



HP ThinPro 5.0

Administrator Guide

© Copyright 2014 Hewlett-Packard  
Development Company, L.P.

Microsoft, Windows, and Windows Vista are  
U.S. registered trademarks of the Microsoft  
group of companies.

Confidential computer software. Valid  
license from HP required for possession,  
use or copying. Consistent with FAR 12.211  
and 12.212, Commercial Computer  
Software, Computer Software  
Documentation, and Technical Data for  
Commercial Items are licensed to the U.S.  
Government under vendor's standard  
commercial license.

The information contained herein is subject  
to change without notice. The only  
warranties for HP products and services are  
set forth in the express warranty statements  
accompanying such products and services.  
Nothing herein should be construed as  
constituting an additional warranty. HP shall  
not be liable for technical or editorial errors  
or omissions contained herein.

Second Edition: August 2014

First Edition: June 2014

Document Part Number: 761886-002

## 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 by submitting a request online at <ftp://ftp.hp.com/pub/tcdebian/pool/thinpro50/source/>.



## About this guide

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

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



---

# Table of contents

<b>1 Welcome</b> .....	<b>1</b>
Finding more resources .....	1
Comparison of ThinPro and Smart Zero .....	1
Document organization .....	2
<b>2 Getting started</b> .....	<b>3</b>
<b>3 Navigating the interface</b> .....	<b>4</b>
Using the taskbar .....	4
Using the Connection Manager controls .....	5
Viewing system information .....	6
Hiding the system information screens .....	6
<b>4 Control Panel configurations</b> .....	<b>7</b>
Control Panel overview .....	8
Client aggregation .....	11
Configuring client aggregation .....	12
Configuring the aggregation clients .....	12
Configuring the aggregation server .....	13
Display preferences .....	13
Configuring printers .....	13
Redirecting USB devices .....	14
Network settings .....	14
Wired network settings .....	15
Wireless network settings .....	15
DNS settings .....	16
IPSec rules .....	16
Configuring VPN settings .....	17
Configuring HP Velocity .....	17
Customization Center .....	17
HP ThinState .....	18
Managing an HP ThinPro image .....	18
Capturing an HP ThinPro image to an FTP server .....	18
Deploying an HP ThinPro image using FTP or HTTP .....	19
Capturing an HP ThinPro image to a USB flash drive .....	19
Deploying an HP ThinPro image with a USB flash drive .....	20

Managing an HP ThinPro configuration .....	20
Saving an HP ThinPro configuration to an FTP server .....	20
Restoring an HP ThinPro configuration using FTP or HTTP .....	20
Saving an HP ThinPro configuration to a USB flash drive .....	21
Restoring an HP ThinPro configuration from a USB flash drive .....	21
VNC Shadowing .....	21
Certificates .....	22
Certificate Manager .....	22
SCEP Manager .....	22
DHCP options .....	23
<b>5 Common connection configurations .....</b>	<b>24</b>
Common connection settings .....	24
Kiosk Mode .....	25
<b>6 Citrix connections .....</b>	<b>26</b>
Citrix connection management features .....	26
Citrix Receiver features .....	26
HDX MediaStream support matrix .....	27
Citrix connection support matrix .....	28
Citrix general settings .....	28
Citrix connection-specific settings .....	31
<b>7 RDP connections .....</b>	<b>32</b>
RDP features .....	32
RDP general settings .....	32
RDP connection-specific settings .....	32
Using RemoteFX with RDP .....	35
Using multi-monitor sessions with RDP .....	35
Using multimedia redirection with RDP .....	36
Using device redirection with RDP .....	36
Using USB redirection with RDP .....	36
Using mass storage redirection with RDP .....	37
Using printer redirection with RDP .....	37
Using audio redirection with RDP .....	38
Using smart card redirection with RDP .....	38
<b>8 VMware Horizon View connections .....</b>	<b>39</b>
VMware Horizon View settings .....	39
Using multi-monitor sessions with VMware Horizon View .....	41



Using keyboard shortcuts with VMware Horizon View .....	41
Using Multimedia Redirection with VMware Horizon View .....	42
Using device redirection with VMware Horizon View .....	42
Using USB redirection with VMware Horizon View .....	42
Using mass storage redirection with VMware Horizon View .....	42
Using printer redirection with VMware Horizon View .....	42
Using audio redirection with VMware Horizon View .....	42
Using smart card redirection with VMware Horizon View .....	43
Using webcam redirection with VMware Horizon View .....	43
Changing the VMware Horizon View protocol type .....	44
VMware Horizon View HTTPS and certificate management requirements .....	44
VMware Horizon View USB device families .....	45
<b>9 Web Browser connections .....</b>	<b>47</b>
Web Browser general settings .....	47
Web Browser connection-specific settings .....	47
<b>10 Additional connection types (ThinPro configuration only) .....</b>	<b>48</b>
TeemTalk connection settings .....	48
XDMCP connection settings .....	50
SSH connection settings .....	50
Telnet connection settings .....	52
Custom connection settings .....	52
<b>11 HP Smart Client Services .....</b>	<b>53</b>
Supported operating systems .....	53
Prerequisites for HP Smart Client Services .....	53
Obtaining HP Smart Client Services .....	53
Viewing the Automatic Update website .....	54
Creating an Automatic Update profile .....	54
Updating clients .....	54
Using the broadcast update method .....	54
Using the DHCP tag update method .....	55
Example of performing DHCP tagging .....	55
Using the DNS alias update method .....	55
Using the manual update method .....	56
Performing a manual update .....	56
<b>12 Using the Profile Editor .....</b>	<b>57</b>
Accessing the Profile Editor .....	57

Loading a client profile .....	57
Modifying a client profile .....	57
Selecting the platform of a client profile .....	57
Selecting the connection type of a client profile .....	58
Modifying the registry settings of a client profile .....	58
Enabling or disabling menu items on clients .....	58
Enabling or disabling user configurations on clients .....	58
Adding files to a client profile .....	59
Adding a configuration file to a client profile .....	59
Adding certificates to a client profile .....	59
Adding a symbolic link to a client profile .....	60
Saving the client profile .....	60
Configuring a serial or parallel printer .....	60
Obtaining the printer settings .....	60
Setting up printer ports .....	61
Installing printers on the server .....	61
<b>13 Troubleshooting .....</b>	<b>62</b>
Troubleshooting network connectivity .....	62
Troubleshooting firmware corruption .....	62
Reimaging client device firmware .....	63
Troubleshooting Citrix password expiration .....	63
Using system diagnostics to troubleshoot .....	63
Saving system diagnostic data .....	63
Uncompressing the system diagnostic files .....	63
Uncompressing the system diagnostic files on Windows-based systems .....	64
Uncompressing the system diagnostic files in Linux- or Unix-based systems ..	64
Viewing the system diagnostic files .....	64
Viewing files in the Commands folder .....	64
Viewing files in the /var/log folder .....	64
Viewing files in the /etc folder .....	64
<b>Appendix A USB updates .....</b>	<b>65</b>
<b>Appendix B BIOS tools .....</b>	<b>66</b>
BIOS settings tool .....	66
BIOS flashing tool .....	66
<b>Appendix C Resizing the flash drive partition .....</b>	<b>67</b>

<b>Appendix D Customizing the Smart Zero login screen .....</b>	<b>68</b>
Customizing the screen background .....	68
Common attributes .....	68
Elements .....	70
Image .....	72
Text .....	73
 <b>Appendix E Registry keys .....</b>	 <b>76</b>
root > Audio .....	77
root > CertMgr .....	78
root > ConnectionManager .....	78
root > ConnectionType .....	78
root > ConnectionType > custom .....	79
root > ConnectionType > firefox .....	82
root > ConnectionType > freerdp .....	85
root > ConnectionType > ssh .....	92
root > ConnectionType > teemtalk .....	96
root > ConnectionType > telnet .....	99
root > ConnectionType > view .....	102
root > ConnectionType > xdmcp .....	108
root > ConnectionType > xen .....	112
root > DHCP .....	122
root > Dashboard .....	122
root > Display .....	123
root > Network .....	126
root > SCIM .....	130
root > Serial .....	130
root > SystemInfo .....	131
root > TaskMgr .....	131
root > USB .....	131
root > auto-update .....	135
root > background .....	136
root > config-wizard .....	137
root > desktop .....	137
root > entries .....	138
root > keyboard .....	138
root > logging .....	139
root > mouse .....	140
root > screensaver .....	140
root > security .....	141
root > sshd .....	141

root > time .....	141
root > touchscreen .....	142
root > translation .....	143
root > usb-update .....	143
root > users .....	143
root > vncserver .....	146

<b>Index</b> .....	<b>149</b>
--------------------	------------

# 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 <a href="http://www.hp.com/support">http://www.hp.com/support</a>	Image updates and add-ons Documentation for HP software not covered in detail in this guide <b>TIP:</b> If your search results cannot locate the software you are looking for, search for the thin client model instead.
Microsoft support website <a href="http://support.microsoft.com">http://support.microsoft.com</a>	Documentation for Microsoft software not covered in detail in this guide
Citrix support website <a href="http://www.citrix.com/support">http://www.citrix.com/support</a>	Documentation for Citrix software not covered in detail in this guide
VMware support website <a href="http://www.vmware.com/support">http://www.vmware.com/support</a>	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
<b>Available connection types</b>	<ul style="list-style-type: none"><li>• Citrix</li><li>• RDP</li><li>• VMware Horizon View</li><li>• Web Browser (Firefox)</li><li>• TeamTalk</li><li>• XDMCP</li><li>• SSH</li><li>• Telnet</li><li>• Custom</li></ul>	<ul style="list-style-type: none"><li>• Citrix</li><li>• RDP</li><li>• VMware Horizon View</li><li>• Web Browser (Firefox)</li></ul>
<b>Number of connections supported at a time</b>	Multiple	One
<b>Kiosk Mode default setting</b>	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 4](#)—Provides an overview of the different components of the interface.
- [Control Panel configurations on page 7](#)—Describes the connection-related settings and configurations in the Control Panel and details some of the more advanced configurations.
- [Common connection configurations on page 24](#)—Describes settings that are common to all connection types and configuring a client for Kiosk Mode.
- [Citrix connections on page 26](#)—Describes the settings and configurations for the Citrix connection type.
- [RDP connections on page 32](#)—Describes the settings and configurations for the RDP connection type.
- [VMware Horizon View connections on page 39](#)—Describes the settings and configurations for the VMware Horizon View connection type.
- [Web Browser connections on page 47](#)—Describes the settings for the Web Browser connection type.
- [Additional connection types \(ThinPro configuration only\) on page 48](#)—Describes the settings for the TeamTalk, XDMCP, SSH, Telnet, and Custom connection types.
- [HP Smart Client Services on page 53](#)—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 57](#)—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 62](#)—Describes common troubleshooting issues and solutions.
- [USB updates on page 65](#)—Describes how to install add-ons and profile updates from a USB flash drive.
- [BIOS tools on page 66](#)—Describes how to view and update BIOS settings and flash a new BIOS version.
- [Resizing the flash drive partition on page 67](#)—Describes how to increase the size of the flash drive partition.
- [Customizing the Smart Zero login screen on page 68](#)—Describes the common attributes and elements used in customizing the client login screen background.
- [Registry keys on page 76](#)—Lists the paths, functions, and options for the HP ThinPro registry keys.

---


## 2 Getting started

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 14](#) 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 53](#). 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.

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 18](#)), use the Control Panel to make all of the desired configurations first. See [Navigating the interface on page 4](#) and [Control Panel configurations on page 7](#) 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

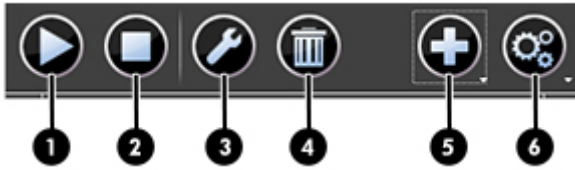


**Table 3-1** Taskbar components

1	<b>Connection Manager</b> —Use to start, stop, add, edit, and delete remote connections. See <a href="#">Using the Connection Manager controls on page 5</a> for more information.
2	<b>Control Panel</b> —Use to configure the client, switch between Administrator Mode and User Mode, and check for software updates. See <a href="#">Control Panel overview on page 8</a> for more information.
3	<b>System Information</b> —Use to view system, network, and software information about the client. See <a href="#">Viewing system information on page 6</a> for more information.
4	<b>Application area</b> —Displays the icons for the currently open applications.  <b>TIP:</b> You can hold down <b>Ctrl+Alt</b> and then press <b>Tab</b> repeatedly to select an application to bring to the foreground.
5	<b>System tray</b> —Provides quick access to the audio mixer and the virtual keyboard, and displays the current network status. If the language is set to Chinese, Japanese, or Korean, an icon providing quick access to the Smart Common Input Method (SCIM) controls will also be shown.
6	<b>Date and time</b> —Displays the current date and time. Click to access the date and time settings.
7	<b>Power button</b> —Use to log out of, reboot, or power off the client.



# Using the Connection Manager controls



1	<b>Start</b> —Starts the selected connection.
2	<b>Stop</b> —Stops the selected connection.
3	<b>Edit</b> —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	<b>Delete</b> —Deletes the selected connection.
5	<b>Add</b> —Allows you to add a new connection.  <b>NOTE:</b> See <a href="#">Comparison of ThinPro and Smart Zero on page 1</a> for a list of the available connection types.
6	<b>Settings</b> —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 24](#)
- [Citrix connections on page 26](#)
- [RDP connections on page 32](#)
- [VMware Horizon View connections on page 39](#)
- [Web Browser connections on page 47](#)
- [Additional connection types \(ThinPro configuration only\) on page 48](#)

## 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: <ul style="list-style-type: none"><li>• <b>Ping</b>—Specify an IP address of another device on the network to attempt to establish contact.</li><li>• <b>DNS Lookup</b>—Use this tool to resolve a domain name into an IP address.</li><li>• <b>Trace Route</b>—Use this tool to track the path that a network packet takes from one device to another.</li></ul>
Software Information	Displays the name and version number of the software installed on the client.
System Logs	Displays the following logs: <ul style="list-style-type: none"><li>• Network Manager</li><li>• Smart Zero Client Service</li><li>• DHCP Wired Leases</li><li>• DHCP Wireless Leases</li><li>• Kernel</li><li>• X Server</li><li>• Connection Manager</li></ul> Check <b>Enable Debug Mode</b> to display additional information that might be requested by HP support for troubleshooting purposes.  Click <b>Diagnostic</b> to save a diagnostic file. For more information, see <a href="#">Using system diagnostics to troubleshoot on page 63</a> .

## Hiding the system information screens

See [root > SystemInfo on page 131](#) 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 <a href="#">Client aggregation on page 11</a> .
Display Preferences	Lets you configure and test options for both a primary and secondary display.  For more information, see <a href="#">Display preferences on page 13</a> .
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 <a href="#">Configuring printers on page 13</a> .
Touch Screen	Lets you configure touch screen options.
USB Manager	Lets you configure the redirection options for USB devices.  For more information, see <a href="#">Redirecting USB devices on page 14</a> .
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 <a href="http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page">http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page</a> .

**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 <a href="#">Network settings on page 14</a> .
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: <ul style="list-style-type: none"><li>• Switch between the ThinPro and Smart Zero configurations</li><li>• Configure desktop and taskbar options</li><li>• Select which connection types and control panel utilities standard users have access to</li></ul> For more information, see <a href="#">Customization Center on page 17</a> .

**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.  <b>NOTE:</b> 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 <i>HP Device Manager Administrator Guide</i> .
Automatic Update	Lets you configure the Automatic Update server manually. For more information, see <a href="#">HP Smart Client Services on page 53</a> .
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. For more information about HP Easy Tools, see the <i>HP Easy Tools Administrator Guide</i> .
Snapshots	Lets you restore the client to a previous state or to its default factory configuration.
SSHD Manager	Enables access through a secure shell.

**Table 4-3 Control Panel > Management (continued)**

Menu option	Description
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 <a href="#">HP ThinState on page 18</a> .
VNC Shadow	Lets you configure VNC Shadowing options.  For more information, see <a href="#">VNC Shadowing on page 21</a> .

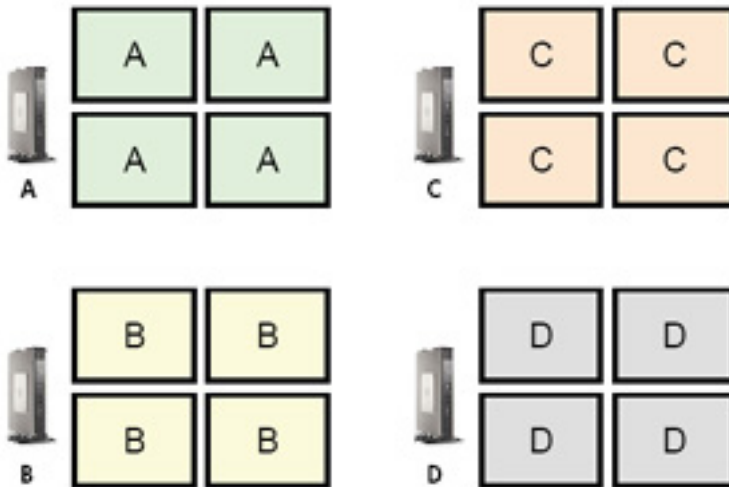
**Table 4-4 Control Panel > Advanced**

Menu option	Description
Certificates	Opens the Certificate Manager, which lets you easily import, view, or remove certificates.  For more information, see <a href="#">Certificate Manager on page 22</a> .
CPU Manager	Lets you choose between <b>Balanced</b> and <b>High Performance</b> CPU performance.
DHCP Options	Lets you configure DHCP options.  For more information, see <a href="#">DHCP options on page 23</a> .
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.

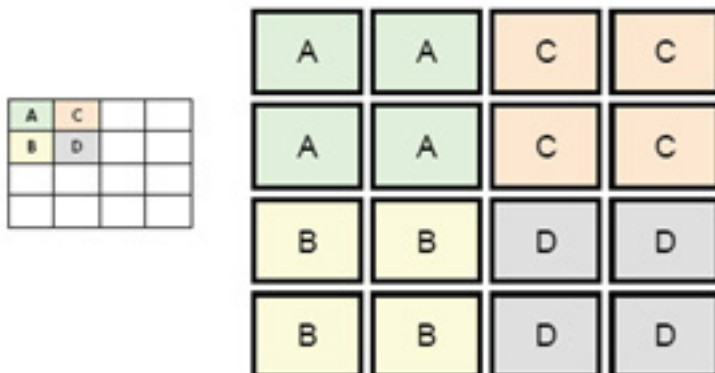
## Client aggregation

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.

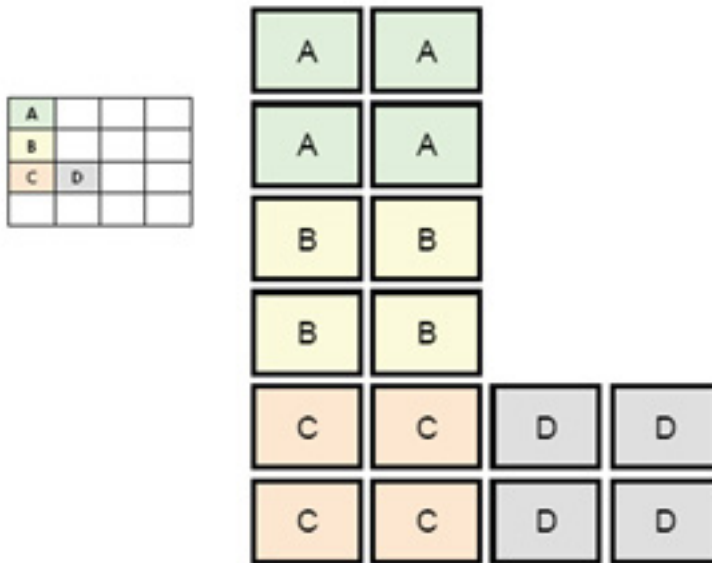


Client aggregation allows you to arrange the four clients on a 4x4 grid. The following illustration shows one possible arrangement.



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 12](#)
2. [Configuring the aggregation server on page 13](#)

## 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.
- 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 <b>Automatic</b> .
Connection Method	Lets you choose between <b>Automatic</b> and <b>Static</b> . If your network environment is using DHCP, then the <b>Automatic</b> option should work without any further configurations needed.  If <b>Static</b> is selected, the <b>Static Address Configuration</b> 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: <ul style="list-style-type: none"> <li>• None</li> <li>• 802.1X-TTLS</li> <li>• 802.1X-PEAP</li> <li>• 802.1X-TLS</li> </ul> <p>Note the following about TTLS and PEAP:</p> <ul style="list-style-type: none"> <li>• The <b>Inner Authentication</b> option should be set to whatever your server supports.</li> <li>• The <b>CA Certificate</b> setting should point to the server's certificate on the local client.</li> <li>• The <b>Username</b> and <b>Password</b> are the user's credentials.</li> </ul> <p>Note the following about TLS:</p> <ul style="list-style-type: none"> <li>• The <b>CA Certificate</b> setting should point to the server's certificate on the local client.</li> <li>• If your <b>Private Key</b> file is .p12 or .pfx, then the <b>User Certificate</b> setting can be left blank.</li> <li>• The <b>Identity</b> setting should be the username that corresponds to the user certificate.</li> <li>• The <b>Private Key Password</b> setting is the password of the user's private key file.</li> </ul>

## 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.
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).

Option	Description
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 <b>Automatic</b> and <b>Static</b> . If your network environment is using DHCP, then the <b>Automatic</b> option should work without any further configurations.  If <b>Static</b> is selected, the <b>Static Address Configuration</b> 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: <ul style="list-style-type: none"> <li>• None</li> <li>• WEP</li> <li>• WPA/WPA2-PSK</li> <li>• 802.1X-TTLS</li> <li>• 802.1X-PEAP</li> <li>• 802.1X-TLS</li> <li>• EAP FAST</li> </ul> <p>For WEP and WPA/WPA2-PSK, you just need to enter the network key and click <b>OK</b>.</p> <p>For EAP-FAST, set <b>Anonymous Identity</b>, <b>Username</b>, <b>Password</b>, and <b>Provisioning Method</b>. You do not need to change the PAC file settings.</p> <p>See <a href="#">Wired network settings on page 15</a> for more information about TTLS, PEAP, and TLS.</p>

## 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	Use these boxes to set proxy server information using the following format:
FTP Proxy	<code>http://&lt;ProxyServer&gt;:&lt;Port&gt;</code>
HTTPs Proxy	HP recommends using the <code>http://</code> prefix for all three proxy settings because it is supported better.
	<b>NOTE:</b> The proxy settings are set to the <code>http_proxy</code> , <code>ftp_proxy</code> , and <code>https_proxy</code> 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 <b>Administrator/User Mode Switch</b> option from the Control Panel in User Mode.
Enable X host access control security	When enabled, only the systems listed in the <b>XHost Access Control List</b> area are allowed to remotely control the thin client.
Enable USB Update	Enables updates to be installed from a USB flash drive. See <a href="#">USB updates on page 65</a> 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 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. 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 configuration

An HP ThinPro configuration file contains the connections and settings configured using the Control Panel utilities. A configuration file is specific to the version of HP ThinPro in which it was created.

### Saving an HP ThinPro configuration to an FTP server

To save an HP ThinPro configuration to an FTP server:

---

 **IMPORTANT:** The directory on the FTP server where you intend to save the configuration file 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 configuration using FTP or HTTP

To restore an HP ThinPro configuration 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 configuration to a USB flash drive

To save an HP ThinPro configuration 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 configuration from a USB flash drive

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

1. Insert the USB flash drive containing the configuration file 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.

Option	Description
VNC Read Only	Makes the VNC session read-only.
VNC Use Password	Makes a password required when accessing the client using VNC. Click <b>Set Password</b> 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 59](#).

 **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.  <b>NOTE:</b> This option is not available for the VMware Horizon View connection type.
Auto start priority	Determines the order that connections will auto-start. <b>0</b> means auto-start is disabled. The other values determine the startup order, with <b>1</b> being the highest priority.
Share credentials with screensaver	Enables users to unlock the local screensaver using their credentials for that connection.  <b>NOTE:</b> 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.  <b>NOTE:</b> 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.

# 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 17](#)) 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 support matrix on page 27](#) 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 support matrix

---

 **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	<ul style="list-style-type: none"><li>• 24 fps</li></ul>
Resolution	<ul style="list-style-type: none"><li>• 1080p</li><li>• 720p</li></ul>
Video containers	<ul style="list-style-type: none"><li>• WMV</li><li>• AVI</li><li>• MPG</li><li>• MPEG</li><li>• MOV</li><li>• MP4</li></ul>
Video codecs	<ul style="list-style-type: none"><li>• WMV2</li><li>• WMV3 / VC-1</li><li>• H.264 / AVC / MPEG-4 Part 10</li></ul>

**Table 6-1** HDX MediaStream support matrix (continued)

Feature	Support
	<ul style="list-style-type: none"> <li>• MPEG-4 Part 2</li> <li>• H.263</li> <li>• DivX</li> <li>• Xvid</li> <li>• MPEG1</li> </ul>
Audio codecs	<ul style="list-style-type: none"> <li>• MP3</li> <li>• WMA</li> <li>• AAC</li> <li>• PCM</li> <li>• mpeg-audio</li> <li>• MLAW / ULAW</li> </ul>

## 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 5](#).

**Table 6-3** XEN Connection General Settings Manager > Options

Option	Description
Enable 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.



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

Option	Description
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 Off Screen Surface	Directs the ICA Client to draw screen updates to an in-memory bitmap rather than to the screen, improving bandwidth efficiency.
Enable Session Sharing	Enable the session to be shared.
Enable Auto Reconnect	Enable automatic reconnection of dropped connections.
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
Minimum Bitmap Cache Size	Minimize the bitmap cache size.
Use Data Compression	Use data compression for this connection.
Enable Middle Button Paste	Enables a middle mouse button click to perform a paste operation.
Use Disk Cache for Bitmaps	Use a disk cache for connection bitmaps.
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.
Webcam/Headset Optimizations	Uses high-level webcam/headset redirection.
Sound	Specifies the sound quality to be used. Valid options are: <b>High Quality</b> , <b>Med Quality</b> , and <b>Low Quality</b> .
Speed Screen	Valid options are: <b>Auto</b> , <b>On</b> , and <b>Off</b> .
Mouse Click Feedback	Valid options are: <b>Auto</b> , <b>On</b> , and <b>Off</b> .
Local Text Echo	Controls keyboard latency reduction. The recommended setting is <b>Auto</b> .
Encryption Level	Specifies the encryption level of an ICA session.
Monitor Network Connectivity	Exits to the local GUI if the network connection is broken.

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

Option	Description
Allow Audio Input	Allow audio input from the thin client.

**Table 6-4 XEN Connection General Settings Manager > Local Resources (continued)**

Option	Description
Auto Printer Creation	Automatically create a printer.
Enable Dynamic Drive Mapping	Automatically maps USB devices that are plugged in during the session.
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
Enable Seamless Windows	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: <b>Full Screen</b> , <b>Fixed Size</b> , <b>Percentage of Screen Size</b> .
Default Window Colors	Establish the default window colors. Options are: <b>16</b> , <b>256</b> , <b>16-bit</b> , <b>24-bit</b> , <b>Automatic</b> .
Default 256 Color Mapping	This option is only enabled if <b>Default Window Colors</b> is set to <b>256</b> . Options are: <b>Shared - Approximate Colors</b> and <b>Private - Exact Colors</b> .

**Table 6-6 XEN Connection General Settings Manager > Firewall**

Option	Description
Proxy Type	Options are: <b>None - direct</b> , <b>SOCKS</b> , <b>Secure - HTTPS</b> , <b>Use browser settings</b> , <b>Automatically detect proxy</b> .
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
Handling of keyboard shortcuts	Specifies how function keys should be handled. Options are: <b>Translated</b> , <b>Direct in full screen desktops only</b> , and <b>Direct</b> .
Stop Direct key handling	Not enabled when the option <b>Handling of keyboard shortcuts</b> is set to <b>Translated</b> .
<List of keyboard shortcuts>	Only enabled when <b>Handling of keyboard shortcuts</b> is <b>Translated</b> or <b>Direct in full screen desktops only</b> .

**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.
Auto Logout Delay with Single App	When using a Citrix server with a single published resource, this specifies the number of seconds between the closing of a Xen published resource and when the user is automatically logged out and returned to the initial login screen.

**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 5](#).

**Table 6-9 Citrix Connection Manager > Page 1**

Option	Description
Name	The connection name.
Server 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.
Storefront Connection	Indicates that this connection is to Citrix's new StoreFront connection service.
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.
Show applications on desktop	Shows remote resources on the local desktop.



**NOTE:** See [Common connection settings on page 24](#) 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

## RDP general settings

The following table describes the settings available in the RDP7 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 5](#).

**Table 7-1 RDP7 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 RDP7 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 5](#).

**Table 7-2 RDP7 Connection Manager > Page 1**

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 RDP7 Connection Manager > Page 2**

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	Sets the window size to <b>full</b> , <b>fixed</b> , or <b>percent</b> .
	Alternate Shell	
Percentage Size	Standard Desktop	If <b>Window Size</b> is set to <b>percent</b> , this option sets the percentage of the screen that a desktop window occupies.  <b>NOTE:</b> The resulting sizes might be rounded. <b>NOTE:</b> RemoteFX supports only a fixed list of resolutions.
	Alternate Shell	
Fixed Size	Standard Desktop	If <b>Window Size</b> is set to <b>fixed</b> , this option sets the width and height in pixels that the desktop window occupies.
	Alternate Shell	
Application	Remote Application	Specifies the path of the application to run.  If using RDP Seamless Windows mode, type the path of <code>seamlessrdpshell.exe</code> on your server, followed by a space and then the path of the application to run. See the following example:  <code>c:\seamless\seamlessrdpshell.exe c:\Program Files\Microsoft\Word.exe</code>
Command	Alternate Shell	Specifies the application that will run in <b>Alternate Shell</b> mode. Enter the command that executes the application. For example, to run Microsoft Word, type <code>Word.exe</code> .
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 <code>C:\Program Files\Microsoft</code> .

**Table 7-4 RDP7 Connection Manager > Page 3**

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 certificate check	If enabled, the validity of the RDP server's identity and certificate are verified.
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.
Hostname to send	Normally, the client's hostname is used for Client Access Licenses. This field allows a different value to be sent.

**Table 7-5 RDP7 Connection Manager > Page 4**


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 RDP7 Connection Manager > Page 5**

Option	Description
Choose your connection speed to optimize performance	<p>Selecting a connection speed (<b>LAN</b>, <b>Broadband</b>, or <b>Modem</b>) will enable or disable the following options to optimize performance:</p> <ul style="list-style-type: none"> <li>• <b>Desktop background</b></li> <li>• <b>Font smoothing</b></li> <li>• <b>Desktop composition</b></li> <li>• <b>Show contents of window while dragging</b></li> <li>• <b>Menu and window animation</b></li> <li>• <b>Themes</b></li> </ul>

**Table 7-6 RDP7 Connection Manager > Page 5 (continued)**

Option	Description
	Selecting <b>Client Preferred Settings</b> 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.
Warning Timeout	Specifies the amount of time in milliseconds 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.  <b>TIP:</b> HP recommends increasing the timeout value for networks that experience frequent busy periods or momentary outages.
Recovery Timeout	Specifies the amount of time in milliseconds 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 milliseconds 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 24](#) for information about the settings available on the final page of the RDP7 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 value 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**

## 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 RDP7 Connection Manager.

---

 **NOTE:** When using RFX, the supported screen resolution is 1280x768 only. This causes small black bars to appear on the sides of the connection.

 **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 value of the following registry key value 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 value 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
<code>root/USB/root/holdProtocolStatic</code>	1	Makes sure that the USBR type will not be automatically changed when a connection is set or unset
<code>root/USB/root/protocol</code>	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 60](#) 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 RDP7 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 USB device families](#)

## 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 5](#).

**Table 8-1 VMware Horizon View Connection Manager > Page 1**

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 > Page 2**

Option	Description
Automatic login	When enabled, the user is automatically logged in when the connection is established. <b>NOTE:</b> HP recommends enabling this option.
Allow Smartcard login	Enables smart card login. <b>NOTE:</b> For more information on smart cards, see <a href="#">Using smart card redirection with VMware Horizon View on page 43</a> .

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

Option	Description
Close After Disconnect	<p>Makes the VMware Horizon View client close automatically after users log out of their desktops or the session terminates with an error.</p> <p>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.</p> <p>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.</p>
Hide top Menu bar	<p>Makes the top menu bar invisible for users.</p> <p>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.</p>
Connection Security Level	<p>Use the <b>Connection Security Level</b> to adjust the security level that the VMware Horizon View client uses when connecting to the server.</p> <p><b>NOTE:</b> For more information, see <a href="#">VMware Horizon View HTTPS and certificate management requirements on page 44</a> for details on how connection security levels behave.</p>
Command Line Arguments	<p>Enter any desired command line arguments to be used for the connection.</p> <p>For more help on using advanced command line arguments, do one of the following:</p> <ul style="list-style-type: none"> <li>On the command line, enter <code>vmware-view--help</code>.</li> <li>See the Linux Horizon View client documentation provided by VMware at <a href="http://www.vmware.com">http://www.vmware.com</a>.</li> </ul> <p><b>NOTE:</b> This option does not apply to the Teradici-accelerated PCoIP client.</p>

**Table 8-3 VMware Horizon View Connection Manager > Page 3**


Option	Description
Enable motion events	Enables motion events for this connection.
Enable data compression	Uses data compression for this connection.
Enable 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.
Hostname to send	Sends the hostname to the remote system for this connection.
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	<p>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.</p> <p>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</p>

**Table 8-3 VMware Horizon View Connection Manager > Page 3 (continued)**

Option	Description
	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 <b>Model</b> in the printer properties.

**Table 8-4 VMware Horizon View Connection Manager > Page 4**

Option	Description
Enable MMR	Enables multimedia redirection.
Choose your connection speed to optimize performance	<p>Selecting a connection speed (<b>LAN</b>, <b>Broadband</b>, or <b>Modem</b>) will enable or disable the following options to optimize performance:</p> <ul style="list-style-type: none"><li>• <b>Desktop background</b></li><li>• <b>Font smoothing</b></li><li>• <b>Desktop composition</b></li><li>• <b>Show contents of window while dragging</b></li><li>• <b>Menu and window animation</b></li><li>• <b>Themes</b></li></ul> <p>Selecting <b>Client Preferred Settings</b> will allow the client to choose which options to use. You can also select your own custom combination of options.</p>

 **NOTE:** See [Common connection settings on page 24](#) 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** options 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 36](#).

## 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 36](#).

### 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 37](#).

### 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 37](#) 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\DisableAudioCapture` 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 38](#) 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 36](#) 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 under **Desktop**, select a pool that supports one of the following protocols:
  - PCoIP
  - RDP 2
2. On the pull-down list, select a connection type.

 **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 8-5** VMware Horizon View certificate security levels

		Security level		
		Refuse insecure connections	Warn	Allow all connections
Certificate trust	Trusted	Trusted	Trusted	Trusted



**Table 8-5 VMware Horizon View certificate security levels (continued)**

		Security level		
<b>Self-signed</b>	Error	Warning	Warning	Untrusted
<b>Expired</b>	Error	Warning	Warning	Untrusted
<b>Untrusted</b>	Error	Error	Error	Untrusted

**Table 8-6 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
Warning	Connects with a certificate warning dialog and displays a red unlock icon
Error	Does not allow the connection

## VMware Horizon View USB device families

**Table 8-7 VMware Horizon View USB device families**

Family	Family name
Vendor	vendor
Unknown	unknown
Other	other
Audio In	audio-in
Audio Out	audio-out
Communications	comm
Human Interface Device	hid
Bootable HID	hid-bootable
Force Feedback Device	physical
Imaging	imaging
Printer	printer
Mass Storage	storage
Smartcard Reader	smart-card
Security	security
Video	video
Wireless Adapter	wireless
Bluetooth	bluetooth

**Table 8-7** VMware Horizon View USB device families (continued)


<b>Family</b>	<b>Family name</b>
Wireless USB	wusb
PDA	Pda

# 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 5](#).

**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 5](#).

**Table 9-2 Web Browser Connection Manager > Page 1**

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 24](#) 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 5](#).

**Table 10-1 TeemTalk Connection Manager**

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 24](#) 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 on page 48](#).

**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: <b>TCP/IP</b> , <b>Serial</b> , <b>SSH2</b> , and <b>SSL</b> .
Connection	The connection method to be used. Advanced connection options can be configured via the button.
Emulation	Emulation types are: <b>hp70092</b> , <b>IBM 3151</b> , <b>IBM3270 Display</b> , <b>IBM3270 Printer</b> , <b>IBM5250 Display</b> , <b>IBM5250 Printer</b> , <b>MD Prism</b> , <b>TA6530</b> , <b>VT Series</b> , and <b>Wyse</b> .

**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 <a href="#">Table 10-5 TeemTalk Session Wizard &gt; Page 3 &gt; Preferences on page 49</a> .
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 <b>Save Preferences</b> . It will be restored on the next system launch.  <b>NOTE:</b> Click <b>Save Preferences</b> 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.  <b>NOTE:</b> This option does not become effective until the next system launch and overrides the <b>Show Configuration Bar</b> and <b>Save Current Window Position</b> 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:  <code>/ display html links Firefox</code>
Command Line Start Up Options	Use to specify an alternate location for the startup options.  <b>NOTE:</b> For specific information on HP TeemTalk Command Line Startup Options, see the <i>HP TeemTalk Terminal Emulator User Guide</i> .


**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 5](#).

**Table 10-7** New XDMCP connection configuration settings


Option	Description
Name	The connection name.
Type	The XDMCP connection type. Valid options are: <b>chooser</b> , <b>query</b> , and <b>broadcast</b> .
Address	This value is required if the <b>Type</b> value is set to <b>query</b> .
Use font server	Use a remote X font server instead of locally installed fonts.
Font server	Font server is not enabled unless the <b>Use font server</b> 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 24](#) 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 SSH 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 5](#).

**Table 10-8** New SSH connection configuration settings


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: <b>7X14</b> , <b>5X7</b> , <b>5X8</b> , <b>6X9</b> , <b>6X12</b> , <b>7X13</b> , <b>8X13</b> , <b>8X16</b> , <b>9X15</b> , <b>10X20</b> , and <b>12X24</b> .

 **NOTE:** See [Common connection settings on page 24](#) 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 5](#).

**Table 10-9** New Telnet connection configuration settings


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: <b>7X14</b> , <b>5X7</b> , <b>5X8</b> , <b>6X9</b> , <b>6X12</b> , <b>6X13</b> , <b>7X13</b> , <b>8X13</b> , <b>8X16</b> , <b>9X15</b> , <b>10X20</b> , and <b>12X24</b> .

 **NOTE:** See [Common connection settings on page 24](#) 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 5](#).

**Table 10-10** New Custom connection configuration settings

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 24](#) 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 57](#)) 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 62](#).

## 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 <code>auto-update</code> .
Data Type	Select <b>String</b> .
Code	Type <code>137</code> .
Description	Type <code>HP Automatic Update</code> .

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. 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. The client profile contains connection information, settings, and files that the clients download and use in the self-configuration process.

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 76](#) 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 60](#).

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=0.815 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 17](#)), you can easily install add-ons and deploy profiles using a USB flash drive.

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
<code>hptc-bios-cfg -g [options] [filename]</code>	Retrieves the current BIOS settings and saves them to the specified file so they can be viewed or modified (CPQSETUP.TXT by default).
<code>hptc-bios-cfg -s [options] [filename]</code>	Writes the BIOS settings from the specified file (CPQSETUP.TXT by default) to the BIOS.
<code>hptc-bios-cfg -h</code>	Displays a list of options. The options are platform-dependent, so use this command to view the options that are available for that particular platform.

### BIOS flashing tool

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

Syntax	Description
<code>hptc-bios-flash [options] &lt;ImageName&gt;</code>	Flashes the BIOS with the specified BIOS image.
<code>hptc-bios-cfg -h</code>	Displays a list of options. The options are platform dependent, so use this command to view the options that are available for your particular platform.

---

## 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.

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

Syntax	Description
<code>resize-image</code>	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.  <b>NOTE:</b> It is not possible to decrease the partition size. The entered value must be larger than the current partition size.
<code>resize-image--size &lt;size&gt;</code>	Using this syntax, you can provide directly the target partition size as a parameter, and then confirm the change.
<code>resize-image--no-prompt</code> —or— <code>resize-image--no-prompt--size &lt;size&gt;</code>	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.  <b>TIP:</b> 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 <b>alignment</b> table as well.

**Table D-7 Login Screen > Common Attributes > alignment**

Type	Description
Parameter	[left   hcenter   right] [top   vcenter bottom]
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   desktop   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	<b>name, color, padding</b> <ul style="list-style-type: none"> <li><b>color</b>—specifies the solid background color of the screen, if no gradients are specified</li> </ul>

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

Type	Description
	<ul style="list-style-type: none"> <li><b>padding</b>—specifies the default padding for all subsequent elements</li> </ul>

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

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

**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   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   squared]
Example	metric: linear;
Default	squared
Use	For radial gradients, the metric specifies whether the color interpolation between points is done with a dx <sup>2</sup> +dy <sup>2</sup> 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	<p>When in the matching locale, this text will be used for the string. The supported text strings are as follows:</p> <ul style="list-style-type: none"> <li>• de_DE (German)</li> <li>• en_US (English)</li> <li>• es_ES (Spanish)</li> <li>• fr_FR (French)</li> <li>• ja_JP (Japanese)</li> <li>• zh_CN (Simplified Chinese)</li> </ul> <p><b>NOTE:</b> The file encoding is UTF-8.</p>

**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	<p>If no matching localized text is specified, this text string will be used instead.</p> <p><b>NOTE:</b> The text rendering engine does not support HTML-style markup.</p>

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

Type	Description
Parameter	locale-specific fontName
Example	font-ja_JP: kochi-gothic;
Default	Not applicable
Use	<p>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 <b>/usr/share/fonts/ truetype</b>. For Japanese text, it might be necessary to select kochi-gothic; for Simplified Chinese text, u mi ng.</p>

**Table D-23** Login screen > Text > font

Type	Description
Parameter	fontName

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

Type	Description
Example	font: DejaVuSerif-Bold
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 settings of these registry keys can be modified in two different ways:

- 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

This section describes the registry keys, functions, options, and descriptions in the **root > Audio** folder.

**Table E-1** root > Audio

Registry key	Description
root/Audio/AdjustSoundPath	Indicates the full path to the default sound played when the playback volume is changed through the audio mixer control panel or systray. By default, this is a three-chord ding.
root/Audio/OutputMute	<b>1</b> —Mute the internal speaker and headphone jack. <b>0</b> —Do not mute the internal speaker and headphone jack.
root/Audio/OutputScale	Indicates the volume scale setting (1–400) for the internal speaker and headphone jack.
root/Audio/OutputScaleAuto	When set to <b>1</b> (auto mode), OutputScale is set to 130 on the t610 and t610 PLUS, set to 63 on the t5565 and t510, and set to 100 for all other hardware. <b>1</b> —Sets OutputScale value on basis of hardware type. <b>0</b> —Does not set OutputScale value on basis of hardware type.
root/Audio/OutputVolume	Indicates the volume setting for the internal speaker and headphone jack, scaling from 1 to 100.
root/Audio/PlaybackDevice	Indicates the device to use for playback. <b>1</b> is the internal audio controller. <b>2</b> and <b>3</b> are for additional devices, such as a USB headset.
root/Audio/RecordDevice	Indicates the device to use for capture. <b>0</b> is automatic. <b>1</b> is the internal audio controller. <b>2</b> and <b>3</b> are for additional devices, such as a USB headset.
root/Audio/RecordMute	<b>1</b> —Mute the microphone jack. <b>0</b> —Do not mute the microphone jack.
root/Audio/RecordScale	Indicates the volume scale setting (1–400) for the microphone jack.
root/Audio/RecordScaleAuto	When set to <b>1</b> (auto mode), RecordScale is set to 100.

**Table E-1** root > Audio (continued)

Registry key	Description
	1—Sets RecordScale value on basis of hardware type. 0—Does not set RecordScale value on basis of hardware type.
root/Audio/RecordVolume	Indicates the volume setting for the microphone jack, scaling from 1 to 100.
root/Audio/VisibleInSystray	Indicates whether a speaker icon is visible in the system tray. 0—Icon is not visible 1—Icon is visible

## root > CertMgr

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

## root > ConnectionManager

This section describes the registry keys, functions, options, and descriptions in the **root > ConnectionManager** folder.

**Table E-2** root > ConnectionManager

Registry key	Description
root/ConnectionManager/customLogoPath	
root/ConnectionManager/defaultConnection	This must be set to a valid connection using the format '[type]:[label]' to properly launch a connection at startup. For example, 'xen:Default Connection'.
root/ConnectionManager/minHeight	The default is 260.
root/ConnectionManager/minWidth	The default is 400.
root/ConnectionManager/splashLogoPath	Indicates the full path to the default image displayed while a connection is loading. This is the splash screen that will be seen after clicking <b>Connect</b> on the HP ThinPro control panel.
root/ConnectionManager/useKioskMode	
root/ConnectionManager/useSplashOnConnectionStartup	By default, this is disabled for Smart Zero and enabled for ThinPro. Set to '1' to enable the splash screen image specified by 'splashLogoPath' on connection startup.

## root > ConnectionType

This section describes the registry keys, functions, options, and descriptions in the **root > ConnectionType** folders as follows.

## root > ConnectionType > custom

This section describes the registry keys and functions in the **root > ConnectionType > custom** folder.

**Table E-3** root > ConnectionType > custom

Registry key	Description
root/ConnectionType/custom/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/custom/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/custom/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/custom/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/custom/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>1</b> to allow, <b>0</b> to deny access. <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>0</b> .
root/ConnectionType/custom/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow, <b>0</b> to deny access. <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/custom/connections/{UUID}/autoReconnect	When set to <b>1</b> , the connection will be restarted when it is closed or disconnected. This is frequently useful for kiosk style applications. When set to <b>0</b> , the connection will not restart when closed or disconnected.
root/ConnectionType/custom/connections/{UUID}/autoReconnectDelay	Indicates the amount of time in seconds to wait before restarting the connection. The default of <b>0</b> will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to <b>1</b> .
root/ConnectionType/custom/connections/{UUID}/autostart	When set to <b>1</b> , the connection will be automatically started on boot. This is useful for kiosk style applications. By default, connections are not automatically started.
root/ConnectionType/custom/connections/{UUID}/autostartDelay	Indicates the amount of time in seconds to wait before starting the connection on boot. The default of <b>0</b> will cause the connection to start immediately upon boot. This setting takes effect only when 'autostart' is set to <b>1</b> .
root/ConnectionType/custom/connections/{UUID}/beforeStartingCommand	Indicates the command to execute before the connection starts.
root/ConnectionType/custom/connections/{UUID}/command	Indicates the real command for the custom connection to execute.
root/ConnectionType/custom/connections/{UUID}/connectionEndAction	This key is reserved for use.
root/ConnectionType/custom/connections/{UUID}/coord	This key is reserved for use.

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

Registry key	Description
root/ConnectionType/custom/connections/{UUID}/dependConnectionId	This key is reserved for use.
root/ConnectionType/custom/connections/{UUID} / extraEnvValues/{UUID}/key	Indicates the extra environment variable for a custom connection.
root/ConnectionType/custom/connections/{UUID} / extraEnvValues/{UUID}/value	Indicates the extra environment variable value for a custom connection.
root/ConnectionType/custom/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to <code>root/ConnectionType/&lt;type&gt;/connections/</code> . This can be set in the SSH connection's UI.
root/ConnectionType/custom/connections/{UUID}/hasDesktopIcon	Enables or disables the desktop icon for a telnet connection.
root/ConnectionType/custom/connections/{UUID}/label	The name of the connection. For Smart Zero, this will typically be set to 'Default Connection' and does not show in the user interface.
root/ConnectionType/custom/connections/{UUID}/startMode	If set to the default <b>focus</b> 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 makes sure that on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/custom/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/generalSettingsEditor	The internal application name to use when launching the general settings editor for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This icon is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/custom/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/custom/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/custom/coreSettings/label	The name to display for this connection type in the connection type selection menu.

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

Registry key	Description
root/ConnectionType/custom/coreSettings/serverRequired	Indicates whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/custom/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process.
root/ConnectionType/custom/coreSettings/watchPid	If set to <b>1</b> , the application specified by 'appName' is monitored to detect the connection. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/wrapperScript	The name of 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	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/custom/gui/CustomManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/custom/gui/CustomManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/custom/gui/CustomManager/widgets/ autoReconnect	Controls the state for the <b>Auto reconnect</b> widget in the Custom Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/ autostart	Controls the state for the <b>Auto start priority</b> widget in the Custom Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/ command	Controls the state for the <b>Enter command to run</b> widget in the Custom Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/ fallBackConnection	Controls the state for the <b>Fallback Connection</b> widget in the Custom Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/ hasDesktopIcon	Controls the state for the <b>Show icon on desktop</b> widget in the Custom Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/ label	Controls the state for the <b>Name</b> widget in the Custom Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the

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

Registry key	Description
	widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/waitForNetwork	Controls the state for the <b>Wait for network before connection</b> widget in the Custom Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

## root > ConnectionType > firefox

This section describes the registry keys and functions in the **root > ConnectionType > firefox** folder.

**Table E-4** root > ConnectionType > firefox

Registry key	Description
root/ConnectionType/firefox/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/firefox/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/firefox/connections/{UUID}/address	The IP or hostname of the remote host to connect to.
root/ConnectionType/firefox/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/firefox/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/firefox/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>0</b> .
root/ConnectionType/firefox/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/firefox/connections/{UUID}/autoReconnect	When set to <b>1</b> , the connection will be restarted when it is closed or disconnected. This is frequently useful for kiosk style applications. When set to <b>0</b> , the connection will not restart when closed or disconnected.
root/ConnectionType/firefox/connections/{UUID}/autoReconnectDelay	Indicates the amount of time in seconds to wait before restarting the connection. The default of <b>0</b> will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to <b>1</b> .
root/ConnectionType/firefox/connections/{UUID}/autostart	When set to <b>1</b> , the connection will be automatically started on boot. This is useful for kiosk style applications. By default, connections are not automatically started.

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

Registry key	Description
root/ConnectionType/firefox/connections/{UUID}/autostartDelay	Indicates the amount of time in seconds to wait before starting the connection on boot. The default of 0 will cause the connection to start immediately upon boot. This setting takes effect only when 'autostart' is set to 1.
root/ConnectionType/firefox/connections/{UUID}/beforeStartingCommand	The command to execute before the connection starts.
root/ConnectionType/firefox/connections/{UUID}/connectionEndAction	This key is reserved for use.
root/ConnectionType/firefox/connections/{UUID}/coord	This key is reserved for use.
root/ConnectionType/firefox/connections/{UUID}/dependConnectionId	This key is reserved for use.
root/ConnectionType/firefox/connections/{UUID}/enablePrintDialog	Indicates whether the user is allowed to use the Print dialog of the Web Browser.
root/ConnectionType/firefox/connections/{UUID} / extraEnvValues/{UUID}key	The extra environment variable for the connection.
root/ConnectionType/firefox/connections/{UUID} / extraEnvValues/{UUID}value	The extra environment variable value for the connection.
root/ConnectionType/firefox/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to root/ConnectionType/<type>/connections/.
root/ConnectionType/firefox/connections/{UUID}/fullscreen	Enables the Web Browser to start in full-screen mode.
root/ConnectionType/firefox/connections/{UUID}/hasDesktopIcon	If set to 1, an icon for the connection will be shown on the desktop. Not applicable to Smart Zero.
root/ConnectionType/firefox/connections/{UUID}/kioskMode	Enables the Web Browser's Kiosk Mode.
root/ConnectionType/firefox/connections/{UUID}/label	The name of the connection. For Smart Zero, this will typically be set to 'Default Connection' and does not show in the user interface.
root/ConnectionType/firefox/connections/{UUID}/startMode	If set to the default <b>focus</b> 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/firefox/connections/{UUID}/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This makes sure that on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/firefox/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.

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

Registry key	Description
root/ConnectionType/firefox/coreSettings/generalSettingsEditor	The internal application name to use when launching the general settings editor for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This icon is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/firefox/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/firefox/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/firefox/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/firefox/coreSettings/restartIdleTime	The idle time in minutes before the browser restarts. When set to the default of 0, the restart is not activated.
root/ConnectionType/firefox/coreSettings/serverRequired	Indicates whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/firefox/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process.
root/ConnectionType/firefox/coreSettings/wrapperScript	The name of 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	Preserves the user's preferences after each session.
root/ConnectionType/firefox/gui/FirefoxManager/name	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/firefox/gui/FirefoxManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/firefox/gui/FirefoxManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Controls the state for the <b>URL</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Controls the state for the <b>Auto reconnect</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart	Controls the state for the <b>Auto start priority</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to



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

Registry key	Description
	<b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog	Controls the state for the <b>Enable print dialog</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection	Controls the state for the <b>Fallback Connection</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon	Controls the state for the <b>Show icon on desktop</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/kioskMode	Controls the state for the <b>Enable kiosk mode</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/label	Controls the state for the <b>Name</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/startMode	This key has no function.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/waitForNetwork	Controls the state for the <b>Wait for network before connection</b> widget in the Web Browser Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

## root > ConnectionType > freerdp

This section describes the registry keys and functions in the **root > ConnectionType > freerdp** folder.

**Table E-5** root > ConnectionType > freerdp

Registry key	Description
root/ConnectionType/freerdp/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/freerdp/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.

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

Registry key	Description
root/ConnectionType/freerdp/connections/{UUID}/ExtraArgs	Specify extra arguments to the xfreerdp client. Run 'xfreerdp —help' from a terminal to see all available arguments.
root/ConnectionType/freerdp/connections/{UUID}/SingleSignOn	
root/ConnectionType/freerdp/connections/{UUID}/address	The IP or hostname of the remote host to connect to.
root/ConnectionType/freerdp/connections/{UUID}/application	Specifies an alternate shell to use. It can also be the name of an available application.
root/ConnectionType/freerdp/connections/{UUID}/attachToConsole	
root/ConnectionType/freerdp/connections/{UUID}/audioLatency	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	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>0</b> .
root/ConnectionType/freerdp/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/freerdp/connections/{UUID}/autoReconnect	When set to <b>1</b> , the connection will be restarted when it is closed or disconnected. This is frequently useful for kiosk style applications. When set to <b>0</b> , the connection will not restart when closed or disconnected.
root/ConnectionType/freerdp/connections/{UUID}/autoReconnectDelay	Indicates the amount of time in seconds to wait before restarting the connection. The default of <b>0</b> will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to <b>1</b> .
root/ConnectionType/freerdp/connections/{UUID}/autostart	When set to <b>1</b> , the connection will be automatically started on boot. This is useful for kiosk style applications. By default, connections are not automatically started.
root/ConnectionType/freerdp/connections/{UUID}/autostartDelay	Indicates the amount of time in seconds to wait before starting the connection on boot. The default of <b>0</b> will cause the connection to start immediately upon boot. This setting takes effect only when 'autostart' is set to <b>1</b> .
root/ConnectionType/freerdp/connections/{UUID}/certificateCheck	When set to the default of <b>1</b> , certificates are checked. When set to <b>0</b> , certificates are ignored.
root/ConnectionType/freerdp/connections/{UUID}/clipboardExtension	When set to the default of <b>0</b> , inter-session RDP clipboard functionality is disabled. When set to <b>1</b> , the clipboard is enabled between both RDP sessions and RDP sessions and the local system.
root/ConnectionType/freerdp/connections/{UUID}/compression	If set to <b>1</b> , compression of RDP data between client and server will be enabled. Setting to ' <b>0</b> ' will disable compression. Compression is enabled by default.

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

Registry key	Description
root/ConnectionType/freerdp/connections/{UUID}/dependConnectionId	
root/ConnectionType/freerdp/connections/{UUID}/directory	Specifies the startup directory where an alternate shell application is executed.
root/ConnectionType/freerdp/connections/{UUID}/disableMMRwithRFX	If not 0, disables multimedia redirection if a valid remoteFX session is established.
root/ConnectionType/freerdp/connections/{UUID}/domain	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	
root/ConnectionType/freerdp/connections/{UUID}/extraEnvValues/{UUID}/value	
root/ConnectionType/freerdp/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection_mgr list' on the client, or by navigating to root/ConnectionType/<type>/connections/.
root/ConnectionType/freerdp/connections/{UUID}/frameAcknowledgeCount	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 acknowledge will not be used in the client-server interactions.
root/ConnectionType/freerdp/connections/{UUID}/gatewayAddress	Identifies the RD Gateway server name or address.
root/ConnectionType/freerdp/connections/{UUID}/gatewayDomain	Specifies the default domain to supply to the gateway during login. Usually, this setting is used with kiosk-style applications where a generic username 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.
root/ConnectionType/freerdp/connections/{UUID}/gatewayPassword	Specifies 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 username is used to login. If gatewayUsesSameCredentials is to 1, this value is disabled.
root/ConnectionType/freerdp/connections/{UUID}/gatewayPort	Specifies the port number to use when contacting the RDP server. This key can be left empty. The most common value is <b>443</b> .
root/ConnectionType/freerdp/connections/{UUID}/gatewayUser	Specifies the default username to supply to the gateway during login. Usually, this setting is used with kiosk-style applications where a generic username is used to login. If gatewayUsesSameCredentials is to 1, this value is disabled.
root/ConnectionType/freerdp/connections/{UUID}/gatewayUsesSameCredentials	If set to 1, the device uses the same credentials to connect to the gateway as are used to connect to the final server.
root/ConnectionType/freerdp/connections/{UUID}/hasDesktopIcon	If set to 1, an icon for the connection will be shown on the desktop. Not applicable to Smart Zero.

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

Registry key	Description
root/ConnectionType/freerdp/connections/{UUID}/label	The name of the connection show in the Control Center. For Smart Zero, this will typically be set to 'Default Connection' and does not show in the user interface.
root/ConnectionType/freerdp/connections/{UUID}/localPartitionRedirection	If set to <b>0</b> , the storage extension for local non-USB storage partitions—other than those used by HP ThinPro—is disabled. If set to <b>1</b> , the local non-USB storage partitions are redirected through the storage extension in the RDP connection.
root/ConnectionType/freerdp/connections/{UUID}/mouseMotionEvents	When set to <b>0</b> , mouse motion events will not be sent to the server. This may prevent some user feedback such as tooltips from functioning properly.
root/ConnectionType/freerdp/connections/{UUID}/offScreenBitmaps	When set to <b>0</b> , off-screen bitmaps will be disabled. This might slightly increase performance but will cause blocks of the screen to be updated asynchronously, causing screen transitions to update non-uniformly.
root/ConnectionType/freerdp/connections/{UUID}/password	The default password to supply to the remote host during login. This value will be stored 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 <b>1</b> , allows desktop composition, such as translucent borders, if supported by the server. Turning it off may improve performance on low-bandwidth connections. Generally, this affects only RemoteFX.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagFontSmoothing	If set to <b>1</b> , allows font smoothing when supported by the server and enabled. Turning it off can improve performance on low-bandwidth connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoCursorSettings	If set to <b>1</b> , disables cursor blinking, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoCursorShadow	If set to <b>1</b> , turns off mouse cursor shadows, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoMenuAnimations	If set to <b>1</b> , turns off menu animations, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoTheming	If set to <b>1</b> , turns off user interface themes, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWallpaper	If set to <b>1</b> , turns off the desktop wallpaper, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWindowDrag	If set to <b>1</b> , turns off full-content window drag, which can improve performance on low-bandwidth RDP connections. The window outline will be used instead.
root/ConnectionType/freerdp/connections/{UUID}/port	The port number to use when contacting the RDP server. By default, this is set to <b>3389</b> and will rarely need to be changed.
root/ConnectionType/freerdp/connections/{UUID}/portMapping	If set to <b>1</b> , the following local serial and parallel ports will be redirected to the remote host: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/freerdp/connections/{UUID}/printerMapping	If set to <b>1</b> , the CUPS printer redirection plugin will be activated, causing all printers defined locally through CUPS to be redirected to the remote host.

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

Registry key	Description
root/ConnectionType/freerdp/connections/{UUID}/rdpEncryption	If set to <b>1</b> , standard RDP encryption will be used to encrypt all data between the client and server.
root/ConnectionType/freerdp/connections/{UUID}/remoteApp	Specifies the name of an available application to run in remoteApp, or RAIL, mode.
root/ConnectionType/freerdp/connections/{UUID}/remoteFx	Use RemoteFX, if available.
root/ConnectionType/freerdp/connections/{UUID}/seamlessWindow	If set to <b>1</b> , the window decorations are disabled. This might 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	
root/ConnectionType/freerdp/connections/{UUID}/sendHostname	The supplied text will be sent to the remote host as the client hostname. If left blank, the system hostname will be sent to the hostname.  <b>NOTE:</b> The general settings key 'root/ConnectionType/freerdp/coreSettings/sendHostname' must be set to 'hostname' for this key to be used.
root/ConnectionType/freerdp/connections/{UUID}/smartcard	If set to <b>1</b> , local smart card authentication will be allowed on the remote host. This will disable the Network Level Authentication (NLA).
root/ConnectionType/freerdp/connections/{UUID}/sound	If set to <b>0</b> , audio redirection is disabled. If set to <b>1</b> , the playback and recording devices are redirected to the RDP connection. If set to <b>2</b> , USB audio devices are redirected as specified in the USB Manager.  HP recommends setting this value to <b>1</b> so that USB audio devices are not redirected to the host. This will improve audio quality and ensure that client audio that is redirected via other methods (such as Multimedia Redirection) matches local audio settings.
root/ConnectionType/freerdp/connections/{UUID}/startMode	If set to the default <b>focus</b> 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	The number of milliseconds to wait after losing connection with the server before presenting an error dialog box and closing the connection. Disabled if <b>0</b> .
root/ConnectionType/freerdp/connections/{UUID}/timeoutRecovery	The number of milliseconds to wait after losing connection for networking to recover without trying a forced reconnection.
root/ConnectionType/freerdp/connections/{UUID}/timeoutWarning	The number of milliseconds to wait after losing connection with the server before warning the user that connection has been lost. Disabled if <b>0</b> .
root/ConnectionType/freerdp/connections/{UUID}/usbMiscRedirection	If set to <b>0</b> , the redirection is disabled for all USB devices other than those handled by sound, printerMapping, portMapping, usbStorageRedirection, and localPartitionRedirection. If set to <b>2</b> , all other USB devices are redirected in the RDP connection according to the USB Manager.
root/ConnectionType/freerdp/connections/{UUID}/usbStorageRedirection	If set to <b>0</b> , the storage extension for the USB storage devices is disabled. If set to <b>1</b> , the USB storage devices are

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

Registry key	Description
	redirected in the RDP connection according to the storage extension. If set to <b>2</b> , the USB storage devices are redirected in the RDP connection according to the USB Manager.
root/ConnectionType/freerdp/connections/{UUID}/username	The default username to supply to the remote host during login. Generally, this setting is used for kiosk style applications where a generic username is used for login.
root/ConnectionType/freerdp/connections/{UUID}/waitForNetwork	If set to <b>1</b> , the connection will not be launched until networking is available. This makes sure that on a slow network, the connection does not launch before networking is available, causing 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 if the application were part of the local environment. See the remoteApp setting. If set to Alternate Shell, allows the invocation of a non-standard shell. See the application and directory settings.
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	If not empty, provide an XKB layout ID to bypass the system keyboard. To access the list of available IDs, enter in a terminal: <code>xfreerdp --kbd-list</code> .
root/ConnectionType/freerdp/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning	If set to <b>1</b> , zero-login need not run a dialog when there is network link death, because the protocol handles such situations.
root/ConnectionType/freerdp/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/generalSettingsEditor	The internal application name to use when launching the general settings editor for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This icon is the small icon to the left of the connection name in the connection dialog.

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

Registry key	Description
root/ConnectionType/freerdp/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/freerdp/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	The number of seconds to wait for an initial response from the RDP server before giving up.
root/ConnectionType/freerdp/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/freerdp/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process.
root/ConnectionType/freerdp/coreSettings/watchPid	If set to <b>1</b> , the application specified by 'appName' will be monitored to detect the connection. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/wrapperScript	The name of 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 is the number of seconds before any error dialogs for the connection will time out. Set to <b>0</b> to pause 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 opens a dialog to update their password. When set to <b>1</b> , that button and dialog do not appear.
root/ConnectionType/freerdp/general/enableMMR	If set to <b>1</b> , the MMR plugin will be 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	Set to change the default audio backend, both in and out, for high-level audio redirection.
root/ConnectionType/freerdp/general/sendHostname	If set to the default <b>hostname</b> , the system hostname will be sent to the remote host. This is typically used by an administrator to identify the client machine associated with a particular RDP session. The hostname sent can be overridden by setting the key 'sendHostname' in the connection specific settings. If set to <b>mac</b> , the MAC address of the first available network adapter will be sent instead of the hostname.
root/ConnectionType/freerdp/general/sttyInitialSettings	Identifies the serial ports' initial settings as defined by the stty tool.

## root > ConnectionType > ssh

This section describes the registry keys and functions in the **root > ConnectionType > ssh** folder.

**Table E-6** root > ConnectionType > ssh

Registry key	Description
root/ConnectionType/ssh/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/ssh/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow access, <b>0</b> to deny access.
root/ConnectionType/ssh/connections/{UUID}/address	Specifies the IP or hostname of the remote SSH host to connect to. This setting is specified by each connection.
root/ConnectionType/ssh/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/ssh/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/ssh/connections/{UUID}/application	Specifies the application to run.
root/ConnectionType/ssh/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to ' <b>1</b> ' to allow access, <b>0</b> to deny access.  <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to ' <b>0</b> '.
root/ConnectionType/ssh/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow access, <b>0</b> to deny access.  <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/ssh/connections/{UUID}/autoReconnect	If <b>1</b> , the system will attempt to automatically restart the connection after it has been closed. <code>autoStart</code> is frequently used in conjunction with this setting.
root/ConnectionType/ssh/connections/{UUID}/autoReconnectDelay	Indicates the amount of time in seconds to wait before restarting the connection. The default of <b>0</b> will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when <code>autoReconnect</code> is set to <b>1</b> .
root/ConnectionType/ssh/connections/{UUID}/autoStart	If greater than <b>0</b> , the system will attempt to automatically start the connection when the client is booted. <code>autoReconnect</code> is frequently used in conjunction with this setting.
root/ConnectionType/ssh/connections/{UUID}/autoStartDelay	Indicates the amount of time in seconds to wait before starting the connection on boot. The default of <b>0</b> will cause the connection to start immediately upon boot. This setting takes effect only when 'autoStart' is set to <b>1</b> .
root/ConnectionType/ssh/connections/{UUID}/backgroundColor	Specifies the background color for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/beforeStartingCommand	The full path to a script or binary to run before the connection has started.



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

Registry key	Description
root/ConnectionType/ssh/connections/{UUID}/compression	Enables compression for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/connectionEndAction	This key is reserved for use.
root/ConnectionType/ssh/connections/{UUID}/coord	This key is reserved for use.
root/ConnectionType/ssh/connections/{UUID}/dependConnectionId	This key is reserved for use.
root/ConnectionType/ssh/connections/{UUID}/extraEnvValues/{UUID}/key	The extra environment variable for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/extraEnvValues/{UUID}/value	The extra environment variable value for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to <code>root/ConnectionType/&lt;Type&gt;/connections/</code> .
root/ConnectionType/ssh/connections/{UUID}/font	Specifies the font size for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/foregroundColor	Specifies the foreground color for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/fork	Enables fork into background for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/hasDesktopIcon	Enables desktop icon for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/isInMenu	This key is reserved and not working.
root/ConnectionType/ssh/connections/{UUID}/label	The name of the connection. This is used by 'root/ConnectionManager/defaultConnection' to specify which connection to launch on startup as well as within the Connection Manager.
root/ConnectionType/ssh/connections/{UUID}/port	Specifies the port number to use when contacting the SSH server. The default is <b>22</b> .
root/ConnectionType/ssh/connections/{UUID}/startMode	If set to the default <b>focus</b> and the connection is already started, the connection is given focus. Otherwise, an error returns stating that the connection is already started.
root/ConnectionType/ssh/connections/{UUID}/tty	Enables TTY allocation to be forced for an SSH connection.
root/ConnectionType/ssh/connections/{UUID}/username	Specifies the default username to supply to the remote host during login.
root/ConnectionType/ssh/connections/{UUID}/waitForNetwork	If set to <b>1</b> , the connection will not be launched until networking is available. This makes sure that, on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/ssh/connections/{UUID}/x11	Enables X11 forwarding for an SSH connection.
root/ConnectionType/ssh/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.

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

Registry key	Description
root/ConnectionType/ssh/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/ssh/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/ssh/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/ssh/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/ssh/coreSettings/serverRequired	Tells whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/ssh/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process gracefully.
root/ConnectionType/ssh/coreSettings/watchPid	If set to <b>1</b> , the application specified by 'appName' will be monitored to detect the connection. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/wrapperScript	The name of 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	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/ssh/gui/SshManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/ssh/gui/SshManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/ssh/gui/SshManager/widgets/address	Controls the state for the <b>Address</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/application	Controls the state for the <b>Run application</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

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

Registry key	Description
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Controls the state for the <b>Auto reconnect</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/autostart	Controls the state for the <b>Auto start priority</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor	Controls the state for the <b>Background color</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/compression	Controls the state for the <b>Compression</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection	Controls the state for the <b>Fallback Connection</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/font	Controls the state for the <b>Font</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/foregroundColor	Controls the state for the <b>Foreground color</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/fork	Controls the state for the <b>Fork into background</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/hasDesktopIcon	Controls the state for the <b>Show icon on desktop</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/isInMenu	This key is reserved for use.
root/ConnectionType/ssh/gui/SshManager/widgets/label	Controls the state for the <b>Name</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

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

Registry key	Description
root/ConnectionType/ssh/gui/SshManager/widgets/port	Controls the state for the <b>Port</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/tty	Controls the state for the <b>Force TTY allocation</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/username	Controls the state for the <b>User name</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/waitForNetwork	Controls the state for the <b>Wait for network before connection</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/x11	Controls the state for the <b>X11 connection forwarding</b> widget in the Secure Shell Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

## root > ConnectionType > teemtalk

This section describes the registry keys and functions in the root > ConnectionType > teemtalk folder.

**Table E-7** root > ConnectionType > teemtalk

Registry key	Description
root/ConnectionType/teemtalk/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/teemtalk/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow access, <b>0</b> to deny access.
root/ConnectionType/teemtalk/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/teemtalk/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/teemtalk/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>'1'</b> to allow access, <b>0</b> to deny access.
	<b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>'0'</b> .

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

Registry key	Description
root/ConnectionType/teemtalk/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow access, <b>0</b> to deny access.  <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/teemtalk/connections/{UUID}/autoReconnect	If <b>1</b> , the system will attempt to automatically restart the connection after it has been closed. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autoReconnect" is frequently used in conjunction with this setting.
root/ConnectionType/teemtalk/connections/{UUID}/autostart	If greater than <b>0</b> , the system will attempt to automatically start the connection when the client is booted. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autoReconnect" is frequently used in conjunction with this setting.
root/ConnectionType/teemtalk/connections/{UUID}/beforeStartingCommand	The full path to a script or binary to run before the connection has started.
root/ConnectionType/teemtalk/connections/{UUID}/connectionEndAction	This key is reserved for use.
root/ConnectionType/teemtalk/connections/{UUID}/coord	This key is reserved for use.
root/ConnectionType/teemtalk/connections/{UUID}/dependConnectionId	This key is reserved for use.
root/ConnectionType/teemtalk/connections/{UUID}/extraEnvValues/{UUID}/key	The extra environment variable for the connection.
root/ConnectionType/teemtalk/connections/{UUID}/extraEnvValues/{UUID}/value	The extra environment variable value for the connection.
root/ConnectionType/teemtalk/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to <code>root/ConnectionType/&lt;Type&gt;/connections/</code> .
root/ConnectionType/teemtalk/connections/{UUID}/hasDesktopIcon	If set to <b>1</b> , the connection will appear on the ThinPro desktop. Not applicable to Smart Zero.
root/ConnectionType/teemtalk/connections/{UUID}/isInMenu	This key is reserved for use.
root/ConnectionType/teemtalk/connections/{UUID}/label	The name of the connection. This is used by 'root/ConnectionManager/defaultConnection' to specify which connection to launch on startup as well as within the Connection Manager.
root/ConnectionType/teemtalk/connections/{UUID}/startMode	If set to the default <b>focus</b> and the connection is already started, the connection is given focus. Otherwise, an error returns stating that the connection is already started.
root/ConnectionType/teemtalk/connections/{UUID}/systembeep	Enables system beep for the connection.
root/ConnectionType/teemtalk/connections/{UUID}/ttsName	Indicates the TeemTalk profile name.
root/ConnectionType/teemtalk/connections/{UUID}/waitForNetwork	If set to <b>1</b> , the connection will not be launched until networking is available. This makes sure that, on a slow

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

Registry key	Description
	network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/teemtalk/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/generalSettingsEditor	The internal application name to use when launching the general settings editor for this connection type. This key should not need to be modified.
root/ConnectionType/teemtalk/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/teemtalk/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/teemtalk/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/teemtalk/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/teemtalk/coreSettings/serverRequired	Tells whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/teemtalk/coreSettings/stopProcess	The behavior that should occur when 'connection_mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process gracefully.
root/ConnectionType/teemtalk/coreSettings/wrapperScript	The name of 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/teemtalk/gui/TeemtalkManager/name	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/teemtalk/gui/TeemtalkManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/teemtalk/gui/TeemtalkManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autoReconnect	Controls the state for the <b>Auto reconnect</b> widget in the TeemTalk Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

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

Registry key	Description
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autostart	Controls the state for the <b>Auto start priority</b> widget in the TeemTalk Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/hasDesktopIcon	Controls the state for the <b>Show icon on desktop</b> widget in the TeemTalk Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/isInMenu	This key is reserved for use.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/label	Controls the state for the <b>Name</b> widget in the TeemTalk Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/waitForNetwork	Controls the state for the <b>Wait for network before connection</b> widget in the TeemTalk Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

## root > ConnectionType > telnet

This section describes the registry keys and functions in the **root > ConnectionType > telnet** folder.

**Table E-8** root > ConnectionType > telnet

Registry key	Description
root/ConnectionType/telnet/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/telnet/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow access, <b>0</b> to deny access.
root/ConnectionType/telnet/connections/{UUID}/address	The address of the remote host to connect to.
root/ConnectionType/telnet/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/telnet/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/telnet/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>'1'</b> to allow access, <b>0</b> to deny access.  <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>'0'</b> .
root/ConnectionType/telnet/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow access, <b>0</b> to deny access.

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

Registry key	Description
	<b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/telnet/connections/{UUID}/autoReconnect	If <b>1</b> , the system will attempt to automatically restart the connection after it has been closed. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autostart" is frequently used in conjunction with this setting.
root/ConnectionType/telnet/connections/{UUID}/autostart	If greater than <b>0</b> , the system will attempt to automatically start the connection when the client is booted. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autoReconnect" is frequently used in conjunction with this setting.
root/ConnectionType/telnet/connections/{UUID}/backgroundColor	Specifies the background color of the connection.
root/ConnectionType/telnet/connections/{UUID}/beforeStartingCommand	The full path to a script or binary to run before the connection has started.
root/ConnectionType/telnet/connections/{UUID}/connectionEndAction	This key is reserved for use.
root/ConnectionType/telnet/connections/{UUID}/coord	This key is reserved for use.
root/ConnectionType/telnet/connections/{UUID}/dependConnectionId	This key is reserved for use.
root/ConnectionType/telnet/connections/{UUID}/extraEnvValues/{UUID}/key	The extra environment variable for the connection.
root/ConnectionType/telnet/connections/{UUID}/extraEnvValues/{UUID}/value	The extra environment variable value for the connection.
root/ConnectionType/telnet/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to <code>root/ConnectionType/&lt;Type&gt;/connections/</code> .
root/ConnectionType/telnet/connections/{UUID}/font	Specifies the font size for the connection.
root/ConnectionType/telnet/connections/{UUID}/foregroundColor	Specifies the foreground color of the connection.
root/ConnectionType/telnet/connections/{UUID}/hasDesktopIcon	Enables the desktop icon for the connection.
root/ConnectionType/telnet/connections/{UUID}/label	The name of the connection. This is used by 'root/ConnectionManager/defaultConnection' to specify which connection to launch on startup as well as within the Connection Manager.
root/ConnectionType/telnet/connections/{UUID}/locale	Specifies the locale of the connection.
root/ConnectionType/telnet/connections/{UUID}/port	Specifies the server's port for the connection. The default is <b>23</b> .
root/ConnectionType/telnet/connections/{UUID}/startMode	If set to the default <b>focus</b> and the connection is already started, the connection is given focus. Otherwise, an error returns stating that the connection is already started.



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

Registry key	Description
root/ConnectionType/telnet/connections/{UUID}/waitForNetwork	If set to <b>1</b> , the connection will not be launched until networking is available. This makes sure that, on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/telnet/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	The internal application name to use when launching the general settings editor for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/telnet/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/telnet/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/telnet/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/telnet/coreSettings/serverRequired	Tells whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/telnet/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process gracefully.
root/ConnectionType/telnet/coreSettings/wrapperScript	The name of 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	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/telnet/gui/TelnetManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/telnet/gui/TelnetManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/telnet/gui/TelnetManager/widgets/address	Controls the state for the <b>Address</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the

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

Registry key	Description
	widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/autoReconnect	Controls the state for the <b>Auto reconnect</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart	Controls the state for the <b>Auto start priority</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor	Controls the state for the <b>Background color</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection	Controls the state for the <b>Fallback Connection</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor	Controls the state for the <b>Foreground color</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon	Controls the state for the <b>Show icon on desktop</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/label	Controls the state for the <b>Name</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/port	Controls the state for the <b>Port</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork	Controls the state for the <b>Wait for network before connection</b> widget in the Telnet Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.

## root > ConnectionType > view

This section describes the registry keys and functions in the **root > ConnectionType > view** folder.

**Table E-9** root > ConnectionType > view

Registry key	Description
root/ConnectionType/view/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/view/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow access, <b>0</b> to deny access.
root/ConnectionType/view/connections/{UUID}/ExtraArgs	Specifies extra arguments to the VMware Horizon View client. Run <code>view_client --help</code> or <code>vmware-view --help</code> from a terminal to see all available arguments.
root/ConnectionType/view/connections/{UUID}/SingleSignOn	
root/ConnectionType/view/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/view/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/view/connections/{UUID}/appInMenu	
root/ConnectionType/view/connections/{UUID}/appOnDesktop	
root/ConnectionType/view/connections/{UUID}/attachToConsole	
root/ConnectionType/view/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>'1'</b> to allow access, <b>0</b> to deny access.  <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>'0'</b> .
root/ConnectionType/view/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow access, <b>0</b> to deny access.  <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/view/connections/{UUID}/autoReconnect	If <b>1</b> , the system will attempt to automatically restart the connection after it has been closed. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autostart" is frequently used in conjunction with this setting.
root/ConnectionType/view/connections/{UUID}/autoReconnectDelay	Indicates the amount of time in seconds to wait before restarting the connection. The default of <b>0</b> will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to <b>1</b> .
root/ConnectionType/view/connections/{UUID}/automaticLogin	When enabled, the VMware Horizon View client attempts to automatically login if all fields are provided. If this is not enabled, users must click <b>Connect</b> in the VMware Horizon View client to contact the VMware Horizon View Connection Server, login, and select a desktop.
root/ConnectionType/view/connections/{UUID}/autostart	If greater than <b>0</b> , the system will attempt to automatically start the connection when the client is booted. If required, credentials should be supplied through the <code>zero-login/</code>

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

Registry key	Description
	defaultCredentials field. "autoReconnect" is frequently used in conjunction with this setting.
root/ConnectionType/view/connections/{UUID}/autostartDelay	Indicates the amount of time in seconds to wait before starting the connection on boot. The default of 0 will cause the connection to start immediately upon boot. This setting takes effect only when 'autostart' is set to 1.
root/ConnectionType/view/connections/{UUID}/beforeStartingCommand	The full path to a script or binary to run before the connection has started.
root/ConnectionType/view/connections/{UUID}/closeAfterDisconnect	If set to 1, the connection will be closed after the first desktop is disconnected. If this is not enabled, the VMware Horizon View client will return 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	
root/ConnectionType/view/connections/{UUID}/dependConnectionId	
root/ConnectionType/view/connections/{UUID}/desktop	If specified, the named desktop will automatically launch upon login.  <b>NOTE:</b> By default, if there is only one desktop available, it will automatically launch without needing to be specified.
root/ConnectionType/view/connections/{UUID}/directory	
root/ConnectionType/view/connections/{UUID}/domain	The domain to provide to the VMware Horizon View server. If no domain is specified, the default domain will be used.
root/ConnectionType/view/connections/{UUID}/enableSingleMode	
root/ConnectionType/view/connections/{UUID}/extraEnvValues/{UUID}/key	
root/ConnectionType/view/connections/{UUID}/extraEnvValues/{UUID}/value	
root/ConnectionType/view/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to root/ConnectionType/<Type>/connections/.
root/ConnectionType/view/connections/{UUID}/fullscreen	When set to 1, the VMware Horizon View client will be started in full-screen mode.
root/ConnectionType/view/connections/{UUID}/hasDesktopIcon	If set to 1, the connection will appear on the ThinPro desktop. Not applicable to Smart Zero.
root/ConnectionType/view/connections/{UUID}/hideMenuBar	If set to 1, the top menu bar within the desktop will be hidden. This bar is used to manage remote devices and start other desktops. By default, it is shown for ThinPro and hidden for Smart Zero.
root/ConnectionType/view/connections/{UUID}/isInMenu	If set to 1, the connection will appear in the ThinPro taskbar. Not applicable to Smart Zero.

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

Registry key	Description
root/ConnectionType/view/connections/{UUID}/label	The name of the connection. This is used by 'root/ConnectionManager/defaultConnection' to specify which connection to launch on startup as well as within the Connection Manager.
root/ConnectionType/view/connections/{UUID}/password	The default password to supply to the remote host during login. This value will be stored 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	The address of the remote host to connect to. This is typically a URL such as 'https://server.domain.com'.
root/ConnectionType/view/connections/{UUID}/sessionEndAction	
root/ConnectionType/view/connections/{UUID}/singleDesktop	
root/ConnectionType/view/connections/{UUID}/smartcard	Enabling this will forward any locally attached smart cards to the remote host, allowing them to be used by applications on the remote host. This does not enable smart card login for the VMware Horizon View server login, only for the remote host.
root/ConnectionType/view/connections/{UUID}/startMode	If set to the default <b>focus</b> and the connection is already started, it will be given focus. Otherwise, an error will be returned stating the connection is already started.
root/ConnectionType/view/connections/{UUID}/username	The default username to supply to the remote host during login. Generally, this setting is used for kiosk style applications where a generic username is used for login.
root/ConnectionType/view/connections/{UUID}/viewSecurityLevel	If set to the default <b>Refuse insecure connections</b> , the VMware Horizon View client will not allow the user to connect to the server if the server's SSL certificate is invalid. If set to <b>Warn</b> , the VMware Horizon View client will warn if the server's certificate cannot be verified, and if it is self-signed or expired, the user still will not be allowed to connect. If set to <b>Allow all connections</b> , the server certificate will not be verified and connections to any server will be allowed.
root/ConnectionType/view/connections/{UUID}/waitForNetwork	If set to <b>1</b> , the connection will not be launched until networking is available. This makes sure that, on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/attachToConsole	
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/audioLatency	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. This is frequently used to reduce network bandwidth.

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

Registry key	Description
	<b>NOTE:</b> Reducing color depth to a level not supported by the video driver may cause screen corruption or launch failures.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/compression	If set to <b>1</b> , compression of RDP data between client and server will be enabled. Setting to ' <b>0</b> ' will disable compression. Compression is enabled by default.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/disableMMRwithRFX	If not <b>0</b> , disables multimedia redirection if a valid remoteFX session is established.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/frameAcknowledgeCount	This is 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 <b>0</b> , frame acknowledge will not be used in the client-server interactions.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/general/enableMMR	If set to <b>1</b> , enables the multimedia redirection plugin, causing supported codecs played through Windows Media Player to be redirected to the client. This improves 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 the default of <b>hostname</b> , sends the system hostname to the remote host. This is typically used by an administrator to identify the client machine associated with a particular RDP session. The hostname sent can be overridden by setting the key 'sendHostname' in the connection specific settings. If set to <b>mac</b> , sends the MAC address of the first available network adapter instead of the hostname.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/mouseMotionEvents	When set to <b>0</b> , mouse motion events will not be sent to the server. This may prevent some user feedback such as tooltips from functioning properly.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/offScreenBitmaps	When set to <b>0</b> , off-screen bitmaps will be disabled. This might slightly increase performance but will cause blocks of the screen to be updated asynchronously, causing screen transitions to update non-uniformly.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagDesktopComposition	If set to <b>1</b> , allows desktop composition, such as translucent borders, if supported by the server. Turning it off may improve performance on low-bandwidth connections. Generally, this affects only RemoteFX.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagFontSmoothing	If set to <b>1</b> , allows font smoothing when supported by the server and enabled. Turning it off can improve performance on low-bandwidth connections.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoCursorSettings	If set to <b>1</b> , disables cursor blinking, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoCursorShadow	If set to <b>1</b> , turns off mouse cursor shadows, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoMenuAnimations	If set to <b>1</b> , turns off menu animations, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoTheming	If set to <b>1</b> , turns off user interface themes, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoWallpaper	If set to <b>1</b> , turns off the desktop wallpaper, which can improve performance on low-bandwidth RDP connections.

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

Registry key	Description
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoWindowDrag	If set to <b>1</b> , turns off full-content window drag, which can improve performance on low-bandwidth RDP connections. The window outline will be used instead.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/portMapping	If set to <b>1</b> , the following local serial and parallel ports will be redirected to the remote host: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/printerMapping	If set to <b>1</b> , the CUPS printer redirection plugin will be activated, causing all printers defined locally through CUPS to be redirected to the remote host.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/rdpEncryption	If set to <b>1</b> , standard RDP encryption will be used to encrypt all data between the client and server.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/remoteFx	Use RemoteFX, if available.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/sendHostname	The supplied text will be sent to the remote host as the client hostname. If left blank, the system hostname will be sent to the hostname.  <b>NOTE:</b> The general settings key 'root/ConnectionType/freerdp/coreSettings/sendHostname' must be set to 'hostname' for this key to be used.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/sound	When set to the default <b>Bring to this computer</b> , sound will be redirected from the remote host to the client using a standard virtual channel. When set to <b>Leave at remote computer</b> , sound will be left at the remote host. This might be useful when using a USB-redirected audio device. If set to any other value, audio will be disabled.  HP recommends that sound be set to <b>Bring to this computer</b> because this will improve audio quality and ensure that any client audio redirected through other virtual channels such as MMR matches local audio settings.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/timeoutError	The number of milliseconds to wait after losing connection with the server before presenting an error dialog box and closing the connection. Disabled if <b>0</b> .
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/timeoutWarning	The number of milliseconds to wait after losing connection with the server before warning the user that connection has been lost. Disabled if <b>0</b> .
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/xkbLayoutId	If not empty, provide an XKB layout ID to bypass the system keyboard. To access the list of available IDs, enter in a terminal: <code>xfreerdp --kbd-list</code> .
root/ConnectionType/view/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/view/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/view/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.

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

Registry key	Description
root/ConnectionType/view/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/view/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/view/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/view/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/view/coreSettings/serverRequired	Tells whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/view/coreSettings/stopProcess	The behavior that should occur when 'connection_mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process gracefully.
root/ConnectionType/view/coreSettings/watchPid	If set to <b>1</b> , the application specified by 'appName' will be monitored to detect the connection. This key should not need to be modified.
root/ConnectionType/view/coreSettings/wrapperScript	The name of 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 'rdesktop --help' in the client terminal.
root/ConnectionType/view/gui/viewManager/name	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/view/gui/viewManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/view/gui/viewManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/view/gui/viewManager/widgets/autostart	
root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection	
root/ConnectionType/view/gui/viewManager/widgets/label	

## root > ConnectionType > xdmcp

This section describes the registry keys and functions in the root > ConnectionType > xdmcp folder.



**Table E-10** root > ConnectionType > xdmcp

Registry key	Description
root/ConnectionType/xdmcp/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/xdmcp/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/xdmcp/connections/{UUID}/address	The address of the remote host to connect to.
root/ConnectionType/xdmcp/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/xdmcp/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/xdmcp/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>0</b> .
root/ConnectionType/xdmcp/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/xdmcp/connections/{UUID}/autoReconnect	If set to <b>1</b> , the system will attempt to automatically restart the connection after it has been closed. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autostart" is frequently used in conjunction with this setting.
root/ConnectionType/xdmcp/connections/{UUID}/autostart	If greater than <b>0</b> , the system will attempt to automatically start the connection when the client is booted. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autoReconnect" is frequently used in conjunction with this setting.
root/ConnectionType/xdmcp/connections/{UUID}/beforeStartingCommand	The full path to a script or binary to run before the connection has started.
root/ConnectionType/xdmcp/connections/{UUID}/color	The color depth for the GUI or display of the connection.
root/ConnectionType/xdmcp/connections/{UUID}/connectionEndAction	This key does not have a function.
root/ConnectionType/xdmcp/connections/{UUID}/coord	The connection's window position.
root/ConnectionType/xdmcp/connections/{UUID}/dependConnectionId	This key does not have a function.
root/ConnectionType/xdmcp/connections/{UUID}/extraEnvValues/{UUID}/key	The key for the extraEnv value of the connection.
root/ConnectionType/xdmcp/connections/{UUID}/extraEnvValues/{UUID}/value	The value corresponding to the key for the extraEnv of the connection.
root/ConnectionType/xdmcp/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the

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

Registry key	Description
	desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to root/ConnectionType/<type>/connections/.
root/ConnectionType/xdmcp/connections/{UUID}/fontServer	When userFontServer is 1, the registry is used to specify that font server address.
root/ConnectionType/xdmcp/connections/{UUID}/hasDesktopIcon	If set to 1, an icon for the connection is shown on the desktop.
root/ConnectionType/xdmcp/connections/{UUID}/isInMenu	If set to 1, there is a menu item for the connection. This key does not function yet.
root/ConnectionType/xdmcp/connections/{UUID}/label	The name of the connection. This is used by root/ConnectionManager/defaultConnection to specify which connection to launch on startup, as well as within the Connection Manager.
root/ConnectionType/xdmcp/connections/{UUID}/refreshRate	The refresh rate of the display for the connection.
root/ConnectionType/xdmcp/connections/{UUID}/startMode	If set to the default <b>focus</b> and the connection is already started, it will be given focus. Otherwise, an error will be returned stating the connection is already started.
root/ConnectionType/xdmcp/connections/{UUID}/type	Specifies the XDMCP connection type. If set to <b>chooser</b> , all available hosts are listed and the user can select which one to connect to. If set to <b>query</b> , an XDMCP request is sent to the specified host directly. If set to <b>broadcast</b> , 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 makes sure that on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/xdmcp/connections/{UUID}/windowSize	The client window size for the connection.
root/ConnectionType/xdmcp/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/audio	The audio setting for the connection type. There is no audio support for XDMCP.
root/ConnectionType/xdmcp/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/desktopButton	A customized desktop button for XDMCP. This key is not supported.
root/ConnectionType/xdmcp/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor	The internal application name to use when launching the general settings editor for this connection type. This key should not need to be modified.

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

Registry key	Description
root/ConnectionType/xdmcp/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This icon is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/xdmcp/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/xdmcp/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This icon is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/xdmcp/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/xdmcp/coreSettings/serverRequired	Tells whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/xdmcp/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process.
root/ConnectionType/xdmcp/coreSettings/watchPid	If set to <b>1</b> , the application specified by 'appName' will be monitored to detect the connection. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/wrapperScript	The name of 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	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/xdmcp/gui/XdmcpManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/xdmcp/gui/XdmcpManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/address	Controls the state for the <b>Address</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect	Controls the state for the <b>Auto reconnect</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autostart	Controls the state for the <b>Auto start priority</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/color	This key has no function.

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

Registry key	Description
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/fontServer	Controls the state for the <b>Font server</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/hasDesktopIcon	Controls the state for the <b>Show icon on desktop</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/isInMenu	This key has no function.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/label	Controls the state for the <b>Name</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/refreshRate	This key has no function.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/type	This key has no function.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/useFontServer	Controls the state for the <b>Use font server</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/waitForNetwork	Controls the state for the <b>Wait for network before connection</b> widget in the XDMCP Connection Manager. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/windowSize	This key has no function.

## root > ConnectionType > xen

This section describes the registry keys and functions in the **root > ConnectionType > xen** folder.

**Table E-11** root > ConnectionType > xen

Registry key	Description
root/ConnectionType/xen/authorizations/user/add	Indicates whether the user has permission to add a new connection of this type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/xen/authorizations/user/general	Indicates whether the user has permission to modify the general settings for this connection type using the Control Center. Not applicable to Smart Zero. Set to <b>1</b> to allow, <b>0</b> to deny access.
root/ConnectionType/xen/connections/{UUID}/SingleSignOn	

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

Registry key	Description
root/ConnectionType/xen/connections/{UUID}/address	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	The full path to a script or binary to run after the connection has been started.
root/ConnectionType/xen/connections/{UUID}/afterStoppedCommand	The full path to a script or binary to run after the connection has finished.
root/ConnectionType/xen/connections/{UUID}/applnMenu	If set to <b>1</b> , all applications for this connection will be displayed in the dashboard menu.
root/ConnectionType/xen/connections/{UUID}/appOnDesktop	If set to <b>1</b> , all applications for this connection will be displayed on the desktop.
root/ConnectionType/xen/connections/{UUID}/authorizations/user/edit	Indicates whether the user has permission to modify the connection settings for this connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection can be edited in Administrator Mode even when this key is set to <b>0</b> .
root/ConnectionType/xen/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to <b>1</b> to allow, <b>0</b> to deny access.  <b>NOTE:</b> The connection will always be available to launch in Administrator Mode.
root/ConnectionType/xen/connections/{UUID}/autoLaunchSingleApp	If set to <b>1</b> and there is only a single application or desktop returned by the Citrix server, automatically launches that resource.
root/ConnectionType/xen/connections/{UUID}/autoReconnect	If set to <b>1</b> , the system will attempt to automatically restart the connection after it has been closed. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autostart" is frequently used in conjunction with this setting.
root/ConnectionType/xen/connections/{UUID}/autoReconnectAppsOnLogin	If set to <b>1</b> , the system attempts to reconnect any active or disconnected Citrix sessions upon an initial login.
root/ConnectionType/xen/connections/{UUID}/autoReconnectDelay	Indicates the amount of time in seconds to wait before restarting the connection. The default of <b>0</b> will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to <b>1</b> .
root/ConnectionType/xen/connections/{UUID}/autoStartDesktop	To automatically start the first desktop available when you launch a Citrix connection, set the key value to <b>1</b> .
root/ConnectionType/xen/connections/{UUID}/autoStartResource	To automatically start a desktop or an application when you launch a Citrix connection, set the value of following key to the name of the desktop or application you want to start.
root/ConnectionType/xen/connections/{UUID}/autostart	If greater than <b>0</b> , the system will attempt to automatically start the connection when the client is booted. If required, credentials should be supplied through the <code>zero-login/defaultCredentials</code> field. "autoReconnect" is frequently used in conjunction with this setting.
root/ConnectionType/xen/connections/{UUID}/autostartDelay	Indicates the amount of time in seconds to wait before starting the connection on boot. The default of <b>0</b> will cause

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

Registry key	Description
	the connection to start immediately upon boot. This setting takes effect only when 'autostart' is set to 1.
root/ConnectionType/xen/connections/{UUID}/beforeStartingCommand	The full path to a script or binary to run before the connection has started.
root/ConnectionType/xen/connections/{UUID}/connectionEndAction	
root/ConnectionType/xen/connections/{UUID}/coord	
root/ConnectionType/xen/connections/{UUID}/dependConnectionId	
root/ConnectionType/xen/connections/{UUID}/disableSaveCredentials	
root/ConnectionType/xen/connections/{UUID}/domain	The domain to provide to the XenDesktop Server. If no domain is specified, the default domain for the server will be used.
root/ConnectionType/xen/connections/{UUID}/enablePNADesktopIcons	
root/ConnectionType/xen/connections/{UUID}/enablePNAStartMenuItems	
root/ConnectionType/xen/connections/{UUID}/extraEnvValues/{UUID}/key	
root/ConnectionType/xen/connections/{UUID}/extraEnvValues/{UUID}/value	
root/ConnectionType/xen/connections/{UUID}/fallBackConnection	When set to the UUID of another available connection, that connection will be autostarted if the current connection fails or experiences an error and fails to start. The UUID of the desired fallback connection is typically found by running 'connection-mgr list' on the client, or by navigating to <code>root/ConnectionType/&lt;type&gt;/connections/.</code>
root/ConnectionType/xen/connections/{UUID}/folder	
root/ConnectionType/xen/connections/{UUID}/fullscreen	When set to <b>1</b> , the ICA client will be started in full-screen mode.
root/ConnectionType/xen/connections/{UUID}/hasDesktopIcon	If set to <b>1</b> , an icon for the connection will be shown on the desktop. Not applicable to Smart Zero.
root/ConnectionType/xen/connections/{UUID}/isInMenu	
root/ConnectionType/xen/connections/{UUID}/label	The name of the connection. This is used by <code>root/ConnectionManager/defaultConnection</code> to specify which connection to launch on startup, as well as within the Connection Manager.
root/ConnectionType/xen/connections/{UUID}/logOnMethod	
root/ConnectionType/xen/connections/{UUID}/password	If set, this password will be supplied as the default to the login dialog if the user and domain match their defaults here. Typically used with autostart connections.
root/ConnectionType/xen/connections/{UUID}/requireCredentialsDirectConnect	Set to <b>0</b> to prevent a prompt for user credentials when using a direct connection. By default, user is prompted for access credentials by the server when launching an application.

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

Registry key	Description
root/ConnectionType/xen/connections/{UUID}/savePassword	
root/ConnectionType/xen/connections/{UUID}/smoothRoamWhenAutostartResource	If set to <b>1</b> , the resource is autostarted when smooth roam is successful. Set to <b>0</b> to disable.
root/ConnectionType/xen/connections/{UUID}/startMode	If set to the default <b>focus</b> and the connection is already started, it will be given focus. Otherwise, an error will be returned stating the connection is already started.
root/ConnectionType/xen/connections/{UUID}/storeFrontConn	
root/ConnectionType/xen/connections/{UUID}/useCredentials	
root/ConnectionType/xen/connections/{UUID}/username	The default username to supply to the remote host during login. Generally, this setting is used for kiosk style applications where a generic username is used for login.
root/ConnectionType/xen/connections/{UUID}/waitForNetwork	If set to <b>1</b> , the connection will not be launched until networking is available. This makes sure that on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/xen/coreSettings/appName	The internal application name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch	This setting applies to Citrix servers with multiple published apps or desktops. If <b>less than 0</b> , no auto-logout is performed. Otherwise, it is the number of seconds between the closing of the last Xen application and the time the Xen desktop will be automatically closed. Citrix process delays can extend the auto-logout time.
root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch	This setting applies to Citrix servers with multiple published apps or desktops. If <b>less than 0</b> , no auto-logout is performed. Otherwise, it is the number of seconds between the closing of the last Xen application and the time the Xen desktop will be automatically closed. Citrix process delays can extend the auto-logout time.
root/ConnectionType/xen/coreSettings/autoLogoutDelaySingleApp	This setting applies to Citrix servers with a single published app or desktop. If <b>less than 0</b> , no auto-logout is performed. Otherwise, it is the number of seconds between the closing of the last Xen application and the time the Xen desktop will be automatically closed. Citrix process delays can extend the auto-logout time.
root/ConnectionType/xen/coreSettings/className	The internal X Windows application class name to use when tracking the PID of the connection for connection status monitoring. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/editor	The internal application name to use when launching the connection editor for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/generalSettingsEditor	The internal application name to use when launching the general settings editor for this connection type. This key should not need to be modified.

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

Registry key	Description
root/ConnectionType/xen/coreSettings/icon16Path	The internal application icon path for the 16x16 pixel icon for this application. This icon is the small icon to the left of the connection name in the connection dialog.
root/ConnectionType/xen/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/ConnectionType/xen/coreSettings/icon48Path	The internal application icon path for the 48x48 pixel icon for this application. This icon is the large icon in the top left of the connection editor for this connection type.
root/ConnectionType/xen/coreSettings/label	The name to display for this connection type in the connection type selection menu.
root/ConnectionType/xen/coreSettings/serverRequired	Tells whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/xen/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is <b>close</b> , which will send a standard kill signal to the process. When set to <b>kill</b> , the process specified by 'appName' will be forcefully killed. When set to <b>custom</b> , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process.
root/ConnectionType/xen/coreSettings/watchPid	If set to <b>1</b> , the application specified by 'appName' will be monitored to detect the connection. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/wrapperScript	The name of 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	Directly maps to the Citrix INI file setting <code>TWIMode=boolean</code> , which controls seamless mode for published applications. The default is <b>1</b> .
root/ConnectionType/xen/general/TWIModeResizeType	The default is <b>1</b> .
root/ConnectionType/xen/general/allowReadOn{AthruZ}	Set to <b>1</b> to allow the user to read the mapped drive from the remote host. If this is set to <b>0</b> , no files will show up in the mapped drive on the remote host.
root/ConnectionType/xen/general/allowWriteOn{AthruZ}	Set to <b>1</b> to allow the user to write to the mapped drive from the remote host. If this is set to <b>0</b> , the user will be able to read and copy files off of the drive, but will not be able to make any changes or add new files to the drive.
root/ConnectionType/xen/general/async	Directly maps to the Citrix INI file setting <code>CommPollSize=boolean</code> , which enables asynchronous polling. The default is <b>0</b> for 'Off'.
root/ConnectionType/xen/general/autoReconnect	Directly maps to the Citrix INI file setting <code>TransportReconnectEnabled=boolean</code> , which enables automatic session reconnect. The default is <b>0</b> .  <b>NOTE:</b> This is not the same as the connection-specific 'autoReconnect'. This reconnect occurs internally within the Citrix client without restarting the connection.
root/ConnectionType/xen/general/bitmapCacheSize	Directly maps to the Citrix INI file setting <code>PersistentCacheMinBitmap=integer</code> , which is the



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

Registry key	Description
	minimum size of bitmap for caching. The default is <b>8192</b> . On all clients, this is set to a default of <b>2048</b> .
root/ConnectionType/xen/general/colorDepth	Forces ICA to use a specific color depth for all connections. This is usually done in either specialized environments where the automatic depth selection fails or in very slow networks to reduce congestion.
root/ConnectionType/xen/general/colorMapping	Set to <b>Shared - Approximate Colors</b> to enable and <b>Private - Exact Colors</b> to disable. Enabled by default. Maps to the Citrix INI file setting <code>ApproximateColors=boolean</code> , which uses approximate colors from the default colormap rather than a private colormap and precise colors. Used only when the <code>DesiredColor</code> value is 2 (256 colors). The default is <b>False</b> .
root/ConnectionType/xen/general/defaultBrowserProtocol	Set to <b>TCP/IP HTTP Browser</b> by default. Can be set to <b>SSL/TLS HTTPS Browser</b> or <b>TCP/IP Browser</b> . Maps to the Citrix INI file setting <code>BrowserProtocol=[UDP HTTP TCP]</code> , which controls the protocol used to locate the ICA host for the connection. If not specified, the default value from the [WFClient] section of <code>wfclient.ini</code> is used.
root/ConnectionType/xen/general/drivePathMappedOn{ <b>AthruZ</b> }	The local filesystem directory to map to the remote host. Typically, this is set to <b>/media</b> to allow all connected USB drives to be mapped to the remote host through a single drive letter.
root/ConnectionType/xen/general/enableAlertSound	Set to the default <b>1</b> to enable Windows alert sounds. Set to <b>0</b> to disable. Indirectly maps to the Citrix INI file setting <code>DisableSound=boolean</code> , which disables Windows alert sounds. The default is <b>False</b> .
root/ConnectionType/xen/general/enableAudioInput	Set to the default <b>1</b> to enable audio input. This will set both the 'AllowAudioInput' and 'EnableAudioInput' settings to <b>1</b> in the <code>wfclient.ini</code> and <code>appsrv.ini</code> .
root/ConnectionType/xen/general/enableCursorColors	Set to <b>0</b> to disable the use of the X11 Render extension required for color cursors. This might fix graphical cursor corruption in some cases.
root/ConnectionType/xen/general/enableDataCompression	Set to the default <b>1</b> to enable data compression, or set to <b>0</b> to disable. Directly maps to the Citrix INI file setting <code>Compress=boolean</code> , which controls data compression.
root/ConnectionType/xen/general/enableDriveMapping	Allows directories on the local filesystem to be forwarded to the remote host through a virtual drive. Typically, <b>/media</b> would be mapped to <b>Z</b> to allow USB drives to be forwarded to the remote host. If USB redirection is enabled, this should be disabled to prevent storage conflicts. To be properly mapped to the remote host in this fashion, the USB device must use one of the following filesystems: FAT32, NTFS, ext2, or ext3.
root/ConnectionType/xen/general/enableDynamicDriveMapping	When enabled, USB storage devices are dynamically mapped on the Citrix server and static drive mappings are not required.
root/ConnectionType/xen/general/enableForceDirectConnect	Set to <b>1</b> to force the connection to bypass the Citrix Web Interface and PNAgent services. Authentication will occur on the server after the initial connection has been made.

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

Registry key	Description
root/ConnectionType/xen/general/enableH264Compression	Set to <b>0</b> to disable deep compression codec support and text tracking. When H264Compression is enabled, it provides better performance of rich and professional graphics applications on WAN networks as compared to the JPEG codec.
root/ConnectionType/xen/general/enableHDXFlashRedirection	Control the behavior of HDX Flash Redirection by setting it to <b>Always</b> , <b>Ask</b> , or <b>Never</b> . The default is "Always", which is to use HDX Flash Redirection if possible and not prompt the user. "Ask" will dynamically prompt the user within the session. "Never" will disable the feature.
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	Control the behavior of HDX Flash Server Side Content Fetching by setting it to <b>Enabled</b> or <b>Disabled</b> . The default is <b>Disabled</b> , where the client fetches for content.
root/ConnectionType/xen/general/enableHDXMediaStream	Set to <b>0</b> to disable HDX MediaStream. When HDX MediaStream is disabled, media files will still play through standard streaming, but the quality might not be as high.
root/ConnectionType/xen/general/enableMapOn{A thru Z}	Allows drive mapping to occur using the specified drive on the remote host. Must be set to a valid local directory for drive mapping to work properly. Other drive letters are also available when all keys are shown.
root/ConnectionType/xen/general/enableOffScreenSurface	Directly maps to the Citrix INI file setting <code>EnableOSS=boolean</code> , which enables the server to create and use X pixmaps for off-screen drawing. Reduces bandwidth in 15- and 24-bit color at the expense of X server memory and processor time. The default is <b>On</b> .
root/ConnectionType/xen/general/enableSmartCard	If set to <b>1</b> , 'DisableCtrlAltDel' will be set to 'Off' and smart card login will be enabled. If set to <b>0</b> , 'SmartCardAllowed' will be set to 'Off', disabling smart card login.
root/ConnectionType/xen/general/enableWindowsAlertSounds	
root/ConnectionType/xen/general/encryptionLevel	Directly maps to the Citrix INI file setting <code>EncryptionLevelSession=[None   Basic   RC5 (128 bit - Login Only)   RC5 (40 bit)   RC5 (56 bit)   RC5 (128 bit)]</code> , which specifies the level of encryption on a per-connection basis. Encryption protocols for all levels are defined in the [EncryptionLevelSession] section of module.ini.
root/ConnectionType/xen/general/fontSmoothingType	Specifies font smoothing type for the session.
root/ConnectionType/xen/general/hotKey{1 thru 15}Char	The hotkey character to forward to the remote session. For example, F1 for hotKey1Char.
root/ConnectionType/xen/general/hotKey{1 thru 15}Shift	The key shift state combination used to activate the chosen hotkey character. Defaults to <b>Ctrl+Shift</b> . Can be set to <b>Shift</b> , <b>Ctrl</b> , <b>Alt</b> , <b>Alt+Shift</b> , <b>Alt+Ctrl</b> , or <b>Ctrl+Shift</b> .
root/ConnectionType/xen/general/httpAddresses/{UUID}/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Directly maps to the Citrix INI file setting <code>KeyPassthroughEscapeChar=string</code> , which is the key for the keyboard command to disable the transparent keyboard mode. The default is <b>F2</b> . All clients are set to <b>F1</b> by default.

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

Registry key	Description
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Directly maps to the Citrix INI file setting <code>KeyPassthroughEscapeShift=string</code> , which is the key for the keyboard command to disable the transparent keyboard mode. The default is <b>Ctrl</b> . All clients are set to <b>Alt</b> by default.
root/ConnectionType/xen/general/lastComPortNum	The number of mapped serial ports. Set to <b>0</b> to disable serial ports mapping.
root/ConnectionType/xen/general/localTextEcho	Can be set to <b>On</b> , <b>Off</b> , or the default <b>Auto</b> . Indirectly maps to the Citrix INI file setting <code>ZLKeyboardMode=[0 1 2]</code> , which controls keyboard latency reduction.  0=off  1=always on  2=dynamic selection based on actual latency
root/ConnectionType/xen/general/monitorNetwork	Monitor network connectivity. Set to <b>Off</b> to monitor nothing. Set to <b>Local network link status only</b> to only monitor the status of the local network link. Set to <b>Server online status</b> to monitor both the status of the local network link and the server's connectivity. If it is broken, exit to log in to the GUI for the client or disconnect the connection for HP ThinPro.
root/ConnectionType/xen/general/mouseClickFeedback	Can be set to <b>On</b> , <b>Off</b> , or the default <b>Auto</b> . Indirectly maps to the Citrix INI file setting <code>ZLKeyboardMode=[0 1 2]</code> , which controls keyboard latency reduction.  0=off  1=always on  2=dynamic selection based on actual latency
root/ConnectionType/xen/general/mouseMiddleButtonPaste	Directly maps to the Citrix INI file setting <code>MouseSendsControlV=boolean</code> , which enables a middle-button paste emulation function for Windows sessions. The default is <b>False</b> . All clients are set to <b>0</b> by default.
root/ConnectionType/xen/general/noInfoBox	Directly maps to the Citrix INI file setting <code>PopupOnExit=boolean</code> , which causes the client manager, <code>wfcmgr</code> , to pop up when a client session terminates.
root/ConnectionType/xen/general/printerAutoCreation	Set to <b>0</b> to disable printer mapping.
root/ConnectionType/xen/general/proxyAddress	The proxy address to use if a manual proxy setting is selected through 'proxyType'.
root/ConnectionType/xen/general/proxyPassword	The proxy password to use if a manual proxy setting is selected through 'proxyType'. This field will be encrypted using rc4 encryption.
root/ConnectionType/xen/general/proxyPort	The proxy port to use if a manual proxy setting is selected through 'proxyType'.
root/ConnectionType/xen/general/proxyType	Selects the type of proxy to use for XenDesktop connections. 'Use Browser settings' is supported only if a local browser is installed.
root/ConnectionType/xen/general/proxyUser	The proxy user to use if a manual proxy setting is selected through 'proxyType'.
root/ConnectionType/xen/general/serverCheckTimeout	

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

Registry key	Description
root/ConnectionType/xen/general/sessionSharingClient	Directly maps to the Citrix INI file setting <code>EnableSessionSharingClient=boolean</code> , which sends session-sharing requests to other ICA sessions on the same X display. The default is <b>False</b> . All clients are set to <b>1</b> by default.
root/ConnectionType/xen/general/sound	Can be set to the default <b>High Quality</b> , <b>Med Quality</b> , <b>Low Quality</b> , or <b>Disabled</b> . Quality indirectly maps to the Citrix INI file setting <code>AudioBandwidthLimit=[0 1 2]</code> .  0=high  1=medium  2=low
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/{UUID}/address	
root/ConnectionType/xen/general/transparentKeyPassthrough	Can be set to <b>Translated (Local)</b> , <b>Direct in full screen desktops only (FullScreenOnly)</b> , or <b>Direct (Remote)</b> . Indirectly maps to the Citrix INI file setting <code>TransparentKeyPassthrough=string</code> , which enables keyboard shortcut sequences defined by the local Windows manager in the session. Keywords are Local, Remote, and FullScreenOnly. The default is <b>FullScreenOnly</b> .
root/ConnectionType/xen/general/twRedundantImageltems	Controls the number of screen areas that will be tracked in Thinwire 2 to prevent any redundant drawing of bitmap images. An adequate value for a session with 1024x768 resolution is 300. Use with <code>EnableOSS=False</code> , <code>Default=0</code> .
root/ConnectionType/xen/general/useAlternateAddress	Directly maps to the Citrix INI file setting <code>UseAlternateAddress=boolean</code> , which uses an alternate address for firewall connections. The default is <b>False</b> . All clients are set to <b>0</b> by default.
root/ConnectionType/xen/general/useBitmapCache	Directly maps to the Citrix INI file setting <code>PersistentCacheEnabled=boolean</code> . The default is <b>False</b> . All clients are set to <b>0</b> by default.
root/ConnectionType/xen/general/useEUKS	Controls use of Extended Unicode Keyboard Support on Windows servers. The default is <b>0</b> .  0—No EUKS  1—EUKS used as fallback  2—Use EUKS whenever possible
root/ConnectionType/xen/general/useLocalIM	Directly maps to the Citrix INI file setting <code>useLocalIME=boolean</code> , which uses the local X input method to interpret keyboard input. This is supported only for European languages. The default is <b>True</b> . All clients are set to <b>1</b> by default.
root/ConnectionType/xen/general/waitForNetwork	If set to <b>1</b> , the connection will not be launched until networking is available. This makes sure that, on a slow network, the connection does not launch before networking is available, causing a failure.

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

Registry key	Description
root/ConnectionType/xen/general/webcamSupport	Select the appropriate option to use the webcam. Enable HDX optimization for webcam, redirect the webcam to VMware Horizon View, or disable it completely.
root/ConnectionType/xen/general/windowHeight	If 'windowSize' is set to <b>Fixed Size</b> , this key will be used to set the height of the window in pixels.
root/ConnectionType/xen/general/windowPercent	If 'windowType' is set to <b>Percentage of Screen Size</b> , this key will be used to set the size of the window. Valid values are 0–100.
root/ConnectionType/xen/general/windowSize	When set to <b>Full Screen</b> (the default), the connection will be maximized without borders on all available screens. When set to <b>Percentage of Screen Size</b> the 'windowSizePercentage' key can be used to specify the size of the window as a percentage as the total screen area. When set to <b>Fixed Size</b> the 'windowSizeWidth' and 'windowSizeHeight' keys can be used to specify the size of the window in pixels. To have "Percentage of Screen Size" take effect "enableForceDirectConnect" has to be set to <b>1</b> and "seamlessWindow" has to be set to <b>0</b> .  <b>NOTE:</b> This setting will only work with XenApp and only if the server allows direct connections.
root/ConnectionType/xen/general/windowWidth	If 'windowSize' is set to 'Fixed Size', this key will be used to set the width of the window in pixels
root/ConnectionType/xen/gui/XenDesktopPanel/disabled	Set to <b>1</b> to disable the Xen Desktop Panel and its taskbar. Usually, set to <b>1</b> when autoStartResource or autoStartDesktop is enabled.
root/ConnectionType/xen/gui/XenManager/name	The name of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/xen/gui/XenManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/xen/gui/XenManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/ConnectionType/xen/gui/XenManager/widgets/address	
root/ConnectionType/xen/gui/XenManager/widgets/appInMenu	
root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop	
root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource	
root/ConnectionType/xen/gui/XenManager/widgets/autostart	
root/ConnectionType/xen/gui/XenManager/widgets/domain	
root/ConnectionType/xen/gui/XenManager/widgets/enablePNADesktopIcons	

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

Registry key	Description
root/ConnectionType/xen/gui/XenManager/widgets/enablePNASStartMenuItems	
root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection	
root/ConnectionType/xen/gui/XenManager/widgets/folder	
root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon	
root/ConnectionType/xen/gui/XenManager/widgets/isInMenu	
root/ConnectionType/xen/gui/XenManager/widgets/label	
root/ConnectionType/xen/gui/XenManager/widgets/password	
root/ConnectionType/xen/gui/XenManager/widgets/storeFrontConn	
root/ConnectionType/xen/gui/XenManager/widgets/username	
root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork	
root/ConnectionType/xen/gui/fbpanel/autohide	Whether to autohide the taskbar. Set to 'true' to <b>autohide</b> the taskbar.
root/ConnectionType/xen/gui/fbpanel/edge	The default position of the taskbar when more than one published desktop or application is available.
root/ConnectionType/xen/gui/fbpanel/hidden	Set to <b>1</b> to completely hide the taskbar. Can be hidden 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

This section describes the registry keys, functions, options, and descriptions in the **root > Dashboard** folder.



**NOTE:** The dashboard is the same thing as the taskbar. The terminology in the registry will be revised in a future release of HP ThinPro.

**Table E-12** root > Dashboard

Registry key	Description
root/Dashboard/GUI/Clock	When set to the default of <b>1</b> , the clock is shown in the taskbar.
root/Dashboard/GUI/ConnectionManager	When set to the default of <b>1</b> , the connection manager is shown in the taskbar.

**Table E-12** root > Dashboard (continued)

Registry key	Description
root/Dashboard/GUI/ControlPanel	When set to the default of <b>1</b> , the Control Panel is shown in the taskbar.
root/Dashboard/GUI/PowerButton	When set to the default of <b>1</b> , the power button is shown in the taskbar.
root/Dashboard/GUI/SystemInformation	When set to the default of <b>1</b> , the system information button is shown in the taskbar.
root/Dashboard/GUI/SystemTray	When set to the default of <b>1</b> , the system tray is shown in the taskbar.
root/Dashboard/GUI/TaskBar	When set to the default of <b>1</b> , the taskbar is shown.
root/Dashboard/General/AlwaysOnTop	When set to the default of <b>1</b> , the taskbar is always on top of the other windows in the screen.
root/Dashboard/General/AutoHide	This key controls the auto-hide features of the taskbar. When set to <b>1</b> , the taskbar automatically hides after the mouse leaves it. When set to the default of <b>0</b> , the taskbar is always visible.
root/Dashboard/General/EnterLeaveTimeout	The timeout (in milliseconds) required to trigger the taskbar to slide on or off the screen. This option is only used when autohide is enabled.
root/Dashboard/General/IconSize	Controls the size of the icons on the taskbar.
root/Dashboard/General/Length	The length of the taskbar's main panel.
root/Dashboard/General/LengthToScreenSide	When set to the default of <b>1</b> , the length of the taskbar is both fixed and equal to the length of the screen side to which it is anchored. When set to <b>0</b> , the length is automatic.
root/Dashboard/General/PanelDockSide	The docking side of the taskbar's main panel in the screen.
root/Dashboard/General/RemainPixel	The visible pixels when the taskbar slides in.
root/Dashboard/General/SlidingTimeout	The amount of time (in milliseconds) it takes for the taskbar to slide on and off the screen. This option is only used when autohide is enabled.
root/Dashboard/General/Width	The width of the taskbar's main panel.

## root > Display

This section describes the registry keys, functions, options, and descriptions in the **root > Display** folder.

**Table E-13** root > Display

Registry key	Description
root/Display/Configuration/displaymode	Specifies the display mode of the unit. A value of <b>0</b> denotes standard mode (1–4 monitors), whereas a value of <b>1</b> denotes a 6-monitor mode. The HP t610 with the appropriate add-on card is the only supported hardware.
root/Display/Configuration/hexlayout	Specifies the layout in six-monitor mode. See the displaymode key.

**Table E-13 root > Display (continued)**

Registry key	Description
root/Display/Configuration/hexprofile	Specifies the profile used in six-monitor mode. See the displaymode key.
root/Display/Configuration/primaryprofile	This must always be set to <b>default</b> .
root/Display/Configuration/quaternarymode	If supported, specifies the position of the fourth monitor relative to the primary monitor.  0—Same As 1—Above 2—Right Of 3—Left Of 4—Below 5—None  <b>NOTE:</b> This is hardware dependent and is not supported on all models. The HP t5335z does not support two monitors.
root/Display/Configuration/quaternaryprofile	Specifies the profile name used for the fourth monitor.
root/Display/Configuration/quaternaryrelative	Indicates which monitor is referenced to set the position of the fourth monitor. See the tertiarymode key.
root/Display/Configuration/secondaryConnector	Specifies the secondary connector.
root/Display/Configuration/secondarymode	If supported, specifies the position of the secondary monitor relative to the primary monitor.  0—Same As 1—Above 2—Right Of 3—Left Of 4—Below 5—None  <b>NOTE:</b> This is hardware dependent and is not supported on all models. The HP t5335z does not support two monitors.
root/Display/Configuration/secondaryorientation	
root/Display/Configuration/secondaryprofile	Specifies the profile name used for the second monitor.
root/Display/Configuration/swapstate	Specifies which connector contains the primary monitor. This is hardware-dependent and might not be implemented on all models. Generally, <b>0</b> means the primary monitor is on the VGA connector and <b>1</b> means the 'other' connector. For the HP t5565z, <b>0</b> means the primary is on the DVI-I connector and <b>1</b> means the primary is on the DVI-D connector. The HP t5335z does not support two monitors.
root/Display/Configuration/tertiarymode	If supported, specifies the position of the third monitor relative to the primary monitor.  0—Same As 1—Above



**Table E-13** root > Display (continued)

Registry key	Description
	<p>2—Right Of</p> <p>3—Left Of</p> <p>4—Below</p> <p>5—None</p> <p><b>NOTE:</b> This is hardware dependent and is not supported on all models. The HP t5335z does not support two monitors.</p>
root/Display/Configuration/tertiaryprofile	Specifies the profile name for the third monitor.
root/Display/Configuration/tertiaryrelative	Indicates which monitor is referenced to set the position of the third monitor. See the tertiarymode key.
root/Display/Profiles/{UUID}/colorScaling	The color temperature or direct RGB scaling for thin clients with built-in monitors. The entry is a six-digit hex value RRGGBB, where fffff would indicate full (100%) scaling on all three color channels.
root/Display/Profiles/{UUID}/depth	The display bit depth per pixel. A higher bit depth means better quality, but more data and thus a lower performance.
root/Display/Profiles/{UUID}/height	The desired monitor resolution height. A value of <b>0</b> means auto-detect the resolution.
root/Display/Profiles/{UUID}/label	Display profile name. This should be <b>default</b> .
root/Display/Profiles/{UUID}/orientation	<p>Specifies monitor orientation:</p> <p>0—Normal</p> <p>1—Rotate left</p> <p>2—Rotate right</p> <p>3—Invert</p>
root/Display/Profiles/{UUID}/refresh	<p>Specifies the desired monitor refresh rate; not all refresh rates are supported for all resolutions. The values supported by the client depend on the monitor. A value of <b>0</b> means auto-detect the refresh rate.</p> <p><b>IMPORTANT:</b> Picking a refresh rate that is not supported by the monitor attached to the client results in a black screen. HP recommends leaving this set to <b>0</b>.</p>
root/Display/Profiles/{UUID}/width	The desired monitor resolution width. A value of <b>0</b> means auto-detect the resolution.
root/Display/userLock	If set to <b>1</b> and the display settings have been modified by the user, then the display settings are preserved and the profile's settings are discarded.
root/Display/userLockEngaged	Flag set to 1 after a user modification. If set to <b>1</b> as well as userLock, then the display settings are preserved and the profiles settings are discarded. This key should not need to be modified.

## root > Network

This section describes the registry keys, functions, options, and descriptions in the **root > Network** folder.

**Table E-14** root > Network

Registry key	Description
root/Network/ActiveDirectory/Domain	Active Directory domain.
root/Network/ActiveDirectory/DynamicDNS	Enable dynamic DNS.
root/Network/ActiveDirectory/Enabled	Enables Active Directory.
root/Network/ActiveDirectory/Method	Method used to provide user credentials.
root/Network/ActiveDirectory/Password	Active Directory domain user password, only valid in static method.
root/Network/ActiveDirectory/Username	Active Directory domain username, only valid in static method.
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 through DHCP. Up to three IPv4 or IPv6 addresses may be specified, separated by commas.
root/Network/DefaultHostnamePattern	Specifies the default hostname pattern that a thin client uses to generate a new hostname when the hostname registry key and hostname in /etc/hostname are both empty. In the pattern, use % as a delimiter. For example, the format HPTC%MAC:1-6% means that HPTC is the prefix and the thin client MAC is used for characters 1-6. So a thin client with MAC address 11:22:33:44:55:66 generates the hostname HPTC112233.
root/Network/FtpProxy	FTP proxy address.
root/Network/Hostname	Hostname of the client.
root/Network/HttpProxy	HTTP proxy address.
root/Network/HttpsProxy	HTTPS proxy address.
root/Network/IPSec/IPSecRules/{UUID}/DstAddr	Destination address for the IPsec rule.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethod	Authentication method for the IPsec rule. Enter <b>PSK</b> to use a pre-shared key and <b>Certificate</b> to use certificate files.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethodCACert	When the authentication method is 'Certificate', the CA certificate file's path is saved in this key.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethodClientCert	When the authentication method is 'Certificate', the client certificate file's path is saved in this key.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethodPresharedKey	When the authentication method is 'PSK', the pre-shared key value is saved in this key.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethodPrivateKey	When the authentication method is 'Certificate', the client certificate file's corresponding private key file path is saved in this key.
root/Network/IPSec/IPSecRules/{UUID}/MMDHGroup	Phase 1 Diffie-Hellman group.
root/Network/IPSec/IPSecRules/{UUID}/MMEncryptionAlg	Phase 1 encryption algorithm.

**Table E-14 root > Network (continued)**

Registry key	Description
root/Network/IPSec/IPSecRules/{UUID}/MMIntegrityAlg	Phase 1 integrity algorithm.
root/Network/IPSec/IPSecRules/{UUID}/MMLifetimeMinutes	Phase 1 lifetime.
root/Network/IPSec/IPSecRules/{UUID}/QMAHEnable	Enables Phase 2 AH.
root/Network/IPSec/IPSecRules/{UUID}/QMAHIntegrityAlg	Phase 2 AH integrity algorithm.
root/Network/IPSec/IPSecRules/{UUID}/QMESPEnable	Enables Phase 2 ESP.
root/Network/IPSec/IPSecRules/{UUID}/QMESPEncryptionAlg	Phase 2 ESP encryption algorithm.
root/Network/IPSec/IPSecRules/{UUID}/QMESPIntegrityAlg	Phase 2 ESP integrity algorithm.
root/Network/IPSec/IPSecRules/{UUID}/QMLifetimeSeconds	Phase 2 lifetime.
root/Network/IPSec/IPSecRules/{UUID}/RuleDescription	Description for the IPsec rule, such as purpose for creating the rule.
root/Network/IPSec/IPSecRules/{UUID}/RuleEnable	Rule enable or disable flag. When set to <b>1</b> the rule will be enabled. Set to <b>0</b> to disable the rule.
root/Network/IPSec/IPSecRules/{UUID}/RuleName	Name of the IPsec rule.
root/Network/IPSec/IPSecRules/{UUID}/SrcAddr	Source address for the IPsec rule.
root/Network/IPSec/IPSecRules/{UUID}/TunnelDstAddr	Tunnel destination address for the IPsec rule.
root/Network/IPSec/IPSecRules/{UUID}/TunnelEnable	Enables tunnel setting for the IPsec rule. When enabled, the rule is 'apply to tunnel mode'.
root/Network/IPSec/IPSecRules/{UUID}/TunnelSrcAddr	Tunnel source address for the IPsec rule.
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 through 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	Auto-starts VPN on system boot.
root/Network/VPN/Domain	VPN domain.
root/Network/VPN/Gateway	VPN gateway.
root/Network/VPN/Group	VPN group.
root/Network/VPN/GroupPassword	VPN group password.
root/Network/VPN/Password	VPN user password.
root/Network/VPN/Type	VPN type.
root/Network/VPN/Username	VPN user name.
root/Network/VPN/vpncSecurity	VPNC security level.
root/Network/Wired/DefaultGateway	The default gateway the device will use to communicate to the internet. Typically, this is the address of the router.

**Table E-14** root > Network (continued)

Registry key	Description
	<b>NOTE:</b> This setting will take effect only when 'Method' is set to 'Static'.
root/Network/Wired/EnableDefGatewayasDNS	If set to 1, the default gateway is Name Server.
root/Network/Wired/EthernetSpeed	The link speed of the primary ethernet network interface. Automatic will allow it to choose the fastest available link speed, (usually 1 Gbps or 100 Mbps 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 or hubs that do not perform appropriate auto-negotiation.
root/Network/Wired/IPAddress	The IPv4 address of the device. This setting will take effect only when 'Method' is set to 'Static'.
root/Network/Wired/IPv6Enable	Set this key to 1 when working in an IPv6 environment.
root/Network/Wired/Interface	The default ethernet interface or NIC.
root/Network/Wired/MTU	Set the MTU on a wired link whether it uses a static address or a DHCP-acquired IP address.
root/Network/Wired/Method	When set to <b>Automatic</b> , the device will use DHCP to attempt to retrieve network settings. When set to <b>'Static'</b> , the 'IPAddress', 'SubnetMask', and 'DefaultGateway' can be set manually using the available keys. HP does not recommend using 'Static' in a generic client profile, as it will cause all clients to receive the same IP address.
root/Network/Wired/Security/CACert	Path to the CA certification file.
root/Network/Wired/Security/Identity	Identity or anonymous identity.
root/Network/Wired/Security/InnerAuth	PEAP inner authentication protocols.
root/Network/Wired/Security/InnerAuthTTLS	TTLS inner authentication protocols.
root/Network/Wired/Security/PEAPVersion	PEAP version.
root/Network/Wired/Security/Password	Password.
root/Network/Wired/Security/PrivateKey	Path to the private key file, only for use in TLS authentication.
root/Network/Wired/Security/Type	Wired 802.1x authentication types.
root/Network/Wired/Security/UserCert	Path to the user certification file, only for use in TLS authentication.
root/Network/Wired/Security/Username	Username.
root/Network/Wired/SubnetMask	The subnet mask of the device; for example, 255.255.255.0 for a standard class C subnet. This setting will take effect only when 'Method' is set to 'Static'.
root/Network/Wireless/DefaultGateway	The default gateway the device will use to communicate to the internet. Typically, this is the address of the router. This setting will take effect only when 'Method' is set to 'Static'.
root/Network/Wireless/EnableDefGatewayAsDNS	If set to 1, the default gateway is Name Server.
root/Network/Wireless/IPAddress	The IPv4 address of the device. This setting will take effect only when 'Method' is set to 'Static'.

**Table E-14 root > Network (continued)**

Registry key	Description
root/Network/Wireless/IPv6Enable	Set this key to <b>1</b> when working in an IPv6 environment.
root/Network/Wireless/Interface	The default wireless interface or wireless network adapter.
root/Network/Wireless/Method	When set to <b>Automatic</b> , the device will use DHCP to attempt to retrieve network settings. When set to 'Static', the 'IPAddress', 'SubnetMask', and 'DefaultGateway' can be set manually using the available keys. HP does not recommend using 'Static' in a generic client profile, as it will cause all clients to receive the same IP address.
root/Network/Wireless/PowerEnable	Set this key to <b>0</b> to disable to power management of the wireless network card.
root/Network/Wireless/SSID	The selected wireless access point SSID.
root/Network/Wireless/SSIDHidden	The hidden status of the selected wireless access point SSID.
root/Network/Wireless/Security/CACert	Path to the CA certification file.
root/Network/Wireless/Security/EAPFASTPAC	Path to the EAP FAST authentication PAC file.
root/Network/Wireless/Security/EAPFASTProvision	EAP FAST authentication fast provisioning option.
root/Network/Wireless/Security/Identity	Identity or anonymous identity.
root/Network/Wireless/Security/InnerAuth	PEAP inner authentication protocols.
root/Network/Wireless/Security/InnerAuthTTLS	TTLS inner authentication protocols.
root/Network/Wireless/Security/PEAPVersion	PEAP version.
root/Network/Wireless/Security/Password	Password.
root/Network/Wireless/Security/PrivateKey	Path to the private key file, only used in TLS authentication.
root/Network/Wireless/Security/Type	Wireless authentication types.
root/Network/Wireless/Security/UserCert	Path to the user certification file, only for use in TLS authentication.
root/Network/Wireless/Security/Username	Username.
root/Network/Wireless/Security/WEPAuth	WEP authentication type.
root/Network/Wireless/Security/WEPIndex	WEP password index, only for use in WEP.
root/Network/Wireless/SubnetMask	The subnet mask of the device; for example, 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	Disables the left-click menu on the network system tray icon that allows you to start, stop, and restart the network connection.
root/Network/disableRightClickMenu	Disables the right-click menu on the network system tray icon that allows you to start, stop, and restart the network connection.
root/Network/iPeak/ShowStatus	If set to <b>1</b> , Network Manager displays the HP Velocity status in the systray icon.
root/Network/iPeak/Status	If set to <b>1</b> , HP Velocity is enabled. When enabled, it does not affect network packet transmission if the server side

**Table E-14** root > Network (continued)

Registry key	Description
	component is not detected. If set to <b>2</b> , HP Velocity is in monitor mode and only monitors network status.
root/Network/userLock	If set to <b>1</b> and the display settings have been modified by the user, then the display settings are preserved and the profile's settings are discarded.
root/Network/userLockEngaged	Flag set to 1 after a user modification. If set to <b>1</b> as well as userLock, then the display settings are preserved and the profiles settings are discarded. This key should not need to be modified.

## root > SCIM

This section describes the registry keys, functions, options, and descriptions in the **root > SCIM** folder.

**Table E-15** root > SCIM

Registry key	Description
root/SCIM/ScimEnabled	If set to <b>1</b> , SCIM is enabled for CJK input.
	<b>NOTE:</b> This key is available only if the East Asia languages client kit is installed.

## root > Serial

This section describes the registry keys, functions, options, and descriptions in the **root > Serial** folder.

**Table E-16** root > Serial

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

## root > SystemInfo

This section describes the registry keys, functions, options, and descriptions in the **root > SystemInfo** folder.

**Table E-17** root > SystemInfo

Registry key	Description
root/SystemInfo/Pages/General	Enables or disables the General tab. If set to <b>0</b> , users cannot see this tab of the System Information panel.
root/SystemInfo/Pages/NetTools	Enables or disables the Net Tools tab. If set to <b>0</b> , users cannot see this tab of the System Information panel.
root/SystemInfo/Pages/Network	Enables or disables the Network tab. If set to <b>0</b> , users cannot see this tab of the System Information panel.
root/SystemInfo/Pages/SoftwareInformation	Enables or disables the Software Information tab. If set to <b>0</b> , users cannot see this tab of the System Information panel.
root/SystemInfo/Pages/SystemLogs	Enables or disables the System Logs tab. If set to <b>0</b> , users cannot see this tab of the System Information panel.
root/SystemInfo/authorized	Enables the System Information button in the ThinPro Control Center.

## root > TaskMgr

This section describes the registry keys, functions, options, and descriptions in the **root > TaskMgr** folder.

**Table E-18** root > TaskMgr

Registry key	Description
root/TaskMgr/General/AlwaysOnTop	Sets the Task Manager window to always be on top.

## root > USB

This section describes the registry keys, functions, options, and descriptions in the **root > USB** folder.

**Table E-19** root > USB

Registry key	Description
root/USB/Classes/<Defined at Interface level>/ClassID	USB class ID number.
root/USB/Classes/<Defined at Interface level>/DisplayName	USB class name.
root/USB/Classes/<Defined at Interface level>/State	Whether this class is mapped to the remote computer.
root/USB/Classes/<Defined at Interface level>/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Application Specific Interface/ClassID	USB class ID number.
root/USB/Classes/Application Specific Interface/DisplayName	USB class name.
root/USB/Classes/Application Specific Interface/Status	Whether this class is mapped to the remote computer.

**Table E-19 root > USB (continued)**

Registry key	Description
root/USB/Classes/Application Specific Interface/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Audio/ClassID	USB class ID number.
root/USB/Classes/Audio/DisplayName	USB class name.
root/USB/Classes/Audio/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Audio/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Audio and Video Devices/ClassID	USB class ID number.
root/USB/Classes/Audio and Video Devices/DisplayName	USB class name.
root/USB/Classes/Audio and Video Devices/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Audio and Video Devices/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/CDC Data/ClassID	USB class ID number.
root/USB/Classes/CDC Data/DisplayName	USB class name.
root/USB/Classes/CDC Data/State	Whether this class is mapped to the remote computer.
root/USB/Classes/CDC Data/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Communications/ClassID	USB class ID number.
root/USB/Classes/Communications/DisplayName	USB class name.
root/USB/Classes/Communications/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Communications/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Content Security/ClassID	USB class ID number.
root/USB/Classes/Content Security/DisplayName	USB class name.
root/USB/Classes/Content Security/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Content Security/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Diagnostic Device/ClassID	USB class ID number.
root/USB/Classes/Diagnostic Device/DisplayName	USB class name.
root/USB/Classes/Diagnostic Device/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Diagnostic Device/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Hub/ClassID	USB class ID number.
root/USB/Classes/Hub/DisplayName	USB class name.
root/USB/Classes/Hub/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Hub/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.



**Table E-19 root > USB (continued)**

Registry key	Description
root/USB/Classes/Human Interface Device/ClassID	USB class ID number.
root/USB/Classes/Human Interface Device/DisplayName	USB class name.
root/USB/Classes/Human Interface Device/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Human Interface Device/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Imaging/ClassID	USB class ID number.
root/USB/Classes/Imaging/DisplayName	USB class name.
root/USB/Classes/Imaging/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Imaging/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Mass Storage/ClassID	USB class ID number.
root/USB/Classes/Mass Storage/DisplayName	USB class name.
root/USB/Classes/Mass Storage/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Mass Storage/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Miscellaneous Device/ClassID	USB class ID number.
root/USB/Classes/Miscellaneous Device/DisplayName	USB class name.
root/USB/Classes/Miscellaneous Device/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Miscellaneous Device/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Personal Healthcare/ClassID	USB class ID number.
root/USB/Classes/Personal Healthcare/DisplayName	USB class name.
root/USB/Classes/Personal Healthcare/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Personal Healthcare/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Physical Interface Device/ClassID	USB class ID number.
root/USB/Classes/Physical Interface Device/DisplayName	USB class name.
root/USB/Classes/Physical Interface Device/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Physical Interface Device/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Printer/ClassID	USB class ID number.
root/USB/Classes/Printer/DisplayName	USB class name.
root/USB/Classes/Printer/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Printer/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/ShowTab	When set to <b>1</b> , the Classes tab shows in the USB Manager GUI.

**Table E-19 root > USB (continued)**

Registry key	Description
root/USB/Classes/Smart Card/ClassID	USB class ID number.
root/USB/Classes/Smart Card/DisplayName	USB class name.
root/USB/Classes/Smart Card/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Smart Card/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Vendor Specific Class/ClassID	USB class ID number.
root/USB/Classes/Vendor Specific Class/DisplayName	USB class name.
root/USB/Classes/Vendor Specific Class/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Vendor Specific Class/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Video/ClassID	USB class ID number.
root/USB/Classes/Video/DisplayName	USB class name.
root/USB/Classes/Video/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Video/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Classes/Wireless/ClassID	USB class ID number.
root/USB/Classes/Wireless/DisplayName	USB class name.
root/USB/Classes/Wireless/State	Whether this class is mapped to the remote computer.
root/USB/Classes/Wireless/Visible	Indicates whether the class is shown on the UI, not shown on the UI, or disabled.
root/USB/Devices/{UUID}/DisplayName	The name that shows in the USB Manager UI. If not supplied, the USB Manager attempts to generate an appropriate name using device information.
root/USB/Devices/{UUID}/ProductID	Product ID of the device.
root/USB/Devices/{UUID}/State	Whether this class is mapped to the remote computer. If <b>0</b> , does not redirect. If <b>1</b> , uses defaults. If <b>2</b> , redirects.
root/USB/Devices/{UUID}/VendorID	Vendor ID of the device.
root/USB/root/holdProtocolStatic	If set to <b>1</b> , does not switch the remote USB protocol based on which value is chosen. Always leave it at the value in root/protocol.
root/USB/root/mass-storage/allowed	If set to <b>1</b> , mass storage devices will be auto-mounted when the protocol is "local".
root/USB/root/mass-storage/read-only	If set to <b>1</b> , when mass storage devices are auto-mounted locally, they will be mounted read-only.
root/USB/root/opendebug	If set to <b>1</b> , a debug message writes to /tmp/USB-mgr-log.
root/USB/root/protocol	Keeps track of the current owner of the remote USB. Used internally only.

## root > auto-update

This section describes the registry keys, functions, options, and descriptions in the **root > auto-update** folder.

**Table E-20** root > auto-update

Registry key	Description
root/auto-update/DNSAliasDir	Indicates the default root directory on the SCS server for DNS alias mode.
root/auto-update/ManualUpdate	Set to <b>1</b> to disable checking the DHCP tag and DNS alias, broadcasting for Automatic Update server URLs, and setting the Automatic Update server manually. If this is set, then the password, path, protocol, user, and ServerURL must be set to make sure that the update server is known.
root/auto-update/ScheduledScan/Enabled	Set to <b>1</b> to have the clients perform periodic scans of the Automatic Update server to check for updates. If set to <b>0</b> , clients check for updates only during boot.
root/auto-update/ScheduledScan/Interval	The amount of time to wait between scheduled update scans. Specify the period in HH:MM format. Intervals longer than 24 hours can be specified. For example, to schedule updates every 48 hours, set Interval to <b>48:00</b> .
root/auto-update/ScheduledScan/Period	Clients randomly activate their scheduled scan during the defined period. Use a long period to avoid cases where all the clients update at the same time, causing network congestion. Specify the period in HH:MM format. For example, to spread the client updates throughout a 2.5 hour period, set Period to <b>02:30</b> .
root/auto-update/ScheduledScan/StartTime	The start of the first scheduled scan in HH:MM format using the 24-hour time format. For example, 4:35 pm is entered as <b>16:35</b> .
root/auto-update/ServerURL	The IP or domain name of the update server used when ManualUpdate is enabled.
root/auto-update/enableOnBootup	Set to <b>0</b> to disable Automatic Update on boot. By default, this is set to <b>1</b> , which allows Automatic Update to check for system updates.
root/auto-update/gui/auto-update/ManualUpdate	Controls the state of the <b>Enable manual configuration</b> widget in the Automatic Update utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/auto-update/gui/auto-update/ServerURL	Controls the state of the <b>Server</b> widget in the Automatic Update utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/auto-update/gui/auto-update/enableOnBootup	Controls the state of the <b>Enable Automatic Update on system startup</b> widget in the Automatic Update utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/auto-update/gui/auto-update/password	Controls the state of the <b>Password</b> widget in the Automatic Update utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget

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

Registry key	Description
	is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/auto-update/gui/auto-update/protocol	Controls the state of the <b>Protocol</b> widget in the Automatic Update utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/auto-update/gui/auto-update/tag	This key has no function.
root/auto-update/gui/auto-update/user	Controls the state of the <b>User name</b> widget in the Automatic Update utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/auto-update/password	The desired password when ManualUpdate is enabled. This is used only when the protocol is set to ftp. This field is stored, encrypted, within the profile.
root/auto-update/path	The desired relative path from the default server URL when ManualUpdate is enabled. Typically, this is empty or set to <b>auto-update</b> .
root/auto-update/protocol	Set to <b>ftp</b> , <b>http</b> , or <b>https</b> to define the desired update server protocol when ManualUpdate is enabled.
root/auto-update/tag	This previous indicated the tag number used for DHCP 137 and is now obsolete and not detected.
root/auto-update/user	The desired user when ManualUpdate is enabled. This is used only when the protocol is set to <b>ftp</b> .

## root > background

This section describes the registry keys, functions, options, and descriptions in the **root > background** folder.

**Table E-21** root > background

Registry key	Description
root/background/desktop/color	When the theme setting is <b>none</b> , this key is the default color used by the user-defined theme. If the theme setting is not none, this setting has no function.
root/background/desktop/imagePath	When the theme setting is <b>none</b> , this key is the desktop background image path used by the user-defined theme. If the theme setting is not none, this setting has no function.
root/background/desktop/lastBrowseDir	When the theme setting is <b>none</b> , this key is the last used directory. If the theme setting is not none, this setting has no function.

**Table E-21 root > background (continued)**

Registry key	Description
root/background/desktop/style	When the theme setting is <b>none</b> , this key defines how the image is put on the desktop. If the theme setting is not none, this setting has no function.
root/background/desktop/theme	The system theme setting. This value is set through the GUI. The valid settings are listed by the themes that exist on the system. Set to <b>none</b> to let the user define the theme.

## root > config-wizard

This section describes the registry keys, functions, options, and descriptions in the **root > config-wizard** folder.

**Table E-22 root > config-wizard**

Registry key	Description
root/config-wizard/FirmwareUpdate/firmwareUpdateTimeout	The timeout period (in seconds) that the thin client checks for updates. Set to <b>-1</b> for no timeout.
root/config-wizard/FirmwareUpdate/firmwareUpdateURL	The FTP URL for image updates.
root/config-wizard/enableConnectionCheck	When set to <b>0</b> , the connection session check is disabled. When set to the default of <b>1</b> , the connection session check is enabled on boot.
root/config-wizard/enableNetworkCheck	When set to <b>0</b> , the network check is disabled. When set to the default of <b>1</b> , the network check is enabled on boot.
root/config-wizard/updateCheck	When set to <b>1</b> , the update check is enabled. The default <b>0</b> disables the update check at boot.

## root > desktop

This section describes the registry keys, functions, options, and descriptions in the **root > desktop** folder.

**Table E-23 root > desktop**

Registry key	Description
root/desktop/shortcuts/default-Close/command	Specifies the command
root/desktop/shortcuts/default-Close/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/default-Lock/command	Specifies the command
root/desktop/shortcuts/default-Lock/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/default-MaximizeWindow/command	Specifies the command
root/desktop/shortcuts/default-MaximizeWindow/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/default-MinimizeAll/command	Specifies the command
root/desktop/shortcuts/default-MinimizeAll/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/default-MinimizeWindow/command	Specifies the command

**Table E-23** root > desktop (continued)

Registry key	Description
root/desktop/shortcuts/default-MinimizeWindow/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/default-NextWindow/command	Specifies the command
root/desktop/shortcuts/default-NextWindow/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/default-Shutdown/command	Specifies the command
root/desktop/shortcuts/default-Shutdown/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/default-ToggleFullscreen/command	Specifies the command
root/desktop/shortcuts/default-ToggleFullscreen/shortcut	Specifies the shortcut name.
root/desktop/shortcuts/reset-display-prefs/command	Specifies the command
root/desktop/shortcuts/reset-display-prefs/shortcut	Specifies the shortcut name.

## root > entries

This section describes the registry keys, functions, options, and descriptions in the **root > entries** folder.

**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

This section describes the registry keys, functions, options, and descriptions in the **root > keyboard** folder.

**Table E-25** root > keyboard

Registry key	Description
root/keyboard/SystrayMenu/keyboardLayout	When set to the default of <b>1</b> , the right-click menu on the keyboard systray icon offers an option to open the Keyboard Layout utility.
root/keyboard/SystrayMenu/languages	When set to the default of <b>1</b> , the right-click menu on the keyboard systray icon offers an option to open the Language Selection utility.

**Table E-25 root > keyboard (continued)**

Registry key	Description
root/keyboard/SystrayMenu/virtualKeyboard	When set to the default of <b>1</b> , the right-click menu on the keyboard systray icon offers an option to open the virtual keyboard.
root/keyboard/VisibleInSystray	When set to the default of <b>1</b> , an indicator in the system tray displays the current keyboard layout.
root/keyboard/XkbLayout	An internal key used to map the model/layout to an XKB keyboard layout. This key should not need to be modified.
root/keyboard/XkbModel	An internal key used to map the model/layout to an XKB keyboard model. This key should not need to be modified.
root/keyboard/XkbOptions	An internal key used to map the model/layout to XKB keyboard options. This key should not need to be modified.
root/keyboard/XkbVariant	An internal key used to map the model/layout to an XKB keyboard variant. This key should not need to be modified.
root/keyboard/enable2	If set to <b>1</b> , the secondary keyboard layout 'layout2' can be switched to through the keyboard shortcut defined by 'switch'.
root/keyboard/layout	The keyboard layout defines what symbols the keys generate. This is frequently language dependent. English (en), Spanish (es), French (fr), German (de), and Japanese (jp) are the most common layouts.
root/keyboard/layout2	The secondary keyboard layout.
root/keyboard/model	The keyboard model defines which keys are where on the keyboard. The most common is the standard 'pc104' or international 'pc105'. Other models are also supported.
root/keyboard/model2	The secondary keyboard model.
root/keyboard/numlock	If set to the default <b>1</b> , the numlock function will be turned on at boot; otherwise, the numlock light will be turned off.
root/keyboard/rdp_kb	An internal key used to map the model/layout to an RDP keyboard map. This key should not need to be modified.
root/keyboard/switch	Used to set the keyboard shortcut to switch between the first and second layout, if 'enable2' is set. Valid values are <b>grp:ctrl_shift_toggle</b> , <b>grp:ctrl_alt_toggle</b> , and <b>grp:alt_shift_toggle</b> .
root/keyboard/variant	The keyboard variant defines slight variations in the layout. Typically, the <b>wincompat</b> variation is used, as it most closely matches Windows keyboard layouts.
root/keyboard/variant2	The secondary keyboard variant.

## root > logging

This section describes the registry keys, functions, options, and descriptions in the **root > logging** folder.

**Table E-26** root > logging

Registry key	Description
root/logging/general/debug	If set to <b>1</b> , debugging will be enabled on 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

This section describes the registry keys, functions, options, and descriptions in the **root > mouse** folder.

**Table E-27** root > mouse

Registry key	Description
root/mouse/MouseHandedness	Whether the mouse is right-handed or left-handed. <b>0</b> for right-handed, <b>1</b> for left-handed.
root/mouse/MouseSpeed	The acceleration of the mouse pointer. Typically a number from 0–25 is in the usable range. <b>0</b> will completely disable acceleration, causing the pointer to move at a constant slow, but measurable pace.
root/mouse/MouseThreshold	The number of pixels before acceleration will be enabled. <b>0</b> will set the acceleration to a natural curve that gradually scales acceleration, allowing for both precise and quick movements.

## root > screensaver

This section describes the registry keys, functions, options, and descriptions in the **root > screensaver** folder.

**Table E-28** root > screensaver

Registry key	Description
root/screensaver/ctrlbindkey	Set to <b>1</b> to start the screen lock.
root/screensaver/enableCustomLogo	Set to <b>1</b> to use a customized picture for the screen lock.
root/screensaver/enableDPMS	Set to <b>0</b> to disable monitor power management. This causes the monitor to stay on unless turned off manually.
root/screensaver/enableScreensaver	Set to <b>1</b> to enable the screen saver.
root/screensaver/enableSleep	Set to <b>0</b> to disable sleep.
root/screensaver/lockScreen	Set to <b>1</b> to require a password when the user switches from the screen lock state to the normal working state.
root/screensaver/mode	Sets the rendering mode for the screen saver picture. Set to <b>Center</b> to put the picture in the center of the screen, <b>Stretch</b> to stretch the picture to fit the screen, <b>Tile</b> to show the picture in tiled mode, and <b>Default</b> to fill the picture without any further processing.



**Table E-28** root > screensaver (continued)

Registry key	Description
root/screensaver/off	Timeout delay to turn the monitor off (in minutes).
root/screensaver/standby	Timeout delay to put the monitor into standby (in minutes).
root/screensaver/suspend	Timeout delay to suspend the monitor (in minutes).
root/screensaver/timeoutScreensaver	Timeout delay to start the screen saver (in minutes).
root/screensaver/timeoutSleep	Timeout delay to put the thin client to sleep (in minutes).

## root > security

This section describes the registry keys, functions, options, and descriptions in the **root > security** folder.

**Table E-29** root > security

Registry key	Description
root/security/mustLogin	Set to <b>1</b> to force all users to log in before accessing the desktop.

## root > sshd

This section describes the registry keys, functions, options, and descriptions in the **root > sshd** folder.

**Table E-30** root > sshd

Registry key	Description
root/sshd/enabled	Set to <b>1</b> to enable the ssh daemon so that the user can access the thin client through ssh.
root/sshd/userAccess	Set to <b>1</b> to allow non-administrators to connect to the thin client through ssh.

## root > time

This section describes the registry keys, functions, options, and descriptions in the **root > time** folder.

**Table E-31** root > time

Registry key	Description
root/time/NTPServers	A comma-separated list of NTP servers to use. Private NTP servers or large virtual NTP clusters such as 'pool.ntp.org' are the best choices to minimize server load. Clear this field to return to using DHCP servers (tag 42) instead of a fixed list.
root/time/TimeServerIPAddress	This is the time server used by the Linux net command. These servers are typically the DC servers on the corporate network. Use this when the NTP servers are either not configured or not responding. The Linux net command

**Table E-31 root > time (continued)**

Registry key	Description
	identifies this server on its own; however, a specific server IP address can be provided here if desired.
root/time/WebServerURL	Specifies the web server URL. This server is queried using the http protocol to fetch the time. This URL can be within the intranet or over the internet.
root/time/timezone	Used to manually specify the timezone. Timezones should be specified in the following format: '[region]/[subregion]' as defined by 'Linux timezone:' in the client date and time control panel menu item.
root/time/use24HourFormat	Choose according to locale:  0—AM/PM format  1—24-hour format
root/time/useDHCPTimezone	If set to 1, clients will attempt to set the timezone through DHCP. To properly set the timezone through this key, make sure that the DHCP server for the clients forwards the 'code' DHCP tag (usually tag 101, though 100 and 2 can work).
root/time/useNTPServers	Set to 1 to enable the use of NTP time servers to synchronize the client clock. If this is enabled, make sure an NTP server is specified via DHCP or the 'NTPServers' key.

## root > touchscreen

This section describes the registry keys, functions, options, and descriptions in the **root > touchscreen** folder.

**Table E-32 root > touchscreen**

Registry key	Description
root/touchscreen/calibrated	This key is reserved for use.
root/touchscreen/enabled	Set to 1 to enable the touchscreen module in the system.
root/touchscreen/maxx	This key is reserved for use.
root/touchscreen/maxy	This key is reserved for use.
root/touchscreen/minx	This key is reserved for use.
root/touchscreen/miny	This key is reserved for use.
root/touchscreen/port	The device port to connect to the touchscreen.
root/touchscreen/swapx	This key is reserved for use.
root/touchscreen/swapy	This key is reserved for use.
root/touchscreen/type	The controller type for the touchscreen.

## root > translation

This section describes the registry keys, functions, options, and descriptions in the **root > translation** folder.

**Table E-33** root > translation

Registry key	Description
root/translation/coreSettings/localeMapping/{ <b>language</b> }	An internal key used to provide the text string next to the appropriate language on the language selector. This key should not need to be modified.
root/translation/coreSettings/localeSettings	Changes 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), and fr_FR (French). Other locales, such as ja_JP (Japanese) and zh_CN (Chinese), might be available as client updates.
root/translation/gui/LocaleManager/name	The name of the settings editor for this application. This key should not need to be modified.
root/translation/gui/LocaleManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/translation/gui/LocaleManager/title	The window title of the settings editor for this application. This key should not need to be modified.
root/translation/gui/LocaleManager/widgets/localeSettings	Controls the locale setting widget in the Language utility. This box should be hidden and the key's value should be <b>inactive</b> . This key should not need to be modified.

## root > usb-update

This section describes the registry keys, functions, options, and descriptions in the **root > usb-update** folder.

**Table E-34** root > usb-update

Registry key	Description
root/usb-update/authentication	Controls whether or not an administrator password is required for USB updates.
root/usb-update/enable	Enables or disables USB auto-update detection.
root/usb-update/height	The height of the user interface in pixels.
root/usb-update/searchMaxDepth	The depth of the subdirectories to be searched for updates. Setting a high search depth might cause delays on USB keys that have thousands of directories.
root/usb-update/width	The width of the user interface in pixels.

## root > users

This section describes the registry keys, functions, options, and descriptions in the **root > users** folder.

**Table E-35 root > users**

Registry key	Description
root/users/gui/hptc-user-rights/name	The name of the GUI. This key should not be modified.
root/users/gui/hptc-user-rights/status	The status of the GUI. This key should not be modified.
root/users/gui/hptc-user-rights/title	The title of the GUI. This key should not be modified.
root/users/root/password	The password for Administrator Mode. If empty, Administrator Mode is locked. Administrator Mode gives access to all control panel items.
root/users/user/SSO	
root/users/user/WOL	Enables Wake on LAN feature.
root/users/user/XHostCheck	Enables X host access control security.
root/users/user/apps/hptc-ad-dns-mgr/authorized	If set to <b>1</b> , the AD/DDNS Manager item will be enabled for users.
root/users/user/apps/hptc-agent-mgr/authorized	If set to <b>1</b> , the HPDM Manager item will be enabled for users.
root/users/user/apps/hptc-auto-update/authorized	If set to <b>0</b> , users will not be able to access Automatic Update server settings. The default configuration is disabled because clients will receive their Automatic Update server URL through broadcast or DHCP tag.
root/users/user/apps/hptc-background-mgr/authorized	If set to <b>1</b> , the Background Manager item will be enabled for users.
root/users/user/apps/hptc-bluetooth-manager/authorized	If set to <b>0</b> , users will not be able to use the Bluetooth Manager anymore.
root/users/user/apps/hptc-cda/authorized	If set to <b>1</b> , the CDA mode Manager item will be enabled for users.
root/users/user/apps/hptc-cert-mgr/authorized	If set to <b>0</b> , users will not be able to access Certificate Manager settings. This might be useful in a DHCP-only environment where all certificate manager settings are given to clients by the DHCP server.
root/users/user/apps/hptc-clientaggregation-mgr/authorized	If set to <b>1</b> , the Client Aggregation Manager item will be enabled for users.
root/users/user/apps/hptc-date-mgr/authorized	If set to <b>0</b> , users will not be able to access local client date and time settings. This might be useful in an environment where the client date and time is set by NTP.
root/users/user/apps/hptc-dhcp-mgr/authorized	If set to <b>1</b> , the DHCP Manager item will be enabled for users.
root/users/user/apps/hptc-display-prefs/authorized	If set to <b>0</b> , users will not be able to modify the screen resolution, bit depth, or refresh rate.
root/users/user/apps/hptc-easy-update/authorized	If set to <b>1</b> , the Easy Update Manager item will be enabled for users.
root/users/user/apps/hptc-i18n-mgr/authorized	If set to <b>1</b> , the locales control panel item will be enabled for users.
root/users/user/apps/hptc-keyboard-layout/authorized	If set to <b>1</b> , the full keyboard layout control panel item will be enabled for users.
root/users/user/apps/hptc-mixer/authorized	If set to <b>0</b> , the full-size mixer control panel will be disabled for users. It is usually redundant, as the mini control covers the same functions.

**Table E-35 root > users (continued)**

Registry key	Description
root/users/user/apps/hptc-mouse/authorized	If set to <b>0</b> , users will not be able to modify local client mouse settings. Users will still be able to modify mouse settings through remote host settings.
root/users/user/apps/hptc-network-mgr/authorized	If set to <b>0</b> , users will not be able to access network settings. This might be useful in a DHCP-only environment where all network settings are given to clients by the DHCP server.
root/users/user/apps/hptc-printer-mgr/authorized	If set to <b>0</b> , users will not be able to set Windows driver values for locally attached printers, which might prevent some printers from mapping to remote sessions properly. This setting does not affect USB redirection.
root/users/user/apps/hptc-restore/authorized	If set to <b>1</b> , users will be able to manage restore points.
root/users/user/apps/hptc-screenlock-mgr/authorized	If set to <b>1</b> , the Screensaver Manager item will be enabled for users.
root/users/user/apps/hptc-security/authorized	If set to <b>1</b> , the security item will be enabled for users.
root/users/user/apps/hptc-shortcut-mgr/authorized	If set to <b>1</b> , the shortcut manager item will be enabled for users.
root/users/user/apps/hptc-sshd-mgr/authorized	If set to <b>1</b> , the Secure Shell Daemon Manager will be enabled for users.
root/users/user/apps/hptc-task-mgr/authorized	If set to <b>1</b> , the Task Manager item will be enabled for users.
root/users/user/apps/hptc-text-editor/authorized	If set to <b>1</b> , the text editor will be enabled for users.
root/users/user/apps/hptc-thinstate/authorized	If set to <b>1</b> , the ThinState Manager item will be enabled for users.
root/users/user/apps/hptc-touchscreen/authorized	If set to <b>1</b> , the Touchscreen Manager item will be enabled for users.
root/users/user/apps/hptc-usb-mgr/authorized	If set to <b>1</b> , the USB Manager item will be enabled for users.
root/users/user/apps/hptc-user-rights/authorized	If set to <b>1</b> , the ThinPro Configuration Manager item will be enabled for users.
root/users/user/apps/hptc-vncshadow/authorized	If set to <b>1</b> , the VNC Shadowing control panel item will be enabled for users.
root/users/user/apps/hptc-xterm/authorized	If set to <b>0</b> , a root X terminal control panel item will be enabled for users.  <b>WARNING!</b> Enabling root terminal access is a security risk and not recommended in a production environment. The root terminal should only be enabled for use in debugging a protected, non-production environment.
root/users/user/apps/scim-setup/authorized	If set to <b>1</b> , the SCIM control panel item will be enabled for users.  <b>NOTE:</b> SCIM is used for Asian language input and might not be present on the system without the installation of an Asian language kit.
root/users/user/hideDesktopPanel	If set to <b>1</b> , then desktop panels such as fbpanel or taskbar will not be started or shown on the desktop. If set to <b>1</b> in Kiosk Mode, then the power button will be displayed in the user interface.

**Table E-35 root > users (continued)**

Registry key	Description
root/users/user/kioskMode	
root/users/user/launchConnectionManager	Enables the launch of the connection manager at startup.
root/users/user/rightclick	Enables the right-click menu for the desktop.
root/users/user/ssconnectiontype	
root/users/user/switchAdmin	Allows the user to switch to Admin Mode.
root/users/user/xhosts/{UUID}/xhost	The XHost address/name in the XHost access control list.

## root > vncserver

This section describes the registry keys, functions, options, and descriptions in the **root > vncserver** folder.

**Table E-36 root > vncserver**

Registry key	Description
root/vncserver/coreSettings/enableVncShadow	Set to <b>1</b> to enable the VNC Shadow server for the thin client.
root/vncserver/coreSettings/userNotificationMessage	The notification message that is shown to the user.
root/vncserver/coreSettings/vncNotifyShowTimeout	Set to <b>1</b> to set a timeout on the notification message.
root/vncserver/coreSettings/vncNotifyTimeout	The notification message that is shown if vncNotifyShowTimeout is enabled. After the timeout, the message is hidden.
root/vncserver/coreSettings/vncNotifyUser	Set to <b>1</b> to enable a notification message when a VNC client attempts to connect to the thin client.
root/vncserver/coreSettings/vncPassword	The password for VNC if vncUsePassword is enabled.
root/vncserver/coreSettings/vncReadOnly	Set to <b>1</b> to restrict VNC to view-only mode. VNC clients can only watch.
root/vncserver/coreSettings/vncRefuseInDefault	Set to <b>1</b> to refuse the connection if the user does not accept or deny the notification message. Set to <b>0</b> to accept the connection if the user does not accept or deny the notification message.
root/vncserver/coreSettings/vncTakeEffectRightNow	Set to <b>1</b> to cause VNC setting to take effect immediately.
root/vncserver/coreSettings/vncUsePassword	Set to <b>1</b> to cause VNC to use a password to authenticate client access.
root/vncserver/coreSettings/vncUseSSL	Controls whether SSL is used for the VNC connection. The default is <b>0</b> .
root/vncserver/gui/VNCShadowManager/name	The name of the settings editor for this application. This key should not need to be modified.
root/vncserver/gui/VNCShadowManager/status	The active status of the settings editor for this application. This key should not need to be modified.
root/vncserver/gui/VNCShadowManager/title	The window title of the settings editor for this application. This key should not need to be modified.

**Table E-36** root > vncserver (continued)

Registry key	Description
root/vncserver/gui/VNCShadowManager/widgets/enableVncShadow	Controls the state for the <b>Enable VNC Shadow</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/userNotificationMessage	Controls the state for the <b>User Notification Message</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout	Controls the state for the <b>VNC Show Timeout for Notification</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout	Controls the state for the numerical widget that specifies the notification timeout value in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser	Controls the state for the <b>VNC Notify User to Allow Refuse</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncPassword	Controls the state for the <b>Set Password</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly	Controls the state for the <b>VNC Read Only</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault	Controls the state for the <b>Refuse connections in default</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow	Controls the state for the <b>Re-set VNC server right now</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword	Controls the state for the <b>VNC Use Password</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL	Controls the state for the <b>VNC Use SSL</b> widget in the VNC Shadowing utility. If set to <b>active</b> , the widget is visible in the UI and the user can interact with it. If set to <b>inactive</b> , the

**Table E-36** root > vncserver (continued)

Registry key	Description
	widget is hidden. If set to <b>read-only</b> , the widget is visible in the read-only state.



# Index

## A

- AD/DDNS Manager 9
- add-ons 1
- audio redirection
  - RDP 38
  - VMware Horizon View 42

## B

- Background Manager 9

## C

- Certificate Manager 22
- certificates
  - installing 22
  - VMware Horizon View 44
- Citrix
  - HDX MediaStream 27
  - settings, connection-specific 31
  - settings, general 28
  - support matrix 28
- client aggregation 11
  - client configuration 12
  - server configuration 13
- client login screen
  - customizing 68
- client profile
  - adding files 59
  - adding symbolic link 60
  - certificates 59
  - loading 57
  - modifying 57
  - registry settings 58
  - saving 60
- clients
  - updating. *See* updating clients
- Connection Manager controls 5
- connections
  - common settings 24
  - hiding 9
  - types 1
- Control Panel
  - AD/DDNS Manager 9
  - Background Manager 9
  - Client Aggregation 11

- Customization Center 9
- Date and Time 9
- DHCP Option Manager 23
- Display Preferences 13
- Easy Update 9
- Keyboard Shortcuts 10
- Language 9
- Mouse 8
- Network 14
  - overview 8
- SCEP Manager 10
- SCIM Input Method Setup 8
- Screensaver 9
- Security 9
- Serial Manager 10
- Snapshots 9
- Sound 8
- SSHD Manager 9
- Task Manager 10
- Text Editor 10
- ThinState. *See* HP ThinState
- Touch Screen 8
- utilities, hiding 9
- VNC Shadow 21
- X Terminal 10
- custom connections 52

## D

- date and time settings 9
- device redirection
  - RDP 36
  - VMware Horizon View 42
- DHCP options 23
- display preferences 13
- display profiles 13

## E

- Easy Update 9

## F

- finding more resources 1

## G

- getting started 3

## H

- HDX MediaStream 27
- HP Device Manager. *See* HPDM Agent
- HP Smart Client Services
  - installing 53
  - overview 53
  - Profile Editor. *See* Profile Editor supported operating systems 53
- HP TeemTalk. *See* TeemTalk
- HP Velocity 17
- HPDM Agent 9

## I

- image updates 1
- imaging. *See* HP ThinState interface
  - navigating 4

## K

- keyboard shortcuts 10
- Kiosk Mode 25

## L

- language settings 9

## M

- mass storage redirection
  - RDP 37
  - VMware Horizon View 42
- MMR
  - VMware Horizon View 42
- mouse settings 8
- multimedia redirection
  - RDP 36

## N

- network settings
  - accessing 14
  - DNS 16
  - HP Velocity 17
  - IPSec 16
  - VPN 17

- wired 15
- wireless 15

**P**

- parallel printer configuration 60
- passwords, change 9
- printer configuration 60
- printer redirection
  - RDP 37
  - VMware Horizon View 42
- printers 13
- Profile Editor
  - using 57

**R**

- RDP
  - audio redirection 38
  - device redirection 36
  - mass storage redirection 37
  - multi-monitor sessions 35
  - multimedia redirection 36
  - printer redirection 37
  - RemoteFX 35
  - settings, connection-specific 32
  - settings, general 32
  - smart card redirection 38
  - USB redirection 36
- registry keys 76
- RemoteFX 35
- RFX. *See* RemoteFX

**S**

- SCEP Manager 10, 22
- SCIM 8
- screensaver settings 9
- security settings 9
- Serial Manager 10
- serial printer configuration 60
- smart card redirection
  - RDP 38
  - VMware Horizon View 43
- snapshots 9
- sound settings 8
- SSH 50
- SSHD Manager 9
- system diagnostics 63
- system information
  - viewing 6
- system information screens
  - hiding 6

**T**

- Task Manager 10
- taskbar
  - using 4
- TeemTalk 48
- Telnet 52
- text editor 10
- ThinState. *See* HP ThinState
- touch screen settings 8
- troubleshooting 62
  - firmware corruption 62
  - network connectivity 62
  - using system diagnostics 63

**U**

- updating clients
  - broadcast update 54
  - DHCP tagging update 55
  - DNS alias update 55
  - manual update 56
- USB redirection
  - RDP 36
  - USB Manager 14
  - VMware Horizon View 42

**V**

- VMware Horizon View
  - audio redirection 42
  - certificate security levels 44
  - certificates 44
  - changing protocols 44
  - device redirection 42
  - keyboard shortcuts 41
  - mass storage redirection 42
  - MMR 42
  - multi-monitor sessions 41
  - printer redirection 42
  - settings 39
  - smart card redirection 43
  - USB redirection 42
  - webcam redirection 43
- VNC Shadowing 21

**W**

- Web Browser
  - settings, connection-specific 47
  - settings, general 47
- webcam redirection
  - VMware Horizon View 43

- websites
  - Citrix support 1
  - HP support 1
  - Microsoft support 1
  - VMware support 1

**X**

- X Terminal 10
- XDMCP 50