



HP ThinPro 8.1 Administrator Guide

SUMMARY

This guide is for administrators of HP thin clients based on the HP ThinPro operating system.

Legal information

© Copyright 2023 HP Development Company, L.P.

AMD and ATI are trademarks of Advanced Micro Devices, Inc. Citrix and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, Windows Vista, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. NVIDIA is a registered trademark of NVIDIA Corporation in the U.S. and other countries. UNIX is a registered trademark of The Open Group. VMware, Horizon, and View are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

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: October 2023

First Edition: August 2022

Document Part Number: N81161-001

Open source software

This product includes software licensed under an open source software license, such as the GNU General Public License and the GNU Lesser General Public License or other open source license. To the extent HP has an obligation or, in its sole discretion, chooses to make the source code for such software available under the applicable open source software license, source code for the software can be obtained from the following location:

<https://ftp.hp.com/pub/tcdebian/pool/ThinPro8.1/open-sources.html>

.

User input syntax key

Text that you must enter into a user interface is indicated by `fixed-width font`.

User input syntax key

Item	Description
<code>Text without brackets or braces</code>	Items you must type exactly as shown
<code><Text inside angle brackets></code>	A placeholder for a value you must provide; omit the brackets
<code>[Text inside square brackets]</code>	Optional items; omit the brackets
<code>{Text inside braces}</code>	A set of items from which you must choose only one; omit the braces
<code> </code>	A separator for items from which you must choose only one; omit the vertical bar
<code>...</code>	Items that can or must repeat; omit the ellipsis

Table of contents

1 Getting started	1
Finding more information.....	1
Choosing an OS configuration	1
Choosing a remote management service.....	2
Starting the thin client for the first time	3
Switching between administrator mode and user mode	3
HP Disk Encryption	3
TPM 2.0 and HP Disk Encryption.....	4
Prerequisites for using HP Disk Encryption.....	4
Turning on HP Disk Encryption	4
Turning off HP Disk Encryption	4
Suspending HP Disk Encryption	5
Resuming HP Disk Encryption.....	5
Commands to encrypt, decrypt, or suspend HP Disk Encryption	6
2 ThinPro PC Converter	7
Deployment tool.....	7
Compatibility check and installation	7
Licensing	8
License types.....	8
System tray icon	8
Notifications	9
System information.....	9
Desktop background watermark	9
System update tools.....	9
Royalty-bearing software.....	9
Connections	9
3 GUI overview.....	10
Desktop	10
Taskbar	11
4 Connection configuration	14
Creating a new connection shortcut.....	14
Desktop icon management.....	14
Desktop connection management.....	14
Connection Manager (ThinPro only).....	15

Advanced connection settings	16
Kiosk mode	17
5 Connection types	19
Citrix	19
Citrix Connection Manager	19
Connection	19
Configuration	20
General Settings	21
Options	21
Local Resources	23
Window	24
Self-Service	24
Firewall	25
Keyboard Shortcuts	25
Session	26
Advanced	26
RDP	26
RDP per-connection settings	27
Network	27
Service	27
Window	28
Options	29
Local Resources	30
Experience	30
Advanced	31
RemoteFX	31
RDP multi-monitor sessions	31
RDP multimedia redirection	32
RDP device redirection	32
RDP USB redirection	32
RDP mass storage redirection	33
RDP printer redirection	33
RDP audio redirection	34
RDP smart card redirection	34
VMware Horizon View	34
VMware Horizon View per-connection settings	34
Network	34
General	35
Security	36
RDP Options	37
RDP Experience	38
Advanced	39
VMware Horizon View multi-monitor sessions	39
VMware Horizon View keyboard shortcuts	39
VMware Horizon View device redirection	39
VMware Horizon View USB redirection	39
VMware Horizon View audio redirection	40

VMware Horizon View smart card redirection	40
VMware Horizon View webcam redirection	41
VMware Horizon View COM port redirection	41
Changing the VMware Horizon View protocol	41
VMware Horizon View HTTPS and certificate management requirements	41
Web Browser	43
Web Browser per-connection settings	43
Configuration	43
Preferences	43
Advanced	43
AVD (Azure Virtual Desktop)	43
AVD per-connection settings	44
Configuration	44
Window	44
Options	45
Local Resources	46
TTerm	46
Configuration	47
Additional connection types (ThinPro only)	47
XDMCP	47
Configuration	47
Advanced	48
Secure Shell	48
Configuration	48
Advanced	49
Telnet	49
Configuration	49
Advanced	49
Custom	49
Configuration	50
Advanced	50
6 HP True Graphics	51
Server-side requirements	51
Client-side requirements	51
Client-side configuration	51
Compression settings	52
Window settings	52
Monitor layout and hardware limitations	52
Tips & best practices	52
7 Active Directory integration	54
Login screen	54
Single sign-on	54
Desktop	54
Screen lock	55

Administrator mode	55
Settings and the domain user	56
8 Start menu	57
Connection management	57
Switch to Administrator/Switch to User	57
System Information.....	57
Control Panel.....	57
Tools.....	57
Power	58
Search.....	58
9 Control Panel.....	59
Opening Control Panel.....	59
System.....	59
Network settings.....	60
Opening Network Manager.....	60
Wired network settings	60
Wireless network settings	61
Cellular settings	62
General settings.....	64
DHCP options	65
Opening the DHCP Option Manager	65
Request or ignore DHCP options.....	65
Changing a DHCP code.....	65
Information about DHCP options	65
Imprivata Setup.....	65
Component Manager	66
Opening Component Manager	66
Removing components	66
Undoing a change.....	67
Applying the changes permanently.....	67
Security.....	67
Security settings.....	68
Local Accounts.....	68
Encryption.....	68
Options.....	69
Certificates.....	69
Certificate Manager.....	69
SCEP Manager	69
SIM.....	70
Manageability.....	70
Active Directory configuration.....	71
Status tab.....	71
Options tab.....	72
HP ThinState.....	72

Managing an HP ThinPro image.....	72
Capturing an HP ThinPro image to an FTP server	72
Deploying an HP ThinPro image using FTP or HTTP.....	73
Capturing an HP ThinPro image to a USB flash drive	73
Deploying an HP ThinPro image with a USB flash drive	74
Managing a client profile.....	74
Saving a client profile to an FTP server	74
Restoring a client profile using FTP or HTTP	75
Saving a client profile to a USB flash drive.....	75
Restoring a client profile from a USB flash drive	75
VNC Shadowing.....	76
SNMP	76
Enabling SNMP with Private Configuration File.....	77
Enabling SNMP with Community List.....	77
Disabling SNMP	77
Capsule Update	78
Input Devices	78
Hardware	79
Display management	80
Redirecting USB devices.....	80
Configuring printers	80
Bluetooth.....	81
Appearance	81
Customization Center	82
Snapshots.....	82
10 System Information	84
11 HP Smart Client Services.....	85
Supported operating systems	85
Prerequisites for HP Smart Client Services.....	85
Viewing the Automatic Update website	85
Creating an Automatic Update profile	86
MAC-address-specific profiles.....	86
Updating thin clients.....	87
Using the broadcast update method.....	87
Using the DHCP tag update method	87
Example of performing DHCP tagging.....	87
Using the DNS alias update method	88
Using the manual update method	88
Performing a manual update	88
12 Profile Editor	89
Opening Profile Editor.....	89
Loading a client profile	89
Client profile customization	89

Selecting the platform for a client profile	89
Configuring a default connection for a client profile.....	90
Modifying the registry settings of a client profile	90
Adding files to a client profile.....	90
Adding a configuration file and certificates to a client profile.....	91
Adding a configuration file to a client profile	91
Adding certificates to a client profile	91
Adding a symbolic link to a client profile.....	92
Saving the client profile.....	92
Serial or parallel printer configuration.....	92
Obtaining the printer settings	92
Setting up printer ports.....	93
Installing printers on the server	93
13 Troubleshooting	95
Troubleshooting network connectivity.....	95
Troubleshooting Citrix password expiration	95
Using system diagnostics to troubleshoot	96
Saving system diagnostic data	96
Uncompressing the system diagnostic files	96
Uncompressing the system diagnostic files on Windows-based systems	96
Uncompressing the system diagnostic files in Linux- or Unix-based systems.....	96
Viewing the system diagnostic files.....	97
Viewing files in the Commands folder	97
Viewing files in the /var/log folder	97
Viewing files in the /etc folder	97
Appendix A USB updates	98
USB updates.....	98
HP ThinUpdate	98
Appendix B BIOS tools (desktop thin clients only).....	99
BIOS settings tool.....	99
BIOS flashing tool.....	99
Appendix C Resizing the flash drive partition.....	100
Appendix D mclient command	101
Appendix E HP ThinPro Configuration	103
HP ThinPro configuration profile: profile.xml.....	103
Configuration files of a profile.xml	103
Deployment of a profile.xml.....	104
User registry lock	104
HP ThinPro configuration after an image update.....	105
How to complete a profile.xml.....	105
Appendix F Ephemeral mode	106

Basic usage of an On Boot Snapshot.....	106
System Information.....	106
Util: hptc-snapper.....	106
Restart Plan.....	107
Restart Plan On Boot Snapshot.....	107
Restart Plan Automatic restart.....	107
Restart Plan registry settings.....	107
Automatic Update	109
Scenario 1: Updates on top of the On Boot Snapshot	109
Scenario 2: automatic reset of the On Boot Snapshot after an update	110
HPDM.....	110
How to work in Ephemeral mode with any version of ThinPro.....	110
On Boot Snapshot	111
Reset of the On Boot Snapshot	111
Automatic restarts	111
How to update ThinPro 8.1 when the Restart Plan settings define an On Boot Snapshot.....	111
HPDM sequence of tasks to push a ThinPro profile while an On Boot Snapshot is set.....	111
HPDM sequence of tasks to update some registry settings while an On Boot Snapshot is set.....	112


Appendix G Registry keys 113

Audio	113
Bluetooth.....	114
CertMgr.....	115
ComponentMgr.....	115
ConnectionManager	115
ConnectionType	116
custom.....	116
firefox.....	119
freerdp.....	124
ssh	133
telnet.....	138
TTerm.....	141
view.....	143
AVD.....	152
xdmcp.....	156
xen.....	160
DHCP.....	173
Dashboard	173
Imprivata	174
InputMethod	175
Network.....	175
Power	186
ScepMgr.....	187
Search.....	188

Serial.....	188
SystemInfo.....	189
TaskMgr.....	189
USB.....	190
auto-update.....	190
background	193
boot.....	194
config-wizard.....	194
desktop.....	194
domain	196
entries.....	197
firewall.....	197
hwh264	198
keyboard.....	198
license.....	199
logging	199
login.....	200
mouse.....	200
restore-points	201
screensaver.....	201
security.....	203
shutdown.....	204
sshd	204
time.....	205
touchscreen.....	206
translation	207
usb-update.....	207
users.....	208
vncserver	211
zero-login.....	213
SNMP	214
Index.....	215

1 Getting started

This guide is for administrators of HP thin clients based on the HP ThinPro operating system and assumes that you will log in to the system as an administrator when modifying system configurations or using administrative tools as described in this guide.

 **NOTE:** HP ThinPro has two possible OS configurations: ThinPro and Smart Zero. HP ThinPro-based thin clients can be purchased with either OS configuration as the default, and you can switch between OS configurations via Control Panel.

For more information about each OS configuration, see [Choosing an OS configuration on page 1](#). For more information about switching between OS configurations, see [Customization Center on page 82](#).

Finding more information

Information resources for ThinPro and other software are available online.


 **NOTE:** Information at websites listed in this table might be available in English only.

Table 1-1

Resource	Contents
HP support website http://www.hp.com/support	Administrator guides, hardware reference guides, white papers, and other documentation. Search for the thin client model, and then see the User Guides section of the support page for that model. NOTE: HP Device Manager (HPDM), HP Cloud Endpoint Manager (HPCEM), and HP ZCentral Remote Boost Software each have a dedicated support page. For these products, search for the app name instead, and then see the User Guides section.
Microsoft support website http://support.microsoft.com	Documentation for Microsoft® software
Citrix support website http://www.citrix.com/support	Documentation for Citrix® software
VMware support website http://www.vmware.com/support	Documentation for VMware® software

Choosing an OS configuration

HP ThinPro includes two OS configurations, each tailored for a different thin client deployment scenario:

- The **ThinPro** OS configuration is the complete version of the operating system and is the most suitable for multipurpose environments that require advanced administration or end-user customization. Features of this OS configuration include the following:

- Boots to the ThinPro desktop or Active Directory login screen
- Has more connection types than Smart Zero
- Allows multiple connections (of any supported type) to be configured and run simultaneously
- The **Smart Zero** OS configuration is a simpler, more secure version of the operating system and is the most suitable for single-purpose, kiosk-style environments that require minimal administration and little to no end-user customization. Features of this OS configuration include the following:
 - Boots directly to a virtual session and hides the desktop, a feature also known as “kiosk mode”
 - Has fewer connection types than ThinPro
 - Supports only one connection to be configured and run at a time
 - Does not support Active Directory authentication or single sign-on



NOTE: You can switch between OS configurations via Control Panel (see [Customization Center on page 82](#)).

You can also customize some of the default settings of each OS configuration; for example, to change which connection types are available, enable kiosk mode for ThinPro, or boot to the desktop for Smart Zero.

For more information about kiosk mode, see [Kiosk mode on page 17](#).

The following table lists the default available connection types for each OS configuration.

Table 1-2 OS configurations

OS configuration	Default available connection types
ThinPro	<ul style="list-style-type: none"> • Citrix® • RDP • VMware® Horizon® View™ • Web Browser (Firefox) • XDMCP • Secure Shell • Telnet • Custom
Smart Zero	<ul style="list-style-type: none"> • Citrix • RDP • VMware Horizon View • Web Browser (Firefox)

Choosing a remote management service

Regardless of the OS configuration, you can use these remote management services to manage HP ThinPro-based thin clients:

- **HP Device Manager (HPDM)** is the existing device management software for HP Thin Clients and is ideal for environments of all sizes. HPDM supports devices that run HP ThinPro OS and Windows® 10 IoT OS and provides a greater variety of management capabilities than HP Smart Client Services.
- **HP Smart Client Services** can manage HP ThinPro-based thin clients only and is optimized for use with Smart Zero and a “zero management” scenario. For more information, see [HP Smart Client Services on page 85](#).
- **HP Cloud Endpoint Manager (HPCEM)** is a new, cloud-ready device management solution that is currently in development and will eventually replace HPDM. HPCEM features real-time device monitoring, policy-based management, and proactive notifications that help you achieve ultimate productivity. For more information about HPCEM or to download HPDM, visit the Cloud Client Software webpage.

HP recommends evaluating the management service that is most useful for your environment. HP does not recommend mixing management service strategies within the same environment because doing so might lead to unintended results.

Starting the thin client for the first time

When you first start a new HP ThinPro-based thin client, a setup program runs automatically. The Initial Setup Wizard allows you to select a language, select the keyboard mapping, select a network connection, and configure the date and time settings.



TIP: To modify the configuration of a single thin client and then copy and deploy the configuration to other thin clients, first use the Initial Setup Wizard and Control Panel to modify the configuration, and then deploy the configuration using HPDM, HPCEM, or HP ThinState. For more information, see [GUI overview on page 10](#) or [Control Panel on page 59](#). For more information about HP ThinState, see [HP ThinState on page 72](#).

Switching between administrator mode and user mode

Follow the instructions outlined below to switch between administrator and user mode.

- Right-click the desktop or select **Start**, and then select **Switch to Administrator** from the menu.

For more information about the desktop, see [Desktop on page 10](#).

For more information about Control Panel, see [Taskbar on page 11](#) and [Control Panel on page 59](#).



NOTE: The first time you switch to administrator mode, you are prompted to set up an administrator password. The administrator password must be entered every subsequent time you switch to administrator mode. When Active Directory authentication is enabled, you can also switch to administrator mode by entering the domain credentials of a person in the domain admin group.

When in administrator mode, the screen is surrounded by a red border.

HP Disk Encryption

You typically use HP Disk Encryption for the following types of tasks:



NOTE: HP Disk encryption is off by default.

- Encrypt a disk where ThinPro Operating System is installed

- Decrypt an encrypted disk
- Suspend disk encryption on an encrypted disk to make changes that affect the locked state of TPM 2.0

TPM 2.0 and HP Disk Encryption

Trusted Platform Module (TPM) 2.0 keeps the key used to encrypt or decrypt the disk secure.

When TPM 2.0 is not installed, you cannot turn on HP Disk Encryption. When TPM 2.0 is installed and you turn on HP Disk Encryption, TPM 2.0 locks the encrypted disk in a “trusted” state (PCR values used by TPM 2.0). For example, when the disk is in the process of being encrypted or is resuming from a suspended state, TPM 2.0 locks the encrypted disk in a “trusted” state.

When you start ThinPro from an encrypted disk, PCR values are calculated and verified against the PCR values of the trusted state. If the values are the same, the key used to encrypt the disk can be retrieved to unlock the encrypted disk, the data on the encrypted disk can be read out, and ThinPro can start normally. If TPM 2.0 detects that the system is in a state different from the trusted state, the encrypted disk cannot be unlocked, and ThinPro cannot start.

Prerequisites for using HP Disk Encryption

To be able to turn on HP Disk Encryption, the following criteria must be met:

- TPM 2.0 is present.
- A valid HP ThinPro license is present.
- You can log on with an administrative account.

A standard user does not have permissions for encrypting or decrypting a disk or suspending disk encryption.

Turning on HP Disk Encryption

Follow these steps to turn on HP Disk Encryption:

1. In **Control Panel**, select **Security > Disk Encryption**.
2. Verify that the **Encryption** state is **OFF**.
3. To restart immediately after encryption is complete, select **Reboot automatically after encryption done**.

Otherwise, you must manually reboot the computer after the encryption.

4. Select the **Turn on Encryption** button.

When disk encryption starts, all applications stop and a new window opens, showing the progress. If a problem occurs, select **Details** for information. The desktop reopens after the encryption is complete.

Turning off HP Disk Encryption

When you turn off encryption, you are decrypting the disk. Follow these steps to turn off HP Disk Encryption:

1. In **Control Panel**, select **Security > Disk Encryption**.
2. Verify that the **Encryption** state is **ON**.

3. To restart immediately after decryption is complete, select **Reboot automatically after encryption done**.

Otherwise, you must manually reboot the computer after the decryption.

4. Select the **Turn off Encryption** button.

When disk decryption starts, all applications stop and a new window opens, showing the progress. If a problem occurs, select **Details** for information. The desktop reopens after the decryption is complete.

Suspending HP Disk Encryption

You can suspend HP Disk Encryption to access encrypted data on a disk that uses HP Disk Encryption. This makes the encryption key available in the clear on the hard disk, meaning that its key protectors are not enabled and it is a “clear” key.

Suspending HP Disk Encryption does not mean that data on the disk is decrypted. Instead, suspension means that the key used to decrypt and unlock the data is available in the clear to everyone. New data written to the disk is still encrypted.

Suspension of HP Disk Encryption is necessary when a change made to the system changes the PCR values that match the trusted state. There are a few changes that can cause such changes in PCR values, as shown below. Other changes require the explicit, manual suspension of HP Disk Encryption.

The following changes do not require explicit suspension of HP Disk Encryption. Instead, encryption is automatically suspended before these changes are made:

- Upgrading a ThinPro Service Pack that contains signed kernels and kernel modules via HP EasyUpdate, HP Auto-Update, or USB Update
- Switching btrfs snapshots that causes signed kernels and kernel modules to be switched
- Factory resetting that causes signed kernels and kernel modules to be switched

The following changes require you to manually suspend HP Disk Encryption:

- Upgrading BIOS
- Upgrading signed kernels and kernel modules

To manually suspend HP Disk Encryption:

1. In **Control Panel**, select **Security > Disk Encryption**.
2. Verify that the **Encryption** state is **ON**.
3. Select the **Suspend** button.

Resuming HP Disk Encryption

Resuming HP Disk Encryption is transparent to the user. After suspending HP Disk Encryption, the administrator can make changes to the system, such as upgrading the BIOS or upgrading signed kernels and kernel modules. HP Disk Encryption automatically resumes when you restart the computer, and new PCR values are calculated and updated as a new trusted state.

Commands to encrypt, decrypt, or suspend HP Disk Encryption

Use the following commands with HP Disk Encryption to encrypt, decrypt, or suspend HP Disk Encryption:

- To encrypt HP Disk Encryption

```
# hptc-diskencrypt-reboot -e
```

- To decrypt HP Disk Encryption

```
# hptc-diskencrypt-reboot -d
```

- To suspend HP Disk Encryption

```
# hptc-diskencrypt-suspend
```



NOTE: Certain operations do not work when the disk is encrypted. This includes:

- Cached Imaging operations (capture and deploy)
 - ThinState Image Capture
-

2 ThinPro PC Converter

Starting with ThinPro 7.1, you can use ThinPro on hardware other than HP Thin Clients by using HP ThinPro PC Converter Deployment Tool. The system must meet these minimum requirements:

- CPU: Any 64 bit x86 CPU.
- Memory: 4 GB of RAM, with at least 1 GB free for operating system use.
- Storage: 8 GB or more of internal storage for installation.
- Graphics: Intel®, ATI™/AMD®, or NVIDIA®. If the graphics card is not recognized, you can use limited-performance VESA mode.
- Audio: Audio support is optional.
- Networking: A recognized wired or wireless network adapter.
- USB: HP recommends USB Type-C® high-performance flash drives.
- Licensing: The ThinPro software must be properly licensed.

The first time that a system boots with ThinPro, a compatibility check window appears showing the compatibility status of the system of each of these requirements.

Deployment tool

HP ThinPro PC Converter Deployment Tool allows you to run ThinPro on a PC that runs Microsoft Windows and that meets the minimum requirements. This tool allows for the creation of a USB flash drive containing the ThinPro image. You can boot and run the ThinPro image from the created USB flash drive or you can install the ThinPro image directly onto the PC. You also have the option of creating a mass-deployment image deployable by remote management tools.

For more details, see the *HP ThinPro PC Converter Deployment Tool Administrator Guide*.

Compatibility check and installation

The first time that ThinPro is booted from a USB flash drive, the Compatibility Check window appears. The Compatibility Check tool assesses the hardware on the system to see if it meets the minimum requirements and whether the ThinPro software has recognized the device and assigned a device driver. If the system does not meet minimum requirements, or if required hardware is not found, the Compatibility Check tool will display a warning and additional information.



NOTE: The Compatibility Check tool does only a cursory examination of the hardware and driver state. It does not perform detailed functionality checks such as sending network packets, playing audio files, testing for bad blocks of memory, or evaluating performance. HP cannot guarantee that all hardware components in the PC will work well with ThinPro, even if the Compatibility Check tool determines that the PC is compatible.

If ThinPro is running from a USB flash drive, and if the Compatibility Check passes all the required checks, two buttons appear at the bottom of the window. The first button allows the ThinPro software

to be installed directly onto internal storage. The second button allows you to run ThinPro from the USB flash drive without direct installation onto the PC.



NOTE: The installation button will only appear with a USB flash drive created with the Installer Flash Drive option of the Deployment Tool. The Bootable Flash Drive option does not allow installation.

When installing ThinPro onto the PC, you have the option of saving the settings that were configured while running ThinPro from the USB flash drive. If the settings are not saved, the default factory image of ThinPro will be installed.

The Compatibility Check tool can also be started manually from the administrator tools list under the start button.

Licensing

Supported HP Thin Clients are auto-licensed and do not need license files. If a system is auto-licensed, many of the licensing information sources listed below will not be visible.

All other systems need valid license files to run ThinPro. You get license files from the HP Inc. Software Depot.

The Deployment Tool prompts you to browse to valid license files. The files you select will be automatically copied when you create a bootable ThinPro USB flash drive, and also when you create a mass-deployment image.

If the Deployment Tool and valid licenses are used to install ThinPro onto a device, you do not need to manually install license files. However, if you install ThinPro through some other means, you might have to copy license files to the `/persistent/licenses` directory on the device. You can use HPDM, HPCEM, or some other mechanism to perform this deployment.

License types

There are three types of license files:

- A Trial License allows you to run ThinPro for a short time without paying any licensing fees.
- A Unit License allows you to run a particular version of ThinPro indefinitely. It also denotes that royalty fees have been paid, and it unlocks any royalty-bearing software.
- A Support License gives access to system patches and enhancements and allows the system to be upgraded to newer versions of ThinPro.

Depending on the combination of licenses present on the system, various features will be made visible, hidden, or disabled.

System tray icon

A system tray icon indicates the licensing state of the system.

Table 2-1 System tray icon




Icon	Description
	Valid license.

Table 2-1 System tray icon (continued)

Icon	Description
	License near expiration.
	Invalid license (such as an expired trial license).

Hovering over the systray icon gives information about active licenses found on the system. A right-click will launch the System Info app with the **License** tab selected.

Notifications

Notifications might pop up above the system tray icon periodically.

Courtesy notifications warn when a support license or a trial license is approaching expiration. You can disable courtesy notifications through certain registry settings. See [Registry keys on page 113](#) for more information.

Other notifications warn of licensing errors such as expired, missing, or invalid license files. You cannot disable these types of notifications.

System information

The Software License Tab of the System Information application shows both the overall licensing state of the system and details on each license file found on the system, including start and end dates, license count, license serial number, and other information.

Desktop background watermark

Watermark text is displayed on the desktop background with a trial license or with an expired or invalid combination of licenses. You cannot disable this watermark text.

System update tools

If a system is not auto-licensed and it does not have an active support license, the patches and upgrades shown by Easy Update and other system-update tools will be limited.

Royalty-bearing software

Some software used by ThinPro has royalties attached. An example is any feature using H.264 video decoding. If the system is not auto-licensed and no valid unit license is found on the system, royalty-bearing software will be disabled. Trial licenses do not enable royalty-bearing software.


Connections

If no valid license combination is found on the system, the ability to create remote connections to other systems might be limited or disabled.

3 GUI overview

Desktop

The section describes the GUI of the desktop.

 **NOTE:** The following image demonstrates the desktop for ThinPro with a U.S. locale setting. For Smart Zero, the taskbar is vertical and right-aligned by default, and the desktop theme varies by connection type. The display format of some taskbar information varies by locale setting.

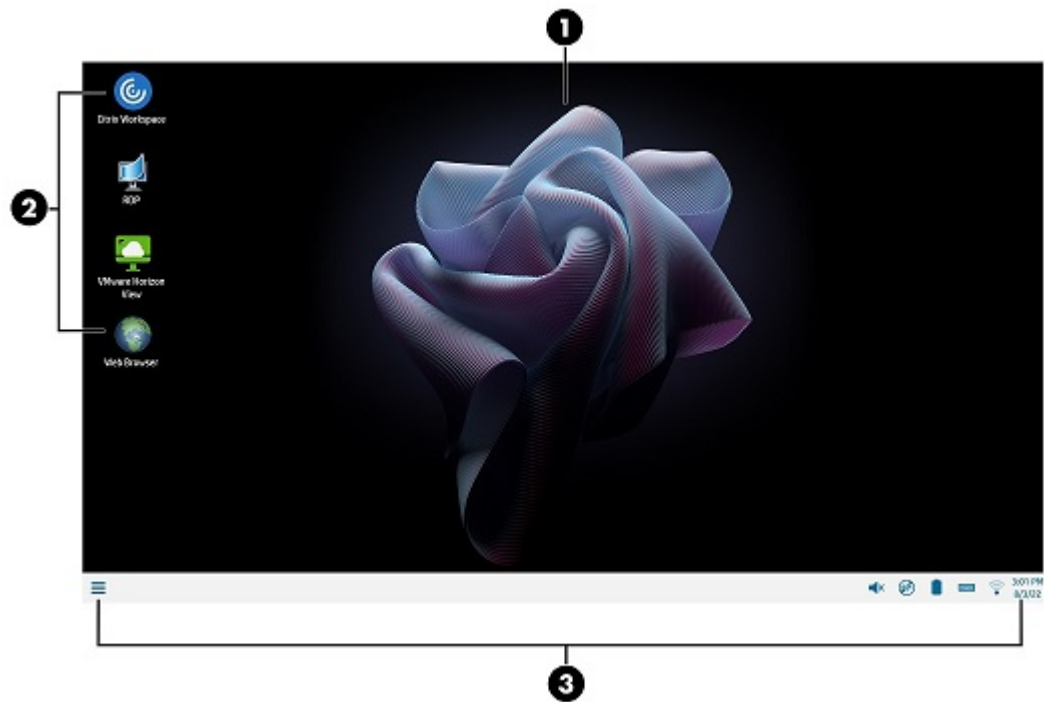


Table 3-1

Item		Description
(1)	Desktop	<p>In ThinPro, you can arrange connection shortcuts in the desktop area and customize the background theme.</p> <p>In Smart Zero, the desktop is replaced by a customizable login screen with a theme specific to the chosen connection type.</p>
(2)	Connection shortcuts	Double-click a connection shortcut to launch a connection. Right-click the icon to display a menu of actions related to the current connection and select to drag the icon to a new location.
(3)	Taskbar	Provides quick access to programs and system functions (see Taskbar on page 11 for more information).

Taskbar

Section describes the taskbar.


 **NOTE:** The following image demonstrates the taskbar for ThinPro with a U.S. locale setting. For Smart Zero, the taskbar is vertical and right-aligned by default. The display format of some taskbar information varies by locale setting.



Table 3-2

Item		Description
(1)	Start	Displays a main menu. For more information, see Start menu on page 57 .
(2)	Application area	Displays the icons for the currently open applications. TIP: You can hold down Ctrl+Alt and then press Tab repeatedly to select an application to bring to the foreground.

Table 3-2 (continued)

Item	Description
(3) System tray	<p>Provides quick access to or provides information about certain functions and services.</p> <p>Place the cursor over a system tray item to display a tool-tip (select items only). Select to start a configuration action, and right-click to display a menu.</p> <p>Items in the system tray can include the following, but some items might not appear depending on the system configuration:</p> <ul style="list-style-type: none"> • Audio mixer • Keyboard: Select this icon to change the keyboard layout, open the virtual keyboard, or change the system layout. Right-click to open the virtual keyboard. To display the name of the current keyboard layout, hover over the icon. • Network status: The network status icon shows the network connection type that is currently active. Hover the mouse over this icon to display the status of current network connection. Select or right-click this icon to open the Network Manager system tray menu and all the supported connection types are listed from top to bottom based on its connectivity priority in the system. <p>NOTE: You can view the status of the following connection types:</p> <ul style="list-style-type: none"> • Wired connection • Wi-Fi connection • Cellular connection <p>You can also create a Wi-Fi network connection. With proper permission, you can also edit the Cellular connection settings and manage the SIM PIN. You can also select Airplane Mode to enable/disable wireless connections and select Network Information to show more details about network connections.</p> <p>You can also perform the following actions:</p> <ul style="list-style-type: none"> – Create a Wi-Fi network connection. – With proper permission, edit the Cellular connection settings and manage the SIM PIN. – Select Airplane Mode to enable/disable wireless connections. – Select Network Information to show more details about network connections. <ul style="list-style-type: none"> • Automatic Update status: The Automatic Update icon is displayed when Automatic Update is checking for updates or updating the computer. To view more information, select the icon. If ThinPro cannot find a valid automatic-update server or if the registry key to display the icon is disabled, the icon is not displayed. • Intelligent Input Bus (Ibus): Ibus is an input method (IM) framework for multilingual input in Unix-like operating systems. • Battery icon: To open Power Manager, right-click this icon and select Adjust Power Settings. • User icon: Indicates that Active Directory authentication is enabled. Select to lock the screen or update the domain password. To display the current user, hover over the icon. • License icon: Indicates the state of ThinPro Licensing. Hover over the icon to see details on the currently-active licenses and right-click to go to the System Info page to see more licensing detail. This is not visible on current HP thin clients, as they are auto-licensed.

Table 3-2 (continued)

Item		Description
(4)	Date and time	Displays the current date and time and opens the date and time settings.

4 Connection configuration

Connection management can be done directly from the desktop as well as through the legacy Connection Manager or the Start menu. By default, the desktop displays an icon as a shortcut for each configured connection.

When you first start the computer, several sample connection icons are displayed on the desktop. You can create a new, generic connection shortcut for any of the connection types supported by ThinPro.

For more information on the legacy Connection manager see [Connection Manager \(ThinPro only\) on page 15](#).

Creating a new connection shortcut

To create a new connection shortcut:

- Right-click the desktop, and then select **Create**.

Desktop icon management

All icons are automatically placed into a grid. You can click and drag an icon to any other grid position on the desktop. After an icon has been moved to a grid position, it is pinned in that position. It stays in that position even if other connection shortcuts are added, deleted, or rearranged.

Any icons not pinned to a grid position are floating. They might be automatically moved when connection shortcuts are added, deleted, or rearranged. To change a pinned icon to a floating icon, right-click the icon and clear **Pin Position**.

Desktop connection management

Connection management can be done directly from the desktop as well as through the legacy Connection Manager or the Start menu. By default, the desktop displays an icon as a shortcut for each configured connection.

When you first start the computer, several sample connection icons are displayed on the desktop. You can create a new, generic connection shortcut for any of the connection types supported by ThinPro.

For more information on the legacy Connection manager see [Connection Manager \(ThinPro only\) on page 15](#).

You can start, stop, edit, copy, rename, or delete each connection. If user editing is not enabled, non-administrator users can only start or stop a connection.

- To manage a connection on the desktop, right-click the connection icon, and then select an action.




NOTE: If user editing is not enabled, you must switch to administrator mode to manage a connection.

- **Start/Stop:** Starts a connection or stops an active connection. You can also double-click the connection icon. When the connection is active, a green circle is displayed on the connection icon, and the connection icon is displayed in the taskbar. When a connection starts, if any connection parameters are missing, a dialog box asks for the missing parameters. For example, because none of the starting icons have a remote server defined, a dialog box asks for the address or name of the remote server when the connection is started.
- **Edit:** Opens the complete connection editor.
- **Copy:** Creates a copy of the connection with all the parameters of the original connection and a unique name.
- **Rename:** Allows you to rename the connection. You can also double-click the text beneath the connection icon or use the connection editor.
- **Delete:** Deletes the connection.

Connection Manager (ThinPro only)

This section identifies Connection Manager components and explains how to open Connection Manager.

 **NOTE:** HP recommends using the connection shortcuts. However, you can use the legacy Connection Manager interface.

The following image demonstrates Connection Manager with a U.S. locale setting.



Table 4-1

Item	Description	
(1)	Connection list	Lists the configured connections and whether each connection is active or inactive.
(2)	Start	Starts the selected connection.
(3)	Stop	Stops the selected connection.
(4)	Edit	Lets you edit the selected connection.

Table 4-1 (continued)

Item	Description
(5) Delete	Deletes the selected connection.
(6) Add	Lets you add a new connection. NOTE: See Choosing an OS configuration on page 1 for a list of the available connection types.
(7) Settings	Lets you edit general settings for Citrix connections. These settings apply to all connections of that type.

To open Connection Manager:

1. In administrator mode, select **Start**, and then type `Connection Manager` in the search box.
2. Select **Connection Manager**.

For more information about configuring connections, see the following:

- [Connection configuration on page 14](#)
- [Connection types on page 19](#)

Advanced connection settings

The following table describes the settings that are available under the Advanced category when editing a connection of any connection type.



NOTE: These settings affect only the connection that you are currently configuring.

Table 4-2 Advanced connection settings

Option	Description
Fallback Connection	Specifies the fallback connection. If the connection fails to start, the fallback connection will attempt to start instead. NOTE: This option is not available for the VMware Horizon View connection type.
Auto start priority	Determines the order that connections will auto-start. 0 means auto-start is disabled. The other values determine the startup order, with 1 being the highest priority.
Share credentials with screensaver	Enables users to unlock the local screen saver using their credentials for that connection. NOTE: This option is only available for the Citrix, RDP, and VMware Horizon View connection types.
Auto reconnect	If enabled, this connection will attempt to auto-reconnect if the connection is dropped. NOTE: Stopping a connection via Connection Manager will prevent an auto-reconnection.
Wait for network before connecting	Disable this option if your connection doesn't need the network to start or if you don't want to wait for network to start the connection.

Table 4-2 Advanced connection settings (continued)

Option	Description
Show icon on desktop	<p>If enabled, a desktop icon is created for this connection. This option is enabled by default.</p> <p>If disabled, the connection is not visible on the desktop, but is visible in the Start menu and Connection Manager.</p>
Allow the user to launch this connection	If enabled, this connection can be launched by an end user.
Allow the user to edit this connection	If enabled, this connection can be modified by an end user.
Login dialog options	<p>Enable or disable these options to configure the login dialog for the connection.</p> <p>NOTE: This option is only available for the Citrix, RDP, and VMware Horizon View connection types.</p> <p>The following options are available:</p> <ul style="list-style-type: none">• Show server field• Show username field• Show password field• Show domain field• Show 'remember me' checkbox <p>NOTE: This option saves the user name and domain, but the password still needs to be entered each time.</p>

Kiosk mode

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



TIP: The remote host can be configured to start resources automatically upon login, making the kiosk mode experience seamless.

The easiest way to configure a thin client for kiosk mode is to switch it to Smart Zero (see [Customization Center on page 82](#)) and configure a connection. When this is done, the following settings are set automatically:

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

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

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



TIP: When in kiosk mode, to minimize the connection and return to the local desktop, press **Ctrl+Alt+End**.

5 Connection types

Citrix

The following table describes the supported Citrix Virtual Apps and Desktops backends.

Table 5-1 Citrix Virtual Apps and Desktops backends

Access type	Virtual Apps and Desktops version
PNAgent (legacy)	2206 and 2203 LTSR or later
Web browser	2206 and 2203 LTSR or later
StoreFront	2206 and 2203 LTSR or later

The following table describes the supported Citrix XenApp/XenDesktop® backends.

Table 5-2 Citrix XenApp/XenDesktop backends

Access type	XenApp/XenDesktop version
PNAgent (legacy)	7.6 LTSR and 7.15 LTSR and 7.16 or later
Web browser	7.6 LTSR and 7.15 LTSR and 7.16 or later
StoreFront	7.6 LTSR and 7.15 LTSR and 7.16 or later

Citrix Connection Manager

This section describes the settings that are available under various categories when editing a Citrix connection.



NOTE: Connection, configuration, and advanced settings affect only the connection you are currently configuring. General settings affect all Citrix connections.

Connection

The following table describes the settings that are available under the Connection category when editing a Citrix connection.

Table 5-3 Connection

Option	Description
Name	The connection name.

Table 5-3 Connection (continued)

Option	Description
URL	<p>Citrix service URL or Citrix server FQDN.</p> <p>Examples:</p> <ul style="list-style-type: none"> For all modes, it can be the FQDN. Example: myserver.com For PNAgent, it should be the config.xml URL. Example: myserver.com/citrix/pnagent/config.xml For Storefront, it should be the store URL. Example: myserver.com/Citrix/storefront/mystore/discovery For Netscaler, it should be the netscaler URL. Example: mynetscaler.com
Credentials	<p>Sets the authentication mode to one of the following:</p> <ul style="list-style-type: none"> Anonymous login: For StoreFront servers that allow unauthenticated (anonymous) users. Use Single Sign-On credentials: The credentials used at login are also used to start the connection. Ask for credentials at connection start: There are no pre-supplied credential components. Use predefined user, password, and/or domain: Some or all of the credentials are stored and supplied for the connection. Use predefined smart card: The connection is expected to be used with a smart card for authentication. Other credential types: RSA, Azure, and multi-factors authentication.
User	The username for this connection.
Password	The password for this connection.
Domain	The domain name for this connection (optional).
Test connection	Checks the URL and the credentials.

Configuration

The following table describes the settings that are available under the Configuration category when editing a Citrix connection.

Table 5-4 Configuration

Option	Description
Auto Reconnect Applications on Login	<p>With this option selected, resources that were open when the user last logged out will be reopened when they log in again.</p> <p>TIP: If not using the Citrix SmoothRoaming feature, disable this option to increase your connection speed.</p>


Table 5-4 Configuration (continued)

Option	Description
Autostart mode	<p>Lets you set a specific application or desktop to start automatically when the Citrix connection begins. If set to Auto Start Single Resource, and if there is a single published resource, that resource starts automatically.</p> <p>NOTE: This option has no effect if Auto Reconnect Applications on Login is selected and there are applications to reconnect to.</p> <p>If you have selected Auto Start Application or Auto Start Desktop, select the Enumeration button to retrieve a list of resources (applications or desktops) and display them in Citrix Connection Manager, which enables you to select resources to start automatically upon connection.</p> <p>If you have selected Auto Start Single Resource, select the Enumeration button to retrieve the number of resources. If there is only one resource, it is started automatically upon connection.</p>
Show resources	<p>With this option selected, you must then select where to display the resources:</p> <ul style="list-style-type: none"> • In a window: Displays resources in a window. • Directly on desktop: Displays resources on the desktop.
Show resources in the Start Menu	With this option selected, remote resources from the connection are shown in the Start menu.
Auto save store	If this option is selected, save the store discovery URL.

General Settings

To edit the general settings:

- In Citrix Connection Manager, select the **General Settings** tab, and then select **Xen Connection General Settings Manager**.

 **NOTE:** These settings affect all Citrix connections.

Options

The following table describes the settings that are available under the Options category when editing the Citrix general settings.

Table 5-5 Options

Option	Description
Enable HDX MediaStream	Enables HDX MediaStream.
Enable MultiMedia	Enables multimedia.
Enable Connection Bar	Enables the connection bar.
Enable Auto Reconnect	Enables automatic reconnection of dropped connections.
Enable Session Reliability	Enables the Citrix Session Reliability feature. See Citrix documentation for more information.
Enable keyboard layout synchronization	Enables keyboard layout synchronization between client and VDA.

Table 5-5 Options (continued)

Option	Description
Enable Smart Card Channel	Enables the smart card channel feature. NOTE: If you want to use a smart card in the Citrix session but are not using a smart card connection, enable this option.
Enable FIDO2 Authentication Channel	Enables FIDO2 authentication virtual channel. NOTE: You must restart the system to apply the settings.
Enable Battery Status Indicator	Enables the battery status indicator in the session for the mobile thin client.
Session Reliability Timeout (seconds)	Specifies the session reliability timeout in seconds. The default is 180 seconds.
Enable Clipboard Redirection	Enables clipboard redirection.
Session Reliability Notification	The session window is grayed out and a countdown timer shows the time until the next reconnection attempt.
Use Data Compression	Uses data compression for this connection.
Enable H264 Compression	Enables H.264 compression. See Citrix documentation to determine if this method of data compression is best for your use cases.
Enable Middle Button Paste	Enables the middle mouse button paste function.
Enable cursor color inverting	The cursor color inverts based on the background color of a text. As a result, you can easily locate the position of the cursor in the text.
UDP audio through Citrix Gateway	Enables UDP audio through the Citrix Gateway. NOTE: Technical previews are available for customers to test in their non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix does not accept support cases for feature previews but welcomes feedback for improving them. Citrix might or might not act on feedback based on its severity, criticality, and importance. It is advised that Beta builds are not deployed in production environments.
Support for multiple audio devices	If this option is selected, Citrix displays all available local audio devices in a session with their names.
Enable UDP audio	Enables UDP audio.
Enhancement to Teams Audio Configuration	Configures echo cancellation, auto gain control and noise suppression options to troubleshoot MS Teams audio issues (like robotic voice, high CPU causing choppy audio, and so on).
Improved audio echo cancellation	Enables audio echo cancellation. NOTE: By design, the echo cancellation feature is disabled for high quality audio.
Enable CEF-based BCR	Enables Chromium Embedded Framework (CEF) for Citrix browser content redirection.
User Agent String	Specifies a User Agent string to be used for requests sent to the Citrix server. This option is useful for a NetScaler configuration.
Enable jitter buffer	Ensures clear audio even when the network latency fluctuates.
Sound	Sets the sound quality or disables sound entirely.

Table 5-5 Options (continued)

Option	Description
Transport Protocol	<p>Specifies the transport protocol for the connection and whether to use a fallback transport protocol.</p> <ul style="list-style-type: none"> • Off (default): Use TCP. • On: Use UDP and do not fall back to TCP on failure. • Preferred: Try UDP first and fall back to TCP on failure.
Logging	<p>Sets the debug log level.</p> <ul style="list-style-type: none"> • Verbose • Normal • Only errors (default) • Disabled

Local Resources

The following table describes the settings that are available under the Local Resources category when editing the Citrix general settings.

Table 5-6 Local Resources

Option	Description
Citrix USB Redirection Status	<p>To configure, select USB Manager. See Redirecting USB devices on page 80.</p> <ul style="list-style-type: none"> • Enabled: USB redirection is supported for the Citrix connection. • Disabled: USB redirection is disabled for the Citrix connection.
Printers	<p>Controls how local printer redirection is handled.</p> <ul style="list-style-type: none"> • Printer mapping • USB Redirection • Disable
Webcam	<p>Controls how local webcam and audio input redirection is handled.</p> <ul style="list-style-type: none"> • HDX Webcam • USB Redirection • Disable
Audio	<p>Controls how local audio device redirection is handled.</p> <ul style="list-style-type: none"> • HDX Audio • USB Redirection • Disable

Table 5-6 Local Resources (continued)

Option	Description
Drive Mapping/Redirection	Specifies the method used to access the local drive. NOTE: Select only one method of drive redirection. <ul style="list-style-type: none">• USB Redirection: Enables USB redirection. For more options, open USB Manager.• Dynamic Drive Mapping: Enables dynamic drive mapping.• Static Drive Mapping (Legacy): Enables static drive mapping, which allows you to specify drive mappings to local paths. To specify these paths, select Configure Mapping Folders.

Window

The following table describes the settings that are available under the Window category when editing the Citrix general settings.

Table 5-7 Monitor

Option	Description
TWI Mode	Lets you display a single seamless window on the local ThinPro desktop as if it were a native application.
Enable DPI matching	Enables DPI matching.
Enable screen pin	Enables pinning a multi-monitor screen layout.
Default Window Size	When TWI Mode is set to Force Seamless Off , this controls the default window size.
Default Window Colors	Sets the default color depth.
Left Monitor	When Show the Virtual Desktop on all monitors is disabled, these fields let you specify how the virtual desktop is displayed across specific monitors.
Right Monitor	
Top Monitor	
Bottom Monitor	

Self-Service

The following table describes the settings that are available under the Self-Service category when editing the Citrix general settings (for Workspace mode only).

Table 5-8 Self-Service

Option	Description
Option 1 Enable Kiosk Mode	Configure a user device to start up in kiosk mode, in which self-service starts in full screen mode.
Option 1.1 Show taskbar	Specifies whether the taskbar is displayed or not. Customization Center has more options to customize taskbar.
Option 1.2 Enable shared user mode	Multiple users could share the device.
Option 2 Disable Citrix Workspace - Preferences	Disable Citrix menu item - Preferences in Self-Service UI.

Table 5-8 Self-Service (continued)

Option	Description
Option 3 Disable Citrix Connection Center	Disable Citrix menu item – Connection Center in Self-Service UI.

Firewall

The following table describes the settings that are available under the Firewall category when editing the Citrix general settings.

Table 5-9 Firewall

Option	Description
Proxy Type	Specifies the proxy type.
Proxy Address	The IP address of the proxy server.
Proxy Port	The port for connection to the proxy server.
Username	The username to use for connection to the proxy server.
Password	The password to use for connection to the proxy server.
Use Alternate Address for Firewall Connection	The Citrix ICA Client will request the alternate address defined for the server when contacting servers inside the firewall. The alternate address must be specified for each server in a server farm.

Keyboard Shortcuts

The following table describes the settings that are available under the Keyboard Shortcuts category when editing the Citrix general settings.

Table 5-10 Keyboard Shortcuts

Option	Description
Enable UseLocalIM	Uses the local input method to interpret keyboard input. This is supported only for European languages.
Use EUKS Number	Controls the usage of Extended Unicode Keyboard Support (EUKS) on Windows servers. Valid options are described below: <ul style="list-style-type: none"> 0: EUKS is not used. 1: EUKS is used as a fallback. 2: EUKS is used whenever possible.
Keyboard Mapping File	Specifies the keyboard mapping file. Select Auto to allow the file to be selected automatically. Otherwise, select a specific mapping file. NOTE: To use your own keyboard mapping file, save it in the folder: <code>/usr/lib/ICAClient/keyboard/</code> .
Keyboard layout synchronization mode [Technical Preview]	Set keyboard layout synchronization mode: <ul style="list-style-type: none"> Sync only once - when session starts Allow dynamic sync Don't sync

Table 5-10 Keyboard Shortcuts (continued)

Option	Description
Keyboard input mode [Technical Preview]	Set keyboard input mode: <ul style="list-style-type: none"> • Scancode • Unicode

Session

The following table describes the settings that are available under the Session category when editing the Citrix general settings.

Table 5-11 Session

Option	Description
Auto Logout Delay Before App Launch	When using a Citrix server with multiple published resources, this specifies the number of seconds to allow a user to launch an app after login before the system automatically logs out and returns to the initial login screen.
Auto Logout Delay After App Close	When using a Citrix server with multiple published resources, this specifies the number of seconds between the closing of the last Xen published resource and when the user is automatically logged out and returned to the initial login screen.
Server Check Timeout	To perform a basic connectivity check to the selected server and port, set this option to a value other than the default -1.

TIP: Setting any of these values to less than 0 will disable auto-logout.

NOTE: Citrix processing delays might increase the auto-logout time.

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

RDP

The RDP client is based on FreeRDP 2.9 and meets the following requirements for RDP:

- Hardware-accelerated RemoteFX
- MMR supported when connecting to Windows hosts with the Desktop Experience feature enabled
- USBR supported when connecting to RDP servers that enable it
- RemoteApp supported



NOTE: You can upgrade the RDP client to the newer version of FreeRDP by installing the new FreeRDP add-on.

RDP per-connection settings

This section describes the settings that are available under various categories when editing an RDP connection.



NOTE: These settings affect only the connection you are currently configuring.

Network

The following table describes the settings that are available under the Network category when editing an RDP connection.

Table 5-12 Network

Option	Description
Connection Name	A custom name for this connection.
Server Name/Address	<p>The IP address or server name for this connection, or the RD Web Access feed URL. If required, the port can be appended to the server after a colon (by default, the port is 3389 for a direct RDP connection).</p> <p>NOTE: The RD Web Access feed URL must begin with <code>https://</code>. By default, this is added automatically as specified by the <code>rdWebFeedUrlPattern</code> registry key, which defines the pattern of the URL.</p>
Credentials	<ul style="list-style-type: none">• Use Single Sign-On credentials: The credentials used at login are also used to start the connection.• Ask for credentials at connection start: There are no presupplied credential components.• Use predefined user, password, and/or domain: Some or all of the credentials are stored and supplied for the connection.• Use predefined smart card: The connection is expected to be used with a smart card for authentication.
User	The username for this connection.
Password	The password for this connection.
Domain	The domain name for this connection (optional).
Use RD Gateway	Enables additional RD Gateway options, such as the gateway address, port, and credentials.

Service

The following table describes the settings that are available under the Service category when editing an RDP connection.

Table 5-13 Service

Option	Description
Service	<p>Sets the RDP service to one of the following:</p> <ul style="list-style-type: none"> Remote Computer: When using this service, a direct RDP connection is created to a remote computer. A remote application or alternate shell can optionally be started upon connection. The following additional options are available for a Remote Computer service: <ul style="list-style-type: none"> If Mode is set to Remote Application, the Application field specifies the path of the application to run. If Mode is set to Alternate Shell, the Command field specifies the command that executes the application to run in the alternate shell. For example, to run Microsoft® Word, type <code>Word.exe</code>. <p>If Mode is set to Alternate Shell, the Directory field specifies the server's working directory path for the application's program files. For example, the working directory for Microsoft Word is <code>C:\Program Files\Microsoft</code>.</p> RD Web Access: When using this service, a list of RemoteApp resources is retrieved from the server and presented to the user, and the actual RDP connection is started when a resource is selected. The following additional options are available for RD Web Access: <ul style="list-style-type: none"> Keep resource selection window open: With this option selected, users can open multiple resources simultaneously from the resource selection window. Auto-start single resource: With this option selected, and if there is a single published resource, that resource will start automatically upon connection. Resource filter and Web Feed Browser: These can be used to limit the remote resources that will be made available to the user in the resource selection window. Auto-disconnect timeout: With this option selected, you can set how long a Web Access connection can be maintained before it is automatically closed as a security measure. <p>NOTE: An advantage of using RD Web Access is that it handles the details of brokered connections and the Load Balance URL automatically.</p> <p>For more information, see the HP ThinPro white paper <i>RD Web Access Deployment Example</i> (available in English only).</p>

Window

The following table describes the settings that are available under the Window category when editing an RDP connection.

Table 5-14 Window

Option	Description
Hide window decorations	This setting makes sure that screen elements such as the menu bar, minimize and close options, and borders of the window pane are not displayed.
Window size	Sets the window size to full , fixed , or percent .

Table 5-14 Window (continued)

Option	Description
Percentage Size	<p>If Window Size is set to percent, this option sets the percentage of the screen that a desktop window occupies.</p> <p>NOTE: The resulting sizes might be rounded.</p> <p>NOTE: RemoteFX supports only a fixed list of resolutions.</p>
Fixed Size	<p>If Window Size is set to fixed, this option sets the width and height in pixels that the desktop window occupies.</p>
Enable dynamic resolution	<p>If enabled, resolution updates send to the RDP server when the window is resized.</p>

Options

The following table describes the settings that are available under the Options category when editing an RDP connection.

Table 5-15 Options

Option	Description
Enable motion events	If enabled, mouse motions are continuously relayed to the RDP server.
Enable data compression	Enables bulk compression of data between the RDP server and RDP client.
Enable deprecated RDP encryption	Enables last-generation RDP encryption when NLA is not available.
Enable offscreen cache	If enabled, off-screen memory is used to cache bitmaps.
Attach to admin console	Attaches the connection to the administrator console port.
Cross-session copy/paste	If enabled, copy and paste are enabled between different RDP sessions.
Enable Progressive RemoteFX Codec	<p>Enables the RemoteFX Progressive Codec, which transmits the desktop in a series of sharper and sharper images.</p> <p>NOTE: This codec might cause visual artifacts on desktops with highly dynamic content, so this codec can be disabled, if necessary.</p>
Enable Multimedia Redirection	Allows multimedia files to be sent directly to the client for local playback.
Certificate verification policy	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Ignore the certificate checks altogether • Accept certificate unconditionally on first connect • Warn if the certificate does not match • Automatically abort connection if the certificate does not match
Send hostname as	For per-device licensing, this selects how the client hostname is sent to the RDP server. Select hostname or mac .
Hostname to send	<p>Normally, the thin client's hostname is used for Client Access Licenses. This field allows a different value to be sent.</p> <p>TIP: Select the (i) icon next to this option for more information.</p>
Load Balance Info	<p>Use this option with a brokered RDP connection.</p> <p>TIP: Select the (i) icon next to this option for more information.</p>

Local Resources

The following table describes the settings that are available under the Local Resources category when editing an RDP connection.



NOTE: HP recommends high-level device redirection for all local devices unless there is a specific reason to use USB redirection (USBR) instead. For more information, see the HP ThinPro white paper *USB Manager* (available in English only).

Table 5-16 Local Resources

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

Experience

The following table describes the settings that are available under the Experience category when editing an RDP connection.

Table 5-17 Experience

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

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

RemoteFX

RemoteFX 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 RemoteFX codec and send screen updates to the RDP client. RemoteFX 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.

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



NOTE: For more information, see the HP ThinPro white paper *Enabling RemoteFX for RDP* (available in English only).

RDP multi-monitor sessions

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

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

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



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



NOTE: For more information about RDP multi-monitor sessions, see the HP ThinPro white paper *True Multi-Monitor Mode for RDP* (available in English only).

RDP multimedia redirection

Multimedia redirection (MMR) is a technology that integrates with Windows Media Player on the remote host and streams the encoded media to the RDP 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. The RDP 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 thin 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.



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

RDP device redirection

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

RDP USB redirection

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 thin 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 thin client. Some devices such as mass storage, printers, and audio devices might use additional options for redirection.

Note the following additional information about USB redirection with RDP:

- The server must support USB redirection for it to be available to the thin client. General-purpose USB redirection is supported with RDVH servers with RemoteFX, Windows 8, Windows 10, Windows Server 2012, and Windows Server 2016.
- The protocol in USB Manager in Control Panel must be set to RDP.
- For RDP connections, the controls in USB Manager determine if a USB device is redirected. The settings for the individual connection determine how a USB device is redirected.

RDP mass storage redirection

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 thin client, the thin 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 thin client will be mounted. The supported file systems are FAT32, NTFS, ISO9660 (CD-ROMs), UDF (DVD-ROMs), and ext3.
- The device will be treated as a directory; common drive tasks like formatting and modification of the disk label will not be available.

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

Table 5-18 RDP mass storage redirection

Registry entry	Value to set	Description
root/USB/root/protocol	local	Makes sure that the RDP connection does not attempt to redirect any devices to the remote session

RDP printer redirection

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 thin client.

A generic postscript driver is used if no driver is specified, but additional printer features might be available if the printer is set up locally with a specific Windows driver. 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 **Model** in the printer properties.



NOTE: See [Serial or parallel printer configuration on page 92](#) for more information.

RDP audio redirection

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

See the following notes about using audio redirection with RDP:

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

RDP smart card redirection

To enable smart card login for an RDP connection:

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.

- Select **Use predefined smart card** in the RDP Connection Manager.

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

This technology requires drivers for the smart card reader driver to be installed on the thin 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.

VMware Horizon View

VMware Horizon View per-connection settings

This section describes the settings that are available under various categories when editing a VMware Horizon View connection.



NOTE: These settings affect only the connection you are currently configuring.

Network

The following table describes the settings that are available under the Network category when editing a VMware Horizon View connection.

Table 5-19 Network

Option	Description
Name	Enter a name for this connection.
Address	Enter the hostname or IP address of a VMware Horizon View server.
Credentials	<ul style="list-style-type: none"> • Log in anonymously using unauthenticated access • Use Single Sign-On credentials: The credentials used at login are also used to start the connection. • Ask for credentials at connection start: There are no pre-supplied credential components. • Use predefined user, password, and/or domain: Some or all of the credentials are stored and supplied for the connection. • Use predefined smart card: The connection is expected to be used with a smart card for authentication.
User	Enter the username to use for the connection.
Password	Enter the password to use for the connection.
Domain	Enter the domain to use for the connection.

General

The following table describes the settings that are available under the General category when editing a VMware Horizon View connection.

Table 5-20 General

Option	Description
Enable MMR	<p>Enables multimedia redirection for BLAST and PCoIP connections.</p> <p>NOTE: HP recommends disabling this option.</p> <p>For connections made with RDP protocol, use the Enable Multimedia Redirection option. See RDP Options on page 37.</p>
Enable USB auto-connect when inserted	Enable USB device redirection when a USB device is inserted.
Enable USB auto-connect at startup	Enable USB device redirection when a VMware View connection starts.
Send Ctrl + Alt + Del to virtual desktop	Enable sending Ctrl + Alt + Del to virtual desktop directly.
Allow Horizon Client data sharing	If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects and receives anonymous data on client systems to prioritize hardware and software compatibility.
Enable client drive redirection	<p>Enables the shared folder feature for BLAST and PCoIP connections. This option is enabled by default.</p> <p>NOTE: You can map USB storage devices via CDR (client drive redirection). To disable USB storage USB devices in the session, disable USB redirection and this feature (CDR).</p>
Automatic login	<p>When enabled, the user is automatically logged in when the connection is established.</p> <p>NOTE: HP recommends enabling this option.</p>

Table 5-20 General (continued)

Option	Description
Virtualization pack for Skype for Business	Enables virtualization of Skype for Business. NOTE: Video calls might use most of the processing power of a thin client. HP recommends disabling this option. Skype for Business is discontinued.
Default Desktop	Specifies a desktop to start automatically when a VMware Horizon View connection is launched.
Preferred Protocol	Lets you select PCoIP, RDP, or BLAST as the preferred protocol or choose to select the protocol later.
Application Size	Sets the application window size. You can select All Monitors , Full Screen , Large Window , or Small Window .
Desktop Size	Sets the desktop window size. You can select All Monitors , Full Screen , Large Window , or Small Window .
Printers	Controls how local printer redirection is handled: <ul style="list-style-type: none"> • Integrated printing • USB Redirection • Disable NOTE: For connections made with RDP protocol, see RDP printer redirection on page 33 .
Launch client software in minimized mode	If selected, the Horizon client window remains minimized and hidden in the background when the user-specified remote desktop or published application launches.

Security

The following table describes the settings that are available under the Security category when editing a VMware Horizon View connection.

Table 5-21 Security

Option	Description
Close After Disconnect	<p>Makes the VMware Horizon View client close automatically after users log out of their desktops or the session terminates with an error.</p> <p>This option is a security feature designed so that users do not need to take an additional step to fully log out after they are finished with their desktop session.</p> <p>This option is enabled by default for security purposes but can be disabled if users find that they are often switching to a new desktop pool after logging out of a session and do not want to fully log in again.</p>
Hide top Menu bar	<p>Makes the top menu bar invisible for users.</p> <p>This option enabled by default. Disable it if users prefer to access options for window size or desktop pool selection in a VMware Horizon View session.</p>
Prevent users from changing server address	If enabled, end users cannot change the server address.
Enable session roaming monitor	Closes the connection if the session roams from another client. This option is supported on only PCoIP connections.

Table 5-21 Security (continued)

Option	Description
Skip checking the certification revocation list	If selected, the Horizon client does not check the certification revocation list when connecting to the server.
Certificate verification policy	Select one of the following: <ul style="list-style-type: none"> • Allow all connections • Warn • Refuse insecure connections

Table 5-22 BLAST options

Option	Description
Allow H.264 decoding	Allows H264 decoding in the Horizon client.
Allow BlastCodec decoding	You can enable or disable the use of BlastCodec decoding to receive remote screen content on the client interface.
Allow High Color Accuracy (reduces battery life and performance)	If selected, this option allows increasing color fidelity.
Allow High Efficiency Video decoding (HEVC)	If selected, H265 decoding is allowed in Horizon client.
Allow Blast connections to use operating system proxy settings	Use Network Manager to setup system proxy.

RDP Options

The following table describes the settings that are available under the RDP Options category when editing a VMware Horizon View connection.

Table 5-23 RDP Options

Option	Description
Enable motion events	Enables motion events for this connection.
Enable data compression	Uses data compression for this connection.
Enable deprecated RDP encryption	Enables encryption for this connection.
Enable offscreen cache	If enabled, off-screen memory is used to cache bitmaps.
Attach to admin console	Attaches the connection to the administrator console port.
Cross-session copy/paste	If enabled, copy and paste are enabled between different RDP sessions.
Enable Progressive RemoteFX Codec	Enables the RemoteFX Progressive Codec, which transmits the desktop in a series of sharper and sharper images.
Enable Multimedia Redirection	Allows multimedia files to be sent directly to the client for local playback. For more information, see RDP multimedia redirection on page 32 .
Automatic reconnection maximum retries	Set reconnection maximum retries. Default is 30.
Send hostname as	For per-device licensing, this selects how the client hostname is sent to the RDP server. Select hostname or mac .

Table 5-23 RDP Options (continued)

Option	Description
Hostname to send	<p>Normally, the thin client's hostname is used for Client Access Licenses. This field allows a different value to be sent.</p> <p>TIP: Select the (i) icon next to this option for more information.</p>
Load Balance Info	<p>Use this option with a brokered RDP connection.</p> <p>TIP: Select the (i) icon next to this option for more information.</p>
Remote computer sound	Specifies where the remote computer's sound should be played (remotely or locally) or if it should not be played at all.
Enable port mapping	Maps the thin client's serial and parallel ports to the remote session.
Enable printer mapping	<p>Maps the local print queue to the remote session. Use this option if either USB redirection is unavailable on the remote host or the printer is a parallel or serial printer. Configure the printer to use a local printer spooler, and the VMware Horizon View client automatically sets up a remote printer that sends print spooling commands through a virtual channel from the remote host to the thin client.</p> <p>This method requires both that the printer be configured on the thin client and a Windows driver be specified on the thin client because the VMware Horizon View 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.</p>
Shared folders	Add, Remove, or Edit shared folders.

RDP Experience

The following table describes the settings that are available under the RDP Experience category when editing a VMware Horizon View connection.

Table 5-24 RDP Experience

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

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

VMware Horizon View multi-monitor sessions

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.

VMware Horizon View keyboard shortcuts

Windows keyboard shortcuts

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

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

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



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

Media keys

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

VMware Horizon View device redirection

VMware Horizon View USB redirection

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

To support composite USB devices USB redirection, set `root/ConnectionType/view/connections/<UUID>/useCurrentViewConfig` to 1, and edit the `/etc/vmware/config` file directly.


For more information on USBR, including device- and class-specific redirection, see [RDP USB redirection on page 32](#).

VMware Horizon View audio redirection


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

The VMware Horizon View client supports high-level audio-record redirection only via the PCoIP connection type on x86 units when connecting to a server running VMware Horizon View 5.2 Feature Pack 2 or higher or the BLAST connection type on x86 units when connecting to a server running VMware Horizon View 7.x or higher. If you need audio-recording support and are using a different configuration, use one of the following methods:

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

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


- If you have a USB headset with a microphone, you can use USBR. Set the USB headset to be redirected into the session. The headset will show up as an audio device. By default, USB audio devices are not redirected and the VMware Horizon View client uses high-level audio redirection. To redirect the USB headset, use the thin 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 selected under the devices to be redirected.


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

VMware Horizon View smart card redirection


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

1. Be sure smart card login is enabled in the VMware Horizon View Connection Manager (Credentials->Use predefined smart card).
2. Select a PKCS11 Security module for the smart card. You might want to contact the vendor of the card for a PKCS11 security module for the card. By default, there are Open source pkcs11 modules in the ThinPro Image, but these modules might not work for the card.
3. After starting the connection, the VMware Horizon client displays the valid certificate subject and asks for PIN. 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 thin client. See [RDP smart card redirection on page 34](#) 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.

VMware Horizon View webcam redirection


The VMware Horizon View client supports high-level webcam redirection only through RTAV using x86 units connected to a back-end server running VMware Horizon View 5.2 Feature Pack 2 or higher.

Other connection methods do not support high-level webcam redirection and can redirect webcams only using USBR. Based on internal testing and validation, HP has found that the performance of a webcam connected through basic USBR performs poorly. HP does not recommend the use of this configuration and suggests that customers who require this function test using x86 units with RTAV technology to ensure satisfactory levels of performance. With USBR, the webcam might perform poorly or not at all. See [RDP USB redirection on page 32](#) for more information.

VMware Horizon View COM port redirection

To enable COM port redirection for VMware Horizon View connection:

- Set `root/ConnectionType/view/general/enableComPortRedirection` to 1 in regeditor.


 **NOTE:** By default, this setting is enabled.


Changing the VMware Horizon View protocol

VMware Horizon View Client can use either the PCoIP, RDP, or BLAST protocol.

To change the protocol:

1. In VMware Horizon View Client, select a pool that supports one of the supported protocols.
2. Under the **Connection** menu, select **Settings**.
3. Change the protocol by using the drop-down box next to **Connect Via**.

 **NOTE:** Use VMware Horizon View Manager to set which protocol should be used for each desktop pool.

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

VMware Horizon View HTTPS and certificate management requirements

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

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

- Use Certificate Manager to import the certificate from a file or URL.

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

The following table describes certificate trust when the security level is set to **Refuse insecure connections**.

Table 5-25 Refuse insecure connections

Certificate trust	Result
Trusted	Trusted
Self-signed	Error
Expired	Error
Untrusted	Error

The following table describes certificate trust when the security level is set to **Warn**.

Table 5-26 Warn

Certificate trust	Result
Trusted	Trusted
Self-signed	Warning
Expired	Warning
Untrusted	Error

The following table describes certificate trust when the security level is set to **Allow all connections**.

Table 5-27 Allow all connections

Certificate trust	Result
Trusted	Trusted
Self-signed	Untrusted
Expired	Untrusted
Untrusted	Untrusted

The following table describes the connection behavior associated with each result.

Table 5-28 Connection behavior

Result	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

Web Browser

Web Browser per-connection settings

This section describes the settings that are available under various categories when editing a Web Browser connection.



NOTE: These settings affect only the connection you are currently configuring.

Configuration

The following table describes the settings that are available under the Configuration category when editing a Web Browser connection.

Table 5-29 Configuration

Option	Description
Name	The connection name.
URL	The URL for the connection.
Intended Use	Lets you specify how USB redirection is performed when the Web Browser connection starts. Select Citrix , RDP , or Internet .
Allow smartcard login	Allows you to use smart-card authentication for a connection if you select a URL or icon that starts a remote connection.
Enable kiosk mode	Enables kiosk mode.
Enable full screen	Uses full screen mode for the connection.
Enable print dialog	Enables the print dialog box.

Preferences

Use these options to configure the Web Browser. These options can be shared by multiple Web Browser connections or be specific to a single connection.

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

AVD (Azure Virtual Desktop)

AVD (Azure Virtual Desktop) is part of the Microsoft Azure[®] system and provides access to cloud-based remote desktops and remote applications. The AVD client for ThinPro is an add-on that you can obtain from ThinUpdate or Easy Update. Restart after you install AVD to create AVD connections. In Addition to AVD, the AVD client also supports Windows 365[®]. For the Zoom UC optimization plugin for ThinPro, see the Zoom website.

AVD per-connection settings

This section describes the AVD per-connection settings.



NOTE: These settings affect only the connection that you are currently configuring.

Configuration

The following table describes the settings that are available under the **Configuration** category when you edit a AVD connection.

Table 5-30

Option	Description
Name	The connection name.
Workspace URL	The URL for the connection. For example, https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery .
Credentials	<ul style="list-style-type: none">• Ask for credentials at connection start.• Use predefined user, password, and domain.
Username	The user name for this connection.
Password	The password for this connection.
Domain	The domain for this connection.

Window

The following table describes the settings that are available under the **Window** category when editing an AVD connection.

Table 5-31

Option	Description
Window Size	<p>Sets the Window Size to one of the following:</p> <p>Full-desktop: The remote session is launched in full screen mode and covers all monitors that are connected to the client.</p> <p>Fullscreen: The remote session is launched in full screen mode on the primary screen only.</p> <p>Maximized: The remote session is launched in full screen mode on the primary screen only, leaving space for the taskbar.</p> <p>If Hide window decorations is selected, all window decorations of the fixed sized window are removed, including title bar and window borders.</p> <p>Fixed: The remote session is launched in a fixed-sized window.</p> <p>Fixed/Width: Sets width of the fixed-sized session window.</p> <p>Fixed/Height: Sets height of the fixed-sized session window.</p>



NOTE: You open AVD remote applications within a single ThinPro window. You can minimize or resize applications within this window. Use **Alt+Tab** to cycle through the active applications.

Options

The following table describes the settings that are available under the Options category when you edit an AVD connection.

Table 5-32 AVD connection options and their descriptions

Option	Description
Autofill credentials	Autofills credentials into login page.
Headless mode	Autofills credentials into hidden login page.
Remember me	Creates encrypted token cache so that web authentication dialog is not required on every launch.
Forget Me	Clears the encrypted token cache that is created when Remember me is selected.
Autostart Workspace	Specifies the workspace from which a resource starts automatically (optional).
Autostart Resource	Specifies the name of a resource to be started automatically.
Autoclose AVD Feed Window	Automatically closes an AVD feed window when a session window is closed.
Set local time zone	Sets remote session time zone from the local system's time zone.
Disable the menu bar	Disables the menu bar in the session window.

Table 5-32 AVD connection options and their descriptions (continued)

Option	Description
Disable the dropdown bar	Disables the drop-down bar that appears when the session window is fullscreen.
Close button	Enables the Close button on drop-down bar.
Minimize button	Enables minimize button on the drop-down list.
Maximize button	Enables maximize button on the drop-down list.
Ctrl+Alt+D	Adds Ctrl+ Alt+Delete to list of keyboard shortcuts on the drop-down list.

Local Resources

The following table describes the settings that are available under the Local Resources category when editing an AVD connection.

Table 5-33

Option	Description
Audio Output	Determines whether audio output is redirected.
Audio Input	Determines whether audio input is redirected.
Filesystem	Determines whether removable storage is redirected.
Smart Cards	Determines whether smart cards are redirected.
Clipboard	Determines whether clipboard is redirected.
Virtual Channel Plugins	Determines whether virtual channel plugins are enabled or disabled. Must be enabled for Zoom UC optimization plugin.
Camera	Determines whether camera is redirected.

TTerm

Because TTerm is not included with the base image, you must download it and install it separately.

To install the TTerm package:

1. Download `thinpro-tterm-<version>.xar`, and copy it to ThinClient.
2. Install the `.xar` package.
3. Restart.

To configure and use TTerm connection:

1. Right-click the desktop, select **Create**, select **Other**, and select **TTerm**, which creates a TTerm connection on the desktop.
2. Right-click the **TTerm Connection**, select **Edit**, and then edit the connection.

Configuration

The following table describes the settings that are available under the Configuration category when editing an TTERM connection.

Table 5-34 Configuration options

Option	Description
Name	The connection name.
Open Profile Directory	It opens TTerm Linux Profile Directory to create, modify, and delete profiles.
Profile(s)	<p>Set the profile or profile named list.</p> <p>Examples:</p> <ul style="list-style-type: none">Start a session with profile name default: Set the value to default.Start a session with profile named New profile and two sessions with profile named default: Set the value to New profile default default.
Monitor settings	<p>Full screen: TTerm opens in Full screen mode.</p> <p>Maximized: TTerm opens in maximized mode.</p>
View configuration	<ul style="list-style-type: none">Enable Menu barEnable ToolbarEnable status barEnable session panel

Additional connection types (ThinPro only)

This section describes the settings that are available under various categories when editing additional connection types.



NOTE: By default, these connection types are not available in Smart Zero. For more information, see [Choosing an OS configuration on page 1](#).

XDMCP

This section describes the settings that are available under various categories when editing an XDMCP connection.



NOTE: These settings affect only the connection you are currently configuring.

Configuration

The following table describes the settings that are available under the Configuration category when editing an XDMCP connection.

Table 5-35 Configuration

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

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

Secure Shell

This section describes the settings that are available under various categories when editing a Secure Shell connection.



NOTE: These settings affect only the connection you are currently configuring.

Configuration

The following table describes the settings that are available under the Configuration category when editing an SSH connection.

Table 5-36 Configuration

Option	Description
Name	The connection name.
Address	The IP address of the remote system.
Port	The remote port to use for the connection.
User name	The username to use for the connection.
Run application	The application to run to make the connection.
Compression	Select this option if you want to compress the data sent between the server and thin client.
X11 connection forwarding	If the server has an X server on it, select this option to allow the user to open user interfaces from the SSH session and display them locally on the thin client.
Force TTY allocation	Select this option and specify a command to initiate a temporary session to run the command. Once the command has completed, the session will terminate. If no command is specified, then the session will run normally as if the option were not selected.
Foreground color	The default color of the text in the SSH session.

Table 5-36 Configuration (continued)

Option	Description
Background color	The default color of the background in the SSH session.
Font	Valid options are: 7X14, 5X7, 5X8, 6X9, 6X12, 7X13, 8X13, 8X16, 9X15, 10X20, and 12X24.

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

Telnet

This section describes the settings that are available under various categories when editing a Telnet connection.



NOTE: These settings affect only the connection you are currently configuring.

Configuration

The following table describes the settings that are available under the Configuration category when editing a Telnet connection.

Table 5-37 Configuration

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

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

Custom

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



NOTE: These settings affect the connection you are currently configuring only.

Configuration

The following table describes the settings that are available under the Configuration category when editing a Custom connection.

Table 5-38 Configuration

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

Advanced

This section references where you can find information about Advanced connection settings under the Advanced category, when editing a connection.



NOTE: See [Advanced connection settings on page 16](#) for information about the settings available under the Advanced category when editing a connection.

6 HP True Graphics

HP True Graphics offloads rich multimedia content to the thin client's GPU, delivering high-frame-rate images and boosting efficiency.

Server-side requirements

See the following table for a list of supported server-side products of the independent software vendor (ISV) you are using for your virtual desktop infrastructure (VDI).

Table 6-1 Server-side requirements

ISV	Supported products
Citrix®	XenApp®/XenDesktop® 7.0 or newer IMPORTANT: The Citrix server must support sending session data in H.264 format (a Citrix technology known as SuperCodec). H.264 is enabled by default and is processed using the DeepCompressionV2 encoder, a CPU-based compression algorithm.
VMware®	VMware Horizon™ 6.0 and newer VMware Horizon View™ 5.2 and 5.3 VMware View® 5.1

Client-side requirements

See the following table for a list of supported thin client operating systems and supported client-side software from the ISV you are using for your VDI.



 **NOTE:** HP True Graphics are not available with a Trial ThinPro license.

Table 6-2 Client-side requirements

Supported operating systems	Supported Citrix clients	Supported VMware clients
HP ThinPro 5.0 and newer	Citrix Receiver 13.1.1 and newer NOTE: A version of Citrix Receiver that supports HP True Graphics is preinstalled starting with HP ThinPro 5.2 and is available as an add-on for HP ThinPro 5.0 and 5.1.	VMware Horizon Client 4.0 and newer (using the Blast protocol)

Client-side configuration

This section describes the client-side configuration.

 **NOTE:** The information in this section applies to Citrix only. For VMware, simply use the Blast protocol to enable HP True Graphics.

Compression settings

To enable HP True Graphics on HP ThinPro:

- Select the **Enable H264 Compression** general setting for Citrix connections.



NOTE: Some screen data, such as text, might be sent using methods other than H.264. In general, it is best to keep this feature enabled, but for troubleshooting or specific use cases, the following registry keys can be set to **0** to disable this feature:

- `root/ConnectionType/xen/general/enableTextTracking`
- `root/ConnectionType/xen/general/enableSmallFrames`

Window settings

To force remote applications to run in windowed mode:

- Set the **TWI Mode** general setting for Citrix connections to **Force Seamless Off**.

Monitor layout and hardware limitations

Consider the following limitations on monitor layout:

- Most configurations with a maximum of two monitors that have a 1920 × 1200 resolution are supported.
- HP t630 Thin Client: This model supports a maximum of two monitors at 1920 × 1200 or one monitor at 3840 × 2160.
- HP t730 Thin Client: This model supports a maximum of three monitors at 1920 × 1200.
- Rotated monitors might not display correctly.
- If you are using HP True Graphics with two monitors and trying to play a video using HDX MediaStream, the video will fail because H.264 supports only two hardware decode sessions, which are being consumed by the monitors.



NOTE: HDX MediaStream is also trying to leverage local hardware decoding of H.264, which causes the issue.

Tips & best practices

Consider the following when using HP True Graphics:

- After connecting to a remote desktop, you can use Citrix HDX Monitor to determine which encoder is being used for the session by examining the **Component_Encoder** value under the **Graphics - Thinwire Advanced** section. If the value reads **DeepCompressionV2Encoder** or **DeepCompressionEncoder**, then the server is properly sending the data in a format that is accelerated by HP True Graphics.



NOTE: If legacy graphics are being forced via a server policy, such as **CompatibilityEncoder** or **LegacyEncoder**, the server is compressing graphics in a method that is compatible with older versions of Citrix clients, and HP True Graphics will not provide enhanced performance.

- HP True Graphics might provide some benefits to older versions of XenDesktop if using HDX 3D Pro. Benefits are not provided if HDX 3D Pro is used with the visual quality set to **Always Lossless**, because then the graphical information is not sent to the thin client in H.264 format.

7 Active Directory integration

By using Active Directory integration, you can force users to log in to the thin client using domain credentials. Optionally, those credentials can be encrypted and stored and then later supplied to remote connections as they start, which is a process known as single sign-on.



NOTE: Enabling authentication requires no special domain permissions.

There are two modes in which Active Directory integration can operate. By simply enabling authentication against the domain, domain credentials can be used for the following operations:

- Logging in to the thin client
- Starting a connection using Single Sign-On
- Switching to administrator mode using administrative credentials
- Unlocking a locked screen using the login credentials
- Overriding a locked screen using administrative credentials

The thin client can also be formally joined to the domain. This adds the thin client to the domain's database and might enable dynamic DNS, where the thin client informs the DNS server of changes in its IP address or hostname association. Unlike domain authentication, a formal join requires credentials of a domain user authorized to add clients to the domain. Joining to the domain is optional. All domain functions except dynamic DNS are available without joining.

Login screen

When domain authentication is enabled, ThinPro displays a domain login screen upon startup. The login screen also includes options that might be necessary to configure before logging in.

The background desktop layout, login dialog style, login dialog text, and which buttons are available can all be adjusted via registry settings and/or configuration file settings. For more information, see the HP ThinPro white paper *Login Screen Customization* (available in English only).

If the system detects that the user tried to log in with expired credentials, they are prompted to update their credentials.


Single sign-on

After a domain user has logged in, the credentials that were used can also be presented at startup to any connection configured to use them. This allows a user to sign in to the thin client and start Citrix, VMware Horizon View, and RDP sessions without having to enter their credentials again, for as long as they are logged in to the thin client.

Desktop

Once the user has successfully logged in using domain credentials, an Active Directory icon is available on the taskbar. The user can select the icon to perform the following functions:

- Show who is logged in to the system
- Lock the screen
- Change the domain password

 **NOTE:** Domain password changes from ThinPro can fail for various reasons. Here are a couple of known failure modes:

Password changes can fail if you have the following options enabled in the AD Security policies:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security\Minimum session security for NTLM SSP based (including secure RPC) clients

Require NTLMv2 session security

Require 128-bit encryption

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security\Minimum session security for NTLM SSP based (including secure RPC) server

Require NTLMv2 session security

Require 128-bit encryption

Minimum Password Age Policy not set to 0:

GPO Default Domain Policy Comp Config\Policies\Windows Setting\Security Settings\Account Policies>Password Policy\Minimum password age:

Setting this value to 0 might help workaround the limit but likely is not acceptable with the customer.

The customer must use alternative AD practices to help end users change an expired password in those scenarios.

Screen lock

The screen can be locked due to inactivity timeout or through manual locking. If the screen was locked by a domain user, the unlock dialog expects the user to provide the same domain password they used to log in. Like the login dialog, there are options provided, plus one additional function: screen unlock. If the screen-unlock button is selected, the unlock screen instead requires the root (administrator) password or any set of domain credentials in the domain admin group, which was designated during domain authentication setup. When the user supplies override credentials, the screen does not return to the desktop; it instead returns to the login screen.

Administrator mode

In addition to the traditional method of using the root password to enter administrator mode, the domain credentials of a user in the designated domain administrator group can be used to switch to administrator mode.

Settings and the domain user

When a domain user is logged in, any changes to settings are saved in a registry layer that applies only to that user. This includes newly created connections.

If the user has made no changes to system settings or connections, the system defaults will apply instead.

When the system is changed to administrator mode, settings and connection changes are no longer being made to the user-specific layer of the registry. Instead, while in administrator mode, all changes apply instead to the base-level registry. In that way, a change to a setting while in administrator mode applies to all users unless there is a user-specific, custom setting already specified.

8 Start menu

To open the Start menu, select **Start**.

Connection management

The menu lists all the available connections. Right-click the connection name to manage that connection or select it to start the connection. If the connection is running, selecting it stops the connection.

For more information on connection management, see [Desktop connection management on page 14](#).

Switch to Administrator/Switch to User

This option allows you to switch between administrator mode and user mode.

System Information

This option starts the System Information application.

For more information, see [System Information on page 84](#).

Control Panel

This option starts Control Panel.

For more information, see [Control Panel on page 59](#).

Tools

There are many system tools provided, including one to start programs, such as a text terminal, or to run the Initial Setup Wizard a second time. If you are logged in as a user, only authorized tools are displayed. If this list is empty, the Tools menu entry is hidden.

Table 8-1 Tools

Menu option	Description
X Terminal	Lets you execute Linux commands.
Wireless Statistics	Lets you view information about wireless access points.
Check for Updates	Searches for updates from the server.
Text Editor	Opens a basic text editor for viewing and editing text files.
Task Manager	Lets you monitor the CPU usage and the CPU usage history for the thin client.
Snipping Tool	Lets you take a snapshot of a rectangular selection of the screen, a specific window, or the entire screen.
Registry Editor	Opens the ThinPro Registry Editor.

Table 8-1 Tools (continued)

Menu option	Description
Initial Setup Wizard	Starts the Initial Setup Wizard.
Compatibility Check	Runs the ThinPro Compatibility Check tool, which assesses the system's suitability for running ThinPro.

Power

These options allow you to log out, shut down the computer, restart the computer, or enable the Sleep state.

An administrator can restrict the options visible to a user using the Power Manager tool. See [System on page 59](#).

Search

When you type in the search box, a set of potential matches for your search are displayed from most likely to least likely. The search includes the visible names of controls, tools, and connections and associated aliases and synonyms. For example, in administrator mode, typing `encryption` displays the Security control, because that control offers encryption parameters.

To see all available options, type a space in the search box or select the magnifying glass icon.

Search also returns the options to create new connections of all available types. This can be used to manage connections.

9 Control Panel

Control Panel lets you modify the system configuration.

Opening Control Panel

To open control panel:

- Select **Start**, and then select **Control Panel**.



NOTE: You can also search for a specific Control Panel function using the Start menu search box.



NOTE: All Control Panel items are accessible in administrator mode. In user mode, only Control Panel items that are enabled by the administrator for use by users are accessible.



TIP: To specify which Control Panel items end users have access to, open Control Panel, select **Appearance**, select **Customization Center**, and then select or clear items in the **Applications** list.

System

This section describes the system configuration.

Table 9-1

Menu option	Description
Date and Time	Lets you configure the time zone and the date and time options.
Network	Lets you configure network settings. For more information, see Network settings on page 60 .
DHCP Options	Lets you configure DHCP options. For more information, see DHCP options on page 65 .
Power Manager	Lets you configure power management settings such as a screen saver and screen lock, CPU settings, when to turn off the display, and when to enter the Sleep state. In administrator mode, you can restrict access to power-related options (such as Reboot) on a system-wide basis.
Imprivata Setup	Lets you enable Imprivata Appliance Mode and specify an Imprivata server, see Imprivata Setup on page 65 .
Component Manager	Lets you remove system components. For more information, see Component Manager on page 66 .
Factory Reset	Lets you restore the thin client to its default factory configuration.
Snapshots	Lets you restore the thin client to a previous state or to its default factory configuration.

Network settings

Network settings can be configured using Network Manager.

Opening Network Manager

To open the Network Manager:

- Select **System** and then select **Network** in Control Panel.

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

Wired network settings

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

Table 9-2 Wired network settings

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

Wireless network settings

Use this tab to add, edit, and delete wireless profiles that correspond to wireless networks.

The following tables describe the options available when adding or editing a wireless profile.



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



TIP: You can also access these settings by selecting the network status icon in the taskbar.

Use the **Wireless** tab to configure general settings.

Table 9-3 Wireless network settings

Option	Description
Scan AP	Scans for available wireless networks.
SSID	Use this box to manually enter the SSID of the wireless network if it is not found by the scan.
Wireless Band	Select Auto , 2.4GHz , or 5GHz .
SSID Hidden	Enable this option if the SSID of the wireless network is set to be hidden (not broadcasting).
Enable IPv6	Enables IPv6. IPv4 is used by default, and they cannot be used at the same time.
Enable Power Management	Enables the power management feature for the wireless adapter.
Connection Method	<p>Lets you select between Automatic and Static. If your network environment is using DHCP, then the Automatic option should work without any further configurations.</p> <p>If Static is selected, the Static Address Configuration settings will become available. Be sure to input these values according to whether you are using IPv4 or IPv6.</p>
Security Settings	<p>Lets you set the authentication setting to one of the following:</p> <ul style="list-style-type: none">• None• WEP• WPA3/SAE• WPA/WPA2-PSK• 802.1X-TTLS• 802.1X-PEAP• 802.1X-TLS• EAP-FAST <p>For WEP and WPA/WPA2-PSK, you just need to enter the network key and select OK.</p> <p>For EAP-FAST, set Anonymous Identity, Username, Password, and Provisioning Method. You do not need to change the PAC file settings.</p> <p>See Wired network settings on page 60 for more information about TTLS, PEAP, and TLS.</p>
Auto Connect	This option is reserved for future use.
Enable Wireless	Enables the wireless adapter.

Use the **IPv4** tab to configure IPv4 connection settings.

Table 9-4 IPv4 connection settings

Option	Description
IPv4 Enabled	Enables IPv4.
IPv4 Method	<p>Lets you select between Automatic and Static. If your network environment is using DHCP, then the Automatic option should work without any further configurations.</p> <p>If Static is selected, the Static Address Configuration settings are displayed, and you must enter the IPv4 settings.</p>

Use the **IPv6** tab to configure IPv6 connection settings.

Table 9-5 IPv6 connection settings

Option	Description
IPv6 Enabled	<p>Enables the usage of an IPv6 global address.</p> <p>NOTE: HP ThinPro tries to obtain an IPv6 global address via route advertisement or DHCPv6.</p>
IPv6 Method	<p>Lets you select between Automatic and Static. If your network environment is using DHCP, then the Automatic option should work without any further configurations.</p> <p>If Static is selected, the Static Address Configuration settings are displayed, and you must enter the IPv6 settings.</p>

Use the **Security** tab to configure the connection security settings.

Table 9-6 Connection security settings

Option	Description
Authentication	<p>Lets you set the authentication setting to one of the following:</p> <ul style="list-style-type: none"> • None • WEP • WPA/WPA2-PSK • WPA/WPA2 Enterprise-TTLS • WPA/WPA2 Enterprise-PEAP • WPA/WPA2 Enterprise-TLS • EAP-FAST <p>For WEP and WPA/WPA2-PSK, you just need to enter the network key and select OK.</p> <p>For EAP-FAST, set Anonymous Identity, Username, Password, and Provisioning Method. You do not need to change the PAC file settings.</p> <p>See Wired network settings on page 60 for more information about TTLS, PEAP, and TLS.</p>

Cellular settings

Use this tab to configure Cellular settings and manage Access Point Names (APNs). This tab is only shown when a supported cellular modem is detected on a limited group of HP Mobile Thin Client models,

for example, if an Intel XMM 7560 modem module is detected on a HP mt645. The list of supported cellular modems is extended as new cellular modems are supported.



NOTE: If no SIM card is detected in the SIM card slot, a SIM card logo with a back slash is shown to indicate that no SIM is present. User must insert a SIM card and continue to view and edit Cellular Settings.



NOTE: If the inserted SIM card is in the Locked state, a SIM logo with a padlock is shown to indicate the SIM card is in Locked state. You must enter the Personal Identification Number code (PIN) to unlock the SIM card and continue to view and edit Cellular Settings.



NOTE: Like other Network settings, you cannot access Cellular settings from the Control Panel. There is a Cellular Settings entry in the Network Manager system tray menu by default, and you can access Cellular settings from Network Manager system tray menu. If administrators need to limit users from accessing Cellular settings, they can set registry key `root/Network/WWAN/UserCanManageWwanConn` to 0 and the entry disappears.



TIP: You can unlock the SIM card from the Network settings system tray menu.

Table 9-7 Enable Cellular

Option	Description
Enable Cellular	An administrator can decide to enable or disable Cellular on this device.

Table 9-8 Cellular Information

Option	Description
Carrier	Read-only. The name of the mobile carrier retrieved from the SIM card.
Country	Read-only; the country retrieved from the SIM card.
IMSI	International Mobile Subscriber Identification Number, a number to identify the subscriber.

Use the Connections settings table to configure Cellular connection settings, when the SIM card is available. The following table describes the options available for a connection:

Table 9-9 Connection settings

Option	Description
Default Cellular Connection	Use this check box to select the only active connection among all connections.
Data Roaming	Use this check box to enable data roaming.
IP Type	Select IPv4 , IPv6 , or IPv4/IPv6 .
APN	Select an Access Point Name from the list of APNs provided by APN settings . See APN settings for more information.

Select the **APN Manager** button to open APN settings. If the SIM card can be recognized from a known mobile carrier, some APNs are populated automatically to create, edit an APN. The following table describes the options available for an APN.

Table 9-10 APN settings

Option	Description
Name	The name used to represent an APN in Connections settings .
APN	The Access Point Name used by the mobile carrier.
Username	The user name used by the mobile carrier.
Password	The password used by the mobile carrier.

Command to upgrade Cellular Modem's Firmware

```
hptc-modem-update [options] <list of firmware files>
```

<list of firmware file>: A list of firmware and CustPack files separated by spaces.

The command also provides the firmware upgrade result. When the upgrade is successful, a restart dialog box opens and you can select whether to restart. If you do not choose the restart option, the unit will restart after the default restart timer runs out. If the upgrade fails, the command prints a **PLEASE TRY TO FLASH AGAIN** message.

If upgrading the firmware fails, use option `-d` and run the command `hptc-modem-update -d <list of firmware files>`. This command generates debug log `/var/log/fw.log` while upgrading firmware. The log is helpful for analyzing the reason for the failure.

General settings

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

Table 9-11 General settings

Option	Description
Hostname	The hostname is generated automatically according to the MAC address of the thin client. You can alternatively set a custom hostname.
Proxy Mode	Use this option so enable or disable proxy settings.
Use the same proxy for all	Use HTTP Proxy setting for all other proxy settings.
HTTP Proxy	Use these boxes to set proxy server information using the following format:
FTP Proxy	<code>http://<address>:<port></code>
HTTPS Proxy	HP recommends using the <code>http://</code> prefix for all three proxy settings because it is supported better. NOTE: The proxy settings are set to the <code>http_proxy</code> , <code>ftp_proxy</code> , and <code>https_proxy</code> environmental variables for the system.
Socks proxy	Use this box to set proxy server information using the following format, even when Use the same proxy for all is selected: <code>socks5://<address>:<port></code> NOTE: The proxy setting is set to the <code>all_proxy</code> environmental variable for the system.

Table 9-11 General settings (continued)

Option	Description
Ignore Hosts	This setting is a list of addresses to be ignored by proxy settings.

DHCP options

How to configure and manage DHCP options.

Opening the DHCP Option Manager


To open the DHCP Option Manager:

- Select **System** and then select **DHCP Options** in Control Panel.

Request or ignore DHCP options

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

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

 **TIP:** The drop-down list allows you to filter which DHCP tags are displayed.


- Select or deselect the check boxes in the **Requested** column.

Changing a DHCP code

To change a DHCP code:

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

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

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


Information about DHCP options

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

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

Imprivata Setup

The following two packages are included with ThinPro.

 **IMPORTANT:** As of September 2023, the first released build of the ThinPro 8.1 image does not include the Imprivata mode by default. It will be available soon via a next ThinPro Service Pack after it is supported again by Imprivata and HP.

- Imprivata OneSign Bootstrap loader: onesign-bootstrap-loader or onesign-generic-bootstrap-loader
- HP Imprivata helper scripts (vendor launch scripts): hptc-imprivata-helper

When Imprivata Appliance Mode is enabled, the OneSign Bootstrap loader connects on the specified Imprivata OneSign server and installs or updates the Imprivata ProvelD Embedded agent (PIE agent).


The Imprivata ProvelD agent is installed into the directory `/usr/lib/imprivata/runtime/`.

The Imprivata ProvelD agent uses the HP helper scripts to launch a VDI client. A VDI client is either a Citrix, a VMware, or an RDP client.

The HP helper scripts are installed in the directory `/usr/lib/Imprivata-helper/`.

The Imprivata agents use two log files:

- `/usr/lib/imprivata/runtime/log/OneSign.log`
- `/usr/lib/imprivata/runtime/log/OneSignAgent.log`

 **NOTE:** More information can be found at <http://documentation.imprivata.com>.

 **NOTE:** Verify that the certificate of the Imprivata OneSign server is valid on ThinPro. You might have to install it or its Root CA certificate. See [Certificate Manager on page 69](#).


To open the Imprivata Setup:


- Select **System** and then select **Imprivata Setup** in Control Panel.

Component Manager

Component Manager lets you remove system components that are not used in your environment, which might be desirable to reduce the image size or increase security. For example, if Citrix connections are never used in your environment, you might want to remove the Citrix component.

As components are removed, the new configuration can be tested before you apply the changes permanently. You can also undo changes that were made, if the changes have not yet been applied permanently.

 **IMPORTANT:** After the new configuration is applied permanently, all snapshots are removed and a new factory snapshot is created. Removed components cannot be restored after this point.

 **NOTE:** Removing components might not reduce the use of local disk space, but it should reduce the size of any disk images created from the local system.

To open the Component Manager:

Opening Component Manager


To open Component Manager:

- Select **System** and then select **Component Manager** in Control Panel.

Removing components

To remove components:

1. In the Component Manager, select the desired components.

 **TIP:** To select multiple components, use **Ctrl** or **Shift**.

2. Select **Remove Component(s)**.

3. If the confirmation dialog appears, select **OK**.
4. After the components are removed, test the new configuration.


Undoing a change

You can undo each change, one at a time, if the changes have not yet been applied permanently. A restart of the thin client is required after each undo.

To undo a change made with the Component Manager:


1. In the Component Manager, select **Revert Last Change**.
2. Select **Yes** to restart the thin client.

Repeat this process for as many changes you want to undo.

 **IMPORTANT:** If you take a snapshot of the image while testing a new configuration, you cannot undo the changes via the Component Manager. Those changes can be undone only by restoring a previous snapshot via the Snapshots tool. However, this does not work if the changes have already been applied permanently, because that function deletes all existing snapshots. If changes have already been applied permanently, you must reinstall the operating system to restore most removed components. Some components (such as Citrix, RDP, and VMware Horizon View) might be available as add-ons on the web and can be restored by reinstalling them.

Applying the changes permanently

To apply changes made with the Component Manager permanently:

 **IMPORTANT:** After the new configuration is applied permanently, all snapshots are removed and a new factory snapshot is created. Removed components cannot be restored after this point.

1. In the Component Manager, select **Apply Component Configuration**.
2. Select **Yes**.

Security

This section describes the Security configuration.

Table 9-12

Menu option	Description
Security	For more information, see Security settings on page 68 .
Change Domain Password	If a domain is being used, lets you change the domain password.
Certificates	Opens Certificate Manager, which lets you easily import, view, or remove certificates. For more information, see Certificate Manager on page 69 .
Firewall Manager	Lets you configure firewall settings.
SCEP Manager	Allows for network-based certificate management.

Security settings


Security settings can be configured using Security Manager. To open Security Manager, select **Security** and then select **Security** in Control Panel.

See the following sections for more information about the different tabs in Security Manager.


- [Local Accounts on page 68](#)
- [Encryption on page 68](#)
- [Options on page 69](#)

Local Accounts

The Local Accounts tab can be used to change the local root and user account passwords or to disable authentication using those accounts.

 **CAUTION:** Disabling the root and/or user accounts might leave your system in an unusable state unless Active Directory authentication is enabled. For example, if the root account is disabled, you will only be able to change to administrator mode using domain credentials of an administrator. However, disabling the local accounts might improve security when Active Directory authentication is enabled because you no longer have to maintain and update a shared secret such as the thin client's root password.

If Active Directory authentication has been used and there is any cached data for domain users on the thin client, you can also delete the user's cached data from this tab.

 **NOTE:** If the user logged in using a domain account, they cannot delete their own account's data because it would leave the system in an indeterminate state.

Encryption

Active Directory credentials and other secrets can be hashed for functions like screen-unlock and/or encrypted and stored on the system for single sign-on.

The hash algorithm for creating a password's hash can be selected from this menu. The default, script, is a well-accepted key derivation function. Argon2, another key derivation function is also available, as well as conventional hashes SHA-256 and SHA-512. The advantage of a key derivation function is that it is computationally expensive to compute a rainbow table that matches plain-text passwords to precomputed hash values, whereas conventional hashes are meant to execute as fast as possible. All hashes are stored with 128 or more bits of random salt which changes each time the password hash is computed and stored.

Encrypted passwords are used in situations where they can be reversed and supplied to connections when they start (single sign-on). The encryption algorithm can be selected here from a wide variety supported by OpenSSL. Unless there is a good reason to select a different value, HP recommends using the default encryption algorithm, which is generally regarded as a modern, secure algorithm by the security community. The number of salt bits and key bits will vary from one algorithm to another and you can get details by pressing the info button next to the algorithm selector. Encryption keys are unique per thin client and are stored in a place that only administrators can read. Furthermore, only certain authorized applications on the system can do decryption.

Both hashes and encrypted secrets can be set with a time-to-live. If the amount of time between when the secret was hashed or encrypted and the time when it is used or decrypted exceeds the time-to-live, the hash-match or decryption will fail.

By default, the single sign-on password is usable for only one day, but any passwords stored with connection or network settings can be used indefinitely.

Options

Local user must log in: If this option is selected when Active Directory authentication is disabled, the login screen still appears at startup and logout. In this situation, the local user or root credentials must be used to gain access to the system.

Enable secret peek: If enabled, most password and secret entry fields on the system display a small eyeball icon on the right side. When that eyeball icon is selected by pressing and holding down the left mouse button, the secret is displayed in plain text as long as the mouse button is held down. As soon as the button is released, the secret is again obscured.

Use domain text entry: If enabled, a separate Domain input field is provided for the domain name where applicable. If disabled, the domain is determined by the value entered in the User field instead. For instance, if the User field contains "mike@mycorp", the domain is assumed to be "mycorp". If the user field is "graycorp\mary", the domain is assumed to be "graycorp".

Allow administrators to override screen lock: If enabled, you can override a locked screen and return it to the login screen or ThinPro desktop, just as if the user had manually logged out of the thin client.

Certificates

This section describes information about using certificates.



NOTE: For more information about using certificates in Linux, go to <https://www.openssl.org/docs/>.

Certificate Manager

To open Certificate Manager:

- Select **Security** and then select **Certificates** in Control Panel.

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

If desired, use Profile Editor to attach the certificate to a profile, as described in [Adding certificates to a client profile on page 91](#).



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

SCEP Manager

To open the SCEP Manager:

- Select **Security** and then select **SCEP Manager** in Control Panel.

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

During an enrollment or renewal, the SCEP Manager generates the thin client's private key and certificate request, and then it sends the request to the CA on the SCEP server. When the CA issues the certificate, the certificate is returned and placed in the thin client's certificate store. OpenSSL uses the certificate for connection verification.



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

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



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

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



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

SIM

This section describes how to manage a SIM Personal Identification Number (PIN) code. The tool is not present if a supported cellular modem is not found in the system or the cellular modem is disabled in the system. You must insert a SIM card into the SIM slot before you can manage a SIM PIN.



NOTE: You can access the SIM PIN from the Control Panel, and you can also access the SIM PIN management from a Manage SIM PIN entry in the Network Manager system tray menu. If administrators want to restrict users from accessing SIM PIN management, they can set registry key `root/users/user/apps/hptc-sim-mgr/authorized` to 0, and make the SIM entry disappear from Control Panel. They can also make the **Manage SIM PIN** entry disappear from the system tray menu.

The contents shown in the SIM Control Panel might vary, depending upon the state of the SIM card. This table shows the allow actions permitted for the four different states.

Table 9-13 SIM card states

State	Allowed actions
The SIM card is in Unlocked state	Lock the SIM card by creating a new PIN code.
The SIM card is in Locked state	Change the PIN code or remove the PIN code. You must have the correct PIN code to perform the actions.
The SIM card is in Locked state and incorrect PIN codes have been entered three times	Requires you to enter the PUK (PIN Unlocking Key) code. You must have the correct PUK code to create a new PIN code.
The SIM card is in Locked state and incorrect PIN codes have been entered three times; subsequently, incorrect PUK codes have been entered 10 times	A notice is displayed that says the SIM card is Locked permanently. You must ask your mobile carrier to unlock the SIM card for you.

Manageability

This section describes the Manageability configuration.

Table 9-14

Menu option	Description
Active Directory	For more information, see Active Directory configuration on page 71 .

Table 9-14 (continued)

Menu option	Description
Automatic Update	Lets you configure the Automatic Update server manually. For more information, see HP Smart Client Services on page 85 .
Easy Update	Launches HP Easy Tools. For more information, see the user guide for HP Easy Tools.
HPDM Agent	Lets you configure the HP Device Manager (HPDM) Agent. For more information, see the <i>Administrator Guide</i> for HPDM.
HPCEM Agent	Lets you configure the HP Cloud Endpoint Manager (HPCEM) Agent. For more information, see the <i>Administrator Guide</i> for HPCEM.
SSHD Manager	Enables access through a secure shell.
ThinState	HP ThinState lets you make a copy of or restore the entire operating system image or just its configuration settings. For more information, see HP ThinState on page 72 .
VNC Shadow	Lets you configure VNC Shadowing options. For more information, see VNC Shadowing on page 76 .

Active Directory configuration

Status tab

This control lets you activate or deactivate authentication against a domain, joining the domain, and various domain-related options.

After you make a change to domain parameters on the Status tab, the page shows a pending action and you must select **Apply** to make that action happen. Joining or unjoining the domain requires credentials with permissions to perform that operation. After enabling authentication or joining the domain, some of the sub-parameters might be marked as read-only because it is not possible to change them at that point in time. Instead, you must unjoin or disable authentication altogether and then apply the changes. Then you can re-enable authentication or join with altered sub-parameters.

Table 9-15 Status tab

Option	Description
Domain name	If the thin client can determine the domain name using DHCP options, it will be displayed here. Otherwise you will have to enter the fully-qualified domain name manually.
Authenticate against domain	When enabled, domain credentials can be used, as outlined in the Active Directory Integration section of this guide.

Table 9-15 Status tab (continued)

Option	Description
Require thin client login	This is on by default, and it causes the system to boot up into the domain login screen. If disabled, domain credentials can still be used to switch to administrator mode or to override a locked screen, but single sign-on will not be available.
Workgroup	Usually this is auto-detected from information provided by network servers, but you can use this as a manual override if you have an unusual network topology.
Domain controllers	These are usually detected using DNS lookups, but you can specify them manually if your network is not supplying that information.
Join the thin client to the domain	As explained in the chapter on Active Directory Integration, this option lets you formally add the thin client to the Active Directory's databases.
Organizational Unit (OU)	The thin client is usually added to the "Computers" OU of the database, but you can manually enter a different value here if your database schema demands it.
Dynamic DNS	If enabled, the thin client will try to update the DNS server whenever its IP-address/hostname association changes.

Options tab

This section describes the Options within the Options tab.

Table 9-16

Option	Description
Enable single sign-on	If enabled, a password supplied at login is encrypted and saved on the system. When a connection starts with SSO credentials configured, it can decrypt the password and pass it to the connection so that it can be used for remote login.
Domain login group	If enabled, login is restricted to users in the listed domain group.
Domain admin group	If enabled, escalation to administrator mode and screen-lock override is limited to members of the listed domain group.
Enable cached domain login	If enabled, a hash of the user's password is saved on the system and can be used for login even when the Active Directory server is inaccessible.
Retain user preferences at logout	If this option is enabled, any setting changes made by a domain user are stored in a place where those settings are applied only to that user. If this option is disabled, any such user-specific changes are discarded when the user logs out.
Allow domain password changes	If enabled, expired passwords result in a prompt that allows the user to update their password, and they can manually update their password using the user icon on the taskbar.


HP ThinState

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

Managing an HP ThinPro image

Capturing an HP ThinPro image to an FTP server


To capture an HP ThinPro image to an FTP server:

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

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

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

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


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

6. Select **Finish**.

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

Deploying an HP ThinPro image using FTP or HTTP

To deploy an HP ThinPro image using FTP or HTTP:


 **IMPORTANT:** If you stop a deployment before it is finished, the previous image is not restored and the contents of the USB flash drive of the thin client will be corrupted.

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

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


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

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

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

Capturing an HP ThinPro image to a USB flash drive

To capture an HP ThinPro image to USB flash drive:

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

1. Select **Management > ThinState** in Control Panel.
2. Select **the HP ThinPro image**, and then select **Next**.
3. Select **make a copy of the HP ThinPro image**, and then select **Next**.
4. Select **create a bootable USB flash drive**, and then select **Next**.


The thin client restarts and then prompts you to enter a USB flash drive.

5. Insert a USB flash drive into a USB port on the thin client.
6. Select the USB flash drive, and then select **Finish**.


A new window displays the progress. If a problem occurs, select **Details** for information. The desktop reappears after the capture is complete.

Deploying an HP ThinPro image with a USB flash drive

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

 **IMPORTANT:** If you stop a deployment before it is finished, the previous image is not restored and the contents of the USB flash drive of the thin client will be corrupted. In this state, the thin client must be reimaged using a USB flash drive.

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

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


Managing a client profile

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

 **NOTE:** A client profile can also be preconfigured and deployed using Profile Editor and Automatic Update (see [Profile Editor on page 89](#) and [HP Smart Client Services on page 85](#) for more information).

Saving a client profile to an FTP server

To save a client profile to an FTP server:

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

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

3. Select **save the configuration**, and then select **Next**.
4. Select **on a FTP server**, and then select **Next**.
5. Enter the FTP server information in the fields.
6. Select **Finish**.

Restoring a client profile using FTP or HTTP

To restore a client profile using FTP or HTTP:

1. Select **Management > ThinState** in Control Panel.
2. Select **the HP ThinPro configuration**, and then select **Next**.
3. Select **restore a configuration**, and then select **Next**.
4. Select **on a remote server**, and then select **Next**.
5. Select either the FTP or HTTP protocol, and then type the server information in the fields.



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

6. Select **Finish**.

Saving a client profile to a USB flash drive

To save a client profile to a USB flash drive:

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

Restoring a client profile from a USB flash drive

To restore a client profile from a USB flash drive:

1. Insert the USB flash drive containing the profile into a USB port on the target thin client.
2. Select **Management > ThinState** in Control Panel.
3. Select **the HP ThinPro configuration**, and then select **Next**.
4. Select **restore a configuration**, and then select **Next**.

5. Select **on a USB key**, and then select **Next**.
6. Select the USB key.
7. Select **Browse**.
8. Double-click the desired configuration file on the USB key.
9. Select **Finish**.

VNC Shadowing

To access the VNC Shadow tool:

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

To increase security, HP recommends leaving VNC disabled unless it is needed for remote diagnosis. Then, disable VNC when remote access to the thin client is no longer necessary.

- Select **Manageability** and then select **VNC Shadow** in Control Panel.



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

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

Table 9-17 VNC Shadowing

Option	Description
Enable VNC Shadow	Enables VNC Shadowing.
VNC Read Only	Makes the VNC session read-only.
VNC Use Password	Makes a password required when accessing the thin client using VNC. Select Set Password to set the password.
Show "Stop Shadowing" Button	If enabled, a Stop Shadowing button shows in the top left corner of the remote system. It stops VNC shadowing when pressed.
VNC Allow Loopback Only	If enabled, you can connect to the VNC server only from this thin client that is identified by the loopback address.
VNC Notify User to Allow Refuse	Enables a notification dialog on the remote system that informs the remote user when someone is attempting to connect using VNC. The user can refuse either allow or refuse access.
Automatically close the notification after (seconds)	Closes the User Notification Message after x seconds.
User Notification Message	Allows you to display a message in the notification dialog to the remote user.
Refuse connections in default	If enabled, the VNC connection will be refused by default when the timer expires.
Re-set VNC server right now	Resets the VNC server after applying the new settings.

SNMP

SNMP is a network protocol for collecting and organizing information about managed devices on networks and for modifying that information to change device behavior.

Three versions of SNMP have been developed. SNMPv1 is the original version, but SNMPv2c and SNMPv3 are more widely used. HP daemon supports all versions of SNMP protocols.

SNMP daemon behavior is defined by `/etc/snmp/snmpd.conf`. `snmpd.conf`, which supports many options. ThinPro's GUI offers limited support for these options, which might be useful in basic cases. You must provide your own `snmpd` configuration file if ThinPro GUI does not meet your needs. You must edit the `/etc/snmp/snmpd.conf` manually. You must also enable `root/snmp/agentBehaviour/usePrivateConfFile`, or the next apply will overwrite your configuration changes.



NOTE: SNMP is a highly extensible and customizable protocol. ThinPro provides a simple GUI tool to configure SNMP agent on ThinPro. Users can configure the SNMP agent that allows basic SNMP queries about the device. Users are encouraged to configure advanced SNMP features, for example, Extending private OID and Using SNMPv3.

Configuration file for the SNMP agent is `/etc/snmp/snmpd.conf` on ThinPro. See the man page of `snmpd.conf(5)` for details about configuring SNMP agent.

Enabling SNMP with Private Configuration File

You can enable SNMP with a Private Configuration File.

1. Select **Manageability > SNMP** in Control Panel.
2. Select **SNMP Enable** to enable SNMP agent on ThinPro.
3. Select **Use Private Configuration File**.
4. Copy the private configuration file to `/etc/snmp/snmpd.conf`.
5. Select **Apply** to start SNMP agent.

Enabling SNMP with Community List

You can enable SNMP with Community List.

1. Select **Manageability > SNMP** in Control Panel.
2. Select **SNMP Enable** to enable SNMP agent on ThinPro.
3. Deselect **Use Private Configuration File** if it is selected.
4. Select Add/Edit/Delete community to change SNMP v1/v2c communities in **Community List**, three attributes of a community can be configured.
 - Enter `name` of the community list in the field.
 - Select **Permission** to be Read-Only or Read-Write.
 - Enter `Accessible OID` of the community list in the field.
5. Select **Apply** to start SNMP agent.

Disabling SNMP

Follow the instructions to disable SNMP.

1. Select **Manageability > SNMP** in Control Panel.
2. Clear **SNMP Enable** to disable SNMP agent on ThinPro.

3. Select **Apply** to stop SNMP agent.

Capsule Update

ThinPro supports capsule update. You must get the BIOS package in capsule format, which usually ends with .cab, and then follow this procedure.

1. Transfer the BIOS package onto ThinClient.
2. Switch to admin mode and launch an xterm.
3. Run:
 - a. `/usr/sbin/hptc-bios-capsule-update <bios capsule file name>`
 - b. `reboot -f`

Upon restart, the system updates the BIOS.

4. Check your BIOS version in sysinfo or use the `dmidecode` command to verify the result.

Alternatively, you can call `hptc-bios-flash` and provide a bios capsule file. `Hptc-bios-flash` can detect the file type and invoke `hptc-bios-capsule-update` automatically.



NOTE: Not all ThinClient models and BIOS support capsule update. Switch to the standard BIOS update method if BIOS capsule update fails.

Input Devices

This section describes the input devices.

Table 9-18

Menu option	Description
Keyboard	Lets you change the keyboard layout to accommodate the language used by the primary keyboard and the secondary keyboard.
Keyboard Shortcuts	Lets you create, modify, and delete keyboard shortcuts.
Mouse	Lets you configure the mouse speed and whether mouse input is right-handed or left-handed. On thin clients with a TouchPad, this menu option also lets you disable or enable the TouchPad.
Touch Screen	Lets you configure touch screen options.

Table 9-18 (continued)

Menu option	Description
Ibus	<p>Lets you configure Ibus (Intelligent Input Bus) for multilingual input.</p> <p>Ibus is not enabled by default. To enable Ibus:</p> <p>Control Panel>Input Devices>Ibus Input Method>Start IBUS on boot</p> <p>The Default Ibus configuration file can be modified or restored to factory settings from the Control Panel as well.</p> <p>After reboot, the Ibus tray icon appears. Select the icon to choose language. Right-click the icon for more configuration options.</p> <p>NOTE: Ibus in ThinPro is preloaded with Chinese, Japanese, and Korean languages. To add additional languages:</p> <ol style="list-style-type: none"> 1. Right-click the Ibus system tray icon. 2. Select the Input Method tab. 3. Select Add.

Hardware

This section describes the Hardware configuration.

Table 9-19

Menu option	Description
Display	<p>Lets you configure and test display options.</p> <p>For more information, see Display management on page 80.</p>
Sound	<p>Lets you control the playback, input devices, and input audio levels.</p>
USB Manager	<p>Lets you configure the redirection options for USB devices.</p> <p>For more information, see Redirecting USB devices on page 80.</p>
Serial Manager	<p>Lets you configure serial devices.</p>
Printers	<p>Lets you set up local and network printers. Local printers can be shared across the network.</p> <p>For more information, see Configuring printers on page 80.</p>
Bluetooth	<p>Lets you set up Bluetooth services and attach devices.</p> <p>For more information, see Bluetooth on page 81.</p>

Display management

Display management allows you to configure screen settings and apply these changes in session. To open display management:

Control Panel>Hardware>Display Management.

Redirecting USB devices

To redirect USB devices:

1. In Control Panel, select **Hardware**, and then select **USB Manager**.
2. On the **Protocol** page, select a remote protocol.

If the setting is **Local**, you can also specify the options **allow devices to be mounted** and **mount devices read-only**.
3. On the **Devices** page, you can enable or disable redirection for individual devices if necessary.
4. On the **Classes** page, you can select specific device classes to be redirected to remote sessions.
5. When you are finished, select **Apply**.

Configuring printers

To configure a printer:

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



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

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



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

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

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



NOTE: HP recommends that you type the correct driver name into the **Windows Driver** box. The driver must also be installed on the Windows server for the printer to work properly. If a driver is not specified, a generic postscript driver is used. Using a specific Windows driver might enable more printer functions.

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

Repeat this process to configure additional printers if necessary.



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

Bluetooth

The Bluetooth service is disabled by default. Enable Bluetooth allows the systemd service (Bluez) to start at startup. See `/etc/systemd/bluetooth.service.d/10-bluetooth-enabled.conf`.

After you enable the service, you can access Bluetooth from the icon visible in the system tray of the taskbar.

Decide whether the users can:

- See the Bluetooth icon in the system tray.
- Turn the Bluetooth interface on or off.
- See the list of connected devices.
- Access the device scanner. You can use the scanner to add or remove a device. Users can also remove devices with the scanner.

You can disable the notification messages from the system tray icon by setting the timeout to zero.

ThinPro works well with most audio headsets, mice, and keyboards. You need a PIN to pair with a keyboard. You might have to contact HP support to pair with other devices.



NOTE: The devices returned by the device scanner are filtered according to the registry settings `root/Bluetooth/SystrayApp/DeviceFilter/majorClass` and `root/Bluetooth/SystrayApp/DeviceFilter/services`.

Appearance

This sections describes the Appearance configuration.

Table 9-20

Menu option	Description
Background Manager	<p>Lets you configure the background theme and dynamically display system information (such as the hostname, IP address, hardware model, and MAC address of the thin client) in the background.</p> <p>For more information, see the HP ThinPro white paper <i>Login Screen Customization</i> (available in English only).</p>
Customization Center	<p>Lets you do the following:</p> <ul style="list-style-type: none">• Switch between the ThinPro and Smart Zero configurations• Configure desktop and taskbar options• Select which connection types and Control Panel items end users have access to <p>For more information, see Customization Center on page 82.</p>

Table 9-20 (continued)

Menu option	Description
Language	Lets you display the HP ThinPro interface in a different language.

Customization Center

Follow the instructions here to open Customization Center.

- Select **Appearance** and then select **Customization Center** in Control Panel.

The button at the top of the **Desktop** page can be used to switch between the ThinPro and Smart Zero configurations. See [Choosing an OS configuration on page 1](#) for more information about the differences between the two configurations.



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

Before switching to Smart Zero mode, the domain authentication function on the thin client should be disabled. Domain authentication and Smart Zero mode are incompatible.

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

Table 9-21 Customization options

Option	Description
Launch the Connection Manager at startup	When enabled, Connection Manager launches automatically at system startup.
Enable right-click menu	Disable this option to disable the context menu that appears when you right-click the desktop
Enable X host access control security	When enabled, only the systems listed in the XHost Access Control List area are allowed to remotely control the thin client.
Enable USB Update	Enables updates to be installed from a USB flash drive. See USB updates on page 98 for more information.
Authenticate USB Update	Disable this option to allow end users to install updates via USB.
Allow user to switch to administrator mode	Disable this option to remove the Administrator/User Mode Switch option from Control Panel in user mode.
Time before cancelling administrator mode	Specifies the idle timeout (in minutes) after which administrator mode will be terminated. If set to 0 or negative, administrator mode will never be automatically terminated.

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

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

Snapshots

A snapshot is a copy of the ThinPro filesystem at a given time. A snapshot can restore a previous state of the ThinPro configuration.

By default, a snapshot is marked as the factory snapshot. This is the snapshot that is restored with the simpler config panel: Factory Reset.

The value of the `tmp/restore-points/factory` registry key reflects the name of the currently configured Factory Snapshot.

Since ThinPro 8.1, a snapshot can be marked as the On Boot snapshot. The On Boot Snapshot is restored on each boot. The modifications made in meantime are then lost.

The value of the `tmp/restore-points/on-boot` registry key reflects the name of the currently configured On Boot Snapshot.

The Component Manager and the Restart Plan make an usage of the snapshots. If enabled, the Restart Plan takes over the On Boot Snapshot.

Command line util: `hptc-snapper`



NOTE: A snapshot is part of the filesystem, it cannot be distributed to another device. Distribute the whole ThinPro image instead.

10 System Information

In the Start menu, select **System Information** to view system, network, and software information. The following table describes the information that is displayed on each panel.

Table 10-1 System Information

Panel	Description
General	Displays information about the BIOS, operating system, CPU, and memory.
Network	Displays information about the network interface, gateway, and DNS settings.
Net Tools	<p>Provides the following tools for monitoring and troubleshooting purposes:</p> <ul style="list-style-type: none">• Ping: Specify an IP address of another device on the network to attempt to establish contact.• DNS Lookup: Use this tool to resolve a domain name into an IP address.• Trace Route: Use this tool to track the path that a network packet takes from one device to another.
Software Information	<p>Displays a list of installed add-ons on the Service Packs tab and software version information on the Software Installed tab.</p> <p>TIP: You can also access the Administrator Guide (this document) from this screen.</p>
Software License	Displays the EULA for the HP ThinPro operating system and, if not auto-licensed, information about ThinPro licenses on the system.
System Logs	<p>Displays the following logs:</p> <ul style="list-style-type: none">• Authorization and Security• Connection Manager• DHCP Leases• General System Log• Kernel• Network Manager• Smart Client Services• X Server• OneSign <p>In administrator mode, the debug level can be changed to display additional information that might be requested by HP support for troubleshooting purposes.</p> <p>Select Diagnostic to save a diagnostic file. For more information, see Using system diagnostics to troubleshoot on page 96.</p>



NOTE: See [SystemInfo on page 189](#) for information about registry keys that can be used to hide the System Information screens.

11 HP Smart Client Services

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

HP ThinPro detects an Automatic Update server upon startup and configures settings accordingly. This feature simplifies device installation and maintenance.

To obtain HP Smart Client Services, go to <https://ftp.hp.com/pub/tcdebian/SmartClientServices/>.

Supported operating systems

HP Smart Client Services supports the following operating systems:

- Windows Server® 2019
- Windows Server 2016
- Windows 10
- Windows Server 2012 R2
- Windows Server 2012



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

Prerequisites for HP Smart Client Services

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

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

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

Viewing the Automatic Update website

Instructions to view the Automatic Update website.

1. On the server desktop, select **Start > Control Panel**, and then select **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)\HP\HP Smart Client Service\auto-update`

Creating an Automatic Update profile

Automatic Update uses profiles to deploy a configuration to thin clients.

By default, when you create a profile using Profile Editor, the tool lets you save it to the following folder:

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

You can also export an existing profile from a thin client using HP ThinState and copy the profile to this location.

When searching for updates, HP ThinPro looks for this folder and applies the profile saved there. This ensures that all thin clients use the same configuration.

For more information on using Profile Editor see [Profile Editor on page 89](#).

MAC-address-specific profiles

Automatic Update profiles can be created for a single MAC address. This can be useful when some thin clients need a different configuration.

Profiles for a single MAC address must be stored on the Automatic Update server, in the following folder:

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

When searching for updates, HP ThinPro looks for the generic profile first, and then a MAC-address-based profile. These profiles are merged and installed together on the thin client. The MAC-address-based profile takes precedence; that is, if the same registry key has a different value in both files, the value in the MAC-address-based profile is used.

This ensures that a shared configuration can be provided to all thin clients, but a specific customization can be added, if necessary.

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

1. Obtain the MAC address of the thin client using the system info. For example, the following steps use the MAC address `00fcab8522ac`.
2. Use Profile Editor to create or modify a client profile (see [Profile Editor on page 89](#)) until you are ready to save the client profile.
3. In **Profile Editor**, select the **Finish** link in the left-hand pane to access the **Current profile** pane.
4. Select **Save profile as** to save the client profile as the following:

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

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

Updating thin clients

Using the broadcast update method

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



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



TIP: To verify that the broadcast updates are working, run Profile Editor and make some changes. Connect the thin client and verify that it has downloaded the new profile. If it has not, see [Troubleshooting on page 95](#).

Using the DHCP tag update method

On the Windows Server systems, DHCP tagging enables a thin client to update. Use this method to update specific thin 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, select the domain where the thin clients are connected.
3. In the right pane of the **DHCP** screen, expand and right-click **IPv4**, and then select **Set Predefined Options**.
4. In the **Predefined Options and Values** dialog, select **Add**.
5. In the **Option Type** box, configure the options as described in the following table.

Table 11-1

Field	Entry
Name	Enter <code>auto-update</code> .
Data Type	Select String .
Code	Enter <code>137</code> .
Description	Enter <code>HP Automatic Update</code> .

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

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

8. To complete the setup, select **OK**. DHCP tagging is now ready to update specific thin 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 thin clients to access a single update server across the entire domain, thus simplifying management for deployments with many subnets and DHCP servers.

To configure the DNS alias update method:

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

Using the manual update method

Use the manual update method to connect a thin client to a specific server for an update. Also, use this method if you want to test an update on a single thin client before pushing the update to many thin clients, or if you have specific updates to be installed on only one or two thin 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 **Profile Editor** to modify these settings at root/auto-update.



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

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

Performing a manual update

To perform a manual update:

1. Select **Management > Automatic Update** in Control Panel.
2. Select **Enable manual configuration**.
3. Set the **Protocol** as **http**.
4. In the **Server** field, enter the update server hostname and port in the following format:

```
<hostname>:18287
```

5. In the **Path** field, enter the following:

```
auto-update
```

6. Select **Preserve thin client configuration** if you want to preserve all previously configured settings.
7. Select **OK**, and then the thin client will pull the updates.

12 Profile Editor

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



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

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

Opening Profile Editor

To open Profile Editor:

- Select **Start**, select **All Programs**, select **HP**, select **HP Automatic Update Server**, and then select **Profile Editor**.

Loading a client profile

The name of the currently-loaded client profile is indicated on the initial screen of Profile Editor.

To load a different client profile:

1. At the initial screen of Profile Editor, select the link that displays the name of the currently-loaded client profile.
2. Navigate to a client profile, and then select **Open**.

Client profile customization

Selecting the platform for a client profile

The choice of the platform sets the default settings of the Registry screen. The add-ons and service packs visible by the Profile Editor can also complete these settings. Use the **Platform** screen in Profile Editor to do the following:

- Select the desired HP ThinPro image version that is compatible with your hardware
- Choose between ThinPro and Smart Zero
- View installed add-ons and service packs that provide additional registry settings



NOTE: Add-ons and service packs should be placed in the following directory:

C:\Program Files (x86)\HP\HP Smart Client Service\auto-update\Packages

In some contexts such as with HPDM, it can be convenient for the Profile Editor to look up for add-ons and service packs in a custom directory. The default path of the auto-update directory can be overridden by:

1. The environment variable "HP_AUTO_UPDATE_PATH"
2. The Windows registry value of "HP_AUTO_UPDATE_PATH" under the Windows registry key "HKEY_CURRENT_USER\SOFTWARE\HP Inc\AutoUpdate"
3. If no environment variable or Windows registry value is set and the "auto-update" folder does not exist in the running directory of Profile Editor, the auto-update directory is given by "C:\ProgramData\HP Inc\HP Smart Client Service\auto-update".

Place any add-ons and service packs in: "<auto-update directory>\Packages".

To configure a client profile's platform settings:

1. On the **Platform** screen in Profile Editor, select an **OS Build ID** that corresponds to the desired image version.



IMPORTANT: You can create a different client profile for each hardware type.



NOTE: If an add-on or a service pack is installed, it is displayed automatically in the Add-ons and service packs box. The header of the .xar file might contain some additional or modified registry settings that are visible in the Registry screen.

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



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

Configuring a default connection for a client profile

To configure a default connection for a client profile:

1. On the **Connection** screen in Profile Editor, choose the desired connection type from the **Type** drop-down list.



NOTE: The available connection types differ depending on whether you chose ThinPro or Smart Zero on the Platform screen.

2. In the **Server** field, enter the name or IP address of the server.

Modifying the registry settings of a client profile

To change default registry settings for a client profile:

1. On the **Registry** screen in Profile Editor, expand the folders in the **Registry settings** tree to locate the registry setting you want to change.
2. Select the registry key, and then enter the desired value in the **Value** field.



NOTE: See [Registry keys on page 113](#) for a comprehensive list and description of registry keys.

Adding files to a client profile

Use the **Files** screen in Profile Editor to add configuration files that will be installed on the thin client automatically when the client 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 thin client. Use this when the file needs to be accessed from more than one directory.

Adding a configuration file and certificates to a client profile

Instructions for adding configuration file and certificates to a client profile.


Adding a configuration file to a client profile

You can add configuration files to a client profile and specify the folder path in which the files are installed.


1. On the **Files** screen in Profile Editor, select **Add a file**.
2. Select **Import File**, locate the file to be imported, and then select **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, enter the path where the file will be installed on the thin client.
4. In the **File details** section, 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. Select **Save** to finish adding the configuration file to the client profile.

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

Adding certificates to a client profile

Client profiles automatically include certificates that are imported to a standard client certificate store.

The following applications are supported:

- VMware Horizon View, Citrix, RDP
- Automatic Update
- HP Smart Client Services
- Web browser stores

To import other certificates to a client profile:

1. On the **Files** screen in Profile Editor, select **Add a file**.

2. Select **Import File**, locate the certificate, and then select **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. Select **Save** to finish adding the certificate to the client profile.
5. After installing the client profile, use **Certificate Manager** to confirm that the certificate was imported properly.

Adding a symbolic link to a client profile

Instructions for adding a symbolic link to a client profile.

1. On the **Files** screen in Profile Editor, select **Add a file**.
2. In the **Type** drop-down list, select **Link**.
3. In the **Symbolic link details** section, set the **Link** field to the path of the desired file already installed on the thin client.
4. Select **Save** to finish adding the symbolic link.

Saving the client profile

Instructions to save the client profile.



NOTE: In some contexts, the Profile Editor might have to "Run as administrator" to have permission to override the profile.

1. In **Profile Editor**, select **Finish** in the left-hand pane to access the **Current profile** screen.
2. Select **Save Profile** to save to the current client profile, or select **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. Select the **Finish** button in the **Current profile** screen to exit Profile Editor.

Serial or parallel printer configuration


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

Obtaining the printer settings

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

1. For most printers, press and hold the **Feed** button while turning the device on.

2. After a few seconds, release the **Feed** button. This allows the printer to enter a test mode and print the required information.

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

Setting up printer ports

Instructions for setting up printer ports.


1. In **Profile Editor**, select **Registry**, and then enable the **Show all settings** check box.
2. Enable printer port mapping for your connection type:
 - Citrix: No action is required.
 - RDP: Navigate to **root > ConnectionType > freerdp**. Right-click the **connections** folder, select **New connection**, and then select **OK**. Set the **portMapping** registry key to 1 to enable printer port mapping.
 - VMware Horizon View: Navigate to **root > ConnectionType > view**. Right-click the **connections** folder, select **New connection**, and then select **OK**. Under the **xfreerdpOptions** folder, set the **portMapping** registry key to 1 to enable printer port mapping.
3. Navigate to **root > Serial**. Right-click the **Serial** folder, select **New UUID**, and then select **OK**.
4. Under the new directory, set the **baud**, **dataBits**, **flow**, and **parity** values to the ones obtained in [Obtaining the printer settings on page 92](#).

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


Installing printers on the server

Instructions for installing printers on the server.

1. On the Windows desktop, select **Start > Printers and Faxes**.
2. Select **Add Printer**, and then select **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, select **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 `hptc001` and a serial printer, select the port with **(hptc001:COM1)**. For a parallel printer, select **(hptc001: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 select **Next**.
8. Assign a name to the printer. To use it as the default printer, select **Yes**, and then select **Next**.
9. To share the printer, select **Share name** and assign it a share name. Otherwise, select **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 thin client disconnects from the server, the printer will need to be set up again the next time the thin client connects.

13 Troubleshooting

Troubleshooting network connectivity

Instructions to troubleshoot network connectivity.

1. Ping a server by completing the following steps:
 - a. Select the System Information button on the taskbar, and then select the **Net Tools** tab.
 - b. Under **Select Tool**, select **Ping**.
 - c. In the **Target Host** box, enter the server address, and then select **Start Process**.

If the ping is successful, the system displays 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 thin client might be disconnected from the network and experience a long delay with no system output.

2. If the thin client does not respond to the ping, complete the following steps:
 - a. Check the network cable and check the network settings in Control Panel.
 - b. Try pinging other servers or thin clients.
 - c. If you can reach other thin 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. Select the System Information button on the taskbar, and then select the **System Logs** tab.
 - b. Check for any errors in the logs.
 - c. If there is an error, then the **Server is not set up** notification appears. Verify that the server is set up properly and that HP Smart Client Services is running.

Troubleshooting 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 thin 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 collects files and command outputs of the thin client that can be used to help solve issues without physical access to the thin client. This information contains log files from the BIOS information and the processes active at the time the system diagnostics were run.



TIP: You can change the **Debug level** setting in the **System Logs** tab of the **System Information** window to specify the amount of information to be included 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.

For the most useful logs, set the level to capture a high level of detail before reproducing the problem and creating a diagnostic report.

Saving system diagnostic data

Instructions for saving system diagnostic data.

1. Insert a USB flash drive into the thin client.
2. Select the System Information button on the taskbar, and then select the **System Logs** tab.
3. Select **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

SHORT DESCRIPTION

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

Instructions for uncompressing the system diagnostic files in Linux- or Unix-based systems.

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

Viewing the system diagnostic files

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

Viewing files in the Commands folder

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

Table 13-1 Files in the Commands folder

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

Viewing files in the /var/log folder

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

Viewing files in the /etc folder

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

A USB updates

When USB updates are enabled you can use a USB flash drive to simultaneously install multiple add-ons and certificates, as well as deploy a profile.

For more information on how to enable USB updates see [Customization Center on page 82](#).

USB updates

Follow the instructions here to enable USB updates.

When USB updates are enabled, (see Customization Center on page 61) you can use a USB flash drive to simultaneously install multiple add-ons and certificates, as well as deploy a profile.

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



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

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

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

3. Select the check boxes next to the updates you want to install, and then select **Install**.
4. After installation, restart the thin client if prompted.

HP ThinUpdate

HP ThinUpdate allows you to download images and add-ons from HP and create bootable USB flash drives for image deployment. For more information see the *Administrator Guide* for HP ThinUpdate.

B BIOS tools (desktop thin clients only)

There are two kinds of BIOS tools for HP ThinPro:

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

These tools can be run via an X terminal.

BIOS settings tool

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

 **NOTE:** Changes do not take effect until the next reboot.

Table B-1

Syntax	Description
<code>hptc-bios-cfg -G <file name></code>	Retrieves the current BIOS settings and saves them to the specified file so they can be viewed or modified (CPOSETUP.TXT by default).
<code>hptc-bios-cfg -S <file name></code>	Writes the BIOS settings from the specified file (CPOSETUP.TXT by default) to the BIOS.
<code>hptc-bios-cfg -h</code>	Displays a list of options.

BIOS flashing tool

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


 **NOTE:** Changes do not take effect until the next reboot.

Table B-2 Syntax for the BIOS flashing tool

Syntax	Description
<code>hptc-bios-flash <image name></code>	Prepares the system to update the BIOS during the next restart. This command automatically copies the files into the correct location and prompts you to restart the thin client. NOTE: This command requires that the Tool-less update option in the BIOS settings is set to Auto .
<code>hptc-bios-flash -h</code>	Displays a list of options.

C Resizing the flash drive partition

To use all of the available disk space of a flash drive, you have to modify the partition size and expand the file system to take up that additional space. You can complete this task by running the `resize-image` script using an X terminal.



NOTE: Resizing the flash drive partition image does not work on encrypted disks.



IMPORTANT: HP thin clients that ship from the factory with HP ThinPro use the entire flash drive. The image capture methods capture the smallest possible image, allowing images from larger flash drives to be deployed onto smaller flash drives that have enough space for the captured image. Resizing the flash drive partition is no longer necessary for HP thin clients that ship from the factory with HP ThinPro. For thin clients with HP ThinPro that are not using the entire flash drive for any reason, see the following information.



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

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

Table C-1 Syntax for the `resize-image` script

Syntax	Description
<code>resize-image</code>	When called with no parameters, the script displays the current size of the partition and the amount of available space on the flash drive. The script prompts you to enter the target partition size and then confirm the change. The change takes effect after the next thin client restart. NOTE: You cannot decrease the partition size. The entered value must be larger than the current partition size.
Example: <code>resize-image --size 1024</code>	Using this syntax, you can specify the target partition size in megabytes (MB) as a parameter and then confirm the change.
<code>resize-image --no-prompt</code>	Using this syntax, the script runs automatically with no user interaction required.
- or -	
<code>resize-image --no-prompt --size <size in MB></code>	If no specific size is given as a parameter simultaneously, the partition size is increased to the maximum size.
Example: <code>resize-image --no-prompt --size 1024</code>	TIP: This noninteractive mode is useful for scripting and performing this operation from a remote administration tool such as HPDM and HPCem.

D mclient command

The command client to manticore daemon is `mclient`, which maintains the configuration registry and applies new settings. You need to be root in order to use `mclient` command in most cases. You can get help on `mclient` if you run `mclient` without any argument.

ThinPro 7.2 currently supports the following commands:

```
# mclient
MANTICORE Registry command line frontend

mclient [--quiet] <command>

mclient commands :
  wait-daemon [timeout seconds]
  set <regkey> <regvalue> [regparam]
  get <regkey> [regparam] | [regparam lang]
  gettree <regkey> [regparam] | [regparam lang]
  contains <regkey>
  commit [regkey]
  [--sync] apply [regkey]
  rollback [regkey]
  watch <regkeylist> [timeout]
  changes
  create <regkey> [keytype]
  delete <regkey>
  import <file>
  export <rootDir> <file>

mclient args :
  regkey : string
  regkeylist : string space separated
  regvalue : string
  regparam : string (value|type|regexp|description)
  timeout : int
  keytype : string (string|rc4|uuid|char|ipv4|ipv6|ipaddr|number|float|
  date|bool|crypt|encrypted)
```

Furthermore, you can get bash auto-completion capability after running following command on ThinPro:

```
# . /etc/bash_completion.d/mclient
```

Modifications to the configuration registry are carried out in three steps:

1. Add, modify, or delete the value.
2. Issue the `mclient commit` command to commit the change and save the changes to the disk.
3. Issue the `mclient apply` command to apply the changes.



NOTE: HP recommends to perform a complete restart so that the new settings are carried out.

Other useful mclient usages include:

You can use mclient export and mclient import to export or import a branch of the registry. These commands are useful if you need to export a connection or Wi-Fi setting but not the whole configuration.

For example, if you have configured a Wi-Fi connection on ThinPro, you can find out the registry branch where this configuration is saved:

```
# mclient -q get root/Network/Wireless/Profiles
root/Network/Wireless/Profiles/{de0ff9cb-7f9d-48ba-9ac3-89d28cfad469}#
mclient -q get root/Network/Wireless/Profiles/
{de0ff9cb-7f9d-48ba-9ac3-89d28cfad469}/SSID
NETGEAR89-5G
```



NOTE: {de0ff9cb-7f9d-48ba-9ac3-89d28cfad469} is the sample UUID found on the test system. You might have a different UUID for your connection configuration.

Then you can export the config using this command:

```
# mclient export root/Network/Wireless/Profiles/
{de0ff9cb-7f9d-48ba-9ac3-89d28cfad469} wifi.xml
```

The result wifi.xml can be imported to other machines later.

The tool /usr/bin/mencrypt can be convenient to set the value of the registry keys with an encrypted type, for example:

```
# mclient set root/Network/
Wireless/Profiles/{ de0ff9cb-7f9d-48ba-9ac3-89d28cfad469}/Security/PSK/
PreSharedKey "$(echo -n 'my shared key' | mencrypt)"
# mclient commit root/Network
# mclient apply root/Network
```

E HP ThinPro Configuration

An HP ThinPro configuration contains configuration files and registry settings. If most of the configuration settings are in the ThinPro registry, which is also called the *Manticore registry*. However, some settings are not defined in the registry, such as those for the display configuration. These settings are typically defined in specific configuration files.

HP ThinPro configuration profile: profile.xml

An HP ThinPro configuration profile does not contain the `/etc` directory as a whole. Instead, a profile includes a list of designated directories and files. Similarly, a profile does not contain all the registry settings but includes the modified registry keys only.

When an HP ThinPro configuration profile is saved by the *HP ThinState* and *Profile Editor* tools, the profile is usually named `profile.xml`. This file contains the modified registry settings and the designated configuration directories and files. A `profile.xml` file is commonly deployed from a device management server such as Automatic Update or HPDM.

HP ThinState is a tool that runs on ThinPro. You can use it to export an HP ThinPro configuration profile from a thin client that could then be restored or deployed on another thin client. The *export-profile.sh* and *import-profile.sh* scripts are used underneath.

On HP ThinPro, the *regeditor* and *mclient* tools provide access to the registry settings.

Profile Editor runs on Windows and is part of Smart Client Services and HPDM. You would typically use Profile Editor to create a ThinPro configuration profile. You can use Profile Editor to edit a `profile.xml` file exported from HP ThinState.

For more details about HP ThinState, see [Control Panel on page 59](#). For more details about Profile Editor, see [Profile Editor on page 89](#).

Configuration files of a profile.xml

In a `profile.xml` file, the configuration directories and files are under the `Profile/ProfileFiles` XML path. They are Base64 encoded.

You can find a list of the configuration directories and files that are included in the HP ThinPro Configuration profile in any of the following sources:

- Manticore plugins that got a file named profile

See: `/usr/share/manticore/plugins/*/profile`.

- `/etc/hptc-profile`
- Contents of the `/writable/misc/` directory

ThinPro 8.1 has the following list of directories and files:

- `/etc/firefox`
- `/etc/ssl/cert`

- /home/user/Desktop
- /home/user/firefox
- /persistent/licenses
- /persistent/*.xml
- /usr/local/share/ca-certificates
- /usr/share/manticore/plugins/migration-mgr/profile
- /writable/etc/hptc-locale.d/ibus.userconfig
- /writable/home/user/.bashrc
- /writable/logs/.ctxlogconf
- /writable/misc
- /writable/usr/local/share/ca-certificates



NOTE: The Profile Editor primarily uses the `/etc/hptc-profile` file to keep track of the last files that were imported from a `profile.xml` file into ThinPro.



TIP: You can append directories and files to an `/etc/hptc-profile` file to include them in a `profile.xml` file made from `export-profile.xml`. However, unlike the Profile Editor, `export-profile.sh` doesn't include `/etc/hptc-profile` by default. You can resolve this issue by adding `/etc/hptc-profile` to a custom ThinPro image or by appending `/etc/hptc-profile` to itself.



TIP: Although it is rarely used, you can run the `/tmp/hptc-profile.deleted` command to list the files and directories to be removed while you are importing a `profile.xml` file. Use the Profile Editor to add `/tmp/hptc-profile.deleted` to a `profile.xml` file.

Deployment of a profile.xml

When you restore or deploy an HP ThinPro configuration profile on a device, all the registry keys are reset to their default value. Then, the modified registry keys defined in the `profile.xml` file are imported and are applied. That is, the registry keys that are not available in the imported `profile.xml` file are deleted or are reset to their default value.

Unlike the registry keys, the configuration files are not reset to their initial content. Only the files available in the `profile.xml` file are overridden.

User registry lock

Users can prevent some registry keys from being overridden during the deployment of a `profile.xml` file. This ability is disabled by default, but it can be enabled when a registry plugin defines the special setting named `userLock` and when you set it to 1. Under those circumstances, the user modifications are restored at the end of the `profile.xml` deployment.

For example, perhaps a user prefers to use a mouse with a left-hand configuration. With the `userLock` setting enabled, the user can preserve this choice during upcoming updates of the configuration.

The feature is effective only after the user modifies the plugin's settings. The `userLockEngaged` flag is then set to 1 by the Control Panel. In the meantime, the settings can still be updated through a `profile.xml` file even though the user lock is enabled.

Table E-1 User registry lock configurations

userLock	userLockEngaged	Action while importing a profile
0	0	profile.xml's settings are applied on the thin client
0	1	profile.xml's settings are applied on the thin client
1	0	profile.xml's settings are applied on the thin client
1	1	profile.xml's settings are discarded and the user's settings are preserved

You can enable a user lock in the following ThinPro 8.1 plugins:

- root/Audio/userLock
- root/Network/userLock
- root/keyboard/userLock
- root/mouse/userLock

HP ThinPro configuration after an image update

The ThinPro configuration is usually lost after a ThinPro image update. However, Automatic Update or HPDM typically restore the configuration after the update.

Most of the imaging tools can preserve the current configuration during a ThinPro image update. HP ThinState, HP Easy Update, and HPDM have an option to retain the HP ThinPro configuration during a ThinPro image update. Using this option means that a profile.xml file is put aside before the image update and restored afterwards. Automatic Update does not preserve the HP ThinPro configuration by default, but still has this option within its manual configuration.


How to complete a profile.xml

A profile.xml file includes a selection of configuration files. This selection might be incomplete after the HP ThinPro configuration was customized. In such a case, a configuration is not fully replicated on another device or not fully restored after an image update.

To add a selection of files in a profile.xml file, you can edit /etc/hptc-profile with the list of directories and files to be included.


Example of the /etc/hptc-profile content:

```
/etc/hptc-profile
/home/user/.config/xfce4/xfconf/xfce-perchannel-xml/displays.xml
/etc/mycustom
/home/user/.config/myconfig
```

 **NOTE:** /etc/hptc-profile lists itself on purpose.


F Ephemeral mode

Introduced on ThinPro 8.1, the Ephemeral mode ensures that all data is wiped out after each boot. The Ephemeral mode combines the ThinPro Restart Plan settings with possibly a ThinPro snapshot (aka On Boot Snapshot). The On Boot Snapshot is restored on each boot. Once set up, the ThinPro sessions restarts fresh on a regular basis. This mode purges leftover files, data and processes.

 **WARNING!** It is easy to forget if an On Boot Snapshot was enabled. While modifying the ThinPro configuration as an administrator, there is today no visible reminder. Think to disable or to reset the On Boot Snapshot once the configuration was modified. The previous configuration is restored on the next boot otherwise.

Basic usage of an On Boot Snapshot

Define an On Boot Snapshot in the Snapshots config panel. The On Boot column was added to this end. The designated snapshot is restored on each boot.

 **NOTE:** You cannot export a snapshot (and its On Boot property) via a ThinPro configuration profile. Exporting and importing a whole ThinPro image is the only way to proceed. However if the On Boot Snapshot does not exist yet on a first restart, it is possible to automatically create the On Boot Snapshot while ThinPro is starting; see the Restart Plan settings.

System Information

The information about the current base snapshot is available in System Information.

The *Base snapshot* field is renamed as *Restored snapshot* or *Created snapshot* according to the current ThinPro state.

See also the registry keys under `tmp/SystemInfo/general/`.

Util: hptc-snapper

Use this command to define an On Boot Snapshot in the Snapshots config panel.

```
~# hptc-snapper --help
Usage: hptc-snapper <command> [arguments]
(...)
hptc-snapper -b|--get-on-boot
Print the name of the On Boot snapshot. The On Boot snapshot is
systematically restored on each boot.
hptc-snapper -B|--set-on-boot <name>
Set the given snapshot as the On Boot snapshot.
(...)
```


Restart Plan

Unlike the On Boot snapshot defined in the Snapshots config panel, the Restart Plan defines some registry settings that can be handled via a ThinPro configuration profile. They are lighter to handle from the remote management tools than a whole ThinPro image.


Restart Plan On Boot Snapshot

When enabled, the Restart Plan takes over the On Boot snapshot. Then, you cannot define it from the Snapshots config panel anymore.

An On Boot Snapshot is not mandatory. If you define one while applying the Restart Plan settings, a question series ensures that the snapshot becomes available.

 **IMPORTANT:** With an On Boot Snapshot set up, any further modification of the ThinPro configuration is dropped on the next restart. At any time, you can reset the On Boot Snapshot by selecting the button *Reset the snapshot now*.

The setting *Automatic snapshot reset* is convenient to defer the creation of the On Boot Snapshot on the next boot. We can also take advantage of it to apply the Restart Plan settings from the remote management tools, see below the sections dedicated to Automatic Update and HPDM.

 **IMPORTANT:** Defining an On Boot Snapshot that is not available and that is not automatically created is an invalid configuration. In that case, the ThinPro system is locked on the next restart. To unlock the system, you must apply new settings remotely or the ThinPro image must be redeployed.

Restart Plan Automatic restart

Relying on a "natural" restarts cadence to ensure a fresh state of the system might be insufficient. The Restart Plan gives a few possibilities to restart the system automatically.

Check the setting *after the last connection stopped* to automatically restart when all the Citrix, VMWare, Web Browser and other ThinPro connections have stopped.

By default, you can set *Calendar events* according to some basic recurrences such as hourly or daily. *Calendar events*, *Random delay*, *User notification timeout* and *Maximum postpone delay* are manually editable. For more details, see the Linux manuals *systemd.timer(5)* and *systemd.time(7)*. Use a semicolon separated list to provide more than one calendar event.

The involved systemd timer is: `hptc-restart-plan.timer`.

The *Random delay* setting is to avoid a restart storm at the very same time of a fleet of thin clients.

The user cannot cancel the automatic restart, but the user can postpone it according to the settings *User notification timeout* and *Maximum postpone delay*.

Restart Plan registry settings

Restart Plan registry keys.

Table F-1 Restart Plan registry keys

Registry key	Type	Default value	Description
<code>root/RestartPlan/enableRestartPlan</code>	bool	0	If set to 1, the Restart Plan is enabled.

Table F-1 Restart Plan registry keys (continued)

Registry key	Type	Default value	Description
root/RestartPlan/Recurrences/			The settings are related to automatic restart recurrences and how the user notification is presented.
root/RestartPlan/Recurrences/afterLastConnection	bool	0	If set to 1, the system automatically restarts after the last connection stopped.
root/RestartPlan/Recurrences/enabled	bool	0	Use this key to enable or disable automatic restarts.
root/RestartPlan/Recurrences/maxPostponeDelay	string	1h	Use this key to cause a delay in seconds or set it with a timespan that defines the maximum delay that the user can use to postpone the automatic restart. See also <i>systemd.time(7)</i> .
root/RestartPlan/Recurrences/notificationTimeout	string	1min	Timeout in seconds or set with a timespan string which defines how much time the user notification is displayed before the system automatically restarts. See also <i>systemd.time(7)</i> .
root/RestartPlan/Recurrences/onCalendarEvents			Semicolon separated list of calendar events as defined by the <i>systemd OnCalendar</i> setting. See also <i>systemd.timer(5)</i> and <i>systemd.time(7)</i> .
root/RestartPlan/Recurrences/randomizedDelaySec	string	0	<i>systemd RandomizedDelaySec</i> setting in seconds or set with a timespan string. You can use this delay to spread the automatic restarts of a fleet of thin clients over time. See also <i>systemd.timer(5)</i> and <i>systemd.time(7)</i> .
root/RestartPlan/Snapshot/			If enabled, the On Boot Snapshot is restored on each restart.
root/RestartPlan/Snapshot/autoReset	bool	0	If set to 0, the On Boot Snapshot never resets automatically. It is still possible to reset the snapshot manually from the Control Panel or with the command: <code>hptc-restart-plan-helper --reset-snapshot</code> . If set to 1, the On Boot Snapshot can reset automatically. For example, the snapshot is automatically deleted when a new configuration profile is applied and is automatically created on next restart.

Table F-1 Restart Plan registry keys (continued)

Registry key	Type	Default value	Description
root/RestartPlan/Snapshot/enabled	bool	0	If set to 1 along with enableRestartPlan, the On Boot Snapshot is restored on each restart. If set to 0, no snapshot is restored on restart, the system starts normally.
root/RestartPlan/Snapshot/name	string		Name of the On Boot Snapshot to create or restore on restarts. Note: if empty, the name Restart Plan is used.
root/RestartPlan/Snapshot/resetUuid	string		System key, UUID which works with autoReset=1 to check whether the On Boot Snapshot has to be reset upon the import of a new configuration. You normally do not need to modify this setting.

Utils


- hptc-snapper --help
- hptc-restart-plan-helper --help
- journalctl -t restart-plan
- systemd-analyze calendar <calendar event>
- systemd-analyze timespan <timespan>
- systemctl status hptc-restart-plan.timer

Automatic Update

When an On Boot snapshot is defined, the simplest but heaviest scenario to bring some updates is to make up a new ThinPro image and to deploy it. In addition to this scenario, several other scenarios are possible.

Scenario 1: Updates on top of the On Boot Snapshot

A first scenario, is to deploy on devices a ThinPro image which have a preset On Boot snapshot and root/auto-update/rebootAfterPackageUpdate set to 0. After each boot, the snapshot is restored and the updates are systematically installed on top of the On Boot Snapshot. This works if the updates do not require the devices to restart. In this scenario, *no Restart Plan settings* are involved.

 **WARNING!** keeping root/auto-update/rebootAfterPackageUpdate set to 1 makes an infinite loop: restoration of the On Boot snapshot -> package or add-on installation -> reboot -> restoration of the On Boot snapshot -> and so on.


Scenario 2: automatic reset of the On Boot Snapshot after an update


A second scenario is to deploy a ThinPro configuration profile and to automatically reset the On Boot Snapshot. In addition to defining the On Boot Snapshot among the Restart Plan settings, set `root/RestartPlan/Snapshot/autoReset` to 1.

In that scenario, ThinPro triggers a restart of the device once the profile is installed. The On Boot Snapshot is created during that restart and the snapshot is restored on next restarts.

To bring a configuration update, modify the profile. Once the new profile is installed, ThinPro deletes the initial On Boot Snapshot and triggers a restart of the device. A new On Boot Snapshot is automatically created during that restart. The new On Boot Snapshot is restored on next restarts.

To bring a package or add-on update, the profile must be modified as well. The profile is installed last and allows ThinPro to trigger the reset of the On Boot Snapshot as showed above. Any slight modification of the profile is valid. For instance, set `root/RestartPlan/Snapshot/resetUuid` to any string of your choice (`resetUuid` is not an actual setting, ThinPro overrides it while importing the profile).

 **WARNING!** Keeping `root/RestartPlan/Snapshot/autoReset` set to 0 locks the ThinPro system if an On Boot Snapshot doesn't preexist. If the On Boot Snapshot preexists, ThinPro doesn't delete the snapshot and the updates are systematically reinstalled on top of the On Boot Snapshot. This latter behavior is a valid use case.

 **WARNING!** By not modifying the profile along with a package or add-on update, we get an infinite loop similar to the one evoked in the first scenario. Similarly you can set `root/auto-update/rebootAfterPackageUpdate` to 0, then the package updates are systematically reinstalled on each restart after the restoration of the On Boot Snapshot.


HPDM

ThinPro 8.1 is supported since HPDM 5.0.11. You can go to <http://www.hp.com/go/hpdm> for more information. You can also see the *HP Device Manager 5.0 Administrator's Guide*.

This section of the appendix describes how to set up an Ephemeral mode from HPDM.

The first subsection describes how to work with an Ephemeral mode whatever the version of ThinPro. Only using some HPDM rules and templates. A second subsection describes how to update ThinPro 8.1 which got an On Boot Snapshot.

The second subsection describes how to update ThinPro 8.1 which got an On Boot Snapshot.

 **NOTE:** Unless you need to deploy the entire ThinPro image, you cannot deploy a given snapshot on ThinPro. Applying registry settings, deploying a profile, or deploying add-ons is easier and faster over the network.

How to work in Ephemeral mode with any version of ThinPro


You can rely on HPDM rules and templates to work with an Ephemeral mode that is similar to the mode you work with by using ThinPro 8.1 On Boot Snapshot and the Restart Plan settings. ThinPro 8.1 is not required for you to achieve this type of Ephemeral mode. None of the new Restart Plan settings are required. You can use any version of ThinPro that is supported.


On Boot Snapshot

You can use several solutions to restore a snapshot on each boot, but a simple one is to create a rule that is run *on every startup* and based on the *_File and Registry* template.

1. Prepare and deploy ThinPro with a snapshot named, for example, *HPDM_On_Boot_Snapshot*.
2. Using the `hptc-snapper --restore HPDM_On_Boot_Snapshot --noreboot` script, create an HPDM rule based on the *_File and Registry* template.

The rule in this procedure does not restore the snapshot immediately, but it prepares ThinPro to have the snapshot restored during the next restart.

 **IMPORTANT:** Before you update ThinPro, disable the rule you created and restart once. Otherwise, the updates get lost on next restart. After the restart, reset *HPDM_On_Boot_Snapshot* and the rule.

 **IMPORTANT:** It is not possible to create a rule executed *on every startup* with the *_Manage Snapshot* template. This template requires ThinPro to restart, we get an infinite loop of ThinPro restarting.

Reset of the On Boot Snapshot

To reset the On Boot Snapshot after an update, create a sequence of tasks based on the *_Manage Snapshot* template. The first task deletes the snapshot, and the second task creates it again.

Automatic restarts

To periodically restart thin clients, schedule a rule based on the *_Reboot Device* template.

Enable the Task Deferment options to postpone the restart.

How to update ThinPro 8.1 when the Restart Plan settings define an On Boot Snapshot

If updating ThinPro from HPDM when the Restart Plan settings define an On Boot Snapshot, follow the instructions outlined in this section to update ThinPro from HPDM.

You can use different methods to update ThinPro when an On Boot Snapshot is defined. The following subsections are a few proposals mostly based on some sequence of tasks based on the *_Template Sequence* template.

HPDM sequence of tasks to push a ThinPro profile while an On Boot Snapshot is set

HPDM makes it possible to mimic the Automatic Update scenarios seen earlier with some tasks based on the *_Capture Profile* and *_Deploy Profile* templates. You can use the Profile Editor from a task based on the *_Deploy Profile* template. However, HPDM is more flexible than Automatic Update because it allows additional actions.

A task based on the *_Deploy Profile template* requires an automatic restart of the device. Therefore, it can be valuable to set `root/RestartPlan/Snapshot/autoReset` to 1 to automatically reset the On Boot Snapshot during that restart.

1. In a sequence of tasks, start with a *_Reboot* task. This task ensures that the On Boot Snapshot is restored without modification before applying the update.
2. Prepare a profile in a task based on *_Deploy Profile* with `root/RestartPlan/Snapshot/autoReset` set to 1. You can edit the profile with the Profile Editor.

3. Send the sequence to the devices to get them updated.

If you want to keep `root/RestartPlan/Snapshot/autoReset` set to 0, you can use a more elaborated sequence by taking advantage of `hptc-restart-plan-helper`. After the first restart, you must discard the On Boot Snapshot because you do not want the snapshot to be restored after the profile deployment. After the profile is deployed, ThinPro restarts in a locked state because the On Boot Snapshot is not available. The HPDM sequence can proceed with a reset of the On Boot Snapshot and a final restart to get out of the locked state.

Use the following commands in the two additional tasks that are based on a script of the *_File and Registry* template:

- `hptc-restart-plan-helper --delete-snapshot`
- `hptc-restart-plan-helper --reset-snapshot <description>`

HPDM sequence of tasks to update some registry settings while an On Boot Snapshot is set

You can use the *_Apply Setting* template to make the setting simpler than the *_Deploy Profile* template, because it does not involve a restart.

1. In a sequence of tasks, starts with a *_Reboot* task. This task ensures that the On Boot Snapshot is restored without modification before applying the update.
2. Prepare a task based on the *_Apply Setting* (or any other task that does not require the device to restart).
3. Prepare a task based on a script of the *_File and Registry* template: `hptc-restart-plan-helper --reset-snapshot "reset from HPDM"`

G Registry keys

HP ThinPro registry keys are grouped into folders and can be modified in several different ways.

- Using a **_File and Registry** task in HPDM and HPCEM
- Using the Registry Editor component of Profile Editor and then deploying the new profile
- Using Registry Editor in the HP ThinPro user interface, which is available in the Tools menu in administrator mode

Each top-level section in this appendix corresponds to one of the top-level registry folders.



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

Audio

Audio registry keys.

Table G-1 Audio registry keys

Registry key	Description
root/Audio/AdjustSoundPath	Sets the full path to the sound played when the playback volume is changed via the volume controls.
root/Audio/JackRetask	<p>This registry key applies only to thin clients that have re-purposable jacks.</p> <p>For the t730's lower front port:</p> <ul style="list-style-type: none">• 0/1: No change / headphone• 2: Microphone <p>For the t630's back port:</p> <ul style="list-style-type: none">• 0: No change / line in• 1: Headphone / line out <p>You must restart the thin client after changing these settings.</p>
root/Audio/OutputMute	If set to 1, the internal speaker and headphone jack are muted.
root/Audio/OutputScale	Sets the volume scale for the internal speaker and headphone jack, ranging from 1 to 400.
root/Audio/OutputScaleAuto	If set to 1, the <code>OutputScale</code> value will be set automatically based on the thin client model.
root/Audio/OutputVolume	Sets the volume for the internal speaker and headphone jack, ranging from 1 to 100.
root/Audio/PlaybackDevice	Sets the device to use for playback.
root/Audio/PulseBuffer	The recommended range for this value is between 1024 and 8192. A value that is too high might cause jittering in playback, while a value that is too low might cause the thin client to crash.

Table G-1 Audio registry keys (continued)

Registry key	Description
root/Audio/RecordDevice	Sets the device to use for capture.
root/Audio/RecordMute	If set to 1, the microphone jack is muted.
root/Audio/RecordScale	Sets the volume scale for the microphone jack, ranging from 1 to 400.
root/Audio/RecordScaleAuto	If set to 1, the <code>RecordScale</code> value will be set automatically based on the thin client model.
root/Audio/RecordVolume	Sets the volume for the microphone jack, ranging from 1 to 100.
root/Audio/VisibleInSystray	If set to 1, a speaker icon is visible in the system tray.
root/Audio/shortcutPassThrough	Defines the apps that allow audio shortcuts to be passed through using a space-separated list. The available options are <code>freerdp</code> , <code>view</code> , and <code>xen</code> .

Bluetooth

Bluetooth registry keys.

Table G-2 Bluetooth registry keys

Registry key	Description
root/Bluetooth/enableBluetooth	If set to 1, the Bluetooth service is started.
root/Bluetooth/visibleInSystemTray	If set to 1 as well as <code>enableBluetooth</code> , the Bluetooth system tray icon is displayed.
root/Bluetooth/SystrayApp/DeviceFilter/ majorClass	Major Device Class Filter. Semicolon-separated list of decimal numbers of the device classes. The string after a colon is ignored. Known classes are 0:Miscellaneous; 1:Computer; 2:Phone; 3:LAN/Network Access Point; 4:Audio/Video; 5:Peripheral; 6:Imaging; 7:Wearable; 8:Toy; 9:Health; 31:Uncategorized. The devices that advertise one of the specified classes show up in the device scanner. Filter more relevant classes with Classic Bluetooth devices. An empty string disables the filter.
root/Bluetooth/SystrayApp/DeviceFilter/ services	Services Filter. Semicolon-separated list of 16-bit UUIDs or full 128-bit UUIDs. The string after a colon is ignored. 16-bit UUIDs are completed with the suffix 0000-1000-8000-00805f9b34fb to get a full Bluetooth Service 128-bit UUID. Relevant GATT Services are defined here: https://www.bluetooth.com/specifications/gatt/services/ . The devices that advertise one of the specified UUIDs show up in the scanner. Filter more UUIDs relevant with Bluetooth Smart devices. An empty string disables the filter. NOTE: The Services Filter is ignored when the Major Device Class of a given device matches in the Major Device Class Filter.
root/Bluetooth/SystrayApp/devices	If set to 1, the paired and connected Bluetooth remote devices are displayed.

Table G-2 Bluetooth registry keys (continued)

Registry key	Description
root/Bluetooth/SystrayApp/messageTimeout	Amount of time in seconds to display message notifications on top of the system tray icon. If set to 0, the notifications are disabled. A notification can open when a device has just been connected, for instance.
root/Bluetooth/SystrayApp/scanner	If set to 1, the Bluetooth scanner is displayed. Adding or removing paired Bluetooth remote devices is also possible with this setting.
root/Bluetooth/SystrayApp/switch	If set to 1, the Bluetooth switch to turn the Bluetooth adapter on or off is displayed.

CertMgr

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

ComponentMgr

ComponentMgr registry key.

Table G-3 ComponentMgr registry key

Registry key	Description
root/ComponentMgr/ NotShowDeleteSnapshotWarning	If set to 1, warning information will not be shown while deleting a snapshot.

ConnectionManager

ConnectionManager registry keys.

Table G-4 ConnectionManager registry keys

Registry key	Description
root/ConnectionManager/ createSampleConnections	If set to 1, sample user-modifiable connection icons are created on the desktop on first boot.
root/ConnectionManager/customLogoPath	
root/ConnectionManager/defaultConnection	To properly launch a connection on startup, this must be set to a valid connection using the format <type>:<label>, as shown in the following example: xen:Default Connection.
root/ConnectionManager/minHeight	
root/ConnectionManager/minWidth	
root/ConnectionManager/splashLogoPath	Sets the full path to the image displayed while a connection is loading.
root/ConnectionManager/useKioskMode	

Table G-4 ConnectionManager registry keys (continued)

Registry key	Description
root/ConnectionManager/ useSplashOnConnectionStartup	If set to 1, the image set by <code>splashLogoPath</code> is enabled. By default, this is enabled for ThinPro and disabled for Smart Zero.

ConnectionType

custom

ConnectionType/custom registry keys.

Table G-5 ConnectionType/custom registry keys

Registry key	Description
root/ConnectionType/custom/authorizations/ user/add	If set to 1, an end user has permission to add a new connection of this type using Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/custom/authorizations/ user/general	If set to 1, an end user has permission to modify the general settings for this connection type using Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/custom/connections/ <UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/custom/connections/ <UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/custom/connections/ <UUID>/authorizations/user/edit	If set to 1, an end user has permission to modify the connection settings for this connection.
root/ConnectionType/custom/connections/ <UUID>/authorizations/user/execution	If set to 1, an end user has permission to execute this connection.
root/ConnectionType/custom/connections/ <UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/custom/connections/ <UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when <code>autoReconnect</code> is set to 1.
root/ConnectionType/custom/connections/ <UUID>/autostart	If set to a value of 1-5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/custom/connections/ <UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/custom/connections/ <UUID>/command	Sets the main command for the custom connection to execute.
root/ConnectionType/custom/connections/ <UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/connections/ <UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/connections/ <UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.

Table G-5 ConnectionType/custom registry keys (continued)

Registry key	Description
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/custom/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/custom/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/custom/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/custom/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to <code>Default Connection</code> and does not display in the UI.
root/ConnectionType/custom/connections/<UUID>/startMode	If set to the default <code>focus</code> and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/custom/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/custom/coreSettings/USBrelevant	Specifies if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/custom/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/custom/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/custom/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.
root/ConnectionType/custom/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/custom/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/custom/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/custom/coreSettings/label	Sets the name to display for this connection type in the UI.

Table G-5 ConnectionType/custom registry keys (continued)

Registry key	Description
root/ConnectionType/custom/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in Connection Manager and the configuration wizard that displays during initial setup. A higher value moves the connection type towards the top of the list. If set to 0, the connection type is hidden from the configuration wizard and is shown last in Connection Manager. Connection types with the same priority are listed in alphabetical order.
root/ConnectionType/custom/coreSettings/serverRequired	Sets whether a server name or address is unused, optional, or required for this connection type.
root/ConnectionType/custom/coreSettings/stopProcess	Sets the behavior that should occur when <code>connection-mgr stop</code> is called on this connection. By default this is <code>close</code> , which will send a standard kill signal to the process. When set to <code>kill</code> , the process specified by <code>appName</code> will be forcefully killed. When set to <code>custom</code> , a custom execution script specified by <code>wrapperScript</code> will be executed with the argument <code>stop</code> to terminate the process gracefully.
root/ConnectionType/custom/coreSettings/tier	Specifies the relative importance of this connection type and the order in which it is listed in the Create menu.
root/ConnectionType/custom/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by <code>appName</code> . This key should not need to be modified.
root/ConnectionType/custom/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/custom/gui/CustomManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/gui/CustomManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/gui/CustomManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect	Controls the state of the Auto reconnect widget in Custom Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/autostart	Controls the state of the Auto start priority widget in Custom Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/command	Controls the state of the Enter command to run widget in Custom Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/CustomManager/widgets/fallBackConnection	Controls the state of the Fallback Connection widget in Custom Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.

Table G-5 ConnectionType/custom registry keys (continued)

Registry key	Description
root/ConnectionType/custom/gui/ CustomManager/widgets/hasDesktopIcon	Controls the state of the Show icon on desktop widget in Custom Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/ CustomManager/widgets/label	Controls the state of the Name widget in Custom Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/custom/gui/ CustomManager/widgets/waitForNetwork	Controls the state of the Wait for network before connecting widget in Custom Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.

firefox

ConnectionType/firefox registry keys.

Table G-6 ConnectionType/firefox registry keys

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

Table G-6 ConnectionType/firefox registry keys (continued)

Registry key	Description
root/ConnectionType/firefox/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/connections/<UUID>/enablePrintDialog	If set to 1, the Print dialog in the web browser can be used.
root/ConnectionType/firefox/connections/<UUID>/enableSmartCard	If set to 1, smart card login is enabled for Citrix connections created via the web browser.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/firefox/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/firefox/connections/<UUID>/forbiddenFiles	This registry key only works when Allow connections to manage their own settings is selected in the Web Browser Connection General Settings Manager. The files listed in this registry key's value will be removed after a Web Browser connection is ended. The file names should be separated by a comma, and a wildcard is supported. For example: *.rdf,cookies.sqlite
root/ConnectionType/firefox/connections/<UUID>/fullscreen	If set to 1, the web browser will start in full screen. If kioskMode is disabled, the browser UI is accessible in full screen mode.
root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/firefox/connections/<UUID>/intendedUse	Sets the intended usage of this Web Browser connection to Citrix, RDP, or Internet.
root/ConnectionType/firefox/connections/<UUID>/kioskMode	If set to 1, the web browser will launch in kiosk mode, meaning that the web browser will start in full screen (even if fullscreen is set to 0) and the browser UI is inaccessible.
root/ConnectionType/firefox/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to Default Connection and does not display in the UI.
root/ConnectionType/firefox/connections/<UUID>/manageOwnPrefs	If set to 1, the connection manages its own preferences and stores them in the following location: /etc/firefox/<UUID>. If set to 0, the connection uses shared preferences.
root/ConnectionType/firefox/connections/<UUID>/showBackForwardButton	If set to 1, the web browser's Back and Forward buttons are displayed when kiosk mode is enabled.
root/ConnectionType/firefox/connections/<UUID>/showHomeButton	If set to 1, the web browser's Home button is displayed when kiosk mode is enabled.
root/ConnectionType/firefox/connections/<UUID>/showSearchBar	If set to 1, the web browser's search bar is displayed when kiosk mode is enabled.

Table G-6 ConnectionType/firefox registry keys (continued)

Registry key	Description
root/ConnectionType/firefox/connections/<UUID>/showTabsBar	If set to 1, the web browser's tabs are displayed when kiosk mode is enabled.
root/ConnectionType/firefox/connections/<UUID>/showTaskBar	If set to 1, the web browser's taskbar is displayed when kiosk mode is enabled.
root/ConnectionType/firefox/connections/<UUID>/showUrlBarRefreshButton	If set to 1, the web browser's URL bar and Refresh button are displayed when kiosk mode is enabled.
root/ConnectionType/firefox/connections/<UUID>/startMode	If set to the default <code>focus</code> and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/firefox/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/firefox/coreSettings/USBrelevant	Specifies if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/firefox/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/firefox/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/firefox/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.
root/ConnectionType/firefox/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/firefox/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/firefox/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/firefox/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/firefox/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/firefox/coreSettings/restartIdleTime	Sets the time in minutes before the web browser restarts when the system is not receiving user input. If set to 0, restart is disabled.
root/ConnectionType/firefox/coreSettings/serverRequired	Sets whether a server name or address is <code>unused</code> , <code>optional</code> , or <code>required</code> for this connection type.

Table G-6 ConnectionType/firefox registry keys (continued)

Registry key	Description
root/ConnectionType/firefox/coreSettings/stopProcess	Sets the behavior that should occur when <code>connection-mgr stop</code> is called on this connection. By default this is <code>close</code> , which will send a standard kill signal to the process. When set to <code>kill</code> , the process specified by <code>appName</code> will be forcefully killed. When set to <code>custom</code> , a custom execution script specified by <code>wrapperScript</code> will be executed with the argument <code>stop</code> to terminate the process gracefully.
root/ConnectionType/firefox/coreSettings/tier	Specifies the relative importance of this connection type and the order in which it is listed in the Create menu.
root/ConnectionType/firefox/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/firefox/general/enableUserChanges	If set to 1, the settings configured in the Firefox Preferences dialog will be saved after each session.
root/ConnectionType/firefox/gui/FirefoxManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/gui/FirefoxManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/gui/FirefoxManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Controls the state of the URL widget in Web Browser Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Controls the state of the Auto reconnect widget in Web Browser Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart	Controls the state of the Auto start priority widget in Web Browser Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog	Controls the state of the Enable print dialog widget in Web Browser Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection	Controls the state of the Fallback Connection widget in Web Browser Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon	Controls the state of the Show icon on desktop widget in Web Browser Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.

Table G-6 ConnectionType/firefox registry keys (continued)

Registry key	Description
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/kioskMode	Controls the state of the Enable kiosk mode widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/label	Controls the state of the Name widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showBackForwardButton	Controls the state of the Show Back and Forward Button widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showHomeButton	Controls the state of the Show Home Button widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showSearchBar	Controls the state of the Show Search Bar widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showTabsBar	Controls the state of the Show Tabs Bar widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/showTaskBar	Controls the state of the Show Task Bar widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/ showUrlBarRefreshButton	Controls the state of the Show URL Bar and Refresh Button widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/startMode	Controls the state of the Enable full screen widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/firefox/gui/ FirefoxManager/widgets/waitForNetwork	Controls the state of the Wait for network before connecting widget in Web Browser Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.

freerdp

ConnectionType/freerdp registry keys.

Table G-7 ConnectionType/freerdp registry keys

Registry key	Description
root/ConnectionType/freerdp/authorizations/user/add	If set to 1, an end user has permission to add a new connection of this type using Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/ExtraArgs	Specifies extra arguments for the xfreerdp client. Run <code>xfreerdp --help</code> from an X terminal to see all available arguments.
root/ConnectionType/freerdp/connections/<UUID>/SingleSignOn	If enabled, the user, domain, and password combination for the RDP connection is saved to unlock the screen saver.
root/ConnectionType/freerdp/connections/<UUID>/address	Sets the hostname or IP address to connect to. The port number can be appended on the end after a colon character, for example, <code>servername:3389</code>
root/ConnectionType/freerdp/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/freerdp/connections/<UUID>/application	Specifies an alternate shell or application to run.
root/ConnectionType/freerdp/connections/<UUID>/attachToConsole	
root/ConnectionType/freerdp/connections/<UUID>/audioLatency	Sets the average milliseconds of offset between the audio stream and the display of corresponding video frames after decoding.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/edit	If set to 1, an end user has permission to modify the connection settings for this connection.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/execution	If set to 1, an end user has permission to execute this connection.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when <code>autoReconnect</code> is set to 1.
root/ConnectionType/freerdp/connections/<UUID>/autostart	If set to a value of 1-5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/freerdp/connections/<UUID>/bandwidthLimitation	If set to a value greater than 0, the value represents an approximate bandwidth limitation for downloading and uploading in kilobytes per second. If set to 0 (the default), there is no limitation.
root/ConnectionType/freerdp/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/freerdp/connections/<UUID>/clipboardExtension	If set to 1, clipboard functionality is enabled between different RDP sessions and between RDP sessions and the local system.
root/ConnectionType/freerdp/connections/<UUID>/compression	If set to 1, compression of RDP data sent between the client and the server is enabled.

Table G-7 ConnectionType/freerdp/registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/credentialsType	Specifies the credential type between <code>sso</code> (single sign-on), <code>startup</code> (credentials are requested at startup), <code>password</code> (preconfigured user/domain/password), or <code>smartcard</code> (preconfigured smart card).
root/ConnectionType/freerdp/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/freerdp/connections/<UUID>/directory	Specifies the startup directory where an alternate shell application is executed.
root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX	If set to 1, multimedia redirection is disabled if a valid RemoteFX session is established.
root/ConnectionType/freerdp/connections/<UUID>/domain	Sets the default domain to supply to the remote host during login. If a domain is not specified, the default domain for the remote host will be used.
root/ConnectionType/freerdp/connections/<UUID>/enableMMR	If set to 1, the Multimedia Redirection add-on is enabled, causing supported codecs played through Windows Media Player to be redirected to the client.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/freerdp/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount	Sets the number of video frames the server can push without waiting for acknowledgement from the client. Lower numbers result in a more responsive desktop but lower frame rate. If set to 0, frame acknowledgement is not used in the client-server interactions.
root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress	Sets the RD Gateway server name or address.
root/ConnectionType/freerdp/connections/<UUID>/gatewayCredentialsType	Specifies the credential type between whether credentials are to be supplied by <code>sso</code> (single sign-on), <code>startup</code> (credentials are requested at startup), or <code>password</code> (preconfigured user/domain/password).
root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain	Sets the default domain to supply to the RD Gateway during login. Usually, this setting is used with kiosk-style applications where a generic user name is used to log in. If <code>gatewayUsesSameCredentials</code> is set to 1, this value is disabled.
root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled	If set to 1, the RD Gateway is expected to be used.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword	Sets the default password to supply to the RD Gateway during login. This value is usually encrypted. Usually, this setting is used with kiosk-style applications where a generic user name is used to log in. If <code>gatewayUsesSameCredentials</code> is set to 1, this value is disabled.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPort	Sets the port number to use when contacting the RDP server. This value can be left empty. The most common value is 443.

Table G-7 ConnectionType/freerdp registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/gatewayUser	Sets the default user name to supply to the RD Gateway during login. Usually, this setting is used with kiosk-style applications where a generic user name is used to log in. If gatewayUsesSameCredentials is set to 1, this value is disabled.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUsesSameCredentials	If set to 1, the same credentials that are used to connect to the final server are used to connect to the RD Gateway.
root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/hostnameType	If set to hostname, the system hostname is sent to the remote host. This is typically used to identify the thin client associated with a particular RDP session. The sent hostname can be overridden using sendHostname in the connection-specific settings. If set to mac, the MAC address of the first available network adapter is sent instead of the hostname.
root/ConnectionType/freerdp/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/freerdp/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this is typically set to Default Connection and does not display in the UI.
root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo	This value is the load balancing cookie sent for brokering purposes to the server upon connection. This value corresponds to the loadbalanceinfo field in the .rdp file. By default, the value is empty.
root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection	If set to 1, the local non-USB storage partitions are redirected to the remote host via the Storage extension. If set to 0, the extension is disabled for non-USB storage partitions that are not used by HP ThinPro.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/domain	If set to 1, the Domain field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/password	If set to 1, the Password field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/rememberme	If set to 1, the Remember me check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/server	If set to 1, the Server box is shown in the login dialog for the connection. If set to 2, the box is shown but disabled. If set to 0, the box is hidden. If set to 3, the system settings are used.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/showpassword	If set to 1, the Show password check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/smartcard	If set to 1, the Smart card login check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden. This check box might not appear if no smart card is detected, even if this option is enabled.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/username	If set to 1, the User Name field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.

Table G-7 ConnectionType/freerdp/registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/mouseMotionEvents	If set to 0, mouse motion events are not sent to the server. This can prevent some user feedback such as tooltips from functioning properly.
root/ConnectionType/freerdp/connections/<UUID>/offScreenBitmaps	If set to 0, off-screen bitmaps are disabled. This setting can increase performance slightly but will cause blocks of the screen to update asynchronously, causing screen transitions to update non-uniformly.
root/ConnectionType/freerdp/connections/<UUID>/password	Sets the default password to supply to the remote host during login. This value will be encrypted. Generally, this setting is used for kiosk-style applications where a generic password is used for login.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagDesktopComposition	If set to 1, desktop composition (such as translucent borders) is allowed if supported by the server. Turning off desktop composition can improve performance for low-bandwidth connections. Generally, this affects only RemoteFX. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagFontSmoothing	If set to 1, font smoothing is allowed if supported by the server and enabled. Turning off font smoothing can improve performance on low-bandwidth connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorSettings	If set to 1, cursor blinking is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorShadow	If set to 1, mouse cursor shadows are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoMenuAnimations	If set to 1, menu animations are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoTheming	If set to 1, user interface themes are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWallpaper	If set to 1, the desktop wallpaper is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWindowDrag	If set to 1, full-content window dragging is disabled, which can improve performance on low-bandwidth RDP connections. The window outline is used instead. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/freerdp/connections/<UUID>/portMapping	If set to 1, all serial and parallel ports are redirected to the remote host via the Ports extension. If set to 0, the extension is disabled.
root/ConnectionType/freerdp/connections/<UUID>/printerMapping	If set to 1, all printers defined locally via CUPS are redirected to the remote host via the Printers extension. If set to 0, the extension is disabled. If set to 2, the USB printers are redirected as configured in USB Manager.

Table G-7 ConnectionType/freerdp registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoDisconnectTimeout	Sets the number of minutes there can be no RemoteApp and Desktop resource running before the connection ends automatically. A countdown counter is displayed during the last 20 seconds, providing the user an opportunity to disarm the timer. If set to 0 (the default), the timer is disabled.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoStartSingleResource	If set to 1, and if only a single published resource (RemoteApp program or virtual desktop) is returned by the server, that resource will be started automatically.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/alias	Specifies the alias of a resource for the resource filter. RemoteApp and Desktop resources with a matching alias will be available to users.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/name	Specifies the name of a resource for the resource filter. RemoteApp and Desktop resources with a matching name will be available to users.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/keepResourcesWindowOpened	If set to 0, the resource selection window is closed automatically after a resource has started. If set to 1, the resource selection window is kept open after resources have started. This allows a user to start several resources before closing the resource selection window.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/trustedPublisherSha1Thumbprints	Specifies a comma-separated list of SHA1 thumbprints of the trusted resource publishers. Note that a certificate that matches one of these thumbprints is not verified. Import the publisher's root CA for better security. Also see the registry key <code>verifyPublisherSignature</code> and Certificate Manager in Control Panel.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/verifyPublisherSignature	If set to 1, the publisher's signature is verified when available in published .rdp files. Only resources with a valid signature from a trusted publisher can be run. If set to 0, no verification of the signature is done. Also see the registry key <code>trustedPublisherSha1Thumbprints</code> .
root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering	If set to 1, non-RemoteFX graphics performance is increased at the cost of less frequent screen updates.
root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs	If set to 1, RDP 8 codecs are used if available. This setting should be disabled only in the case of a defect specific to RDP 8 codecs. Disabling this setting might also disable more advanced codecs.
root/ConnectionType/freerdp/connections/<UUID>/rdpEncryption	If set to 1, standard RDP encryption is used to encrypt all data between the client and the server.
root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec	If set to 1, RDP 8 H.264 codecs are used if available. This setting has known visual errors, particularly in multi-monitor configurations, and should be considered experimental and unsupported. Enabling this setting simply advises the server that the thin client supports H.264 for desktop display. The server must also support H.264, and the server makes the final decision about what codecs are used. This setting affects only the desktop codecs. It does not affect multimedia redirection codecs.
root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec	If set to 1, RDP 8 progressive codecs are used if available. This setting should be disabled only in the case of a defect specific to RDP 8 progressive codecs. Disabling this setting might also disable more advanced codecs.

Table G-7 ConnectionType/freerdp/registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/redirectPreference	For redirection, the RDP client is given several destination possibilities. It normally tries them in the following order: FQDN, Primary IP, IP List, NetBIOS. If FQDN is not desired, one of the alternatives can be tried first by setting this registry key. If the specified method does not work, the RDP client falls back to the original order. A setting of <code>auto</code> forces the original order.
root/ConnectionType/freerdp/connections/<UUID>/remoteApp	Specifies the name of an available application to run in Remote Application Integrated Locally (RAIL) mode.
root/ConnectionType/freerdp/connections/<UUID>/remoteAppEnabled	WARNING! FreeRDP 1 has limited support of the RemoteApp programs. If set to 1, the RemoteApp programs can be set up in the FreeRDP connection editor and are visible among the RD Web Access resources. See also: <code>remoteApp</code> , <code>windowMode</code> , <code>application</code> and <code>directory</code> .
root/ConnectionType/freerdp/connections/<UUID>/remoteDesktopService	If set to <code>Remote Computer</code> , a direct RDP connection to a remote computer is done. If set to <code>RD Web Access</code> , a connection to an RD Web Access service is done first to retrieve a feed of the published RemoteApp resources.
root/ConnectionType/freerdp/connections/<UUID>/remoteFx	If set to 1, RemoteFX in the style of RDP 7.1 is used if available. This setting is deprecated and might disappear in a future release of HP ThinPro. This setting should be disabled only in the case of a defect specific to RemoteFX protocol. Disabling this setting might also disable more advanced codecs.
root/ConnectionType/freerdp/connections/<UUID>/requireEncryptionOracleRemediation	If set to 1, the Remote Desktop Client refuses to connect to servers that do not offer suitable protections. This addresses Microsoft security vulnerability CVE-2018-0886.
root/ConnectionType/freerdp/connections/<UUID>/scCertificate	If a preconfigured smart card login is selected, this gives an identifier corresponding to the certificate on that smart card to be used for authentication.
root/ConnectionType/freerdp/connections/<UUID>/scPin	If a preconfigured smart card login is selected, this gives the PIN or password for that smart card.
root/ConnectionType/freerdp/connections/<UUID>/scRedirection	If set to 1, all local smart card readers are redirected to the remote host but are not used for the Network Level Authentication (NLA) of the RDP session. NOTE: If <code>credentialsType</code> is set to <code>smartcard</code> or <code>smartcard</code> is set to 1, <code>scRedirection</code> is ignored, depending on the HP ThinPro version. In this configuration, the smart card readers are always redirected.
root/ConnectionType/freerdp/connections/<UUID>/seamlessWindow	If set to 1, window decorations are disabled. This can be desirable in a multi-monitor configuration to allow the connection to be set to the size of the primary monitor.
root/ConnectionType/freerdp/connections/<UUID>/securityLevel	Sets the certificate security level. If set to 0, all connections are allowed. If set to 1, remembered hosts are selected and a warning dialog is shown if verification is not passed. If set to 2, remembered hosts are not selected and a warning dialog is shown if verification is not passed. If set to 3, all insecure connections are refused.
root/ConnectionType/freerdp/connections/<UUID>/sendHostname	Sets the thin client hostname that is sent to the remote host. If left blank, the system hostname is sent. The registry key <code>root/ConnectionType/freerdp/general/sendHostname</code> must be set to <code>hostname</code> for this key to be used.

Table G-7 ConnectionType/freerdp/registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/showConnectionGraph	This is a diagnostic function. If set to 1, when the session starts, a separate program will be started to graph the connection's health.
root/ConnectionType/freerdp/connections/<UUID>/showRDPDashboard	If set to 1, when the session starts, a separate window displays RDP performance and status.
root/ConnectionType/freerdp/connections/<UUID>/smartcard	If set to 1, local smartcard authentication to the remote host is allowed. Currently, this will disable Network Level Authentication (NLA).
root/ConnectionType/freerdp/connections/<UUID>/sound	If set to 1, the playback and recording devices are redirected to the remote host via the <code>Audio</code> extension. If set to 0, the extension is disabled. If set to 2, the USB audio devices are redirected as configured in USB Manager. Generally, HP recommends setting this value to 1 so that high-level audio redirection is used. This will improve audio quality and ensure that client audio redirected via other extensions (such as <code>Multimedia Redirection</code>) matches local audio settings.
root/ConnectionType/freerdp/connections/<UUID>/startMode	If set to the default <code>focus</code> and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/freerdp/connections/<UUID>/timeoutError	Sets the number of milliseconds to wait after losing the connection before giving up on reconnecting with the server. If set to 0, reconnection is attempted forever.
root/ConnectionType/freerdp/connections/<UUID>/timeoutRecovery	Sets the number of milliseconds to wait after losing the connection for networking to recover without trying a forced reconnect.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarning	Sets the number of milliseconds to wait after losing the connection before warning the user that the connection has been lost.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarningDialog	If set to 1, when an end-to-end connection drop is detected, a dialog is displayed and the screen will turn grayscale. Otherwise, messages are written to the connection log and the session freezes.
root/ConnectionType/freerdp/connections/<UUID>/timeoutsEnabled	If set to 1, end-to-end connection health checks are done.
root/ConnectionType/freerdp/connections/<UUID>/tlsVersion	Sets the version of Transport Layer Security to be used during the early stages of negotiation with the RDP server. Either set this to match the version of TLS used by your RDP server, or try setting it to <code>auto</code> . NOTE: There are some server-side defects in some unpatched RDP servers that can cause the auto setting to fail, so it is not the default setting.
root/ConnectionType/freerdp/connections/<UUID>/usbMiscRedirection	If set to 0, redirection is disabled for all other USB devices except those handled by <code>sound</code> , <code>printerMapping</code> , <code>portMapping</code> , <code>usbStorageRedirection</code> , and <code>localPartitionRedirection</code> . If set to 2, all other USB devices are redirected to the remote host as configured in USB Manager.
root/ConnectionType/freerdp/connections/<UUID>/usbStorageRedirection	If set to 1, USB storage devices are redirected to the remote host via the <code>Storage</code> extension. If set to 0, the extension is disabled. If set to 2, USB storage devices are redirected as configured in USB Manager.

Table G-7 ConnectionType/freerdp/registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/connections/<UUID>/username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.
root/ConnectionType/freerdp/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/freerdp/connections/<UUID>/windowMode	If set to Remote Application, RDP will run in Remote Application Integrated Locally (RAIL) mode. This requires that the RemoteApp server allows the desired application to run as a remote application. The application will be displayed in a separate window within the desktop environment, making it look like the application is part of the local system. Also see the remoteApp registry key. If set to Alternate Shell, a non-standard shell is invoked. Also see the application and directory registry keys.
root/ConnectionType/freerdp/connections/<UUID>/windowSizeHeight	
root/ConnectionType/freerdp/connections/<UUID>/windowSizePercentage	
root/ConnectionType/freerdp/connections/<UUID>/windowSizeWidth	
root/ConnectionType/freerdp/connections/<UUID>/windowType	
root/ConnectionType/freerdp/connections/<UUID>/x11Capture	This is a diagnostic function. If set to 1, X11 operations are captured for later playback.
root/ConnectionType/freerdp/connections/<UUID>/x11CaptureDir	This is a diagnostic function. The value sets the directory for X11 capture files.
root/ConnectionType/freerdp/connections/<UUID>/x11LogAutoFlush	This is a diagnostic function. If set to 1, the X11 logfile is more frequently flushed to disk.
root/ConnectionType/freerdp/connections/<UUID>/x11Logfile	This is a diagnostic function. The value sets the path to the X11 logfile.
root/ConnectionType/freerdp/connections/<UUID>/x11Logging	This is a diagnostic function. If set to 1, X11 operations are logged.
root/ConnectionType/freerdp/connections/<UUID>/x11Synchronous	This is a diagnostic function. If set to 1, X11 operations are not buffered.
root/ConnectionType/freerdp/connections/<UUID>/xkbLayoutId	Sets an XKB layout ID for bypassing the system keyboard. To see the list of available IDs, enter the following command in an X terminal: xfreerdp --kbd-list.
root/ConnectionType/freerdp/coreSettings/USBrelevant	Specifies if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/freerdp/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning	If set to 1, the operating system does not generate a dialog indicating that networking is down because the connection protocol handles such situations.

Table G-7 ConnectionType/freerdp registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/freerdp/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.
root/ConnectionType/freerdp/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/freerdp/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/freerdp/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	Sets the number of seconds to wait for an initial response from the RDP server before giving up.
root/ConnectionType/freerdp/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/freerdp/coreSettings/stopProcess	Sets the behavior that should occur when <code>connection-mgr stop</code> is called on this connection. By default this is <code>close</code> , which will send a standard kill signal to the process. When set to <code>kill</code> , the process specified by <code>appName</code> will be forcefully killed. When set to <code>custom</code> , a custom execution script specified by <code>wrapperScript</code> will be executed with the argument <code>stop</code> to terminate the process gracefully.
root/ConnectionType/freerdp/coreSettings/tier	Specifies the relative importance of this connection type and the order in which it is listed in the Create menu.
root/ConnectionType/freerdp/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by <code>appName</code> . This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/freerdp/coreSettings/wrapperScriptGeneration	Lets Connection Manager know what type of parameters to pass to the wrapper script.
root/ConnectionType/freerdp/general/autoReconnectDialogTimeout	If <code>autoReconnect</code> is enabled, this key sets the number of seconds before timing out any error dialogs for the connection. If set to 0, the dialogs wait indefinitely for user interaction.
root/ConnectionType/freerdp/general/disablePasswordChange	When a remote login fails due to bad credentials, the user is presented with a button that brings up a dialog for updating their password. If this key is set to 1, that button and dialog are not displayed.

Table G-7 ConnectionType/freerdp registry keys (continued)

Registry key	Description
root/ConnectionType/freerdp/general/preferredAudio	Sets the default audio backend for high-level audio redirection (both in and out).
root/ConnectionType/freerdp/general/rdWebFeedUrlPattern	Sets the pattern used to build the RD Web Access URL. The host of the URL, e.g. myserver.com, is replaced by the value of the connection's Address field. This pattern is not used when the address is already a URL.
root/ConnectionType/freerdp/general/serialPortsDriver	This setting ensures a better compatibility with the expected underlying Windows driver SerCx2.sys, SerCx.sys, or Serial.sys.
root/ConnectionType/freerdp/general/serialPortsPermissive	If set to 1, errors for unsupported features will be ignored.

ssh

SSH registry keys.

Table G-8 SSH registry keys

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

Table G-8 SSH registry keys (continued)

Registry key	Description
root/ConnectionType/ssh/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/ssh/connections/<UUID>/compression	Enables compression for an SSH connection.
root/ConnectionType/ssh/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/ssh/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/ssh/connections/<UUID>/font	Sets the font size for the connection.
root/ConnectionType/ssh/connections/<UUID>/foregroundColor	Sets the foreground color for the connection.
root/ConnectionType/ssh/connections/<UUID>/fork	If set to 1, the Fork into background option is enabled for the connection.
root/ConnectionType/ssh/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/ssh/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/ssh/connections/<UUID>/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to <code>Default Connection</code> and does not display in the UI.
root/ConnectionType/ssh/connections/<UUID>/loginfields/server	If set to 1, the Server box is shown in the login dialog for the connection. If set to 2, the box is shown but disabled. If set to 0, the box is hidden. If set to 3, the system settings are used.
root/ConnectionType/ssh/connections/<UUID>/loginfields/username	If set to 1, the User Name box is shown in the login dialog for the connection. If set to 2, the box is shown but disabled. If set to 0, the box is hidden. If set to 3, the system settings are used.
root/ConnectionType/ssh/connections/<UUID>/port	Sets the port number to use when contacting the SSH server. The default is 22.
root/ConnectionType/ssh/connections/<UUID>/startMode	If set to the default <code>focus</code> and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/ssh/connections/<UUID>/tty	If set to 1, the Force TTY allocation option is enabled for the connection.

Table G-8 SSH registry keys (continued)

Registry key	Description
root/ConnectionType/ssh/connections/<UUID>/username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.
root/ConnectionType/ssh/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/ssh/connections/<UUID>/x11	If set to 1, the X11 connection forwarding option is enabled for the connection.
root/ConnectionType/ssh/coreSettings/USBrelevant	Specifies if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/ssh/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/ssh/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.
root/ConnectionType/ssh/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/ssh/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/ssh/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/ssh/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/ssh/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/ssh/coreSettings/serverRequired	Sets whether a server name or address is unused , optional , or required for this connection type.
root/ConnectionType/ssh/coreSettings/stopProcess	Sets the behavior that should occur when <code>connection-mgr stop</code> is called on this connection. By default this is <code>close</code> , which will send a standard kill signal to the process. When set to <code>kill</code> , the process specified by <code>appName</code> will be forcefully killed. When set to <code>custom</code> , a custom execution script specified by <code>wrapperScript</code> will be executed with the argument <code>stop</code> to terminate the process gracefully.
root/ConnectionType/ssh/coreSettings/tier	Specifies the relative importance of this connection type and the order in which it is listed in the Create menu.

Table G-8 SSH registry keys (continued)

Registry key	Description
root/ConnectionType/ssh/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by <code>appName</code> . This key should not need to be modified.
root/ConnectionType/ssh/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/ssh/gui/SshManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/gui/SshManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/gui/SshManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/ssh/gui/SshManager/widgets/address	Controls the state of the Address widget in Secure Shell Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/application	Controls the state of the Run application widget in Secure Shell Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Controls the state of the Auto reconnect widget in Secure Shell Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/autostart	Controls the state of the Auto start priority widget in Secure Shell Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor	Controls the state of the Background color widget in Secure Shell Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/compression	Controls the state of the Compression widget in Secure Shell Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection	Controls the state of the Fallback Connection widget in Secure Shell Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.

Table G-8 SSH registry keys (continued)

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

telnet

ConnectionType/telnet registry keys.

Table G-9 ConnectionType/telnet registry keys

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

Table G-9 ConnectionType/telnet registry keys (continued)

Registry key	Description
root/ConnectionType/telnet/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/telnet/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/telnet/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to <code>Default Connection</code> and does not display in the UI.
root/ConnectionType/telnet/connections/<UUID>/locale	Sets the locale of the connection.
root/ConnectionType/telnet/connections/<UUID>/loginfields/server	If set to 1, the Server box is shown in the login dialog for the connection. If set to 2, the box is shown but disabled. If set to 0, the box is hidden. If set to 3, the system settings are used.
root/ConnectionType/telnet/connections/<UUID>/port	Sets the port number to use when contacting the server. The default is 23.
root/ConnectionType/telnet/connections/<UUID>/startMode	If set to the default <code>focus</code> and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/telnet/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/telnet/coreSettings/USBrelevant	Specifies if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/telnet/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/telnet/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/telnet/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.
root/ConnectionType/telnet/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/telnet/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/telnet/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/telnet/coreSettings/label	Sets the name to display for this connection type in the UI.

Table G-9 ConnectionType/telnet registry keys (continued)

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

Table G-9 ConnectionType/telnet registry keys (continued)

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

TTerm

TTerm registry keys.

Table G-10 TTerm registry keys

Registry key	Description
root/ConnectionType/tterm/connections/ <UUID>/ authorizations/user/edit	If set to 1, end users have permission to modify the connection settings for this connection.
root/ConnectionType/tterm/connections/ <UUID>/ authorizations/user/execution	If set to 1, end users have permission to run this connection.
root/ConnectionType/tterm/connections/ <UUID>/ loginfields/password	If set to 1, the <i>Password</i> field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden. If set to 3, system settings take precedence.
root/ConnectionType/tterm/connections/ <UUID>/ waitForNetwork	If set to 1, the connection will not be launched until networking is available so that, on a slow network, the connection does not launch before networking is available, which could cause a failure.

Table G-10 TTerm registry keys (continued)

Registry key	Description
root/ConnectionType/tterm/connections/<UUID>/autoReconnect	If set to 1, the connection restarts when it is closed or disconnected.
root/ConnectionType/tterm/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. Do not change this value.
root/ConnectionType/tterm/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this is typically set to Default Connection and does not show in the UI.
root/ConnectionType/tterm/connections/<UUID>/full-screen	Runs the connection in full-screen mode, if set.
root/ConnectionType/tterm/connections/<UUID>/maximized	Runs the connection in maximized mode, if set.
root/ConnectionType/tterm/connections/<UUID>/sessionPanel	If it is not in full-screen mode, set it to 0 to clear session panel at start.
root/ConnectionType/tterm/connections/<UUID>/profile/name	Profile name is saved here. Do not edit it manually; use connection manager instead.
root/ConnectionType/tterm/connections/<UUID>/profile/ttexp	Profile file is saved here. Do not edit it manually; use connection manager instead.
root/ConnectionType/tterm/connections/<UUID>/iconPosition	For pinned desktop icons, an x,y pair. For floating icons, leave this string blank.
root/ConnectionType/tterm/connections/<UUID>/autostart	If set to a value of 1-5, the connection starts automatically after the system starts, with the value of 1 having the highest priority.
root/ConnectionType/tterm/connections/<UUID>/address	Sets the host name or IP address to connect to.
root/ConnectionType/tterm/connections/<UUID>/locale	Sets the locale of the connection.
root/ConnectionType/tterm/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/tterm/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/tterm/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/tterm/connections/<UUID>/afterStartedCommand	Sets the command to run after the connection has been started.

Table G-10 TTerm registry keys (continued)

Registry key	Description
root/ConnectionType/tterm/connections/<UUID>/afterStoppedCommand	Sets the command to run after the connection has been stopped.
root/ConnectionType/tterm/connections/<UUID>/beforeStartingCommand	Sets the command to run before the connection starts.
root/ConnectionType/tterm/connections/<UUID>/startMode	If set to the default <code>focus</code> 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/tterm/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. Do not change this value.
root/ConnectionType/tterm/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/tterm/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. Do not change this value.

view

VMware Horizon View registry keys.

Table G-11 ConnectionType/view registry keys

Registry key	Description
root/ConnectionType/view/authorizations/user/add	If set to 1, an end user has permission to add a new connection of this type using Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/view/authorizations/user/commandLineBox	If set to 1, an end user has permission to enter command-line arguments in VMware Horizon View Connection Manager.
root/ConnectionType/view/authorizations/user/general	If set to 1, an end user has permission to modify the general settings for this connection type using Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/view/connections/<UUID>/ExtraArgs	Specifies extra arguments for the VMware Horizon View client. Run <code>view_client --help</code> or <code>vmware-view --help</code> from an X terminal to see all available arguments.
root/ConnectionType/view/connections/<UUID>/SingleSignOn	
root/ConnectionType/view/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/view/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/view/connections/<UUID>/allowBlacklistedDrivers	If set to 1, allows VMware Horizon View connections to enable the H.264 feature with AMD open-source graphic drivers. If set to 0, VMware Horizon View connections disable hardware acceleration with blacklisted drivers (such as AMDGPU and Radeon).

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/appInMenu	If set to 1, all applications for this connection will be displayed in the taskbar menu.
root/ConnectionType/view/connections/<UUID>/appOnDesktop	If set to 1, all applications for this connection will be displayed on the desktop.
root/ConnectionType/view/connections/<UUID>/applicationSize	Sets the size in which the VMware Horizon View client will launch applications.
root/ConnectionType/view/connections/<UUID>/attachToConsole	
root/ConnectionType/view/connections/<UUID>/authorizations/user/edit	If set to 1, an end user has permission to modify the connection settings for this connection.
root/ConnectionType/view/connections/<UUID>/authorizations/user/execution	If set to 1, an end user has permission to execute this connection.
root/ConnectionType/view/connections/<UUID>/autoHideMenuBar	
root/ConnectionType/view/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/view/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when <code>autoReconnect</code> is set to 1.
root/ConnectionType/view/connections/<UUID>/automaticLogin	If set to 1, the VMware Horizon View client will attempt to log in automatically if all fields are provided. If set to 0, users have to select Connect manually in the VMware Horizon View client, log in, and select a desktop.
root/ConnectionType/view/connections/<UUID>/autostart	If set to a value of 1-5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/view/connections/<UUID>/autostartDelay	Reserved for future use.
root/ConnectionType/view/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/view/connections/<UUID>/closeAfterDisconnect	If set to 1, the connection is ended after the first desktop is closed. If set to 0, the VMware Horizon View client returns to the desktop selection screen. This is enabled by default to prevent users from accidentally leaving the connection at the desktop selection screen after logging off.
root/ConnectionType/view/connections/<UUID>/closeAfterRoaming	If set to 1, the VMware connection will be disconnected if it is roamed to another place..
root/ConnectionType/view/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/connections/<UUID>/credentialsType	Specifies the credential type between <code>anonymous</code> (unauthenticated access), <code>sso</code> (single sign-on), <code>startup</code> (credentials are requested at startup), <code>password</code> (preconfigured user/domain/password), or <code>smartcard</code> (preconfigured smart card).
root/ConnectionType/view/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/desktop	If specified, the named desktop will launch automatically upon login. By default, if there is only one desktop available, it will launch automatically without needing to be specified.
root/ConnectionType/view/connections/<UUID>/desktopSize	Sets the size in which the VMware Horizon View client will launch the desktop.
root/ConnectionType/view/connections/<UUID>/directory	
root/ConnectionType/view/connections/<UUID>/disableMaximizedApp	If set to 1, window size settings for maximized applications are disabled.
root/ConnectionType/view/connections/<UUID>/domain	Sets the domain to provide to View Connection Server. If no domain is specified, the default domain for the server is used.
root/ConnectionType/view/connections/<UUID>/enableCDR	If set to 1, the Client Drive Redirection add-on is enabled.
root/ConnectionType/view/connections/<UUID>/enableMMR	If set to 1, the Multimedia Redirection add-on is enabled via the Blast/PCoIP protocol, causing supported codecs played through Windows Media Player to be redirected to the client. This greatly improves full-screen and high-definition video playback for codecs such as WMV9, VC1, and MPEG4. Video is rendered locally using the CPU power.
root/ConnectionType/view/connections/<UUID>/enableMediaProvider	If set to 1, the VMware Horizon Virtualization Pack for Skype Business component is enabled. This component enables Linux users to redirect Skype for Business calls with the VMware Horizon View Client.
root/ConnectionType/view/connections/<UUID>/enableSeamlessWindow	If set to 1, the VMware Horizon View client starts applications in seamless window mode.
root/ConnectionType/view/connections/<UUID>/enableSingleMode	
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/view/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/view/connections/<UUID>/fullscreen	If set to 1, the VMware Horizon View client launches in full screen mode when started.
root/ConnectionType/view/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/view/connections/<UUID>/hideMenuBar	If set to 1, the top menu bar within the desktop is hidden. This bar is used to manage remote devices and start other desktops.
root/ConnectionType/view/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/view/connections/<UUID>/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to <code>Default Connection</code> and does not display in the UI.

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/lockServer	If set to 1, end users are prevented from changing the server address.
root/ConnectionType/view/connections/<UUID>/loginfields/domain	If set to 1, the Domain field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.
root/ConnectionType/view/connections/<UUID>/loginfields/password	If set to 1, the Password field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.
root/ConnectionType/view/connections/<UUID>/loginfields/rememberme	If set to 1, the Remember me check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden.
root/ConnectionType/view/connections/<UUID>/loginfields/server	If set to 1, the Server box is shown in the login dialog for the connection. If set to 2, the box is shown but disabled. If set to 0, the box is hidden. If set to 3, the system settings are used.
root/ConnectionType/view/connections/<UUID>/loginfields/showpassword	If set to 1, the Show password check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden.
root/ConnectionType/view/connections/<UUID>/loginfields/smartcard	If set to 1, the Smart card login check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden. This check box might not appear if no smart card is detected, even if this option is enabled.
root/ConnectionType/view/connections/<UUID>/loginfields/username	If set to 1, the User Name field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.
root/ConnectionType/view/connections/<UUID>/networkCondition	Allows the selection of the network conditions for the best experience.
root/ConnectionType/view/connections/<UUID>/password	Sets the default password to supply to the remote host during login. This value will be encrypted. Generally, this setting is used for kiosk-style applications where a generic password is used for login.
root/ConnectionType/view/connections/<UUID>/preferredProtocol	Sets the preferred protocol.
root/ConnectionType/view/connections/<UUID>/printerMapping	If set to 1, all printers defined locally via CUPS are redirected to the remote host via ThinPrint. If set to 0, the printer mapping is disabled. If set to 2, the USB printers are redirected as configured in USB Manager.
root/ConnectionType/view/connections/<UUID>/saveCredentials	
root/ConnectionType/view/connections/<UUID>/sendCtrlAltDelToVM	
root/ConnectionType/view/connections/<UUID>/server	Sets the address of the remote host to connect to. This is typically a URL such as <code>http://server.domain.com</code> .
root/ConnectionType/view/connections/<UUID>/sessionEndAction	
root/ConnectionType/view/connections/<UUID>/singleDesktop	

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/smartcard	If set to 1, locally-attached smart cards are forwarded to the remote host, allowing them to be used by applications on the remote host. This only enables smart card login for the remote host, not for View Connection Server.
root/ConnectionType/view/connections/<UUID>/startMode	If set to the default <code>focus</code> 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/view/connections/<UUID>/usbAutoConnectAtStartup	
root/ConnectionType/view/connections/<UUID>/usbAutoConnectOnInsert	
root/ConnectionType/view/connections/<UUID>/useCurrentViewConfig	If set to 1, the HP scripts do not create a new <code>/etc/vmware/config</code> file, and the VMware Horizon View client uses the current <code>/etc/vmware/config</code> file.
root/ConnectionType/view/connections/<UUID>/username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.
root/ConnectionType/view/connections/<UUID>/viewSecurityLevel	If set to <code>Refuse insecure connections</code> , the VMware Horizon View client will not allow a user to connect to View Connection Server if the server's SSL certificate is invalid. If set to <code>Warn</code> , the VMware Horizon View client will display a warning if the server's certificate is not able to be verified, and if the certificate is self-signed or expired, the user still will not be allowed to connect. If set to <code>Allow all connections</code> , the server certificate will not be verified and connections to any server will be allowed.
root/ConnectionType/view/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/attachToConsole	
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/audioLatency	Sets the average milliseconds of offset between the audio stream and the display of corresponding video frames after decoding.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/clipboardExtension	If set to 1, clipboard functionality is enabled between different RDP sessions and between RDP sessions and the local system.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/colorDepth	This setting is deprecated. It is used to reduce the color depth of the connection below that of the native desktop resolution. Frequently, this has been used to reduce network bandwidth. Reducing color depth to a level not supported by the video driver can cause screen corruption or launch failures.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/compression	If set to 1, compression of RDP data sent between the client and the server is enabled.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/disableMMRwithRFX	If set to 1, multimedia redirection is disabled if a valid RemoteFX session is established.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/enableMMR	If set to 1, the Multimedia Redirection add-on is enabled, causing supported codecs played through Windows Media Player to be redirected to the client.

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/frameAcknowledgeCount	Sets the number of video frames the server can push without waiting for acknowledgement from the client. Lower numbers result in a more responsive desktop but lower frame rate. If set to 0, frame acknowledgement is not used in the client-server interactions.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname	If set to <code>hostname</code> , the system hostname is sent to the remote host. This is typically used to identify the thin client associated with a particular RDP session. The sent hostname can be overridden using <code>sendHostname</code> in the connection-specific settings. If set to <code>mac</code> , the MAC address of the first available network adapter is sent instead of the hostname.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/hostnameType	If set to <code>hostname</code> , the system hostname is sent to the remote host. This is typically used to identify the thin client associated with a particular RDP session. The sent hostname can be overridden using <code>sendHostname</code> in the connection-specific settings. If set to <code>mac</code> , the MAC address of the first available network adapter is sent instead of the hostname.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo	This value is the load balancing cookie sent for brokering purposes to the server upon connection and corresponds to the <code>loadbalanceinfo</code> field in the .rdp file. By default, the value is empty.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents	If set to 0, mouse motion events are not sent to the server. This can prevent some user feedback such as tooltips from functioning properly.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/offScreenBitmaps	If set to 0, off-screen bitmaps are disabled. This can increase performance slightly but will cause blocks of the screen to update asynchronously, causing screen transitions to update non-uniformly.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagDesktopComposition	If set to 1, desktop composition (such as translucent borders) is allowed if supported by the server. Turning off desktop composition can improve performance for low-bandwidth connections. Generally, this only affects RemoteFX. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagFontSmoothing	If set to 1, font smoothing is allowed if supported by the server and enabled. Turning off font smoothing can improve performance on low-bandwidth connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorSettings	If set to 1, cursor blinking is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorShadow	If set to 1, mouse cursor shadows are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoMenuAnimations	If set to 1, menu animations are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoTheming	If set to 1, user interface themes are disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWallpaper	If set to 1, the desktop wallpaper is disabled, which can improve performance on low-bandwidth RDP connections. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWindowDrag	If set to 1, full-content window dragging is disabled, which can improve performance on low-bandwidth RDP connections. The window outline is used instead. If set to 2, the value is selected based on the thin client performance.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/portMapping	If set to 1, the following serial and parallel ports are redirected to the remote host: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/printerMapping	If set to 1, all printers defined locally via CUPS are redirected to the remote host.
root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering	If set to 1, non-RemoteFX graphics performance is increased at the cost of less frequent screen updates.
root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs	If set to 1, RDP 8 codecs are used if available. This setting should be disabled only in the case of a defect specific to RDP 8 codecs. Disabling this setting might also disable more advanced codecs.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/rdpEncryption	If set to 1, standard RDP encryption is used to encrypt all data between the client and the server.
root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec	If set to 1, RDP 8 H.264 codecs are used if available. This setting has known visual errors, particularly in multi-monitor configurations, and should be considered experimental and unsupported. Enabling this setting simply advises the server that the thin client supports H.264 for desktop display. The server must also support H.264, and the server makes the final decision on what codecs are used. This setting affects only the desktop codecs. It does not affect multimedia redirection codecs.
root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec	If set to 1, RDP 8 progressive codecs are used if available. This setting should be disabled only in the case of a defect specific to RDP 8 progressive codecs. Disabling this setting might also disable more advanced codecs.
root/ConnectionType/freerdp/connections/<UUID>/redirectPreference	For redirection, the RDP client is given several destination possibilities. It normally tries them in the following order: FQDN, Primary IP, IP List, NetBIOS. If FQDN is not desired, one of the alternatives can be tried first by setting this registry key. If the specified method does not work, the RDP client falls back to the original order. A setting of <code>auto</code> forces the original order.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/remoteFx	If set to 1, RemoteFX is used if available.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sendHostname	Sets the thin client hostname that is sent to the remote host. If left blank, the system hostname is sent. The registry key <code>root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname</code> must be set to <code>hostname</code> for this key to be used.

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sound	If set to <code>Bring to this computer</code> , sound is redirected from the remote host to the client using a standard virtual channel. If set to <code>Leave at remote computer</code> , sound is left at the remote host. This can be useful when using a redirected USB audio device. If set to any other value, audio is disabled. Generally, HP recommends setting this value to <code>Bring to this computer</code> and not redirecting USB playback devices to the remote host. This will improve audio quality and ensure that client audio redirected via other virtual channels (such as <code>Multimedia Redirection</code>) matches local audio settings.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutError	Sets the number of milliseconds to wait after losing the connection before giving up on reconnecting with the server. If set to 0, reconnection is attempted forever.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutRecovery	Sets the number of milliseconds to wait after losing the connection for networking to recover without trying a forced reconnect.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarning	Sets the number of milliseconds to wait after losing the connection before warning the user that the connection has been lost.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarningDialog	If set to 1, when an end-to-end connection drop is detected, a dialog is displayed and the screen will turn grayscale. Otherwise, messages are written to the connection log and the session freezes.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutsEnabled	If set to 1, end-to-end connection health checks are done.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/tlsVersion	Sets the version of Transport Layer Security to be used during the early stages of negotiation with the RDP server. Either set this to match the version of TLS used by your RDP server, or try setting it to <code>auto</code> . NOTE: There are some server-side defects in some unpatched RDP servers that can cause the <code>auto</code> setting to fail, so it is not the default setting.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/xkbLayoutId	Sets an XKB layout ID for bypassing the system keyboard. To see the list of available IDs, enter the following command in an X terminal: <code>xfreerdp --kbd-list</code> .
root/ConnectionType/view/coreSettings/USBrelevant	Indicates if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/view/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/view/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/view/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/view/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/view/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/view/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/view/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/view/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/view/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/view/coreSettings/serverRequired	Sets whether a server name or address is <i>unused</i> , <i>optional</i> , or <i>required</i> for this connection type.
root/ConnectionType/view/coreSettings/stopProcess	Sets the behavior that should occur when <code>connection-mgr stop</code> is called on this connection. By default this is <code>close</code> , which will send a standard kill signal to the process. When set to <code>kill</code> , the process specified by <code>appName</code> will be forcefully killed. When set to <code>custom</code> , a custom execution script specified by <code>wrapperScript</code> will be executed with the argument <code>stop</code> to terminate the process gracefully.
root/ConnectionType/view/coreSettings/tier	Specifies the relative importance of this connection type and the order in which it is listed in the Create menu.
root/ConnectionType/view/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by <code>appName</code> . This key should not need to be modified.
root/ConnectionType/view/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/view/coreSettings/wrapperScriptGeneration	Lets Connection Manager know what type of parameters to pass to the wrapper script.
root/ConnectionType/view/general/enableComPortRedirection	
root/ConnectionType/view/general/rdpOptions	Options specified here will be forwarded directly to the RDP client if RDP is used as the display protocol for the VMware Horizon View connection. To see a full list of options, enter the following command in an X terminal: <code>rdesktop --help</code> .
root/ConnectionType/view/gui/viewManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/gui/viewManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/view/gui/viewManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.

Table G-11 ConnectionType/view registry keys (continued)

Registry key	Description
root/ConnectionType/view/gui/viewManager/widgets/autostart	Controls the state of the Auto start priority widget in VMware Horizon View Connection Manager. If set to active , the widget is visible in the UI and the user can interact with it. If set to inactive , the widget is hidden. If set to read-only , the widget is visible in the read-only state.
root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection	Controls the state of the Fallback Connection widget in VMware Horizon View Connection Manager. If set to active , the widget is visible in the UI and the user can interact with it. If set to inactive , the widget is hidden. If set to read-only , the widget is visible in the read-only state.
root/ConnectionType/view/gui/viewManager/widgets/label	Controls the state of the Name widget in VMware Horizon View Connection Manager. If set to active , the widget is visible in the UI and the user can interact with it. If set to inactive , the widget is hidden. If set to read-only , the widget is visible in the read-only state.

AVD

AVD registry keys.

Table G-12 AVD registry keys

Registry key	Description
root/ConnectionType/wvd/connections/<UUID>/loginfields/server	If set to 1, the Server field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden. If set to 3, system settings take precedence.
root/ConnectionType/wvd/connections/<UUID>/loginfields/username	If set to 1, the User Name field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden. If set to 3, system settings take precedence.
root/ConnectionType/wvd/connections/<UUID>/loginfields/password	If set to 1, the Password field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden. If set to 3, system settings take precedence.
root/ConnectionType/wvd/connections/<UUID>/loginfields/showPassword	If set to 1, the Show password button is shown in the login dialog for the connection. If set to 2, the button is shown but disabled. If set to 0, the button is hidden. If set to 3, system settings take precedence. For ThinPro 6.2 and later, use the systemwide security setting instead.
root/ConnectionType/wvd/connections/<UUID>/loginfields/domain	If set to 1, the Domain field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden. If set to 3, system settings take precedence.
root/ConnectionType/wvd/connections/<UUID>/loginfields/smartcard	If set to 1, the Smart card login check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden. If set to 3, system settings take precedence. This check box might not appear if no smart card is detected, even if this option is enabled.
root/ConnectionType/wvd/connections/<UUID>/loginfields/domainAwareUsername	If set to 1, the user name is domain aware, whatever the visibility of the domain field. Typically, the user name can be an email address.

Table G-12 AVD registry keys (continued)

Registry key	Description
root/ConnectionType/wvd/connections/<UUID>/ loginfields/rememberme	If set to 1, the Remember me check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden. If set to 3, system settings take precedence.
root/ConnectionType/wvd/connections/<UUID>/ seamlessWindow	If set to 1, window decorations are disabled, which can be useful in a multi-monitor configuration to allow the connection to be set to the size of the primary monitor or full desktop.
root/ConnectionType/wvd/connections/<UUID>/ windowType	This setting is ignored for Smart Zero.
root/ConnectionType/wvd/connections/<UUID>/ windowSizeWidth	Width of the fixed window. This setting is ignored for Smart Zero.
root/ConnectionType/wvd/connections/<UUID>/ windowSizeHeight	Height of the fixed window. This setting is ignored for Smart Zero.
root/ConnectionType/wvd/connections/<UUID>/ displayScalePercent	Amount to scale display in percent. Range is from 100% to 500%.
root/ConnectionType/wvd/connections/<UUID>/ autofillCredentials	If set to 1, the credentials are automatically set in the Microsoft authentication dialog.
root/ConnectionType/wvd/connections/<UUID>/ rememberMe	If set to 1, the credentials are automatically set in the Microsoft authentication dialog.
root/ConnectionType/wvd/connections/<UUID>/ headlessMode	If set to 1, an attempt is made to authenticate with the available credentials without showing the Microsoft authentication dialog.
root/ConnectionType/wvd/connections/<UUID>/ autostartWorkspace	Specifies the workspace from which a resource is to be started automatically. Not required for a resource to start automatically.
root/ConnectionType/wvd/connections/<UUID>/ autostartResource	Specifies a resource to be started automatically.
root/ConnectionType/wvd/connections/<UUID>/ autoCloseAvdFeed	If set to 1, the AVD feed window is closed automatically when a resource is closed.
root/ConnectionType/wvd/connections/<UUID>/ disableMenuBar	If set to 1, the menu bar is not shown in the session window.
root/ConnectionType/wvd/connections/<UUID>/ disableDropdown	If set to 1, the drop-down menu that appears in full-screen mode will not be present.
root/ConnectionType/wvd/connections/<UUID>/ dropdownClose	If set to 1, the drop-down menu will have a button to close the window.
root/ConnectionType/wvd/connections/<UUID>/ dropdownMaximize	If set to 1, the drop-down menu will have a button to maximize the window.
root/ConnectionType/wvd/connections/<UUID>/ dropdownMinimize	If set to 1, the drop-down menu will have a button to minimize the window.
root/ConnectionType/wvd/connections/<UUID>/ dropdownMinimize	If set to 1, the drop-down menu will have a button to minimize the window.
root/ConnectionType/wvd/connections/<UUID>/ dropdownCtrlAltD	If set to 1, the drop-down menu will have Ctrl +Alt + Delete as a keyboard shortcut.
root/ConnectionType/wvd/connections/<UUID>/ localTimezone	If set to 1, the session time zone is set based on the local system time zone.

Table G-12 AVD registry keys (continued)

Registry key	Description
root/ConnectionType/wvd/connections/<UUID>/audioOut	If set to 1, audio playback through AVD connections is enabled.
root/ConnectionType/wvd/connections/<UUID>/audioIn	If set to 1, audio recording (microphone) through AVD connections is enabled.
root/ConnectionType/wvd/connections/<UUID>/filesystem	If 0, file system redirection is disabled; if 1, the list in <code>filesystemList</code> is redirected; if 2, only removable media file systems are redirected.
root/ConnectionType/wvd/connections/<UUID>/filesystemList	A comma-separated list of redirected directories when <code>filesystem</code> is 1.
root/ConnectionType/wvd/connections/<UUID>/scRedirection	If set to 1, smartcards can be accessed in this AVD connection.
root/ConnectionType/wvd/connections/<UUID>/clipboard	If 0, AVD clipboards are not shared with the ThinPro; if 1, the clipboard is shared with all ThinPro applications; if 2, the clipboard is shared only between AVD sessions.
root/ConnectionType/wvd/connections/<UUID>/virtual	If set to 1, the AVD virtual channel is enabled.
root/ConnectionType/wvd/connections/<UUID>/camera	If set to 1, cameras can be accessed in AVD connections.
root/ConnectionType/wvd/connections/<UUID>/ExtraArgs	Specifies extra arguments for the AVD-client. Run <code>wvd-feed --help</code> from an X terminal to see all available arguments.
root/ConnectionType/wvd/connections/<UUID>/authorizations/user/edit	If set to 1, an end user has permission to modify the connection settings for this connection.
root/ConnectionType/wvd/connections/<UUID>/authorizations/user/execution	If set to 1, an end user has permission to run this connection.
root/ConnectionType/wvd/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available so that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/wvd/connections/<UUID>/autoReconnect	If set to 1, the connection is restarted when it is closed or disconnected.
root/ConnectionType/wvd/connections/<UUID>/autostartDelay	Sets the amount of time in seconds to wait before starting the connection after the system starts. The default of 0 causes the connection to start immediately. This setting takes effect only when <code>autostart</code> is set to 1.
root/ConnectionType/wvd/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 causes the connection to reconnect immediately. This setting only takes effect only when <code>autoReconnect</code> is set to 1.

Table G-12 AVD registry keys (continued)

Registry key	Description
root/ConnectionType/wvd/connections/ <UUID>/ forbiddenFiles	This registry key works only when <code>Allow connections</code> to manage their own settings is selected in the Web Browser Connection General Settings Manager. The files listed in this registry key's value are removed before the Web Browser connection is started. The file names should be separated by a comma, and a wildcard is supported. For example: <code>*.rdf,cookies.sqlite</code>
root/ConnectionType/wvd/connections/ <UUID>/ extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/wvd/connections/ <UUID>/ extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/wvd/connections/ <UUID>/ extraEnvValues/<UUID>/ credentialsType	Specifies whether credentials are to be supplied by Single Sign-On, requested at startup, or a supplied as a preconfigured user, domain, and password.
root/ConnectionType/wvd/connections/ <UUID>/ username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.
root/ConnectionType/wvd/connections/ <UUID>/domain	If the <code>credentialsType</code> is <code>password</code> , this setting supplies the default domain to the remote host during login. If a domain is not specified, the default domain for the remote host will be used.
root/ConnectionType/wvd/connections/ <UUID>/ SingleSignOn	If enabled, the user, domain, and password combination of the RDP connection is saved to be used to unlock the screensaver.
root/ConnectionType/wvd/connections/ <UUID>/ password	Sets the default password to supply to the remote host during login. This value will be encrypted. Generally, this setting is used for kiosk-style applications where a generic password is used for login.
root/ConnectionType/wvd/connections/ <UUID>/ workspaceURL	Sets the workspace URL to provide to wvd. If no URL is specified, the default URL for the AVD is used.
root/ConnectionType/wvd/connections/ <UUID>/ allowInsecureConnections	If set to 1, the insecure connection will be allowed to proceed.
root/ConnectionType/wvd/connections/ <UUID>/ securityLevelclcl	Sets the certificate security level. If set to 0, all connections are allowed. If set to 1, remembered hosts are checked, and a warning dialog is shown if verification is not passed. If set to 2, remembered hosts are not checked, and a warning dialog is shown if verification is not passed. If set to 3, all insecure connections are refused.
root/ConnectionType/wvd/connections/ <UUID>/ coord	This registry key is either used internally or reserved for future use. Do not change this value.
root/ConnectionType/wvd/connections/ <UUID>/ autostart	If set to a value of 1-5, the connection starts automatically after the system starts, with the value of 1 having the highest priority.
root/ConnectionType/wvd/connections/ <UUID>/ dependConnectionId	This registry key is either used internally or reserved for future use. Do not change this value.

Table G-12 AVD registry keys (continued)

Registry key	Description
root/ConnectionType/wvd/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/wvd/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/wvd/connections/<UUID>/startMode	If set to the default <code>focus</code> 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/wvd/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to <code>Default Connection</code> and does not display in the UI.
root/ConnectionType/wvd/connections/<UUID>/iconPosition	For pinned desktop icons, an x,y pair. For floating icons, leave this string blank.
root/ConnectionType/wvd/connections/<UUID>/afterStartedCommand	Sets the command to run after the connection starts.
root/ConnectionType/wvd/connections/<UUID>/afterStoppedCommand	Sets the command to run after the connection stops.
root/ConnectionType/wvd/connections/<UUID>/beforeStartingCommand	Sets the command to run before the connection starts.
root/ConnectionType/wvd/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. Do not change this value.

xmcp

XDMCP registry keys.

Table G-13 XDMCP registry keys

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

Table G-13 XDMCP registry keys (continued)

Registry key	Description
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/execution	If set to 1, an end user has permission to execute this connection.
root/ConnectionType/xdmcp/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/xdmcp/connections/<UUID>/autostart	If set to a value of 1-5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/xdmcp/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/xdmcp/connections/<UUID>/color	Sets the color depth of the display for the connection.
root/ConnectionType/xdmcp/connections/<UUID>/connectionEndAction	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/xdmcp/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/xdmcp/connections/<UUID>/fontServer	Sets the address of the font server to use. The registry key <code>useFontServer</code> must also be set to 1.
root/ConnectionType/xdmcp/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/xdmcp/connections/<UUID>/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to <code>Default Connection</code> and does not display in the UI.
root/ConnectionType/xdmcp/connections/<UUID>/loginfields/server	If set to 1, the Server box is shown in the login dialog for the connection. If set to 2, the box is shown but disabled. If set to 0, the box is hidden. If set to 3, the system settings are used.
root/ConnectionType/xdmcp/connections/<UUID>/refreshRate	Sets the refresh rate of the display for the connection.
root/ConnectionType/xdmcp/connections/<UUID>/startMode	If set to the default <code>focus</code> and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/xdmcp/connections/<UUID>/type	Sets the XDMCP connection type. If set to <code>chooser</code> , all available hosts are listed and the user can select which one to connect to. If set to <code>query</code> , an XDMCP request is sent to the specified host directly. If set to <code>broadcast</code> , all available hosts are listed and the first one is connected to automatically.

Table G-13 XDMCP registry keys (continued)

Registry key	Description
root/ConnectionType/xdmcp/connections/<UUID>/useFontServer	If set to 1, the font server is enabled. If set to 0, the local font is used.
root/ConnectionType/xdmcp/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/xdmcp/connections/<UUID>/windowSize	Sets the window size of the connection.
root/ConnectionType/xdmcp/coreSettings/USBrelevant	Specifies if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/xdmcp/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/audio	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/desktopButton	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/xdmcp/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.
root/ConnectionType/xdmcp/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/xdmcp/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/xdmcp/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/xdmcp/coreSettings/label	Sets the name to display for this connection type in the UI.
root/ConnectionType/xdmcp/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/xdmcp/coreSettings/serverRequired	Sets whether a server name or address is unused, optional, or required for this connection type.

Table G-13 XDMCP registry keys (continued)

Registry key	Description
root/ConnectionType/xdmcp/coreSettings/stopProcess	Sets the behavior that should occur when <code>connection-mgr stop</code> is called on this connection. By default this is <code>close</code> , which will send a standard kill signal to the process. When set to <code>kill</code> , the process specified by <code>appName</code> will be forcefully killed. When set to <code>custom</code> , a custom execution script specified by <code>wrapperScript</code> will be executed with the argument <code>stop</code> to terminate the process gracefully.
root/ConnectionType/xdmcp/coreSettings/tier	Specifies the relative importance of this connection type and the order in which it is listed in the Create menu.
root/ConnectionType/xdmcp/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by <code>appName</code> . This key should not need to be modified.
root/ConnectionType/xdmcp/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/xdmcp/gui/XdmcpManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/gui/XdmcpManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/gui/XdmcpManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/address	Controls the state of the Address widget in XDMCP Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect	Controls the state of the Auto reconnect widget in XDMCP Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autostart	Controls the state of the Auto start priority widget in XDMCP Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/color	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/fontServer	Controls the state of the Font server widget in XDMCP Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/hasDesktopIcon	Controls the state of the Show icon on desktop widget in XDMCP Connection Manager. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/isInMenu	This registry key is either used internally or reserved for future use. The value should not be changed.

Table G-13 XDMCP registry keys (continued)

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

xen

ConnectionType/xen registry keys.

Table G-14 ConnectionType/xen registry keys

Registry key	Description
root/ConnectionType/xen/authorizations/user/add	If set to 1, an end user has permission to add a new connection of this type using Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/xen/authorizations/user/general	If set to 1, an end user has permission to modify the general settings for this connection type using Connection Manager. This key has no effect on Smart Zero.
root/ConnectionType/xen/connections/<UUID>/SingleSignOn	If set to 1, the connection shares credentials with the screen saver.
root/ConnectionType/xen/connections/<UUID>/address	Sets the address of the remote host to connect to. This is typically a URL such as <code>http://server.domain.com</code> .
root/ConnectionType/xen/connections/<UUID>/afterStartedCommand	Sets the command to execute after the connection has been started.
root/ConnectionType/xen/connections/<UUID>/afterStoppedCommand	Sets the command to execute after the connection has been stopped.
root/ConnectionType/xen/connections/<UUID>/allowSaveConnInfo	

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/connections/<UUID>/appInMenu	If set to 1, all applications for the connection are displayed in the taskbar menu.
root/ConnectionType/xen/connections/<UUID>/appInWindowOrOnDesktop	If set to 1 and appOnDesktop is enabled, all applications for the connection are displayed in a broker window. If set to 0, the applications for the connection are displayed directly on the desktop.
root/ConnectionType/xen/connections/<UUID>/appOnDashboard	If set to 1, all applications for the connection will be displayed on the taskbar.
root/ConnectionType/xen/connections/<UUID>/appOnDesktop	If set to 1, all applications for the connection will be displayed on the desktop.
root/ConnectionType/xen/connections/<UUID>/authorizations/user/edit	If set to 1, an end user has permission to modify the connection settings for this connection.
root/ConnectionType/xen/connections/<UUID>/authorizations/user/execution	If set to 1, an end user has permission to execute this connection.
root/ConnectionType/xen/connections/<UUID>/autoLaunchSingleApp	If set to 1, and if only a single published application or desktop is returned by the Citrix server, that resource will be launched automatically.
root/ConnectionType/xen/connections/<UUID>/autoReconnect	If set to 1, the connection will be restarted when it is closed or disconnected.
root/ConnectionType/xen/connections/<UUID>/autoReconnectAppsOnLogin	If set to 1, the system will attempt to reconnect any active or disconnected Citrix sessions upon initial login.
root/ConnectionType/xen/connections/<UUID>/autoReconnectDelay	Sets the amount of time in seconds to wait before reconnecting the session. The default of 0 will cause the connection to reconnect immediately. This setting only takes effect when autoReconnect is set to 1.
root/ConnectionType/xen/connections/<UUID>/autoRefreshInterval	Controls the amount of time in seconds before the resources are cleared and refreshed again from the server. Set to -1 to disable. It is normally not required to frequently refresh the resources from the server.
root/ConnectionType/xen/connections/<UUID>/autoStartDesktop	If set to 1 and if autoStartResource is empty, the first desktop to become available when the connection is started will be launched automatically.
root/ConnectionType/xen/connections/<UUID>/autoStartResource	Sets the name of the desktop or application to start automatically when the connection is launched.
root/ConnectionType/xen/connections/<UUID>/autoStartWithGuessing	If set to 1, the connection tries to launch autoStartDesktop or autoStartResource first. If the connection cannot launch either successfully, it tries to launch another resource by guessing.
root/ConnectionType/xen/connections/<UUID>/autostart	If set to a value of 1-5, the connection will be started automatically after the system boots, with the value of 1 having the highest priority.
root/ConnectionType/xen/connections/<UUID>/autostartDelay	Reserved for future use.
root/ConnectionType/xen/connections/<UUID>/beforeStartingCommand	Sets the command to execute before the connection starts.
root/ConnectionType/xen/connections/<UUID>/connectionMode	Sets the Citrix connection mode for the connection.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/connections/<UUID>/connectionStopAction	Defines the action to be done when the connection is ended from Connection Manager. The available options are <code>disconnect</code> and <code>logoff</code> .
root/ConnectionType/xen/connections/<UUID>/continueWithNewPassword	If set to 1, after resetting the password, the connection continues to launch with the new password. If set to 0, after resetting the password, the current connection closes.
root/ConnectionType/xen/connections/<UUID>/coord	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/connections/<UUID>/credentialsType	Specifies the credential type between <code>anonymous</code> (unauthenticated access), <code>sso</code> (single sign-on), <code>startup</code> (credentials are requested at startup), <code>password</code> (preconfigured user/domain/password), or <code>smartcard</code> (preconfigured smart card).
root/ConnectionType/xen/connections/<UUID>/dependConnectionId	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/connections/<UUID>/domain	Sets the domain to provide to the XenDesktop server. If no domain is specified, the default domain for the server is used.
root/ConnectionType/xen/connections/<UUID>/enableRSAToken	CAUTION: This functionality is unsupported. If set to 1, the user will be prompted before connecting for a security token value to use when authenticating with NetScaler Gateway.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/key	Sets the name of an extra environment variable for use with the connection.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/value	Sets the value of an extra environment variable for use with the connection.
root/ConnectionType/xen/connections/<UUID>/fallBackConnection	Sets the fallback connection via its UUID.
root/ConnectionType/xen/connections/<UUID>/folder	
root/ConnectionType/xen/connections/<UUID>/forceHttps	If set to 1, only HTTPS connections are allowed.
root/ConnectionType/xen/connections/<UUID>/fullscreen	If set to 1, the Citrix client launches in full-screen mode when started.
root/ConnectionType/xen/connections/<UUID>/hasDesktopIcon	If set to 1, the desktop icon for this connection is enabled. This key has no effect on Smart Zero.
root/ConnectionType/xen/connections/<UUID>/iconPosition	Sets the x,y coordinates of a pinned desktop icon. If not specified, the icon floats.
root/ConnectionType/xen/connections/<UUID>/ignoreCertCheck	If set to 1, certificate checks are ignored for the connection.
root/ConnectionType/xen/connections/<UUID>/label	Sets the connection name that is displayed in the UI. On Smart Zero, this will typically be set to <code>Default Connection</code> and does not display in the UI.
root/ConnectionType/xen/connections/<UUID>/logOnMethod	
root/ConnectionType/xen/connections/<UUID>/loginfields/domain	If set to 1, the Domain field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/connections/<UUID>/loginfields/password	If set to 1, the Password field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.
root/ConnectionType/xen/connections/<UUID>/loginfields/rememberme	If set to 1, the Remember me check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden.
root/ConnectionType/xen/connections/<UUID>/loginfields/server	If set to 1, the Server box is shown in the login dialog for the connection. If set to 2, the box is shown but disabled. If set to 0, the box is hidden. If set to 3, the system settings are used.
root/ConnectionType/xen/connections/<UUID>/loginfields/showpassword	If set to 1, the Show password button is shown in the login dialog for the connection. If set to 2, the button is shown but disabled. If set to 0, the button is hidden.
root/ConnectionType/xen/connections/<UUID>/loginfields/smartcard	If set to 1, the Smart card login check box is shown in the login dialog for the connection. If set to 2, the check box is shown but disabled. If set to 0, the check box is hidden. This check box might not appear if no smart card is detected, even if this option is enabled.
root/ConnectionType/xen/connections/<UUID>/loginfields/username	If set to 1, the User Name field is shown in the login dialog for the connection. If set to 2, the field is shown but disabled. If set to 0, the field is hidden.
root/ConnectionType/xen/connections/<UUID>/password	Sets the default password to supply to the remote host during login. This value will be encrypted. Generally, this setting is used for kiosk-style applications where a generic password is used for login.
root/ConnectionType/xen/connections/<UUID>/resListRequest	If set to 1, a connection only lists the resources without launching them or downloading icons.
root/ConnectionType/xen/connections/<UUID>/saveNewUrl	This is an internal value. If set to <code>ToBeAsked</code> , the script prompts the user. If set to <code>Auto</code> , the script does not prompt the user, and whether the URL is saved depends on the case. If set to <code>Yes</code> , the user asked to save the new URL. If set to <code>No</code> , the user asked to not save the new URL.
root/ConnectionType/xen/connections/<UUID>/savePassword	
root/ConnectionType/xen/connections/<UUID>/smartCardModuleKey	Specifies the security module to use for a smart card connection.
root/ConnectionType/xen/connections/<UUID>/startMode	If set to the default <code>focus</code> and the connection is already started, the connection will be given focus. Otherwise, an error will be returned stating that the connection is already started.
root/ConnectionType/xen/connections/<UUID>/subscribedOnly	If set to 1, only subscribed resources for the connection are displayed.
root/ConnectionType/xen/connections/<UUID>/unplugSmartCardAction	Sets the action to perform when a smart card is unplugged during a connection. <code>disconnect</code> will disconnect the current session. <code>close</code> will close all the opened resources. <code>noaction</code> will do nothing.
root/ConnectionType/xen/connections/<UUID>/useCurrentCitrixConfig	
root/ConnectionType/xen/connections/<UUID>/username	Sets the default user name to supply to the remote host during login. Generally, this setting is used for kiosk-style applications where a generic user name is used for login.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/connections/<UUID>/waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/xen/coreSettings/USBrelevant	Specifies if this connection type is USB-relevant. If it is, it might have a USB plugin for redirecting USB devices.
root/ConnectionType/xen/coreSettings/appName	Sets the internal application name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch	This setting applies to Citrix servers with multiple published resources. If less than 0, no auto-logout is performed. Otherwise, this setting dictates the number of seconds between the closing of the last Xen published resource and when the user is logged out automatically and returned to the initial login screen. Citrix process delays might extend the auto-logout time.
root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch	This setting applies to Citrix servers with multiple published resources. If less than 0, no auto-logout is performed. Otherwise, this setting dictates the number of seconds allowed to pass while no applications are launched before the user is logged out automatically and returned to the initial login screen. Citrix process delays might extend the auto-logout time.
root/ConnectionType/xen/coreSettings/className	Sets the internal application class name to use for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/connectionUtil	Sets the Citrix connection utility for the connection.
root/ConnectionType/xen/coreSettings/credsCache	Specifies whether the Connection Manager caches the credentials for further use.
root/ConnectionType/xen/coreSettings/editor	Sets the internal application name to use when Connection Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/generalSettingsEditor	Sets the internal application name to use when the General Settings Manager is launched for this connection type. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/icon	Specifies the icon from the icon theme set to use for this connection.
root/ConnectionType/xen/coreSettings/icon16Path	Sets the path to the 16 × 16 pixel icon for this application.
root/ConnectionType/xen/coreSettings/icon32Path	Sets the path to the 32 × 32 pixel icon for this application.
root/ConnectionType/xen/coreSettings/icon48Path	Sets the path to the 48 × 48 pixel icon for this application.
root/ConnectionType/xen/coreSettings/iconActive	Reserved for future use.
root/ConnectionType/xen/coreSettings/label	Sets the name to display for this connection type in the UI.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/coreSettings/priorityInConnectionLists	Sets the priority of this connection type when it is displayed in Connection Manager and the Configuration Wizard that displays during initial setup. A higher value will move the connection type towards the top of the list. If set to 0, the connection type is hidden from Configuration Wizard and is shown last in Connection Manager. Connections types with the same priority are listed in alphabetical order.
root/ConnectionType/xen/coreSettings/retryTimeout	This setting applies when a virtual machine is restarting and is not yet available to launch as a Citrix resource. If set to a negative number, reconnection is not attempted. Otherwise, it gives the time (in seconds) that HP ThinPro attempts to reconnect to the virtual machine.
root/ConnectionType/xen/coreSettings/serverRequired	Sets whether a server name or address is <i>unused</i> , <i>optional</i> , or <i>required</i> for this connection type.
root/ConnectionType/xen/coreSettings/stopProcess	Sets the behavior that should occur when <code>connection-mgr stop</code> is called on this connection. By default this is <code>close</code> , which will send a standard kill signal to the process. When set to <code>kill</code> , the process specified by <code>appName</code> will be forcefully killed. When set to <code>custom</code> , a custom execution script specified by <code>wrapperScript</code> will be executed with the argument <code>stop</code> to terminate the process gracefully.
root/ConnectionType/xen/coreSettings/tier	Specifies the relative importance of this connection type and the order in which it is listed in the Create menu.
root/ConnectionType/xen/coreSettings/watchPid	If set to 1, the connection is monitored under the name specified by <code>appName</code> . This key should not need to be modified.
root/ConnectionType/xen/coreSettings/wrapperScript	Sets the script or binary to execute when launching this connection type. This is the primary script handling all connection settings and command line arguments for the connection. This key should not need to be modified.
root/ConnectionType/xen/coreSettings/wrapperScriptGeneration	Lets Connection Manager know what type of parameters to pass to the wrapper script.
root/ConnectionType/xen/general/CGPAddress	<p>Specifies the CGP address using the syntax <code>hostname:port</code>.</p> <p>Optionally, instead of specifying the hostname, you can type an asterisk (*). This will use the value from the connection's address registry key as the host. For example: <code>*:2598</code></p> <p>The port value is optional. If you do not specify a port value, the default of 2598 is used. If a connection on port 2598 fails, the thin client tries to establish a connection on port 1494.</p>
root/ConnectionType/xen/general/TWIMode	Controls seamless mode for published applications. This setting directly maps to the Citrix .ini file setting <code>TWIMode</code> .
root/ConnectionType/xen/general/TWIModeResizeType	This setting directly maps to the Citrix .ini file setting <code>TWIMoveResizeType</code> .
root/ConnectionType/xen/general/allowReadOnA ... allowReadOnZ	If set to 1, a user can read the mapped drive.
root/ConnectionType/xen/general/allowWriteOnA ... allowWriteOnZ	If set to 1, a user can write to the mapped drive.
root/ConnectionType/xen/general/async	If set to 1, asynchronous polling is enabled. This setting directly maps to the Citrix .ini file setting <code>CommPollSize</code> .

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/general/ autoReconnect	If set to 1, automatic session reconnection is enabled. This is not the same as the connection-specific auto-reconnect. This occurs internally within the Citrix client without restarting the connection. This setting directly maps to the Citrix .ini file setting <code>TransportReconnectEnabled</code> .
root/ConnectionType/xen/general/ bitmapCacheSize	Sets the minimum size for bitmap caching. This setting directly maps to the Citrix .ini file setting <code>PersistentCacheMinBitmap</code> .
root/ConnectionType/xen/general/ bottomMonitor	Sets the screen area of the bottom monitor to show the virtual desktop. If set to 0, the monitor is not used to show the virtual desktop.
root/ConnectionType/xen/general/colorDepth	Forces a specific color depth for all connections. This is usually done only in specialized environments where the automatic depth selection fails or in very slow networks to reduce congestion.
root/ConnectionType/xen/general/colorMapping	If set to <code>Shared - Approximate Colors</code> , approximate colors from the default colormap are used. If set to <code>Private - Exact Colors</code> , precise colors are used. This setting directly maps to the Citrix .ini file setting <code>ApproximateColors</code> .
root/ConnectionType/xen/general/ contentRedirection	If set to 1, links from web content are sent from the server to the client so that the client can try to open them locally.
root/ConnectionType/xen/general/ debugLogLevel	If set to 0, no debug log is created. If set to 3, an error level log is created. If set to 4, a warning level log is created. If set to 7, all debug level logs are created.
root/ConnectionType/xen/general/ defaultBrowserProtocol	Controls the protocol used to locate the host for the connection. If not specified, the default value from the <code>[WFClient]</code> section of <code>wfclient.ini</code> is used. This setting directly maps to the Citrix .ini file setting <code>BrowserProtocol</code> .
root/ConnectionType/xen/general/ drivePathMappedOnA ... drivePathMappedOnZ	Sets the local filesystem directory to map to the remote host. Typically this is set to <code>/media</code> to allow all connected USB drives to be mapped to the remote host via a single drive letter.
root/ConnectionType/xen/general/ enableAlertSound	If set to 1, Windows alert sounds are enabled. This setting indirectly maps to the Citrix .ini file setting <code>DisableSound</code> .
root/ConnectionType/xen/general/ enableClipboard	If set to 1, clipboard redirection is enabled.
root/ConnectionType/xen/general/ enableConnectionBar	If set to 1, enables Citrix Desktop Viewer in the session user interface. By default, this setting is set to 0 (disabled) on the client side because this value is set on the client by the ICA file for a desktop session.
root/ConnectionType/xen/general/ enableCursorColors	If set to 1, colored cursors are enabled. Setting this to 0 might fix graphical cursor corruption in some cases.
root/ConnectionType/xen/general/ enableDataCompression	If set to 1, data compression is enabled. This setting directly maps to the Citrix .ini file setting <code>Compress</code> .
root/ConnectionType/xen/general/ enableDriveMapAndRedirect	If set to 1, mapping and redirection for USB storage devices is enabled.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/general/ enableDriveMapping	If set to 1, directories on the local filesystem can be forwarded to the remote host via a virtual drive. Typically /media is mapped to z to allow USB drives to be forwarded to the remote host. If USB redirection is enabled, this setting should be disabled to prevent storage conflicts. To be properly mapped to the remote host in this fashion, the USB device must use one of the following filesystems: FAT32, NTFS, ext2, ext3.
root/ConnectionType/xen/general/ enableDynamicDriveMapping	If set to 1, USB storage devices will be dynamically mapped on the Citrix server. If set to 0, dynamic mapping of USB storage devices is disabled.
root/ConnectionType/xen/general/ enableH264Compression	If set to 1, H.264 compression is enabled. The H.264 codec provides better performance of rich and professional graphics applications on WAN networks than the JPEG codec.
root/ConnectionType/xen/general/ enableHDXFlashRedirection	NOTE: This feature is supported for the 32-bit version of HP ThinPro only. Controls the behavior of HDX Flash Redirection. If set to Always, HDX Flash Redirection is used if possible, and the user is not prompted. If set to Ask, the user is prompted. If set to Never, the feature is disabled.
root/ConnectionType/xen/general/ enableHDXFlashServerContentFetch	NOTE: This feature is supported for the 32-bit version of HP ThinPro only. Controls the behavior of HDX Flash Server-Side Content Fetching. If disabled, the client will fetch for content.
root/ConnectionType/xen/general/ enableHDXMediaStream	If set to 1, HDX MediaStream is enabled. If set to 0, media files will still play via standard streaming, but the quality might not be as high.
root/ConnectionType/xen/general/enableHWH264	If set to 1, and if enableH264Compression is also set to 1, hardware compression for H.264 is enabled. If set to 0, H.264 compression will be handled by software.
root/ConnectionType/xen/general/ enableMapOnA ... enableMapOnZ	If set to 1, a local filesystem directory can be mapped to this drive on the remote host. The corresponding drivePathMappedOn registry key must be set to a valid local directory for drive mapping to work properly.
root/ConnectionType/xen/general/ enableMultiMedia	If set to 1, multimedia is enabled. HDX Lync might have a conflict when this setting is enabled. This setting maps directly to the multimedia in the virtual channels section of the Citrix .ini file settings. Enable this setting when HDX MediaStream is enabled.
root/ConnectionType/xen/general/ enableOffScreenSurface	If set to 1, the server can use the X PixMap format for off-screen drawing. This reduces bandwidth in 15-bit and 24-bit color modes at the expense of X server memory and processor time. This setting directly maps to the Citrix .ini file setting EnableOSS.
root/ConnectionType/xen/general/ enableRC4128SHA	
root/ConnectionType/xen/general/enableRC4MD5	
root/ConnectionType/xen/general/ enableSessionReliability	If set to 1, Citrix Session Reliability is enabled. Session Reliability changes the way sessions are resumed after losing a network connection. See Citrix documentation for more information on Session Reliability.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/general/enableSmallFrames	If set to 1, small non-H.264 rectangle updates are enabled for H.264. enableTextTracking must also be enabled for this to have an effect.
root/ConnectionType/xen/general/enableSmartCard	If set to 1, smart card login is enabled.
root/ConnectionType/xen/general/enableTLRSA	
root/ConnectionType/xen/general/enableTextTracking	If set to 1, optimized lossless text overlays are enabled for H.264.
root/ConnectionType/xen/general/enableUSBRedirection	If set to 1, USB storage devices will be redirected.
root/ConnectionType/xen/general/encryptionLevel	Sets the level of encryption. Encryption protocols for all levels are defined in the [EncryptionLevelSession] section of module.ini. This setting directly maps to the Citrix .ini file setting [EncryptionLevelSession].
root/ConnectionType/xen/general/fontSmoothingType	Sets the font smoothing type.
root/ConnectionType/xen/general/hotKey<1thru15>Char	Sets the hot key to forward to the remote session when the key or key combination set in the corresponding hotKeyShift is pressed.
root/ConnectionType/xen/general/hotKey<1thru15>Shift	Sets the key or key combination used to activate the hot key set in the corresponding hotKeyChar.
root/ConnectionType/xen/general/httpAddresses/<UUID>/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Sets the keyboard key for disabling the transparent keyboard mode. This setting directly maps to the Citrix .ini file setting KeyPassthroughEscapeChar.
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Sets the keyboard key combination for disabling the transparent keyboard mode. This setting directly maps to the Citrix .ini file setting KeyPassthroughEscapeShift.
root/ConnectionType/xen/general/keyboardMappingFile	Specifies a keyboard mapping file for a Citrix session. By default, the startup script selects a keyboard mapping file based on the keyboard layout.
root/ConnectionType/xen/general/lastComPortNum	Sets the number of mapped serial ports. If set to 0, serial port mapping is disabled.
root/ConnectionType/xen/general/leftMonitor	Sets the screen area of the left monitor to show the virtual desktop. If set to 0, the monitor is not used to show the virtual desktop.
root/ConnectionType/xen/general/localTextEcho	Controls keyboard latency reduction. This setting indirectly maps to the Citrix .ini file setting ZLKeyboardMode.
root/ConnectionType/xen/general/monitorNetwork	If set to Off, network connectivity is not monitored. If set to Local network link status only, only the local network link status is monitored. If set to Server online status, both the local network link status and server connectivity are monitored.
root/ConnectionType/xen/general/mouseClickFeedback	Controls mouse latency reduction. This setting indirectly maps to the Citrix .ini file setting ZLMouseMode.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/general/ mouseMiddleButtonPaste	If set to 1, middle mouse button paste emulation for Windows sessions is enabled. This setting directly maps to the Citrix .ini file setting <code>MouseSendsControlV</code> .
root/ConnectionType/xen/general/noInfoBox	If set to 1, the client manager (wfcmgr) will not display when a client session terminates. This setting directly maps to the Citrix .ini file setting <code>PopupOnExit</code> .
root/ConnectionType/xen/general/ printerAutoCreation	If set to 0, printer mapping is disabled. If set to 1, printers defined locally will be mapped to the connection. If set to 2, USB printers are redirected as configured in USB Manager.
root/ConnectionType/xen/general/proxyAddress	Sets the proxy address to use if a manual proxy setting is selected via <code>proxyType</code> .
root/ConnectionType/xen/general/ proxyPassword	Sets the proxy password to use if a manual proxy setting is selected via <code>proxyType</code> . This password will be encrypted using rc4 encryption.
root/ConnectionType/xen/general/proxyPort	Sets the proxy port to use if a manual proxy setting is selected via <code>proxyType</code> .
root/ConnectionType/xen/general/proxyType	Sets the type of proxy to use for XenDesktop connections. The value <code>Use Browser settings</code> is only supported if a local browser is installed.
root/ConnectionType/xen/general/proxyUser	Sets the proxy username to use if a manual proxy setting is selected via <code>proxyType</code> .
root/ConnectionType/xen/general/rightMonitor	Sets the screen area of the right monitor to show the virtual desktop. If set to 0, the monitor is not used to show the virtual desktop.
root/ConnectionType/xen/general/saveLogs	If set to 1, detailed log information is saved after the session ends. This log information will be saved to the following directory: <code>/tmp/debug/citrix/<date>/</code>
root/ConnectionType/xen/general/selfservice/ disableConfigMgr	If set to 1, session-sharing requests are sent to other Citrix sessions on the same X display. This setting directly maps to the Citrix .ini file setting <code>EnableSessionSharingClient</code> .
root/ConnectionType/xen/general/selfservice/ disableConnectionCenter	
root/ConnectionType/xen/general/selfservice/ enableKioskMode	
root/ConnectionType/xen/general/selfservice/ sharedUserMode	
root/ConnectionType/xen/general/selfservice/ showTaskBarInKioskMode	
root/ConnectionType/xen/general/ serverCheckTimeout	
root/ConnectionType/xen/general/ sessionReliabilityTTL	Specifies the session reliability timeout in seconds. This configures the Session Reliability Time To Live (TTL).
root/ConnectionType/xen/general/ showOnAllMonitors	If set to 1, the virtual desktop will be shown on all monitors.
root/ConnectionType/xen/general/ smartCardModuleMap/CoolKeyPK11	Specifies the path to the CoolKey PKCS #11 smart card security module.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/general/smartCardModuleMap/GemaltoDotNet	Specifies the path to the Gemalto .NET smart card security module.
root/ConnectionType/xen/general/sound	Sets the sound quality. This setting indirectly maps to the Citrix .ini file setting AudioBandwidthLimit.
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/<UUID>/address	
root/ConnectionType/xen/general/topMonitor	Sets the screen area of the top monitor to show the virtual desktop. If set to 0, the monitor is not used to show the virtual desktop.
root/ConnectionType/xen/general/transparentKeyPassthrough	Controls how certain Windows key combinations handled. If set to Translated, the key combinations apply to the local desktop. If set to Direct in full screen desktops only, the key combinations apply to the remote session only when it is in full screen mode. If set to Direct, the key combinations always apply to the remote session as long as the window has focus. This setting indirectly maps to the Citrix .ini file setting TransparentKeyPassthrough.
root/ConnectionType/xen/general/transportProtocol	Sets the transport protocol. If set to On (default), the connection uses UDP and does not fall back on TCP if there is a failure. If set to Off, the connection uses TCP. If set to Preferred, the connection tries to use UDP first and falls back on TCP if there is a failure.
root/ConnectionType/xen/general/twRedundantImageItems	Controls the number of screen areas that will be tracked in ThinWire to prevent redundant drawing of bitmap images. An adequate value for 1024 × 768 sessions is 300.
root/ConnectionType/xen/general/useAlternateAddress	If set to 1, an alternate address is used for firewall connections. This setting directly maps to the Citrix .ini file setting UseAlternateAddress.
root/ConnectionType/xen/general/useBitmapCache	If set to 1, the persistent disk cache is enabled. The persistent disk cache stores commonly-used graphical objects such as bitmaps on the hard disk of the thin client. Using the persistent disk cache increases performance across low-bandwidth connections but reduces the amount of available disk space on the thin client. For thin clients on high-speed LANs, usage of the persistent disk cache is not necessary. This setting directly maps to the Citrix .ini file setting PersistentCacheEnabled.
root/ConnectionType/xen/general/useEUKS	Controls the use of Extended Unicode Keyboard Support (EUKS) on Windows servers. If set to 0, EUKS is not used. If set to 1, EUKS is used as a fallback. If set to 2, EUKS is used whenever possible.
root/ConnectionType/xen/general/useLocalIM	If this setting is enabled, the local X input method is used to interpret keyboard input. This is supported for European languages only. This setting directly maps to the Citrix .ini file setting useLocalIME.
root/ConnectionType/xen/general/userAgent	The string from this key will be presented by the Citrix client and will be helpful for administrators to know where the connection request is from.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/general/ waitForNetwork	If set to 1, the connection will not be launched until networking is available. This ensures that, on a slow network, the connection does not launch before networking is available, which could cause a failure.
root/ConnectionType/xen/general/ webcamFramesPerSec	Controls the HDXWebCamFramesPerSec variable in the All_Regions.ini file.
root/ConnectionType/xen/general/webcamHeight	Controls the HDXWebCamHeight variable in the All_Regions.ini file.
root/ConnectionType/xen/general/ webcamQuality	Controls the HDXWebCamQuality variable in the All_Regions.ini file. Valid input ranges from 1 to 63.
root/ConnectionType/xen/general/ webcamSupport	If set to 0, the webcam and webcam audio are disabled. If set to 1, the webcam and webcam audio are enabled, with compression. If set to 2, USB redirection of the webcam and webcam audio is enabled.
root/ConnectionType/xen/general/webcamWidth	Controls the HDXWebCamWidth variable in the All_Regions.ini file.
root/ConnectionType/xen/general/windowHeight	Sets the height of the window in pixels if windowSize is set to Fixed Size.
root/ConnectionType/xen/general/ windowPercent	Sets the size of the window as a percentage if windowSize is set to Percentage of Screen Size.
root/ConnectionType/xen/general/windowSize	If set to Default, the server-side settings are used. If set to Full Screen, the window is maximized without borders on all available screens. If set to Fixed Size, the windowHeight and windowWidth registry keys can be used to specify the size of the window in pixels. If set to Percentage of Screen Size, the windowPercent key can be used to specify the size of the window as a percentage. For Percentage of Screen Size to take effect, enableForceDirectConnect must be set to 1 and TWIMode must be set to 0. This setting only works with XenApp and only if the server allows direct connections. This setting does not work with XenDesktop.
root/ConnectionType/xen/general/windowWidth	Sets the width of the window in pixels if windowSize is set to Fixed Size.
root/ConnectionType/xen/gui/XenDesktopPanel/ disabled	If set to 1, the Xen Desktop panel and its taskbar are disabled. This is usually used when autoStartResource or autoStartDesktop is enabled.
root/ConnectionType/xen/gui/XenManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/gui/XenManager/ status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/gui/XenManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/ConnectionType/xen/gui/XenManager/ widgets/address	Controls the state of the Service URL widget in Citrix Connection Manager. If set to active, the widget is visible in the UI and the user can interact with it. If set to inactive, the widget is hidden. If set to read-only, the widget is visible in the read-only state.

Table G-14 ConnectionType/xen registry keys (continued)

Registry key	Description
root/ConnectionType/xen/gui/XenManager/widgets/appInMenu	Controls the state of the Show applications on taskbar widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop	Controls the state of the Show applications on desktop widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect	Controls the state of the Auto reconnect widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop	Controls the state of the Auto Start Desktop widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource	Controls the state of the Auto Start Resource widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/autostart	Controls the state of the Auto start priority widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/domain	Controls the state of the Domain widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection	Controls the state of the Fallback Connection widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/folder	
root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon	Controls the state of the Show icon on desktop widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/ConnectionType/xen/gui/XenManager/widgets/label	Controls the state of the Name widget in Citrix Connection Manager. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.

Table G-14 ConnectionType/xen registry keys (continued)

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

DHCP

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

Dashboard

Dashboard registry keys.



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

Table G-15 Dashboard registry keys

Registry key	Description
root/Dashboard/GUI/Clock	If set to 1, the clock is shown on the taskbar.
root/Dashboard/GUI/DomainUser	If set to 1, the domain-user icon is shown on the taskbar if the system is in domain-login mode.
root/Dashboard/GUI/PowerButton	If set to 1, the power button is shown on the taskbar.
root/Dashboard/GUI/Search	If set to 1, the Search button is shown on the taskbar.
root/Dashboard/GUI/SystemTray	If set to 1, the system tray is shown on the taskbar.
root/Dashboard/GUI/TaskBar	If set to 1, the application area is shown on the taskbar.
root/Dashboard/General/AutoHide	If set to 1, the taskbar auto-hides.
root/Dashboard/General/EnterLeaveTimeout	Sets the amount of time in milliseconds before the taskbar will hide or show when <code>AutoHide</code> is enabled.

Table G-15 Dashboard registry keys (continued)

Registry key	Description
<code>root/Dashboard/General/IconSize</code>	Sets the size of the icons on the taskbar. If set to -1, the size of the icon is based on the width of the taskbar.
<code>root/Dashboard/General/Length</code>	Sets the length of the taskbar.
<code>root/Dashboard/General/LengthToScreenSide</code>	If set to 1, the length of taskbar is fixed and equal to the length of the side of the screen to which it is anchored.
<code>root/Dashboard/General/PanelDockSide</code>	Sets the side of the screen to which the taskbar is docked.
<code>root/Dashboard/General/SlidingTimeout</code>	Sets the amount of time in milliseconds that it takes for the taskbar to hide or show when <code>AutoHide</code> is enabled.
<code>root/Dashboard/General/Width</code>	Sets the width of the taskbar. If set to -1, the width is scaled based on the height of the primary monitor.

Imprivata

Imprivata registry keys.

Table G-16 Imprivata registry keys

Registry key	Description
<code>root/Imprivata/enableImprivata</code>	If set to 1, Imprivata ProveID Embedded will be enabled. By default, it is 0.
<code>root/Imprivata/enableWMRightClickMenu</code>	If set to 1, the Window Manager right click menu is enabled. This is useful when the regular desktop is not available. The menu items are adjustable according to the Power Manager and the Customization Center configuration.
<code>root/Imprivata/enableWMShortcuts</code>	If set to 1, the Window Manager shortcuts are enabled. By default, the shortcuts are disabled to preserve the Imprivata agent environment.
<code>root/Imprivata/ImprivataServer</code>	URL of the Imprivata Server. Setting <code>root/users/user/apps/hptc-imprivata-mgr/authorized</code> to 1 allows the current user to modify the Imprivata setup.
<code>root/Imprivata/USBr/Devices</code>	Lists some USB devices with a predefined redirection rule specific to the remote connections launched using the Imprivata environment. For each USB device, the redirection rule is given by the setting: <code>forcedState</code> . Requires OneSign ProveID Embedded 6.2 with the ability to use the vendor scripts set.
<code>root/Imprivata/x11SessionFilter</code>	If <code>enableImprivata</code> is true, <code>/etc/X11/Xsession.d/19-imprivata-session-fork</code> takes over the X session. <code>x11SessionFilter</code> defines the X session files that are filtered out of the X session list of files. <code>x11SessionFilter</code> is a semicolon separated list of the session files to be excluded. Wildcards are usable.
<code>root/Imprivata/Imprivata.conf/Vdi/useVendorLaunchScript</code>	If set to 1, the HP's helper scripts are used to launch a VDI session. The legacy and deprecated scripts are used otherwise. For this setting to take effect, the X session has to be restarted. Imprivata.conf setting: <code>use-vendor-launch-script</code>

Table G-16 Imprivata registry keys (continued)

Registry key	Description
root/Imprivata/RdpHelper/rdpFileTemplate	Template of the .rdp file that is completed by the RDP helper with the "full address" field.
root/Imprivata/SysInfo/citrix-wfica-client	Path to the Citrix wfica client.
root/Imprivata/SysInfo/device-model	The string returned by the hptc-hws-id --hw command is used by default. Set the value to get a more relevant string.
root/Imprivata/SysInfo/logo	Path to the Imprivata partner logo.
root/Imprivata/SysInfo/persistent-data-folder	Path to a folder where the ProvelD Embedded components can be stored, eg: /writable/imprivata-sys-info-data or /writable/misc/imprivata-sys-info-data if the folder contents need to be part of a profile.
root/Imprivata/SysInfo/primary-monitor	If empty the primary monitor is automatically detected. Set the value to force a specific monitor, eg: DisplayPort-0.
root/Imprivata/SysInfo/rdp-client	Path to the Microsoft RDP client.
root/Imprivata/SysInfo/rds-client	Path to the Microsoft RDS client.
root/Imprivata/SysInfo/vmware-client	Path to the VMware Horizon View client.
root/Imprivata/USBr/Devices/<class id>:<product id>/forcedState	Sets whether this device is forced to be mapped to the remote host as follows: -1=Ignore Device; 0=Do Not Redirect; 1=Use Defaults; 2=Redirect.
root/Imprivata/USBr/Devices/<class id>:<product id>/info	Device information.
root/Imprivata/VmwareViewHelper/skipCrlRevocationCheck	If set to 1, the connection will skip certificate revocation list check for VMware Horizon Client 5.4 or later.
root/Imprivata/VmwareViewHelper/useCurrentViewConfig	If set to 1, the HP script does not create a new /etc/vmware/config file and the view client uses the current /etc/vmware/config file.

InputMethod

InputMethod registry key.

Table G-17 InputMethod registry key

Registry key	Description
root/InputMethod/enablelbus	

Network

Network registry keys.

Table G-18 Network registry keys

Registry key	Description
root/Network/ActiveDirectory/Domain	This registry key is either used internally or reserved for future use. The value should not be changed.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/ActiveDirectory/DynamicDNS	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Enabled	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Method	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Password	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/ActiveDirectory/Username	This registry key is either used internally or reserved for future use. The value should not be changed.
root/Network/DNSServers	Additional DNS servers for domain name resolution can be specified here. The specified servers will be used in addition to any servers retrieved via DHCP. Up to three IPv4 or IPv6 addresses can be specified, separated by commas.
root/Network/DefaultHostnamePattern	Sets the default hostname pattern to use when generating a new hostname. This is used if the <code>Hostname</code> registry key and <code>/etc/hostname</code> are both empty. The hostname pattern uses % as a delimiter. In the example <code>HPTC%MAC:1-6%</code> , <code>HPTC</code> would be the prefix, and the first six characters of the thin client MAC address would follow. So if the MAC address of the thin client is <code>11:22:33:44:55:66</code> , the generated hostname would be <code>HPTC112233</code> . If the pattern is <code>TC%MAC%</code> , the generated hostname would be <code>TC112233445566</code> . If the pattern is <code>HP%MAC:7%</code> , the generated hostname would be <code>HP1122334</code> .
root/Network/EncryptWpaConfig	If set to 1, the password is encrypted.
root/Network/FtpProxy	Sets the FTP proxy address. HP recommends using the following format for this value because the <code>http</code> prefix is better supported: <code>http://ProxyServer:Port</code>
root/Network/Hostname	Sets the hostname of the thin client.
root/Network/HttpProxy	Sets the HTTP proxy address. HP recommends using the following format: <code>http://ProxyServer:Port</code>
root/Network/HttpsProxy	Sets the HTTPS proxy address. HP recommends using the following format for this value because the <code>http</code> prefix is better supported: <code>http://ProxyServer:Port</code>
root/Network/IPSec/IPSecRules/<UUID>/DstAddr	Sets the destination address for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethod	Sets the authentication method for the IPSec rule. <code>PSK</code> is for using a pre-shared key, and <code>Certificate</code> is for using certificate files.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodCACert	If the authentication method is <code>Certificate</code> , the CA certificate file path is saved in this registry key.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodClientCert	If the authentication method is <code>Certificate</code> , the client certificate file path is saved in this registry key.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPresharedKey	If the authentication method is <code>PSK</code> , the pre-shared key value is saved in this registry key.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPrivateKey	If the authentication method is <code>Certificate</code> , the private key file path that corresponds with the client certificate is saved in this registry key.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/IPSec/IPSecRules/<UUID>/MMDHGroup	Sets the phase 1 Diffie-Hellman group.
root/Network/IPSec/IPSecRules/<UUID>/MMEncryptionAlg	Sets the phase 1 encryption algorithm.
root/Network/IPSec/IPSecRules/<UUID>/MMIntegrityAlg	Sets the phase 1 integrity algorithm.
root/Network/IPSec/IPSecRules/<UUID>/MMLifetimeMinutes	Sets the phase 1 lifetime.
root/Network/IPSec/IPSecRules/<UUID>/QMAHEnable	Enables phase 2 AH.
root/Network/IPSec/IPSecRules/<UUID>/QMAHIntegrityAlg	Sets the phase 2 AH integrity algorithm.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEnable	Enables phase 2 ESP.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEncryptionAlg	Sets the phase 2 ESP encryption algorithm.
root/Network/IPSec/IPSecRules/<UUID>/QMESPIntegrityAlg	Sets the phase 2 ESP integrity algorithm.
root/Network/IPSec/IPSecRules/<UUID>/QMLifetimeSeconds	Sets the phase 2 lifetime.
root/Network/IPSec/IPSecRules/<UUID>/RuleDescription	Sets the description for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/RuleEnable	If set to 1, the rule is enabled.
root/Network/IPSec/IPSecRules/<UUID>/RuleName	Sets the name for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/SrcAddr	Sets the source address for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/TunnelDstAddr	Sets the tunnel destination address for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/TunnelEnable	Enables tunnel mode for the IPSec rule.
root/Network/IPSec/IPSecRules/<UUID>/TunnelSrcAddr	Sets the tunnel source address for the IPSec rule.
root/Network/KeepPreviousDNS	If set to 1, previously-configured DNS servers and search domains not generated by the Network Manager will be kept in resolv.conf. If set to 0, resolv.conf will be overwritten completely.
root/Network/SearchDomains	Additional search domains for FQDN resolution can be specified here. The specified domains will be appended to any incomplete server definitions in an attempt to generate an FQDN that can be resolved via DNS. For example, a search domain of mydomain.com will allow the server definition myserver to resolve properly to myserver.mydomain.com, even if the DNS server does not have myserver in its name resolution tables. Up to five additional search domains can be specified.
root/Network/VPN/AutoStart	If set to 1, VPN starts automatically when the system starts up.

Table G-18 Network registry keys (continued)

Registry key	Description
<code>root/Network/VPN/PPTP/Domain</code>	Sets the PPTP domain.
<code>root/Network/VPN/PPTP/Gateway</code>	Sets the PPTP gateway.
<code>root/Network/VPN/PPTP/Password</code>	Sets the PPTP user password.
<code>root/Network/VPN/PPTP/Username</code>	Sets the PPTP username.
<code>root/Network/VPN/Type</code>	Sets the VPN type.
<code>root/Network/VPN/VPNC/DPDEndianess</code>	Sets the endianness of the DPD sequence number (see rfc3706). 0: big endian; 1: little endian. Try toggling this if the session aborts intermittently for no apparent reason.
<code>root/Network/VPN/VPNC/DPDInterval</code>	Sets the DPD interval (see rfc3706) in seconds.
<code>root/Network/VPN/VPNC/DebugLevel</code>	Sets the debug level to either 0, 1, 2, 3, or 99. This generates a lot of logs. Enable this only when you need to troubleshoot a VPN issue.
<code>root/Network/VPN/VPNC/Domain</code>	Sets the VPNC domain.
<code>root/Network/VPN/VPNC/Gateway</code>	Sets the VPNC gateway.
<code>root/Network/VPN/VPNC/Group</code>	Sets the VPNC group.
<code>root/Network/VPN/VPNC/GroupPassword</code>	Sets the VPNC group password.
<code>root/Network/VPN/VPNC/IKEDHGroup</code>	Sets the VPNC IKE Diffie-Hellman group.
<code>root/Network/VPN/VPNC/LocalUDPPort</code>	Sets the local UDP port to use for VPNC. If set to 0, a random port will be used. This setting is valid only when the NAT traversal mode (<code>NATMode</code>) is <code>cisco-udp</code> .
<code>root/Network/VPN/VPNC/NATMode</code>	Sets the VPNC NAT traversal mode.
<code>root/Network/VPN/VPNC/Password</code>	Sets the VPNC user password.
<code>root/Network/VPN/VPNC/PerfectForwardSecrecy</code>	Sets the VPNC Diffie-Hellman group to use for Perfect Forward Secrecy (PFS).
<code>root/Network/VPN/VPNC/Security</code>	Sets the VPNC security level.
<code>root/Network/VPN/VPNC/Username</code>	Sets the VPNC username.
<code>root/Network/VisibleInSystray</code>	If set to 1, the network icon is visible in the system tray.
<code>root/Network/Wired/DefaultGateway</code>	Sets the default gateway the device will use to communicate with the Internet. Typically this is the IP address of the router. This setting takes effect only when <code>Method</code> is set to <code>Static</code> .
<code>root/Network/Wired/EnableDefGatewayAsDNS</code>	If set to 1, the default gateway will also be the name server.
<code>root/Network/Wired/EthernetSpeed</code>	Sets the link speed of the primary Ethernet network interface. <code>Automatic</code> allows the fastest available link speed to be used, which is usually 1 Gbps or 100 Mbps/Full depending on the switch. The link speed can also be forced to a single speed (100 Mbps or 10 Mbps) and duplex mode (Full or Half) to support switches and hubs that do not perform appropriate auto-negotiation.
<code>root/Network/Wired/IPAddress</code>	Sets the IPv4 address of the thin client. This setting will only take effect when <code>Method</code> is set to <code>Static</code> .
<code>root/Network/Wired/IPv6Enable</code>	If set to 1, IPv6 is enabled.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/Wired/Interface	Sets the default Ethernet interface or NIC.
root/Network/Wired/MTU	Sets the MTU. It does not matter if the IP address is static or DHCP-acquired.
root/Network/Wired/Method	If set to <i>Automatic</i> , the thin client will use DHCP to attempt to retrieve network settings. If set to <i>Static</i> , the values of the <i>IPAddress</i> , <i>SubnetMask</i> , and <i>DefaultGateway</i> registry keys are used. HP does not recommend using <i>Static</i> in a generic client profile because it will cause all thin clients to receive the same IP address.
root/Network/Wired/Profiles/<UUID>/AutoConnect	If set to 1, automatic connection to the network is enabled.
root/Network/Wired/Profiles/<UUID>/EthernetSpeed	Sets the link speed of the primary Ethernet network interface. <i>Automatic</i> allows the fastest available link speed to be used, which is usually 1 Gbps or 100 Mbps/full depending on the switch. The link speed can be forced to a combination of a single speed (100 Mbps or 10 Mbps) and duplex mode (<i>Full</i> or <i>Half</i>) to support switches and hubs that do not perform auto-negotiation.
root/Network/Wired/Profiles/<UUID>/IPv4/Address	Sets the IPv4 address of the client. This setting takes effect only if <i>Method</i> is set to <i>Static</i> .
root/Network/Wired/Profiles/<UUID>/IPv4/DefaultGateway	Sets the default gateway that the device uses to communicate with the Internet. Typically, this is the IP address of the router. This setting takes effect only if <i>Method</i> is set to <i>Static</i> .
root/Network/Wired/Profiles/<UUID>/IPv4/Enabled	If set to 1, IPv4 is enabled for this profile.
root/Network/Wired/Profiles/<UUID>/IPv4/Method	If set to <i>Automatic</i> , the client uses DHCP to attempt to retrieve network settings. If set to <i>Static</i> , the values of the <i>Address</i> , <i>SubnetMask</i> , and <i>DefaultGateway</i> registry keys are used. HP does not recommend using <i>Static</i> in a generic client profile, because all clients would use the same IP address.
root/Network/Wired/Profiles/<UUID>/IPv4/SubnetMask	Sets the subnet mask of the device, such as 255.255.255.0 (for a standard class C subnet). This setting takes effect only if <i>Method</i> is set to <i>Static</i> .
root/Network/Wired/Profiles/<UUID>/IPv6/Address	Sets the IPv6 address of the client. This setting takes effect only if <i>Method</i> is set to <i>Static</i> .
root/Network/Wired/Profiles/<UUID>/IPv6/DefaultGateway	Sets the default gateway that the device uses to communicate with the Internet. Typically, this is the IP address of the router. This setting takes effect only if <i>Method</i> is set to <i>Static</i> .
root/Network/Wired/Profiles/<UUID>/IPv6/Enabled	If set to 1, IPv6 is enabled for this profile.
root/Network/Wired/Profiles/<UUID>/IPv6/Method	If set to <i>Automatic</i> , the client uses DHCP to attempt to retrieve network settings. If set to <i>Static</i> , the values of the <i>Address</i> , <i>SubnetMask</i> , and <i>DefaultGateway</i> registry keys are used. HP does not recommend using <i>Static</i> in a generic client profile, because all clients would use the same IP address. If set to <i>Automatic</i> , the client uses DHCP to attempt to retrieve network settings. If set to <i>Static</i> , the values of the <i>Address</i> , <i>SubnetMask</i> , and <i>DefaultGateway</i> registry keys are used. HP does not recommend using <i>Static</i> in a generic client profile, because all clients would use the same IP address.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/Wired/Profiles/<UUID>/IPv6/SubnetMask	Sets the subnet mask of the device, which is usually the IPv6 prefix length. This setting takes effect only if Method is set to Static.
root/Network/Wired/Profiles/<UUID>/MTU	Sets the MTU. It does not matter if the IP address is static or acquired by DHCP.
root/Network/Wired/Profiles/<UUID>/Priority	Reserved for wired network.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity	Sets the anonymous identity for PEAP authentication.
root/Network/Wired/Profiles/<UUID>/EAPPEAP/CACert	Sets the path to the CA certificate file for PEAP authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Sets the PEAP inner authentication protocol.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Sets the PEAP version.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Password	Sets the password for PEAP authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Username	Sets the username for PEAP authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/CACert	Sets the path to the CA certificate file for TLS authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/Identity	Sets the identity for TLS authentication.
root/Network/Wired/Profiles/<UUID>/EAPTLS/PrivateKey	Sets the path to a private key file for TLS authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Sets the password to a private key file for TLS authentication.
root/Network/Wired/Profiles/<UUID>/EAPTLS/UserCert	Sets the path to a user certificate file for TLS authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/AnonyIdentity	Sets the anonymous identity for TTLS authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/CACert	Sets the path to a CA certificate file for TTLS authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/InnerAuth	Sets the TTLS inner authentication protocol.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/Password	Sets the password for TTLS authentication.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/Username	Sets the username for TTLS authentication.
root/Network/Wired/Profiles/<UUID>/Security/Type	Sets the wired authentication type.
root/Network/Wired/Profiles/<UUID>/WiredInterface	Sets the wired interface for the profile.
root/Network/Wired/Security/CACert	Sets the path to CA certificate file.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/Wired/Security/EnableMachineAuth	If set to 1, machine authentication for PEAP is enabled.
root/Network/Wired/Security/Identity	Sets the identity or anonymous identity.
root/Network/Wired/Security/InnerAuth	Sets the PEAP inner authentication protocol.
root/Network/Wired/Security/InnerAuthTTLS	Sets the TTLS inner authentication protocol.
root/Network/Wired/Security/MachineAuthName	Stores the machine account name when machine authentication is enabled.
root/Network/Wired/Security/MachineAuthPassword	Stores the machine account password when machine authentication is enabled.
root/Network/Wired/Security/PEAPVersion	Sets the PEAP version.
root/Network/Wired/Security/Password	Sets the password.
root/Network/Wired/Security/PrivateKey	Sets the path to a private key file. This is only used for TLS authentication.
root/Network/Wired/Security/Type	Sets the 802.1x authentication type.
root/Network/Wired/Security/UserCert	Sets the path to a user certificate file. This is only used for TLS authentication.
root/Network/Wired/Security/Username	Sets the username.
root/Network/Wired/SubnetMask	Sets the subnet mask of the device, such as 255.255.255.0 (for a standard class C subnet). This setting will only take effect when <i>Method</i> is set to <i>Static</i> .
root/Network/Wired/UseWiredProfiles	If set to 1, the wired connection is configured in profile mode, which can connect to multiple wired networks. If set to 0, it can connect to only one wired network.
root/Network/Wired/WirelessSwitch	If set to 0, a wired network and a wireless network can be connected simultaneously. If set to 1, the wired network takes priority over the wireless network; that is, if the wired network cannot connect, a configured wireless network is used.
root/Network/Wireless/DefaultGateway	Sets the default gateway the device will use to communicate with the Internet. Typically this is the IP address of the router. This setting will only take effect when <i>Method</i> is set to <i>Static</i> .
root/Network/Wireless/EnableDefGatewayAsDNS	If set to 1, the default gateway will also be the name server.
root/Network/Wireless/EnableWireless	If set to 1, wireless functionality is enabled. If set to 0, wireless functionality is disabled.
root/Network/Wireless/IPAddress	Sets the IPv4 address of the thin client. This setting will only take effect when <i>Method</i> is set to <i>Static</i> .
root/Network/Wireless/IPv6Enable	If set to 1, IPv6 is enabled.
root/Network/Wireless/Interface	Sets the default wireless interface or wireless network adapter.
root/Network/Wireless/Method	If set to <i>Automatic</i> , the thin client will use DHCP to attempt to retrieve network settings. If set to <i>Static</i> , the values of the <i>IPAddress</i> , <i>SubnetMask</i> , and <i>DefaultGateway</i> registry keys are used. HP does not recommend using <i>Static</i> in a generic client profile because it will cause all thin clients to receive the same IP address.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/Wireless/PowerEnable	If set to 1, power management of the wireless network card is enabled.
root/Network/Wireless/Profiles/<UUID>/AutoConnect	If set to 1, automatic connection to the SSID is enabled.
root/Network/Wireless/Profiles/<UUID>/IPv4/Address	Sets the IPv4 address of the client. This setting takes effect only if Method is set to Static.
root/Network/Wireless/Profiles/<UUID>/IPv4/DefaultGateway	Sets the default gateway the device uses to communicate with the Internet. Typically, this is the IP address of the router. This setting takes effect only if Method is set to Static.
root/Network/Wireless/Profiles/<UUID>/IPv4/Enabled	If set to 1, IPv4 is enabled for this profile.
root/Network/Wireless/Profiles/<UUID>/IPv4/Method	If set to Automatic, the client uses DHCP to retrieve network settings. If set to Static, the values of the Address, SubnetMask, and DefaultGateway registry keys are used. HP does not recommend using Static in a generic client profile, because all clients using that profile would use the same IP address.
root/Network/Wireless/Profiles/<UUID>/IPv4/SubnetMask	Sets the subnet mask of the device, such as 255.255.255.0 (for a standard class C subnet). This setting takes effect only if Method is set to Static.
root/Network/Wireless/Profiles/<UUID>/IPv6/Address	Sets the IPv6 address of the client. This setting takes effect only if Method is set to Static.
root/Network/Wireless/Profiles/<UUID>/IPv6/DefaultGateway	Sets the default gateway the device uses to communicate with the Internet. Typically, this is the IP address of the router. This setting takes effect only if Method is set to Static.
root/Network/Wireless/Profiles/<UUID>/IPv6/Enabled	If set to 1, IPv6 is enabled for this profile.
root/Network/Wireless/Profiles/<UUID>/IPv6/Method	If set to Automatic, the client uses DHCP to attempt to retrieve network settings. If set to Static, the values of the Address, SubnetMask, and DefaultGateway registry keys are used. HP does not recommend using Static in a generic client profile, because all clients would use the same IP address.
root/Network/Wireless/Profiles/<UUID>/IPv6/SubnetMask	Sets the subnet mask of the device, which is usually the IPv6 prefix length. This setting takes effect only if Method is set to Static.
root/Network/Wireless/Profiles/<UUID>/PowerEnable	If set to 1, power management of the wireless network card is enabled.
root/Network/Wireless/Profiles/<UUID>/Priority	Defines the priority of the network. For a wireless network, a larger number means a higher priority. High priority is preferred for a wireless network connection.
root/Network/Wireless/Profiles/<UUID>/SSID	Sets the wireless access point to use via SSID.
root/Network/Wireless/Profiles/<UUID>/SSIDHidden	Specifies whether the SSID of the wireless access point is hidden.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/AnonyIdentity	Sets the anonymous identity for EAP-FAST authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/FastProvision	Sets the provisioning option for EAP-FAST authentication.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/PACFile	Sets the path to the PAC file for EAP-FAST authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Password	Sets the password for EAP-FAST authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Username	Sets the username for EAP-FAST authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity	Sets the anonymous identity for EAP PEAP authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/CACert	Sets the path to the CA certificate file for EAP PEAP authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Sets the PEAP inner authentication protocol.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Sets the PEAP version.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Password	Sets the password for EAP PEAP authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Username	Sets the username for EAP PEAP authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/CACert	Sets the path to the CA certificate file for TLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/Identity	Sets the identity for TLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKey	Sets the path to a private key file for TLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Sets the password to a private key file for TLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/UserCert	Sets the path to a user certificate file for TLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/AnonyIdentity	Sets the anonymous identity for TTLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/CACert	Sets the path to a CA certificate file for TTLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/InnerAuth	Sets the TTLS inner authentication protocol.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/Password	Sets the password for TTLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/Username	Sets the username for TTLS authentication.
root/Network/Wireless/Profiles/<UUID>/Security/PSK/HexdecimalMode	
root/Network/Wireless/Profiles/<UUID>/Security/PSK/PreSharedKey	Sets the password for PSK authentication.
root/Network/Wireless/Profiles/<UUID>/Security/Type	Sets the wireless authentication type.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/Wireless/Profiles/<UUID>/Security/WEP/AuthType	Sets the WEP authentication type.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/Key	Sets the WEP password.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/KeyIndex	Sets the WEP password index.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessBand	Specifies the frequency range selection. Select <code>Auto</code> to scan all wireless channels; select <code>2.4GHz</code> to scan only 2.4 GHz channels; select <code>5GHz</code> to scan only 5 GHz channels.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessInterface	Sets the wireless interface for the profile.
root/Network/Wireless/Roaming/enableRoamingOptions	If set to 1, wireless roaming options are configurable.
root/Network/Wireless/Roaming/longScanInterval	Specifies how often, in seconds, to scan for an access point with a stronger signal when the signal strength is above the roaming threshold. The default is 60.
root/Network/Wireless/Roaming/roamingNap	Specifies how often, in seconds, the connection sleeps when the <code>wpa_applicant</code> status changes. This helps reduce spurious Wi-Fi events from breaking live connections when roaming occurs.
root/Network/Wireless/Roaming/roamingThreshold	Sets the minimum signal strength, in dBm, allowed before attempting to roam to a stronger access point. Note that this value is negative.
root/Network/Wireless/Roaming/scanInterval	Sets how often, in seconds, to scan for a stronger access point when the signal strength is below the roaming threshold.
root/Network/Wireless/SSID	Sets the wireless access point to use via its SSID.
root/Network/Wireless/SSIDHidden	Specifies if the SSID of the wireless access point is hidden.
root/Network/Wireless/SSIDWhiteList	Specifies a whitelist for wireless access points. If this registry key's value is not empty, only the SSIDs specified in the value will be shown in the wireless access point scan results. Use a semicolon to separate the SSIDs.
root/Network/Wireless/Security/CACert	Sets the path to CA certificate file.
root/Network/Wireless/Security/EAPFASTPAC	Sets the path to the PAC file for EAP-FAST authentication.
root/Network/Wireless/Security/EAPFASTProvision	Sets the provisioning option for EAP-FAST authentication.
root/Network/Wireless/Security/Identity	Sets the identity or anonymous identity.
root/Network/Wireless/Security/InnerAuth	Sets the PEAP inner authentication protocol.
root/Network/Wireless/Security/InnerAuthTTLS	Sets the TTLS inner authentication protocol.
root/Network/Wireless/Security/PEAPVersion	Sets the PEAP version.
root/Network/Wireless/Security/Password	Sets the password.
root/Network/Wireless/Security/PrivateKey	Sets the path to a private key file. This is only used for TLS authentication.
root/Network/Wireless/Security/Type	Sets the wireless authentication type.

Table G-18 Network registry keys (continued)

Registry key	Description
root/Network/Wireless/Security/UserCert	Sets the path to a user certificate file. This is only used for TLS authentication.
root/Network/Wireless/Security/Username	Sets the username.
root/Network/Wireless/Security/WEPAuth	Sets the WEP authentication type.
root/Network/Wireless/Security/WEPIndex	Sets the WEP password index.
root/Network/Wireless/SubnetMask	Sets the subnet mask of the device, such as 255.255.255.0 (for a standard class C subnet). This setting will only take effect when <code>Method</code> is set to <code>Static</code> .
root/Network/Wireless/UseWirelessProfiles	If set to 1, the wireless connection is configured in profile mode, which can connect to multiple wireless networks. This is useful for mobile computing. If set to 0, only one configured wireless network can be connected.
root/Network/Wireless/WirelessBand	Specifies the frequency range selection. Select <code>Auto</code> to scan all wireless channels; select <code>2.4GHz</code> to scan only 2.4 GHz channels; select <code>5GHz</code> to scan only 5 GHz channels.
root/Network/Wireless/WpaDriver	Specifies the driver used by <code>wpa_supplicant</code> (wext by default). <code>nl80211</code> is the only other driver that is currently supported.
root/Network/Wireless/bcmwlCountryOverride	Overrides the country value from the BIOS in case the BIOS does not have the necessary value. The <code>bcmwl</code> driver accepts the <code>wl_country</code> option, which is retrieved from BIOS values on an as-needed basis (only Indonesia is supported currently). A system restart is required for any changes to take effect.
root/Network/Wireless/disableUserCreateWirelessProfile	If set to 1, user accounts cannot create wireless profiles from the wireless system tray.
root/Network/Wireless/disableUserWirelessProfileTrayMenu	If set to 1, the wireless menu of the wireless system tray icon is disabled for the user account.
root/Network/Wireless/disableWirelessProfileTrayMenu	If set to 1, the wireless menu of the wireless system tray icon is disabled.
root/Network/Wireless/tryAutoWirelessIfUserFailed	If set to 1, if a user tries to connect to a wireless AP and fails, the wireless module tries to connect wirelessly using all available profiles. If set to 0, if a user tries to connect to a wireless AP and fails, the wireless status is set to disconnected. This is a fallback function.
root/Network/disableLeftClickMenu	If set to 1, the left-click menu for the network system tray icon is disabled.
root/Network/disableRightClickMenu	If set to 1, the right-click menu for the network system tray icon is disabled.
root/Network/enableVPNMenu	If set to 1, the left-click VPN menu accessible from the network taskbar icon is enabled.
root/Network/userLock	If set to 1, and if the network settings have been modified by the user, the network settings are preserved when importing a client profile.
root/Network/userLockEngaged	This registry key is set to 1 automatically after the network settings have been modified by the user. You normally do not need to modify this setting.

Power

Registry keys for power settings.

Table G-19 Power registry keys

Registry key	Description
root/Power/applet/VisibleInSystray	If set to 1, the battery icon is displayed in the system tray.
root/Power/buttons/logout/authorized	If set to 1, the logout function is available.
root/Power/buttons/power/authorized	If set to 1, the power function is available.
root/Power/buttons/poweroff/authorized	If set to 1, the poweroff function is available.
root/Power/buttons/reboot/authorized	If set to 1, the reboot function is available.
root/Power/buttons/sleep/authorized	If set to 1, the Sleep function is available.
root/Power/currentPowerPlan	This registry key selects which power plan is used. This is automatically set to default.
root/Power/default/AC/brightness	Sets the default brightness percentage level for when the mobile thin client is plugged in.
root/Power/default/AC/cpuMode	Sets the CPU mode for a power plan while the computer is connected to AC power. By default, it is set to performance.
root/Power/default/AC/lidAction	Sets the action that occurs when the computer lid is closed while the computer is connected to AC power. By default, it is set to Sleep.
root/Power/default/AC/powerButtonAction	Sets the action that occurs when the power button is pressed while the computer is connected to AC power. By default, it is set to shutdown.
root/Power/default/AC/sleep	Sets the value (in minutes) that the computer waits before it enters the Sleep state while the computer is connected to AC power. By default, it is set to 30. If set to 0, the computer never enters the Sleep state.
root/Power/default/AC/standby	Sets the value (in minutes) that the computer waits before the display turns off while the computer is connected to AC power. By default, it is set to 15. If set to 0, the computer never enters standby mode.
root/Power/default/AC/timeoutDim	This key is currently not in use.
root/Power/default/battery/brightness	Sets the default brightness percentage level for when the mobile thin client is not plugged in.
root/Power/default/battery/cpuMode	Sets the CPU mode for a power plan while the computer is not connected to AC power. By default, it is set to ondemand.
root/Power/default/battery/critical/criticalBatteryAction	Sets the action to perform when the battery is at the critical charge level, defined by <code>criticalBatteryLevel</code> .
root/Power/default/battery/critical/criticalBatteryLevel	Sets the percentage threshold for when the battery is considered to be at a critical level of power.
root/Power/default/battery/lidAction	Sets the action that occurs when the computer lid is closed while the computer is not connected to AC power. By default, it is set to Sleep.
root/Power/default/battery/low/brightness	Sets the default brightness percentage level for when the battery is running low on power.
root/Power/default/battery/low/cpuMode	Sets the CPU mode (performance or on demand).

Table G-19 Power registry keys (continued)

Registry key	Description
root/Power/default/battery/low/lowBatteryLevel	Sets the percentage of battery power left for when the battery is considered to be at a low level of power.
root/Power/default/battery/low/sleep	Sets the value (in minutes) that the computer waits before it enters the Sleep state while the computer is not connected to AC power. By default, it is set to 30. If set to 0, the computer never enters the Sleep state.
root/Power/default/battery/low/standby	Sets the value (in minutes) that the computer waits before the display turns off while the computer is not connected to AC power. By default, it is set to 15. If set to 0, the computer never enters standby mode.
root/Power/default/battery/low/timeoutDim	This key is currently not in use.
root/Power/default/battery/powerButtonAction	Specifies what to do when power button is pressed.
root/Power/default/battery/sleep	Sets how many minutes to wait before entering Sleep. 0 = never.
root/Power/default/battery/standby	Sets how many minutes to wait before turning off the display. 0 = never.
root/Power/default/battery/timeoutDim	This key is currently not in use.

ScepMgr

ScepMgr registry keys.

Table G-20 ScepMgr registry keys

Registry key	Description
root/ScepMgr/General/AutoRenew/Enabled	If set to 1, certificates will be renewed automatically before they expire.
root/ScepMgr/General/AutoRenew/TimeFrame	Sets the number of days before a certificate's expiration date that the SCEP Manager will try to renew the certificate automatically.
root/ScepMgr/IdentifyingInfo/CommonName	Sets the common name to use for SCEP identifying information, such as your name or the Fully-Qualified Domain Name (FQDN) of the device. The FQDN is used by default if this value is left empty.
root/ScepMgr/IdentifyingInfo/CountryName	Sets the country or region to use for SCEP identifying information.
root/ScepMgr/IdentifyingInfo/EmailAddress	Sets the email address to use for SCEP identifying information.
root/ScepMgr/IdentifyingInfo/LocalityName	Sets the locality name to use for SCEP identifying information, such as a city name.
root/ScepMgr/IdentifyingInfo/OrganizationName	Sets the organization name to use for SCEP identifying information, such as a company name or government organization name.
root/ScepMgr/IdentifyingInfo/OrganizationUnitName	Sets the organizational unit name to use for SCEP identifying information, such as a department name or section name.

Table G-20 ScepMgr registry keys (continued)

Registry key	Description
root/ScepMgr/IdentifyingInfo/StateName	Sets the state or province to use for SCEP identifying information.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/CertFileChanged	The registry key is used only to inform other applications that a certificate file has changed. This should not need to be modified.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/DontVerifyPeer	This registry key is used for https only. If set to 1, the SCEP client does not verify the server certificate. This key is set to 0 by default.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/KeySize	Sets the key size to use for the generated key pair.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerName	Sets the SCEP server name.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerUrl	Sets the SCEP server URL, which is necessary for the SCEP client to enroll a certificate.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Code	Contains the status code of the SCEP enrollment. This value is read-only.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Detail	Contains detailed information about the SCEP enrollment. This value is read-only.

Search

Search settings registry keys.

Table G-21 Search settings registry keys

Registry key	Description
root/Search/Category/Miscellaneous/CheckForUpdate	
root/Search/Category/Miscellaneous/Logout	
root/Search/Category/Miscellaneous/Reboot	
root/Search/Category/Miscellaneous/ShutDown	
root/Search/Category/Miscellaneous/Sleep	
root/Search/Category/Miscellaneous/SwitchToAdmin	
root/Search/Category/Regeditor/byDir	
root/Search/Category/Regeditor/byKey	
root/Search/Category/Regeditor/byValue	
root/Search/Category/Regeditor/byWhole	

Serial

Serial device registry keys.

Table G-22 Serial device registry keys

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

SystemInfo

System Information registry keys.

Table G-23 System Information registry keys

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

TaskMgr

Task Manager registry key.

Table G-24 Task Manager registry key

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

USB

USB registry keys.

Table G-25 USB registry keys

Registry key	Description
root/USB/Classes/<Defined at Interface level>/ClassID	Sets the USB class ID number.
root/USB/Classes/<Defined at Interface level>/DisplayName	Sets the USB class name. NOTE: Defined at Interface level.
root/USB/<Defined at Interface level>/Classes/State	Sets whether the class is mapped to the remote host. NOTE: Defined at Interface level.
root/USB/<Defined at Interface level>/Classes/Visible	Sets whether the class is shown in the UI, not shown in the UI, or disabled. NOTE: Defined at Interface level.
root/USB/Devices/<UUID>/DisplayName	Sets the name to show in USB Manager. If not supplied, USB Manager will attempt to generate an appropriate name using device information.
root/USB/Devices/<UUID>/ProductID	Sets the product ID of the device.
root/USB/Devices/<UUID>/State	Sets whether this device is mapped to the remote host as follows: 0 = Do Not Redirect; 1 = Use Defaults; 2 = Redirect.
root/USB/Devices/<UUID>/VendorID	Sets the vendor ID of the device.
root/USB/root/autoSwitchProtocol	If set to 1, the remote USB protocol will switch automatically based on which protocol is chosen.
root/USB/root/mass-storage/allowed	If set to 1, mass storage devices will be mounted automatically when the protocol is <code>local</code> .
root/USB/root/mass-storage/read-only	If set to 1, when mass storage devices are mounted automatically, they will be mounted as read-only.
root/USB/root/protocol	Sets which protocol owns remote USB. Valid values depend on which protocols are installed on the system but can include <code>local</code> , <code>xen</code> , <code>freerdp</code> , and <code>view</code> .
root/USB/root/showClasses	If set to 1, the Classes section is shown in the USB Manager.

auto-update

Registry keys for Automatic Updates.

Table G-26 Registry keys for Automatic Updates

Registry key	Description
root/auto-update/DNSAliasDir	Sets the default root directory for DNS alias mode on the server hosting HP Smart Client Services.
root/auto-update/LockScreenTimeout	Specifies the timeout (in minutes) after which the screen will unlock during an automatic update. If set to 0, the screen will be unlocked throughout the entire automatic update until the update is complete.
root/auto-update/ManualUpdate	If set to 1, the DHCP tag, DNS alias, and broadcast update methods for Automatic Update are disabled. When performing a manual update, the <code>password</code> , <code>path</code> , <code>protocol</code> , <code>user</code> , and <code>ServerURL</code> registry keys must be set to ensure the update server is known.
root/auto-update/ScheduledScan/Enabled	If set to 1, the thin client performs periodic scans of the Automatic Update server to check for updates. If set to 0, the thin client will only check for updates at system startup.
root/auto-update/ScheduledScan/Interval	Sets the amount of time to wait between scheduled update scans. This should be specified in the <code>HH:MM</code> format. Intervals longer than 24 hours can be specified. For example, to have the scans occur every 48 hours, set this to <code>48:00</code> .
root/auto-update/ScheduledScan/Period	Thin clients will randomly activate their scheduled scan throughout the defined period. Using a long period avoids cases where all thin clients update at exactly the same, which could cause network congestion. The period should be specified in the <code>HH:MM</code> format. For example, to spread thin client updates over a 2.5-hour period, set this to <code>02:30</code> .
root/auto-update/ScheduledScan/StartTime	Sets the start time of the first scheduled update scan period in the format <code>HH:MM</code> , using the 24-hour time format. For example, 4:35 p.m. would be <code>16:35</code> .
root/auto-update/ServerURL	Sets the IP address or domain name of the update server used when <code>ManualUpdate</code> is enabled.
root/auto-update/VisibleInSystray	If set to 1, the Automatic Update system tray icon is enabled.
root/auto-update/checkCertSig	If set to 1, the certificate signature is verified.
root/auto-update/checkCustomSig	If set to 1, the custom packages signature is verified.
root/auto-update/checkImgSig	Reserved for future use.
root/auto-update/checkPackageSig	If set to 1, the packages signature is verified.
root/auto-update/checkProfileSig	If set to 1, the profiles signature is verified.
root/auto-update/enableLockScreen	If set to 1, the screen locks while an automatic update is in progress.
root/auto-update/enableOnBootup	If set to 1, Automatic Update is enabled at system startup.
root/auto-update/enableSystrayLeftClickMenu	If set to 1, the left-click menu for the Automatic Update system tray icon is enabled.
root/auto-update/enableSystrayRightClickMenu	If set to 1, the right-click menu for the Automatic Update system tray icon is enabled.
root/auto-update/gui/auto-update/ManualUpdate	Controls the state of the Enable manual configuration widget in the Automatic Update tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.

Table G-26 Registry keys for Automatic Updates (continued)

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

background

Background Sysinfo registry keys.

Table G-27 Background Sysinfo registry keys

Registry key	Description
root/background/bginfo/alignment	Sets the Background Sysinfo text alignment.
root/background/bginfo/enabled	If set to 1, system information is displayed on the desktop background (Background Sysinfo).
root/background/bginfo/horizontalLocation	Sets the Background Sysinfo location on the X-axis in a percentage.
root/background/bginfo/interval	Sets the Background Sysinfo text refresh interval in seconds.
root/background/bginfo/preset	Sets the Background Sysinfo preset file to use. If set to <i>none</i> , you can customize the settings in Background Manager.
root/background/bginfo/shadowColor	Sets the Background Sysinfo shadow color.
root/background/bginfo/shadowOffset	Sets the Background Sysinfo shadow offset. If set to 0, the shadow is disabled.
root/background/bginfo/text	Sets the Background Sysinfo text. For more information, see the HP ThinPro white paper <i>Login Screen Customization</i> (available in English only).
root/background/bginfo/textColor	Sets the Background Sysinfo text color.
root/background/bginfo/textSize	Sets the Background Sysinfo text size.
root/background/bginfo/verticalLocation	Sets the Background Sysinfo location on the Y-axis in a percentage.
root/background/desktop/color	Specifies the solid color, the background color if any is visible behind the image, or the top color in a gradient.
root/background/desktop/color2	If theme is set to <i>gradient</i> , this key stores the bottom color in the gradient.
root/background/desktop/imagePath	If theme is set to either <i>none</i> or <i>image</i> , this key stores the desktop background image path used by the user-defined theme.
root/background/desktop/lastBrowseDir	If theme is set to <i>none</i> , this key stores the last used directory.
root/background/desktop/style	If theme is set to <i>none</i> , this key stores how the background image is placed on the desktop (such as <i>center</i> , <i>tile</i> , <i>stretch</i> , <i>fit</i> , and <i>fill</i>).
root/background/desktop/theme	Specifies the system theme setting. This value is set via the Background Manager tool in Control Panel. The valid values depend on the themes that exist on the system. This can be set to <i>none</i> or <i>image</i> to let the user define a background image, to <i>auto</i> to have the system automatically set the appropriate protocol's theme for Smart Zero, or to <i>default</i> to use the default theme for ThinPro, or one of several predefined themes.
root/background/desktop/updateInterval	Sets the background refresh interval in seconds.

boot

Boot registry keys.

Table G-28 Boot registry keys

Registry key	Description
<code>root/boot/enablePlymouth</code>	
<code>root/boot/extraCmdline</code>	

config-wizard

Config-wizard registry keys

Table G-29 Config-wizard registry keys

Registry key	Description
<code>root/config-wizard/configWizardOptions</code>	Specifies, in a space-separated list, which configuration wizard options are displayed. By default, all options (language, keyboard, network, datetime, end) are listed.
<code>root/config-wizard/disableAllChecksAtStartup</code>	If set to 1, all checks at startup are disabled. If set to 0, you can enable/disable each type of check individually with the registry keys <code>enableConnectionCheck</code> , <code>enableNetworkCheck</code> , and <code>enableUpdateCheck</code> .
<code>root/config-wizard/enableConfigWizard</code>	If set to 1, the configuration wizard at system startup is enabled.
<code>root/config-wizard/enableConnectionCheck</code>	If set to 1, the connection check at system startup is enabled.
<code>root/config-wizard/enableNetworkCheck</code>	If set to 1, the network check at system startup is enabled.
<code>root/config-wizard/showNetworkSettingsButton</code>	If set to 1, the network settings button is shown in the network check window.

desktop

Desktop registry keys.

Table G-30 Desktop registry keys

Registry key	Description
<code>root/desktop/preferences/arrangeBy</code>	Specifies whether to arrange icons by name or type.
<code>root/desktop/preferences/fontFamily</code>	Specifies the font used for desktop icons.
<code>root/desktop/preferences/gridSize</code>	Specifies, in pixels, the desktop icon grid size. If set to a value less than 64, the size is computed as a proportion of the monitor size.
<code>root/desktop/preferences/iconGlowColor</code>	Specifies the color that glows behind the desktop icon when a pointer hovers over it. Valid strings are in the style <code>QColor::setNamedColor()</code> . If not set, the system chooses a color that contrasts with the background.

Table G-30 Desktop registry keys (continued)

Registry key	Description
root/desktop/preferences/iconPercent	Specifies the percentage of the grid size to use for the icon. If the value is greater than 0, it is calculated as a proportion of the grid size.
root/desktop/preferences/iconShadowColor	Specifies the shadow color behind the desktop icon and text. Valid strings are in the style <code>QColor::setNamedColor()</code> . If not set, the system chooses a color that contrasts with the background.
root/desktop/preferences/menu/arrange/authorized	Specifies whether users can use the arrange function on the desktop.
root/desktop/preferences/menu/create/authorized	Specifies whether users can create connections from the right-click menu on the desktop.
root/desktop/preferences/menu/drag/authorized	Specifies whether users can drag and drop icons on the desktop.
root/desktop/preferences/menu/lockScreen/authorized	Specifies whether users can lock the screen from the right-click menu on the desktop.
root/desktop/preferences/menu/logout/authorized	Specifies whether users can log out from the right-click menu on the desktop.
root/desktop/preferences/menu/modeSwitch/authorized	Specifies whether users can switch to administrator mode from the right-click menu on the desktop.
root/desktop/preferences/menu/power/authorized	Specifies whether users can access the power submenu from the right-click menu on the desktop.
root/desktop/preferences/menu/poweroff/authorized	Specifies whether users can turn off the system from the right-click menu on the desktop.
root/desktop/preferences/menu/reboot/authorized	Specifies whether users can restart the system from the right-click menu on the desktop.
root/desktop/preferences/menu/sleep/authorized	Specifies whether users can put the system into the Sleep state from the right-click menu on the desktop.
root/desktop/preferences/menu textSize	Specifies the height of the desktop menu text in pixels. If nonpositive, the height is calculated as a proportion of the monitor size.
root/desktop/preferences/screenMargin	Specifies the margin between the screen edges and icons.
root/desktop/preferences/textBold	Specifies whether to bold the text.
root/desktop/preferences/textColor	Specifies the text color for the desktop icons. Valid strings are in the style <code>QColor::setNamedColor()</code> . If not set, the system chooses a color that contrasts with the background.
root/desktop/preferences/textShadowColor	Specifies the shadow color behind desktop icons and text. Valid strings are in the style <code>QColor::setNamedColor()</code> . If not set, the system chooses a color that contrasts with the text color.
root/desktop/preferences/textSize	Specifies the height of the desktop icon text in pixels. If nonpositive, the height is calculated as a proportion of the monitor size.
root/desktop/shortcuts/<action>/command	Sets the command that is run by the shortcut.
root/desktop/shortcuts/<action>/enabled	If set to 1, the shortcut is enabled.
root/desktop/shortcuts/<action>/shortcut	Sets the shortcut name.

Table G-30 Desktop registry keys (continued)

Registry key	Description
root/desktop/shortcuts/<action>/shortcutsMode	Sets the shortcut mode.

domain

Domain registry keys.

Table G-31 Domain registry keys

Registry key	Description
root/domain/OU	Specifies the organizational unit associated with the thin client's domain membership.
root/domain/allowSmartcard	This key is currently unused.
root/domain/cacheDomainLogin	If enabled, a hash of domain login credentials is saved to disk so that subsequent logins can occur even if the Active Directory server is inaccessible.
root/domain/ddns	If enabled, the thin client attempts to update the DNS server with its hostname and IP address during each DHCP renewal.
root/domain/domain	Specifies the domain to which this thin client is joined or to which this thin client is authenticating against.
root/domain/domainAdminGroup	If <code>enableDomainAdmin</code> is enabled, members of this AD group can switch the thin client to administrator mode.
root/domain/domainControllers	Specifies a comma-separated list of domain controllers to use with this domain. If left blank (recommended), automatic lookup of domain controllers is performed using DNS instead.
root/domain/domainJoined	Indicates if the thin client has been formally added to the domain.
root/domain/domainUsersGroup	If <code>enableDomainUsers</code> is enabled, domain logins are limited to direct members of this group. Nested groups are not supported for this feature.
root/domain/enableDomainAdmin	If set to 1, members of the group listed in <code>domainAdminGroup</code> can switch the thin client to administrator mode. If set to 0, the local root account must be used to perform local administrative tasks.
root/domain/enableDomainUsers	If set to 1, domain logins are limited to members of the group listed in <code>domainUserGroup</code> . If set to 0, any valid domain credential is permitted to log in to the thin client.
root/domain/enablePasswordChange	If set to 1, the user can change their domain password directly from the thin client.
root/domain/enableSSO	If enabled, encrypted current credentials are cached in memory and they can be reused when starting remote connections.
root/domain/loginAtStart	If set to 1, and if the thin client has been added to a domain, a login screen is displayed when the thin client starts up. Otherwise, the legacy ThinPro shared desktop is displayed at startup.

Table G-31 Domain registry keys (continued)

Registry key	Description
root/domain/retainUserRegistry	If set to 1, any custom setting changes made by the user are retained between login sessions.
root/domain/workgroup	Specifies the workgroup or “short domain” associated with the thin client’s domain membership. This is also referred to as the NetBIOS domain name during creation of the Active Directory domain. This value is usually auto-detected during domain authentication by looking up the value from a domain controller.

entries

Entries registry keys.

Table G-32 Entries registry keys

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

firewall

Registry keys for firewall settings.

Table G-33 Registry keys for firewall settings

Registry key	Description
root/firewall/direct/pptp-rule	
root/firewall/icmp-blocks	
root/firewall/interfaces	
root/firewall/masquerade	
root/firewall/ports	
root/firewall/services/<service>/checked	
root/firewall/services/<service>/description	
root/firewall/services/<service>/destinations/ipv4	
root/firewall/services/<service>/destinations/ipv6	

Table G-33 Registry keys for firewall settings (continued)

Registry key	Description
root/firewall/services/<service>/modules	
root/firewall/services/<service>/port-protocols	
root/firewall/services/<service>/short	
root/firewall/sources	
root/firewall/startAtBoot	

hwh264

hwh264 registry key.

Table G-34 hwh264 registry key

Registry key	Description
root/hwh264/force2x4k	<p>HP does not recommend changing the value of this key.</p> <p>In some Citrix H264 desktop configurations, large desktop streams with dual monitors cause a flickering effect. H264 is usually disabled for large streams due to this issue.</p>

keyboard

Registry keys for keyboard settings.

Table G-35 Registry keys for keyboard settings

Registry key	Description
root/keyboard/DrawLocaleLetter	If set to 1, the keyboard system tray icon will draw the language locale string instead of using static images.
root/keyboard/SystrayMenu/keyboardLayout	If set to 1, the right-click menu on the keyboard system tray icon offers an option to open the Keyboard Layout tool in Control Panel.
root/keyboard/SystrayMenu/languages	If set to 1, the right-click menu on the keyboard system tray icon offers an option to open the Language tool in Control Panel.
root/keyboard/SystrayMenu/virtualKeyboard	If set to 1, the right-click menu on the keyboard system tray icon offers an option to open the virtual keyboard.
root/keyboard/VisibleInSystray	If set to 1, the keyboard system tray icon is displayed and indicates the current keyboard layout.
root/keyboard/XkbLayout	This is an internal key used to map to an XKB keyboard layout. This key should not need to be modified.
root/keyboard/XkbModel	This is an internal key used to map to an XKB keyboard model. This key should not need to be modified.
root/keyboard/XkbOptions	This is an internal key used to map to XKB keyboard options. This key should not need to be modified.

Table G-35 Registry keys for keyboard settings (continued)

Registry key	Description
root/keyboard/XkbVariant	This is an internal key used to map to an XKB keyboard variant. This key should not need to be modified.
root/keyboard/enable2	If set to 1, the secondary keyboard layout can be switched to via the keyboard shortcut defined by <code>switch</code> .
root/keyboard/layout	Sets the primary keyboard layout.
root/keyboard/layout2	Sets the secondary keyboard layout.
root/keyboard/model	Sets the primary keyboard model.
root/keyboard/model2	Sets the secondary keyboard model.
root/keyboard/numlock	If set to 1, the Num Lock function is enabled at system startup. This registry key is intentionally ignored on mobile thin clients.
root/keyboard/switch	Sets the keyboard shortcut for switching between the first and second keyboard layout (<code>enable2</code> must also be set to 1). Valid values are as follows: <code>grp:ctrl_shift_toggle</code> , <code>grp:ctrl_alt_toggle</code> , <code>grp:alt_shift_toggle</code> .
root/keyboard/variant	Sets the primary keyboard variant.
root/keyboard/variant2	Sets the secondary keyboard variant.

license

Registry keys for license notification settings.

Table G-36 Registry keys for license notification settings

Registry key	Description
root/license/courtesyNotificationEnable	If set to 1, systray notifications are enabled as license expiration approaches.
root/license/courtesyNotificationInterval	If positive, number of hours between courtesy notifications.
root/license/courtesyNotificationStart	If positive, courtesy notifications start this many days before expiration.
root/license/courtesyNotificationText	If not blank, this text is used in courtesy notifications. %1 is replaced with the number of days left before expiration; %2 is replaced with the expiration date.
root/license/watermark	This value is read-only.

logging

Logging registry keys.

Table G-37 Logging registry keys

Registry key	Description
root/logging/general/debugLevel	Sets the debug level. This value will be leveraged by other modules to generate the corresponding logs.

Table G-37 Logging registry keys (continued)

Registry key	Description
<code>root/logging/general/showDebugLevelBox</code>	If set to 1, the Debug level option on the System Logs tab of the System Information window will be available to end users. If set to 0, the option is available to administrators only.

login

Login settings registry keys.

Table G-38 Login settings registry keys

Registry key	Description
<code>root/login/buttons/configure/authorized</code>	If set to 1, the Configuration button is available at the login screen.
<code>root/login/buttons/info/authorized</code>	If set to 1, the System Information button is available at the login screen.
<code>root/login/buttons/keyboard/authorized</code>	If set to 1, keyboard layout settings can be configured at the login screen.
<code>root/login/buttons/locale/authorized</code>	If set to 1, language settings can be configured at the login screen.
<code>root/login/buttons/mouse/authorized</code>	If set to 1, mouse settings can be configured at the login screen.
<code>root/login/buttons/onscreenKeyboard/authorized</code>	If set to 1, the onscreen keyboard is available at the login screen.
<code>root/login/buttons/power/authorized</code>	If set to 1, the power button is available at the login screen.
<code>root/login/buttons/poweroff/authorized</code>	If set to 1, the shut down function is available at the login screen.
<code>root/login/buttons/reboot/authorized</code>	If set to 1, the restart function is available at the login screen.
<code>root/login/buttons/show/authorized</code>	If set to 1, the button drawer containing additional options is available at the login screen.
<code>root/login/buttons/sleep/authorized</code>	If set to 1, the Sleep function is available at the login screen.
<code>root/login/buttons/touchscreen/authorized</code>	If set to 1, touch screen settings can be configured at the login screen. The registry key <code>root/touchscreen/enabled</code> must also be enabled.
<code>root/login/rememberedDomain</code>	
<code>root/login/rememberedUser</code>	

mouse

Mouse settings registry keys.

Table G-39 Mouse settings registry keys

Registry key	Description
<code>root/mouse/MouseHandedness</code>	If set to 0, the mouse is right-handed. If set to 1, the mouse is left-handed.
<code>root/mouse/MouseSpeed</code>	Sets the acceleration of the mouse pointer. Typically, a value from 0 to 25 is in the usable range. A value of 0 completely disables acceleration, causing the mouse to move at a constant slow, but measurable pace.
<code>root/mouse/MouseThreshold</code>	Sets the number of pixels before mouse acceleration is enabled. A value of 0 sets the acceleration to a natural curve that gradually scales acceleration, allowing for both precise and quick movements.
<code>root/mouse/disableTrackpadWhileTyping</code>	If set to 1, the trackpad will temporarily be disabled while typing. If set to 0, the trackpad will not be temporarily disabled while typing.
<code>root/mouse/enableNaturalScrolling</code>	If set to 1 (default), Natural Scrolling is enabled on the trackpad. If set to 0, Natural Scrolling is disabled on the trackpad.
<code>root/mouse/enableTrackpad</code>	If set to 1, the trackpad is enabled. If set to 0, the trackpad is disabled.
<code>root/mouse/enableTrackpadTapping</code>	If set to 0 (default), the tap-to-click behavior of the trackpad is disabled. If set to 1, tap-to-click behavior is enabled.
<code>root/mouse/enableTwoFingerScrolling</code>	If set to 1 (default), two finger scrolling is enabled on the trackpad. If set to 0, two finger scrolling is disabled on the trackpad.
<code>root/mouse/gui</code>	

restore-points

Registry key for restore-points.

Table G-40 Registry settings for restore-points

Registry key	Description
<code>tmp/restore-points/factory</code>	Specifies which snapshot to use for a factory reset.
<code>tmp/restore-points/on-boot</code>	Specifies which snapshot to restore after each restart. If not set, nothing is done.

screensaver

Screensaver settings registry keys.

Table G-41 Screensaver settings registry keys

Registry key	Description
<code>root/screensaver/SlideShowAllMonitors</code>	If set to 1, the screen saver slide show will be shown on all monitors. If set to 0, the slide show will be shown on the primary monitor only.
<code>root/screensaver/SlideShowInterval</code>	Sets the interval in seconds for switching images in the screen saver slide show.

Table G-41 Screensaver settings registry keys (continued)

Registry key	Description
<code>root/screensaver/SlideShowPath</code>	Specifies the directory that contains the images for the screen saver slide show.
<code>root/screensaver/buttons/configure/authorized</code>	If set to 1, the Configuration button is available while the screen is locked.
<code>root/screensaver/buttons/info/authorized</code>	If set to 1, the System Information button is available while the screen is locked.
<code>root/screensaver/buttons/keyboard/authorized</code>	If set to 1, keyboard layout settings can be configured while the screen is locked.
<code>root/screensaver/buttons/locale/authorized</code>	If set to 1, language settings can be configured while the screen is locked.
<code>root/screensaver/buttons/mouse/authorized</code>	If set to 1, mouse settings can be configured while the screen is locked.
<code>root/screensaver/buttons/onscreenKeyboard/authorized</code>	If set to 1, the onscreen keyboard is available while the screen is locked.
<code>root/screensaver/buttons/power/authorized</code>	If set to 1, the power button is available while the screen is locked.
<code>root/screensaver/buttons/poweroff/authorized</code>	If set to 1, the shut down function is available while the screen is locked.
<code>root/screensaver/buttons/reboot/authorized</code>	If set to 1, the restart function is available while the screen is locked.
<code>root/screensaver/buttons/show/authorized</code>	If set to 1, the button drawer containing additional options is available while the screen is locked.
<code>root/screensaver/buttons/sleep/authorized</code>	If set to 1, the Sleep function is available while the screen is locked.
<code>root/screensaver/buttons/touchscreen/authorized</code>	If set to 1, touch screen settings can be configured while the screen is locked. The registry key <code>root/touchscreen/enabled</code> must also be enabled.
<code>root/screensaver/enableCustomLogo</code>	If set to 1, the custom image defined in <code>logoPath</code> is used for the screen saver.
<code>root/screensaver/enableDPMS</code>	If set to 0, monitor power management is disabled. This causes the monitor to always stay on unless turned off manually.
<code>root/screensaver/enableScreensaver</code>	If set to 1, the screen saver is enabled.
<code>root/screensaver/enableSleep</code>	If set to 1, Sleep is enabled.
<code>root/screensaver/lockScreen</code>	If set to 1 and you are logged into administrator mode, a password is required to return to the desktop from the screen saver.
<code>root/screensaver/lockScreenDomain</code>	If set to 1 and the system is in domain mode, a password is required to return to the desktop from the screen saver.
<code>root/screensaver/lockScreenUser</code>	If set to 1 and you are not logged in as an administrator and the system is not in domain mode, a password is required to return to the desktop from the screen saver.
<code>root/screensaver/logoPath</code>	Sets the path to a custom image to use for the screen saver.

Table G-41 Screensaver settings registry keys (continued)

Registry key	Description
root/screensaver/mode	Sets the rendering mode for the screen saver image (such as Center, Tile, Expand, and Stretch). If set to Default, the image is displayed without any processing. If set to SlideShow, the screen saver will cycle through images in the directory specified by SlideShowPath.
root/screensaver/off	Sets the timeout delay in minutes before the monitor turns off.
root/screensaver/origImageCopyPath	This is the path where the custom image is saved when mode is set to Default.
root/screensaver/solidColor	If useSolidColor is on and enableCustomLogo is off, this solid color is used for the screen saver.
root/screensaver/standby	Sets the timeout delay in minutes before the monitor goes into standby mode.
root/screensaver/suspend	Sets the timeout delay in minutes before the monitor goes into suspend mode.
root/screensaver/timeoutScreensaver	Sets the timeout delay in minutes before the screen saver starts.
root/screensaver/timeoutSleep	Sets the timeout delay in minutes before the thin client goes into the Sleep state.
root/screensaver/useSolidColor	If set to 1 and enableCustomLogo is off, the value of the solidColor key is used by the screen saver.

security

Security settings registry keys.

Table G-42 Security settings registry keys

Registry key	Description
root/security/SecurityFeatures/ SpeculativeStoreBypassControl	Controls whether mitigations for Speculative Store Bypass (CVE-2018-3639) are enabled. By default, these mitigations are not enabled. To enable them, set the key value to on. For any change to this key to take effect, reboot the computer.
root/security/authenticationFailDelay	Sets the approximate time, in milliseconds, to delay after a failed login attempt. The actual time will vary plus or minus 25% of this value. For example, use a value of 3000 to obtain a delay of approximately 3 seconds.
root/security/domainEntryMode	If set to 1, the domain is expected to be entered in a separate text field labeled Domain . If set to 0, the domain is expected to be entered as part of the User field.
root/security/enableLockOverride	If set to 1, administrators can override the screen lock of a local desktop.
root/security/enableSecretPeek	If set to 1, password and PIN dialogs will have a button that, while selected, will show the entered password/PIN in clear text.

Table G-42 Security settings registry keys (continued)

Registry key	Description
root/security/encryption/identity/encryptedSecretCipher	Sets the algorithm for symmetric encryption of a secret. All algorithms use an appropriate amount of random salt, which is regenerated each time the secret is stored. The encryption key is different on each thin client, and encryption and decryption are available only to authorized programs. The supported cipher list includes most OpenSSL ciphers and ChaCha20-Poly1305.
root/security/encryption/identity/encryptedSecretTTL	Sets the number of seconds since the last successful login that a stored encrypted secret will be considered valid. If set to a negative number, encrypted secrets will not time out.
root/security/encryption/identity/encryptedSecretTTLnonSSO	Specifies the number of seconds that a stored, non-SSO encrypted secret is considered valid. If set to a nonpositive number, encrypted secrets do not time out.
root/security/encryption/identity/secretHashAlgorithm	Sets the algorithm for creating a hash of a secret. Key Derivation Functions (KDFs) such as scrypt or argon2 are better than straightforward hashes because it is not quick to compute a rainbow dictionary using a KDF. All algorithms use an appropriate amount of random salt, which is regenerated each time the secret is hashed. The supported list includes scrypt, Argon2, SHA-256, and SHA-512 (though the latter two are not KDFs).
root/security/encryption/identity/secretHashTTL	Sets the number of seconds since the last successful login that a stored hashes of secrets will be considered valid. If set to a negative number, hashes of secrets will not time out.
root/security/mustLogin	If set to 1, all users are forced to log in before accessing the desktop.

shutdown

Shutdown settings registry keys.

Table G-43 Shutdown settings registry keys

Registry key	Description
root/shutdown/enableAutomaticShutdownTimeout	If set to 1, a progress bar is shown in the shutdown/restart/logout confirmation dialog box. If the question is not answered in time, automatically shutdown/restart/logout.
root/shutdown/timeOfAutomaticShutdownTimeout	Sets the wait time for automatic shutdown timeout.

sshd

sshd registry keys.

Table G-44 sshd registry keys

Registry key	Description
root/sshd/disableWeakCipher	If set to 1, disable the CBC mode cipher and other known weak ciphers, such as 3DES, arcfour, etc.

Table G-44 sshd registry keys (continued)

Registry key	Description
root/sshd/disableWeakHmac	If set to 1, disable 96 bit hmac and any sha1-based and md5-based hmac.
root/sshd/disableWeakKex	If set to 1, disable key exchange algorithms that have DH with SHA1.
root/sshd/enabled	If set to 1, the SSH daemon is enabled and the thin client can be accessed via SSH.
root/sshd/userAccess	If set to 1, end users can connect to the thin client via SSH.

time

Time and date settings registry keys.

Table G-45 Time registry keys

Registry key	Description
root/time/NTPServers	Specifies NTP servers to use via a comma-separated list. Private NTP servers or large virtual NTP clusters such as <code>pool.ntp.org</code> are the best choices to minimize server load. Clear this value to return to using DHCP servers (tag 42) instead of a fixed list.
root/time/dateFormatLong	An optional way to override the long date format used in various ThinPro tools. For formatting, do a web search for <code>QDate::toString</code> . If left blank, a locale-specific string is usually used.
root/time/dateFormatShort	An optional way to override the short date format used in various ThinPro tools. For formatting, do a web search for <code>QDate::toString</code> . If left blank, a locale-specific string is usually used.
root/time/dateTimeFormatLong	An optional way to override the long date&time format used in various ThinPro tools. For formatting, do a web search for <code>QDate::toString</code> . If left blank, a locale-specific string is usually used.
root/time/dateTimeFormatShort	An optional way to override the short date&time format used in various ThinPro tools. For formatting, do a web search for <code>QDate::toString</code> . If left blank, a locale-specific string is usually used.
root/time/hideCountries	A semicolon-separated list of countries that you want hidden in the time zone selection GUI.
root/time/hideMap	If set to 1, the map is not drawn. This might be preferable in instances where boundaries are in dispute.
root/time/hideWinZones	A semicolon-separated list of Windows-format time zones, such as "(UTC+2:00) Tripoli," that you want hidden in the time zone selection GUI.
root/time/hideZones	A semicolon-separated list of Linux-format time zones, such as "America/Denver", that you want hidden in the time zone selection GUI.

Table G-45 Time registry keys (continued)

Registry key	Description
<code>root/time/timeFormatLong</code>	An optional way to override the long time format used in various ThinPro tools. For formatting, do a web search for <code>QDate::toString</code> . If left blank, a locale-specific string is usually used.
<code>root/time/timeFormatShort</code>	An optional way to override the short time format used in various ThinPro tools. For formatting, do a web search for <code>QDate::toString</code> . If left blank, a locale-specific string is usually used.
<code>root/time/timezone</code>	Sets the time zone. Time zones should be specified as defined by Linux Timezone in the Date and Time tool in Control Panel, and they should be in the following format: <region>/<subregion>
<code>root/time/use24HourFormat</code>	If set to -1, the system chooses the format automatically according to the locale. If set to 0, the a.m./p.m. format is used. If set to 1, the 24-hour format is used.
<code>root/time/useADNSTimeServers</code>	If set to 1, the thin client will attempt to set the time zone via the Active Directory domain controllers auto-discovered on the local network. It does this via the following DNS query for SRV records: <code>_ldap._tcp.dc._msdcs.domain</code> .
<code>root/time/useDHCPTimezone</code>	If set to 1, the thin client will attempt to set the time zone via DHCP. To properly set the time zone via this registry key, ensure that the DHCP server for the thin client forwards the <code>tcodc</code> DHCP tag (which is usually tag 101, although 100 and 2 can work also).
<code>root/time/useNTPServers</code>	If set to 1, the use of NTP time servers to synchronize the thin client clock is enabled. If this is enabled, ensure that an NTP server is specified via DHCP or via <code>NTPServers</code> .

touchscreen

Touchscreen settings registry keys.

Table G-46 Touchscreen settings registry keys

Registry key	Description
<code>root/touchscreen/beep</code>	Defines whether the thin client beeps when the touch screen is used.
<code>root/touchscreen/calibrated</code>	This registry key is either used internally or reserved for future use. The value should not be changed.
<code>root/touchscreen/enabled</code>	If set to 1, touch input is enabled.
<code>root/touchscreen/maxx</code>	This registry key is either used internally or reserved for future use. The value should not be changed.
<code>root/touchscreen/maxy</code>	This registry key is either used internally or reserved for future use. The value should not be changed.
<code>root/touchscreen/minx</code>	This registry key is either used internally or reserved for future use. The value should not be changed.
<code>root/touchscreen/miny</code>	This registry key is either used internally or reserved for future use. The value should not be changed.

Table G-46 Touchscreen settings registry keys (continued)

Registry key	Description
<code>root/touchscreen/port</code>	Specifies the port that is connected to the touch screen.
<code>root/touchscreen/swapx</code>	This registry key is either used internally or reserved for future use. The value should not be changed.
<code>root/touchscreen/swapy</code>	This registry key is either used internally or reserved for future use. The value should not be changed.
<code>root/touchscreen/type</code>	Specifies the controller type of the touch screen.

translation

Translation settings registry keys.

Table G-47 Translation settings registry keys

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

usb-update

USB-update registry keys.

Table G-48 usb-update registry keys

Registry key	Description
<code>root/usb-update/authentication</code>	If set to 1, an administrator password is required to do USB updates.
<code>root/usb-update/enable</code>	If set to 1, USB update auto-detection is enabled.
<code>root/usb-update/height</code>	Sets the height of the USB Update window in pixels.

Table G-48 usb-update registry keys (continued)

Registry key	Description
root/usb-update/searchMaxDepth	Sets the depth of subdirectories to be searched for updates. Setting a high search depth can cause delays on USB flash drives that have thousands of directories.
root/usb-update/width	The width of the USB Update window in pixels.

users

User settings registry keys.

Table G-49 User settings registry keys

Registry key	Description
root/users/root/enablePassword	If enabled, logins to the local root administrator account are enabled. If disabled, only Active Directory administrators can change the thin client to administrator mode.
root/users/root/password	Sets the administrator password. If empty, administrator mode is locked.
root/users/root/timeout	Specifies the idle timeout (in minutes) after which administrator mode will be terminated. If set to 0 or negative, administrator mode will never be automatically terminated.
root/users/user/SSO	This registry key is either used internally or reserved for future use. The value should not be changed.
root/users/user/WOL	If set to 1, Wake On LAN (WOL) is enabled.
root/users/user/XHostCheck	If set to 1, only the systems listed under <code>root/users/user/xhosts</code> are allowed to remotely control the thin client.
root/users/user/apps/hptc-ad-change-password/authorized	If set to 1, the Change Domain Password Control Panel item is accessible by end users.
root/users/user/apps/hptc-ad-mgr/authorized	If set to 1, the Active Directory Control Panel item is accessible by end users.
root/users/user/apps/hptc-agent-mgr/authorized	If set to 1, the HPDM/HPCEM Agent Control Panel item is accessible by end users.
root/users/user/apps/hptc-auto-update/authorized	If set to 1, the Automatic Update Control Panel item is accessible by end users.
root/users/user/apps/hptc-background-mgr/authorized	If set to 1, the Background Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-cert-mgr/authorized	If set to 1, the Certificate Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-compatibility/authorized	If set to 1, the Compatibility Check Control Panel item is accessible by end users.
root/users/user/apps/hptc-component-mgr/authorized	If set to 1, the Component Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-config-wizard/authorized	If set to 1, the Initial Setup Wizard Start menu item is accessible by end users.
root/users/user/apps/hptc-connection-wizard/authorized	If set to 1, Create a Connection is accessible by end users.

Table G-49 User settings registry keys (continued)

Registry key	Description
root/users/user/apps/hptc-control-panel/authorized	If set to 1, Control Panel is accessible by end users.
root/users/user/apps/hptc-date-mgr/authorized	If set to 1, the Date and Time Control Panel item is accessible by end users.
root/users/user/apps/hptc-dhcp-mgr/authorized	If set to 1, the DHCP Options Control Panel item is accessible by end users.
root/users/user/apps/hptc-display-prefs/authorized	If set to 1, the Display Control Panel item is accessible by end users.
root/users/user/apps/hptc-easy-update/authorized	If set to 1, the Easy Update Control Panel item is accessible by end users.
root/users/user/apps/hptc-factory-reset/authorized	If set to 1, the Factory Reset Control Panel item is accessible by end users.
root/users/user/apps/hptc-firewalld-mgr/authorized	If set to 1, the Firewall Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-il18n-mgr/authorized	If set to 1, the Language Control Panel item is accessible by end users.
root/users/user/apps/hptc-ibus-mgr/authorized	If set to 1, the Ibus Input Method Control Panel item is accessible by end users.
root/users/user/apps/hptc-imprivata-mgr/authorized	If set to 1, the Imprivata Setup Control Panel item is accessible by end users.
root/users/user/apps/hptc-keyboard-layout/authorized	If set to 1, the Keyboard Layout Control Panel item is accessible by end users.
root/users/user/apps/hptc-kiosk/authorized	If set to 1, Connection Manager is accessible by end users.
root/users/user/apps/hptc-licenses/authorized	If set to 1, HP License Agreement is accessible by end users.
root/users/user/apps/hptc-mixer/authorized	If set to 1, the Sound Control Panel item is accessible by end users.
root/users/user/apps/hptc-mouse/authorized	If set to 1, the Mouse Control Panel item is accessible by end users.
root/users/user/apps/hptc-network-mgr/authorized	If set to 1, the Network Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-power-mgr/authorized	If set to 1, the Power Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-printer-mgr/authorized	If set to 1, the Printers Control Panel item is accessible by end users.
root/users/user/apps/hptc-regeditor/authorized	If set to 1, Registry Editor is accessible by end users.
root/users/user/apps/hptc-restore/authorized	If set to 1, the Snapshots Control Panel item is accessible by end users.
root/users/user/apps/hptc-scep-mgr/authorized	If set to 1, the SCEP Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-security/authorized	If set to 1, the Security Control Panel item is accessible by end users.

Table G-49 User settings registry keys (continued)

Registry key	Description
root/users/user/apps/hptc-serial-mgr/authorized	If set to 1, the Serial Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-shortcut-mgr/authorized	If set to 1, the Keyboard Shortcuts Control Panel item is accessible by end users.
root/users/user/apps/hptc-snipping-tool/authorized	If set to 1, the Snipping Tool Start menu item is accessible by end users.
root/users/user/apps/hptc-sshd-mgr/authorized	If set to 1, the SSHD Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-switch-admin/authorized	If set to 1, Switch to Administrator/User is accessible by end users.
root/users/user/apps/hptc-sysinfo/authorized	If set to 1, System Information is accessible by end users.
root/users/user/apps/hptc-task-mgr/authorized	If set to 1, the Task Manager Start menu item is accessible by end users.
root/users/user/apps/hptc-text-editor/authorized	If set to 1, the Text Editor Start menu item is accessible by end users.
root/users/user/apps/hptc-thinstate/authorized	If set to 1, the ThinState Control Panel item is accessible by end users.
root/users/user/apps/hptc-touchscreen/authorized	If set to 1, the Touch Screen Control Panel item is accessible by end users.
root/users/user/apps/hptc-update/authorized	If set to 1, Check for Updates is accessible by end users.
root/users/user/apps/hptc-usb-mgr/authorized	If set to 1, the USB Manager Control Panel item is accessible by end users.
root/users/user/apps/hptc-user-rights/authorized	If set to 1, the Customization Center Control Panel item is accessible by end users.
root/users/user/apps/hptc-vncshadow/authorized	If set to 1, the VNC Shadow Control Panel item is accessible by end users.
root/users/user/apps/hptc-wlsstat/authorized	If set to 1, Wireless Statistics is accessible by end users.
root/users/user/apps/hptc-xen-general-mgr/authorized	If set to 1, the Citrix general settings are accessible by end users.
root/users/user/apps/hptc-xterm/authorized	If set to 1, X Terminal is accessible by end users. CAUTION: Enabling X terminal access is a security risk and is not recommended in a production environment. The X terminal should only be enabled for use in debugging a protected, non-production environment.
root/users/user/desktopScaling	Specifies the percentage to increase or decrease the size of desktop elements. If set to 100 (default), standard scaling is used. If set to 50, half the size of standard scaling is used. If set to 200, double the size of standard scaling is used.
root/users/user/enablePassword	If enabled, logins to the local shared account user are enabled.
root/users/user/hideDesktopPanel	If set to 1, desktop panels such as the taskbar are not started or shown in the desktop.
root/users/user/kioskMode	This registry key is either used internally or reserved for future use. The value should not be changed.

Table G-49 User settings registry keys (continued)

Registry key	Description
root/users/user/launchConnectionManager	If set to 1, Connection Manager launches at system startup.
root/users/user/rightclick	If set to 1, the right-click menu for the desktop is enabled.
root/users/user/ssconnectiontype	This registry key is either used internally or reserved for future use. The value should not be changed.
root/users/user/switchAdmin	If set to 1, switching to administrator mode is enabled.
root/users/user/theme	Reserved for future use.
root/users/user/xhosts/<UUID>/xhost	Specifies the IP address or hostname of a system that will be allowed to remotely control the thin client when XHostCheck is enabled.

vncserver

vncserver registry keys.

Table G-50 vncserver registry keys

Registry key	Description
root/vncserver/coreSettings/enableVncShadow	If set to 1, the VNC shadowing server for the thin client is enabled.
root/vncserver/coreSettings/userNotificationMessage	Sets the notification message that is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncAllowLoopbackOnly	If set to 1, only a localhost or loopback address is allowed for VNC connections.
root/vncserver/coreSettings/vncDefaultNumLockStatus	If set to 1, Num Lock is on by default. If set to 0, Num Lock is off by default.
root/vncserver/coreSettings/vncNotifyShowTimeout	If set to 1, a timeout is applied to the notification dialog that is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncNotifyTimeout	Sets the timeout in seconds for the notification dialog that is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncNotifyUser	If set to 1, a notification is shown to the user when someone is attempting to connect to the thin client using VNC.
root/vncserver/coreSettings/vncPassword	Sets the password for VNC shadowing. The key vncUsePassword must also be enabled.
root/vncserver/coreSettings/vncReadOnly	If set to 1, VNC shadowing will operate in view-only mode.
root/vncserver/coreSettings/vncRefuseInDefault	If set to 1, VNC requests are refused automatically if the user does not interact with the notification dialog before the timeout.
root/vncserver/coreSettings/vncStopButton	If set to 1, an always-on-top button is shown on the left corner of the screen. Selecting that button disconnects the VNC session.
root/vncserver/coreSettings/vncTakeEffectRightNow	If set to 1, VNC settings take effect immediately after being modified.

Table G-50 vncserver registry keys (continued)

Registry key	Description
root/vncserver/coreSettings/vncUseHTTP	If set to 1, HTTP port 5800 is open for VNC connections.
root/vncserver/coreSettings/vncUsePassword	If set to 1, the password specified in <code>vncPassword</code> is required for VNC shadowing.
root/vncserver/coreSettings/vncUseSSL	If set to 1, SSL is used for VNC connections.
root/vncserver/gui/VNCShadowManager/name	This registry key is either used internally or reserved for future use. The value should not be changed.
root/vncserver/gui/VNCShadowManager/status	This registry key is either used internally or reserved for future use. The value should not be changed.
root/vncserver/gui/VNCShadowManager/title	This registry key is either used internally or reserved for future use. The value should not be changed.
root/vncserver/gui/VNCShadowManager/widgets/ enableVncShadow	Controls the state of the Enable VNC Shadow widget in the VNC Shadow tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/ userNotificationMessage	Controls the state of the User Notification Message widget in the VNC Shadow tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/vncserver/gui/vncAllowLoopbackOnly	Controls the state of the Allow Loopback Connections Only widget in the VNC Shadow utility. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/ vncNotifyShowTimeout	Controls the state of the VNC Show Timeout for Notification widget in the VNC Shadow tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/ vncNotifyTimeout	Controls the state of the numerical widget in the VNC Shadow tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/ vncNotifyUser	Controls the state of the VNC Notify User to Allow Refuse widget in the VNC Shadow tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/ vncPassword	Controls the state of the Set Password widget in the VNC Shadow tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/ vncReadOnly	Controls the state of the VNC Read Only widget in the VNC Shadow tool. If set to <code>active</code> , the widget is visible in the UI and the user can interact with it. If set to <code>inactive</code> , the widget is hidden. If set to <code>read-only</code> , the widget is visible in the read-only state.

Table G-50 vncserver registry keys (continued)

Registry key	Description
root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault	Controls the state of the Refuse connections in default widget in the VNC Shadow tool. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/vncserver/gui/vncStopButton	Controls the state of the VNC Stop Shadow button widget in the VNC Shadow utility. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow	Controls the state of the Re-set VNC server right now widget in the VNC Shadow tool. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncUseHTTP	Controls the state of the VNC Use HTTP Port 5800 widget in the VNC Shadow tool. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword	Controls the state of the VNC Use Password widget in the VNC Shadow tool. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.
root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL	Controls the state of the VNC Use SSL widget in the VNC Shadow tool. If set to <i>active</i> , the widget is visible in the UI and the user can interact with it. If set to <i>inactive</i> , the widget is hidden. If set to <i>read-only</i> , the widget is visible in the read-only state.

zero-login

Smart Zero registry keys.

Table G-51 Smart Zero registry keys

Registry key	Description
root/zero-login/buttons/configure/authorized	If set to 1, the Configure button is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/info/authorized	If set to 1, the System Information button is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/keyboard/authorized	If set to 1, the Keyboard Layout selection is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/locale/authorized	If set to 1, the Locale selection is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/mouse/authorized	If set to 1, the Mouse selection is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/onscreenKeyboard/authorized	If set to 1, the on-screen keyboard option is available in the login or Smart Zero credentials dialog box.

Table G-51 Smart Zero registry keys (continued)

Registry key	Description
root/zero-login/buttons/power/authorized	If set to 1, the Power button is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/poweroff/authorized	If set to 1, the Poweroff option is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/reboot/authorized	If set to 1, the Reboot option is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/show/authorized	If set to 1, buttons are displayed in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/sleep/authorized	If set to 1, the Sleep option is available in the login or Smart Zero credentials dialog box.
root/zero-login/buttons/touchscreen/authorized	If set to 1, the Touchscreen selection is available in the login or Smart Zero credentials dialog box. NOTE: The root/touchscreen/enabled key must also be set.

SNMP

This table describes the SNMP registry keys.

Table G-52 SNMP

Registry key	Description
root/snmp/agentBehaviour/enable	If set to 1, the SNMP daemon is enabled and the thin client is accessible via SNMP. Be sure that you have a security SNMP configuration or work in a secure network environment.
root/snmp/agentBehaviour/usePrivateConfFile	If set to 1, the SNMP daemon uses a user custom setting file for some advanced features but does not generate snmpd.conf from the registry.
root/snmp/agentBehaviour/listenInterface	This option does not work well with DHCP service, so please set this area blank when you use only one wired interface card or use a wireless card. Set this value to SNMP daemon listen interface for security, only the specified interface on system can access ThinPro via SNMP. NOTE: If this area is blank, the agent is listening to all of the network interfaces.
root/snmp/agentBehaviour/communityList/{UUID}/ communityName	Community Name, only specified community name can access ThinPro.
root/snmp/agentBehaviour/communityList/{UUID}/ permission	Specified a community permission. Read-only can only get system information and read-write can change ThinPro setting.
root/snmp/agentBehaviour/communityList/{UUID}/ accessibleOID	Only OIDs that start with this value can be accessed.

Index

A

- Active Directory 70
- add-ons 1
- administrator mode 3
- audio redirection
 - RDP 34
 - VMware Horizon View 40
- Automatic restart 107

B

- Background Manager 81

C

- Certificate Manager 69
 - certificates
 - installing 69
 - VMware Horizon View 41
- Citrix
 - HP True Graphics 51
 - settings 19
- client profile
 - adding files 90
 - adding symbolic link 92
 - certificates 90
 - customization 89
 - loading 89
 - registry settings 90
 - saving 92
- connections
 - advanced settings 16
 - configuration 14
 - hiding 81
- Control Panel
 - Active Directory 70
 - Background Manager 81
 - Customization Center 81
 - Date and Time 59
 - DHCP Option Manager 65
 - Display 80
 - Easy Update 70
 - Factory Reset 59
 - Keyboard Shortcuts 78
 - Language 81
 - Ibus 78
 - Mouse 78
 - Network 60
 - overview 59

- Power Manager 59
- SCEP Manager 67
- Security 67
- Serial Manager 79
- Snapshots 59
- Snipping Tool 57
- Sound 79
- SSHD Manager 70
- Task Manager 57
- Text Editor 57
- ThinState
 - See* HP ThinState
- Touch Screen 78
- utilities, hiding 81
- VNC Shadow 76
- Wireless Statistics 57
- X Terminal 57
- custom connections 49

D

- date and time settings 59
- device redirection
 - RDP 32
 - VMware Horizon View 39
- DHCP options 65
- display management 80
- display profiles 80

E

- Easy Update 70
- Ephemeral 106

F

- factory reset 59
- finding more information 1

G

- getting started 1
- GUI
 - Connection Manager (ThinPro only) 15
 - desktop 10
 - overview 10
 - taskbar 11

H

- HP Cloud Endpoint Manager 2
 - See* HPCEM Agent
 - See also* remote management service
- HP Device Manager 2
 - See* HPDM Agent
 - See also* remote management service
- HP Disk Encryption 3
- HP Smart Client Services 2
 - installing 85
 - overview 85
- Profile Editor
 - See* Profile Editor
 - See also* remote management service
 - supported operating systems 85
- HP True Graphics 51
- HPCEM Agent 70
- HPDM Agent 70

I

- image updates 1
- imaging
 - See* HP ThinState

K

- keyboard shortcuts 78
- kiosk mode 17

L

- language settings 81
- Ibus 78

M

- mass storage redirection
 - RDP 33
- MMR
 - See* multimedia redirection
- mouse settings 78
- multimedia redirection
 - RDP 32

N

network settings
 accessing 60
 General 64
 wired 60
 wireless 61

O

On Boot Snapshot 106
OS configuration, choosing 1

P

parallel printer configuration 92
passwords, change 67
power management settings 59
Power Manager 59
printer configuration 92
printer redirection
 RDP 33
printers 80
Profile Editor 89

R

RDP
 audio redirection 34
 device redirection 32
 mass storage redirection 33
 multi-monitor sessions 31
 multimedia redirection 32
 printer redirection 33
 RemoteFX 31
 settings, per-connection 27
 smart card redirection 34
 USB redirection 32
registry keys 113
remote management service,
 choosing 2
RemoteFX 31
Restart Plan 107

S

SCEP Manager 67, 69
screen saver settings 59
Secure Shell 48
security settings 67
Serial Manager 79
serial printer configuration 92
SIM PIN 70
Sleep state 59
smart card redirection
 RDP 34
 VMware Horizon View 40

Smart Zero

See OS configuration
snapshots 59
Snapshots 82
Snipping Tool 57
sound settings 79
SSHD Manager 70
system diagnostics 96
System Information 106

T

Task Manager 57
Telnet 49
text editor 57
thin clients
 updating
 See updating thin clients
ThinPro
 See OS configuration
ThinState
 See HP ThinState
touch screen settings 78
troubleshooting 95
 network connectivity 95
 using system diagnostics 96

U

updating thin clients
 broadcast update 87
 DHCP tagging update 87
 DNS alias update 88
 manual update 88
USB redirection
 RDP 32
 USB Manager 80
 VMware Horizon View 39
user mode 3

V

VMware Horizon View
 audio redirection 40
 certificates 41
 changing protocols 41
 device redirection 39
 keyboard shortcuts 39
 multi-monitor sessions 39
 settings, per-connection 34
 smart card redirection 40
 USB redirection 39
 webcam redirection 41
VNC Shadowing 76

W

Web Browser
 settings, per-connection 43
webcam redirection
 VMware Horizon View 41
websites
 Citrix support 1
 HP support 1
 Microsoft support 1
 VMware support 1
wireless statistics 57

X

X Terminal 57
XDMCP 47