0, the Audio extension is disabled. If set to 2, USB audio devices are redirected as configured in the USB Manager. Generally, HP recommends setting this value to 1 and that USB audio devices not be redirected to the host. This will improve audio quality and ensure that client audio redirected via other extensions (such as Multimedia Redirection) matches local audio settings.
root/ConnectionType/xen/general/ enableCursorColors	If set to 1, colored cursors are enabled. Setting this to 0 might fix graphical cursor corruption in some cases.
root/ConnectionType/xen/general/ enableDataCompression	If set to 1, data compression is enabled. This setting directly maps to the Citrix .ini file setting Compress.
root/ConnectionType/xen/general/ enableDriveMapping	If set to 1, directories on the local filesystem can be forwarded to the remote host via a virtual drive. Typically /media is mapped to Z to allow USB drives to be forwarded to the remote host. If USB redirection is enabled, this setting should be disabled to prevent storage conflicts. To be

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
	properly mapped to the remote host in this fashion, the USB device must use one of the following filesystems: FAT32, NTFS, ext2, ext3.
root/ConnectionType/xen/general/enableDynamicDriveMapping	If set to 1, USB storage devices will be dynamically mapped on the Citrix server, and static drive mappings are not required. If set to 0, dynamic mapping of USB storage devices is disabled. If set to 2, USB storage devices are redirected as configured in the USB Manager.
root/ConnectionType/xen/general/enableForceDirectConnect	If set to 1, the connection is forced to bypass the Citrix Web Interface and PNAgent services. Authentication will occur on the server after the initial connection has been made.
root/ConnectionType/xen/general/enableH264Compression	If set to 1, H264 compression is enabled. The H264 codec provides better performance of rich and professional graphics applications on WAN networks than the JPEG codec.
root/ConnectionType/xen/general/enableHDXFlashRedirection	Controls the behavior of HDX Flash Redirection. If set to `Always`, HDX Flash Redirection is used if possible, and the user is not prompted. If set to `Ask`, the user is prompted. If set to `Never`, the feature is disabled.
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	Controls the behavior of HDX Flash Server-Side Content Fetching. If disabled, the client will fetch for content.
root/ConnectionType/xen/general/enableHDXMediaStream	If set to 1, HDX MediaStream is enabled. If set to 0, media files will still play via standard streaming, but the quality might not be as high.
root/ConnectionType/xen/general/enableMapOn<AthruZ>	If set to 1, a local filesystem directory can be mapped to this drive on the remote host. The corresponding `drivePathMappedOn` registry key must be set to a valid local directory for drive mapping to work properly.
root/ConnectionType/xen/general/enableMultiMedia	If set to 1, multimedia is enabled. HDX Lync might have a conflict if this setting is enabled. This setting directly maps to the Citrix .ini file settings in the `MultiMedia in Virtual Channels` section.
root/ConnectionType/xen/general/enableOffScreenSurface	If set to 1, the server can use the `X PixMap` format for off-screen drawing. This reduces bandwidth in 15-bit and 24-bit color modes at the expense of X server memory and processor time. This setting directly maps to the Citrix .ini file setting `EnableOSS`.
root/ConnectionType/xen/general/enableSmartCard	If set to 1, smart card login is enabled.
root/ConnectionType/xen/general/enableWindowsAlertSounds	
root/ConnectionType/xen/general/encryptionLevel	Sets the level of encryption. Encryption protocols for all levels are defined in the `[EncryptionLevelSession]` section of module.ini. This setting directly maps to the Citrix .ini file setting `[EncryptionLevelSession]`.
root/ConnectionType/xen/general/fontSmoothingType	Sets the font smoothing type.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/general/hotKey<1thru15>Char	Sets the hot key to forward to the remote session when the key or key combination set in the corresponding hotKeyShift is pressed.
root/ConnectionType/xen/general/hotKey<1thru15>Shift	Sets the key or key combination used to activate the hot key set in the corresponding hotKeyChar.
root/ConnectionType/xen/general/httpAddresses/<UUID>/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Sets the keyboard key for disabling the transparent keyboard mode. This setting directly maps to the Citrix .ini file setting KeyPassthroughEscapeChar.
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Sets the keyboard key combination for disabling the transparent keyboard mode. This setting directly maps to the Citrix .ini file setting KeyPassthroughEscapeShift.
root/ConnectionType/xen/general/lastComPortNum	Sets the number of mapped serial ports. If set to 0, serial port mapping is disabled.
root/ConnectionType/xen/general/localTextEcho	Controls keyboard latency reduction. This setting indirectly maps to the Citrix .ini file setting ZLKeyboardMode.
root/ConnectionType/xen/general/monitorNetwork	If set to Off, network connectivity is not monitored. If set to Local network link status only, only the local network link status is monitored. If set to Server online status, both the local network link status and server connectivity are monitored.
root/ConnectionType/xen/general/mouseClickFeedback	Controls mouse latency reduction. This setting indirectly maps to the Citrix .ini file setting ZLMouseMode.
root/ConnectionType/xen/general/mouseMiddleButtonPaste	If set to 1, middle mouse button paste emulation for Windows sessions is enabled. This setting directly maps to the Citrix .ini file setting MouseSendsControlV.
root/ConnectionType/xen/general/noInfoBox	If set to 1, the client manager (wfcmgr) will not display when a client session terminates. This setting directly maps to the Citrix .ini file setting PopupOnExit.
root/ConnectionType/xen/general/printerAutoCreation	If set to 0, printer mapping is disabled. If set to 1, printers defined locally will be mapped to the connection. If set to 2, USB printers are redirected as configured in the USB Manager.
root/ConnectionType/xen/general/proxyAddress	Sets the proxy address to use if a manual proxy setting is selected via proxyType.
root/ConnectionType/xen/general/proxyPassword	Sets the proxy password to use if a manual proxy setting is selected via proxyType. This password will be encrypted using rc4 encryption.
root/ConnectionType/xen/general/proxyPort	Sets the proxy port to use if a manual proxy setting is selected via proxyType.
root/ConnectionType/xen/general/proxyType	Sets the type of proxy to use for XenDesktop connections. The value Use Browser settings is only supported if a local browser is installed.
root/ConnectionType/xen/general/proxyUser	Sets the proxy username to use if a manual proxy setting is selected via proxyType.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/general/serverCheckTimeout	
root/ConnectionType/xen/general/sessionSharingClient	If set to 1, session-sharing requests are sent to other Citrix sessions on the same X display. This setting directly maps to the Citrix .ini file setting EnableSessionSharingClient.
root/ConnectionType/xen/general/sound	Sets the sound quality. This setting indirectly maps to the Citrix .ini file setting AudioBandwidthLimit.
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/<UUID>/address	
root/ConnectionType/xen/general/transparentKeyPassthrough	Controls how certain Windows key combinations handled. If set to Translated, the key combinations apply to the local desktop. If set to Direct in full screen desktops only, the key combinations apply to the remote session only when it is in full screen mode. If set to Direct, the key combinations always apply to the remote session as long as the window has focus. This setting indirectly maps to the Citrix .ini file setting TransparentKeyPassthrough.
root/ConnectionType/xen/general/twRedundantImageItems	Controls the number of screen areas that will be tracked in ThinWire to prevent redundant drawing of bitmap images. An adequate value for 1024x768 sessions is 300.
root/ConnectionType/xen/general/useAlternateAddress	If set to 1, an alternate address is used for firewall connections. This setting directly maps to the Citrix .ini file setting UseAlternateAddress.
root/ConnectionType/xen/general/useBitmapCache	If set to 1, the persistent disk cache is enabled. The persistent disk cache stores commonly-used graphical objects such as bitmaps on the hard disk of the client device. Using the persistent disk cache increases performance across low-bandwidth connections but reduces the amount of available client disk space. For clients on high-speed LANs, usage of the persistent disk cache is not necessary. This setting directly maps to the Citrix .ini file setting PersistentCacheEnabled.
root/ConnectionType/xen/general/useEUKS	Controls the use of Extended Unicode Keyboard Support (EUKS) on Windows servers. If set to 0, EUKS is not used. If set to 1, EUKS is used as a fallback. If set to 2, EUKS is used whenever possible.
root/ConnectionType/xen/general/useLocalIM	If this setting is enabled, the local X input method is used to interpret keyboard input. This is supported for European languages only. This setting directly maps to the Citrix .ini file setting useLocalIME.
root/ConnectionType/xen/general/userAgent	The string from this key will be presented by the Citrix client and will be helpful for administrators to know where the connection request is from.
root/ConnectionType/xen/general/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/general/webcamFramesPerSec	Controls the HDXWebCamFramesPerSec variable in the All_Regions.ini file.
root/ConnectionType/xen/general/webcamSupport	If set to 0, the webcam and webcam audio are disabled. If set to 1, the webcam and webcam audio are enabled, with compression. If set to 2, USB redirection of the webcam and webcam audio is enabled.
root/ConnectionType/xen/general/windowHeight	Sets the height of the window in pixels if windowSize is set to Fixed Size.
root/ConnectionType/xen/general/windowPercent	Sets the size of the window as a percentage if windowSize is set to Percentage of Screen Size.
root/ConnectionType/xen/general/windowSize	If set to Default, the server-side settings are used. If set to Full Screen, the window is maximized without borders on all available screens. If set to Fixed Size, the windowWidth and windowHeight registry keys can be used to specify the size of the window in pixels. If set to Percentage of Screen Size, the windowPercent key can be used to specify the size of the window as a percentage. For Percentage of Screen Size to take effect, enableForceDirectConnect must be set to 1 and TWIMode must be set to 0. This setting only works with XenApp and only if the server allows direct connections. This setting does not work with XenDesktop.
root/ConnectionType/xen/general/windowWidth	Sets the width of the window in pixels if windowSize is set to Fixed Size.
root/ConnectionType/xen/gui/XenDesktopPanel/disabled	If set to 1, the Xen Desktop panel and its taskbar are disabled. This is usually used when autoStartResource or autoStartDesktop is enabled.
root/ConnectionType/xen/gui/XenManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/gui/XenManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/gui/XenManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/gui/XenManager/widgets/address	Controls the state of the **Service URL** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/appInMenu	Controls the state of the **Show applications on taskbar** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop	Controls the state of the **Show applications on desktop** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
	If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect`	Controls the state of the **Auto reconnect** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop`	Controls the state of the **Auto Start Desktop** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource`	Controls the state of the **Auto Start Resource** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/autostart`	Controls the state of the **Auto start priority** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/domain`	Controls the state of the **Domain** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection`	Controls the state of the **Fallback Connection** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/folder`	
`root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon`	Controls the state of the **Show icon on desktop** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/ConnectionType/xen/gui/XenManager/widgets/isInMenu`	This registry key is either used internally or reserved for future use. The value should not be changed.
`root/ConnectionType/xen/gui/XenManager/widgets/label`	Controls the state of the **Name** widget in the Connection Manager for this connection type. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

Table E-11 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/gui/XenManager/widgets/password	Controls the state of the **Password** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/username	Controls the state of the **Username** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork	Controls the state of the **Wait for network before connecting** widget in the Connection Manager for this connection type. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/ConnectionType/xen/gui/fbpanel/autohide	If set to true, the taskbar auto-hides.
root/ConnectionType/xen/gui/fbpanel/edge	Sets the default position of the taskbar when more than one published desktop or application is available.
root/ConnectionType/xen/gui/fbpanel/hidden	If set to 1, the taskbar is completely hidden, but only if autoStartResource or autoStartDesktop is enabled.

root > DHCP

This folder exists to support temporary registry keys that are added when the system acquires a DHCP lease. No modification is necessary.

root > Dashboard

NOTE: The dashboard is the same thing as the taskbar.

Table E-12 root > Dashboard

Registry key	Description
root/Dashboard/GUI/Clock	If set to 1, the clock is shown on the taskbar.
root/Dashboard/GUI/ConnectionManager	If set to 1, the Connection Manager button is shown on the taskbar.
root/Dashboard/GUI/ControlPanel	If set to 1, the Control Panel button is shown on the taskbar.
root/Dashboard/GUI/PowerButton	If set to 1, the power button is shown on the taskbar.
root/Dashboard/GUI/SystemInformation	If set to 1, the System Information button is shown on the taskbar.
root/Dashboard/GUI/SystemTray	If set to 1, the system tray is shown on the taskbar.
root/Dashboard/GUI/TaskBar	If set to 1, the application area is shown on the taskbar.
root/Dashboard/General/AlwaysOnTop	If set to 1, the taskbar will always be on top.

Table E-12 root > Dashboard (continued)

Registry key	Description
root/Dashboard/General/AutoHide	If set to 1, the taskbar auto-hides.
root/Dashboard/General/EnterLeaveTimeout	Sets the amount of time in milliseconds before the taskbar will hide or show when AutoHide is enabled.
root/Dashboard/General/IconSize	Sets the size of the icons on the taskbar.
root/Dashboard/General/Length	Sets the length of the taskbar.
root/Dashboard/General/LengthToScreenSide	If set to 1, the length of taskbar is fixed and equal to the length of the side of the screen to which it is anchored.
root/Dashboard/General/PanelDockSide	Sets the side of the screen to which the taskbar is docked.
root/Dashboard/General/RemainPixel	Sets the number of pixels that are still visible when the taskbar hides.
root/Dashboard/General/SlidingTimeout	Sets the amount of time in milliseconds that it takes for the taskbar to hide or show when AutoHide is enabled.
root/Dashboard/General/Width	Sets the width of the taskbar.

root > Display

Table E-13 root > Display

Registry key	Description
root/Display/Configuration/AMDOptions/SWCursor	If set to 1, a software-rendered mouse cursor is used, which fixes issues with multi-monitor cursor corruption but can introduce issues with multimedia playback and touch screens. If set to 0, a hardware-rendered mouse cursor is used, which fixes issues with multimedia playback and touch screens but can introduce random cursor corruption when using more than one monitor. This corruption might require a reboot.
root/Display/Configuration/displaymode	Sets the display mode. If set to 0, the standard mode (a 1–4 monitor configuration) is used. If set to 1, a 6-monitor configuration can be used, but only on supported platforms with the appropriate add-on card.
root/Display/Configuration/hexlayout	Sets the layout in 6-monitor mode.
root/Display/Configuration/hexprofile	Sets the profile used in 6-monitor mode.
root/Display/Configuration/primaryprofile	Sets the profile to use for the primary monitor via the profile name. For Smart Zero, this must always be set to default.
root/Display/Configuration/quaternarymode	Sets the position of the fourth monitor relative to the monitor indicated in quaternaryrelative. This is hardware-dependent and is not supported on all models. Values are defined as follows: 0=Same As; 1=Above; 2=Right Of; 3=Left Of; 4=Below.
root/Display/Configuration/quaternaryprofile	Sets the profile to use for the fourth monitor via the profile name.
root/Display/Configuration/quaternaryrelative	Sets which monitor is used as a reference to set the position of the fourth monitor.

Table E-13 root > Display (continued)

Registry key	Description
root/Display/Configuration/secondaryConnector	Sets the secondary connector.
root/Display/Configuration/secondarymode	Sets the position of the secondary monitor relative to the primary monitor. This is hardware-dependent and is not supported on all models. Values are defined as follows: 0=Same As; 1=Above; 2=Right Of; 3=Left Of; 4=Below.
root/Display/Configuration/secondaryorientation	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Display/Configuration/secondaryprofile	Sets the profile to use for the secondary monitor via the profile name.
root/Display/Configuration/swapstate	Specifies which connector is connected to the primary monitor. This is hardware-dependent and is not supported on all models. Generally, 0 means the primary monitor is on the VGA connector and 1 means the other connector. For the t510, 0 means the primary monitor is on the DVI-I connector, and 1 means the primary monitor is on the DVI-D connector. For platforms with an add-on video card, 0 means the primary monitor is on the built-in video card, and 1 means the primary monitor is on the add-on video card.
root/Display/Configuration/tertiarymode	Sets the position of the third monitor relative to the monitor indicated in tertiaryrelative. This is hardware-dependent and is not supported on all models. Values are defined as follows: 0=Same As; 1=Above; 2=Right Of; 3=Left Of; 4=Below.
root/Display/Configuration/tertiaryprofile	Sets the profile to use for the third monitor via the profile name.
root/Display/Configuration/tertiaryrelative	Sets which monitor is used as a reference to set the position of the third monitor.
root/Display/Profiles/<UUID>/colorScaling	Sets the color temperature or direct RGB scaling for thin clients with built-in monitors. The entry is a 6-digit hex value (RRGGBB), where ffffff would indicate full (100%) scaling on all three color channels.
root/Display/Profiles/<UUID>/depth	Sets the display color depth in bits-per-pixel. A higher color depth means better quality but lower performance.
root/Display/Profiles/<UUID>/height	Sets the monitor resolution height. If set to 0, the resolution is auto-detected.<
root/Display/Profiles/<UUID>/label	Sets the display profile name. For Smart Zero, this must always be set to default.
root/Display/Profiles/<UUID>/orientation	Sets the monitor orientation as follows: 0=Normal; 1=Rotate Left; 2=Rotate Right; 3=Invert.
root/Display/Profiles/<UUID>/refresh	Sets the desired monitor refresh rate. Not all refresh rates are supported for all resolutions. If set to 0, the refresh rate is auto-detected. The supported values are dependent on the monitor. Setting a refresh rate that is not supported by the attached monitor will lead to a black screen. HP recommends leaving this set to 0.
root/Display/Profiles/<UUID>/width	Sets the monitor resolution width. If set to 0, the resolution is auto-detected.

Table E-13 root > Display (continued)

Registry key	Description
root/Display/userLock	If set to 1, and if the display settings have been modified by the user, the display settings are preserved when importing an HP ThinPro profile.
root/Display/userLockEngaged	This sets to 1 after the display settings have been modified by the user. You normally do not need to modify this setting.

root > Network

Table E-14 root > Network

Registry key	Description
root/Network/ActiveDirectory/Domain	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/DynamicDNS	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Enabled	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Method	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Password	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Username	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/DNSServers	Additional DNS servers for domain name resolution can be specified here. The specified servers will be used in addition to any servers retrieved via DHCP. Up to three IPv4 or IPv6 addresses can be specified, separated by commas.
root/Network/DefaultHostnamePattern	Sets the default hostname pattern to use when generating a new hostname. This is used if the Hostname registry key and /etc/hostname are both empty. The hostname pattern uses % as a delimiter. In the example HPTC%MAC:1-6%, HPTC would be the prefix, and the first six characters of the client MAC address would follow. So if the MAC address of the client is 11:22:33:44:55:66, the generated hostname would be HPTC112233. If the pattern is TC%MAC%, the generated hostname would be TC112233445566. If the pattern is HP%MAC:7%, the generated hostname would be HP1122334.
root/Network/FtpProxy	Sets the FTP proxy address. HP recommends using the following format for this value because the http prefix is better supported: http://ProxyServer:Port
root/Network/Hostname	Sets the hostname of the client.
root/Network/HttpProxy	Sets the HTTP proxy address. HP recommends using the following format: http://ProxyServer:Port
root/Network/HttpsProxy	Sets the HTTPS proxy address. HP recommends using the following format for this value because the http prefix is better supported: http://ProxyServer:Port

Table E-14 root > Network (continued)

Registry key	Description
root/Network/IPSec/IPSecRules/<UUID>/DstAddr	Sets the destination address for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethod	Sets the authentication method for the IPSec rule. PSK is for using a pre-shared key, and Certificate is for using certificate files.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodCACert	If the authentication method is Certificate, the CA certificate file path is saved in this registry key.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodClientCert	If the authentication method is Certificate, the client certificate file path is saved in this registry key.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPresharedKey	If the authentication method is PSK, the pre-shared key value is saved in this registry key.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPrivateKey	If the authentication method is Certificate, the private key file path that corresponds with the client certificate is saved in this registry key.
root/Network/IPSec/IPSecRules/<UUID>/MMDHGroup	Sets the phase 1 Diffie-Hellman group.
root/Network/IPSec/IPSecRules/<UUID>/MMEncryptionAlg	Sets the phase 1 encryption algorithm.
root/Network/IPSec/IPSecRules/<UUID>/MMIntegrityAlg	Sets the phase 1 integrity algorithm.
root/Network/IPSec/IPSecRules/<UUID>/MMLifetimeMinutes	Sets the phase 1 lifetime.
root/Network/IPSec/IPSecRules/<UUID>/QMAHEnable	Enables phase 2 AH.
root/Network/IPSec/IPSecRules/<UUID>/QMAHIntegrityAlg	Sets the phase 2 AH integrity algorithm.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEnable	Enables phase 2 ESP.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEncryptionAlg	Sets the phase 2 ESP encryption algorithm.
root/Network/IPSec/IPSecRules/<UUID>/QMESPIntegrityAlg	Sets the phase 2 ESP integrity algorithm.
root/Network/IPSec/IPSecRules/<UUID>/QMLifetimeSeconds	Sets the phase 2 lifetime.
root/Network/IPSec/IPSecRules/<UUID>/RuleDescription	Sets the description for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/RuleEnable	If set to 1, the rule is enabled.
root/Network/IPSec/IPSecRules/<UUID>/RuleName	Sets the name for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/SrcAddr	Sets the source address for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/TunnelDstAddr	Sets the tunnel destination address for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/TunnelEnable	Enables tunnel mode for the IPSec rule.

Table E-14 root > Network (continued)

Registry key	Description
root/Network/IPSec/IPSecRules/<UUID>/TunnelSrcAddr	Sets the tunnel source address for the IPSec rule.
root/Network/KeepPreviousDNS	If set to 1, previously-configured DNS servers and search domains not generated by the Network Manager will be kept in resolv.conf. If set to 0, resolv.conf will be overwritten completely.
root/Network/SearchDomains	Additional search domains for FQDN resolution can be specified here. The specified domains will be appended to any incomplete server definitions in an attempt to generate an FQDN that can be resolved via DNS. For example, a search domain of mydomain.com will allow the server definition myserver to resolve properly to myserver.mydomain.com, even if the DNS server does not have myserver in its name resolution tables. Up to five additional search domains can be specified.
root/Network/VPN/AutoStart	If set to 1, VPN auto-starts when the system boots.
root/Network/VPN/Domain	Sets the VPN domain.
root/Network/VPN/Gateway	Sets the VPN gateway.
root/Network/VPN/Group	Sets the VPN group.
root/Network/VPN/GroupPassword	Sets the VPN group password.
	Sets the VPN user password.
root/Network/VPN/Type	Sets the VPN type.
root/Network/VPN/Username	Sets the VPN username.
root/Network/VPN/VpncSecurity	Sets the VPNC security level.
root/Network/Wired/DefaultGateway	Sets the default gateway the device will use to communicate with the Internet. Typically this is the IP address of the router. This setting will only take effect when Method is set to Static.
root/Network/Wired/EnableDefGatewayAsDNS	If set to 1, the default gateway will also be the name server.
root/Network/Wired/EthernetSpeed	Sets the link speed of the primary Ethernet network interface. Automatic allows the fastest available link speed to be used, which is usually 1 Gbps or 100 Mbps/Full depending on the switch. The link speed can also be forced to a single speed (100 Mbps or 10 Mbps) and duplex mode (Full or Half) to support switches and hubs that do not perform appropriate auto-negotiation.
root/Network/Wired/IPAddress	Sets the IPv4 address of the client. This setting will only take effect when Method is set to Static.
root/Network/Wired/IPv6Enable	If set to 1, IPv6 is enabled.
root/Network/Wired/Interface	Sets the default Ethernet interface or NIC.
root/Network/Wired/MTU	Sets the MTU. It does not matter if the IP address is static or DHCP-acquired.
root/Network/Wired/Method	If set to Automatic, the client will use DHCP to attempt to retrieve network settings. If set to Static, the values of the IPAddress, SubnetMask, and DefaultGateway registry

Table E-14 root > Network (continued)

Registry key	Description
	keys are used. HP does not recommend using `Static` in a generic client profile because it will cause all clients to receive the same IP address.
`root/Network/Wired/Security/CACert`	Sets the path to CA certificate file.
`root/Network/Wired/Security/Identity`	Sets the identity or anonymous identity.
`root/Network/Wired/Security/InnerAuth`	Sets the PEAP inner authentication protocol.
`root/Network/Wired/Security/InnerAuthTTLS`	Sets the TTLS inner authentication protocol.
`root/Network/Wired/Security/PEAPVersion`	Sets the PEAP version.
`root/Network/Wired/Security/Password`	Sets the password.
`root/Network/Wired/Security/PrivateKey`	Sets the path to a private key file. This is only used for TLS authentication.
`root/Network/Wired/Security/Type`	Sets the 802.1x authentication type.
`root/Network/Wired/Security/UserCert`	Sets the path to a user certificate file. This is only used for TLS authentication.
`root/Network/Wired/Security/Username`	Sets the username.
`root/Network/Wired/SubnetMask`	Sets the subnet mask of the device, such as 255.255.255.0 (for a standard class C subnet). This setting will only take effect when `Method` is set to `Static`.
`root/Network/Wireless/DefaultGateway`	Sets the default gateway the device will use to communicate with the Internet. Typically this is the IP address of the router. This setting will only take effect when `Method` is set to `Static`.
`root/Network/Wireless/EnableDefGatewayAsDNS`	If set to 1, the default gateway will also be the name server.
`root/Network/Wireless/IPAddress`	Sets the IPv4 address of the client. This setting will only take effect when `Method` is set to `Static`.
`root/Network/Wireless/IPv6Enable`	If set to 1, IPv6 is enabled.
`root/Network/Wireless/Interface`	Sets the default wireless interface or wireless network adapter.
`root/Network/Wireless/Method`	If set to `Automatic`, the client will use DHCP to attempt to retrieve network settings. If set to `Static`, the values of the `IPAddress`, `SubnetMask`, and `DefaultGateway` registry keys are used. HP does not recommend using `Static` in a generic client profile because it will cause all clients to receive the same IP address.
`root/Network/Wireless/PowerEnable`	If set to 1, power management of the wireless network card is enabled.
`root/Network/Wireless/SSID`	Sets the wireless access point to use via its SSID.
`root/Network/Wireless/SSIDHidden`	Specifies if the SSID of the wireless access point is hidden.
`root/Network/Wireless/Security/CACert`	Sets the path to CA certificate file.
`root/Network/Wireless/Security/EAPFASTPAC`	Sets the path to the PAC file for EAP FAST authentication.

Table E-14 root > Network (continued)

Registry key	Description
root/Network/Wireless/Security/EAPFASTProvision	Sets the provisioning option for EAP FAST authentication.
root/Network/Wireless/Security/Identity	Sets the identity or anonymous identity.
root/Network/Wireless/Security/InnerAuth	Sets the PEAP inner authentication protocol.
root/Network/Wireless/Security/InnerAuthTTLS	Sets the TTLS inner authentication protocol.
root/Network/Wireless/Security/PEAPVersion	Sets the PEAP version.
root/Network/Wireless/Security/Password	Sets the password.
root/Network/Wireless/Security/PrivateKey	Sets the path to a private key file. This is only used for TLS authentication.
root/Network/Wireless/Security/Type	Sets the wireless authentication type.
root/Network/Wireless/Security/UserCert	Sets the path to a user certificate file. This is only used for TLS authentication.
root/Network/Wireless/Security/Username	Sets the username.
root/Network/Wireless/Security/WEPAuth	Sets the WEP authentication type.
root/Network/Wireless/Security/WEPIndex	Sets the WEP password index.
root/Network/Wireless/SubnetMask	Sets the subnet mask of the device, such as 255.255.255.0 (for a standard class C subnet). This setting will only take effect when Method is set to Static.
root/Network/disableLeftClickMenu	If set to 1, the left-click menu for the network system tray icon is disabled.
root/Network/disableRightClickMenu	If set to 1, the right-click menu for the network system tray icon is disabled.
root/Network/iPeak/ShowStatus	If set to 1, the HP Velocity status is displayed as part of the system tray icon.
root/Network/iPeak/Status	If set to 1, HP Velocity is enabled. If set to 2, HP Velocity is enabled in Monitor mode. If set to 0, HP Velocity is disabled.
root/Network/userLock	If set to 1, and if the network settings have been modified by the user, the network settings are preserved when importing an HP ThinPro profile.
root/Network/userLockEngaged	This sets to 1 after the display settings have been modified by the user. You normally do not need to modify this setting.

root > SCIM

Table E-15 root > SCIM

Registry key	Description
root/SCIM/ScimEnabled	If set to 1, SCIM is enabled for Chinese, Japanese, and Korean input.

root > Serial

Table E-16 root > Serial

Registry key	Description
root/Serial/<UUID>/baud	Sets the speed of the serial device.
root/Serial/<UUID>/dataBits	Sets how many bits are in each character.
root/Serial/<UUID>/device	Specifies the serial device attached to the system.
root/Serial/<UUID>/flow	Sets the flow control of the serial device, which is used to communicate stops and starts of the serial communication.
root/Serial/<UUID>/name	Specifies the Windows device port for communicating with the serial device.
root/Serial/<UUID>/parity	Sets the parity bit of the serial device. The parity bit is used for error detection. If set to none, there is no parity detection.

root > SystemInfo

Table E-17 root > SystemInfo

Registry key	Description
root/SystemInfo/Pages/General	If set to 0, the **General** tab of the System Information window is hidden from standard users.
root/SystemInfo/Pages/NetTools	If set to 0, the **Net Tools** tab of the System Information window is hidden from standard users.
root/SystemInfo/Pages/Network	If set to 0, the **Network** tab of the System Information window is hidden from standard users.
root/SystemInfo/Pages/SoftwareInformationTab/ServicePacks	If set to 0, the **Service Packs** tab in the **Software Information** section of the System Information window is hidden from standard users.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInformation	If set to 0, the **Software Information** tab of the System Information window is hidden from standard users.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInstalled	If set to 0, the **Software Installed** tab in the **Software Information** section of the System Information window is hidden from standard users.
root/SystemInfo/Pages/SystemLogs	If set to 0, the **System Logs** tab of the System Information window is hidden from standard users.
root/SystemInfo/authorized	If set to 0, the System Information button on the taskbar is disabled for standard users.

root > TaskMgr

Table E-18 root > TaskMgr

Registry key	Description
root/TaskMgr/General/AlwaysOnTop	If set to 1, the Task Manager window is always on top.

root > USB

Table E-19 root > USB

Registry key	Description
root/USB/Classes/<ClassType>/ClassID	Sets the USB class ID number.
root/USB/Classes/<ClassType>/DisplayName	Sets the USB class name.
root/USB/Classes/<ClassType>/State	Sets whether the class is mapped to the remote host.
root/USB/Classes/<ClassType>/Visible	Sets whether the class is shown in the UI, not shown in the UI, or disabled.
root/USB/Classes/ShowTab	If set to 1, the **Classes** section is shown in the USB Manager.
root/USB/Devices/<UUID>/DisplayName	Sets the name to show in the USB Manager. If not supplied, the USB Manager will attempt to generate an appropriate name using device information.
root/USB/Devices/<UUID>/ProductID	Sets the product ID of the device.
root/USB/Devices/<UUID>/State	Sets whether this device is mapped to the remote host as follows: 0=Do Not Redirect; 1=Use Defaults; 2=Redirect.
root/USB/Devices/<UUID>/VendorID	Sets the vendor ID of the device.
root/USB/root/holdProtocolStatic	If set to 1, the remote USB protocol does not switch based on which protocol is chosen. It always stays at the value defined in root/protocol.
root/USB/root/mass-storage/allowed	If set to 1, mass storage devices will be auto-mounted when the protocol is local.
root/USB/root/mass-storage/read-only	If set to 1, when mass storage devices are auto-mounted locally, they will be mounted as read-only.
root/USB/root/opendebug	If set to 1, a debug message will be written to /tmp/USB-mgr-log.
root/USB/root/protocol	Sets which protocol owns remote USB. Valid values depend on which protocols are installed on the system but can include local, xen, rdp, and view.

root > auto-update

Table E-20 root > auto-update

Registry key	Description
root/auto-update/DNSAliasDir	Sets the default root directory for DNS alias mode on the server hosting HP Smart Client Services.
root/auto-update/ManualUpdate	If set to 1, the DHCP tag, DNS alias, and broadcast update methods for Automatic Update are disabled. When performing a manual update, the password, path, protocol, user, and ServerURL registry keys must be set to ensure the update server is known.
root/auto-update/ScheduledScan/Enabled	If set to 1, the client performs periodic scans of the Automatic Update server to check for updates. If set to 0, the client will only check for updates at system startup.

Table E-20 root > auto-update (continued)

Registry key	Description
root/auto-update/ScheduledScan/Interval	Sets the amount of time to wait between scheduled update scans. This should be specified in the HH:MM format. Intervals longer than 24 hours can be specified. For example, to have the scans occur every 48 hours, set this to 48:00.
root/auto-update/ScheduledScan/Period	Clients will randomly activate their scheduled scan throughout the defined period. Using a long period avoids cases where all clients update at exactly the same, which could cause network congestion. The period should be specified in the HH:MM format. For example, to spread client updates over a 2.5-hour period, set this to 02:30.
root/auto-update/ScheduledScan/StartTime	Sets the start time of the first scheduled update scan period in the format HH:MM, using the 24-hour time format. For example, 4:35 p.m. would be 16:35.
root/auto-update/ServerURL	Sets the IP address or domain name of the update server used when ManualUpdate is enabled.
root/auto-update/VisibleInSystray	If set to 1, the Automatic Update system tray icon is enabled.
root/auto-update/enableOnBootup	If set to 1, Automatic Update is enabled at system startup.
root/auto-update/enableSystrayLeftClickMenu	If set to 1, the left-click menu for the Automatic Update system tray icon is enabled.
root/auto-update/enableSystrayRightClickMenu	If set to 1, the right-click menu for the Automatic Update system tray icon is enabled.
root/auto-update/gui/auto-update/ManualUpdate	Controls the state of the **Enable manual configuration** widget in the Automatic Update utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/auto-update/gui/auto-update/ServerURL	Controls the state of the **Server** widget in the Automatic Update utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/auto-update/gui/auto-update/enableOnBootup	Controls the state of the **Enable Automatic Update on system startup** widget in the Automatic Update utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/auto-update/gui/auto-update/password	Controls the state of the **Password** widget in the Automatic Update utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/auto-update/gui/auto-update/protocol	Controls the state of the **Protocol** widget in the Automatic Update utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.

Table E-20 root > auto-update (continued)

Registry key	Description
root/auto-update/gui/auto-update/tag	This registry key is either used internally or reserved for future use. The value should not be changed.
root/auto-update/gui/auto-update/user	Controls the state of the **User name** widget in the Automatic Update utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/auto-update/password	Sets the password used when ManualUpdate is enabled. This is only used when protocol is set to ftp. This value will be encrypted.
root/auto-update/path	Sets the relative path from the default server URL for when ManualUpdate is enabled. Typically, this is empty or set to auto-update.
root/auto-update/preserveConfig	If set to 1, the current thin client configuration settings will be preserved when an image update occurs via Automatic Update.
root/auto-update/protocol	Sets the protocol used when ManualUpdate is enabled.
root/auto-update/tag	This registry key is obsolete. It previously set the tag number used for DHCP (137). This is now detected via the tag name auto-update.
root/auto-update/user	Sets the username used when ManualUpdate is enabled. This is only used when 'protocol' is set to 'ftp'.

root > background

Table E-21 root > background

Registry key	Description
root/background/desktop/color	If theme is set to none, this key stores the color used by the user-defined theme.
root/background/desktop/imagePath	If theme is set to none, this key stores the desktop background image path used by the user-defined theme.
root/background/desktop/lastBrowseDir	If theme is set to none, this key stores the last used directory.
root/background/desktop/style	If theme is set to none, this key stores how the background image is placed on the desktop (such as center, tile, stretch, fit, and fill).
root/background/desktop/theme	Specifies the system theme setting. This value is set via the Background Manager utility in the Control Panel. The valid values depend on the themes that exist on the system. This can be set to none to let the user define the theme.

root > config-wizard

Table E-22 root > config-wizard

Registry key	Description
root/config-wizard/FirmwareUpdate/firmwareUpdateTimeout	Sets the timeout period in seconds for when checking for updates. If set to -1, there is no timeout.
root/config-wizard/FirmwareUpdate/firmwareUpdateURL	Sets the FTP URL for image updates.
root/config-wizard/FirmwareUpdate/preserveConfig	If set to 1, the current thin client configuration settings will be preserved when an image update occurs via the initial configuration wizard.
root/config-wizard/enableConnectionCheck	If set to 1, the connection check at system startup is enabled.
root/config-wizard/enableNetworkCheck	If set to 1, the network check at system startup is enabled.
root/config-wizard/updateCheck	If set to 1, the update check at system startup is enabled.

root > desktop

Table E-23 root > desktop

Registry key	Description
root/desktop/shortcuts/<action>/command	Sets the command that is run by the shortcut.
root/desktop/shortcuts/<action>/enabled	If set to 1, the shortcut is enabled.
root/desktop/shortcuts/<action>/shortcut	Sets the shortcut name.

root > entries

Table E-24 root > entries

Registry key	Description
root/entries/<UUID>/command	
root/entries/<UUID>/folder	
root/entries/<UUID>/icon	
root/entries/<UUID>/label	
root/entries/<UUID>/metaInfo	
root/entries/<UUID>/onDesktop	
root/entries/<UUID>/onMenu	

root > keyboard

Table E-25 root > keyboard

Registry key	Description
root/keyboard/DrawLocaleLetter	If set to 1, the keyboard system tray icon will draw the language locale string instead of using static images.
root/keyboard/SystrayMenu/keyboardLayout	If set to 1, the right-click menu on the keyboard system tray icon offers an option to open the Keyboard Layout utility in the Control Panel.
root/keyboard/SystrayMenu/languages	If set to 1, the right-click menu on the keyboard system tray icon offers an option to open the Language utility in the Control Panel.
root/keyboard/SystrayMenu/virtualKeyboard	If set to 1, the right-click menu on the keyboard system tray icon offers an option to open the virtual keyboard.
root/keyboard/VisibleInSystray	If set to 1, the keyboard system tray icon is displayed and indicates the current keyboard layout.
root/keyboard/XkbLayout	This is an internal key used to map to an XKB keyboard layout. This key should not need to be modified.
root/keyboard/XkbModel	This is an internal key used to map to an XKB keyboard model. This key should not need to be modified.
root/keyboard/XkbOptions	This is an internal key used to map to XKB keyboard options. This key should not need to be modified.
root/keyboard/XkbVariant	This is an internal key used to map to an XKB keyboard variant. This key should not need to be modified.
root/keyboard/enable2	If set to 1, the secondary keyboard layout can be switched to via the keyboard shortcut defined by switch.
root/keyboard/layout	Sets the primary keyboard layout.
root/keyboard/layout2	Sets the secondary keyboard layout.
root/keyboard/model	Sets the primary keyboard model.
root/keyboard/model2	Sets the secondary keyboard model.
root/keyboard/numlock	If set to 1, the Num Lock function is enabled at system startup.
root/keyboard/rdp_kb	This is an internal key used to map to an RDP keyboard map. This key should not need to be modified.
root/keyboard/switch	Sets the keyboard shortcut for switching between the first and second keyboard layout (enable2 must also be set to 1). Valid values are as follows: grp:ctrl_shift_toggle, grp:ctrl_alt_toggle, grp:alt_shift_toggle.
root/keyboard/variant	Sets the primary keyboard variant.
root/keyboard/variant2	Sets the secondary keyboard variant.

root > logging

Table E-26 root > logging

Registry key	Description
root/logging/general/debug	If set to 1, debugging is enabled for all debug-supported subsystems. This is usually used in conjunction with generateDiagnostic.sh or the System Information **Diagnostic** tool to generate a diagnostic bundle with system debug logs included.

root > mouse

Table E-27 root > mouse

Registry key	Description
root/mouse/MouseHandedness	If set to 0, the mouse is right-handed. If set to 1, the mouse is left-handed.
root/mouse/MouseSpeed	Sets the acceleration of the mouse pointer. Typically, a value from 0 to 25 is in the usable range. A value of 0 completely disables acceleration, causing the mouse to move at a constant slow, but measurable pace.
root/mouse/MouseThreshold	Sets the number of pixels before mouse acceleration is enabled. A value of 0 sets the acceleration to a natural curve that gradually scales acceleration, allowing for both precise and quick movements.

root > screensaver

Table E-28 root > screensaver

Registry key	Description
root/screensaver/ctrllbindkey	This key is used by other applications to trigger the screen lock. Setting the value to 1 starts the screen lock.
root/screensaver/enableCustomLogo	If set to 1, the custom image defined in logoPath is used for the screen saver.
root/screensaver/enableDPMS	If set to 0, monitor power management is disabled. This causes the monitor to always stay on unless turned off manually.
root/screensaver/enableScreensaver	If set to 1, the screen saver is enabled.
root/screensaver/enableSleep	If set to 1, sleep mode is enabled.
root/screensaver/lockScreen	If set to 1, a password is required to return to the desktop from the screen saver.
root/screensaver/logoPath	Sets the path to a custom image to use for the screen saver.
root/screensaver/mode	Sets the rendering mode for the screen saver image (such as Center, Tile, and Stretch). If set to Default, the image is displayed without any processing.

Table E-28 root > screensaver (continued)

Registry key	Description
root/screensaver/off	Sets the timeout delay in minutes before the monitor turns off.
root/screensaver/origImageCopyPath	This is the path where the custom image is saved when mode is set to Default.
root/screensaver/standby	Sets the timeout delay in minutes before the monitor goes into standby mode.
root/screensaver/suspend	Sets the timeout delay in minutes before the monitor goes into suspend mode.
root/screensaver/timeoutScreensaver	Sets the timeout delay in minutes before the screen saver starts.
root/screensaver/timeoutSleep	Sets the timeout delay in minutes before the thin client goes into sleep mode.

root > security

Table E-29 root > security

Registry key	Description
root/security/mustLogin	If set to 1, all users are forced to log in before accessing the desktop.

root > sshd

Table E-30 root > sshd

Registry key	Description
root/sshd/enabled	If set to 1, the SSH daemon is enabled and the client can be accessed via SSH.
root/sshd/userAccess	If set to 1, standard users can connect to the client via SSH.

root > time

Table E-31 root > time

Registry key	Description
root/time/NTPServers	Specifies NTP servers to use via a comma-separated list. Private NTP servers or large virtual NTP clusters such as pool.ntp.org are the best choices to minimize server load. Clear this value to return to using DHCP servers (tag 42) instead of a fixed list.
root/time/TimeServerIPAddress	Sets the time server used by the Linux net command. These servers are typically the domain controller servers on the corporate network. This should be used when NTP servers are not configured or they are not responding. The Linux net

Table E-31 root > time (continued)

Registry key	Description
	command identifies this server on its own. However, specific server IP addresses can be provided here if desired.
root/time/WebServerURL	Sets the web server URL (such as hp.com) to use when fetching the time using the http protocol. This URL can be within an intranet or over the Internet.
root/time/timezone	Sets the time zone. Time zones should be specified as defined by **Linux Timezone** in the **Date and Time** utility in the Control Panel, and they should be in the following format: <region>/<subregion>.
root/time/use24HourFormat	If set to -1, the system chooses the format automatically according to the locale. If set to 0, the a.m./p.m. format is used. If set to 1, the 24-hour format is used.
root/time/useDHCPTimezone	If set to 1, the client attempts to set the time zone via DHCP. To properly set the time zone via this registry key, ensure that the DHCP server for the client forwards the tcode DHCP tag (which is usually tag 101, although 100 and 2 can work also).
root/time/useNTPServers	If set to 1, the use of NTP time servers to synchronize the client clock is enabled. If this is enabled, ensure that an NTP server is specified via DHCP or via NTPServers.

root > touchscreen

Table E-32 root > touchscreen

Registry key	Description
root/touchscreen/calibrated	This registry key is either used internally or reserved for future use. The value should not be changed.
root/touchscreen/enabled	If set to 1, the touch screen input is enabled.
root/touchscreen/maxx	This registry key is either used internally or reserved for future use. The value should not be changed.
root/touchscreen/maxy	This registry key is either used internally or reserved for future use. The value should not be changed.
root/touchscreen/minx	This registry key is either used internally or reserved for future use. The value should not be changed.
root/touchscreen/miny	This registry key is either used internally or reserved for future use. The value should not be changed.
root/touchscreen/port	Specifies the port that is connected to the touch screen.
root/touchscreen/swapx	This registry key is either used internally or reserved for future use. The value should not be changed.
root/touchscreen/swapy	This registry key is either used internally or reserved for future use. The value should not be changed.
root/touchscreen/type	Specifies the controller type of the touch screen.

root > translation

Table E-33 root > translation

Registry key	Description
root/translation/coreSettings/localeMapping/<LanguageCode>	These are internal keys used to provide the text string next to the appropriate language on the language selector. These keys should not need to be modified.
root/translation/coreSettings/localeSettings	Sets the locale for the client. This locale will also be forwarded to the remote connection. Valid locales are en_US (English), de_DE (German), es_ES (Spanish), fr_FR (French), and ru_RU (Russian). Other locales such as ja_JP (Japanese) and zh_CN (Chinese) might be available as client updates.
root/translation/gui/LocaleManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/translation/gui/LocaleManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/translation/gui/LocaleManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/translation/gui/LocaleManager/widgets/localeSettings	Controls the state of the locale setting widget in the Language utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.

root > usb-update

Table E-34 root > usb-update

Registry key	Description
root/usb-update/authentication	If set to 1, an administrator password is required to do USB updates.
root/usb-update/enable	If set to 1, USB update auto-detection is enabled.
root/usb-update/height	Sets the height of the USB Update window in pixels.
root/usb-update/searchMaxDepth	Sets the depth of subdirectories to be searched for updates. Setting a high search depth can cause delays on USB flash drives that have thousands of directories.
root/usb-update/width	The width of the USB Update window in pixels.

root > users

Table E-35 root > users

Registry key	Description
root/users/gui/hptc-user-rights/name	This registry key is either used internally or reserved for future use. The value should not be changed.

Table E-35 root > users (continued)

Registry key	Description
root/users/gui/hptc-user-rights/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/users/gui/hptc-user-rights/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/users/root/password	Sets the administrator password. If empty, Administrator Mode is locked.
root/users/user/SSO	This registry key is either used internally or reserved for future use. The value should not be changed.
root/users/user/WOL	If set to 1, Wake-On-LAN (WOL) is enabled.
root/users/user/XHostCheck	If set to 1, only the systems listed under root/users/user/xhosts are allowed to remotely control the thin client.
root/users/user/apps/hptc-ad-dns-mgr/authorized	If set to 1, the **AD/DDNS Manager** is accessible by standard users.
root/users/user/apps/hptc-agent-mgr/authorized	If set to 1, the **HPDM Agent** is accessible by standard users.
root/users/user/apps/hptc-auto-update/authorized	If set to 1, the **Automatic Update** utility is accessible by standard users.
root/users/user/apps/hptc-background-mgr/authorized	If set to 1, the **Background Manager** is accessible by standard users.
root/users/user/apps/hptc-cert-mgr/authorized	If set to 1, the **Certificate Manager** is accessible by standard users.
root/users/user/apps/hptc-clientaggregation-mgr/authorized	If set to 1, the **Client Aggregation** utility is accessible by standard users.
root/users/user/apps/hptc-date-mgr/authorized	If set to 1, the **Date and Time** utility is accessible by standard users.
root/users/user/apps/hptc-dhcp-mgr/authorized	If set to 1, the **DHCP Option Manager** is accessible by standard users.
root/users/user/apps/hptc-display-prefs/authorized	If set to 1, the **Display Preferences** utility is accessible by standard users.
root/users/user/apps/hptc-easy-update/authorized	If set to 1, the **Easy Update** utility is accessible by standard users.
root/users/user/apps/hptc-i18n-mgr/authorized	If set to 1, the **Language** utility is accessible by standard users.
root/users/user/apps/hptc-keyboard-layout/authorized	If set to 1, the **Keyboard Layout** utility is accessible by standard users.
root/users/user/apps/hptc-mixer/authorized	If set to 1, the **Sound** utility is accessible by standard users.
root/users/user/apps/hptc-mouse/authorized	If set to 1, the **Mouse** utility is accessible by standard users.
root/users/user/apps/hptc-network-mgr/authorized	If set to 1, the **Network Manager** is accessible by standard users.
root/users/user/apps/hptc-printer-mgr/authorized	If set to 1, the **Printers** utility is accessible by standard users.

Table E-35 root > users (continued)

Registry key	Description
root/users/user/apps/hptc-restore/authorized	If set to 1, the **Snapshots** utility is accessible by standard users.
root/users/user/apps/hptc-screenlock-mgr/authorized	If set to 1, the **Screensaver** utility is accessible by standard users.
root/users/user/apps/hptc-security/authorized	If set to 1, the **Security** utility is accessible by standard users.
root/users/user/apps/hptc-shortcut-mgr/authorized	If set to 1, the **Keyboard Shortcut Manager** is accessible by standard users.
root/users/user/apps/hptc-sshd-mgr/authorized	If set to 1, the **SSHD Manager** is accessible by standard users.
root/users/user/apps/hptc-task-mgr/authorized	If set to 1, the **Task Manager** is accessible by standard users.
root/users/user/apps/hptc-text-editor/authorized	If set to 1, the **Text Editor** is accessible by standard users.
root/users/user/apps/hptc-thinstate/authorized	If set to 1, the **ThinState** utility is accessible by standard users.
root/users/user/apps/hptc-touchscreen/authorized	If set to 1, the **Touch Screen** utility is accessible by standard users.
root/users/user/apps/hptc-usb-mgr/authorized	If set to 1, the **USB Manager** is accessible by standard users.
root/users/user/apps/hptc-user-rights/authorized	If set to 1, the **Customization Center** is accessible by standard users.
root/users/user/apps/hptc-vncshadow/authorized	If set to 1, the **VNC Shadow** utility is accessible by standard users.
root/users/user/apps/hptc-xterm/authorized	If set to 1, the **X Terminal** is accessible by standard users. CAUTION: Enabling X terminal access is a security risk and is not recommended in a production environment. The X terminal should only be enabled for use in debugging a protected, non-production environment.
root/users/user/apps/scim-setup/authorized	If set to 1, the **SCIM Input Method Setup** utility is accessible by standard users.
root/users/user/hideDesktopPanel	If set to 1, desktop panels such as the taskbar are not started or shown in the desktop.
root/users/user/kioskMode	This registry key is either used internally or reserved for future use. The value should not be changed.
root/users/user/launchConnectionManager	If set to 1, the Connection Manager launches at system startup.
root/users/user/rightclick	If set to 1, the right-click menu for the desktop is enabled.
root/users/user/ssoconnectiontype	This registry key is either used internally or reserved for future use. The value should not be changed.
root/users/user/switchAdmin	If set to 1, switching to Administrator Mode is enabled.
root/users/user/xhosts/<UUID>/xhost	Specifies the IP address or hostname of a system that will be allowed to remotely control the thin client when `XHostCheck` is enabled.

root > vncserver

Table E-36 root > vncserver

Registry key	Description
root/vncserver/coreSettings/enableVncShadow	If set to 1, the VNC shadowing server for the thin client is enabled.
root/vncserver/coreSettings/userNotificationMessage	Sets the notification message that is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncNotifyShowTimeout	If set to 1, a timeout is applied to the notification dialog that is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncNotifyTimeout	Sets the timeout in seconds for the notification dialog that is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncNotifyUser	If set to 1, a notification is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncPassword	Sets the password for VNC shadowing. The key vncUsePassword must also be enabled.
root/vncserver/coreSettings/vncReadOnly	If set to 1, VNC shadowing will operate in view-only mode.
root/vncserver/coreSettings/vncRefuseInDefault	If set to 1, VNC requests are refused automatically if the user does not interact with the notification dialog before the timeout.
root/vncserver/coreSettings/vncTakeEffectRightNow	If set to 1, VNC settings take effect immediately after being modified.
root/vncserver/coreSettings/vncUsePassword	If set to 1, the password specified in vncPassword is required for VNC shadowing.
root/vncserver/coreSettings/vncUseSSL	If set to 1, SSL is used for VNC connections.
root/vncserver/gui/VNCShadowManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/vncserver/gui/VNCShadowManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/vncserver/gui/VNCShadowManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/vncserver/gui/VNCShadowManager/widgets/enableVncShadow	Controls the state of the **Enable VNC Shadow** widget in the VNC Shadow utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/userNotificationMessage	Controls the state of the **User Notification Message** widget in the VNC Shadow utility. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout	Controls the state of the **VNC Show Timeout for Notification** widget in the VNC Shadow utility. If set to active, the widget is visible in the UI and the user can interact with it. If

Table E-36 root > vncserver (continued)

Registry key	Description
	set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout`	Controls the state of the numerical widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser`	Controls the state of the **VNC Notify User to Allow Refuse** widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncPassword`	Controls the state of the **Set Password** widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly`	Controls the state of the **VNC Read Only** widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault`	Controls the state of the **Refuse connections in default** widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow`	Controls the state of the **Re-set VNC server right now** widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword`	Controls the state of the **VNC Use Password** widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.
`root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL`	Controls the state of the **VNC Use SSL** widget in the VNC Shadow utility. If set to `active`, the widget is visible in the UI and the user can interact with it. If set to `inactive`, the widget is hidden. If set to `read-only`, the widget is visible in the read-only state.

Index

A
AD/DDNS Manager 10
add-ons 1
audio redirection
  RDP 40
  VMware Horizon View 46

B
Background Manager 10

C
Certificate Manager 23
certificates
  installing 23
  VMware Horizon View 48
Citrix
  HDX MediaStream 28
  settings, connection-specific 32
  settings, general 29
  support matrix 29
client aggregation 12
  client configuration 13
  server configuration 14
client login screen
  customizing 72
client profile
  adding files 62
  adding symbolic link 63
  certificates 62
  loading 60
  modifying 60
  registry settings 61
  saving 63
clients
  updating. *See* updating clients
Connection Manager controls 6
connections
  common settings 25
  hiding 10
  types 1
Control Panel
  AD/DDNS Manager 10
  Background Manager 10
  Client Aggregation 12
  Customization Center 10
  Date and Time 10
  DHCP Option Manager 24
  Display Preferences 14
  Easy Update 10
  Keyboard Shortcuts 11
  Language 10
  Mouse 9
  Network 15
  overview 9
  SCEP Manager 11
  SCIM Input Method Setup 9
  Screensaver 10
  Security 10
  Serial Manager 11
  Snapshots 10
  Sound 9
  SSHD Manager 11
  Task Manager 11
  Text Editor 11
  ThinState. *See* HP ThinState
  Touch Screen 9
  utilities, hiding 10
  VNC Shadow 22
  X Terminal 11
custom connections 55

D
date and time settings 10
device redirection
  RDP 39
  VMware Horizon View 46
DHCP options 24
display preferences 14
display profiles 14

E
Easy Update 10

F
finding more resources 1

G
getting started 3

H
HDX MediaStream 28
HP Device Manager. *See* HPDM Agent
HP Smart Client Services
  installing 56
  overview 56
  Profile Editor. *See* Profile Editor
  supported operating systems 56
HP TeemTalk. *See* TeemTalk
HP Velocity 18
HPDM Agent 10

I
image updates 1
imaging. *See* HP ThinState
interface
  navigating 5

K
keyboard shortcuts 11
Kiosk Mode 26

L
language settings 10

M
mass storage redirection
  RDP 39
  VMware Horizon View 46
MMR
  VMware Horizon View 45
mouse settings 9
multimedia redirection
  RDP 38

N
network settings
  accessing 15
  DNS 17
  HP Velocity 18
  IPSec 18
  VPN 18

wired 16
wireless 16

P
parallel printer configuration 63
passwords, change 10
printer configuration 63
printer redirection
RDP 40
VMware Horizon View 46
printers 14
Profile Editor
using 60

R
RDP
audio redirection 40
device redirection 39
mass storage redirection 39
multi-monitor sessions 38
multimedia redirection 38
printer redirection 40
RemoteFX 37
settings, connection-specific 34
settings, general 34
smart card redirection 41
USB redirection 39
registry keys 80
RemoteFX 37
RFX. *See* RemoteFX

S
SCEP Manager 11, 23
SCIM 9
screensaver settings 10
security settings 10
Serial Manager 11
serial printer configuration 63
smart card redirection
RDP 41
VMware Horizon View 47
snapshots 10
sound settings 9
SSH 53
SSHD Manager 11
system diagnostics 67
system information
viewing 7
system information screens
hiding 7

T
Task Manager 11
taskbar
using 5
TeemTalk 51
Telnet 55
text editor 11
ThinState. *See* HP ThinState
touch screen settings 9
troubleshooting 66
firmware corruption 66
network connectivity 66
using system diagnostics 67

U
updating clients
broadcast update 57
DHCP tagging update 58
DNS alias update 58
manual update 59
USB redirection
RDP 39
USB Manager 15
VMware Horizon View 46

V
VMware Horizon View
audio redirection 46
certificate security levels 48
certificates 48
changing protocols 47
device redirection 46
keyboard shortcuts 45
mass storage redirection 46
MMR 45
multi-monitor sessions 45
printer redirection 46
settings 42
smart card redirection 47
USB redirection 46
webcam redirection 47
VNC Shadowing 22

W
Web Browser
settings, connection-specific 50
settings, general 50
webcam redirection
VMware Horizon View 47
websites
Citrix support 1
HP support 1
Microsoft support 1
VMware support 1

X
X Terminal 11
XDMCP 53