



HP Device Manager 4.6

Administrator Guide

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

Pentium is a trademark of Intel Corporation in the U.S. and other countries. Microsoft and Windows are U.S. registered trademarks of the Microsoft group of companies. Java is a registered trademark of Oracle and/or its affiliates.

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.

First Edition: February 2014

Document Part Number: 762788-001

Table of contents

1 Introduction	1
What is HP Device Manager?	1
Overview	2
HPDM Console	3
HPDM Server	3
HPDM Gateway	3
HPDM Agent	3
Repositories	4
Terms and definitions	5
Finding the latest updates	5
2 Getting started with HPDM	6
System requirements	7
HPDM Server requirements	7
HPDM Gateway requirements	7
HPDM Console requirements	8
HPDM Agent requirements	9
Master Repository Controller requirements	11
Network requirements	11
Port requirements	11
Installing HPDM	12
Installing an HPDM 4.6 Service Pack	13
Using the HPDM Console	13
Logging in to the HPDM Console	13
HPDM Console overview	13
Operating system tabs	14
HPDM Gateway tab	15
Discovering device systems	15
Displaying device properties	16
Basic asset information	16
Collecting complete asset information	17
Displaying complete device asset information	17
Keeping the HPDM Agent updated on device systems	17
3 Device discovery	18
Automatic registration (normal thin clients)	18

Automatic registration (PCoIP zero clients)	19
Using a DNS service record	19
Using a DHCP vendor class option	19
Searching for devices	20
Using the Walking With IP Range method	20
Configuring an IP scope	21
Using the Walking With IP List method	21
Manually registering a device	21
Manually registering multiple devices	22

4 Using tasks 23

Task templates	23
Creating and editing task templates	24
Adding a template to the Favorites	24
Importing and exporting task templates	24
Using template sequences	26
_Template Sequence	27
Basic template sequences	27
Advanced template sequences	27
Tasks	28
Performing a task	28
Task status icons	28
Task parameters	29
Manual tasks	29
Valid Time, Timeout & WOL	29
Target Device List	30
Schedule & Batch Control	30
Task deferment	30
Displaying task properties	30
Configuring task parameters	30
Pausing tasks	31
Continuing tasks	31
Resending tasks	32
Canceling tasks	32
Deleting tasks	32
Displaying task logs	32
Displaying a task's success rate	32
Opening VNC Viewer for shadowing	32
Opening a Result Template	32
Viewing tasks from all users	33
Task rules	33

Adding a new rule	33
5 Device management	34
Viewing devices	34
Deleting devices	35
Grouping devices	35
Setting group information using a DHCP tag	35
Switch to Manual Grouping	36
Adding a new Manual Group	36
Dynamic Grouping	36
Creating a new Dynamic Grouping scheme	36
Switching to a Dynamic Group	36
Filtering devices	37
Creating a new Device Filter	37
Editing a Device Filter	37
Filter Security	37
Checking network connection status	38
Printing information about devices	38
Printing device information	38
Shadowing devices	39
Power management	39
Managing normal thin clients	39
Changing a device's hostname	39
Capturing and deploying connections	40
Cloning and deploying settings	40
Applying custom settings	40
Managing files and registry settings	41
Capturing files	42
Deploying files	42
Deleting files	43
Managing device registry settings	43
Cloning registry settings	43
Adding, editing, and deleting registry settings	44
Remotely executing commands	44
Remotely executing Windows scripts	45
Pausing a _File and Registry task	45
Adding or removing program records	45
Running a script	46
Enrolling certificates with SCEP	46
Managing PCoIP zero clients	46
Capturing connections	46

Deploying connections	47
Updating firmware	47
6 Imaging operations	48
Imaging support matrix	49
Imaging without PXE	50
Capturing an image without PXE	50
Preserved settings during an image capture without PXE	51
Deploying an image without PXE	51
Preserved settings during an image deployment without PXE	52
Imaging with PXE	52
Capturing an image with PXE	52
Deploying an image with PXE	53
Configuring your environment for PXE imaging	53
Configuring a DHCP server for PXE imaging	53
The DHCP server is installed on a different machine from the HPDM Server	53
The DHCP server is installed on the same machine as the HPDM Server	53
Configuring a Linux DHCP server for PXE imaging	54
Configuring routers for PXE imaging	55
Configuring BIOS settings on legacy Neoware devices for PXE imaging	55
7 Repository management	56
Initializing from wizard	56
Selecting the file protocol to use	56
Configuring the Master Repository	56
Configuring the Child Repositories	57
Deleting Child Repositories	57
Exporting repositories	57
Importing repositories	57
Synchronizing repositories	58
Content management	58
Viewing detailed payload information	58
Deleting contents from the Master Repository	58
Downloading contents from the Files Captured category	59
Repository mapping	59
Batch mapping	59
Per device mapping	59

8 Security management	60
User management	60
Adding users	60
Deleting users	60
Assigning users to groups	60
Changing a user's password	60
Assigning Security Filters to Users	61
Adding a group	61
Assigning permissions to groups	61
Assigning users to groups	61
Assigning security filters to groups	61
Deleting groups	62
User authentication with LDAP and Active Directory	62
Configuration	62
Importing users and groups	63
Authentication management	65
Key management	65
HPDM Gateway access control	66
9 Report management	67
Adding a report template	67
Importing a report plug-in file	67
Generating a report using a report template	67
Producing reports	68
HPDM Gateway report	68
Device Information report	68
Device Task report	68
Task report	68
Task Status report	69
Task Log report	69
10 Status Walkers	70
Status Walker	70
Creating a Status Walker	70
Configuring the Status Walker	70
Status Snapshot	71
11 HP FTP Software Component Browser	72
Generating task templates	72
Configuring HP FTP proxy settings	73

12 HPDM Server Backup and Restore Tool	74
Backing up the HPDM Server	75
Restoring the HPDM Server	75
13 HPDM Port Check Tool	77
14 HPDM Agent polling and error logging	78
HPDM Agent polling	78
Error logging	78
HPDM Agent logging	78
HPDM Gateway logging	78
HPDM Server and HPDM Console logging	79
Master Repository Controller logging	80
Appendix A Template reference	81
File and Registry	81
Agent	81
Connections	82
Imaging	82
Operations	82
Settings	83
Template Sequence	84
Appendix B Port reference	85
HPDM Console ports	85
HPDM Server ports	86
HPDM Gateway ports	87
HPDM Agent ports	88
Repository ports	90
Index	93

1 Introduction

What is HP Device Manager?

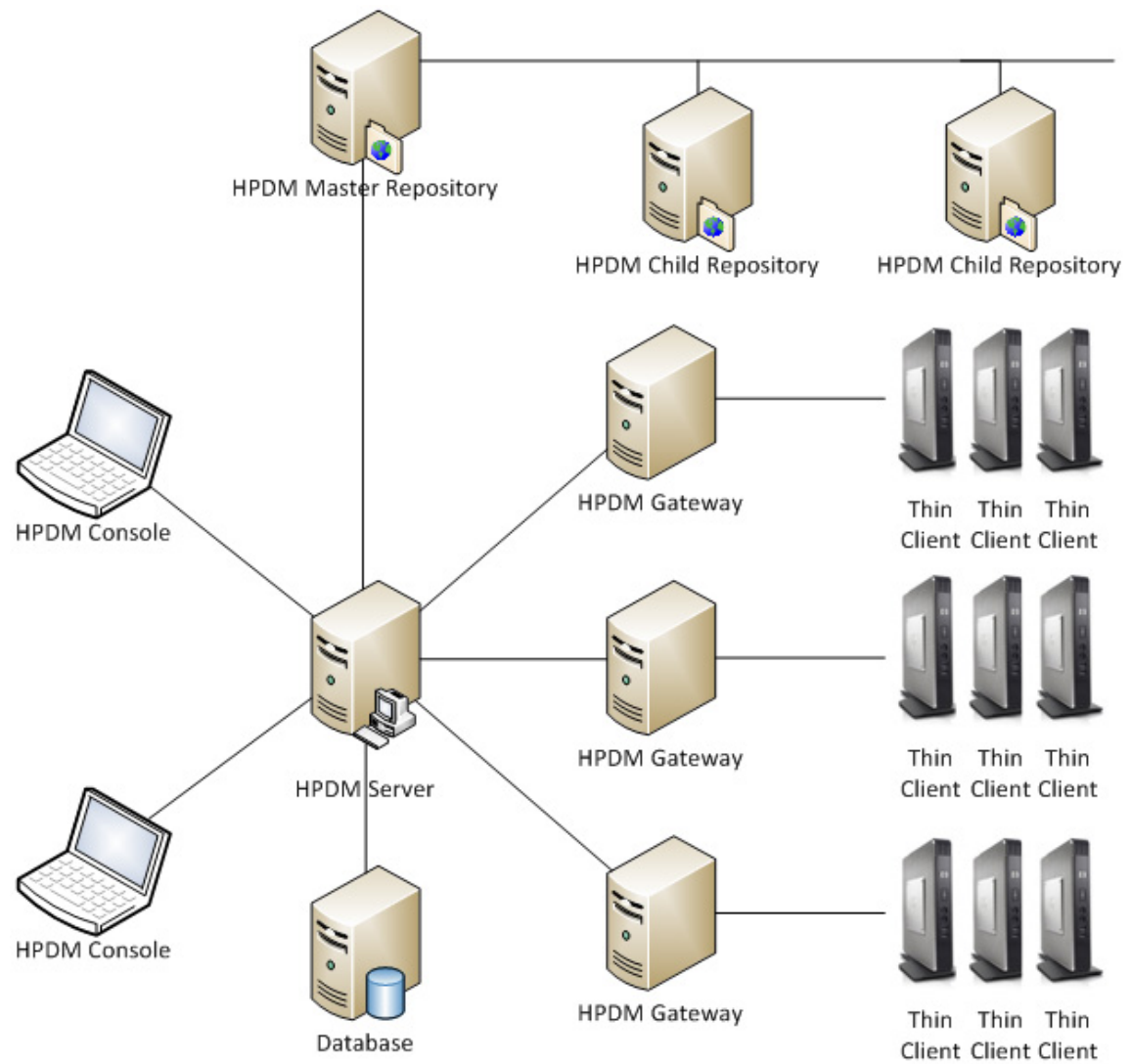
HP Device Manager (HPDM) is a server-based application that provides powerful centralized administration capabilities for thin client devices running HP software. Features of HPDM include the following:

- Centralized management tool
- Thin client administration handled through tasks
- Supports all HP thin client operating systems
- Secure communication channels with data encryption
- Support for WAN environment

Overview

HPDM is structured as a Console–Server–Gateway system.

Figure 1-1 HPDM overview



 **NOTE:** The deployment of the HPDM system is very flexible. See the deployment white paper at <ftp://ftp.hp.com/pub/hpdm/Documentation/WhitePapers/> for more details.

HPDM Console

The HPDM Console is the user interface of HPDM and can be installed on any number of machines. Several HPDM Consoles can interact with an HPDM Server.

The HPDM Console allows system administrators to do the following:

- View details for each controlled device
- Organize device trees
- Create and maintain remote job definitions
- Monitor tasks sent out to devices

HPDM Server

The HPDM Server controls HPDM Agents through the HPDM Gateway.

Tasks, stored as task templates on the HPDM Server, can be sent to each HPDM Agent through each HPDM Agent's respective HPDM Gateway to perform commands as required.



IMPORTANT: There must be only one HPDM Server in the system.

HPDM Gateway

The HPDM Gateway serves as the link between HPDM Agents and the HPDM Server. The HPDM Agents register with the HPDM Gateway when they are started.

Multiple HPDM Gateways may be required for specific network architecture or load balancing, but it is not mandatory. In many cases, installing an HPDM Gateway to manage thousands of devices in different subnets is also an appropriate deployment strategy. In a simple single network environment, the HPDM Gateway and HPDM Server can be hosted on the same computer.



TIP: The machine installed with the HPDM Gateway also normally contains the PXE server installed by HPDM.

HPDM Agent

The HPDM Agent is a software component installed on devices so that HPDM can interact with them. HPDM Agents are embedded into the operating system to enable HPDM to manage devices out-of-the-box (HPDM Agents on older devices may need to be upgraded).

HPDM Agents receive task commands from an HPDM Gateway, execute the commands and report back to the HPDM Gateway with the results.

Repositories

Repositories are where task payload files are stored. HPDM Agents download files from or upload files to repositories according to tasks from the HPDM Server. These files can include but are not limited to the following:


- Device images
- Imaging tools
- HPDM Gateway and HPDM Agent files
- Software components (add-ons)

The components of the repository system are as follows:

- **Master Repository**—Holds all payload files. There can only be one Master Repository in the system.
- **Child Repository**—Holds all or some payload files. There can be multiple Child Repositories.
- **Master Repository Controller**—Manages the payload files in the Master Repository and synchronizes the files with the Child Repositories as requested by the HPDM Server. The Master Repository Controller must be installed on the same computer as the Master Repository.


Repositories are standard file servers and support the following protocols:

- FTP (File Transfer Protocol)
- FTPS (FTP Secure)
- SFTP (Secure FTP)
- SMB (Server Message Block)

 **TIP:** The SMB protocol is a network file-sharing protocol. Its implementation in Windows is known as Shared Folder, and in Linux it is known as Samba. The Common Internet File System (CIFS) protocol is a dialect of SMB.

A repository can use either one or two protocols as follows:

- If using only one protocol, it can be any of the four protocols listed above.
- If using two protocols, one of them must be SMB. SMB is needed for non-cached imaging in Windows Embedded Standard (WES). For the second protocol, one of the other three (FTP/FTPS/SFTP) is recommended for HP ThinPro and HP Smart Zero Core imaging because SMB is not well-supported for those operating systems. All other tasks can use any of the protocols.

 **TIP:** If two protocols are configured for a repository, FTP/FTPS/SFTP will be tried first, unless it's a non-cached WES imaging task.

Terms and definitions

Table 1-1 Terms and definitions

Term	Definition
Device	A device refers to a device managed by HPDM, such as a thin client.
Package	<p>A package is comprised of a description file and a folder that contains payload files. The package name is identical to the folder name, which can be any legal string.</p> <p>The name of the description file follows the convention <code>PackageName-ChecksumString.desc</code>. The checksum is computed from all payload files in alphabetical sequence of filename or folder name with depth-first traversal.</p>
PXE	<p>PXE (Preboot eXecution Environment) is a network protocol used to start up computers using a network interface that is independent of data storage devices or installed operating systems.</p> <p>HPDM utilizes PXE to execute device image extraction and distribution. PXE is an optional imaging mechanism best used for remote system recovery.</p>
Rule	<p>A rule enables you to automate the execution of tasks. Each rule has three parts:</p> <ul style="list-style-type: none">• Filter—Defines which devices the rule applies to• Trigger—Defines when the rule is executed• Template—Defines what operation should be performed on the devices
Task	A task is the scheduled action that execute task templates to a device or group of devices. A task is comprised of a template, an execution schedule, and a list of target devices.
Task template	<p>A task template (or template) is an XML files that define the configuration changes or software updates that administrators want the devices to perform. HPDM provides a variety of built-in task templates for managing devices.</p> <p>Task templates can be imported or exported by using tools in the HPDM Console. New task templates can be downloaded from the HP FTP site and then imported into your HPDM Server.</p>
Template sequence	A template sequence (or sequence) is a special kind of task template that enables you to connect several templates together and send them out for execution in one task.
Write filter	A write filter provides the ability to write-protect a run-time image. By redirecting all write requests to either a separate disk partition or RAM, a write filter allows the run-time image to maintain the appearance of a writable run-time image. Additionally, a write filter provides the ability to deploy a run-time image onto read-only media, such as a CD-ROM.

Finding the latest updates

To find the latest documentation and software updates:

▲ Go to <ftp://ftp.hp.com/pub/hpdm>.

—or—

Go to <http://www.hp.com/support> and search for HP Device Manager (documentation only).

2 Getting started with HPDM

This chapter discusses the following topics:

- [System requirements](#)
- [Installing HPDM](#)
- [Using the HPDM Console](#)
- [Discovering device systems](#)
- [Displaying device properties](#)
- [Keeping the HPDM Agent updated on device systems](#)

System requirements

The following sections describe the minimum system requirements for HPDM.

HPDM Server requirements

Table 2-1 HPDM Server requirements

Component	Requirements
Operating system	Windows Server 2003 with Service Pack 2 (64-bit) Windows Server 2003 R2 with Service Pack 2 (32- and 64-bit) Windows Server 2008 with Service Pack 2 (32-bit) Windows Server 2008 R2 with Service Pack 1 (64-bit) Windows Server 2012 (64-bit)
Third-party software	Java Runtime Environment version 6 update 45 (bundled with installer) One of the following database management systems (DBMS): <ul style="list-style-type: none">• Microsoft SQL Server 2005 or later• PostgreSQL 8.3 or later (bundled with installer)
Hardware	Pentium® IV or greater 1 GB RAM 2 GB free disk space

HPDM Gateway requirements

Table 2-2 HPDM Gateway requirements

Component	Requirements
Operating system	Windows Server 2003 with Service Pack 2 (64-bit) Windows Server 2003 R2 with Service Pack 2 (32- and 64-bit) Windows Server 2008 with Service Pack 2 (32-bit) Windows Server 2008 R2 with Service Pack 1 (64-bit) Windows Server 2012 (64-bit)
Hardware	Pentium IV or greater 1 GB RAM 2 GB free disk space

HPDM Console requirements

Table 2-3 HPDM Console requirements

Component	Requirements
Operating system	Windows Server 2003 with Service Pack 2 (64-bit)
	Windows Server 2003 R2 with Service Pack 2 (32- and 64-bit)
	Windows Server 2008 with Service Pack 2 (32-bit)
	Windows Server 2008 R2 with Service Pack 1 (64-bit)
	Windows Server 2012 (64-bit)
	Windows XP Professional with Service Pack 3 (32-bit)
	Windows 7 Enterprise with Service Pack 1 (64-bit)
Third-party software	Java Runtime Environment version 6 update 45 (bundled with installer)
Hardware	Pentium IV or greater
	1 GB RAM
	1 GB free disk space

HPDM Agent requirements

HPDM provides full support to all HP thin clients within EOL + 3 years and partial support to all other HP thin clients. See the following table for support coverage.

The following matrix shows the device types and operating systems that are supported in HPDM 4.6. Full support (F) means that all existing and new features in HPDM 4.6 are supported. Partial support (P) means that all existing and new features except settings and connections are supported.

Device type	Win XPe	WES 2009	WES 7E (32-bit)	WES 7P (32-bit)	WES 8 (64-bit)	Win CE 6.0	HP ThinPro 4	HP ThinPro 3	HP Smart Zero Core	Teradici
4320t		F	F							
6360t		F	F							
gt7720		P								
gt7725								P		
mt40			F							
mt41			F							
t310										F
t410									F	
t410 AiO									F	
t505		F	F				F			
t510		F	F			F	F		F	
t5145								P		
t5325								P		
t5335									F	
t5400		F								
t5530						P				
t5540						P				
t5545								P		
t5550						F				
t5565							F	F		
t5565z									F	
t5570		F								
t5570e			F							
t5630	P									
t5730	P									
t5735								P		
t5740	F	F								

Device type	Win XPe	WES 2009	WES 7E (32-bit)	WES 7P (32-bit)	WES 8 (64-bit)	Win CE 6.0	HP ThinPro 4	HP ThinPro 3	HP Smart Zero Core	Teradici
t5740e			F							
t5745							F	F		
t610		F	F	F	F		F		F	
t620			F	F	F		F		F	
t820			F	F	F					
NOTE: Client devices should have a minimum of 10 MB of free disk space.										

Master Repository Controller requirements

Table 2-4 Master Repository Controller requirements

Component	Requirements
Operating system	Windows Server 2003 R2 with Service Pack 2 (64-bit) Windows Server 2008 R2 with Service Pack 1 (64-bit) Windows Server 2012 (64-bit)
Hardware	Pentium III or greater 512 MB RAM 2 GB free disk space NOTE: The above hardware is the minimum required for the Master Repository. If there will be a large number of imaging or file-copying operations, then HP recommends using a more powerful system with more free disk space.
Protocol	FTP, FTPS, SFTP, or SMB
Recommended third-party FTP servers	FileZilla Microsoft Internet Information Server (IIS) 6.0 or later freeSSHd

Network requirements

Table 2-5 Network requirements

Component	Requirements
Network	HPDM supports only IPv4 networks. HPDM can image devices using either PXE or non-PXE (preferred) methods. If PXE imaging is desired, make sure that there are no other PXE services running on the network. If you are using an ISC DHCP server, it must be running at least version 3.0.

Port requirements


If you are using a server behind a firewall, you must add ports 1099 and 40002 to the exception ports in the firewall settings.

A number of other UDP and TCP ports are required for device/server communication. See [Port reference on page 85](#) for a list of standard and custom ports required.

Installing HPDM

To install HPDM:


- ▲ Run the HPDM InstallShield Wizard and follow the on-screen instructions.

 **NOTE:** If a previous version of an HPDM component is already installed on the local computer, the installation program will detect it and attempt to perform an update.


See the installation white paper at <ftp://ftp.hp.com/pub/hpdm/Documentation/WhitePapers/> for more details.

If you choose to do a **Custom Setup** during the installation, the HPDM Configuration Wizard will launch to guide you through some key configuration settings:

- **Language Setting**—Select the desired language for the UI of HPDM.
- **Port Checking**—Use this screen to verify that the system's ports are correctly configured and that the system is capable of supporting HPDM.

 **TIP:** If you are installing the HPDM Server behind a firewall, add ports 1099 and 40002 to the exception ports in the firewall settings.

See [Port reference on page 85](#) for detailed port information.

 **NOTE:** You are not required to stop and restart the installation to address port issues.

- **DHCP Settings for PXE**—Select whether or not the DHCP server is located on the local machine. If the DHCP server is not located locally, you need configure the options on it as indicated in the wizard screen.
- **HPDM Gateway configuration**—On this screen, you should configure the following options:
 - **Server address**—Set the address at which the HPDM Gateway will report to the HPDM Server. Using `localhost` will work when both the HPDM Server and HPDM Gateway are on the same system, but it is better practice to use the actual address.
 - **Local NIC**—Set the NIC through which the HPDM Gateway will receive agent reports. If there is only one NIC for the system, this field can be left blank.
 - **Start PXE service when gateway is started**—You should set this to **Yes** for most situations so that the PXE service starts or stops when the HPDM Gateway starts or stops.


For both a **Complete Setup** and a **Custom Setup**, you will need to specify whether you want to create a new or use an existing HPDM database. Follow the on-screen instructions to complete this process.

If the installation is successful, icons of the HPDM Server and HPDM Gateway will be displayed in the system tray as shown below:

Figure 2-1 HPDM Server and HPDM Gateway—System tray icons



A green icon indicates the service is running, a yellow icon indicates the service is starting up or stopping, and a red icon indicates the service has stopped.

 **NOTE:** You can start or stop services and configure the HPDM Gateway settings again by using the menu options displayed when you right-click on the system tray icons.

An icon for the HPDM Console will be displayed on the desktop.

Installing an HPDM 4.6 Service Pack

An HPDM 4.6 Service Pack can only be installed onto a system that has an HPDM 4.6 base installation or a previous version of an HPDM 4.6 Service Pack. If there is only one component (for example, the HPDM Console) of HPDM installed on a system, then an HPDM 4.6 Service Pack will only update the installed component.

An HPDM Service Pack is cumulative. Each Service Pack includes the latest updates, as well as all of the updates from any earlier Service Packs. For example, with a base HPDM 4.6 installation, you only need to apply SP2 to get both the SP1 and SP2 updates.

To install an HPDM Service Pack:

- ▲ Double-click the setup file and follow the on-screen instructions.

After a successful installation of an HPDM Service Pack, the product name will update in the Programs and Features list in the Control Panel to reflect the new Service Pack version.

Using the HPDM Console

Logging in to the HPDM Console

To launch the HPDM Console:

1. Either double-click the **HPDM Console** icon on the Windows desktop, or from the **Start** menu select **Programs > Hewlett-Packard > HP Device Manager > HP Device Manager Console**.
The **Log in** dialog box will appear.
2. Enter the server address of your network's HPDM Server. The address can be entered as an IP address or as a machine name. If the HPDM Console is on the same machine as the HPDM Server, then enter `localhost`.
3. Enter your **Username** and **Password**, and then click **OK** to log in to the HPDM Console.



NOTE: If the HPDM Console version is different from the HPDM Server version, you will see a warning dialog when the HPDM Console starts.

HPDM Console overview

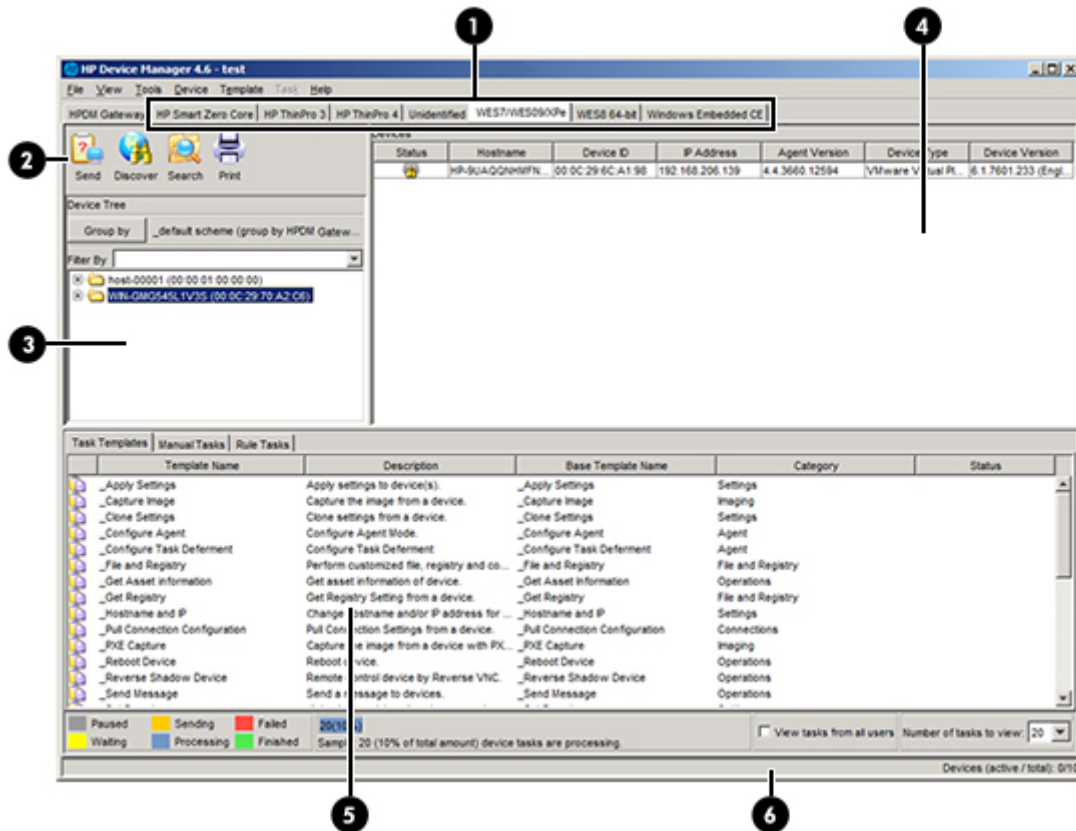
The HPDM Console window consists of three panes and a set of tabs that determines the current view. The exact number of tabs is determined by the number of operating system types that have been identified on the device systems.

There is one tab for each device operating system, one tab for unidentified operating systems, and one tab for the HPDM Gateway view.

Operating system tabs

Each of the operating system tabs produces the following view:

Figure 2-2 HPDM Console—Operating system tabs

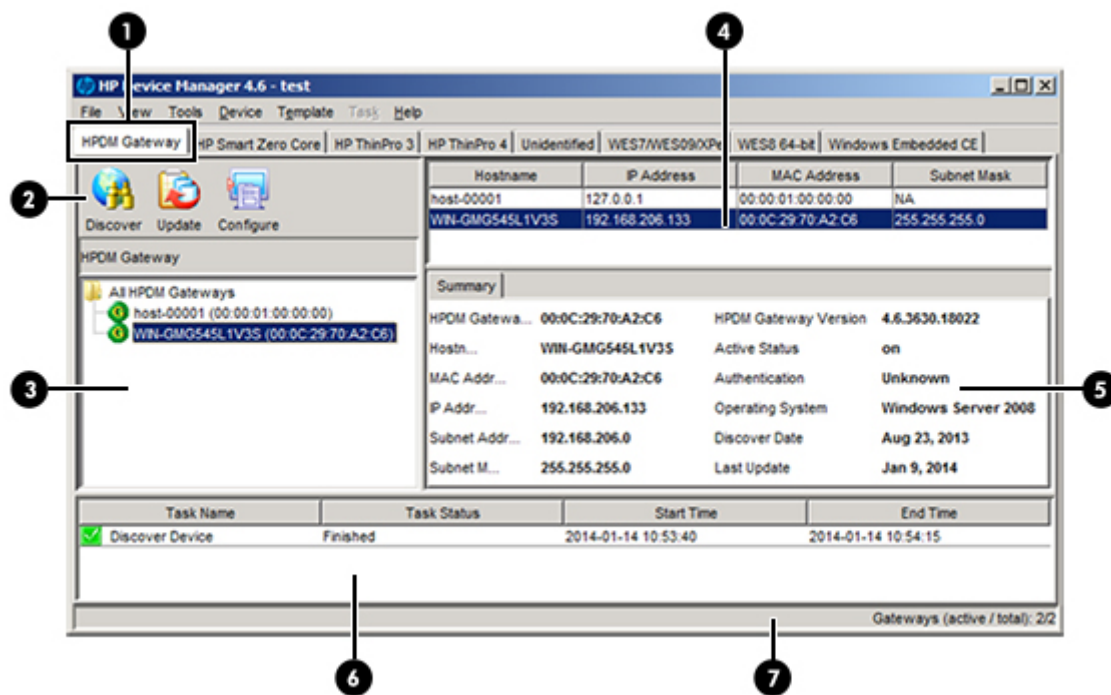


- 1 **Operating system tabs**—These tabs group devices by operating system. Only the tabs for the operating systems currently managed by HPDM will appear.
- 2 **Device toolbar**—Provides quick access to the following functions:
 - Sending tasks
 - Discovering devices or HPDM Gateways
 - Searching for a device
 - Printing device information
- 3 **Device tree**—A hierarchical list of all the devices running the selected operating system, sorted with a custom grouping scheme
- 4 **Device pane**—Displays the devices from the groups (folders) selected in the device tree
- 5 **Task pane**—Contains the following:
 - Task templates that are applicable to the devices listed in the device pane
 - Execution status for manual tasks and rule tasks
- 6 **Status bar**—Shows the total number of active devices, as well as other context-sensitive information

HPDM Gateway tab

Clicking the **HPDM Gateway** tab will display information specific to the currently selected HPDM Gateway.

Figure 2-3 HPDM Console—Gateway tab



- | | |
|---|---|
| 1 | HPDM Gateway tab —Select this tab to manage or find information about HPDM Gateways |
| 2 | Gateway toolbar —Provides quick access to the following functions: <ul style="list-style-type: none">• Discovering devices or HPDM Gateways• Updating an HPDM Gateway• Configuring an HPDM Gateway |
| 3 | Gateway tree —A hierarchical list of all the HPDM Gateways |
| 4 | Gateway pane —Lists the HPDM Gateways |
| 5 | Summary pane —Displays details about the currently selected HPDM Gateway |
| 6 | Task pane —Lists the status of tasks specific to the currently selected HPDM Gateway |
| 7 | Status bar —Shows the total number of active HPDM Gateways |

Discovering device systems

Normally the HPDM Gateway will be able to detect most devices by listening for a network broadcast message made by devices when they start. This solution does require that the HPDM Gateway is running before the device starts up. For more information on this and other methods to add devices to the HPDM asset database, see [Device discovery on page 18](#).

Displaying device properties

HPDM stores asset information about each device it manages. When a device registers with the HPDM Server, it passes just enough basic asset information so that it can be uniquely identified and HPDM can communicate with it. You can both view and export this information.

Basic asset information

To display a device's basic asset information:

- ▲ Double-click a device in the device pane to open the **Device Properties** window.

This window has several pages that contain different categories of asset information. When only basic asset information is available, only the **General**, **Agent**, and **Grouping** pages will have content.

Basic asset information can be used to filter and group your devices. You can define custom grouping information on the Grouping page.

The following tables list the basic asset information available on the General and Agent pages.

Table 2-6 Basic asset information (General)

Item	Description
Device ID	The unique ID that HPDM assigns to the device. The device ID is the first MAC address found on the device.
Hostname	The hostname of the device.
Device Type	The model name of the device.
Device Serial Number	The hardware serial number of the device.
OS Type	The name of the device's operating system.
Device Version	The image version of the device's operating system.
BIOS Version	The BIOS version of the device.
Asset Tag	The asset tag of the device.
Have TPM Module	Indicates whether the device has a Trusted Platform Module (TPM). A TPM is a secure crypto-processor that can store cryptographic keys that protect information and is often called the TPM chip or TPM Security Device. Software can use a TPM to authenticate hardware devices. Currently, some HP thin client models, such as the t610, have a TPM chip built in.
TPM Owned	Indicates whether a TPM is owned. A TPM must be owned before it can be used to secure a computer. The ownership of a TPM is set by assigning a password to it so that only the authorized TPM owner can access and manage the TPM. Only one password exists per TPM, so anyone who knows that password is effectively the TPM owner. Once an owner is set, no other user or software can claim ownership of the TPM.

Table 2-7 Basic asset information (Agent)

Agent Version	The version of the HPDM Agent on the device.
HPDM Gateway ID	The MAC address of the HPDM Gateway that is being used to communicate with the device.
Agent Working Mode	Indicates whether the HPDM Gateway is able to push tasks to the device or if it has to wait for the HPDM Agent to pull tasks from the HPDM Gateway. In some environments, for example where the devices are separated from their HPDM Gateway by a NAT, a device is not addressable by its HPDM Gateway and the HPDM Agent must pull tasks.

Table 2-7 Basic asset information (Agent) (continued)

Agent Pull Interval	Indicates how often the HPDM Agent attempts to pull tasks from the HPDM Gateway.
First Contact Time	The date and time when the device registered with HPDM.
Last Time Online	The date and time of the last time HPDM communicated with the HPDM Agent on the device.

Collecting complete asset information

To collect more information about a device, you must execute a **Get Asset Information** task.

To execute a **Get Asset Information** task:

1. Right-click the device about which you wish to gather information and select **Get Device Asset Information**.
2. Click **OK** when the task creation window appears.
3. Once the task has completed, you can see the extra asset information in the device's **Properties** window.

Displaying complete device asset information

After a successful **Get Asset Information** task, all pages in the Device Properties window will have contents:

- **Software**—Lists software packages installed on the device.
- **Hardware**—Lists CPU, memory, and storage details.
- **Network**—Lists configuration information for each network adapter present on the device.
- **Configuration**—Lists time zone and display settings.
- **Microsoft Hotfix**—Lists Microsoft Hotfix Information (this page is only available when the operating system is WES/XPe).
- **Extended Properties**—Lists the device's extended properties.

Keeping the HPDM Agent updated on device systems

The HPDM Server has built-in rules to automatically update the HPDM Agent on device systems to the latest version.

Each operating system type has a system rule with a startup trigger. When devices start up and report to the HPDM Server, the rule will compare the device's HPDM Agent version to the version in the Master Repository. If the device has an older version, the HPDM Server will send a task to the device to update its HPDM Agent.



NOTE: This rule is disabled by default.

3 Device discovery

Devices must be discovered (added to the HPDM asset database) by HPDM before they can be managed. See the following sections for information on different methods of device discovery:

- [Automatic registration \(normal thin clients\)](#)
- [Automatic registration \(PCoIP zero clients\)](#)
- [Searching for devices](#)
- [Manually registering a device](#)
- [Manually registering multiple devices](#)

Automatic registration (normal thin clients)

When the device is attached to your network, its HPDM Agent will try the following methods to automatically register it with the HPDM Server. The HPDM Agent works through these methods in this order and stops as soon as one is successful.

If the HPDM Agent loses contact with its current HPDM Gateway or the device is rebooted, the automatic registration process restarts and will be run at regular intervals until it is successful.

1. The device will check its own local configuration settings for a preset primary or backup HPDM Gateway to use. These settings can be configured using the following steps:
 - a. Switch to Administrator Mode (see your device operating system documentation for instructions).
 - b. Open the HP Agent applet in the control panel.
 - c. Enter the IP address of the HPDM Gateway in the Current Gateway field.
 - d. Click **OK**.

If the primary HPDM Gateway is set, the HPDM Agent will try to contact it. If that fails and a backup HPDM Gateway is also set, it will then try to contact that. If that also fails, the HPDM Agent will move on to the next method.

2. The HPDM Agent will check the device's DHCP lease file to see if tag 202 is defined. Tag 202 is interpreted as a string representation of the HPDM Server's IP address, followed by a space and then the HPDM Gateway IP address.

For example, if the following value is found associated with tag 202 in the device's DHCP lease file, then the HPDM Agent will attempt to connect to the HPDM Gateway **192.168.1.1**:

```
192.168.1.5 192.168.1.1
```

3. If a DNS server exists on the device's local network, a request is sent to the device to perform a lookup for the DNS name **hpdm-gateway** to identify the HPDM Gateway IP address.
4. The HPDM Agent will send a request to the broadcast address of its subnet. If an HPDM Gateway is present on the subnet, it will reply to the broadcast and the HPDM Agent will connect to it.

Automatic registration (PCoIP zero clients)

Using a DNS service record

HP PCoIP zero clients must have either a static domain name or access to a DHCP server to get the domain name via DHCP option 15 or 12.

If the DHCP server only supports DHCP option 12, the hostname string must contain the domain name.

To create a DNS service record:

1. Open the DNS console, and select the zone containing PCoIP zero clients.
2. Right click to display the menu, and then select **Other New Records** to display the Resource Record Type dialog.
3. Select **Service Location (SRV)** and click the **Create Record** button to display the New Resource Record dialog.
4. Set the Service value to **_pcoip-broker** (recommended) or **_pcoip-tool**. Set the Protocol value to **_tcp**, set the Host offering this service to the fully qualified domain name (FQDN) of the HPDM Gateway, and then click **OK**. Click **Done**.
5. Restart the PCoIP zero clients. They will report to HPDM automatically.

If you want to set one or more backup HPDM Gateways, add other (**_pcoip-broker** or **_pcoip-tool**) service records with different priority values. A lower value means more preferred. Each record points to one HPDM Gateway.

For more information about setting multiple DNS service records for one service, go to http://en.wikipedia.org/wiki/SRV_record.

To troubleshoot this method:

1. Verify the network information, including the IPv4 address and domains, of the PCoIP zero clients.
2. The PCoIP zero clients have an embedded diagnostic tool. Use it to ping the HPDM Gateway address in the DNS service record.

Using a DHCP vendor class option

To create a vendor class:

1. Open the DHCP console, and then select the DHCP server that the PCoIP zero clients are in.
2. Right-click to display the menu, and then select **Define Vendor Classes** to display the DHCP Vendor Classes dialog.
3. Click the **Add** button to display the New Class dialog.
4. Set the Display Name to **PCoIP Endpoint**, set the value to **PCoIP Endpoint**, and then click **OK**.

To set a vendor class option:

1. Right-click the DHCP server to display the menu, and then select **Set Predefined Options** to display the Predefined Options and Values dialog.
2. Set the Option class to **PCoIP Endpoint**, and click **Add** to display the Option Type dialog.

3. Enter **MC Address** in the Name field, set the Data type to **String**, set Code to **1**, and then click **OK**.
4. Set the Value of the MC Address to the IP address of the HPDM Gateway, and then click **OK**.

To enable a vendor class option:

1. Select the **Scope Options** of the Scope that the PColP zero clients are in.
2. Right-click to display the menu, and then select **Configure Options** to display the Scope Options dialog.
3. Select the **Advanced** tab.
4. Set the vendor class to **PCoIP Endpoint**, enable the **MC Address** option, and then click **OK**.
5. Restart the PColP zero clients. They will report to HPDM automatically.

To troubleshoot this method:

1. Verify the network information, including the IPv4 address and domains, of the PColP zero clients.
2. The PColP zero clients have an embedded diagnostic tool. Use it to ping the HPDM Gateway address in the MC Address.

Searching for devices

HPDM can search a range of IP addresses for HPDM Agents and HPDM Gateways. There are two methods: **Walking With IP Range** and **Walking With IP List**. Each of these methods begin in the same manner:

1. In the HPDM Console, click the **HPDM Gateway** tab.
2. Right-click the desired HPDM Gateway and select **Discover Device** in the menu.
3. Select the device type (normal thin client or PColP zero client).
4. Proceed to [Using the Walking With IP Range method on page 20](#) or [Using the Walking With IP List method on page 21](#), depending on the method you wish to use.

Using the Walking With IP Range method

To search using the **Walking With IP Range** method:

1. Select **Walking With IP Range**, and then click **Next**.
2. You can specify the range of IP addresses to search by using either an IP scope or by manually specifying an IP range. An IP scope is a range of IP addresses that you have built and saved for future scans.

To search using an IP scope:

- ▲ Select the **Use Preset IP Scope** checkbox, select an **IP Search Scope**, and then click **OK**.

To search using a manually-specified IP range:

- ▲ Deselect the **Use Preset IP Scope** checkbox, enter a **Starting IP Address** and an **Ending IP Address**, and then click **OK**.

You can check the progress of the discovery by displaying the **HPDM Gateways** tab and selecting the name of the HPDM Gateway. The discovery progress will be displayed in the tasks pane at the bottom of the HPDM Console window.

Configuring an IP scope

To configure an IP scope:

1. In the **Discover by Range** dialog box, select the **Use Preset IP Scope** checkbox, and then select the **Edit** option in the **IP Search Scope** box to display the **Edit IP Walking Scope** dialog box.
2. Select an existing IP scope from the **IP Walking Scopes** list or click **Add** to create a new one.
3. Enter a scope name to be used by HPDM to refer to the new search scope, and then click **OK**.
4. Define the IP address range in which you want HPDM to search for devices by filling in the **Starting IP Address** and **Ending IP Address**. Click **Apply** to save the settings, and then click **OK** to exit.

Using the Walking With IP List method

To search using the **Walking With IP List** method:

1. Select **Walking With IP Range**, and click **Next**.

The **Discover by List** dialog box is displayed.

2. The IP addresses in the **IP List** can be customized according to your specific needs. Refer to the table below for descriptions of each button in the dialog box.

Button	Function
Add	Add a new IP address to the IP list.
Delete	Remove an existing IP address from the list.
Import	Import a *.txt or *.csv file to the IP list.
Export	Export the IP list as a *.txt file.
Copy	Copy the current IP list.
Paste	Paste a copied IP address.

3. Click **OK** to search for HPDM Agents or HPDM Gateways. Once the search has finished, a report will show the devices detected by HPDM. When devices are found, they are added to the HPDM asset database.

Manually registering a device

To manually register a device:


1. In the HPDM Console, click the **HPDM Gateway** tab.
2. Right-click the desired HPDM Gateway and select **Device > Add** from the menu.
3. Enter the device ID, MAC address, and IP address of the device, and then click **OK**.

The manually added device will be added to a tab named **Unidentified**. Once the device reports to HPDM, it will be moved to the tab that matches its operating system.

Manually registering multiple devices

To manually register multiple devices:

1. In the HPDM Console, select **File > Import Devices**.
2. Click **Select**, and then choose a folder that contains text files that describe the devices to import.

 **TIP:** See the white paper *HP Device Manager 4.6 Automated Device Importer* for information on how to configure these files.

3. Click **Import** to register all devices from all text files in that folder.

The manually-added devices will be added to the tab indicated in the files or, if not specified, they will be added to a tab named **Unidentified**. When each device reports to HPDM, it will be moved to the tab that matches its operating system.

4 Using tasks

Task templates

Task templates are displayed in the Task Templates tab of the task pane. The template list consists of six sortable columns:

- **Icon**—Indicates whether the template is a base template, a custom task template, or a favorite custom task template
- **Template Name**—Indicates the name of the template
- **Description**—Shows the description text of the template
- **Base Template Name**—Indicates the base template name of the template
- **Category**—Indicates which category the template belongs to

There are seven categories in HPDM:

- **File and Registry**—A generic template consisting of a customizable combination of tasks for managing device operating systems (see [Managing files and registry settings on page 41](#) for more information)
- **Connections**—Used to get or set the connection settings of a device
- **Agent**—Used to configure HPDM Agent settings and update the HPDM Agent
- **Imaging**—Used to capture or deploy flash-memory images of devices
- **Operations**—Used to perform various operations on a device, such as reboot, shadow, shutdown, and wake up
- **Settings**—Used to change various settings on the device, such as display, network, time, and write filter
- **Template Sequence**—Used to define sequences in which tasks are performed
- **Status**—Indicates the status of each template

The status could be one of the following:

- **Blank (no text)**—Indicates this template is in a normal status and is available for editing and sending tasks.
- **Transferring**—Indicates this template is in a temporary status. The payload required in this template is still transferring. After the transfer finishes, it will change to either a normal or failed status.
- **Failed**—Indicates this template is in an invalid status. There was an error during the transfer of the payload required in this template. You can move the mouse to the text and view details of what kind of error occurred.

Custom task templates, based upon these categories, can be created, edited, deleted, imported, or exported to create specific tasks for devices.

Creating and editing task templates

A set of standard 'blank' task templates belonging to different categories are all listed in the Task Templates tab of the task pane. The names of standard templates begin with the _ (underscore) character, for example: **_File and Registry**.


To create or edit a task template:

1. Double-click an existing template in the **Task Templates** tab of the task pane, or right-click a template then select **Properties** from the pop-up menu.
2. Specify your requirements for the template using the options available. To clear a value of the target device, leave the corresponding field for that value blank on the template.
3. When you have finished defining a new template, click the **Save as** button and enter a name for the new template.
4. Click **OK**. The new template will be created and its name will appear in the **Task Templates** tab of the task pane.

Adding a template to the Favorites

To make it easier to locate templates that are used frequently, you can add them to the **Favorites** as follows:

1. Right-click on the name of the template in the Task Templates tab of the task pane.
2. Select **Add to Favorites** from the pop-up menu.

The icon for the selected template will change to the favorites icon . You can sort the columns by icon to have your favorite templates listed above other templates.

Importing and exporting task templates

You can import or export task templates to share between HPDM systems.

To export task templates:

1. Right-click the template to export and select **Export**.
2. If one or more of the selected templates utilizes payload files, you will be asked if the payload files should also be exported. If you choose to export payload files, the HPDM Console will download them from the Master Repository.
3. Enter the name of the template.
4. Select the destination of the exported file.
5. Click **Export** to export the template(s). Templates with payload files will be exported as ZIP files; otherwise the exported template will be an XML file.

To import task templates:

1. Select **Template > Import > Exported Templates** from menu.
2. Select the XML file, Zip file, or both to import. Only XML files and ZIP files exported from HPDM will be accepted. HPDM 4.4 and 4.5 templates can be imported. Template versions before 4.4 may not be recognized or be compatible.
3. Click **Import**. The file will be added as a new template. Payload files in ZIP format will be uploaded to the Master Repository automatically.



NOTE: Importing task templates since HPDM 4.5 Service Pack 1 have some modifications and limitations:

- a. Importing Update Agent template
 - i. An Update Agent template that is included in a template sequence can be imported. Because payloads belonging to the Update Agent cannot be imported, a dialog box confirming to continue importing the template will appear.
 - ii. Single Update Agent template cannot be imported since HPDM 4.5 Service Pack 1. A confirmation dialog box will appear.
- b. Importing Take TPM Ownership template:
 - i. If no password has been set in the database by Take TPM Ownership, the exported Take TPM Ownership template can be imported.
 - ii. If the Take TPM Ownership password in the database is the same as the exported Take TPM Ownership password, the latter can be imported.
 - iii. If the Take TPM Ownership database password differs from the exported template password, a confirmation dialog box to replace the template password will appear.
- c. If one of the following single templates lacks a payload, a warning dialog box will appear.
 - i. File and Registry containing Copy Files or Deploy Files
 - ii. Apply Easy Tools Configurations
 - iii. Apply Easy Tools Settings
 - iv. PXE Imaging containing Push PXE image to device
 - v. Updating Imaging
 - vi. Deploy Image
 - vii. PXE Deploy
- d. A warning dialog box will appear if deploy files in a sequence template other than Update Agent lacks payload.
- e. For templates exported from HPDM 4.4, it may be necessary to convert the subtasks to new subtasks.
 - i. **Copy Files** in the File and Registry template will convert to **Capture Files** or **Deploy Files** according to its direction.
 - ii. **PXE Image** will convert to **PXE Capture** or **PXE Deploy** according to its actions.
 - iii. **Clone Image** will convert to **Capture Image**.

- iv. **Update Image** will convert to **Deploy Image**.
- v. **Update Agent**, **Apply ET Configurations**, and **Apply ET Settings** will not be converted.
- f. For templates requiring payload, the HPDM Console will perform the following tasks.
 - i. Check for missing required payloads (excluding Update Agent).
 - ii. Convert subtasks to new subtasks when necessary.
 - iii. Guide users to generate a package description file if the new template contains payload.
 - iv. Upload payload to the Master Repository if the new template contains payload.

To generate a template from payload:

1. Select **Template > Import** from the menu, and then select one of the following menu items:
 - **Image Files** (.ibr, .img, .hping, .dd, .dd.gz)
 - **PCoIP firmware** (.all)
 - **Easy Tools Configuration** (.hpcfg)
 - **Easy Tools Settings** (.hpset)
2. Select the file that you want to import.
3. Click **Import**. Then add payload information in the **Package Description Editor** dialog.
4. Click **Generate**. The file will be added as a new template. Payload files will be uploaded to the Master Repository automatically.

To copy an image to another OS:

1. Right-click on a PXE Deploy Image or Deploy Image template in the Task Templates tab of the task pane.
2. Select **Copy to other OS** from the menu.
3. Select the OS type you want to copy the image to and input a name for the new template.
4. Click **OK**. The file will be added as a new template.

Using template sequences

Template sequences are used to combine a set of templates to be executed in a task with a specified order and conditions. A Template Sequence template can contain a maximum of 50 tasks.

A condition is evaluated before the execution of each template of the sequence. This condition controls whether or not the template is executed. The available conditions are:

Table 4-1 Template sequence conditions




Icon	Condition	Description
	anyway	Execute the template regardless of any previous template execution success or failure.

Table 4-1 Template sequence conditions (continued)

Icon	Condition	Description
	success	Execute the template only if the previous template completed successfully.
	failure	Execute the template only if the previous template completed with a failure.

To define a new template sequence:

- ▲ Double-click the standard **_Template Sequence** template to open the Template Editor.

_Template Sequence

HPDM supports two types of template sequences: **Basic** and **Advanced**. A Basic template sequence is a template sequence that uses the same condition between every template that is executed. An Advanced template sequence is a template sequence that allows you to specify a different conditions to control the execution of each template of the sequence.

Basic template sequences

Basic template sequences are defined by clicking the **Content** tab and then clicking **Basic**.

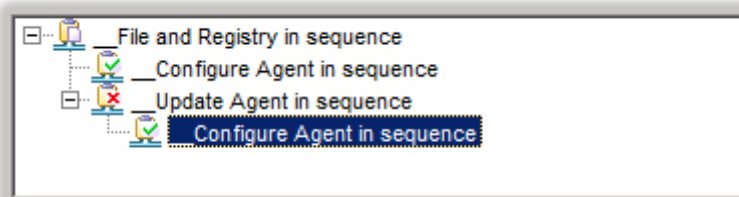
The **Stop sequence on error** checkbox is used to change the template execution condition. If this box is checked, the template sequence will only continue when every template completes with a success status. If the box is clear, every template will be executed in order regardless of previous execution status.

The maximum number of templates in a basic template sequence is 50.

Advanced template sequences

Advanced template sequences are defined by clicking the **Content** tab and then clicking **Advanced**.

Figure 4-1 Template Editor—Template Sequence (Advanced)



This example shows four templates to be executed as follows:

- Unconditionally execute the template **_File and Registry**.
- If the previous template completed successfully, execute the first **_Configure Agent** template and exit the sequence.
- If the initial template fails, execute the **_Update Agent** template.
- If the **_Update Agent** completes successfully, execute the final **_Configure Agent** template and exit.

Each level of templates in an advanced template sequence is called a *dependency level*. An advanced template sequence can have a maximum depth of 50 dependency levels. Each dependency level can have either one **anyway** template or one **success** and one **failure** template.

Tasks

All the tasks that have been sent are monitored and the results are displayed in the task pane. The task pane lists all the tasks that have been sent to devices.

The task list consists of the following columns:

- **Task Name**—Indicates the name of task template used to send this task.
- **Progress and Status**—Indicates the progress and status of the task.
- **Target Device Number**—Indicates the number of devices to which the task was assigned.
- **Create Time**—Indicates when the task was created.
- **Sender**—Indicates the sender of the task. You must have the User Management privilege to see this column.

Performing a task

In order to perform a task on a remote device you must first define a template which provides the instructions to be executed or new settings, then apply that template to the device.

1. To define a template, double-click an existing template in the **Task Templates** tab of the task pane, or right-click a template then select **Properties** from the pop-up menu.
2. Specify your requirements for the template using the options available, then click the **Save as** button and enter a name for the new template.
3. To apply the template to a device or group of devices, either drag the template from the **Task Templates** tab of the task pane and drop it on to the device or group.

—or—

Right-click devices in the device pane or folders in the device tree and select **Send Task** from the pop-up menu to display the **Template Chooser**. Select a category then a template from the templates list, then click **Next**.

4. The **Task Editor** dialog box will appear. Select the **Schedule & Batch Control** tab and specify when and how the task defined in the template is to be performed. If you do not select the **Schedule Task** option and specify a time, the task will be applied to the device as soon as you click the **OK** button.
5. Click **OK** to apply the task to the device.

Task status icons

The meaning of the icons displayed in the **Device Task View** are as follows:

Table 4-2 Task status icons









	Success The task was executed successfully by the device.
	Sending

Table 4-2 Task status icons (continued)

	The task is being sending from HPDM Server through HPDM Gateway to the device and is waiting for a reply.
	Failed / Timeout The task has failed or timed out. (If the task is not complete after finite time, the status of the task will be displayed as Timeout . The error code of the status is 0 .)
	Ready The task is executed and waiting for the user's operation.
	Paused The task has been paused.
	Cancelled The task has been cancelled.
	Waiting The task has been scheduled for sending at a later time, and has not been sent yet.
	Processing The task has been accepted by the device and is being processed.

Task parameters

In HPDM, a task is a combination of a template, an execution schedule, and a list of target devices. The HPDM Console lists tasks in two groups: **Manual Tasks** and **Rule Tasks**. Manual tasks are created directly with the HPDM Console and rule tasks are created indirectly using rules.

You can set task parameters by selecting **Tools > Configuration** from the HPDM Console's menu bar to display the **Configuration Management** dialog box, then expanding the **Task Parameters** item in the left-hand tree pane.

The **Task Parameters** item consists of two sub-items: **Valid Time and Timeout** and **Write Filter, WOL and Task Deferment**. These are described in the following sections.

Manual tasks

Every time you apply a template to a set of devices the Task Editor appears and you create a task. The Task Editor includes the **Contents** tab of the Template Editor. It also contains three additional tabs: **Valid Time, Timeout & WOL**, **Target Device List**, and **Schedule & Batch Control**.

Valid Time, Timeout & WOL

On the **Valid Time, Timeout & WOL** tab of the Task Editor, you can set the **Use Valid Sending Time** to specify an expiration time for task. If the task has not already begun by the specified time, it will not be started.

Exclude Working Hours allows you to delay a task until a time outside of the specified working hours for the target devices.

If a task keeps processing longer than the **Execution Timeout**, it will enter a timeout status and the HPDM Server will try to determine if the task is dead on the target device.

The **WOL before task** option makes it possible to wake up a target device before sending a task to it.

Target Device List

The **Target Device List** tab lists the devices the task will be applied to. You may also add or remove devices to the list using the buttons provided.

Schedule & Batch Control

The **Schedule & Batch Control** tab contains the following sections.

- **Schedule**—This section enables you to specify a date and time for the task to execute.
- **Batch Control**—This section enables you to specify a batch size. This is used when a task is sent to a large number of devices. The batch settings controls how many devices are sent the task at a time thereby giving you some control over the amount of network traffic HPDM generates.
- **Write Filter Policy Setting**—This section enables you to specify how HPDM handles the write filter on devices that have a Windows Embedded operating system.
- **Task Deferment**—This section enables the end user at the target device to defer a reboot or shutdown so that they can finish their work safely. See [Task deferment on page 30](#) for more information

Task deferment

This feature on the device side provides a chance to save work before a reboot/shutdown of the device. When the HPDM Agent needs to reboot/shutdown the device normally, it displays either the **Reboot Required** or the **Shutdown Required** dialog box.

- Users can set the postpone time by dragging the slider and clicking the **Postpone** button to postpone a reboot/shutdown. Users can postpone a reboot or shutdown a maximum of 3 times.
- Users can click **Reboot now** or **Shutdown now** if postponement is not necessary.
- Users can customize the reboot/shutdown title and message info via the **_Configure TaskDeferment** task from the HPDM Console. The maximum length of message info is 255 characters.
- The maximum reminder time is 10 minutes, and the default is 1 minute.
- The maximum postpone time is 8 hours, and the default is 4 hours.

When the HPDM Agent needs to forcibly reboot the device, the task deferment window is not displayed.

Displaying task properties

To display the properties of a task: right-click a task and select **View Task Contents** in the context menu. A **Task Contents** window will be displayed showing detailed information about the assigned task.

Configuring task parameters

Select **Tools > Configuration** from the HPDM Console's menu bar to open the **Configuration Management** dialog box, then click the **Task Parameters** option in the option tree pane to expand it.

The **Task Parameters** option consists of two sub-options: **Valid Time and Timeout** and **Write Filter Policy Setting**. These are described in the following sections.

Valid Time and Timeout

The **Valid Time and Timeout** options enable you to set the duration HPDM will wait for the execution of tasks. You can also specify the start and end time of working hours during which HPDM will not execute tasks. Clicking in an option field will cause the **Description** box to display a short description of that option.

1. Select **Valid Time and Timeout** in the option tree pane of the **Configuration Management** dialog box.
2. Set the time, in minutes, for each category: **Valid Time**, **General Timeout**, **General Batch Interval**, **PXE Batch Interval** and **FTP Batch Interval**.

Set the amount, in devices, for each category: **General Batch Amount**, **PXE, Batch Amount** and **FTP Batch Amount**.

Check the **Exclude Working Hours** option box to input the start and end time of working hours.

Clicking **Restore defaults** will reset the timeout settings to their defaults and set the working hours to **9:00** start and **17:00** end.

3. Click **Apply** to save the new settings.
4. Click **OK** to exit.

Write Filter and WOL

The **Write Filter and WOL** options enable you to specify how the Enhanced Write Filter on XPe devices affects tasks.


1. Select **Write Filter and WOL** in the option tree pane of the **Configuration Management** dialog box.
2. Choose one of the three policy items.
3. Click **Apply** to save the new settings.
4. Click **OK** to exit.

Pausing tasks

To pause a waiting task:

1. Select a waiting task in the task pane.
2. Right-click and select **Pause** from the pop-up menu.

The status of the waiting task will be changed to **Paused**.


 **NOTE:** This operation only is available for waiting tasks.

Continuing tasks

To continue a paused task:

1. Select a paused task in the task pane.
2. Right-click and select **Continue** from the pop-up menu.

The status of the paused task will be changed to **Waiting**.

 **NOTE:** Only paused tasks (tasks that have not been sent) can be continued.


Resending tasks

If a task has finished, you can resend the task to the device.

1. Select the finished task in the task pane.
2. Right-click and select **Resend** from the pop-up menu.


Canceling tasks

To cancel a selected ongoing task, right-click the task and select **Cancel** from the pop-up menu. The system will try to notify the device to cancel the task, and the status of the paused task will be changed to Canceled.

 **NOTE:** Only ongoing tasks (tasks in the Sending or Processing state) can be canceled. Not all tasks can be canceled on the device side. The task might be finished before the system delivers the cancel request. The status of tasks will be updated by following reports if they are not successfully canceled.

Deleting tasks


To delete a selected task, right-click the task and select **Delete** from the pop-up menu.

 **WARNING!** Deleting a task that is in progress may damage the OS image! For example, updating and upgrading tasks, image deployment tasks, and so on.

Displaying task logs

To display the log of a task:

1. Right-click a task in the task pane and select **View device tasks and logs** from the context menu, or double-click a task in the task pane. A **Device Task View** window will appear.
2. Select the target device and click the toggle button below to show/hide task log for selected device. Double-clicking device in the Device Task View has the same effect as clicking the toggle button.

 **NOTE:** To refresh the task log of the selected device task, press F5.

3. Click **Close** to close the log viewer when you have finished.
4. Click **OK**.

Displaying a task's success rate

To display a task's success rate:

- ▲ Right-click a task in the task pane and select either **Success Rate > by Gateway** or **Success Rate > by Subnet**, depending on how you want the information displayed.

Opening VNC Viewer for shadowing

You can open a VNC Viewer for shadowing a device by right-clicking a ready or finished shadowing task and selecting **Open VNC Viewer for Shadowing** from the pop-up menu.

Opening a Result Template

Right-click a ready task and select **Open Results Template** from the menu to open the results of some tasks such as **Get Registry**, **Pull Connection Configuration**, **Capture**, and so on.

Viewing tasks from all users

If you have the User Management privilege, you can select the **View tasks from all users** checkbox in the bottom-right of the task pane to view all tasks sent by all users. You can also resend, pause, continue, cancel, and delete any task sent by any user.

Task rules

In HPDM *rules* enable you to automate the execution of tasks, and you can execute the rules in order. Each rule has three parts: a filter to define to which devices the rule applies, a trigger that defines when the rule is executed, and a template which defines what operation the rules should perform on to the devices.

Rules are defined in the **Rules Management** window which you can access from the **Tools** menu.



NOTE: Only **First Contact** rules and **Startup** rules can be ordered.

Adding a new rule

1. Click the **Add ...** button to open the **Rule Editor** window.
2. Each rule must be given a unique name.
3. Each rule must also have a filter defined. Click on the **Choose ...** button to the right of the filter to open the **Filter Chooser** window.
4. You can then select a pre-existing filter or create a new one by clicking **Add**
5. Once the name and filter are set you can select your trigger. There are three options:
 - **First Contact**—The rule will execute for each device that match its filter criteria once when the device first registers itself with the HPDM Server, or after completing a Factory Reset task.
 - **Startup**—The rule will execute for each device that match its filter criteria every time the device restarts.
 - **Scheduled**—This option expands the 'Rule Editor' window to enable you to specify a time and date for when the rule is executed and also the frequency at which it is repeated.
6. Specify the template to use.



NOTE: Templates containing actions of capturing images or files are not applicable in a task rule.

7. Click **OK** to create the rule.
8. The new rule will be enabled by default. You can disable it by unchecking its check box in the **Rules Management** window.

5 Device management

- [Viewing devices](#)
- [Deleting devices](#)
- [Grouping devices](#)
- [Checking network connection status](#)
- [Printing information about devices](#)
- [Shadowing devices](#)
- [Power management](#)
- [Managing normal thin clients](#)
- [Managing PCoIP zero clients](#)


Viewing devices

To view the currently managed devices in the device pane:

- ▲ Select a folder in the device tree.

To see a menu of applicable commands:

- ▲ Select a folder in the device tree or one or more devices in the device pane, and then right-click.

 **TIP:** All of these commands are also available in the **Device** menu of the HPDM Console.

An HPDM Agent can function in two different modes:

- Pull mode—The HPDM Agent requests (pulls) tasks from the HPDM Gateway at regular intervals.
- Push mode—The HPDM Gateway sends (pushes) tasks to the HPDM Agent as soon as they are received from the HPDM Server.

In the device pane of the HPDM Console, devices are represented by the following icons:



Represents a number of devices that have been grouped together



Indicates that the status of this device cannot be confirmed because an HPDM Gateway managing this device is currently down or disconnected



Indicates the device is currently turned off



Indicates the device is currently in pull mode



Indicates the device is currently in pull-lock mode (the write filter is on)



Indicates the device is currently in push mode



Indicates the device is currently in push-lock mode (the write filter is on)

The following icons are used in the **HPDM Gateway** tab of the HPDM Console:



Represents an HPDM Gateway that is currently active



Represents an HPDM Gateway that is currently down or disconnected

Deleting devices

To delete a device from the device tree:

1. Right-click the folder in the device tree.
2. Select **Delete** from the menu.

All devices under this folder are removed from the device tree.

To delete a device from the device pane:

1. Right-click the device in the device pane.
2. Select **Delete** from the menu.

The selected device is removed from the device pane.

Grouping devices

HPDM enables you to manage your devices both individually and in groups. You can group your devices in two ways:

- Manually (using your own grouping definitions)
- Dynamically (using the device asset information)

In addition, you can use the device asset information to filter the devices. This enables you to divide your devices into sets and then assign those sets to specific administrators.

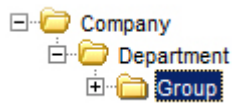
Setting group information using a DHCP tag

You can specify the grouping information a new device will use by setting DHCP tag 203.

Tag 203 enables you to set up to six grouping parameters that can then be used as part of a dynamic grouping scheme. They are labelled *P1-P6*. You can specify any of the six in any order. In addition to this, you can include a special parameter labelled *MG* and set it to a path to use for manual grouping. This path is used to create a subtree in the HPDM Console's device tree when manual grouping is selected.

For example, if the path is set to Company/Department/Group the device tree will show:

Figure 5-1 Setting group information using a DHCP tag



The format that is used by HPDM for tag 203 is as follows. All the parameters are optional but those specified must be assigned a value:

```
P1="valor";P2="valor";P3="valor";P4="valor";P5="valor";P6="valor";MG="valor"
```

For example:

```
P1="Asia";P2="China";P3="Shanghai";MG="Empresa/Departamento/Grupo"
```

Switch to Manual Grouping

1. Click the **Group by** button.
2. Select **Manual Group > _global (system)**.
3. Any **Manual Groups** specified with the DHCP tag will appear automatically.

Adding a new Manual Group

1. Right-click in the device tree panel and select **Manual Group > Add Folder**
2. Enter a name for the new folder.
3. Click **OK**

Devices can be dragged and dropped between manual groups. Manual groups may also be renamed or deleted.

Dynamic Grouping

HPDM enables you to create one or more *dynamic grouping* schemes. Each scheme will create a tree structure based on the criteria selected.

Creating a new Dynamic Grouping scheme

1. Click the **Group by** button.
2. Click **Edit Scheme** and be sure the **Dynamic Scheme** tab is selected.
3. Click **Add** and give the new scheme a name. Click **OK** to accept the new name.
4. Select and order the criteria you want to define in the scheme. **Extension Properties 1-6** correspond to the P1-P6 grouping items you can set with the DHCP tag 203.
5. Click **OK** to exit the **Edit Grouping Scheme** window.

Switching to a Dynamic Group

1. Click the **Group by** button.
2. Select **Dynamic Group**.
3. Select the scheme you wish to use.

Filtering devices

Filtering enables you to work with a subset of your devices. It can be combined with User Privileges to divide the management of your devices between different administrators.

Creating a new Device Filter

1. Select **View** on the main menu then **Device Filter ...**
2. Click **Add** in the **Device Filter Management** window.
3. Give your new filter a name. Click **OK** to accept the name.
4. Click **Add...** in the **Edit Device Filter** dialog box to open the **Choose Criteria Key** dialog box.
5. In the **Choose Criteria Key List** dialog box, select the criteria according to your needs. Click **OK** to open the **Criterion Editor** dialog box for the chosen criterion.
6. Define the operator and value for the new criterion.
7. Repeat steps 4 through 6 to load more criteria. Then click **Save** and **Close**.
8. Select the new filter from the **Filter** drop down list.

Filter can be used as a security filter to limit the access of specified user or group. A filter defines to which devices a rule applies. When you are sending a task, you can use filter to select target devices. Your device tree view can be refined using filter.



NOTE: Device Filter supports adding multiple criteria with the same name.

Editing a Device Filter

To edit a Device Filter:

1. Select **Device Filter** from the **View** menu.
2. Double-click an existing filter or choose an existing filter and then click **Edit...** to open the **Edit Device Filter** dialog box.
3. Click **Add...** in the **Edit Device Filter** dialog box to open the **Choose Criteria Key** dialog box.
4. In the **Candidate Criteria Key List**, select the criteria according to your needs. Click **OK** to open the **Criterion Editor** dialog box for the chosen criterion.
5. Click the arrow button in the **Edit Criteria** section to select conditions in the drop-down menus. For example: **OS Type = HP ThinPro**.
6. If multiple filters exist in the **Criteria List**, you can select **Satisfy all criteria** or **Satisfy any criteria**. Then click **Save** to return to the **Device Filter Management** dialog box.
7. In the **Device Filter Management** dialog box you can edit or remove the selected filter according to your requirements.
8. Click the **Generate Device List** button to create the filtered device list.

Now the administrator can use the device filters to manage the devices in the network.

Filter Security

You can limit the devices a user can see by assigning a filter to that user as his security filter. The procedure is as follows:

1. Display the **Tools** menu and select **User Management**.
2. Select the name of the user on the **Users** tab, then click **Edit**.
3. Display the **Filter** tab.
4. Select the filter to use in the **Security Filter** drop-down list.

When you log on as that user, you will see that only the devices allowed by the selected filter are displayed.

Checking network connection status

You can check the network connection status of a device (i.e. whether it is connected to the network or not).

1. In the device pane, select one or more devices, right-click and select **Check Connection Status** from the context menu.
2. Select the utility you want to use to check the connection status of the device. You can choose from:
 - **Ping**—A basic Internet program that lets you verify that a particular Internet address exists and can accept requests. Pinging is diagnostically used to make sure that a host computer, which you are trying to reach, actually operates.
 - **Trace Route**—This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer.

A window displaying the network connection status of the device will appear.

3. Click **Close**.

Printing information about devices


Printing device information

To print information about any devices listed in the HPDM Console:

1. In the device pane, select the devices you want to print (**Ctrl**-click and/or **Shift**-click them).
2. Click the **Print** icon in the toolbar to display the **Print Device** window. Information about all the selected devices is displayed in the window.
3. Either click **Export** to export the list to a *.csv file. Enter a name and click **Save**.
—or—
Click **Print Preview** to print the device report. The **Print Preview** window opens.
4. If you are satisfied with the preview, click the printer icon or display the **File** menu and select **Print**. Click **OK** if you accept the printing settings.

Shadowing devices

Shadowing enables you to connect to a remote device by SSL tunnel and view and control that device from the HPDM Console. This can be achieved either by using the **_Shadow Device** template available in the **Task Templates** tab of the task pane, or by selecting from the pop-up menu when you right-click on a device as described below.

 **NOTE:** Update the HPDM Agent to the latest version before shadowing a device. Send an **Apply Settings** task to enable the VNC Server.

To shadow a device:

1. Select a group of devices in the device pane or a device in the device tree.
2. Right-click and select **Shadow** from the pop-up menu. The **Task Editor** dialog box will appear.
3. Click **OK**. When the Shadow processing task is complete, the remote desktop of the terminal will be displayed in a separate window.

To Open VNC Viewer for Shadowing:

1. Select a completed **Shadow Device** task in the task pane.
2. Right-click and select **Open VNC Viewer for Shadowing**, or display the **Task** menu and select **Open VNC Viewer for Shadowing**.

The remote desktop of the device will be displayed in a separate window ready for your operations.

Power management

The HPDM Console enables you to reboot, shutdown, and wake a device remotely. This can be achieved either by using the templates available in the Task Templates tab of the task pane, or by selecting from the pop-up menu when you right-click on a device as described below.

 **NOTE:** To wake a device, the Wake On LAN support of the device's BIOS must be enabled.

To shutdown, reboot, or wake a device:

1. Right-click a device in the device pane and select **Power Management > Reboot, Wake On LAN** or **Shutdown** from the context menu.
2. The **Task Editor** dialog box will appear. Click **OK** to perform the task.

When the device receives the task, a warning dialog box will appear on its screen to inform the user that the device will be shut down or restarted.

Managing normal thin clients

Changing a device's hostname

To change a device's hostname:

1. Right-click the desired device in the HPDM Console and select **Rename**.
2. Edit the hostname value and click **OK** to automatically initiate a task.
3. Adjust the task settings as needed in the Task Editor (e.g. Write Filter Policy Setting).
4. Click **OK**.

Capturing and deploying connections

To capture connections:

1. Double-click the **_Pull Connection Configuration** template to open the Template Editor.
2. Use the check boxes to indicate which connection settings to capture.
3. In the **Save result as template** field, enter a name for the result template that will be created to store the captured connections.
4. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
5. Drag and drop the template onto the desired device.
6. Click **OK** to apply the task to the device.

The connections will be captured and stored in a new template with the name you specified in the **Save result as template** field.

To deploy captured connections:

- ▲ Drag and drop the result template of a **_Pull Connection Configuration** task onto the desired devices.

Cloning and deploying settings

To clone settings:

1. Double-click the **_Clone Settings** template to open the Template Editor.
2. Use the check boxes to indicate which settings to clone.
3. In the **Save result as template** field, enter a name for the result template that will be created to store the cloned settings.
4. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
5. Drag and drop the template onto the desired device.
6. Click **OK** to apply the task to the device.

The settings will be cloned and stored in a new template with the name you specified in the **Save result as template** field.


To deploy cloned settings:


- ▲ Drag and drop the result template of a **_Clone Settings** task onto the desired devices.


Applying custom settings


To apply custom settings:

1. Double-click the **_Apply Settings** template to open the Template Editor.
2. Click the **Edit** button.
3. Use the check boxes to indicate which settings to edit.
4. Configure individual settings as desired.

 **NOTE:** The settings available to configure may vary by operating system type and version.

 **NOTE:** When configuring Time Settings, the values available for WES 2009 and XPe devices are unified with those available for WES 7 devices. There are 97 values in all. Some may not be supported by WES 2009 or XPe devices. Also, not all values on WES 2009 and XPe are supported by HPDM templates and tasks.

 **NOTE:** Firefox Browser Settings are only available for HP ThinPro 4.1 and earlier versions.

 **NOTE:** Printer Settings are only available with HP ThinPro. Only configure printer settings after cloning.

The “Address” column and “Port” column can be edited under these circumstances:

- When the **Type** value is **Network**, **Address** and **Port** can be edited.
 - When the **Type** value is **LPT** or **COM**, **Port** can be edited.
 - When the **Type** value is **USB**, nothing can be edited.
-
5. Once the settings are configured, navigate to the **Summary** page. This lists all settings that will be changed by this template.
 6. If the changes are correct, click **Finish** to go back to the Template Editor.
 7. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane
 8. Drag and drop the template onto the desired devices.
 9. Click **OK** to apply the task to the devices.

Managing files and registry settings

The **_File and Registry** template consists of a customizable combination of subtasks for managing files and registry settings on devices.

The following subtasks are available:

- **Capture Files**—See [Capturing files on page 42](#).
- **Deploy Files**—See [Deploying files on page 42](#).
- **Delete Files**—See [Deleting files on page 43](#).
- **Registry**—See [Managing device registry settings on page 43](#).
- **Command**—See [Remotely executing commands on page 44](#).
- **Pause**—See [Pausing a _File and Registry task on page 45](#).
- **Program Record**—See [Adding or removing program records on page 45](#).
- **Script**—See [Running a script on page 46](#).

To customize a **_File and Registry** template:

1. Double-click the **_File and Registry** template to open the Template Editor.
2. **Add**, **Edit**, **Delete**, and rearrange subtasks **Up** and **Down** as necessary.
3. Click **Save as** to name and save the template for later use.

You can also merge two or more **_File and Registry** templates to combine the subtasks from them into one template.

To merge **_File and Registry** templates:

1. Right-click on a **_File and Registry** template, and select **Merge**.
2. Click another **_File and Registry** template, and then click **OK**.
3. Enter a name for the merged template when prompted.

Capturing files


To capture files from devices and save them to the Master Repository:

1. Double-click the **_File and Registry** template to open the Template Editor.
2. Click **Add**, select the **Capture Files** subtask, and then click **OK**.
3. In the Capture Files Editor, specify the path of the file or folder to transfer. Additional lines can be added by clicking **Add**.

The wildcards * and ? are supported in the lowest level of the path or filename. See the following examples.

a*	Specifies all files that start with the letter “a” and are followed by any number of characters.
a?	Specifies all files that start with the letter “a” and are followed by only one other character.
*a	Specifies all files that end with the letter “a” and are preceded by any number of characters.
?a	Specifies all files that end with the letter “a” and are preceded by only one other character.

4. Specify the target path where you want to store the captured files in the Master Repository.

 **TIP:** The target path field accepts parameters that send files captured from different devices (during a single task) to different folders.

5. Select the **Overwrite if exists** option if desired.
6. Click **OK** when you are finished specifying files.
7. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
8. Drag and drop the template onto the desired devices.
9. Click **OK** to apply the task to the devices.

Deploying files

To deploy files to devices:

1. Double-click the **_File and Registry** template to open the Template Editor.
2. Click **Add**, select the **Deploy Files** subtask, and then click **OK**.
3. Add files to transfer by clicking **Add from local** or **Choose upload**.
4. Click **OK** when you are finished specifying files.
5. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
6. Drag and drop the template onto the desired devices.
7. Click **OK** to apply the task to the devices.

Deleting files

To delete files from devices:

1. Double-click the **_File and Registry** template to open the Template Editor.
2. Click **Add**, select the **Delete Files** subtask, and then click **OK**.
3. Add files or folders to delete. Each line has the following options:
 - **File or Folder Name**—Enter the file or folder name to delete. The wildcards * and ? are also supported.
 - **Path On Device**—Enter the path on the device where the file or folder is located.
 - **Delete Recursively**—Set this option to **Yes** if you want to delete all files or folders that match the pattern entered in **File or Folder Name** in all subdirectories under the **Path On Device**. If set to **No**, subdirectories will not be affected.
4. Click **OK** when you are finished specifying files.
5. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
6. Drag and drop the template onto the desired devices.
7. Click **OK** to apply the task to the devices.

Managing device registry settings

You can manage device registry settings in the following ways:


- [Cloning registry settings on page 43](#)
- [Adding, editing, and deleting registry settings on page 44](#)

Cloning registry settings

To clone registry settings from a device:

1. Double-click the **_Get Registry** template to open the Template Editor.
2. Click **Add**, enter the name of the registry node from which you want to clone settings (such as `desktop` for desktop settings), and then click **OK**. The node will appear on the **Registry** tab of the Template Editor.
3. In the **Save result as template** field, enter a name for the result template that will be created to store the cloned registry settings.
4. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
5. Drag and drop the template onto the desired device.
6. Click **OK** to apply the task to the device.

The registry settings will be cloned and stored in a new template with the name you specified in the **Save result as template** field.

 **TIP:** You can view the cloned registry settings by double-clicking the new template, double-clicking the **Registry** subtask, and then expanding the registry node in the **Registry Tree**.

Adding, editing, and deleting registry settings

To add, edit, or delete registry settings:

1. If you want to use a previously generated result template from a **_Get Registry** task, double-click that template, and then double-click the **Registry** subtask.

If you want to create a new template, double-click the **_File and Registry** template to open the Template Editor, and then click **Add**. Select the **Registry** subtask, and then click **OK**.
2. Configure the registry settings in the editor as necessary using the following methods:
 - Use the **Registry Tree** to navigate the registry node and add, rename, or delete registry keys and values.
 - Use the **Registry Settings** pane to add or delete values from the selected registry key.
 - Use the **Action to Perform** pane to add or delete a registry key. If you have modified the key's values individually in the Registry Settings pane, the options in this pane will be greyed out.
 - Click **Import Registry File** to import registry settings.
3. Click **OK** when you are finished editing registry settings.
4. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
5. Drag and drop the template onto the desired devices.
6. Click **OK** to apply the task to the devices.

Remotely executing commands

You can remotely execute commands on a device using the **_File and Registry** template. In this context, a command is anything executable in the device's operating system. This includes the following:

- Applications
- DOS batch files
- Windows scripts



IMPORTANT: You can enter any command; however, HP recommends that these commands be tested on a device first.

To remotely execute commands on a device:

1. Double-click the **_File and Registry** template to open the Template Editor.
2. Click **Add**, select the **Command** subtask, and then click **OK**.
3. In the editor, enter the command in the **Command** column.



TIP: The Windows environmental variable **PATH** might be different on each device, so it is important to enter the full path for each command to make sure it can be found on the device. For example, to execute `xxx.exe` in the directory `C:\Program Files`, enter the command as `C:\Program Files\xxx.exe`.

4. In the **Execute After Reboot** column, select **Yes** if the device should reboot before the command is executed.

5. In the **Wait** column, select **Yes** if the command has to wait for the previous command to finish before executing.
6. If you want to add more commands, click **Add**.
7. Click **OK** when you are finished editing registry settings.
8. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
9. Drag and drop the template onto the desired devices.
10. Click **OK** to apply the task to the devices.

Remotely executing Windows scripts

Windows Script Host is a comprehensive scripting infrastructure that provides the scripting engines Microsoft Visual Basic Scripting Edition and Microsoft Jscript. These engines can be embedded into Windows applications to make it easier to script Windows applications.

For more information on how to write Windows scripts, go to <http://www.msdn.microsoft.com> and search for `windows script`.

To run Windows scripts as a command using HPDM:

- ▲ Add `wscript` before the script name you want to run.



NOTE: `wscript.exe` is located in `C:\Windows\system32`.

Pausing a _File and Registry task

You can pause a **_File and Registry** task to wait for certain events such as a system reboot.

To add a **Pause** subtask to a **_File and Registry** task:

1. In the Template Editor of a **_File and Registry** template, click **Add**, select the **Pause** subtask, and then click **OK**.
2. Specify the pause duration, and then click **OK**.

Adding or removing program records

To add or remove program records:

1. Double-click the **_File and Registry** template to open the Template Editor.
2. Click **Add**, select the **Program Record** subtask, and then click **OK**.
3. In the Program Record Editor, click **Add**.
4. Specify the action type (add or remove).
5. Input the publisher, version, and comments if necessary.
6. Click **OK** when you are finished editing program records.
7. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
8. Drag and drop the template onto the desired devices.
9. Click **OK** to apply the task to the devices.

Running a script

To run a script on a device:

1. Double-click the **_File and Registry** template to open the Template Editor.
2. Click **Add**, select the **Script** subtask, and then click **OK**.
3. In the editor, enter the script content.



IMPORTANT: HPDM supports only batch script on Windows and only shell script on Linux.

4. For Windows platforms only, specify the path to start the script in if necessary.
5. For Windows platforms only, specify the user account to run the script for if necessary.
6. Click **OK** when you are finished editing the script.
7. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
8. Drag and drop the template onto the desired devices.
9. Click **OK** to apply the task to the devices.

Enrolling certificates with SCEP

To enroll certificates with SCEP:

1. Double-click the **_Enroll Certificate with SCEP** template to open the Template Editor.
2. Enter the URL for enrollment and the challenge password.
3. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
4. Drag and drop the template onto the desired device.
5. Click **OK** to apply the task to the device.

Managing PCoIP zero clients

Capturing connections

To capture connections from a PCoIP zero client:

1. Double-click the **_Capture Connections** template to open the Template Editor.
2. In the **Save result as template** field, enter a name for the result template that will be created to store the captured connections.
3. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
4. Drag and drop the template onto the desired device.
5. Click **OK** to apply the task to the device.

The connections will be cloned and stored in a new template that with the name you specified in the **Save result as template** field.

Deploying connections

To deploy connections to PCoIP zero clients:

1. Double-click the **_Deploy Connections** template or the result template of a **_Capture Connections** task to open the Template Editor.
2. If necessary, select the connection type and set the values.
3. Click **Save as**, enter a name for the new template, and then click **OK**. The template is added to the **Task Templates** tab of the task pane.
4. Drag and drop the template onto the desired devices.
5. Click **OK** to apply the task to the devices.

Updating firmware

To update firmware on PCoIP zero clients:

1. Select **Template > Import > PCoIP firmware** from the HPDM Console menu.
2. Click **Browse** to choose a firmware file (.all), and then click **Import**.
3. Click **Generate**, and then wait until the template is created successfully. The template is added to the **Task Templates** tab of the task pane.
4. Drag and drop the template onto the desired devices.
5. Click **OK** to apply the task to the devices.

6 Imaging operations

HPDM can be used to capture an image from a device and deploy it to any number of similar devices. An image is a binary file containing all the data from a device's flash storage.



IMPORTANT: HPDM will not deploy images to devices that are not licensed for the operating system contained in the image.



TIP: There is no license check for HP ThinPro or HP Smart Zero Core, so those operating systems can be interchanged as long as there is enough disk space.

For information about imaging support on different operating systems, see [Imaging support matrix on page 49](#).

To learn more about the different imaging methods available with HPDM, see the following sections:

- [Imaging without PXE on page 50](#) (recommended)
- [Imaging with PXE on page 52](#)

Imaging support matrix

The following table describes which operating systems and HP thin clients are supported for each imaging method.

Table 6-1 Imaging support matrix


	File-based capture	Disk-based capture	File-based deployment	Disk-based deployment	PXE imaging
WES 8					
t610	✓		✓		
WES 7					
t820, t620, t610, t510, t505, t5740e, t5570e, 6360t, mt41, mt40, 4320t	✓		✓	✓	
WES 2009					
t610, t510, t505, t5740, t5570, gt7720	✓		✓	✓	✓
WES 2009					
6360t, t5400, 4320t	✓		✓	✓	
Windows XPe					
t5740, t5730, t5630		✓		✓	✓
HP ThinPro 4					
t620, t610, t510, t505, t5745, t5565		✓		✓	✓
HP ThinPro 3 (x86)					
t5745, t5735, t5565, t5545, t5145, gt7725		✓		✓	✓
HP ThinPro 3 (ARM)					
t5325					
HP Smart Zero Core (x86)					
t620, t610, t510, t5565z		✓		✓	
HP Smart Zero Core (ARM)					
t410, t5335z		✓		✓	
Windows Embedded CE 6.0					
t510, t5550, t5540, t5530		✓		✓	✓




IMPORTANT: Complete image version checking is not available for PXE imaging (for example, Windows XPe version 5.1.502 is compatible with BIOS version 786A1 but not with another BIOS version).

IMPORTANT: Drivers will be missing when deploying a WES 7 or WES 8 image captured from a different HP thin client model. For example, an image captured from a t610 will not work if deployed to a t5570e.


IMPORTANT: PXE imaging does not work with the default HPDM Agent in an HP ThinPro 3 image due to some folder name changes. Please update the HPDM Agent to the latest version before attempting PXE imaging.

 **NOTE:** File-based imaging is the current method used by HPDM for WES imaging. The original imaging method used by HPDM in version 4.4.2 and prior was disk-based imaging.

 **NOTE:** PXE imaging is not supported on the 6360t, t5400, or 4320t because the boot order change tools are unavailable.

Imaging without PXE


Imaging without PXE is the recommended method of imaging with HPDM and requires that the HPDM Agent on the target device is running when the imaging task is sent. The benefit of imaging without PXE is that an HPDM Gateway is not required to be installed in the same subnet as the target devices.

 **TIP:** For WES, make sure that the devices can access the Master Repository's shared folder and have permission to write. The Group Policy might affect write permissions if the shared folder to be accessed is in a domain.


Capturing an image without PXE

To capture an image without PXE:


1. Select the **Task Templates** tab in the task pane, and then double-click on the **_Capture Image** template.
2. In the **Template Editor - Imaging** dialog box, enter a name in the **Image Name** field for the captured image that will be stored in the Master Repository, and then enter information in the **Description** field for the captured image.
3. If the device uses a wireless network, select **Cached Imaging**.

 **NOTE:** If the **Cached Imaging** option is selected, it requires enough free disk space on the device to cache the captured image.

4. Click the **Save as** button, enter a name for this template, and then click **OK**. A new template will appear in the task pane.
5. Drag and drop this template onto a device in the device pane. The **Task Editor** dialog box will appear.
6. In the **Save result as template** field, enter a name for the result template that will be automatically created to enable you to apply the captured image to other devices.
7. Click **OK** to apply the task to the device immediately. When the task is sent, a result template will be created with the name you designated. Its initial status will be "Transferring."
8. When the HPDM Agent on the device receives the task, the device will display a warning message indicating that the device will restart in 30 seconds. After the device restarts, a capture utility will copy the content of the flash storage to the Master Repository.

 **NOTE:** A WES image is stored as an .ibr file, and an HP ThinPro or HP Smart Zero Core image is stored as a .dd.gz file.

9. The device will reboot after capturing has completed.

 **IMPORTANT:** DO NOT turn off the device during this procedure!

The device will then reboot again.

10. The task pane in the HPDM Console will continue to indicate that the task is processing. The captured image is being compressed. After the task is finished and the checksum of the captured image is verified, a new template will appear in the **Task Templates** tab of the task pane with the name you specified.
11. You can now use this template to apply the captured image to other devices by dragging and dropping it onto devices in the device pane or folders in the device tree.

You can view information about the image associated with the template by double-clicking on the name of the template to display the Template Editor dialog box. This will display the name and OS type of the image. Click the **View Details** button, and detailed information of the image will appear.

Preserved settings during an image capture without PXE

Table 6-2 Preserved settings during an image capture without PXE

Operating system	Preserved settings
WES 8	All settings from the source device are preserved on both the source device and the captured image except the hostname, network settings, domain settings, and write filter status.
WES 7	
WES 2009	
HP ThinPro	All settings from the source device are preserved on both the source device and the captured image except the hostname and network settings.
HP Smart Zero Core	

TIP: For WES 7 and WES 2009, if the source device was joined to a domain prior to having its image captured, then domain membership will be lost after capturing the image. It is recommended to remove the source device from any domain prior to capturing the image. There is also a known issue where the Group Policy that controls the domain password complexity will affect local user accounts, resulting in the user requirement to change the password to meet a more strict criteria.

Deploying an image without PXE

There is not a preset template for deploying an image without PXE, but one can be created by capturing an image or by importing an existing image file.


To deploy an image without PXE:


1. Create a deployment template by capturing an image without PXE (see [Capturing an image without PXE on page 50](#)).

—or—


From the menu, click **Template > Import > Image Files > to deploy without PXE**, and the wizard will automatically create a deployment template.

2. Double-click on the deployment template to open the **Template Editor**.
3. Click the **View Details** button to view detailed information about the image package.
4. If the device uses a wireless network, select **Cached Imaging**.

 **NOTE:** If the **Cached Imaging** option is selected, it requires enough free disk space on the device to cache the image file.

 **NOTE:** With cached mode, HPDM only supports deploying **.ibr** images to WES devices or **.dd.gz** images to HP ThinPro devices.

5. If you want to deploy an image to a device that is a different hardware platform from the source device, select **Allow Cross Platform Imaging**. This option only applies to WES, and you need to make sure the image can work well on the target device.
6. Click the **Save as** button to save the template with a new name.
7. Drag and drop the template onto the devices to which you want to deploy the image. The **Task Editor** dialog box will appear, allowing you to edit the same options you were presented with in the Template Editor.
8. Click **OK** to deploy the image to the devices.

 **NOTE:** There will be an automatic BIOS update during a Deploy Image task to install WES7 SP1 on the t5740 or t5740e. The factory BIOS version is 1.03 on the t5740 and t5740e, and WES7 SP1 requires version 1.04.


Preserved settings during an image deployment without PXE

Table 6-3 Preserved settings during an image deployment without PXE

Operating system	Preserved settings
WES 8	<ul style="list-style-type: none"> • Write filter status
WES 7	<ul style="list-style-type: none"> • Hostname
WES 2009	<ul style="list-style-type: none"> • Network settings • Terminal Services license • Windows activation license (WES 8 only)
HP ThinPro	<ul style="list-style-type: none"> • Hostname
HP Smart Zero Core	<ul style="list-style-type: none"> • Network settings

Imaging with PXE

Imaging with PXE requires an HPDM Gateway (which includes a PXE server) to be installed in the same subnet as the target devices. The benefit of imaging with PXE is that the device's operating system is not required to be running during an image deployment, meaning you can deploy an image to a device with a corrupted operating system.

 **TIP:** Some additional configurations might be required for PXE imaging. If you experience problems with PXE imaging, see [Configuring your environment for PXE imaging on page 53](#).

Capturing an image with PXE


To capture an image with PXE:

1. Select the **Task Templates** tab, and double-click the **_PXE Capture** template.
2. Input an image name and a description.
3. Click **Save as** to save the template.

A new PXE Capture template will be listed in the Task Templates tab.

4. Drag the template onto a device, and then input a result template name. Click **OK** to send this PXE Capture task to a device.

5. When the task is sent, a result template will be created with the name you designated. Its initial status will be “Transferring”.
6. After the task is finished, the result template is valid and can be used to send tasks.

 **NOTE:** An image captured for PXE imaging is always in the **.dd.gz** format, regardless of the operating system.

Deploying an image with PXE

There is not a preset template for deploying an image with PXE, but one can be created by capturing an image or by importing an existing image file.

To deploy an image with PXE:


1. Create a deployment template by capturing an image with PXE (see [Capturing an image with PXE on page 52](#)).

—or—

From the menu, click **Template > Import > Image Files > to deploy using PXE**, and the wizard will automatically create a deployment template.

2. Drag the deployment template onto a device.

 **NOTE:** PXE deployment supports deploying **.dd.gz**, **.dd**, **.img**, or **.hping** images.

 **NOTE:** If you want to deploy an image to a device that is shut down, the device must support being woken up and be set to “network boot first” in the BIOS.

Configuring your environment for PXE imaging

The following sections discuss some configurations that might be necessary for PXE imaging:

- [Configuring a DHCP server for PXE imaging](#)
- [Configuring routers for PXE imaging](#)
- [Configuring BIOS settings on legacy Neoware devices for PXE imaging](#)

Configuring a DHCP server for PXE imaging

This section describes how to configure a DHCP server for PXE imaging. The DHCP server is used the PXE boot ROM to retrieve basic networking information.

The DHCP server is installed on a different machine from the HPDM Server

If problems occur during PXE imaging, the DHCP server might need to be checked for certain settings that conflict with PXE. However, on most networks, these issues should not occur.

To configure the DHCP server:

1. Make sure that the DHCP server has not been previously configured for a PXE bootstrap.
2. Make sure that DHCP options 43 and 60 are not set.

The DHCP server should then be ready to be used with PXE.

The DHCP server is installed on the same machine as the HPDM Server

If the DHCP server is installed on the same machine as the HPDM Server, it requires some manual configuration.


These instructions assume the following:

- The network is already configured using DHCP.
- The DHCP server has not been previously configured for a PXE bootstrap.
- There are no other TFTP servers running on the same network.

To configure the DHCP server:

1. Make sure that DHCP option 43 is not set.
2. Add DHCP option 60 by doing the following:

- a. From the Windows Start menu, select **Start > Run**.

 **TIP:** In Windows Server 2012, right-click the lower-left corner of the desktop and select **Run**.

- b. Type `cmd` and click **OK** to open a Command Prompt.

- c. Type `netsh` and press the **Enter** key.

- d. Type `dhcp` and press the **Enter** key.

- e. Type `server \\<server_name>` (using the UNC name for the server).

—or—

Type `server <ip_address>` (using the IP address of the server).


A **dhcp server >** prompt appears in the command window.

- f. Type `add optiondef 60 <name of your choice> STRING 0` and press the **Enter** key.
- g. Type `set optionvalue 60 STRING "PXEClient"` and press the **Enter** key.
- h. To confirm that the settings are correct, type `show optionvalue all` and press the **Enter** key.

3. Add DHCP option 201 by doing the following:

- a. At the **dhcp server >** prompt, type `add optiondef 201 <name of your choice> STRING 0` and press the **Enter** key.

- b. Type `set optionvalue 201 STRING '<HPDM_Gateway_IP_Address>' '40003'` and press the **Enter** key.

 **NOTE:** The `<HPDM_Gateway_IP_Address>` is the address of the server running the HPDM Gateway service. This command must be written exactly as shown above, including the single quotes and single space, as shown in the following example:

```
set optionvalue 201 STRING '192.168.1.100' '40003'
```


- c. To confirm that the settings are correct, type `show optionvalue all` and press the **Enter** key.

The DHCP server should then be ready to be used with PXE.

Configuring a Linux DHCP server for PXE imaging

1. Edit the DHCP server configuration file `/etc/dhcpd.conf`. Add the following lines to the beginning of the file exactly as shown:

```
ddns-update-style ad-hoc;  
Authoritative;  
Option NDM code 201 =string;  
Option vendor-class-identifier "PXEClient";  
Option NDM "`<HPDM_Gateway_IP_Address>' `40003'";
```

 **NOTE:** The <HPDM_Gateway_IP_Address> is the address of the server running the HPDM Gateway service. This command must be written exactly as shown above, including the double quotes, single quotes, and single space, as shown in the following example:

```
Option NDM "`192.168.1.100' `40003'";
```


2. Restart **dhcpcd** to use the new configuration.

Configuring routers for PXE imaging

For PXE imaging to function properly, any network that uses DHCP and has multiple subnets should have an IP helper configured in the router that is between any devices that require a dynamic IP address and the DHCP server. The router will need to be configured to have an additional IP helper address point to the HPDM Gateway.

The following example uses a Cisco router:

1. Enter **Global Configuration** mode.
2. Type `ip forward-protocol udp 67` and press **Enter**.
3. Type `ip forward-protocol udp 68` and press **Enter**.
4. Type `ip helper-address <DHCP_Server_IP_Address>` and press **Enter**.
5. Type `ip helper-address <HPDM_Gateway_IP_address>` and press **Enter**.

 **NOTE:** The above IP addresses should be entered without the < or > characters.

Configuring BIOS settings on legacy Neoware devices for PXE imaging

Before you can capture or deploy an image with PXE on legacy Neoware devices, you must make sure that the source and target devices have their BIOS settings configured correctly.

To configuring BIOS settings on legacy Neoware devices for PXE:

1. Turn on the device and hold down the **Delete** key to display the **CMOS Setup Utility** screen.
2. Select **Advanced BIOS Features** and set the following:

```
First Boot Device [LAN]  
Second Boot Device [HDD-0]
```
3. Press the **Esc** key to return to the initial screen, and then select **Integrated Peripherals > VIA OnChip PCI Device**.
4. Make sure **Onboard Lan Boot ROM** is set to **[Enabled]**.
5. Press the **F10** key, press the **Y** key, and then press **Enter** to save the settings.

7 Repository management

HPDM uses a Master Repository and one or more Child Repositories to store the files needed for its tasks. The Master Repository holds all files deployed by HPDM, while a Child Repository can hold either all or a subset of the files held in the Master Repository. Each repository is a file server to which HPDM will connect using either standard FTP, the encrypted equivalents SFTP and FTPS, or a Shared Folder.

By default, the Master Repository syncs the relevant files to the Child Repositories automatically when a new task is started.

Initializing from wizard

You will be prompted by a wizard to help you initialize the repository system when you start the HPDM Console for the first time.

The wizard consists of two pages:

- Protocol Settings
- Master Repository Configuration

Selecting the file protocol to use


To select the file protocol HPDM should use:

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, click **Protocols**.
3. In the **Protocol Configuration** dialog box, establish the protocol and port you wish to use.


The protocol settings will be applied to all repositories, including the Master and the Child Repositories, and HPDM will only use the protocols to access the repositories.

Configuring the Master Repository

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, select the Master Repository and click **Edit**.
3. In the **Repository Editor** dialog box, configure the **Repository Name**, **Server Address**, **Username**, **Password**, and **Path** settings.


 **NOTE:** Paths specified above must point to the same location you configured for the Master Repository Controller during installation. For example, you put `c:\ftproot\HPDM` during installation, and for FTP you access this folder by `ftp://IP/HPDM`, for Shared Folder you access it by `\\IP\HPDM`, so here you should input **HPDM** for the Path value of the FTP and the Shared Folder.

4. Click **Test** if you want to test the connections you've configured

 **NOTE:** The tests are performed before changes are saved anyway.


5. Click **OK**.

If the address of the Master Repository was changed, the HPDM Server will drop the current connection and try to connect to the Master Repository Controller at the new address.

 **NOTE:** The HPDM Server will need time to establish the connection to the Master Repository Controller. Wait for a while before doing repository-related operations such as managing content.

Configuring the Child Repositories

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, click **Add**.
3. In the **Repository Editor** dialog box, configure the **Repository Name**, **Server Address**, **Username**, **Password**, and **Path** settings.
4. Click **Test** if you want to test the connection to the FTP server or the shared folder before saving.

 **NOTE:** The test is performed before changes are saved anyway.

5. Click **OK**.

Deleting Child Repositories

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, select a Child Repository.
3. Click **Remove**, and then click **Yes** to confirm.


Exporting repositories

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, click **Export**.
3. Browse to the location where you want to save the repository.
4. Click the **Export** button.

Importing repositories

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, click **Import**.
3. Browse to the location where the repository you want to import is located.
4. Click the **Import** button.

Synchronizing repositories

 **TIP:** It is not required to manually synchronize repositories or to schedule an automatic synchronization. The relevant files in the Master Repository are automatically synced to the Child Repositories when a task is started.

To manually synchronize all content to all Child Repositories:

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, click **Sync**.
3. In the **Synchronization** dialog box, click **Sync**.
4. Click **Yes** to confirm.

To schedule a repeated automated synchronization:

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, click **Sync**.
3. In the **Synchronization** dialog box, select the **Enable schedule synchronization** checkbox.
4. Configure the options and schedule as necessary.
5. Click **Save**.

Synchronization, whether manual or automatic, is done in the background. After completion, the **Last Time Synchronized** column in the **Repository Management** dialog box will be updated.

Content management

To view the contents of the Master Repository:

1. Select **Tools > Repository Management** from the HPDM Console menu.
2. In the **Repository Management** dialog box, click **Content**.

Viewing detailed payload information


To view detailed payload information:

- ▲ In the Content Management dialog box, select a category (except Files Captured) in the left panel, then double-click an item in the right panel. A dialog box will appear to display detailed payload information.

Deleting contents from the Master Repository

To delete contents from the Master Repository:

- ▲ In the Content Management dialog box, select an item in the right panel, then click the **Delete** button. A confirmation message will appear. Click **Yes**, and the payload will be deleted.

 **NOTE:** The built-in contents can't be deleted.

Downloading contents from the Files Captured category

To download contents from the Master Repository:

1. In the Content Management dialog box, select an item in the **Files Captured** category, then click the **Download** button.
2. Browse to the location where you want to save it. The content will be downloaded to the local machine.

Repository mapping

HPDM automatically maps each device to the nearest and most convenient repository. This allows the administrator to send tasks to a large number of HPDM Agents and have the device connect automatically to a repository to find the information or applications it may need to perform the task. The payload required for the task will be synchronized automatically before the task is sent to the target devices.

To access the Repository Mapping dialog box:


1. Select **Tools > Repository Management** from the HPDM Console menu.
2. Click **Mapping**.

Batch mapping

You can choose to map devices in a batch by their master HPDM Gateway or subnet address by selecting the corresponding radio button. You can view all mapping results by deselecting the **Show exceptions only** checkbox.

To change the mapping for an HPDM Gateway or subnet address, right-click on it and select one of these options from the pop-up menu:

- **Auto Map**—Automatic mapping (factory default settings). The HPDM Server assigns a repository to each HPDM Gateway or subnet address depending on the IP address.
- **Use Master**—Use the Master Repository.
- **Use Specified**—Choose a repository from a pop-up list for the specified HPDM Gateway or subnet address.

 **NOTE:** An administrator can change the mapping settings of a device or an HPDM Gateway or subnet address at any time.

 **NOTE:** HPDM will automatically map any new device added to the network.

Per device mapping

You can define exception devices for which you want to use a different repository than the one used for batch mapping by adding devices from a filter and assigning them a specified repository.

See [Filtering devices on page 37](#) for details about filters.

8 Security management

There are two forms of security management in HPDM: **User Management** and **Authentication Management**.

User management

Each user account can have customized permissions, according to their level of need. These are assigned through the user groups system.

To view the User Management dialog box:


- ▲ From the HPDM Console's menu bar, click **Tools > User Management**.


Adding users

1. In the User Management dialog box, click **Add** to add a new user. The **Create New User** dialog box will appear.
2. Enter a **Username** for the new user and specify a **Password**. Click **OK** to create the new user.

This user name can be used to log in to the HPDM Console the next time the HPDM Console starts.

See [Assigning users to groups on page 60](#) to add the new user to a user group.

 **NOTE:** The user must be added to a group before it has any permissions to use HPDM.

 **NOTE:** Multiple HPDM Consoles cannot log on to the HPDM Server with the same username at the same time.

Deleting users

1. In the User Management dialog box, select a user from the list in the **Users** tab.
2. Click **Delete**, and then click **Yes** to confirm.

Assigning users to groups

1. In the User Management dialog box, double-click a user from the list in the **Users** tab.
2. Select the **Member Of** tab.
3. Click **Add** to add the user to a new group, or click **Remove** to remove the user from the selected group.

Changing a user's password

1. In the User Management dialog box, right-click on a user from the list in the **Users** tab.
2. Select **Change Password** from the pop-up menu.

3. Enter the **New Password** for the user, and then re-enter it in the **Confirm Password** field.
4. Click **OK** to finish.



NOTE: When you log in as root for the first time, it is strongly recommended that you change the password from the default.

Assigning Security Filters to Users

1. In the User Management dialog box, double-click a user from the list in the **Users** tab.
2. Select the **Filter** tab.
3. Click **Add** to add the filter to this user, or click **Remove** to remove the security filter from this user.

Adding a group

Groups can be used to control user permissions in HPDM.

1. In the User Management dialog box, select the **Groups** tab.
2. Click **Add** to add a new group. This group can now be assigned a set of permissions, and then users can be assigned to this group.

Assigning permissions to groups

1. In the User Management dialog box, right-click on a group from the list in the **Groups** tab.
2. Select **Properties** in the pop-up menu.
3. Select the **Privileges** tab.
4. Select the permissions you wish to assign to the group.
5. Click **OK** to finish.

Assigning users to groups

1. In the User Management dialog box, right-click on a group from the list in the **Groups** tab.
2. Select **Properties** in the pop-up menu.
3. Select the **Users** tab.
4. Use the **Add** and **Delete** buttons to modify the members of this group.
5. Click **OK** to finish.

Assigning security filters to groups

1. In the User Management dialog box, double-click on a group from the list in the **Groups** tab.
2. Select the **Filter** tab.
3. Click **Add** to add the filter to this group, or click **Remove** to remove the security filter from this group.

Deleting groups

1. In the User Management dialog box, select a group from the list in the **Groups** tab.
2. Click the **Delete** button, and then click **Yes** to confirm.

User authentication with LDAP and Active Directory

Users and groups in an Active Directory, or other LDAP servers, can be used to log in to HPDM. This allows reuse of existing login accounts and simplifies the management of who has administrative privileges with HPDM.

Configuration

To configure a connection to a LDAP Server:

1. From the HPDM Console's menu bar, click **Tools > Configuration**.
2. In the Configuration Management dialog box, select **User Authentication** in the left pane.
3. In the **Host** field, type the LDAP server hostname or IP address. If an encrypted connection will be used, the LDAP server must be specified by the hostname.
4. Adjust the **Port**, if necessary. Port 389 is the most common port with TLS or Unencrypted LDAP connections. Port 636 is the port commonly used for a SSL LDAP connection.
5. Select an **Encryption** type.
6. If a TLS or SSL encryption is in use, a **Host Key** must be specified. Do one of the following:
 - ▲ Click **Get Key From Host**. A connection will be created to the LDAP server, and the Host Key will be saved.

—or—

 - ▲ Click **Import From File**. Browse to the Host Key certificate file (in one of the following formats):
 - Key Export File: Host keys can often be exported to a file from the LDAP server. For the Microsoft Active Directory/IIS platform, this Export File can be obtained from `http://<your-ldap-server>/certsrv/certcarc.asp`.
 - Java Keystore: A `hpdmcert.key` file from a previous HPDM installation, or other Java Keystore file, can be imported.
7. In the **Server Type** section, choose a LDAP server type from the **Type** menu.
 - a. **Active Directory**: Specify the Active Directory **Domain**. Only a single Domain is supported.
 - b. **Generic LDAP**:
 - Specify the **Base DN**. A Base DN (Distinguished Name) is required to connect to the LDAP Server. Please refer to your LDAP server documentation for further details about the Base DN.

Examples of Base DN's:

- dc=testnet,dc=com
 - o=company,c=US
 - Specify the **RDN Attribute**. The RDN (Relative Distinguished Name) attribute is the LDAP attribute that specifies the login name of the user. Common values for this include **sAMAccountName** (Active Directory), **UID**, and **CN**.
8. Configure a **Search User**. This Search User will be used in two situations: by the **Import Users and Groups** dialog box to browse the LDAP Server, and to dynamically determine the members of an imported Group. Unless the LDAP supports anonymous search, a search user must be specified. Leave the Username and Password blank to use the anonymous user.
- This **Username** should be specified as a **Distinguished Name**.
- Active Directory Note:** The Distinguished Name uses the LDAP CN attribute instead of the regular login name. To determine the LDAP CN, on the Domain Controller, open **Active Directory Users and Computers**, and double-click the **search user**. On the **General** tab of this **Properties** window is shown the **Display Name**. This **Display Name** is the LDAP CN.
- For example, a Display Name of “HPDM search user” in the Users directory of the domain “testnet.com”, the DN will be:
- CN=hpdm search user,CN=Users,DC=testnet,DC=com**
9. Finally, test the configuration by clicking the **Test** button. When the configuration for the LDAP server has been completed successfully, this test will pass.

Importing users and groups

Now that the LDAP server has been configured, Users and Groups must be imported. This Import process tells HPDM which LDAP users are permitted to log in, and what their privileges are once they do so.

To open the Import Tool:

1. From the HPDM Console's menu bar, click **Tools > User Management**.
2. Click the **Import from LDAP** button.

The **Import Users and Groups** dialog box allows a User or Group to be located via **Browse** and **Search**. The properties of a LDAP object can be evaluated with the **Show Attributes** button. Users and Groups can be added and subsequently imported.

To browse for a User or Group:

1. The **Import Users and Groups** dialog box opens in **Browse** mode. A tree of LDAP objects is shown in the left side of the dialog box.
2. Directories can be expanded by clicking the **Plus** button to the left of a Directory.
3. Some places in the LDAP tree may have many results. If so, a blue **Show 20 more** entry will be present. Click **Show 20 more** to show more results.

To search for a User or Group:

1. Click the **Search** tab in the upper left of the **Import Users and Groups** dialog box.
2. The **Base DN** is the starting point from which the search will be run. All searches will be done recursively from this origin.
3. The Query allows the specification of what to search for. It contains 3 parts: the Attribute, the Search Value, and the Comparison between the two.

- a. The **Attribute**, on the left side of the query, offers several common attributes to search on. If the desired search attribute is not present, type the attribute into this field.
- b. The **Search Value**, on the right side of the query, is what is being searched for. An asterisk, *, can be used as part of the **Search Value**. This permits searching when the full Search Value is unknown. Example: Searching Attribute UID with an Equals comparison for Value *.smith@testnet.com will match all users with a UID that end with .smith@testnet.com.
- c. The **Comparison**, in the middle of the query, offers several ways to compare the value of the attribute to what you are searching for.
 - The **Equals** comparison, =, will find LDAP objects that are equivalent to the search value.
 - The **Greater than or Equals** comparison, >=, will find LDAP objects with an attribute value that is numerically larger than the search value.
 - The **Less than or Equals** comparison, <=, will similarly find LDAP objects with an attribute value that is numerically smaller than the search value.
 - The **Similar to** comparison, ~=, permits searching for attribute values that are similar to the search value.
 - Finally, the **Not Equals** comparison, !=, permits searching for attribute values that are not equivalent to the search value.
4. Finally, press the **Search** button. Results will appear in the **Search** tree to the left. See the procedure **To browse for a User or Group** earlier in this section for more information about browsing the search results.

Adding a User or Group to be Imported:

1. Locate the User or Group, either by **Browse** or **Search**.
2. Add the User or Group using one of the following methods:
 - Double-click the User or Group.
 - or—
 - Click the User or Group and click the **Add** button near the bottom left of the dialog box.
3. The User/Group should now be on the right side.



NOTE: The Users and Groups are not imported until the **Import Button** in the bottom right is clicked. Be sure to click the **Import** button when you are finished importing Users and Groups.

Removing a User or Group from being Imported:

1. Select a User or Group on the right side of the **Import Users and Groups** dialog box.
2. Click the **Remove** button.

Examining a User or Group:

1. Click a User or Group.
2. Click the **Show Attributes** button.
3. If desired, this object can be added to the User/Group to Import list by clicking the Add button.

Import Users or Groups:

1. Locate the Users or Groups with **Browse** or **Search**.
2. Add the User or Group.
3. Click the **Import** button in the lower right corner. The imported Users and Groups will now be visible in the **User Management** dialog box.
4. If a Group has been imported, the privileges of the group must be assigned. Please see [Assigning permissions to groups on page 61](#).

Authentication management

Since the HPDM Server can discover and manage all HPDM Gateways and HPDM Agents on the network, a security problem may occur due to the improper usage of the HPDM Server. To overcome this, HPDM provides an authentication capability for the HPDM Gateways and the HPDM Agents to recognize a secure HPDM Server.

There are two tools for providing authentication: **Key Management** and **HPDM Gateway Access Control**. These are accessed by selecting **Tools > Authentication Management** in the HPDM Console's menu bar.

Key management

An Authentication Key is a plain text password which is input on the HPDM Console. The key will be passed to the devices during the key update process. The devices will check the key passed by HPDM Server when executing tasks.

To update the current Authentication Key:

1. Select **Tools > Authentication Management > Key Management** in the HPDM Console's menu bar to display the **Authentication** dialog box.
2. Enter your user **Password** then click **OK**. The **Key Management** window will appear.
3. Click the **Update Current Key** button to display the **Update Key** dialog box.
4. Enter the new **Password** (i.e. the Authentication Key) and specify the **Expire Interval** (number of days).
5. Click the **OK** button.



NOTE: **Expire Interval** is the time that the password (Key) keeps valid. If an HPDM Agent cannot contact an HPDM Gateway for key information before a specified time (Expiration Interval), the Key will expire, (i.e., no longer in use) and the HPDM Agent will revert to its initial key.

HP recommends that user passwords contain:

- at least eight characters
- letters of both upper and lower cases
- numbers and punctuations as well as letters

To export all Authentication Key(s):

1. Click the **Export All Key(s)** button in the **Key Management** window to display the **Export** dialog box.
2. Browse for a folder to save the current authentication key(s) as a ***.ks** file, then click the **Export** button.

3. The system will prompt you to create and confirm the KeyStore password.
4. In the **Create KeyStore Password** dialog box, enter a KeyStore **Password** and confirm the password in the **Re-enter Password** field.
5. Click the **OK** button.

To import Authentication Key(s):

1. Click the **Import Key(s)** button in the **Key Management** window to display the Import dialog box.
2. Browse for the exported *.ks file, then click the **Import** button.
3. The system will prompt you to enter the KeyStore password.
4. Enter the KeyStore **Password** then click the **OK** button.

Viewing the Key Update Log

To view the **Key Update Log**, click the **View Update Log** button in the **Key Management** window.

In the **Key Update Log List** you can view all the log times and events. You can remove all the logs by clicking the **Clear All Logs** button.

HPDM Gateway access control

The HPDM Server will maintain the acknowledge status of an HPDM Gateway which is specified by the user from the HPDM Console. When an HPDM Gateway is discovered by the HPDM Server, the HPDM Gateway is set as Unknown status. The HPDM Server will not establish any connection with an HPDM Gateway nor receive any messages sent by the banned HPDM Gateway unless the HPDM Gateway is acknowledged.

To control HPDM Gateway access manually:

1. Select **Tools > Authentication Management > HPDM Gateway Access Control** from the HPDM Console's menu bar to display the **Authentication** dialog box.
2. Enter your password then click **OK**. The **HPDM Gateway Access Control** window will appear.
3. Select an HPDM Gateway from the **HPDM Gateway Access Control List**, then click the **Acknowledge** or **Ban** button to recognize or ban the selected HPDM Gateway.



NOTE: If the **Manually control HPDM Gateway access** option is unchecked, the HPDM Gateway with the **Unknown** status is regarded as **Acknowledged**. When this option is selected, the HPDM Gateway with the **Unknown** status is regarded as **Banned** and you need to configure the status of the HPDM Gateway manually.

9 Report management


Adding a report template

To add a report template:


1. Select **Tools > Report Management** from the HPDM Console's menu bar to display the **Report Management** window.
2. Select one report type from the **Report Types** list, then click the **Add** button. A **Set New Report Template Name** dialog box will prompt you to input a report template name.
3. Click **OK** to open the **Edit Report Template** window. In the **Edit Criteria** field, click the ... button to open the **Choose Criteria Key** window. Select a criteria key in the **Candidate Criteria Key List**.

After you have made the selection, click **OK** to return to the **Edit Report Template** window.

4. In the **Edit Criteria** field, select or enter the criteria conditions in the two drop-down lists.
5. Click **Add** to add the criteria into the **Criteria List**, or select an existing criteria, and then click **Edit** to renew the restricted condition.
6. Define operator and value for each criterion.

 **NOTE:** The **Report Template** can contain several criteria and each criteria could have one of two kinds of relationships: **Satisfy All Criteria** or **Satisfy Any Criteria**. So you can select either of them to generate reports.

7. Click **Generate Reports** to generate the report according to the current criteria, or click **Save** to add these criteria to the named template.


 **NOTE:** The modified criteria will not be saved in the template after generating a report. You need to click the **Save** button to save the modified criteria in the template.

Importing a report plug-in file

To import a report plug-in file:

1. Click **Import** in the **Report Management** window, then select a plug-in file (*.jar).
2. Click **Import Plug-in File** to import the file and return to the **Report Management** window. A new report type is added to the **Report Types** list.

You can remove a report type from the list by selecting it then clicking the **Delete** button. You will be prompted to confirm that you want to delete it.

 **NOTE:** The imported report types can be deleted only if there is no template belonging to the reported type.

Generating a report using a report template

To generate a report using a report template:

1. In the **Report Management** window, select a report type from the **Report Types** list and all the report templates belong to the selected type will be displayed in the **Report Templates** list.
2. Select a template from the list then click **Edit**, or double-click on the template to view the template's content.
3. Click **Generate Report** to preview the report.

Producing reports

HPDM enables you to print information about your devices and the tasks you have sent to them. There are six types of report available: *Gateway Information*, *Device Information*, *Device Task Report*, *Task Report*, *Task Status Report*, and *Task Status Log Report*.

HPDM Gateway report

This report lists the basic asset information of the selected HPDM Gateways.

To create an HPDM Gateway report:

1. Select the HPDM Gateway systems for which you want a report.
2. Right-click on the selection and select **Print Device Information ...**.

Device Information report

This report lists the basic asset information and last known online status for the currently selected devices.

To create a Device Information report:

1. Select the device systems for which you want a report.
2. Select **File > Print Device Information** from the HPDM Console menu.

Device Task report

This report is only available when a single device is selected. It lists each task that has been sent to the device with its status and the associated task log. Tasks that have been deleted will not be included.

You will be asked to specify whether you want to see tasks created by all administrator or just the tasks you created. You will also have the option to restrict the report to a specific time period.

To create a Device Task report:

1. Select the device system for which you want a report.
2. Select **File > Print Device Task Report** from the HPDM Console menu.
3. Select the appropriate options in the **Device Task Report** dialog and click **Next >**.

Task report

This report lists the description and status of all tasks that have not been deleted.

To create a Task report:

- ▲ Select **Print Task Report ...** from the **File** menu.

Task Status report

This report lists information about a task's status.

To create a Task Status report:

- ▲ Select a task from the **Device Task View** dialog, right-click and select **Print Preview > Status ...**

Task Log report

This report lists information about a task's status log.

To create a Task Status Log report:

- ▲ Select a task from the **Device Task View** dialog, right-click and select **Print Preview > Log ...**

10 Status Walkers

HPDM has two integrated tools that monitor and record the performance of the devices: **Status Walker** and **Status Snapshot**.



NOTE: The Status Walker has been deprecated and is no longer supported by HP. It is still provided as a tool for your use.

Status Walker

The **Status Walker** tool makes a list of all the IPs available and walks to them; it brings back their status information and displays it. This status report is made in real time. The information is stored in a database placed on the server.



NOTE: The **Status Walker** option is only available for Windows-based HPDM Gateways.

Creating a Status Walker

1. Display the **Tools** menu from the HPDM Console's menu bar and select **Status Walker**. The Status Walker dialog will appear.
2. Click **Add** to create a new walking schedule, or **Edit** to modify an existing one. The **Schedule Editor** dialog box will appear.
3. Select the name of the scope to use in the **Walk the Scope** drop-down menu, or select **Edit** to define a new scope.

Selecting **Edit** will display the **Scope Management** dialog box which enables you to add, edit or remove scopes.

4. Click the **Add** button and enter a name for the new scope.

Click **OK** to display the **Scope Editor** dialog box.

Specify the IP address range in the **Current Item** fields, then click **Add** to add it to the list box on the left. Click **OK** when you have finished defining scopes.

Click **Close** in the **Scope Manager** dialog box to return to the **Schedule Editor**. The scope(s) you defined will be listed in the **Walk the scope** field ready for selection.

5. Select the **Gateway** to use.
6. Use the **Schedule** options to specify the time and frequency of the task.
7. Click **OK**.

The results of scheduled walking tasks will be displayed in the **Walking Tasks** pane at the bottom of the **Status Walker** dialog box.

Selecting a **Finished** walking task then clicking the **View** button will display the status of devices found.

Configuring the Status Walker

You can configure the **Status Walker** to suit your requirements as follows:

1. Select **Tools > Configuration** from the HPDM Console's menu bar to open the **Configuration Management** window.
2. Select the **Status Walker Configuration** item in the left-hand tree pane.



NOTE: You can display a short description of each option by clicking in the option field.

3. Enter a value for the **Walking Group Size**.
4. Define a value for **Walking Timeout**.
5. Click **Apply** to save the settings.
6. Click **OK**.

Status Snapshot

The **Status Snapshot** tool takes a snapshot of the network, that is, it creates a report of the devices' status and stores it on the server to be displayed when the tool is opened. This tool does not work in real time. The **Status Snapshot** settings allow the administrator to schedule the walk and set the frequency.


1. Display the **Tools** menu from the HPDM Console's menu bar and select **Status Snapshot**. The **Status Snapshot** dialog box will appear.
2. Click **Add** to create a new status snapshot schedule, or **Edit** to modify an existing one. The **Schedule Editor** dialog box will appear.
3. Schedule the status snapshot task by specifying its **Frequency** and the **Start Time**.
4. Click **OK**.
5. Click **Close**.

The results of the scheduled status snapshot tasks will be displayed in the **Status Snapshot Tasks** pane at the bottom of the **Status Snapshot** dialog box.

Selecting a **Finished** status snapshot task then clicking the **View** button will display information about the devices found.

11 HP FTP Software Component Browser

The HP FTP Software Component Browser provides a means to automate the process of leveraging software components from the HP public FTP site.

 **IMPORTANT:** This feature requires Internet access. If the system running the HPDM Console or Master Repository Controller cannot access the Internet directly, you must first configure proxy settings. See [Configuring HP FTP proxy settings on page 73](#) for more information.


You can use the HP FTP Software Component Browser to generate task templates by downloading a component. The following component types are available:

- Operating system images—Generate **_Deploy Image** templates
- Applications—Generate **_File and Registry** templates

Generating task templates


To use the HP FTP Software Component Browser to generate task templates:

1. Start the HPDM Console and from the menu, select **Template > Import > HP FTP Software Component Browser**.
2. The dialog will retrieve image and application component information from the HP FTP server. You can use the **Search** function to filter the components. Select one item, then click the **Generate Templates** button.


 **NOTE:** If the HPDM Console or the Master Repository Controller has no direct access to the HP FTP site, click the **Proxy Settings** link to configure proxy settings, or go to **Main Menu > Tools > Configurations**.

Once set, the proxy settings will be stored in the database. All consoles and the Master Repository Controller will use same proxy settings when connecting the HP FTP server.

3. The Package Description Editor dialog will show the default information of the application or image component. You can use the default information or modify it, then click the **Generate** button.

 **NOTE:** If you click the **Thin Client Models** text field, a dialog will allow you to select thin client models. This value will affect the application/image deployment.

4. Select the OS to generate templates to, and click **OK**. A template will be generated in the specified OS.

 **NOTE:** If you select more than one OS, under every OS tabbed panel, one template will be generated.

5. You can see the template in the **Task Templates** tab of the task pane. The template status is **Transferring**. The component from the HP FTP Server will be transferred in the background, and it will be stored in the Master Repository, which stores files as payload of templates. The template is invalid until the transfer completes.
6. After the transfer completes successfully, the template will become valid. You can then send the generated template to the specified device.

Configuring HP FTP proxy settings

Proxy settings must be configured to use the HP FTP Software Component Browser if the system running the HPDM Console or Master Repository Controller cannot access the Internet directly.

To configure HP FTP proxy settings:

1. Select **Tools > Configuration** from the HPDM Console menu.
2. In the **Configuration Management** window, select the **HP FTP Proxy** page.
3. Select one of the following options:
 - **Use automatic configuration script**—Use this option to specify the path to a proxy settings auto-configuration file.
 - **Use manual configuration**—Use this option to manually specify proxy settings.
4. Click **Test** if you want to test the proxy settings.
5. Click **OK**.



NOTE: HPDM only supports HTTP/1.1 (connect method) and SOCK5.

12 HPDM Server Backup and Restore Tool

The HPDM Server Backup and Restore Tool can back up and restore the HPDM Server files and database, including the following items:

- Database schema and data
- [HPDM Installation Root]\Server\task folder
- [HPDM Installation Root]\Server\template folder
- [HPDM Installation Root]\Server\template_plugins folder

Before using the HPDM Server Backup and Restore Tool, note the following:

- This tool requires the credentials of a user account that has the database owner privilege.
- The HPDM Server must be version 4.5 or later.

To start the HPDM Server Backup and Restore Tool:

- ▲ Click **Start > All Programs > Hewlett-Packard > HPDM > HPDM Server Backup and Restore Tool**.

 **TIP:** In Windows Server 2012, click the **HPDM Server Backup and Restore Tool** tile on the Start screen.

The following table describes the fields available in the HPDM Server Backup and Restore Tool.

Table 12-1 HPDM Server Backup and Restore Tool fields


Field	Description
Database Type	Displays the database type, either PostgreSQL or MS SQL Server (cannot be edited)
Host	Displays the HPDM Server hostname or IP address (cannot be edited)
Port	Displays the database's listening port (cannot be edited)
Database	Displays the database name (cannot be edited)
Authentication	Allows the user to select the authentication type, depending on the database type, as follows: <ul style="list-style-type: none">• PostgreSQL—Database Authentication• MS SQL Server—Database Authentication or Windows Authentication
Username	Allows the user to enter the username for an account that has the database owner privilege
Password	Allows the user to enter the password for an account that has the database owner privilege
Backup Folder	Allows the user to specify an already-existing folder in which the backups will be stored

NOTE: The **Messages** pane on the right-hand side of the tool will display progress and results during a backup or restoration.


Backing up the HPDM Server

To back up the HPDM Server:


1. In the HPDM Server Backup and Restore Tool, select the authentication type and enter the credentials of a user account that has the database owner privilege.
2. Specify an already-existing folder in which the backup will be stored.

 **TIP:** Each backup creates a new sub-folder that contains all the backup content, so you can use the same parent folder to store all the backups.

3. Click the **Back up** button.

 **NOTE:** If the Backup Folder path points to a folder that does not already exist or to a sub-folder that corresponds to an existing backup (such as `DMBackup20121107145359`), then the **Back up** button will be disabled.

4. You will be prompted to stop the HPDM Server, which can be done by right-clicking its icon in the system tray and selecting **Stop Device Management Server**. After the HPDM Server is stopped, click **Yes** to continue.


 **CAUTION:** The prompt will not appear again if the HPDM Server is not actually stopped. If the HPDM Server is not stopped, the tool cannot ensure a successful backup, even though the process might continue and finish with a success message.

5. After the backup is complete, restart the HPDM Server by right-clicking its icon in the system tray and selecting **Start Device Management Server**.


Restoring the HPDM Server

To restore the HPDM Server:


1. In the HPDM Server Backup and Restore Tool, select the authentication type and enter the credentials of a user account that has the database owner privilege.
2. Specify the folder of an existing backup (such as `DMBackup20121107145359`).
3. Click the **Restore** button.

 **NOTE:** If the Backup Folder path does not point to an existing backup, then the **Restore** button will be disabled.

4. You will be prompted to stop the HPDM Server, which can be done by right-clicking its icon in the system tray and selecting **Stop Device Management Server**. After the HPDM Server is stopped, click **Yes** to continue.

 **CAUTION:** The prompt will not appear again if the HPDM Server is not actually stopped. If the HPDM Server is not stopped, the tool cannot ensure a successful restoration, even though the process might continue and finish with a success message.

5. After the restoration is complete, restart the HPDM Server by right-clicking its icon in the system tray and selecting **Start Device Management Server**.

 **TIP:** The HPDM Server will not restart if the restoration failed and terminated during the process. In this case, try another restoration from the same or a different backup.



NOTE: A backed-up database can only be restored to a database of the same type. For example, if you back up an SQL Server database, you can only restore it to an SQL Server, not another database type.

13 HPDM Port Check Tool

The HPDM Port Check Tool is a utility for checking the network and service connectivity and firewall port allowance between different components of HPDM. The tool is located at the following path:

```
<HPDM_Installation_Path>\Console\bin\HPDMPortCheck\
```


Copy the tool (the whole folder) to a connection initiator (a thin client), run the tool, and use it to connect to the target component. The command line syntax is as follows:

```
HPDMPortCheck <target> [flags]
```

The <target> machine will be checked. Specify an IP address or hostname.

The [flags] are described in the following table.

Flag	Description
-a	Check the HPDM Agent port (40001).
-g	Check the HPDM Gateway port (40003).
-s	Check the HPDM Server ports (1099, 40002, 40005).
-m	Check the Master Repository Controller port (40012).
-n	Check the HPDM VNC SSL Proxy port (40004).

 **NOTE:** No flag means that all ports will be checked.

See the following examples.

To check if the HPDM Gateway is reachable from the HPDM Agent, use the following command:

```
HPDMPortCheck.exe <Gateway IP address or hostname> -g
```

To check the HPDM Agent port on a machine with the IP address 192.168.1.100, use the following command:

```
HPDMPortCheck 192.168.1.100 -a
```

To check the ports of the HPDM Gateway, HPDM Server, and Master Repository Controller on a machine with the hostname "CorpServer", use the following command:

```
HPDMPortCheck CorpServer -gsm
```

For more information about specific ports, see [Port reference on page 85](#).

14 HPDM Agent polling and error logging

This chapter describes the HPDM Agent polling and error logging capabilities of HPDM.

HPDM Agent polling

The HPDM Gateway can be set to communicate with the HPDM Agent periodically and update device status (on/off) to the HPDM Server. The default interval is 0, which means this process will not occur to save net traffic. A detailed description of its two parameters can be found in the configuration GUI by hovering the mouse cursor over the text.

You may use one of the following methods to change the HPDM Agent polling settings:

- Use the HPDM Gateway configuration dialog, which can be accessed by right-clicking the HPDM Gateway tray icon.
- Send a Configure HPDM Gateway task from the HPDM Console. Choose an HPDM Gateway in the **HPDM Gateways** tab and click **Configure** or right-click the HPDM Gateway and select **Configure HPDM Gateway**.

Error logging

HPDM implements error logging for each of the individual components. The errors are logged according to levels. When you set the logging level of a component, errors of that level and higher are logged.

HPDM Agent logging

Table 14-1 HPDM Agent logging

Level	Description
INFORMATION	Logs of running information, contains no errors
WARNING	Low-level error
ERROR	Significant errors

To change the logging level for the HPDM Agent, either set the log level through the Configure HPDM Agent dialog on the device or send a Configure Agent task to the target device(s).

HPDM Gateway logging

Table 14-2 HPDM Gateway logging

Level	Description
TRACE	Some trace logs; for example, number of HPDM Agents
DEBUG	Internal debug logging
INFO	Log of some report content

Table 14-2 HPDM Gateway logging (continued)

Level	Description
WARN	Low-level error; for example, HPDM Gateway failed to connect to Console/Server at this time, maybe Server is not ready, but HPDM Gateway will retry later
ERROR	Significant errors
FATAL	High-level error; the error will usually prevent HPDM Gateway from running normally

To change the logging level for an HPDM Gateway, use one of the following methods:

- Use the HPDM Gateway configuration dialog, which can be accessed from right-clicking the HPDM Gateway tray icon.
- Send a Configure HPDM Gateway task from the HPDM Console. Choose an HPDM Gateway in the **HPDM Gateways** tab and click **Configure** or right-click the HPDM Gateway and select **Configure HPDM Gateway**.

HPDM Server and HPDM Console logging

Table 14-3 HPDM Server and HPDM Console logging

Level	Description
DEBUG	Low-level debugging information
INFO	Logs of running information, contains no errors
WARN	Logs with warning, means something unexpected happened
FATAL	Fatal errors


To change the logging level of the HPDM Server:

- ▲ Change the value of `hpdn.log.level` in the file `/Server/conf/server.conf`, which is located in the HPDM installation folder.

Log files for the HPDM Server are located in `/Server/logs/`.

To change the logging level of the HPDM Console:

- ▲ Change the value of `hpdn.log.level` in the file `/Console/conf/server.conf`, which is located at `%programdata%/Hewlett-Packard/HP Device Manager`.

 **TIP:** The `%programdata%` folder is an accessible folder under the Windows UAC policy. It refers to either `C:\ProgramData` or `C:\Documents and Settings\All Users\Application Data`, depending on the operating system.

Log files for the HPDM Console are located in `/Console/logs/`.

Master Repository Controller logging

Level	Description
INFORMATION	Logs of running information, contains no errors
WARNING	Low-level error
ERROR	Significant errors

To change the logging level of the Master Repository Controller:

- ▲ Change the value of `LogLevel` in the file `/MasterRepositoryController/Controller.conf`, which is located in the HPDM installation folder.

The log file of the Master Repository Controller is located in `/MasterRepositoryController/log/`.

A Template reference

HPDM separates templates into the following categories:

- [File and Registry](#)
- [Agent](#)
- [Connections](#)
- [Imaging](#)
- [Operations](#)
- [Settings](#)
- [Template Sequence](#)

File and Registry

Table A-1 File and Registry templates

Template	Description
_File and Registry	<p>This template enables you to create a sequence using these sub-templates:</p> <ul style="list-style-type: none">• Set a registry key.• Capture a file from a device.• Deploy a file to a device.• Execute a command on a device.• Delete files on a device.• Pause a sequence.• Add or remove a program record on a device.• Execute a script on a device.
_Get Registry	<p>This template enables you to upload one or more keys from a device's registry.</p>

Agent

Table A-2 HPDM Agent templates

Template	Description
_Configure Agent	<p>This template enables you to configure the HPDM Agent on the target device.</p> <p>NOTE: You can no longer set the current HPDM Gateway by typing 'cur-gateway, back-gateway' in the Backup HPDM Gateway field.</p>

Table A-2 HPDM Agent templates (continued)

Template	Description
_Configure Task Deferment	This template enables you to configure task deferment settings on target devices.
_Update Agent	This template updates HPDM Agent on the target devices to the version stored in your repository. The payload will be synchronized to the mapped repository automatically before the task is sent to the target devices.

Connections

Table A-3 Connection templates

Template	Description
_Pull Connection Configuration	This template will extract the specified connection settings from a device and create a new template to push those connections to other devices.
_Capture Connections	This template will capture connections from PCoIP zero clients.
_Deploy Connections	This template will deploy connections to PCoIP zero clients.

Imaging

Table A-4 Imaging templates

Template	Description
_Capture Image	This template will capture an image from the target device and upload it to the Master Repository. It will also create a new Deploy Image template to install the image to other devices. This template can only be sent to a single device at a time.
_PXE Capture	This template will capture an image with PXE service from the device and upload it to the Master Repository. It will also create a new PXE deploy template to install the image to other devices. This template can only be sent to a single device at a time. NOTE: This template is not available for thin clients running HP Smart Zero Core.
_Update Firmware	This template will update the firmware of PCoIP zero clients. You need to import a firmware file to generate this template.

Operations

Table A-5 Operation templates

Template	Description
_Factory Reset	This template resets the targeted devices to their original configuration. The effects of this differ according to the operating system of the device. The reset to Current Profile option is unique to the HP ThinPro operating system.
_Get Asset Information	This template extracts a full asset report from the targeted devices.
_Reboot Device	This template reboots the targeted devices. A warning message will be displayed on the devices' screen for 15 seconds before the reboot actually takes place.

Table A-5 Operation templates (continued)

Template	Description
_Reverse Shadow Device	This template causes the HPDM Agent on a targeted device to connect to the VNC viewer bundled with the HPDM Console by SSL tunnel. This template is not available for the HPCE thin clients.
_Send Message	This template sends a customized message to targeted devices. This template is not available for HP ThinPro thin clients.
_Shadow Device	This template causes VNC viewer bundled with the HPDM Console to connect to the VNC service on a targeted device by SSL tunnel.
_Shutdown Device	This template shuts down the targeted devices. A warning message will be displayed on the devices' screen for 15 seconds before the reboot actually takes place.
_Start Resource Monitor	<p>This template starts the Resource Monitor for the target device. This template can only be sent to a single device at a time and is not available for HP ThinPro thin clients.</p> <p>When this template is sent to a device successfully, a Resource Monitor dialog will pop up. You can monitor Process, Performance, and Network Disk information.</p>
_Wake Up Device	This template will cause the HPDM Gateway associated with the targeted devices to send them a Wake On LAN message. The Wake device works not only for devices in the same subnet with HPDM Gateway, but also for devices that are not in the same subnet of HPDM Gateway, if the subnet has at least one online HPDM Agent. We can wake up devices behind NAT, if the subnet has at least one online HPDM Agent. During timeout, HPDM Gateway reports the unfinished part as failure.

Settings

Table A-6 Setting templates

Template	Description
_Apply Settings	This template enables you to create a set of custom settings and deploy them to one or more devices.
_Clone Settings	This template enables you to copy a selection of custom settings from one device and deploy them to other devices.
_Deploy Profile	This template is used to configure a profile and deploy it to thin clients running HP Smart Zero Core.
_Enroll Certificate With SCEP	This template enables you to enroll certificates with SCEP on normal thin clients.
_Hostname and IP	<p>This template enables you to change the hostname and IP address of one or more devices. There are two options:</p> <ul style="list-style-type: none"> • Modify specified devices—Only functions when you drag it to one or more target devices. • Set with pattern—Changes hostname and IP with the same pattern.
_Set Domain	The _Set Domain template allows devices to join a domain or a workgroup.
_Set Password	<p>This template enables you to set a password for one or more users on one or more devices. You can check hide password check box to hide the password, or clear the check box it to show the password.</p> <p>NOTE: This template is not available for thin clients running HP Smart Zero Core.</p>

Table A-6 Setting templates (continued)

Template	Description
_Take TPM Ownership	This template enables/activates TPM and sets the TPM owner password and BIOS setup password to take the TPM ownership of the selected devices.
_Write Filter Settings	This template enables you to change the Write Filter settings for a device.

Template Sequence

Table A-7 Template Sequence templates

Template	Description
_Template Sequence	Template sequences are used to combine a set of templates to be executed in a task with a specified order and conditions.

B Port reference

The following sections list the ports used by HPDM:

- [HPDM Console ports](#)
- [HPDM Server ports](#)
- [HPDM Gateway ports](#)
- [HPDM Agent ports](#)
- [Repository ports](#)

HPDM Console ports

Table B-1 HPDM Console ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
5500	SSL VNC Proxy (bundled with HPDM Console)	VNC Viewer (bundled with HPDM Console)	TCP (loopback)	VNC Viewer in Listen Mode (reverse VNC)
5900	VNC Viewer (bundled with HPDM Console)	SSL VNC Proxy (bundled with HPDM Console)	TCP (loopback)	VNC Viewer in Listen Mode (reverse VNC)
40004	SSL VNC Proxy (bundled with HPDM Agent)	VNC Proxy (bundled with HPDM Console)	TCP	SSL VNC Proxy in Listen Mode (reverse VNC)

Table B-2 HPDM Console ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Console	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via the HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	HPDM Console	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via the HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
137	HPDM Console	NetBIOS Name Service	UDP	Allows NetBIOS Name Resolution
138	HPDM Console	NetBIOS Datagram Service	UDP	Allows NetBIOS Datagram transmission and reception

Table B-2 HPDM Console ports (outbound) (continued)

Receiver port	Sender	Receiver	Protocol	Purpose
139	HPDM Console	NetBIOS Session Service	TCP	Allows NetBIOS Session Services connections
445	HPDM Console	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
989 & 990	HPDM Console	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via the HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.
1099	HPDM Console	HPDM Server	TCP	Allows the HPDM Console to query the RMI Registry
5500	SSL VNC Proxy (bundled with HPDM Console)	VNC View (bundled with HPDM Console)	TCP (loopback)	VNC Viewer in Listen Mode (reverse VNC)
5900	VNC Viewer (bundled with HPDM Console)	VNC Proxy (bundled with HPDM Console)	TCP (loopback)	VNC Shadow
40002	HPDM Console	HPDM Server	TCP	Allows the HPDM Console to call remote objects on the HPDM Server by RMI
40004	SSL VNC Proxy (bundled with HPDM Console)	VNC Proxy (bundled with HPDM Agent)	TCP	Port for SSL VNC connection

HPDM Server ports

Table B-3 HPDM Server ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
1099	HPDM Console	HPDM Server	TCP	Allows the HPDM Console to query the RMI Registry
40002	HPDM Console	HPDM Server	TCP	Allows the HPDM Console to call remote objects on the HPDM Server by RMI
40005	HPDM Gateway	HPDM Server	TCP	Allows the HPDM Gateway to send reports to the HPDM Server
40006	HPDM Server	PostgreSQL (bundled with HPDM Server)	TCP (loopback)	The default database PostgreSQL listening port (only needed when PostgreSQL is used)
40009	HPDM Agent	HPDM Server	TCP	Allows the HPDM Agent to send resource information (CPU, RAM, disk I/O, network I/O, processes, etc.) to the HPDM Server. The HPDM Server will send a stop process command to the HPDM Agent.

Table B-4 HPDM Server ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
40000	HPDM Server	HPDM Gateway	UDP	Allows the HPDM Server to poll the HPDM Gateway
40003	HPDM Server	HPDM Server	TCP	Allows the HPDM Server to send tasks to the HPDM Gateway
40006	HPDM Server	PostgreSQL (bundled with HPDM Server)	TCP (loopback)	The default database PostgreSQL listening port (only needed when PostgreSQL is used)
40012	HPDM Server	Master Repository Controller	TCP	Allows the HPDM Server to talk to the Master Repository Controller to manage the Master Repository

HPDM Gateway ports

Table B-5 HPDM Gateway ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
67	PXE Client (thin client side)	HPDM PXE Server (bundled with HPDM Gateway)	UDP	PXE bootstrap
69	PXE Client (thin client side)	HPDM PXE Server (bundled with HPDM Gateway)	UDP	TFTP (Trivial File Transfer Protocol)
4011	PXE Client (thin client side)	Proxy DHCP Service (third-party software)	UDP	Proxy DHCP Service (an alternative to port 67 if port 67 is not available)
40000	HPDM Server HPDM Agent	HPDM Gateway	UDP	Allows the HPDM Server and HPDM Agent to poll the HPDM Gateway
40003	HPDM Server HPDM Agent	HPDM Gateway	TCP	Allows the HPDM Server to send tasks to the HPDM Gateway Allows the HPDM Agent to send reports to the HPDM Gateway
40008	HPDM Gateway	HPDM Gateway Controller	TCP	Allows the HPDM Gateway to notify the HPDM Gateway Controller there are other gateways running in the same subnet

Table B-6 HPDM Gateway ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Gateway	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via the HPDM Console. If you do not use the default ports for your FTP server,

Table B-6 HPDM Gateway ports (outbound) (continued)

Receiver port	Sender	Receiver	Protocol	Purpose
				please configure the firewall appropriately.
22	HPDM Gateway	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via the HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
68	HPDM PXE Server (bundled with HPDM Gateway)	HPDM Imaging Mini Linux Tool (client-side)	UDP	PXE bootstrap
137	HPDM Gateway	NetBIOS Name Service	UDP	Allows NetBIOS Name Resolution
138	HPDM Gateway	NetBIOS Datagram Service	UDP	Allows NetBIOS Datagram transmission and reception
139	HPDM Gateway	NetBIOS Session Service	TCP	Allows NetBIOS Session Services connections
445	HPDM Gateway	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
989 & 990	HPDM Gateway	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via the HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.
40001	HPDM Gateway	HPDM Agent	TCP	Allows the HPDM Gateway to send tasks to the HPDM Agent
40001	HPDM Gateway	HPDM Agent	UDP	Allows the HPDM Agent to receive replies of broadcasting from the HPDM Gateway
40005	HPDM Gateway	HPDM Server	TCP	Allows the HPDM Gateway to send reports to the HPDM Server
40008	HPDM Gateway	HPDM Gateway Controller	TCP (loopback)	Allows the HPDM Gateway to notify the HPDM Gateway Controller there are other gateways running in the same subnet
50000	HPDM Gateway	PCoIP zero clients	TCP	Allows the HPDM Gateway to send tasks to PCoIP zero clients

HPDM Agent ports

Table B-7 HPDM Agent ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
68	DHCP Server	HPDM Agent	UDP	Receive replies for DHCP options

Table B-7 HPDM Agent ports (inbound) (continued)

Receiver port	Sender	Receiver	Protocol	Purpose
68	HPDM PXE Server (bundled with HPDM Gateway)	HPDM Imaging Mini Linux Tool (client-side)	UDP	PXE bootstrap
5500	Windows platform : VNC Server (client-side)	Windows platform : SSL VNC Proxy (bundled with HPDM Agent)	TCP (loopback)	SSL VNC Proxy in Listen Mode (reverse VNC)
5900	SSL VNC Proxy (bundled with HPDM Console)	VNC Server (client-side)	TCP (loopback)	VNC Shadow
40001	HPDM Gateway	HPDM Agent	TCP	Allows the HPDM Gateway to send tasks to the HPDM Agent
40001	HPDM Gateway	HPDM Agent	UDP	Allows the HPDM Agent to receive replies of broadcasting from the HPDM Gateway
40004	SSL VNC Proxy (bundled with HPDM Console)	SSL VNC Proxy (bundled with HPDM Agent)	TCP	VNC SSL Proxy in Listen Mode on the HPDM Agent

Table B-8 HPDM Agent ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Agent	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via the HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	HPDM Agent	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via the HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
67	PXE client (client-side)	HPDM PXE server (bundled with HPDM Gateway)	UDP	PXE bootstrap
67	HPDM Agent	DHCP server	UDP	Allows the HPDM Agent to send DHCP option requests
69	PXE client (client-side)	HPDM PXE server (bundled with HPDM Gateway)	UDP	TFTP (Trivial File Transfer Protocol)
137	HPDM Agent	NetBIOS Name Service	UDP	Allows NetBIOS Name Resolution
138	HPDM Agent	NetBIOS Datagram Service	UDP	Allows NetBIOS Datagram transmission and reception

Table B-8 HPDM Agent ports (outbound) (continued)

Receiver port	Sender	Receiver	Protocol	Purpose
139	HPDM Agent	NetBIOS Session Service	TCP	Allows NetBIOS Session Services connections
445	HPDM Agent	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
5500	Windows platform: VNC Server (client-side)	Windows platform : SSL VNC Proxy (bundled with HPDM Agent)	TCP (loopback)	SSL VNC Viewer in Listen Mode (reverse VNC)
5900	SSL VNC Viewer (bundled with HPDM Console)	VNC Proxy (client-side)	TCP (loopback)	VNC Shadow
989 & 990	HPDM Console	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via the HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.
4011	PXE client (client-side)	Proxy DHCP service (third-party software)	UDP	Proxy DHCP service (an alternative to port 67 if port 67 is not available)
40000	HPDM Agent	HPDM Gateway	UDP	Allows the HPDM Agent to poll the HPDM Gateway
40003	HPDM Agent	HPDM Gateway	TCP	Allows the HPDM Agent to send reports to the HPDM Gateway
40004	Windows: SSL VNC Proxy (bundled with HPDM Agent); HP ThinPro: X11VNC (bundled with platform)	SSL VNC Proxy (bundled with HPDM Console)	TCP	SSL VNC Proxy in Listen Mode (reverse VNC)
40009	HPDM Agent	HPDM Server	TCP	Allows the HPDM Agent to send resource information (CPU, RAM, disk I/O, network I/O, processes, etc.) to the HPDM Server. The HPDM Server will send a stop process command to the HPDM Agent.

Repository ports

Table B-9 Repository ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Console HPDM Gateway HPDM Agent Master Repository Controller	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via the HPDM Console. If you do not use the default ports for your FTP server,

Table B-9 Repository ports (inbound) (continued)

Receiver port	Sender	Receiver	Protocol	Purpose
				please configure the firewall appropriately.
22	HPDM Console HPDM Gateway HPDM Agent Master Repository Controller	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via the HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
137	HPDM Console HPDM Gateway HPDM Agent Master Repository Controller	NetBIOS Name Service	UDP	For File and Printer Sharing to allow NetBIOS Name Resolution
138	HPDM Console HPDM Gateway HPDM Agent Master Repository Controller	NetBIOS Datagram Service	UDP	For File and Printer Sharing to allow NetBIOS Datagram transmission and reception
139	HPDM Console HPDM Gateway HPDM Agent Master Repository Controller	NetBIOS Session Service	TCP	For File and Printer Sharing to allow NetBIOS Session Service connections
445	HPDM Console HPDM Gateway HPDM Agent Master Repository Controller	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
989 & 990	HPDM Console HPDM Gateway HPDM Agent Master Repository Controller	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via the HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.
40012	HPDM Server	Master Repository Controller	TCP	Allows the HPDM Server to talk to the Master Repository Controller to manage the Master Repository (this port is for the Master Repository only)

Table B-10 Repository ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	Master Repository Controller	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via the HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	Master Repository Controller	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via the HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
137	Master Repository Controller	NetBIOS Name Service	UDP	For File and Printer Sharing to allow NetBIOS Name Resolution.
138	Master Repository Controller	NetBIOS Datagram Service	UDP	For File and Printer Sharing to allow NetBIOS Datagram transmission and reception.
139	Master Repository Controller	NetBIOS Session Service	TCP	For File and Printer Sharing to allow NetBIOS Session Service connections.
445	Master Repository Controller	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes.
989 & 990	Master Repository Controller	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via the HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.

Index

A

- Active Directory 62
- authentication key
 - exporting 65
 - importing 66
 - updating 65
 - viewing 66
- authentication management 65

C

- Child Repositories
 - configuring 57
 - deleting 57
 - description 4
- connections
 - capturing 40
 - deploying 40

D

- device discovery 18
 - manual registration 21
 - walking with IP list 21
 - walking with IP range 20
- device filters
 - creating 37
 - editing 37
- devices
 - definition 5
 - deleting 35
 - grouping 35
 - management 34
 - network, checking connection status 38
 - printing information about 38
 - properties, displaying 16
 - reporting 68
 - rules, defining 33
 - settings, applying 40
 - settings, cloning 40
 - shadowing 39
 - tasks, defining 29
 - viewing 34
- DHCP 36
 - server, configuring for PXE imaging 53

- tag 202 18
- tag 203 35, 36

F

- file and registry template 41
 - capture files 42
 - command 44
 - delete files 43
 - deploy files 42
 - pause 45
 - program record 45
 - registry 43
 - script 46
- filters
 - device, editing 37
 - security 37

G

- grouping devices 35

H

- HP FTP Software Component
 - Browser 72
- HPDM Agent
 - Agent 83
 - description 3
- HPDM Console
 - description 3
 - HPDM Gateway tab 15
 - log in 13
 - operating system tabs 14
 - overview 13
 - system requirements 8
- HPDM Gateway
 - access control 66
 - description 3
 - system requirements 7
- HPDM installation 12
- HPDM overview 2
- HPDM Server 33
 - description 3
 - system requirements 7
- HPDM Server Backup and Restore Tool 74

- HPDM updates
 - documentation 5
 - software 5

I

- imaging operations 48
- imaging support matrix 49
- imaging, with PXE. *See* PXE imaging
- imaging, without PXE
 - capturing 50
 - deploying 51
- IP scope, configuring 21

K

- key management 65

L

- LDAP server 62
- log in, HPDM Console 13

M

- Master Repository
 - configuring 56
 - description 4
- Master Repository Controller
 - system requirements 11

N

- network requirements 11

O

- opening VNC viewer 32
- overview 1

P

- package, definition 5
- permissions assigning to groups 61
- port requirements 11
- ports, list of 85
- power management 39
- PXE imaging
 - capturing 52
 - configuring a DHCP server 53

- configuring routers 55
- deploying 53
- on legacy Neoware devices 55

PXE, definition 5

R

reports

- adding template 67
- generating using 67
- importing plug-in file 67
- management 67

repositories 56

- content management 58
- description 4
- exporting 57
- importing 57
- management 56
- synchronizing 58

result template, opening 32

routers, configuring for PXE

- imaging 55

rules, definition 5

S

security

- authentication management 65
- filter 37
- HPDM Gateway access control 66
- key management 65
- management 60
- user authentication 62

shadowing 32

shadowing devices 39

status snapshot 71

status walker 70

system requirements

- HPDM Console 8
- HPDM Gateway 7
- HPDM Server 7
- Master Repository Controller 11
- network 11
- ports 11

T

task templates

- adding to favorites 24
- creating/editing 24

- definition 5
- importing/exporting 24
- list of 81
- management 23

tasks 23

- configuring parameters 30
- continuing 31
- deferment 30
- definition 5
- deleting 32
- displaying logs 32
- displaying properties 30
- displaying success rate 32
- from all users, viewing 33
- icons 28
- management 28
- parameters 29
- pausing 31
- performing 28
- resending 32
- status icons 28

template sequences

- advanced 27
- basic 27
- definition 5

terms and definitions 5

U

user management 60

users

- adding 60
- assigning to groups 60, 61
- authentication 62
- changing password 60
- deleting 60
- importing 63

W

write filters, definition 5