



HP Smart Zero Core 4.3

Administrator's Guide

© Copyright 2013 Hewlett-Packard
Development Company, L.P.

Microsoft, Windows, and Windows Vista are
U.S. registered trademarks of Microsoft
Corporation.

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 2013

First Edition: May 2013

Document Part Number: 727358-002

Table of contents

1 Welcome	1
Intended audience	1
Document organization	1
2 Getting started	2
Logging in to the desktop	2
Selecting a connection type	2
Configuring a basic connection	2
Using the desktop	3
3 Navigating clients	4
Using the client toolbar	4
Understanding the system status icon	4
Using client information screens	5
Using the Status tab	5
Using the Network tab	6
Using the Net Tools tab	6
Using the System Information tab	7
Using the Systems Logs tab	7
Hiding client information screens	7
4 Configuring clients	9
Using the client control panel	9
Accessing the client control panel	9
Using the client control panel (User Mode)	9
Main control panel options (User Mode)	9
Additional control panel options (User Mode)	10
Using the client control panel (Administrator Mode)	11
Main control panel options (Administrator Mode)	11
Additional control panel options (Administrator Mode)	12
Overview of RDP connection features	14
Using Kiosk Mode with RDP	15
Using RemoteFX with RDP	15
Using Multimedia Redirection with RDP	15
Using multi-monitor sessions with RDP	16
Using device redirection with RDP	16

Using USB redirection with RDP	16
Using mass storage redirection with RDP	17
Using printer redirection with RDP	17
Using audio redirection with RDP	18
Using smart card redirection with RDP	18
Setting RDP options	18
Overview of Citrix connection features	19
Citrix connection management features	19
Citrix receiver features	19
HDX MediaStream support matrix	20
Citrix connection support matrix	21
Overview of VMware Horizon View connection features	21
Using Kiosk Mode with VMware Horizon View	21
Using Multimedia Redirection with VMware Horizon View	22
Using multi-monitor sessions with VMware Horizon View	22
Using keyboard shortcuts with VMware Horizon View	22
Using device redirection with VMware Horizon View	23
Using USB redirection with VMware Horizon View	23
Using mass storage redirection with VMware Horizon View	23
Using printer redirection with VMware Horizon View	23
Using audio redirection with VMware Horizon View	23
Using smart card redirection with VMware Horizon View	24
Using webcam redirection with VMware Horizon View	24
Additional VMware Horizon View connection options	25
Using advanced command line arguments with VMware Horizon View	25
Using a Teradici-accelerated t410 system with VMware Horizon View	26
Switching to the standard VMware Horizon View client	26
Changing the VMware Horizon View protocol type	26
Installing certificates on clients	27
VMware Horizon View HTTPS and certificate management requirements	27
Redirecting USB devices	28
Mapping a serial or parallel printer	29
5 Troubleshooting clients	30
Troubleshooting network connectivity	30
Troubleshooting firmware corruption	31
Reimaging client device firmware	31
Troubleshooting serial or parallel printer configuration	31
Troubleshooting Citrix password expiration	31
Using system diagnostics to troubleshoot	32
Saving system diagnostic data	32

Uncompressing the system diagnostic files	32
Uncompressing the system diagnostic files on Windows-based systems	32
Uncompressing the system diagnostic files in Linux- or Unix-based systems ..	32
Viewing the system diagnostic files	32
Viewing files in the Commands folder	33
Viewing files in the /var/log folder	33
Viewing files in the /etc folder	33
6 HP Smart Zero Client Services	34
Supported operating systems	34
Preparing to install HP Smart Zero Client Services	35
Downloading and installing HP Smart Zero Client Services	35
7 Using the Profile Editor	36
Accessing the Profile Editor	36
Loading a client profile	36
Modifying a client profile	36
Selecting the platform of a client profile	36
Selecting the connection type of a client profile	37
Modifying the registry settings of a client profile	37
Enabling or disabling menu items on clients	37
Enabling or disabling user configurations on clients	37
Adding files to a client profile	38
Adding a configuration file to a client profile	38
Adding certificates to a client profile	38
Adding a symbolic link to a client profile	39
Saving the client profile	39
Configuring a serial or parallel printer	39
Obtaining the printer baud rate	40
Setting up printer ports	40
Installing printers on the server	40
8 Using Automatic Intelligence	42
Viewing the Automatic Update website	42
Creating an Automatic Update profile	42
Updating clients	42
Using the broadcast update method	43
Using the DHCP tag update method	43
Example of performing DHCP tagging	43
Using the DNS alias update method	44

Using the manual update method	44
Performing a manual update	44
Using HP Intelligent Delivery Service	45
How HP Intelligent Delivery Service works	45
Starting, stopping, and pausing HP Intelligent Delivery Service	45
Viewing the HP Intelligent Delivery Service application log	45
HP Intelligent Delivery Service registry keys	45
Using HP Device Manager	45

Appendix A Client keyboard language 46

Appendix B Customizing the client login screen 48

Customizing the screen background	48
Common attributes	48
Elements	51
Image	53
Text	53
Customizing the client login dialog box	56
Customizing the central frame	56
Customizing the text for the header	57
Customizing the icon for the header	57

Appendix C HP Smart Zero Core registry settings 58

root > Audio	58
root > ConnectionManager	59
root > ConnectionType	59
root > ConnectionType > freerdp	60
root > ConnectionType > view	64
root > ConnectionType > xen	68
root > Display	77
root > Network	78
root > USB	82
root > keyboard	82
root > logging	83
root > mouse	83
root > printer-mapping-mgr	84
root > printers	84
root > screensaver	84
root > time	85
root > translation	85

root > users	86
root > zero-login	88
Appendix D VMware Horizon View USB configuration	90
USB options in previous HP Smart Zero Core releases	90
VMware Horizon View USB device families	90
Index	92

1 Welcome

This guide is a comprehensive reference that describes how to administer HP Smart Zero Core on HP Smart Zero Clients, as well as the software prerequisites and installation tasks involved with performing a standard or custom server installation.

Intended audience

This guide is intended for administrators and technical personnel who are responsible for installing, configuring, and administering HP Smart Zero Client systems.

Document organization

This guide is divided into the following chapters and appendixes:

- [Getting started on page 2](#)—Describes how to log in to and use the desktop and configure a basic connection.
- [Navigating clients on page 4](#)—Provides an overview of the client toolbar and information screens.
- [Configuring clients on page 9](#)—Describes the settings available in the client control panel, an overview of connection features, and other configurations such as device redirection and printer port mapping.
- [Troubleshooting clients on page 30](#)—Describes common troubleshooting issues and solutions.
- [HP Smart Zero Client Services on page 34](#)—Describes software requirements and provides information on how to use the InstallShield Wizard to perform both a standard installation and a custom installation, as well as start up and launch an HP Smart Zero Client for the first time.
- [Using the Profile Editor on page 36](#)—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.
- [Using Automatic Intelligence on page 42](#)—Defines the Automatic Intelligence directory structure and how to attach configuration files to a profile, and also describes how to view the HP Smart Zero Client Services website and remotely manage client profiles stored on the Automatic Intelligence server.
- [Client keyboard language on page 46](#)—Lists the client keyboard language options.
- [Customizing the client login screen on page 48](#)—Describes the common attributes and elements used in customizing the client login screen background.
- [HP Smart Zero Core registry settings on page 58](#)—Lists the HP Smart Zero Core registry settings. The tables in this section describe the registry key path, application functions, and options as presented in the Registry Editor component of the Profile Editor.
- [VMware Horizon View USB configuration on page 90](#)—Describes USB configuration with VMware Horizon View.

2 Getting started

This chapter includes the following topics:

- [Logging in to the desktop](#)
- [Configuring a basic connection](#)
- [Using the desktop](#)

Logging in to the desktop

During system startup, the client attempts to detect and install settings automatically. If you previously configured the client using either HP Smart Zero Client Services or HP Device Manager, log in to the desktop using the standard login screen.

Selecting a connection type

For small deployments where you do not need device management, the **Select Connection Type** screen will display during the initial setup. Use this screen to select the connection type to be used.

The following default connection types are available:

- Citrix
- Microsoft RDP7
- VMware Horizon View
- Web Browser



TIP: In the login dialog, a yellow warning icon indicates that you did not configure an HP Smart Zero Client Services server. In this case, the client cannot automatically detect an update server. To disable this notification, do one of the following:

Configure an HP Smart Zero Client Services server as described in [HP Smart Zero Client Services on page 34](#).

—or—

Using the Configuration menu, under the **Additional Configuration > Automatic Update** dialog, disable automatic updates.

Configuring a basic connection

To configure a basic connection:

1. In the **Connection Selection** screen, click the type of connection you want to use.
2. In the **Remote Connection Server** dialog box, under server name or address, type one of the following:
 - Server URL
 - Server Hostname
 - Server IP address

3. Click **OK**.
4. Log in to the desktop using the following information:
 - Username
 - Password
 - Domain

 **NOTE:** You only need to configure the connection once. The configuration is stored for future sessions. To change the connection, choose **Select Connection Type** from the configuration menu.

Using the desktop


Desktops typically launch full-screen on all available monitors.

To return to the local desktop from inside a full-screen remote desktop, use this shortcut:

- ▲ Press **Ctrl+Alt+End**.

To toggle between desktop systems, use this shortcut:

- ▲ Press **Ctrl+Alt+Tab**.

 **TIP:** To configure shortcuts, use the Control Panel.

3 Navigating clients






This chapter discusses the following topics:

- [Using the client toolbar](#)
- [Using client information screens](#)

Using the client toolbar

Use the client toolbar to access the client menus and to find information about the state of your system.

Table 3-1 Client toolbar

Item	Description
	Powers on, reboots, or powers off the client.
	Displays the client control panel. For more information, see the following Using the client control panel on page 9 .
	Displays the About this client screen. For more information, see Using client information screens on page 5 .
	Corresponds to the state of your system. For more information, see Understanding the system status icon on page 4 .
	Starts, stops, or resets connection.

Understanding the system status icon


The client toolbar displays a system status icon that corresponds to the state of the system. To retrieve detailed information, click the system status icon.

Table 3-2 System status icon information

System state	Description
Error	An X indicates that there is a critical error such as a lack of a network connection.
Warning	A yellow triangle indicates that there is a non-critical error such as an inability to contact a client service. Clicking the icon clears the warning status.
Busy	A spinning circle indicates that the client is busy and no errors are present. This state appears when a connection is starting or other activity is occurring.
Idle	A question mark indicates that the client is idle and no errors are present. Click the icon for more information.
Updating	Spinning arrows indicate that the client is receiving or installing an update from HP Smart Zero Client Services.

Using client information screens

To access the client information screens:

- ▲ On the client toolbar, click .

To learn more about the tabs available under the **About this client** screen, see the following sections:

- [Using the Status tab](#)
- [Using the Network tab](#)
- [Using the Net Tools tab](#)
- [Using the System Information tab](#)
- [Using the Systems Logs tab](#)
- [Hiding client information screens](#)

Using the Status tab

Use the **Status** tab to monitor and identify issues regarding the system's network, client service, and client connectivity.

The following table describes the items shown on this tab.

Table 3-3 About this client—Status

Item	Description
Network	<p>Displays a green check mark indicator if the system is functioning normally, and shows information including:</p> <ul style="list-style-type: none">• IP address• Gateway• MAC address <p>If the client network is not functioning normally, this item may display a Warning or Error status and message.</p>
Smart Client Service	<p>Displays a green check mark indicator, if normal, and generates a system message that indicates the name of the configured HP Smart Zero Client Services server.</p> <p>If HP Smart Zero Client Services is improperly configured or points to an invalid server, one of the following errors will appear:</p> <ul style="list-style-type: none">• An X and error message indicates that an error has occurred while attempting to retrieve client settings from the server.• A warning message indicates that an error occurred while attempting to retrieve client settings from the server.
Connection	<p>Displays a green check mark if the client is connected to the server.</p> <p>When the connection is improperly set up or points to an invalid server, one of the following errors will appear:</p> <ul style="list-style-type: none">• An X indicates that a connection has not been configured for your system.

Table 3-3 About this client—Status (continued)

Item	Description
	<ul style="list-style-type: none">• A warning message indicates that an error occurred while attempting to connect to the server.

Using the Network tab

Use the **Network** tab to view network and interface settings shown in the three different panes as described in the table below.

Table 3-4 About this client—Network

Pane	Item
Interface	<ul style="list-style-type: none">• Name• State• IP address• Network mask• MAC address• DHCP server address• Interface statistics
Network	<ul style="list-style-type: none">• Default gateway
DNS Settings	<ul style="list-style-type: none">• Hostname• Default domain• Name servers

Using the Net Tools tab

Use the **Net Tools** tab to configure options for monitoring system performance and troubleshoot network issues using the following procedure:

1. In the **Net Tools** tab, under **Select Tool**, choose one of the options described in the following table.

Table 3-5 About this client—Net Tools

Option	Description
Ping	<p>Use this tool to attempt to establish contact with another device on the network using an IP address that you specify.</p> <ul style="list-style-type: none">• If successful, the tool reports the total amount of time in milliseconds it took to receive a response from the device.• If unsuccessful, the tool does not return any data.
DNS Lookup	<p>Use this tool to resolve a domain name into an IP address using the DNS name servers registered under the Network tab.</p>

Table 3-5 About this client—Net Tools (continued)

Option	Description
	The tool returns the IP of the server if it can be resolved. Otherwise, it returns an error code and message.
Trace Route	Use this tool to track the path that a network packet takes from one device to another. <ul style="list-style-type: none">• If successful, the tool reports the path it took through each router or other network device to the destination.• If unsuccessful, the tool returns an error message.

2. Type or select the options you want to monitor.
3. When completed, click **Start Process**.

Using the System Information tab


The **System Information** tab provides the following information about your client:

- Platform
- Total RAM
- Serial number
- OS kernel version
- OS build ID
- Main software installed



Using the Systems Logs tab

The **System Logs** tab displays all the logs placed on the following:

- System kernel
- X Server
- HP Smart Zero Client Services

 **NOTE:** To generate additional diagnostic reports or log information, select **Enable Debug Mode**. This information might be requested by HP for troubleshooting purposes.

Hiding client information screens

1. Click , select **Administrator/User Mode Switch**, and then log in as the Administrator.
2. Under , select **Additional Configuration > Advanced > XTerminal**.
3. On the XTerminal command line, type `regeditor`, and then press **Enter**.
4. In the Registry Editor, under **Smart Client Registry > root/SystemInfo/Pages**, select the item corresponding to the tab you want to hide:
 - General
 - NetTools

- Network
 - SoftwareInformation
 - SystemLogs
5. Set the value to **0**, and then click **Save**.
 6. When completed, reboot the system.

4 Configuring clients

Beyond the basic setup described in [Getting started on page 2](#), there are many additional options available for each connection type. These options provide many unique system configurations and make sure that the client can be customized for most environments.


This chapter includes the topics as follows:

- [Using the client control panel](#)
- [Overview of RDP connection features](#)
- [Overview of Citrix connection features](#)
- [Overview of VMware Horizon View connection features](#)
- [Installing certificates on clients](#)
- [Redirecting USB devices](#)
- [Mapping a serial or parallel printer](#)

Using the client control panel

The client control panel provides users and administrators access to options that allow them configure the client.

Accessing the client control panel

To access the client control panel, click  on the client toolbar. The client control panel supports the following modes of operation:

- User Mode (default)
- Administrator Mode

Using the client control panel (User Mode)

This section describes the client control panel options available in User Mode.

Main control panel options (User Mode)

Table 4-1 Main control panel options (User Mode)

Menu option	Description
Select Connection Type	Lets you configure one of the following connection types: <ul style="list-style-type: none">• Citrix• RDP7• VMware Horizon View• Web Browser

Table 4-1 Main control panel options (User Mode) (continued)

Menu option	Description
Administrator/User Mode Switch	Lets authorized administrators access the Administrator Mode control panel menus. NOTE: Before using this option, be sure to set up a password for the Administrator Mode control panel menus.
Language	Lets you display the client interface in a different language.
Keyboard Layout	Lets you change the keyboard layout to accommodate the language used by the keyboard.
Audio	Lets you control the audio level.
Additional Configuration	Opens the additional options menu. For information about the additional options available in User Mode, see Additional control panel options (User Mode) on page 10 .

Additional control panel options (User Mode)

Table 4-2 Additional control panel options (User Mode)

Menu option	Description
Date and Time	Lets you set up the date and time zone using the following options: <ul style="list-style-type: none">• Time zone• Time• Date• Use NTP time servers specified by DHCP• Use the time server of your choice• Do not use a time server
Display Preferences	Lets you configure and test the following custom options for your display hardware: <ul style="list-style-type: none">• Resolution• Depth• Orientation• Primary display video connector (DVI-I or DVI-D)• Secondary monitor mode
Mouse	Lets you set up custom options for your mouse hardware.
Network	Lets you configure the following network settings: <ul style="list-style-type: none">• Wired settings<ul style="list-style-type: none">◦ Network speed◦ Duplex settings◦ Connection method• DNS settings• IPSec settings


Table 4-2 Additional control panel options (User Mode) (continued)

Menu option	Description
	<ul style="list-style-type: none">• VPN settings• HP Velocity settings• Wireless settings<ul style="list-style-type: none">◦ Duplex settings◦ Connection method <p>NOTE: Many wireless networks have security that requires a different authentication and either a password or key.</p>
Printer Mapping	Lets you set up a printer and share it across the network.

Using the client control panel (Administrator Mode)

This section describes the client control panel options available in Administrator Mode.

To log in as an administrator:

1. On the client toolbar, click .
2. In the menu, select **Administrator/User Mode Switch**.
3. In the **Switch to Admin** box, under **Administrative Password**, type your password and then click **OK**.

Main control panel options (Administrator Mode)

Table 4-3 Main control panel options (Administrator Mode)

Menu option	Description
Edit Default Connection	Lets you edit the following default connection settings, depending on the connection type previously configured: <ul style="list-style-type: none">• Network• Window• Options• Local Resources• Experience• Advanced
Administrator/User Mode Switch	Returns you to User Mode.
Audio	Lets you control the playback and recording levels for the default audio device. The default audio device can be changed by selecting the Sound menu option.
Additional Configuration	Opens the additional options menu. For information about the additional options available in Administrator Mode, see Additional control panel options (Administrator Mode) on page 12 .

Additional control panel options (Administrator Mode)

The additional options available in Administrator Mode under **Additional Configuration** are divided into four categories:

- Peripherals
- Setup
- Management
- Advanced

The following tables describe the options available in each category.

Table 4-4 Additional control panel options (Administrator Mode)—Peripherals

Menu option	Description
Display Preferences	<p>Lets you configure and test a primary and secondary display profile for multiple displays connected to the client. You can configure the following profile information:</p> <ul style="list-style-type: none">• Profile Settings<ul style="list-style-type: none">◦ Profile Name◦ Resolution◦ Depth◦ Primary Monitor Orientation• Primary display video connector• Secondary monitor mode
Keyboard Layout	<p>Lets you configure the following custom keyboard layout settings:</p> <ul style="list-style-type: none">• Primary and Secondary Keyboard Layout• Standard Keyboard Layout Type• Keyboard Model• Keyboard Variant• Minimize Local Keyboard Shortcuts
Mouse	<p>Lets you set up custom options for your mouse hardware.</p>
Printer Mapping	<p>Lets you add, edit, and delete printers.</p> <p>Click Add to add a printer, and define the printer information as follows:</p> <ul style="list-style-type: none">• Port• Model• Printer IP address• Remote Queue name• Windows driver• Activate or deactivate the printer <p>To edit or delete a printer, select a printer, and then click either Edit or Delete.</p>

Table 4-4 Additional control panel options (Administrator Mode)—Peripherals (continued)

Menu option	Description
Sound	Lets you set up the audio input and playback settings for your client.
USB Manager	Lets you configure the redirection options for USB devices.

Table 4-5 Additional administrator control panel options—Setup

Menu option	Description
Date and Time	Lets you set up the date and time zone using the following options: <ul style="list-style-type: none">• Time zone• Time• Date• Use NTP time servers specified by DHCP• Use the time server of your choice• Do not use a time server
Language	Lets you display the client interface in a different language.
Network	Lets you configure the following network settings: <ul style="list-style-type: none">• Wired settings<ul style="list-style-type: none">◦ Network speed◦ Duplex settings◦ Connection method• Wireless settings<ul style="list-style-type: none">◦ Connection method• DNS settings• IPSec settings• VPN settings• HP Velocity settings <p>NOTE: Many wireless networks have security that requires a different authentication and either a password or key.</p>
Security	Lets you set up or change system passwords for the client administrator and user.

Table 4-6 Additional administrator control panel options—Management

Menu option	Description
Automatic Update	Lets you configure the Automatic Update server manually.
Factory Reset	Lets you restore the client to its default factory configuration.
VNC Shadow	Lets you use VNC Shadowing.

Table 4-6 Additional administrator control panel options—Management (continued)

Menu option	Description
	<p>Virtual Network Computing (VNC) is a remote control program that allows a user to view the desktop of a remote machine and control it with a local mouse and keyboard, as if they were sitting in front of that computer.</p> <p>Use VNC Shadowing to:</p> <ul style="list-style-type: none">• Allow another system to access a client from a remote location• Make the VNC sessions read-only• Require a password to access the client when using VNC• Allow a user to refuse VNC access to the client• Reset the VNC server

Table 4-7 Additional administrator control panel options—Advanced

Menu option	Description
Certificates	<p>Lets you use the Certificate Manager to do the following:</p> <ul style="list-style-type: none">• View a locally trusted CA and personal certificates• Import certificates to the client using one of the following methods:<ul style="list-style-type: none">◦ Import the certificate from a USB key◦ Import the certificate from a URL
Keyboard Shortcuts	<p>Lets you use the Keyboard Shortcuts Manager to modify existing shortcuts and create new shortcuts that run custom commands.</p>
Task Manager	<p>Lets you monitor the CPU usage and the CPU usage history for the client.</p>
Text Editor	<p>Lets you edit configuration files or scripts directly from the client.</p>
Xterminal	<p>Lets you execute Linux commands outside the client interface.</p>

Overview of RDP connection features

The RDP client is based on FreeRDP 1.0 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

Using Kiosk Mode with RDP

By default, only the server hostname is required to connect. The login screen identifies and authenticates the user. Additional login information can be set in the Connection Settings dialog box available in Administrator Mode.

To enable Kiosk Mode, where the client performs an automatic login to the remote desktop on boot using predefined user credentials, do the following:

1. In Administrator Mode, click  on the client toolbar.
2. Click **Edit Default Connection**.
3. Type a username and password for the Kiosk user.

 **TIP:** The username is a generic expression with restricted domain privileges.

4. Under **Advanced**, do the following:
 - a. Set the **Autostart Priority** to **1**.
 - b. Select **Autoreconnect**.
5. Click **Save**.
6. Click **Reconnect**.

This causes the RDP session to automatically log in on boot. Additionally, if the connection is ever lost due to a logout, disconnect, or network failure, it will automatically reconnect as soon as the connection is restored. The remote host can be configured to autostart any desired applications on login.

To return to the login screen and minimize the session, press **Ctrl+Alt+End**. This enables you to modify the client settings.


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 RemoteFX is available, it will be used.

To disable RFX, set the registry key value to:

- `root/ConnectionType/freerdp/connections/{UUID}/remoteFx` to `'0'`

 **TIP:** HP recommends that you enable or disable RFX on the remote host.

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 registry key to:

- `root/ConnectionType/freerdp/general/enableMMR` to `'0'`

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

- `root/ConnectionType/freerdp/connections/{UUID}/disableMMRwithRFX` to `'1'`



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

Using multi-monitor sessions with RDP

True multi-monitor support does not require special configuration by the administrator or user. 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. If a different primary monitor is desired, it can be set via the local **Display** settings, available in the **Configuration** menu. 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. The recommended **auto** setting uses DDC to communicate with the monitor and automatically sets the resolution to the preferred native resolution of the monitor.

By default, all RDP sessions will be full-screen and span all monitors to enhance the virtualization experience. Additional window options are available through the **Edit Default Connection** option in the **Configuration** menu. Usually, these options are used only on systems supporting multiple simultaneous connections, such as HP ThinPro.



NOTE: The HP t410 All-in-One Smart Zero Client supports a 1366x768 screen resolution only.

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

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

In systems connected to a Windows 7 SP1 host, RDP supports redirection for a wide variety of USB devices running in a Hyper-V Virtual Machine.

In systems connected to a Windows 8 or Windows Server 2012 host, HP Smart Zero Core enables USB redirection to all installations.

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 use additional options for redirection.

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.

If desired, you can disable mass storage redirection. Turn off USB redirection. Then, change the registry key entries as described in the following table.

Table 4-8 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 39](#) 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.

- 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.
- If USBR is enabled, HP recommends that all USB audio devices be redirected by USBR. This makes sure that all audio is mixed locally to improve quality. If USB redirection of an audio device is required, be sure that the RDP **sound** setting is set to **Leave at remote computer** instead of **Bring to this computer**. Configure this setting using the **Local Resources** page in the **Connection Settings** available in Administrator Mode.


Disable MMR if all audio devices are set to local, because it will only play multimedia through the default audio device.

- Microphone redirection is enabled by default. The default microphone volume might need to be adjusted on the client. This can be done through the **Configuration** menu.
- 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 smartcard login, check the **Allow smartcard login** box on the login screen or within the **Connection Settings**. This will allow the user to connect without first specifying credentials. The RDP client will then 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.

Setting RDP options

For the best user experience, use the **Experience** tab in the **Connection Settings** to set the **Connection Speed** to **LAN**. If bandwidth reduction is required, the connection speed can be set to **Modem**, which will disable all experience options.

The additional options described in the following table can be configured via the check boxes on the **Options** tab.

Table 4-9 General connection options

Connection option	Description
Enable Motion Events	Enabled by default. Sends a message to the RDP server every time the pointing device is moved. If this is disabled, “hover over” options, such as tooltips, often fail to appear.
Enable Data Compression	Enabled by default. Data compression can be disabled to reduce the server and client CPU usage, but this results in a drastic increase in the network bandwidth.
Enable Encryption	Enabled by default. Causes all traffic to be encoded with TLS or RC4 encryption. Can be disabled to reduce the client and host CPU usage.
Force bitmap updates	Enabled by default. Causes bitmaps to be saved even when not shown, increasing the client memory usage but improving the redraw of background images.
Attach to console	Disabled by default. When enabled, RDP can be used to connect to servers that have RDP disabled and only have the Administrator console active. Primarily used for debugging.
Send hostname	Sends the specified text string as the client hostname instead of the system hostname.

Overview of Citrix connection features

A Citrix connection accesses the Citrix SBC (Server-Based Computing) and VDI (Virtual Desktop Infrastructure) services.

Configure a Citrix remote connection with the connection wizard. If the default values do not meet your requirements, use the extended options to complete the connection setup process.

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:

- Latest version at the time of release:
 - 12.1.5 for x86
 - 12.5 for ARM/SoC
- Window size and depth settings
- Seamless window support
- Sound quality settings
 - Low
 - Medium
 - High
 - Disabled
- Static drive mapping
- Dynamic drive mapping
- USB redirection for XenDesktop and VDI-in-a-Box
- 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 20](#) for more information.

- HDX Flash Redirection (x86-only)
- HDX Webcam Compression
- HDX RealTime (MS Lync Optimization) (x86-only)

HDX MediaStream support matrix

Table 4-10 HDX MediaStream support matrix

Feature	Support
Frame rate	<ul style="list-style-type: none"> • 24 fps
Resolution	<ul style="list-style-type: none"> • 1080p • 720p
Video containers	<ul style="list-style-type: none"> • WMV • AVI • MPG • MPEG

Table 4-10 HDX MediaStream support matrix (continued)

Feature	Support
	<ul style="list-style-type: none"> • MOV • MP4
Video codecs	<ul style="list-style-type: none"> • WMV2 • WMV3 / VC-1 • H.264 / AVC / MPEG-4 Part 10 • MPEG-4 Part 2 • H.263 • DivX • Xvid • MPEG1
Audio codecs	<ul style="list-style-type: none"> • MP3 • WMA • AAC • PCM • mpeg-audio • MLAW / ULAW

Citrix connection support matrix

The following table describes the supported Citrix backends.

Table 4-11 Citrix connection support matrix

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



Overview of VMware Horizon View connection features

Using Kiosk Mode with VMware Horizon View


In Kiosk Mode, the client performs an automatic login to a remote desktop using predefined user credentials at startup. If you lose a connection because of a logout, disconnect, or network failure, the connection automatically restores when connectivity returns.

To minimize the session and return to the login screen, use the keyboard shortcut **Ctrl+Alt+End**.

To set up a Kiosk Mode login:

1. As the administrator, click  and select **Edit Connection Settings**.
2. Under **Network**, specify the following settings:
 - Username
 - Password
 - Domain
 - Desktop (If applicable)
3. Click **OK**.
4. Click  and select **Advanced Configuration > Advanced > XTerminal**.
 - a. On the X Terminal command prompt, type `regeditor` and press **Return**.
 - b. In the client registry, set the value as follows:

Value	Entry
Connection Type/view/connections/UUID/autostart	1
Connection Type/view/connections/UUID/autoreconnect registry	1

 **IMPORTANT:** Be sure to click **Save** after each entry.

5. When completed, click **Quit**.
6. Reboot the system.

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 15](#).

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. To switch sessions, the top bar can be enabled by unchecking **Hide top menu bar** in the **General** tab of the **Connection Settings** 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 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 16](#).

 **NOTE:** For information on configuring USB redirection for versions of HP Smart Zero Core that do not use the USB Manager, see [USB options in previous HP Smart Zero Core releases on page 90](#).

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:

- ▲ Disable USBR by using the USB Manager to set the **Remote Protocol** to **Local**.

This creates a network-mapped drive in the virtual desktop session for each internal and external mass storage device connected to the client. The file system format of the storage being remoted does not matter. For example, an ext3-formatted USB key can be used on a Windows connection.

For more details, see [Using mass storage redirection with RDP on page 17](#).

Using printer redirection with VMware Horizon View


For connections made with the PCoIP protocol, USBR supports printers. For connections made with the RDP protocol, see [Using printer redirection with RDP on page 17](#) 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 does not support high level audio-record redirection via the PCoIP connection type. If you need audio-recording support, use one of the following methods:


- If you are using the Teradici PCoIP Client on the t410 system, install the Teradici audio driver from <http://techsupport.teradici.com> on the virtual desktop. This allows high-level audio redirection through either the 3.5 mm jack or a USB headset.

 **NOTE:** Only systems with Teradici PCoIP Client 1.2 or higher support high-level audio redirection using a USB headset. Systems with older versions of the client will redirect the headset through USBR.

- 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 client 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, 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 does 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. In the **Connection Settings** dialog box, under **General**, select **Allow smartcard login**.

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 18](#) 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 does not support high-level webcam redirection. Webcams can be used only if they are redirected using USBR. The webcam might perform poorly or not at all. See [Using USB redirection with RDP on page 16](#) for more information.

Additional VMware Horizon View connection options

To access additional VMware Horizon View connection options in the client, select **Edit Connection Settings > General** in the VMware Horizon View Connection Manager.

The following table describes the general login options in the VMware Horizon View Connection Manager.

Table 4-12 Login options

Option	Description
Automatic Login	<p>Select Automatic Login to make sure that the client uses the following credentials when signing into the broker:</p> <ul style="list-style-type: none">• hostname• username• password <p>If you check the Automatic Login box, this information will fill in the correct fields when the VMware Horizon View client starts. However, to initiate the connection, you need to click Connect.</p> <p>NOTE: HP recommends selecting the Automatic Login box.</p>
Allow Smartcard login	<p>Select Allow Smartcard login to enable smart card login.</p> <p>NOTE: For more information on smart cards, see Using smart card redirection with VMware Horizon View on page 24.</p>
Close After Disconnect	<p>To exit the VMware Horizon View client after users log out of their desktops or the session terminates with an error, select Close After Disconnect.</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>The Close After Disconnect option is enabled by default for security purposes, but may be changed 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>To make the top menu bar invisible for users, select Hide top menu bar.</p> <p>This option enabled by default. You may 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 Connection Security Level to adjust the security level that the VMware Horizon View client uses when connecting to the server.</p> <p>NOTE: For more information, see VMware Horizon View HTTPS and certificate management requirements on page 27 for details on how connection security levels behave.</p>


Using advanced command line arguments with VMware Horizon View

To use advanced command line arguments:

1. In the VMware Horizon View Connection Manager, navigate to **Edit Connection Settings > General**.
2. Under **Command Line Arguments**, enter arguments that pass to the VMware Horizon View client when it starts.


For more help on using advanced command line options, do one of the following:


- On the command line, type `vmware-view--help` and then press [Enter](#).
- See the Linux Horizon View client documentation provided by VMware at <http://www.vmware.com>.

 **NOTE:** The information in this section does not apply to the Teradici-accelerated PCoIP client.

Using a Teradici-accelerated t410 system with VMware Horizon View

A Teradici-accelerated t410 system uses a Teradici PCoIP client to connect to the VMware Horizon View desktop. To verify whether your system is Teradici-accelerated, look for the **teradici-pcoip-client** label listed in the **System Information** pane.

 **NOTE:** Teradici-accelerated units cannot use the RDP protocol to connect with a remote desktop session.


 **NOTE:** The Teradici PCoIP client does not support forwarding traffic via an HTTP proxy. You will need to switch to the standard VMware Horizon View client to connect through a proxy. See [Switching to the standard VMware Horizon View client on page 26](#) for more information.

Switching to the standard VMware Horizon View client

To switch to the standard VMware Horizon View client:

1. Open an Xterminal and run the following command:

```
mv /usr/bin/teradici_signature_check /usr/bin/teradici_signature_check.bak
```


 **IMPORTANT:** The command should be typed on a single line, with a single space before each file path.

2. Restart the client.

To switch back to the Teradici PCoIP-optimized client:

1. Open an Xterminal and run the following command:

```
mv /usr/bin/teradici_signature_check.bak /usr/bin/teradici_signature_check
```

 **IMPORTANT:** The command should be typed on a single line, with a single space before each file path.

2. Restart the client.


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. To access the **Experience** options, use the **Connection Settings** dialog box.


For more details on specific options for RDP connections, see [Setting RDP options on page 18](#).

Installing certificates on clients

Use the Certificate Manager when installing a Certificate Authority (CA) certificate. 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 HP Smart Zero Client Services to attach the certificate to a profile, as described in [Adding certificates to a client profile on page 38](#).

 **NOTE:** For more information, see <http://linux.die.net/man/1/x509>.

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

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:

- In Administrator Mode, access the client control panel and select **Additional Configuration > Advanced > Certificates** to open the Certificate Manager. Then, import the certificate from a file or URL.
- Use a remote profile update to import a certificate.
- In the VMware Horizon View Manager, select **Edit Connection Settings > General**. Set **Connection Security Level** to **Allow all Connections**, and then click **Apply**.


Table 4-13 VMware Horizon View certificate security levels

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


Table 4-14 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

Redirecting USB devices


1. In the client, log in as the Administrator.
2. Click  and select **Additional Configuration > Peripherals > USB Manager**.
3. Select one of the following remote protocols:
 - Citrix
 - RDP7
 - Local
 - VMware Horizon View
4. If the setting is **Local**, you can also specify the options **allow devices to be mounted** and **mount devices read-only**.
5. In the **USB Manager** screen, under **Devices**, view the devices connected the system.
6. To override the default redirection settings, select the devices that require modification.
7. For the selected devices, choose one of the following redirection options:
 - Default
 - Redirect
 - Do not Redirect
8. When completed, select **Apply**, and then click **OK**.

Mapping a serial or parallel printer


1. On the client toolbar, click .
2. Select **Additional Configuration > Printer Mapping**.
3. In the **Printer Mapping** screen, click **Add** to add a printer.
4. In the **HP Printer Creation** dialog box under **Port**, select one of the following options:
 - Parallel
 - Serial #1
 - Serial #2

 **NOTE:** Select **Serial #1** if you have only one serial printer.

5. Under **Model**, type the name and model number of your printer.

 **NOTE:** This is an optional step. However, HP recommends that you do this so that the printer name is displayed in the **Mapping** screen.

6. Under **Windows Driver**, type the name of the Windows printer driver for the printer.

 **NOTE:** This is an optional step. However, HP recommends that you install at least the Generic/Text Only Windows driver in order to use the printer on the server. Without a driver, Windows might not use the printer properly.

7. Select **Active** to activate the new printer.
8. To create the new printer, select **Create**.


When completed, the new printer will be displayed in the **HP Printer Creation** dialog box.

5 Troubleshooting clients

This chapter discusses the following topics:

- [Troubleshooting network connectivity](#)
- [Troubleshooting firmware corruption](#)
- [Troubleshooting serial or parallel printer configuration](#)
- [Troubleshooting Citrix password expiration](#)
- [Using system diagnostics to troubleshoot](#)

Troubleshooting network connectivity


1. Ping the client server by doing the following:
 - a. On the client toolbar, click  to access the **About this client** screen, 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 client 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. On the client toolbar, click  to access the **About this client** screen, 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 Zero 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 serial or parallel printer configuration

Before configuring printer ports, obtain the printer's baud rate from the printer's documentation. If you do not have that documentation, find the baud rate by completing the following:


1. Turn the printer on while pressing and holding the **Feed** button.
2. Release the **Feed** button after a few seconds. The printer will enter a self-test mode and print out 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.

 **NOTE:** Most serial printers will print a diagnostic page when you perform this operation. If your printer will not print the diagnostic page, see the printer's documentation.

To enter the printer's baud rate:

1. Using the **Profile Editor** under **Registry**, select **root/printer-mapping-mgr/{UUID}/BaudRate**.
2. Enter your printer's baud rate.

 **NOTE:** The UUID will match the UUID of the printer in **root/printer**. Look there and match the printer with the UUID in the **root/printer-mapping-mgr**.

3. Click **Save**.
4. Right-click the UUID, and then click **Apply Changes**.


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. On the client toolbar, click  to access the **About this client** screen, 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, type `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 5-1 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**.

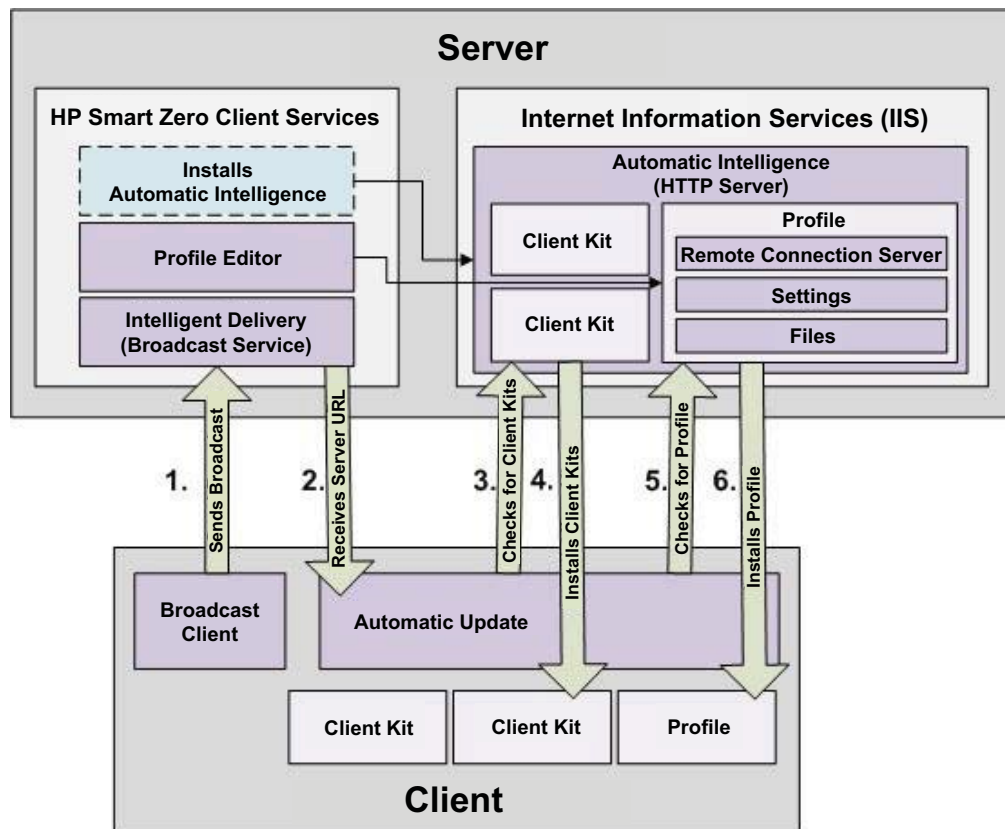
Viewing files in the /etc folder

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

6 HP Smart Zero Client Services

Clients will detect an update server automatically and configure themselves on the first boot. This simplifies device installation and maintenance.


The diagram below describes how the clients communicate with the server when receiving profiles and client update kits.



Supported operating systems

HP Smart Zero 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.

Preparing to install HP Smart Zero Client Services

Before installing HP Smart Zero 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>.

Downloading and installing HP Smart Zero Client Services

To download and install HP Smart Zero Client Services:

1. Go to <http://www.hp.com/support>.
2. Click **Drivers & Software**, type the name of your client model in the field, and then click **SEARCH**.
3. Click on your client model in the list of results.
4. Under **Select operating system**, click **HP Smart Zero Client**.
5. Under **Software - System Management**, locate **Smart Zero Client Services**, and then click the **Download** button.
6. Launch the installation wizard and follow the on-screen instructions to complete the installation.



NOTE: The installation wizard can also be used to add, modify, repair, and remove components of HP Smart Zero Client Services.

7 Using the Profile Editor

HP Smart Zero 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 Appendix C [HP Smart Zero Core registry settings on page 58](#) 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 Zero 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. 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 for HP Smart Zero Core 4.1.1 and later versions 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 Zero Client Services
- Web browser stores (if installed)

To import other certificates to a client profile for HP Smart Zero Core 4.1.1 or later versions:

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.

Installing Citrix certificates on HP Smart Zero Core 4.1.0 and earlier versions

HP Smart Zero Core 4.1.0 and earlier versions do not have the Certificate Manager add-on, and the only certificate store supported in the Profile Editor is the Citrix certificate store. Other stores require you to run client scripts after importing certificates. They also require a custom update.

Follow these steps to install a certificate used in a Citrix session:

1. In the **Additional Configuration Files** pane, click **Add a file**.
2. Click **Import File**, locate the certificate you want to import, 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/lib/ICAClient/keystore/cacerts/<cert>`
4. Click **Save** to finish adding the certificate to the client profile.

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 baud rate](#)
- [Setting up printer ports](#)
- [Installing printers on the server](#)

Obtaining the printer baud rate

Before configuring printer ports, obtain the printer's baud rate. 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—Navigate to **root > ConnectionType > xen > general** and set the **lastComPortNum** registry key to a value from 1–4, depending on the number of mapped printer ports 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**.
4. Set the **Baud** registry key to the baud rate of your serial or parallel printer.

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.

8 Using Automatic Intelligence

This section includes the following topics:

- [Viewing the Automatic Update website](#)
- [Creating an Automatic Update profile](#)
- [Updating clients](#)
- [Using HP Intelligent Delivery Service](#)
- [Using HP Device Manager](#)

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 36](#)) 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 Zero 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 clients on page 30](#).

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 8-1 Example DHCP tagging options

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

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

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

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

Using the DNS alias update method


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

To configure the DNS alias update method:

- ▲ Change the hostname of the server hosting HP Smart Zero 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. On the client toolbar, click .
2. Click **Administrator/User Mode Switch**.
3. In the **Administrator Password** box, type your password, and then click **OK**.
4. Complete the login process by clicking .
5. Select **Additional Configuration > Management > Automatic Update**.
6. In the **Automatic Update** dialog, configure the options as described in the following table.

Table 8-2 Automatic Update options

Field	Entry
Enable Manual Configuration	Select Enable Manual Configuration .
Manual Configuration > Protocol	Select http .
Manual Configuration > Server	Type the following update server hostname and port number: <code><host name>:18287</code>
Path	Type <code>auto-update</code> .

7. When completed, click **OK**. The client now pulls the automatic updates.

Using HP Intelligent Delivery Service

How HP Intelligent Delivery Service works

The Windows service listens for broadcasts from clients on a high-level output. When a broadcast is received, HP Intelligent Delivery Service responds with the URL of the Automatic Intelligence server, which the client uses to check for updates.

Starting, stopping, and pausing HP Intelligent Delivery Service

1. On the server desktop, select **Start > Administrative Tools > Server Manager**.
2. In the left pane of the **Server Manager**, expand **Configuration** and select **Services**.
3. In the center pane, under **Services**, double-click **HP Broadcast Server Service**, and then select **Properties**.
4. In the **HP Broadcast Server Properties** dialog box, under **Service Status**, select one of the following options:
 - **Start Service**
 - **Stop Service**
 - **Pause Service**

Viewing the HP Intelligent Delivery Service application log

1. On the server desktop, select **Start > Administrative Tools > Server Manager**.
2. In the left pane of the **Server Manager**, expand **Diagnostics > Event Viewer > Windows Logs > Application**.
3. The application log is displayed in the center pane under **HPSmartClientService**.

HP Intelligent Delivery Service registry keys

The registry keys used in the HP Intelligent Delivery Service are shown in the following table.

Table 8-3 HP Intelligent Delivery Service registry keys

Registry key	Path
Port	HKLM\SYSTEM\CurrentControlSet\Services\HP Broadcast Server
ServerURL	HKLM\SYSTEM\CurrentControlSet\Services\HP Broadcast Server

Using HP Device Manager

The HP Device Manager Agent runs in the background of the client. Use HP Device Manager to remotely select and manipulate clients' required business needs.

For more information on HP Device Manager, see the *HP Device Manager User Guide*.

A Client keyboard language

Use the **Profile Editor** to modify or set up keyboard languages. Change the registry entries as follows:

- /root/keyboard/model
- /root/keyboard/layout
- /root/keyboard/variant

Table A-1 Keyboard languages

Keyboard	Model	Layout	Variant
Belgium [Belgian French]	pc105	be	wincompat
Brazil [Brazilian Portuguese]	abnt2	br	wincompat
Bulgaria [Bulgarian]	pc105	bg	wincompat
Canada [Canadian French]	pc105	ca	wincompat
Croatia [Croatian]	pc105	hr	wincompat
Czech Republic [Czech]	pc105	cz	wincompat
Denmark [Danish]	pc105	dk	wincompat
Finland [Finnish]	pc105	fi	wincompat
France [French]	pc105	fr	wincompat
Germany [German]	pc105	de	wincompat
Hungary [Hungarian]	pc105	hu	wincompat
Italy [Italian]	pc105	it	wincompat
Japan [Japanese], with "¥" (RDP)	jp106	jp	jp106-hp-yen
Japan [Japanese], with "¥" (RGS)	jp106	jp	jp106-hp
Korea [Korean]	kr106	kr	wincompat
Latin America [Latin American]	pc105	latam	wincompat
Netherlands [Dutch]	pc105	nl	wincompat
Norway [Norwegian]	pc105	no	wincompat
Poland [Polish]	pc104	pl	wincompat
Portugal [Portuguese]	pc105	pt	wincompat
Romania [Romanian]	pc105	ro	wincompat
Russia [Russian]	pc104	ru	wincompat
Slovakia [Slovak]	pc105	sk	wincompat
Slovenia [Slovenian]	pc105	si	wincompat
Spain [Spanish]	pc105	sp	wincompat

Table A-1 Keyboard languages (continued)

Keyboard	Model	Layout	Variant
Sweden [Swedish]	pc105	se	wincompat
Switzerland [Swiss French]	pc105	ch	wincompat-fr_ch
Switzerland [Swiss German]	pc105	ch	wincompat-de_ch
Turkey [Turkish]	pc105	tr	wincompat
Ukraine [Ukrainian]	pc105	ua	wincompat
United Kingdom [English]	pc104	gb	wincompat
United States [English]	pc105	us	wincompat
United States [English], Dvorak	pc105	us	wincompat-dvorak
United States [English], International	pc105	us	wincompat-intl

B Customizing the client 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. Registry entries specify the directories in which these files are stored and can be modified to point to custom directories. For instance, the registry key **root/zero-login/styledir/view** points to the directory containing style elements for the login desktop for VMware Horizon View connections, which defaults to **/etc/hptc-zero-login/styles/view**.

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 B-1 Login Screen > Common Attributes > Name

Type	Description
Parameter	A string
Example	name: ItemName;

Table B-1 Login Screen > Common Attributes > Name (continued)

Type	Description
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 B-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 B-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 B-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 B-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 B-6 Login Screen > Common Attributes > position

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

Table B-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 B-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

Table B-8 Login Screen > Common Attributes > context (continued)

Type	Description
	protocol (if any), or on both. Only some protocols (for example, Citrix XenDesktop) have a desktop screen.

Elements

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

Type	Description
Use	Specifies the global background or padding values.
Common attributes recognized	name, color, padding <ul style="list-style-type: none"> color—specifies the solid background color of the screen, if no gradients are specified padding—specifies the default padding for all subsequent elements

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

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

Table B-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 B-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,

Table B-12 Login Screen > Elements > Custom > Axis (continued)

Type	Description
	the axis specifies whether the radius of the gradient is half-screen height or half-screen width.

Table B-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 ² +dy ² distance calculation (squared) or the square root of number (linear). Squared interpolation is somewhat quicker to draw.

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

Type	Description
Parameter	[true false]
Example	dithered: true;

Table B-15 Login Screen > Elements > Custom > dithered (continued)

Type	Description
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 B-16 Login screen > Image

Type	Description
Use	Specifies an image to overlay a portion of the background.
Common attributes recognized	name, size, alpha, position, alignment, context
Common attributes	See the tables following.

Table B-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 B-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 B-19 Login screen > Text

Type	Description
Use	Specifies a string of text to lay over the background

Table B-19 Login screen > Text (continued)

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

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

Type	Description
Parameter	Localized text
Example	text-de_DE: Dieser Text is in Deutsch.;
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"> • de_DE (German) • en_US (English) • es_ES (Spanish) • fr_FR (French) • ja_JP (Japanese) • zh_CN (Simplified Chinese) <p>NOTE: The file encoding is UTF-8.</p>

Table B-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>NOTE: The text rendering engine does not support HTML-style markup.</p>

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

Type	Description
Parameter	locale-specific fontName
Example	font-ja_JP: kochi-gothic;
Default	Not applicable
Use	When in the matching locale, this font will be used when the string is rendered. See the description for text-locale

Table B-22 Login screen > Text > font-locale (continued)

Type	Description
	previous. The name must match one of the fonts under <code>/usr/share/fonts/ truetype</code> . For Japanese text, it might be necessary to select kochi-gothic; for Simplified Chinese text, u mi ng.

Table B-23 Login screen > Text > font

Type	Description
Parameter	fontName
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 <code>/usr/share/fonts/truetype</code> .

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

Type	Description
Parameter	Size in pixels or in a percentage of screen height.
Example	max-height: 64;

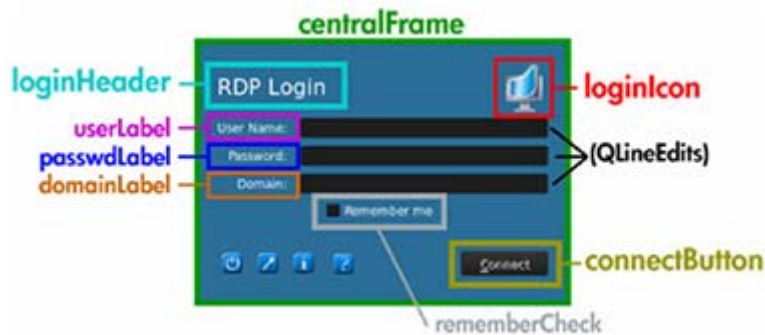
Table B-26 Login screen > Text > max-height (continued)

Type	Description
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.

Customizing the client login dialog box

This section provides examples that describe how to customize the client login dialog box.

Figure B-1 Components in the client login dialog box



The client login dialog box uses one directory per connection type plus a default style that specifies the style elements of the connection's background image and the login window style.

The registry entries specify the directories in which these files are stored and can be modified to point to custom directories. Within a style's directory, files with the `.qss` suffix customize the style elements of the login area.

The `*.qss` files are **Qt stylesheets**. For more information about Qt stylesheets, see <http://qt-project.org/>.

Most of the elements in the login area can be customized using `qss`-style elements. Each has been assigned an ID so they are easily addressable using the `#elementID` selector.

Customizing the central frame

This section provides an example of different ways to customize the central area of the login dialog box.

```
QFrame#centralFrame {
/* Sea green dialog
background-color */ background-color: rgb(46,139,87);
/* Rounded, thicker borders */
border-width: 6px;
border-radius:
16px;
/* Make sure it is at least 400 pixels wide */
```



```
min-width:  
400px; }
```

Customizing the text for the header

This section provides an example of different ways to customize the text in the login header.

```
LoginArea QLabel#loginHeader {  
/* Change the login text at the top */  
qproperty-text: "Login Here";  
color: white;  
font-size: 16pt;  
font-weight: bold;  
}
```



NOTE: Text that is overridden in the .qss file will not be localized when the locale changes.

Customizing the icon for the header

This section provides an example of different ways to customize the icon in the upper-right of the login header.


```
LoginArea QLabel#loginIcon {  
/* Substitute my company logo for the normal  
one. */ image: url  
(/writable/misc/MyCompanyLogo .png); min  
width: 48px;  
min-height: 48px;  
}
```

It can have a different style when it is not enabled:

```
QPushButton#connectButton:dis  
abled { /* Flat gray */  
background: rgb(204,204,204);  
border-radius: 3;  
color: rgb(102,102,102);  
font-size: 12pt;  
}
```

C HP Smart Zero Core registry settings

This section lists the HP Smart Zero Core registry settings for HP Smart Zero Core 4.3. The tables in this section describe the registry key paths, application functions, and options as presented in the Registry Editor component of the Profile Editor.

 **IMPORTANT:** The registry settings listed in this appendix are shared with the HP ThinPro operating system. Some of the settings that are listed might not apply to HP Smart Zero Core.

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

- [root > Audio](#)
- [root > ConnectionManager](#)
- [root > ConnectionType](#)
- [root > Display](#)
- [root > Network](#)
- [root > USB](#)
- [root > keyboard](#)
- [root > logging](#)
- [root > mouse](#)
- [root > printer-mapping-mgr](#)
- [root > printers](#)
- [root > screensaver](#)
- [root > time](#)
- [root > translation](#)
- [root > users](#)
- [root > zero-login](#)

root > Audio

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

Table C-1 root > Audio

Registry key	Valid values	Description
root/Audio/AdjustSoundPath	Not applicable	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/Device		

Table C-1 root > Audio (continued)

Registry key	Valid values	Description
root/Audio/OutputMute	1—Mute the internal speaker and headphone jack. 0—Do not mute the internal speaker and headphone jack.	Not applicable
root/Audio/OutputVolume	1–100	Indicates the volume setting for the internal speaker and headphone jack, scaling from 1 to 100.
root/Audio/PlaybackDevice	1 is the internal audio controller. 2 and 3 are for additional devices, such as a USB headset.	The device to use for playback.
root/Audio/RecordMute	1—Mute the microphone jack. 0—Do not mute the microphone jack.	Not applicable
root/Audio/RecordVolume	1–100	Indicates the volume setting for the microphone jack, scaling from 1 to 100.
root/Audio/VisibleInSystray	0—Icon is not visible 1—Icon is visible	Indicates whether a speaker icon is visible in the system tray.

root > ConnectionManager

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

Table C-2 root > ConnectionManager

Registry key	Valid values	Description
root/ConnectionManager/ customLogoPath		
root/ConnectionManager/ defaultConnection	[type]:[label]	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/ 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 Connect on the HP ThinPro control panel.
root/ConnectionManager/ useKioskMode		
root/ConnectionManager/ useSplashOnConnectionStartup	Set to '1' to enable the splash screen image specified by 'splashLogoPath' on connection startup.	By default, this is disabled on HP Smart Zero Core and enabled on HP ThinPro.

root > ConnectionType

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

root > ConnectionType > freerdp

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

Table C-3 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 HP ThinPro Control Center. Not applicable to HP Smart Zero Core. Set to 1 to allow, 0 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 HP ThinPro Control Center. Not applicable to HP Smart Zero Core. Set to 1 to allow, 0 to deny access.
root/ConnectionType/freerdp/connections/{UUID}/address	The IP or hostname of the remote host to connect to.
root/ConnectionType/freerdp/connections/{UUID}/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 1 to allow, 0 to deny access. NOTE: The connection can be edited in Administrator Mode even when this key is set to 0 .
root/ConnectionType/freerdp/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to modify the connection settings for this connection. Set to 1 to allow, 0 to deny access. NOTE: The connection can be edited in Administrator Mode even when this key is set to 0 .
root/ConnectionType/freerdp/connections/{UUID}/autoReconnect	When set to 1 , the connection will be restarted when it is closed or disconnected. This is frequently useful for kiosk style applications. When set to 0 , 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 0 will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to 1 .
root/ConnectionType/freerdp/connections/{UUID}/autostart	When set to 1 , 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 0 will cause the connection to start immediately upon boot. This setting takes effect only when 'autostart' is set to 1 .
root/ConnectionType/freerdp/connections/{UUID}/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 C-3 root > ConnectionType > freerdp (continued)

Registry key	Description
	NOTE: Reducing color depth to a level not supported by the video driver may cause screen corruption or launch failures.
root/ConnectionType/freerdp/connections/{UUID}/compression	If set to 1 , compression of RDP data between client and server will be enabled. Setting to '0' will disable compression. Compression is enabled by default.
root/ConnectionType/freerdp/connections/{UUID}/dependConnectionId	
root/ConnectionType/freerdp/connections/{UUID}/directory	
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 <code>root/ConnectionType/<type>/connections/</code> .
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}/hasDesktopIcon	If set to 1 , an icon for the connection will be shown on the desktop. Not applicable to HP Smart Zero Core.
root/ConnectionType/freerdp/connections/{UUID}/label	The name of the connection show in the HP ThinPro Control Center. On HP Smart Zero Core, this will typically be set to 'Default Connection' and does not show in the user interface.
root/ConnectionType/freerdp/connections/{UUID}/mouseMotionEvents	When set to 0 , 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 0 , 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 1 , allows desktop composition, such as translucent borders, if supported by the server. Turning it off may

Table C-3 root > ConnectionType > freerdp (continued)

Registry key	Description
	improve performance on low-bandwidth connections. Generally, this affects only RemoteFX.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagFontSmoothing	If set to 1 , 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 1 , disables cursor blinking, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoCursorShadow	If set to 1 , turns off mouse cursor shadows, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoMenuAnimations	If set to 1 , turns off menu animations, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoTheming	If set to 1 , turns off user interface themes, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWallpaper	If set to 1 , turns off the desktop wallpaper, which can improve performance on low-bandwidth RDP connections.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWindowDrag	If set to 1 , 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 3389 and will rarely need to be changed.
root/ConnectionType/freerdp/connections/{UUID}/portMapping	If set to 1 , 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 1 , the CUPS printer redirection plugin will be activated, causing all printers defined locally through CUPS to be redirected to the remote host.
root/ConnectionType/freerdp/connections/{UUID}/rdpEncryption	If set to 1 , standard RDP encryption will be used to encrypt all data between the client and server.
root/ConnectionType/freerdp/connections/{UUID}/remoteFx	Use RemoteFX, if available.
root/ConnectionType/freerdp/connections/{UUID}/seamlessWindow	If set to 1 , window decorations will be 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}/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. NOTE: 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 1 , 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	When set to the default Bring to this computer , sound will be redirected from the remote host to the client using a standard virtual channel. When set to Leave at remote computer , sound will be left at the remote host. This might be useful

Table C-3 root > ConnectionType > freerdp (continued)

Registry key	Description
	<p>when using a USB-redirected audio device. If set to any other value, audio will be disabled.</p> <p>HP recommends that sound be set to Bring to this computer because this will improve audio quality and ensure that any client audio redirected through other virtual channels such as MMR matches local audio settings.</p>
root/ConnectionType/freerdp/connections/{UUID}/startMode	If set to the default focus and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/freerdp/connections/{UUID}/timeoutError	The number of milliseconds to wait after losing connection with the server before presenting an error dialog box and closing the connection. Disabled if 0 .
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 0 .
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 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/freerdp/connections/{UUID}/xkbLayoutId	If not empty, provide an XKB layout ID to bypass the system keyboard. To access the list of available IDs, type 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 1 , 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.
root/Connection Type/freerdp/coreSettings/icon32Path	The internal application icon path for the 32x32 pixel icon for this application.
root/Connection Type/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.

Table C-3 root > ConnectionType > freerdp (continued)

Registry key	Description
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	The number of seconds to wait for an initial response from the RDP server before giving up.
root/Connection Type/freerdp/coreSettings/label	The name of the connection to display under the 'add' button on HP ThinPro and in the connection selection screen on HP Smart Zero Core.
root/ConnectionType/freerdp/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is close , which will send a standard kill signal to the process. When set to kill , the process specified by 'appName' will be forcefully killed. When set to custom , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process.
root/ConnectionType/freerdp/coreSettings/watchPid	If set to 1 , 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/enableMMR	If set to 1 , 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/sendHostname	If set to the default hostname , 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 mac , the MAC address of the first available network adapter will be sent instead of the hostname.

root > ConnectionType > view

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

Table C-4 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 HP ThinPro Control Center. Not applicable to HP Smart Zero Core. Set to 1 to allow, 0 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 HP ThinPro Control Center. Not applicable to HP Smart Zero Core. Set to 1 to allow access, 0 to deny access.
root/ConnectionType/view/connections/{UUID}/afterStartedCommand	The full path to a script or binary to run after the connection has been started.

Table C-4 root > ConnectionType > view (continued)

Registry key	Description
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}/applnMenu	
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 '1' to allow access, 0 to deny access. NOTE: The connection can be edited in Administrator Mode even when this key is set to '0' .
root/ConnectionType/view/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to 1 to allow access, 0 to deny access. NOTE: The connection can be edited in Administrator Mode even when this key is set to 0 .
root/ConnectionType/view/connections/{UUID}/automaticLogin	When enabled, the VMware Horizon View client will attempt to automatically login if all fields are provided. If this is not enabled, users will have to manually click Connect in the VMware Horizon View client to contact the VMware Horizon View server, log in, and select a desktop.
root/ConnectionType/view/connections/{UUID}/autoReconnect	If 1 , 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 0 will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to 1 .
root/ConnectionType/view/connections/{UUID}/autostart	If greater than 0 , 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/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}/colorDepth	

Table C-4 root > ConnectionType > view (continued)

Registry key	Description
root/ConnectionType/view/connections/{UUID}/coord	
root/ConnectionType/view/connections/{UUID}/dependConnectionId	
root/ConnectionType/view/connections/{UUID}/desktop	<p>If specified, the named desktop will automatically launch upon login.</p> <p>NOTE: By default, if there is only one desktop available, it will automatically launch without needing to be specified.</p>
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}/ExtraArgs	Extra arguments to the VMware Horizon View client can be specified here. Run 'view_client --help' or 'vmware-view --help' from a terminal to see all available arguments.
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 HP ThinPro desktop. Not applicable to HP Smart Zero Core.
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 on HP ThinPro and hidden on HP Smart Zero Core.
root/ConnectionType/view/connections/{UUID}/isInMenu	If set to 1 , the connection will appear in the HP ThinPro taskbar. Not applicable to HP Smart Zero Core.
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 HP ThinPro 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	

Table C-4 root > ConnectionType > view (continued)

Registry key	Description
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 focus 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 Refuse insecure connections , 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 Warn , 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 Allow all connections , the server certificate will not be verified and connections to any server will be allowed.
root/ConnectionType/view/connections/{UUID}/waitForNetwork	If set to 1 , the connection will not be launched until networking is available. This makes sure that, on a slow network, the connection does not launch before networking is available, causing a failure.
root/ConnectionType/view/connections/{UUID}/windowSizeHeight	Not applicable to HP Smart Zero Core.
root/ConnectionType/view/connections/{UUID}/windowSizePercentage	
root/ConnectionType/view/connections/{UUID}/windowSizeWidth	Not applicable to HP Smart Zero Core.
root/ConnectionType/view/connections/{UUID}/windowType	Not applicable to HP Smart Zero Core.
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.
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.

Table C-4 root > ConnectionType > view (continued)

Registry key	Description
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 of the connection to display under the 'add' button on HP ThinPro and in the connection selection screen on HP Smart Zero Core.
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 close , which will send a standard kill signal to the process. When set to kill , the process specified by 'appName' will be forcefully killed. When set to custom , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process gracefully.
root/ConnectionType/view/coreSettings/watchPid	If set to 1, 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, type 'rdesktop --help' from 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 > xen

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

Table C-5 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 HP ThinPro Control Center. Not applicable to HP Smart Zero Core. Set to 1 to allow, 0 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 HP ThinPro Control Center. Not applicable to HP Smart Zero Core. Set to 1 to allow, 0 to deny access.
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}/appInMenu	If set to 1 , all applications for this connection will be displayed in the taskbar menu.
root/ConnectionType/xen/connections/{UUID}/appOnDesktop	If set to 1 , 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 1 to allow, 0 to deny access. NOTE: The connection can be edited in Administrator Mode even when this key is set to 0 .
root/ConnectionType/xen/connections/{UUID}/authorizations/user/execution	Indicates whether the user has permission to execute the connection. Set to 1 to allow, 0 to deny access. NOTE: The connection will always be available to launch in Administrator Mode.
root/ConnectionType/xen/connections/{UUID}/autoReconnect	If set to 1 , the system will attempt to automatically restart the connection after it has been closed. If required, credentials should be supplied though the <code>zero-login/defaultCredentials</code> field. "autostart" is frequently used in conjunction with this setting.
root/ConnectionType/xen/connections/{UUID}/autoReconnectDelay	Indicates the amount of time in seconds to wait before restarting the connection. The default of 0 will cause the connection to restart immediately upon close or disconnect. This setting takes effect only when 'autoReconnect' is set to 1 .
root/ConnectionType/xen/connections/{UUID}/autostart	If greater than 0 , the system will attempt to automatically start the connection when the client is booted. If required, credentials should be supplied though 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 0 will cause the connection to start immediately upon boot. This setting takes effect only when 'autostart' is set to 1 .
root/ConnectionType/xen/connections/{UUID}/autoStartDesktop	To automatically start the first desktop available when you launch a Citrix connection, set the key value to 1 .

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
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}/beforeStartingCommand	The full path to a script or binary to run before the connection has started.
root/ConnectionType/xen/connections/{UUID}/clearCredentialsTimeout	
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 root/ConnectionType/<type>/connections/
root/ConnectionType/xen/connections/{UUID}/folder	
root/ConnectionType/xen/connections/{UUID}/fullscreen	When set to 1 , the ICA client will be started in full-screen mode.
root/ConnectionType/xen/connections/{UUID}/hasDesktopIcon	If set to 1 , an icon for the connection will be shown on the desktop. Not applicable to HP Smart Zero Core.
root/ConnectionType/xen/connections/{UUID}/isInMenu	
root/ConnectionType/xen/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 HP ThinPro 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.

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/connections/{UUID}/savePassword	
root/ConnectionType/xen/connections/{UUID}/startMode	If set to the default focus 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}/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 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/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/autoLogoutDelay	This setting applies to Citrix servers with multiple published apps or desktops. If less than 0 , 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 less than 0 , 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.
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 of the connection to display under the 'add' button on HP ThinPro and in the connection selection screen on HP Smart Zero Core.
root/ConnectionType/xen/coreSettings/serverRequired	Tells whether a server name or address is unused, optional, or required for this connection type.

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/coreSettings/stopProcess	The behavior that should occur when 'connection-mgr stop' is called on this connection. By default, this is close , which will send a standard kill signal to the process. When set to kill , the process specified by 'appName' will be forcefully killed. When set to custom , a custom execution script specified by 'wrapperScript' will be executed with argument 'stop' to terminate the process.
root/ConnectionType/xen/coreSettings/watchPid	If set to 1 , 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/allowReadOn{AthruZ}	Set to 1 to allow the user to read the mapped drive from the remote host. If this is set to 0 , no files will show up in the mapped drive on the remote host.
root/ConnectionType/xen/general/allowWriteOn{AthruZ}	Set to 1 to allow the user to write to the mapped drive from the remote host. If this is set to 0 , 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 0 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 0 . NOTE: 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 minimum size of bitmap for caching. The default is 8192 . On all clients, this is set to a default of 2048 .
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 Shared - Approximate Colors to enable and Private - Exact Colors 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 False .
root/ConnectionType/xen/general/defaultBrowserProtocol	Set to TCP/IP HTTP Browser by default. Can be set to SSL/TLS HTTPS Browser or TCP/IP Browser . Maps to the Citrix INI file setting <code>BrowserProtocol=[UDP HTTPonTCP]</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 wfclient.ini is used.

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/general/ drivePathMappedOn{AthruZ}	The local filesystem directory to map to the remote host. Typically, this is set to /media to allow all connected USB drives to be mapped to the remote host through a single drive letter.
root/ConnectionType/xen/general/enableAlertSound	Set to the default 1 to enable Windows alert sounds. Set to 0 to disable. Indirectly maps to the Citrix INI file setting <code>DisableSound=boolean</code> , which disables Windows alert sounds. The default is False .
root/ConnectionType/xen/general/enableAudioInput	Set to the default 1 to enable audio input. This will set both the 'AllowAudioInput' and 'EnableAudioInput' settings to 1 in the <code>wfclient.ini</code> and <code>appsrv.ini</code> .
root/ConnectionType/xen/general/enableDataCompression	Set to the default 1 to enable data compression, or set to 0 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, /media would be mapped to Z 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/enableForceDirectConnect	Set to 1 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.
root/ConnectionType/xen/general/ enableHDXFlashRedirection	Control the behavior of HDX Flash Redirection by setting it to Always , Ask , or Never . 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/enableHDXMediaStream	Set to 0 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{AthruZ}	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 On .
root/ConnectionType/xen/general/enableSmartCard	If set to 1 , 'DisableCtrlAltDel' will be set to 'Off' and smart card login will be enabled. If set to 0 , '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

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
	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/hotKey{1 thru 12}Char	The hotkey character to forward to the remote session. For example, F1 for hotKey1Char.
root/ConnectionType/xen/general/hotKey{1 thru 12}Shift	The key shift state combination used to activate the chosen hotkey character. Defaults to Ctrl+Shift . Can be set to Shift , Ctrl , Alt , Alt+Shift , Alt+Ctrl , or Ctrl+Shift .
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 F2 . All clients are set to F1 by default.
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 Ctrl . All clients are set to Alt by default.
root/ConnectionType/xen/general/localTextEcho	Can be set to On , Off , or the default Auto . 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/mouseClickFeedback	Can be set to On , Off , or the default Auto . 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 False . All clients are set to 0 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 0 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.

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
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/seamlessWindow	Directly maps to the Citrix INI file setting <code>TWIMode=boolean</code> , which controls seamless mode for published applications. All clients are set to 1 by default.
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 False . All clients are set to 1 by default.
root/ConnectionType/xen/general/sound	Can be set to the default High Quality , Med Quality , Low Quality , or Disabled . 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 Translated (Local), Direct in full screen desktops only (FullScreenOnly), or Direct (Remote). 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 FullScreenOnly .
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 False . All clients are set to 0 by default.
root/ConnectionType/xen/general/useBitmapCache	Directly maps to the Citrix INI file setting <code>PersistentCacheEnabled=boolean</code> . The default is False . All clients are set to 0 by default.
root/ConnectionType/xen/general/useEUKS	Controls use of Extended Unicode Keyboard Support on Windows servers. The default is 0 . 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

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
	method to interpret keyboard input. This is supported only for European languages. The default is True . All clients are set to 1 by default.
root/ConnectionType/xen/general/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/xen/general/windowHeight	If 'windowSize' is set to Fixed Size , this key will be used to set the height of the window in pixels.
root/ConnectionType/xen/general/windowPercent	If 'windowType' is set to Percentage of Screen Size , 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 Full Screen (the default), the connection will be maximized without borders on all available screens. When set to Percentage of Screen Size the 'windowSizePercentage' key can be used to specify the size of the window as a percentage as the total screen area. When set to Fixed Size 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 1 and "seamlessWindow" has to be set to 0 . NOTE: 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/fbpanel/autohide	Whether to autohide the taskbar. Set to 'true' to autohide 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 1 to completely hide the taskbar. Can be hidden only if autoStartResource or autoStartDesktop is enabled.
root/ConnectionType/xen/gui/XenDesktopPanel/disabled	Set to 1 to disable the Xen Desktop Panel and its taskbar. Usually, set to 1 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	

Table C-5 root > ConnectionType > xen (continued)

Registry key	Description
root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect	
root/ConnectionType/xen/gui/XenManager/widgets/autostart	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource	
root/ConnectionType/xen/gui/XenManager/widgets/domain	
root/ConnectionType/xen/gui/XenManager/widgets/enablePNADesktopIcons	
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/username	
root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork	

root > Display

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

Table C-6 root > Display

Registry key	Description
root/Display/Configuration/displaymode	Specifies the display mode of the unit. A value of 0 denotes standard mode (1–4 monitors), whereas a value of 1 denotes a 6-monitor mode. The HP t610 with the appropriate add-on card is the only supported hardware.
root/Display/Configuration/primaryprofile	This must always be set to default .
root/Display/Configuration/secondarymode	If supported, specifies the position of the secondary monitor relative to the primary monitor. 0 —Same As 1 —Above

Table C-6 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>NOTE: This is hardware-dependent and is not supported on all models. The HP t5535z does not support two monitors.</p>
root/Display/Configuration/swapstate	Specifies which connector contains the primary monitor. This is hardware-dependent and might not be implemented on all models. Generally, 0 means the primary monitor is on the VGA connector and 1 means the 'other' connector. For the HP t5565z, 0 means the primary is on the DVI-I connector and 1 means the primary is on the DVI-D connector. The HP t5335z does not support two monitors.
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 ffffff 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 width. A value of 0 means auto-detect the resolution.
root/Display/Profiles/{UUID}/label	Display profile name. This should be default .
root/Display/Profiles/{UUID}/orientation	Specifies monitor orientation: <p>0—Normal</p> <p>1—Rotate left</p> <p>2—Rotate right</p> <p>3—Invert</p>
root/Display/Profiles/{UUID}/refresh	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 0 means auto-detect the refresh rate. <p>IMPORTANT: 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 0.</p>
root/Display/Profiles/{UUID}/width	The desired monitor resolution width. A value of ' 0 ' means auto-detect the resolution.

root > Network

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

Table C-7 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 five IPv4 or IPv6 addresses may be specified, separated by commas.
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/iPeak/Status	If set to 1 , HP Velocity will be enabled. This technology adds redundancy to TCP packets in an attempt to correct network loss issues. Even when enabled, it should not affect network packet transmission if the server-side component is not detected.
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 PSK to use a pre-shared key and Certificate 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.
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.

Table C-7 root > Network (continued)

Registry key	Description
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 1 the rule will be enabled. Set to 0 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/Wired/DefaultGateway	The default gateway the device will use to communicate to the internet. Typically, this is the address of the router. NOTE: This setting will take effect only when 'Method' is set to 'Static'.
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/Interface	The default ethernet interface or NIC.

Table C-7 root > Network (continued)

Registry key	Description
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/Method	When set to Automatic , 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/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/Password	Password.
root/Network/Wired/Security/PEAPVersion	PEAP version.
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/Interface	The default wireless interface or wireless network adapter.
root/Network/Wireless/IPAddress	The IPv4 address of the device. This setting will take effect only when 'Method' is set to 'Static'.
root/Network/Wireless/IPv6Enable	Set this key to 1 when working in an IPv6 environment.
root/Network/Wireless/Method	When set to Automatic , 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/Security/CACert	Path to the CA certification file.
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/Password	Password.

Table C-7 root > Network (continued)

Registry key	Description
root/Network/Wireless/Security/PEAPVersion	PEAP version.
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/WEPIIndex	WEP password index, only for use in WEP.
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/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 > USB

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

Table C-8 root > USB

Registry key	Description
root/USB/root/mass-storage/allowed	If set to 1, mass storage devices will be auto-mounted when the protocol is "local".
root/USB/root/mass-storage/read-only	If set to 1, when mass storage devices are auto-mounted locally, they will be mounted read-only.
root/USB/root/protocol	Keeps track of the current owner of the remote USB. Used internally only.

root > keyboard

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

Table C-9 root > keyboard

Registry key	Description
root/keyboard/enable2	If set to 1, 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.

Table C-9 root > keyboard (continued)

Registry key	Description
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 1 , 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 grp:ctrl_shift_toggle , grp:ctrl_alt_toggle , and grp:alt_shift_toggle .
root/keyboard/variant	The keyboard variant defines slight variations in the layout. Typically, the wincompat variation is used, as it most closely matches Windows keyboard layouts.
root/keyboard/variant2	The secondary keyboard variant.
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 > logging

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

Table C-10 root > logging

Registry key	Description
root/logging/general/debug	If set to 1 , 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 C-11 root > mouse

Registry key	Description
root/mouse/MouseHandedness	Whether the mouse is right-handed or left-handed. 0 for right-handed, 1 for left-handed.

Table C-11 root > mouse (continued)

Registry key	Description
root/mouse/MouseSpeed	The acceleration of the mouse pointer. Typically a number from 0–25 is in the usable range. 0 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. 0 will set the acceleration to a natural curve that gradually scales acceleration, allowing for both precise and quick movements.

root > printer-mapping-mgr

This section describes the registry keys, functions, options, and description in the **root > printer-mapping-mgr** folder.

Table C-12 root > printer-mapping-mgr

Registry key	Description
root/printer-mapping-mgr/{UUID}/BaudRate	For serial printers, this defines the baud rate of the printer. By default, this will be set to 9600 .
root/printer-mapping-mgr/{UUID}/Port	An internal key used to identify the port, usually set to the same as <code>root/printers/{UUID}/Port</code> .

root > printers

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

Table C-13 root > printers

Registry key	Description
root/printers/{UUID}/Active	If set to 1, the printer will be marked active and can be redirected to remote sessions.
root/printers/{UUID}/Port	The port for the printer. For a local printer, this will frequently be <code>/dev/ttyS0</code> , <code>/dev/lp0</code> , or <code>/dev/ttyUSB0</code> . If a network printer is defined, this will be set to Network , and a 'ServerIP' key will be defined with the IP address of the printer.
root/printers/{UUID}/PrinterMDL	Set to the printer model. This is a text field used to identify the printer in local and remote sessions.
root/printers/{UUID}/WindowsDriver	Set to the exact Windows Driver model. This is used by RDP and Citrix printer mapping to identify which printer driver to install on the remote host.

root > screensaver

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

Table C-14 root > screensaver

Registry key	Description
root/screensaver/enableDPMS	Set to 0 to disable monitor power management. This will cause the monitor to stay on unless turned off manually.
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 > time

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

Table C-15 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/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 'tcode' 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 > translation

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

Table C-16 root > translation

Registry key	Description
root/translation/coreSettings/localeMapping/{ language }	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:

Table C-16 root > translation (continued)

Registry key	Description
	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	

root > users

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

Table C-17 root > users

Registry key	Description
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/apps/hptc-auto-update/authorized	If set to 0 , 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-cert-mgr/authorized	If set to 0 , 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-color-temp/t410aio/authorized	If set to 0 , users will not be able to modify the screen color temperature.
root/users/user/apps/hptc-date-mgr/authorized	If set to 0 , 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-display-prefs/authorized	If set to 0 , users will not be able to modify the screen resolution, bit depth, or refresh rate.
root/users/user/apps/hptc-display-prefs/t410aio/authorized	If set to 0 users will not be able to modify the screen resolution, bit depth or refresh rate.
root/users/user/apps/hptc-i18n-mgr/authorized	If set to 1 , the locales control panel item will be enabled for users. This is normally disabled because it has a direct control available from <code>root/zero-login/controls</code> .
root/users/user/apps/hptc-keyboard-layout/authorized	If set to 1 , the full keyboard layout control panel item will be enabled for users. This is normally disabled because it has a direct control available from <code>root/zero-login/controls</code> .

Table C-17 root > users (continued)

Registry key	Description
root/users/user/apps/hptc-mixer/authorized	If set to 0 , the full-size mixer control panel will be disabled for users. It is usually redundant, as the mini control covers the same functions. To fully disable volume control, <code>root/zero-login/controls/audio/authorized</code> must also be set to 0 .
root/users/user/apps/hptc-mouse/authorized	If set to 0 , 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 0 , 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-mapping-mgr/authorized	If set to 0 , 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-printer-mgr/authorized	If set to 0 , users will not be able to set Windows driver values for CUPS 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-profile-mgr/authorized	If set to 0 , users will not be able factory reset the client. The only way to factory-reset a device if this control is disabled is to update the client with a new configuration that has this control enabled or to restore the factory image via USB key.
root/users/user/apps/hptc-root-xterm/authorized	If set to 1 , a root X terminal control panel item will be enabled for users. CAUTION: Enabling root terminal access is a security risk and is 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/hptc-shortcut-mgr/authorized	If set to 1 , the shortcut manager item will be enabled for users.
root/users/user/apps/hptc-switch-admin/authorized	If set to 1 , the Admin/User mode Switch will be enabled for users.
root/users/user/apps/hptc-vncshadow/authorized	If set to 1 , the VNC Shadowing control panel item will be enabled for users.
root/users/user/apps/scim-setup/authorized	If set to 1 , the SCIM (Input Method) control panel item will be enabled for users NOTE: SCIM is used for local Asian language input and might not be present on the system without the installation of an Asian language kit.
root/users/user/AutoBrightEnabled	Set to 1 to enable automatic brightness configuration on the HP t410 All-in-one when in 'Power over Ethernet' mode. This feature attempts to lower the brightness when power usage goes above a critical threshold to prevent the Ethernet switch from shutting off power to the unit.
root/users/user/MaxPowerDetectEnabled	Set to 1 to enable the maximum power detection algorithm on the HP t410 All-in-one when in 'Power over Ethernet' mode. This feature attempts to determine the actual maximum power that can be drawn from the Ethernet switch. Shorter Ethernet cables translate to higher maximum power.

Table C-17 root > users (continued)

Registry key	Description
root/users/user/OnDemandCPUThrottleEnabled	Set to 1 to enable on-demand CPU throttling on the HP t410 All-in-one when in 'Power over Ethernet' mode. This feature lowers the CPU frequency when power usage goes above a critical threshold to prevent the Ethernet switch from shutting off power to the unit.
root/users/user/WOLEnabled	Set to 0 to disable Wake On LAN.

root > zero-login

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

Table C-18 root > zero-login

Registry key	Description
root/zerologin/buttons/configure/authorized	Enables or disables the configuration menu. If set to 0 , users will not be able to configure any device settings.
root/zero-login/buttons/info/authorized	Enables or disables the system information panel. If set to 0 , users will not be able to view any information about the system.
root/zerologin/buttons/shutdown/authorized	Enables or disables the shutdown button on the login screen. If set to 0 , users will only be able to power off the device by pressing the power button directly.
root/zero-login/controls/audio/authorized	If set to 0 , users will be unable to change the sound output volume. This might be useful in an environment that should have all sound muted or set to a specific volume. To fully prevent users from changing sound output levels, be sure <code>root/users/user/apps/hptc-mixer/authorizations</code> is also set to 0 .
root/zerologin/controls/connection/authorized	If set to 0 , users will be unable to redefine the connection type. This is disabled by default because it is normally undesirable to allow users to change the connection type in a production environment.
root/zero-login/controls/i18n/authorized	If set to 0 , users will be unable to change the locale. This is useful in a single language environment.
root/zero-login/controls/keyboard/authorized	If set to 0 , users will be unable to change the keyboard layout. This is useful in a single language environment.
root/zero-login/defaultCredentials/domain	If set, this domain name will be supplied as the default to the login dialog if no alternative has been saved through "RememberMe". This is useful in environments where a single domain name is dominantly used.
root/zero-login/defaultCredentials/domainList	Colon-separated list of domains; for example, <code>domain1:domain2:(...)</code> . These domains are made available in a menu on the login screen. A particular domain can be preselected by setting it in the <code>root/zero-login/defaultCredentials/domain</code> registry key.
root/zerologin/defaultCredentials/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 auto-start connections.

Table C-18 root > zero-login (continued)

Registry key	Description
root/zerologin/defaultCredentials/readOnly	If set to 1 , login username, password, and domain will be read-only fields. This is only useful for connections that auto-start and auto-reconnect.
root/zerologin/defaultCredentials /rememberMe	If set to 1 , the username and domain used for a connection will be preserved as defaults for the next time the login dialog appears. For most connection types, the user can toggle this value with the "Remember Me" checkbox.
root/zerologin/defaultCredentials /smartcard	Supplied as the default to the login dialog if the user and domain match their defaults here. Typically, used with autostart connections.
root/zerologin/defaultCredentials /username	If set, this username will be supplied as the default to the login dialog if no alternative has been saved through "RememberMe". Typically, used with autostart connections.
root/zero-login/styledir/default	The directory in which the default style (.qss) and background (.rtf) files reside.
root/zero-login/styledir/rdesktop	The directory in which the default style (.qss) and background (.rtf) files reside for use with rdesktop connections.
root/zero-login/styledir/view	The directory in which the default style (.qss) and background (.rtf) files reside for use with VMware Horizon View connections.
root/zero-login/styledir/xen	The directory in which the default style (.qss) and background (.rtf) files reside for use with Citrix XenDesktop connections.

D VMware Horizon View USB configuration

This appendix includes the following topics:

- [USB options in previous HP Smart Zero Core releases](#)
- [VMware Horizon View USB device families](#)

USB options in previous HP Smart Zero Core releases

To disable USBR on audio devices:


1. In the client registry, modify the entry `/etc/vmware/config`.
2. Add the following line:


```
viewusb.ExcludeFamily = "audio-in;audio-out;"
```

To exclude or include a particular device:

1. Obtain that device's VID and PID.
2. In the client registry, modify the entry `/etc/vmware/config`.
3. Add the appropriate line:

- `Viewusb.ExcludeVidPid = "vid-0f0_pid-0001;vid-**21_pid-*8*a;"`
- `Viewusb.IncludeVidPid = "vid-003a_pid-1234"`

 **NOTE:** The information in this section does not apply to a Teradici-accelerated t410 unit. To control USBR on that unit, upgrade to HP Smart Zero Core 4.3 or higher, which includes a built-in USB Manager GUI.

 **NOTE:** For more information on VMware Horizon View USB configuration, see *Using VMware Horizon View Client for Linux* at <http://www.vmware.com>.

VMware Horizon View USB device families

Table D-1 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

Table D-1 VMware Horizon View USB device families (continued)

Family	Family name
Force Feedback Device	physical
Imaging	imaging
Printer	printer
Mass Storage	storage
Smartcard Reader	smart-card
Security	security
Video	video
Wireless Adapter	wireless
Bluetooth	bluetooth
Wireless USB	wusb
PDA	Pda

Index

A

- Administrator Mode
 - control panel, using 11
 - switching to User Mode 11
- audio redirection
 - RDP 18
 - VMware Horizon View 23
- Automatic Intelligence
 - using 42

C

- certificates
 - installing 27
 - VMware Horizon View 27
- Citrix
 - HDX MediaStream 20
 - overview 19
 - support matrix 21
- client control panel
 - accessing 9
 - using in Administrator Mode 11
 - using in User Mode 9
- client information screens
 - hiding 7
 - using 5
- client login screen
 - customizing 48
- client profile
 - adding files 38
 - adding symbolic link 39
 - certificates 38
 - loading 36
 - modifying 36
 - registry settings 37
 - saving 39
- client toolbar
 - using 4
- clients
 - configuring 9
 - keyboard language 46
 - navigating 4

- troubleshooting 30
- updating. *See* updating clients
- connections
 - configuring 2
 - default types 2
 - edit default 11
 - selecting 2, 9

D

- desktop
 - shortcuts 3
 - using 3
- device redirection
 - RDP 16
 - VMware Horizon View 23

G

- getting started 2

H

- HDX MediaStream 20
- HP Device Manager 45
- HP Intelligent Delivery Service 45
- HP Smart Zero Client Services
 - installing 35
 - overview 34
 - Profile Editor. *See* Profile Editor
 - supported operating systems 34

K

- Kiosk Mode
 - RDP 15
 - VMware Horizon View 21

M

- mass storage redirection
 - RDP 17
 - VMware Horizon View 23
- MMR
 - RDP 15
 - VMware Horizon View 22
- Multimedia Redirection. *See* MMR

P

- parallel printer configuration 39
- printer configuration 39
- printer mapping 29
- printer redirection
 - RDP 17
 - VMware Horizon View 23

- Profile Editor
 - using 36

R

- RDP
 - audio redirection 18
 - device redirection 16
 - experience options 18
 - Kiosk Mode 15
 - mass storage redirection 17
 - MMR 15
 - multi-monitor sessions 16
 - overview 14
 - printer redirection 17
 - RFX 15
 - smart card redirection 18
 - USB redirection 16
- registry settings 58
- RemoteFX. *See* RFX
- RFX 15

S

- serial printer configuration 39
- settings, administrator
 - audio 11
 - automatic update 13
 - certificates 14
 - date and time 13
 - display preferences 12
 - factory reset 13
 - keyboard layout 12
 - keyboard shortcuts 14
 - language 13
 - mouse 12
 - network 13
 - printer mapping 12
 - security 13
 - sound 13
 - task manager 14
 - text editor 14
 - USB 13
 - Xterminal 14
- settings, user
 - audio 10
 - date and time 10
 - display preferences 10
 - keyboard layout 10
 - language 10
 - mouse 10

- network 10
- printer mapping 11
- settings, VNC shadowing
 - factory reset 13
- smart card redirection
 - RDP 18
 - VMware Horizon View 24
- system diagnostics 32
- system status icon 4

- Teradici-accelerated 26
- USB configuration 90
- USB redirection 23
- webcam redirection 24
- VNC shadowing 13

W

- webcam redirection
 - VMware Horizon View 24

T

- troubleshooting
 - firmware corruption 31
 - network connectivity 30
 - printer configuration 31
 - using system diagnostics 32

U

- updating clients
 - broadcast update 43
 - DHCP tagging update 43
 - DNS alias update 44
 - manual update 44
- USB redirection
 - RDP 16
 - USB Manager 28
 - VMware Horizon View 23
- User Mode
 - control panel, using 9
 - switching to Administrator Mode 10

V

- Virtual Network Computing. *See* VNC

- VMware Horizon View
 - audio redirection 23
 - certificates 27
 - changing protocols 26
 - command line arguments 25
 - connection options 25
 - device redirection 23
 - keyboard shortcuts 22
 - Kiosk Mode 21
 - mass storage redirection 23
 - MMR 22
 - multi-monitor sessions 22
 - overview 21
 - printer redirection 23
 - security levels 28
 - smart card redirection 24