# 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 Console requirements .................................................................................................. 7  
      HPDM Server requirements .................................................................................................... 7  
      HPDM Gateway requirements ............................................................................................... 8  
      HPDM Agent requirements ..................................................................................................... 8  
      Master Repository Controller requirements ......................................................................... 8  
      Repository requirements ........................................................................................................ 9  
      Network requirements ............................................................................................................ 9  
   Installing HPDM .......................................................................................................................... 10  
      Installing an HPDM 4.5 Service Pack .................................................................................. 11  
   Using the HPDM Console ............................................................................................................ 11  
      Logging in to the HPDM Console ....................................................................................... 11  
      HPDM Console overview ..................................................................................................... 11  
         Operating system tabs ........................................................................................................... 12  
      HPDM Gateway tab .............................................................................................................. 13  
   Discovering client systems .......................................................................................................... 13  
   Displaying device properties ........................................................................................................ 14  
      Basic asset information ......................................................................................................... 14  
      Collecting complete asset information ................................................................................ 15  
      Displaying complete client asset information ...................................................................... 15  
   Keeping the HPDM Agent updated on client systems ................................................................. 15  

3 Client discovery ........................................................................................................................... 16  
   Discovering a client from the client-side ................................................................................... 16
Discovering a client from the server-side ........................................................................................................ 17
  Using the Walking With IP Range method ...................................................................................................... 17
    Configuring an IP scope .............................................................................................................................. 17
  Using the Walking With IP List method ........................................................................................................ 17
Manually registering a client .......................................................................................................................... 18

4 Using tasks .................................................................................................................................................. 19
  Task templates .............................................................................................................................................. 19
    Creating and editing task templates ........................................................................................................ 20
    Adding a template to the Favorites ........................................................................................................... 20
    Removing a template plugin ..................................................................................................................... 20
    Using Template Sequence templates .................................................................................................... 20
  Importing and exporting task templates ..................................................................................................... 21
  Tasks ............................................................................................................................................................. 23
    Performing a task ........................................................................................................................................ 23
    Task status icons ....................................................................................................................................... 23
    Task settings .............................................................................................................................................. 24
    Task parameters ....................................................................................................................................... 24
      Manual tasks ......................................................................................................................................... 24
      Valid Time, Timeout & WOL .................................................................................................................... 25
      Target Device List ................................................................................................................................. 25
      Schedule & Batch Control ..................................................................................................................... 25
  Applying tasks to devices ............................................................................................................................. 25
  Task deferment ............................................................................................................................................ 26
  Displaying task properties ............................................................................................................................ 26
  Configuring task parameters ......................................................................................................................... 26
  Pausing tasks ............................................................................................................................................... 27
  Continuing tasks .......................................................................................................................................... 27
  Resending tasks .......................................................................................................................................... 27
  Canceling tasks ........................................................................................................................................... 27
  Deleting tasks ............................................................................................................................................... 27
  Displaying task logs .................................................................................................................................... 28
  Opening VNC Viewer for shadowing ........................................................................................................... 28
  Opening a Result Template .......................................................................................................................... 28
  Task rules ..................................................................................................................................................... 28
    Adding a new rule ..................................................................................................................................... 28

5 Device management .................................................................................................................................... 30
  Device icons ................................................................................................................................................... 30
  Deleting devices .......................................................................................................................................... 31
  Grouping devices ......................................................................................................................................... 31
6 Thin client imaging operations ................................................................. 36

Introduction .................................................................................................................. 36
Client BIOS settings for PXE ........................................................................................ 36
Capturing an image from a client with PXE .............................................................. 36
Deploying an image to a client with PXE ................................................................. 37
Capturing an image from an HP thin client ............................................................... 37
Deploying images ........................................................................................................ 38

7 Managing client operating systems ................................................................. 41

Renaming devices (hostname) .................................................................................... 41
Changing connection settings .................................................................................. 41
Changing device settings .......................................................................................... 41
Cloning settings ......................................................................................................... 42
Applying settings ........................................................................................................ 42
Adding devices using MAC addresses ...................................................................... 43
Using File and Registry templates ............................................................................ 43
Merging File and Registry templates ........................................................................ 45
Changing registry settings ......................................................................................... 46
Getting registry settings ........................................................................................... 46
Editing registry settings ............................................................................................ 46
Copying files .............................................................................................................. 47
Capturing files .......................................................................................................... 47
Deploying files .......................................................................................................... 48
Program Record ......................................................................................................... 48
Remote command execution ...................................................................................... 49
8 Repository management ................................................................................................................................. 50

- Initializing from wizard ........................................................................................................................ 50
- Selecting the file protocol to use ........................................................................................................ 50
- Configuring the Master Repository ..................................................................................................... 50
- Configuring the Child Repositories ..................................................................................................... 51
- Deleting Child Repositories ................................................................................................................ 51
- Exporting repositories .......................................................................................................................... 51
- Importing repositories .......................................................................................................................... 51
- Synchronizing repositories .................................................................................................................. 51
- Content management ......................................................................................................................... 51
  - Viewing detailed payload information ................................................................................ 52
  - Deleting contents from the Master Repository ........................................................................ 52
  - Downloading contents from the Files Captured category ................................................... 52
  - Syncing content to the child repositories ................................................................................ 52
- Repository mapping ........................................................................................................................... 52
  - Batch mapping ........................................................................................................................... 52
  - Per device mapping .................................................................................................................... 53

9 Security management ..................................................................................................................................... 54

- User management .............................................................................................................................. 54
  - Adding users .............................................................................................................................. 54
  - Deleting users ......................................................................................................................... 54
  - Assigning users to groups ........................................................................................................ 54
  - Changing a user's password .................................................................................................... 54
  - Assigning Security Filters to Users ........................................................................................ 55
  - Adding a group ......................................................................................................................... 55
  - Assigning permissions to groups ............................................................................................. 55
  - Assigning users to groups ......................................................................................................... 55
  - Assigning security filters to groups .......................................................................................... 55
  - Deleting groups ....................................................................................................................... 56
  - User authentication with LDAP and Active Directory ........................................................ 56
    - Configuration .................................................................................................................... 56
    - Importing users and groups ............................................................................................... 57
- Authentication management ............................................................................................................. 59
  - Key management ....................................................................................................................... 59
  - HPDM Gateway access control .................................................................................................. 60
10 Report management ..................................................................................................................................... 61
   Adding a Report template .......................................................................................................................... 61
   Importing a report plug-in file ............................................................................................................... 61
   Generating a report using a Report template .......................................................................................... 61
   Producing reports ................................................................................................................................... 62
      HPDM Gateway report ......................................................................................................................... 62
      Device Information report ................................................................................................................ 62
      Device Task report .......................................................................................................................... 62
      Task report ........................................................................................................................................ 62
      Task Status report .......................................................................................................................... 63
      Task Log report .................................................................................................................................. 63

11 Template reference ....................................................................................................................................... 64
   File and Registry ................................................................................................................................ 64
      _File and registry .............................................................................................................................. 64
      _Get registry .................................................................................................................................... 64
   HPDM Agent ...................................................................................................................................... 64
      _Configure Agent ............................................................................................................................ 64
      _Configure Task Deferment .............................................................................................................. 64
      _Update Agent .............................................................................................................................. 64
   Connections ....................................................................................................................................... 65
      _Pull Connection Information .......................................................................................................... 65
   Imaging ............................................................................................................................................... 65
      _Capture Image .............................................................................................................................. 65
      _PXE Capture .................................................................................................................................. 65
   Operations .......................................................................................................................................... 65
      _Factory Reset ............................................................................................................................... 65
      _Get Asset Information .................................................................................................................... 65
      _Reboot Device ............................................................................................................................... 65
      _Reverse Shadow Device ................................................................................................................ 65
      _Send Message ............................................................................................................................... 65
      _Shadow Device ............................................................................................................................. 65
      _Shutdown Device .......................................................................................................................... 66
      _Start Resource Monitor ................................................................................................................. 66
      _Wake Up Device ........................................................................................................................... 66
   Settings .............................................................................................................................................. 66
      _Apply Settings ............................................................................................................................... 66
      _Clone Settings ............................................................................................................................... 66
      _Hostname and IP ............................................................................................................................. 66
      _Set Password ................................................................................................................................. 66
      _Write Filter Settings ....................................................................................................................... 66
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 thin client 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:

- Thin client 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 Repositories**—Holds 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>A device (or client) refers to a device managed by HPDM, such as a thin client.</td>
</tr>
<tr>
<td>Packages</td>
<td>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. The name of the description file follows the convention PackageName-C checksumString.desc. The checksum is computed from all payload files in alphabetical sequence of filename or folder name with depth-first traversal.</td>
</tr>
<tr>
<td>PXE</td>
<td>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. HPDM utilizes PXE to execute thin client image extraction and distribution.</td>
</tr>
<tr>
<td>Rules</td>
<td>Rules enable you to automate the execution of tasks. Each rule has three parts:</td>
</tr>
<tr>
<td></td>
<td>● Filter—Defines which client devices the rule applies to</td>
</tr>
<tr>
<td></td>
<td>● Trigger—Defines when the rule is executed</td>
</tr>
<tr>
<td></td>
<td>● Template—Defines what operation should be performed on the client devices</td>
</tr>
<tr>
<td>Tasks</td>
<td>Tasks are the scheduled actions 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 client devices.</td>
</tr>
<tr>
<td>Task templates</td>
<td>Task templates (or templates) are XML files that define the configuration changes or software updates that administrators want the client devices to perform. HPDM provides a variety of built-in task templates for managing client devices.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Template sequences</td>
<td>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.</td>
</tr>
<tr>
<td>Write filters</td>
<td>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. Write filters come in two varieties:</td>
</tr>
<tr>
<td></td>
<td>● Enhanced Write Filter (EWF)</td>
</tr>
<tr>
<td></td>
<td>● File-Based Write Filter (FBWF)</td>
</tr>
</tbody>
</table>

### Finding the latest updates

To find the latest documentation and software updates:

- or —
- Documentation—Go to [http://www.hp.com/support](http://www.hp.com/support) and search for HP Device Manager.

**NOTE:** Check the Revision History tab to ensure you are downloading the latest version of HPDM.
This chapter discusses the following topics:

- System requirements
- Installing HPDM
- Using the HPDM Console
- Discovering client systems
- Displaying device properties
- Keeping the HPDM Agent updated on client systems
System requirements

The following sections describe the minimum system requirements for HPDM.

HPDM Console requirements

Table 2-1 HPDM Console requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows Server 2003 with Service Pack 2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2 with Service Pack 2 (32- and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 with Service Pack 2 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 with Service Pack 1 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows XP Professional with Service Pack 3 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows 7 Enterprise with Service Pack 1 (64-bit)</td>
</tr>
<tr>
<td>Third-party software</td>
<td>Java Runtime Environment version 6 update 2</td>
</tr>
<tr>
<td>NOTE:</td>
<td>Java Runtime Environment is installed with HPDM.</td>
</tr>
<tr>
<td>Hardware</td>
<td>Pentium® III or greater</td>
</tr>
<tr>
<td></td>
<td>512 MB RAM</td>
</tr>
<tr>
<td></td>
<td>256 MB free disk space</td>
</tr>
</tbody>
</table>

HPDM Server requirements

Table 2-2 HPDM Server requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows Server 2003 with Service Pack 2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2 with Service Pack 2 (32- and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 with Service Pack 2 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 with Service Pack 1 (64-bit)</td>
</tr>
<tr>
<td>Third-party software</td>
<td>Java Runtime Environment version 6 update 2</td>
</tr>
<tr>
<td>NOTE:</td>
<td>Java Runtime Environment is installed with HPDM.</td>
</tr>
<tr>
<td></td>
<td>One of the following database management systems (DBMS):</td>
</tr>
<tr>
<td></td>
<td>● Microsoft SQL Server 2005 or later</td>
</tr>
<tr>
<td></td>
<td>● PostgreSQL 8.3 or later (bundled with installer)</td>
</tr>
<tr>
<td>NOTE:</td>
<td>PostgreSQL is included in the HPDM distribution. If you select PostgreSQL as your database, it will be installed from the installation media.</td>
</tr>
<tr>
<td>Hardware</td>
<td>Pentium® III or greater</td>
</tr>
<tr>
<td></td>
<td>512 MB RAM</td>
</tr>
<tr>
<td></td>
<td>512 MB free disk space</td>
</tr>
</tbody>
</table>
HPDM Gateway requirements

Table 2-3 HPDM Gateway requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows Server 2003 with Service Pack 2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2 with Service Pack 2 (32- and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 with Service Pack 2 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 with Service Pack 1 (64-bit)</td>
</tr>
<tr>
<td>Hardware</td>
<td>Pentium® III or greater</td>
</tr>
<tr>
<td></td>
<td>512 MB RAM</td>
</tr>
<tr>
<td></td>
<td>512 MB free disk space</td>
</tr>
</tbody>
</table>

HPDM Agent requirements

Table 2-4 HPDM Agent requirements

<table>
<thead>
<tr>
<th>Operating system</th>
<th>HP thin client hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP XPe*, WES09, WES7E, WES7P</td>
<td>t610, t510, t505, t5740, t5740e, t5570, t5570e, t5400, gt7720, 6360t, mt40</td>
</tr>
<tr>
<td>HP CE 6*</td>
<td>t510, t5550</td>
</tr>
<tr>
<td>HP ThinPro 4</td>
<td>t610, t510, t505, t5745, t5565</td>
</tr>
<tr>
<td>HP ThinPro 3</td>
<td>t5745, t5565</td>
</tr>
<tr>
<td>HP Smart Zero Core</td>
<td>t610, t510, t410, t410 All-in-One, t5565z, t5335z</td>
</tr>
</tbody>
</table>

NOTE: HPDM 4.5 only provides limited support for the operating systems marked with an asterisk. Some features may not work with these operating systems. The latest stable release that has been fully tested with these operating systems is HPDM 4.4 (installer version: 4.4.12440, built on 08/29/2011).

NOTE: Client devices should have a minimum of 2 MB of free disk space.

Master Repository Controller requirements

Table 2-5 Master Repository Controller requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows Server 2003 R2 with Service Pack 2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 with Service Pack 1 (64-bit)</td>
</tr>
<tr>
<td>Hardware</td>
<td>Pentium® III or greater</td>
</tr>
<tr>
<td></td>
<td>512 MB RAM</td>
</tr>
<tr>
<td></td>
<td>2 GB free disk space</td>
</tr>
</tbody>
</table>

NOTE: The above hardware describes the minimum required for the Master Repository. If there will be a large number of imaging or file-copying operations, then it is recommended to use a more powerful system with more free disk space.
Repository requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>FTP, FTPS, SFTP, or SMB</td>
</tr>
<tr>
<td>Recommended third-party FTP servers</td>
<td>FileZilla</td>
</tr>
<tr>
<td></td>
<td>Microsoft Internet Information Server (IIS) 6.0 or later</td>
</tr>
<tr>
<td></td>
<td>freeSSHd</td>
</tr>
</tbody>
</table>

Network requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>HPDM only supports IPv4 networks.</td>
</tr>
<tr>
<td></td>
<td>HPDM can image thin clients using either PXE or non-PXE (preferred) methods. If PXE imaging is desired, then you must make sure there are no other PXE services running on the network.</td>
</tr>
<tr>
<td></td>
<td>A number of UDP and TCP ports are required for client/server communication. See Ports on page 75 for a list of standard and custom ports required.</td>
</tr>
<tr>
<td></td>
<td>If you are using a server behind a firewall, you must add ports 1099 and 40002 to the exception ports in the firewall settings.</td>
</tr>
<tr>
<td></td>
<td>If you are using an ISC DHCP server, it must be running at least version 3.0.</td>
</tr>
</tbody>
</table>
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.


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 Ports on page 75 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.
In some cases, there will be other network configuration changes that may need to be made. See Network configuration on page 72 for more information.

Installing an HPDM 4.5 Service Pack

HPDM 4.5 Service Packs can only be installed onto a system that has HPDM 4.5 or a previous version of an HPDM 4.5 Service Pack. If there is only one component (e.g. HPDM Console) of HPDM installed on a system, then an HPDM 4.5 Service Pack will only update the installed component.

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.

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 client systems.

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

Each of the thin client operating system tabs produces the following view:

Figure 2-2  HPDM Management Console—Operating system tabs

1. Operating system tabs—Group devices by operating system. Only the tabs for the operating system types currently managed by HPDM will appear.

2. Device Toolbar—Provides shortcut icon of tools enabling you to send tasks, print device properties, and discover client devices.

3. Device Tree Pane—Contains the device tree, which is a hierarchical list of all the client devices belonging to the selected operating system type, sorted with a custom grouping scheme.

4. Device Pane—All clients of the selected folders are displayed in this window.

5. Template Pane—The templates that are applicable to the listed client devices are listed here.

6. Task Pane—Displays the execution status for each task. If there is more than one device for a listed task, the status of each device can be found by double-clicking the task. There are two tabs, one for manual tasks and one for tasks generated by rules.

7. Status Bar—Descriptions of various items in the HPDM Console are displayed here when the cursor moves over them.
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. Tree view of HPDM Gateway systems
2. List of tasks applied to the HPDM Gateway

Discovering client systems

Normally the HPDM Gateway will be able to detect most client devices by listening for a network broadcast message made by clients when they start. This solution does require that the HPDM Gateway is running before the client device starts up. For more information on this and other methods to add clients to the HPDM asset database, see Client discovery on page 16.
Displaying device properties

HPDM stores asset information about each client device it manages. When a thin client registers with the HPDM Server, it passes just enough asset information to uniquely identify the client and allow HPDM to communicate with it.

Basic asset information

Double-clicking a client icon in the HPDM Console will open its Properties window. This window has a number of tabs containing different categories of asset information. When only basic asset information is available, only the General tab will be populated. The items included in the basic asset information may be used to filter and group your client views.

Table 2-8  Basic asset information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>The unique ID HPDM assigns to the thin client. It is actually the first MAC address found on the thin client.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The current host name set on the thin client.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The model name of the thin client hardware.</td>
</tr>
<tr>
<td>Device Version</td>
<td>The OS image version reported by the thin client.</td>
</tr>
<tr>
<td>Device Serial Number</td>
<td>The hardware serial number of the thin client.</td>
</tr>
<tr>
<td>OS Type</td>
<td>The name of the thin client’s operating system.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the network adapter on the thin client that HPDM uses to communicate with the thin client.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address HPDM connects to when communicating with the thin client.</td>
</tr>
<tr>
<td>Subnet Address</td>
<td>The subnet over which HPDM communicates to with the thin client.</td>
</tr>
<tr>
<td>HPDM Agent Version</td>
<td>The HPDM Agent version on the thin client.</td>
</tr>
<tr>
<td>HPDM Gateway ID</td>
<td>The MAC address of the HPDM Gateway that is being used to communicate with the thin client.</td>
</tr>
<tr>
<td>HPDM Agent Working Mode</td>
<td>Indicates whether the HPDM Gateway is able to push tasks to the thin client or if it has to wait for the HPDM Agent to pull the tasks from the HPDM Gateway.</td>
</tr>
<tr>
<td>First Contact Time</td>
<td>The date and time when the thin client registered with HPDM.</td>
</tr>
<tr>
<td>Last Time Online</td>
<td>The date and time of the last time HPDM communicated with its HPDM Agent on the thin client.</td>
</tr>
<tr>
<td>BIOS Version</td>
<td>The BIOS version of the thin client.</td>
</tr>
<tr>
<td>Asset Tag</td>
<td>The Asset Tag of the thin client.</td>
</tr>
<tr>
<td>Have TPM Module</td>
<td>Indicates whether or not the thin client has a Trusted Platform Module (TPM) module. TPM refers to a secure crypto-processor that can store cryptographic keys that protect information, often called the &quot;TPM chip&quot; or &quot;TPM Security Device.&quot; 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.</td>
</tr>
<tr>
<td>TPM Owned</td>
<td>Indicates whether or not the TPM is owned. A TPM must be owned before it can be used to help secure a computer. The ownership of a TPM is set by assigning a password to it, which helps make sure only the authorized TPM owner can access and manage the TPM. Only one owner 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.</td>
</tr>
</tbody>
</table>

Table 2-8  Basic asset information
Collecting complete asset information

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

To execute a Get Asset Information task:
1. Right-click the client 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 client’s Properties window.

Displaying complete client asset information

After a successful Get Asset Information task, the additional tabs in the client's Properties window will be populated:

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

Keeping the HPDM Agent updated on client systems

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

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

**NOTE:** This rule is disabled by default.
Clients that have the HPDM Agent installed must be discovered (added to the HPDM asset database) by HPDM before they can be managed. There are three approaches to client discovery:

- Discovering a client from the client-side
- Discovering a client from the server-side
- Manually registering a client

**Discovering a client from the client-side**

When the thin client 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 thin client is rebooted, the automatic registration process restarts and will be run at regular intervals until it is successful.

1. The thin client 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 thin client 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 thin client'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 thin client'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 client's local network, a request is sent to the client 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.
Discovering a client from the server-side

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 HPDM Gateway and select Discover Device in the menu.

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 clients 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.
<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a new IP address to the IP list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Remove an existing IP address from the list.</td>
</tr>
<tr>
<td>Import</td>
<td>Import a *.txt or *.csv file to the IP list.</td>
</tr>
<tr>
<td>Export</td>
<td>Export the IP list as a *.txt file.</td>
</tr>
<tr>
<td>Copy</td>
<td>Copy the current IP list.</td>
</tr>
<tr>
<td>Paste</td>
<td>Paste a copied IP address.</td>
</tr>
</tbody>
</table>

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

### Manually registering a client

To manually register a client with the HPDM Server:

1. Using the HPDM Console, click the **HPDM Gateways** tab.
2. Right-click the HPDM Gateway you wish to have connect to the thin client, and from the menu, select **Device > Add**.
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.
4 Using tasks

Task templates

Task templates are displayed in the template 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 capturing files, deploying files, deleting files, registry changes, running operating system commands, and pauses
  - **Connections**—Used to get or set the connection settings of a device
  - **HPDM Agent**—Used to configure HPDM Agent settings and update the HPDM Agent
  - **Imaging**—Used to capture or deploy flash-memory images of client 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 Template 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 Template 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 Template 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 Template Pane.
2. Select Add to Favorites from the pop-up menu.

The icon for the selected template will change to the favorites icon.

Removing a template plugin

To remove a template plugin:
1. In the Template Plugin Management window, select a record and click the Uninstall button.
2. You will be prompted to confirm that you want to uninstall the selected template. Click Yes to uninstall.
3. The template associated with the uninstalled template plugin will be deleted from the Template Pane.

Using Template Sequence templates

You can specify two or more templates to be performed in a specific order using Template Sequence templates. A Template Sequence template can contain a maximum of 50 tasks.

1. Double-click the standard _Template Sequence template to open the Template Editor.
2. Click the Add button and select a template to add to the sequence from the pop-up menu. The Template Editor for the selected template will be displayed allowing you to edit it.

**NOTE:** You can define new templates to add to the sequence as required, just select the blank template type from the menu.

3. Click OK to add the template to the template sequence.
4. Continue adding templates to the sequence as required. Note that clicking Add after the first template has been added to the sequence will display an additional menu for you to indicate
whether the next template will be actioned after the previous template task has been successful, failed, or anyway (regardless of the result).

5. When you have finished defining the template sequence, click Save as to save the Template Sequence template for later use.

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 either Image Files, Easy Tools Configuration, or Easy Tools Settings.

2. Select the file that you want to import. Only .ibr, .img, .hpimg, .dd, and .dd.gz files can be accepted by importing Image Files; .hpcfg files can be accepted by importing Easy Tools Configuration; .hpset files can be accepted by importing Easy Tools Settings.

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 Template 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.
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 four 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.

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 Template 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 Template Pane and drop it on to the device or group.
   —or—

   Right-click devices in the Device Pane or folders in the Device Tree Pane 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>
<thead>
<tr>
<th>Table 4-1  Task status icons</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>![Success]</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The task was executed successfully by the device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>![Sending]</th>
<th>Sending</th>
</tr>
</thead>
</table>
Table 4-1  Task status icons (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The task is being sending from HPDM Server through HPDM Gateway to the device and is waiting for a reply.</td>
<td></td>
</tr>
<tr>
<td>Failed / Timeout</td>
<td>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.)</td>
</tr>
<tr>
<td>Ready</td>
<td>The task is executed and waiting for the user’s operation.</td>
</tr>
<tr>
<td>Paused</td>
<td>The task has been paused.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>The task has been cancelled.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The task has been scheduled for sending at a later time, and has not been sent yet.</td>
</tr>
<tr>
<td>Processing</td>
<td>The task has been accepted by the device and is being processed.</td>
</tr>
</tbody>
</table>

**Task settings**

In HPDM, a task is a combination of a template, an execution schedule, and a list of target thin clients. The HPDM Console lists tasks in two groups: Manual tasks and Rules tasks. Manual tasks are created directly with the HPDM Console and Rules tasks are created indirectly by the Rules mechanism.

You can specify general task settings by selecting Tools > Configuration from the HPDM Console’s menu bar to display the Configuration Management dialog box, then selecting the Task Settings item in the left-hand tree pane.

The PXE Image option enables you to show progress information for PXE image tasks.

**Task parameters**

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 Policy Setting. These are described in the following sections.

**Manual tasks**

Every time you apply a template to a set of thin clients 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 thin clients.

Target Device List

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

Schedule & Batch Control

The **Schedule & Batch Control** tab contains three sections.

- **Schedule** — This section enables you to specify a date and time for the task to execute.
- **Write Filter Policy Setting** — This section enables you to specify how HPDM handles the Write filter on thin clients that have Microsoft XPe and WES Operating Systems.
- **Batch Control** — This section enables you to specify a batch size. This is used when a task is sent to a large number of thin clients. The batch settings controls how many thin clients are sent the task at a time thereby giving you some control over the amount of network traffic HPDM generates.

Applying tasks to devices

You can apply a task to a device from a defined task template. Assigning a PXE task will cause the thin client to either wake on LAN or reboot.

You can apply tasks to devices either by drag-and-drop or by manually selecting the task.

**NOTE:** You can also cause tasks to be automatically applied to devices that meet specified criteria by setting rules as described in **Task rules on page 28**.

1. Drag a template from the Template Pane and drop it onto devices in the Device Pane or onto folders in the Device Tree Pane.
   
   —or—

   Right-click on devices in the Device Pane or folders in the Device Tree Pane and select **Send Task** from the menu to display the **Template Chooser**. Select a category and a template from the templates list, then click **Next**.

2. The **Task Editor** dialog box will appear. This enables you to make changes to the template and specify how and when the task is to be performed. The **Content** tab allows you to change the properties of the task as desired.

   **NOTE:** If you do not select the **Schedule Task** option and specify a time, the task will be sent to the device as soon as you click the **OK** button.

3. Click **OK** to apply the task to the device.
**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. If you select **Cancel All**, all of the ongoing tasks in the Task Pane will be canceled. 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. If you select **Delete All**, all the tasks in the **Task Pane** will be deleted.
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.

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, Get Connection Configuration, Capture, and so on.

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 thin clients 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 thin clients.

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 thin client that match its filter criteria once when the thin client first registers itself with the HPDM Server, or after completing a Factory Reset task.

- **Startup** — The rule will execute for each thin client that match its filter criteria every time the thin client 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

The HPDM Console can be used to view and manage devices.

To view the currently managed devices in the Device Pane:
▲ Select one or more folders in the Device Tree Pane.

To see a menu of applicable commands:
▲ Select one or more folders in the Device Tree Pane 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.

### Device icons

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Gateway active" /></td>
<td>Represents an HPDM Gateway that is currently active</td>
</tr>
<tr>
<td><img src="image" alt="Gateway inactive" /></td>
<td>Represents an HPDM Gateway that is currently down or disconnected</td>
</tr>
</tbody>
</table>

In the Device Pane of the HPDM Console, devices are represented by the following icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Group" /></td>
<td>Represents a number of devices that have been grouped together</td>
</tr>
<tr>
<td><img src="image" alt="Status unknown" /></td>
<td>Indicates that the status of this device cannot be confirmed because an HPDM Gateway managing this device is currently down or disconnected</td>
</tr>
<tr>
<td><img src="image" alt="Off" /></td>
<td>Indicates the device is currently turned off</td>
</tr>
<tr>
<td><img src="image" alt="Pull mode" /></td>
<td>Indicates the device is currently in pull mode</td>
</tr>
<tr>
<td><img src="image" alt="Pull-lock mode" /></td>
<td>Indicates the device is currently in pull-lock mode (the write filter is on)</td>
</tr>
<tr>
<td><img src="image" alt="Push mode" /></td>
<td>Indicates the device is currently in push mode</td>
</tr>
<tr>
<td><img src="image" alt="Push-lock mode" /></td>
<td>Indicates the device is currently in push-lock mode (the write filter is on)</td>
</tr>
</tbody>
</table>
Deleting devices

To delete a device from the Device Tree Pane:
1. Right-click the folder in the Device Tree Pane.
2. Select Delete from the menu.

All devices under this folder are removed from the Device Tree Pane.

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 thin clients both individually and in groups. It provides two ways to group your thin clients; manually by using your own grouping definitions and dynamically by using the thin clients' asset information. In addition to this, you can filter your thin clients based on their asset information. This enables you to divide your thin clients into sets and assign those sets to specific administrators. Grouping information for new thin clients can be set automatically using a DHCP tag.

Setting group information using a DHCP tag

You can specify the grouping information a new thin client 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 thin client tree panel and select Manual Group > Add Folder
2. Enter a name for the new folder.
3. Click OK

Thin clients 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 thin clients

Filtering enables you to work with a subset of your thin clients. It can be combined with User Privileges to divide the management of your thin clients 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 thin clients 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 criterion 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 thin client by SSL tunnel and view and control that client from the HPDM Console. This can be achieved either by using the _Shadow Device template available in the Template 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 Pane**.
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 client will be displayed in a separate window ready for your operations.

---

**Power management**

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

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

To shutdown, reboot, or wake a client:

1. Select a device from the **Device Pane** in the main Console window.
2. Right-click a client system and select **Power Management > Reboot, Wake On LAN or Shutdown** from the context menu.
3. The **Task Editor** dialog box will appear. Click **OK** to perform the task.

When the client receives the task, a warning dialog box will appear on the screen of the client device to inform the user that the device will be shutdown or restarted.
6 Thin client imaging operations

HPDM can be used to capture an image from one HP thin client and deploy it to any number of similar devices. HPDM can be used in conjunction with a PXE server; however, the preferred method is to use its built-in imaging capabilities. HPDM will only deploy images to thin clients that are licensed for the operating system contained in the image.

Introduction

HPDM can read and write images to and from supported clients. An image file is a binary file containing all the data on a thin client’s flash storage. HPDM manages images through the HPDM Repository Management tool, which also provides utilities to verify image integrity.

The _Capture Image and _Deploy Image templates enable you to capture an image and deploy it to other devices without a PXE server, while the _PXE Capture and _PXE Deploy templates enable you to capture an image and deploy it to other devices with a PXE server.

NOTE: Capturing and deploying images uses the PXE functions of HPDM, and some DHCP server setups may conflict with PXE. Should you experience problems with PXE, gp tp Configuring DHCP servers on page 72.

Client BIOS settings for PXE

NOTE: This procedure is only required on legacy Neoware devices.

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

1. Turn on the thin client 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, select Integrated Peripherals then VIA OnChip PCI Device.

4. Make sure Onboard Lan Boot ROM is set to [Enabled].

5. Press the F10 key then Y and Return to save the settings.

Capturing an image from a client with PXE

You can capture (copy) an image with PXE from any client managed by HPDM and store it as a .dd.gz file in the HPDM Repository so that it can be deployed (written) to other clients. This is achieved using the _PXE Capture template.

To capture an image from a device 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 Task Templates tab.

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

5. When the task is sent, a resulting template will be created with the name you designated. Its initial status will be “Transferring”.

6. After the task is finished, the resulting template will become valid and can be used to send tasks.

   **NOTE:** A PXE-captured image is always in the dd.gz format, regardless of whether it is a WES09 image or an HP ThinPro image.

---

### Deploying an image to a client with PXE

There is no “PXE Deploy” base template under the Task Templates tab.

To deploy an image to a device with PXE:

1. Drag a resulting template of a PXE Capture task to a device.

2. From the menu, click **Template > Import > Image Files > to deploy using PXE** ..., and according to the wizard, it will create a “PXE Deploy” template.

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

   **NOTE:** On HP ThinPro and HP Smart Zero Core, there is no license check. For example, you can deploy an HP ThinPro 4 image to an HP Smart Zero Core device or deploy an HP Smart Zero Core image to an HP ThinPro 4 device, but only if the disk size is large enough.

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

---

### Capturing an image from an HP thin client

The **_Capture Image** template enables you to capture the image of a device and either store the image for backup or apply it to other devices of the same model type and identical flash storage size. This template does not use a PXE server.

To capture an image:

   **NOTE:** For WES, make sure that thin clients can access the Master Repository shared folder and have permission to write. The Group Policy domain may affect write permissions if the shared folder to be accessed is in a domain.

1. Select the **Task Templates** tab in the **Task** pane, 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 thin client uses an advanced network, such as wireless, 802.1x, etc., select **Cached Imaging**.

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

4. If you want to preserve settings when capturing an image, select **Preserve Settings**.

**NOTE:** This option only takes effect on WES7. For other operating systems, please ignore this option.

The following settings will be preserved when capturing a WES7 image:

- **Settings**
  - Auto Logon
  - Internet Explorer home page
  - Local user accounts, including the administrator account, default user account, and other accounts
  - System locale
  - User locale
  - Input locale
  - UI language locale
  - Time zone
  - Region format
  - Location
  - Keyboard layout
  - Notification area
  - Taskbar
  - Desktop wallpaper

- **Connections**
  - Citrix ICA
  - RDP
  - TeemTalk

5. Click the **Save as** button, enter a name for this template, then click **OK**. A new template will appear in the **Task** pane.

6. Drag and drop this template on the device whose image you want to capture in the **Device** pane. The **Task Editor** dialog box will appear.

7. In the **Save result as template** field, enter a name for the resulting template that will be automatically created to enable you to apply the captured image to other clients.

8. Click **OK** to apply the task to the device immediately.
9. When the HPDM Agent on the client receives the task, the client will display a warning message indicating that the device will reboot in 30 seconds.

For HP ThinPro, the client will shut down, then start up in Mini Linux mode and run the capture utility which copies the contents of the flash storage to a .dd.gz file on the Master Repository. The last line on the client display will indicate progress in percentage completed. Note that this may take several minutes.

For WES, the client will shut down, then start up WinPE OS and run the capture utility which copies the contents of the file system to an .ibr file on the Master Repository. There is one dialog box to show the progress in percentage completed. Note that this may take several minutes.

10. The client will reboot after capturing has completed.

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

The client will then reboot again.

11. The Task pane in the HPDM Console will continue to indicate that the task is processing. The captured image is being compressed. When the task has finished, a new template will appear in the Task pane with the name you specified.

12. 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.

**NOTE:** An image captured from WES7 or WES09 via HPDM is a file-based image (.ibr). An image captured from HP ThinPro or HP Smart Zero Core by a “PXE Capture” or “Capture Image” task is always in the .dd.gz format.

**NOTE:** For WES, when HPDM Agent is executing an image task, the message box below will appear and is used to warn that HPDM Agent is doing something in the background and shouldn’t be interrupted.

### Deploying images

There is no “Deploy Image” base template. It can be created by capturing an image or by importing an existing image file.

**NOTE:** For WES file based imaging (.ibr), make sure that thin clients can access the Master Repository shared folder. The Group Policy domain may affect read permissions if the shared folder to be accessed is in a domain.

To deploy an image to one or more devices:

1. In the HPDM Console, display the OS tab containing the name of the clients to which you want to deploy the new image in the Device Pane.

2. Select the Task Templates tab in the Task pane, then double-click on the template you created when capturing an image to display the Template Editor.

3. Click the View Details button to view detailed information about the image package.
4. If the thin client uses an advanced network, such as wireless, 802.1x, etc., select **Cached Imaging**.

**NOTE:** If the **Cached Imaging** option is selected, it requires enough free disk space on the thin client 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.

**NOTE:** For example, if you captured a WES image from a t510 and want to deploy it to a t610, you need to select this option. Otherwise, this Deploy Image task will fail. If you select this option, you need to be sure the captured 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:** HPDM supports deploying .ibr, .img, .hpimg, .dd.gz, and .dd images to WES devices and supports deploying .img, .hpimg, .dd.gz, and .dd images to HP ThinPro 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.
7 Managing client operating systems

Renaming devices (hostname)

To rename a device (hostname) directly from the currently selected grouping view:

1. Right-click the desired thin client in the HPDM Console and select the Rename menu option. The Set hostname dialog will appear.
2. Edit the hostname value and click OK to automatically initiate a settings task.
3. Adjust the task settings as needed in the resulting Task Editor (e.g. Write Filter Policy Setting).
4. Click OK.

Changing connection settings

HP thin client devices are designed to access servers or applications through pre-defined ICA, RDP, terminal emulation or Web browser connections. HPDM enables you to copy these pre-defined connection settings from one thin client to others of the same model and operating system type.

⚠️ CAUTION: Before copying the connection settings of a device, you must make sure that each connection is properly configured and tested on the network where the connections will be used.

1. Configure a thin client device with the required connection settings and make sure the connections work on the network where they will be used.
2. Run the HPDM Console and display the name of the device with the correct connections in the device pane.
3. Double-click on the _Get Connection Configuration template to display the Template Editor.
4. Use the check boxes to indicate which connection settings to retrieve from the device.
5. Enter a name for the template which will be created to store the connection settings.
6. Click Save as ..., enter a name for this template then click OK.
7. Drag and drop the template on the name of the device with the correct connections in the device tree. The Task Editor will appear.
8. Click OK to apply the task to the client device.
9. The connection settings will be copied from the device and stored in a new template which will appear in the Templates Pane with the name you specified in step 5.
10. You can now drag and drop this new template on devices in the device tree to apply the connection settings to them.

Changing device settings

The setup configuration of a device can be changed using templates belonging to the Settings category in the Template Pane.
Cloning settings

1. Double-click the _Clone Settings template to display the Template Editor.
2. Use the check boxes to indicate which settings to retrieve from the device.
3. Enter a name for the template which will be created to store the settings.
4. Click the Save as button, enter a name for this template, and then click OK.
5. Drag and drop the template on the name of the device with the correct settings in the device tree. The Task Editor is displayed.
6. Click OK to apply the task to the client device.
7. The settings will be copied from the device and stored in a new template which will appear in the Templates Pane with the name you specified in step 4.
8. You can now drag and drop this new template on devices in the device tree to apply the settings to them.

Applying settings

1. Double-click the _Apply Settings template to display the Template Editor.
2. Click the Edit button.
3. Use the check boxes to indicate which settings to edit.
4. Click Next or click on the settings titles on in the left hand pane to configure individual settings.

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

**NOTE:** When configuring Time Settings, the values available for WES09 and XPe devices are unified with those available for WES7 devices. There are 97 values in all. Some may not be supported by WES09 or XPe devices. Also, not all values on WES09 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 the Save as button, enter a name for this template, and then click OK.
8. Drag and drop the template on the name of the device with the correct settings in the device tree. The Task Editor will be displayed.
Adding devices using MAC addresses

Devices that are not working and need a new image, or that have not been found by HPDM, can be added to the console using their MAC address. However, devices added to the HPDM Console in this manner cannot be fully managed by HPDM until the HPDM Agent on the device reports to the HPDM Server properly.

You can perform a Wake On LAN to a device that has not previously been reported to the HPDM Server. It will report in and be displayed in the proper operating system tab.

To add a new device using its MAC address:

1. Select Device > Add from the HPDM Console menu bar.
   
The Add Device dialog box will appear.

2. Enter the MAC Address of the device to be added.

3. Select the HPDM Gateway that will connect with the device from the Neoware HPDM Gateway ID drop-down list.

4. Click OK to add the device.
   
A new device will appear in the device tree with the name deviceX, where X is a number. This device will appear as turned off, but you can still interact with the device. For example, you can use Send Task to send a new Imaging template to the device, or Wake on LAN to attempt to start up the device.

Using File and Registry templates

The _File and Registry template is generic in that it consists of a customizable combination of copying files, deleting files, registry changes, running operating system commands, and pauses.

Customizing this template involves adding, deleting, and rearranging a variety of subtasks.

1. Double-click the _File and Registry template to display the Template Editor.

2. Click Add to add a variety of subtasks. (Refer to the following tables for more information on each subtask.)
   
Click Edit to edit a subtask.

Click Delete to delete the selected subtask.

Click Up and Down to rearrange the subtasks as required.

3. After modifying the template, click Save as to save the template for later use.

Table 7-1 Capture Files subtask

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File or folder with full path</td>
<td>The name with the full path of the file or folder to capture from the client device.</td>
</tr>
<tr>
<td>Target path</td>
<td>The location on the Master Repository where to store the file to capture.</td>
</tr>
<tr>
<td>Overwrite</td>
<td>The overwrite flag that appears if the target file already exists on the Master Repository.</td>
</tr>
</tbody>
</table>
Table 7-2  Deploy Files subtask

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File and Folder Name</td>
<td>The name of the file or path to be deployed to the device.</td>
</tr>
<tr>
<td>Path On Device</td>
<td>The path for the files to be copied to on the device.</td>
</tr>
</tbody>
</table>

Table 7-3  Delete Files subtask

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>The file name to be deleted.</td>
</tr>
<tr>
<td>Path On Device</td>
<td>The location of the file.</td>
</tr>
<tr>
<td>Delete Recursively</td>
<td>Delete files matching the pattern in File Name recursively in all subdirectories from the given Path On Device.</td>
</tr>
</tbody>
</table>

Table 7-4  Registry subtask

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Key (Registry tree)</td>
<td>(Registry tree) Add a key at the selected location on the tree.</td>
</tr>
<tr>
<td>Add Value (Registry tree)</td>
<td>(Registry tree) Add a value on the selected key.</td>
</tr>
<tr>
<td>Rename (Registry tree)</td>
<td>(Registry tree) Rename the selected item.</td>
</tr>
<tr>
<td>Delete (Registry tree)</td>
<td>(Registry tree) Delete the selected item.</td>
</tr>
<tr>
<td>Action (Registry settings)</td>
<td>(Registry settings) The action to be applied to the registry table. Set to add to add a key, or delete key to delete a key.</td>
</tr>
<tr>
<td>Type (Registry settings)</td>
<td>(Registry settings) The type of registry key value.</td>
</tr>
<tr>
<td>Value Name (Registry settings)</td>
<td>(Registry settings) Specify a name for the registry key. Double-click on this field to edit it.</td>
</tr>
<tr>
<td>Value Data (Registry settings)</td>
<td>(Registry settings) Specify the data to add to the registry key value. Double-click on this field to edit it.</td>
</tr>
<tr>
<td>Add Key (Key settings)</td>
<td>(Key settings) If this is selected, even if the selected key is empty, the key will still be added to the registry.</td>
</tr>
<tr>
<td>Delete Key and Value (Key settings)</td>
<td>(Key settings) If this is selected, the selected key and all values under it will be deleted. Note that there must be no values under the given key.</td>
</tr>
</tbody>
</table>

Table 7-5  Command subtask

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>The command on the client device to be executed. Enter the full path name of the command on the client device.</td>
</tr>
</tbody>
</table>
Table 7-5  Command subtask (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are using a long file name that contains a space, use quoted strings to indicate where the file name ends and the arguments begin. For example: <code>c:\program files \file.exe</code>.</td>
<td></td>
</tr>
<tr>
<td>Execute After Reboot</td>
<td>Set to Yes if you want the system to reboot and execute the command when it restarts, or No if you want the command to be executed immediately.</td>
</tr>
<tr>
<td>Wait</td>
<td>Set to Yes if the given command has to wait for the previous command to finish before processing, or set to No for simultaneous execution of commands.</td>
</tr>
</tbody>
</table>

Table 7-6  Pause subtask

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours, Minutes, Seconds</td>
<td>The duration of time to pause processing of the template, often in order to wait for certain events, for example a system restart.</td>
</tr>
</tbody>
</table>

Table 7-7  Program Record subtask

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Name</td>
<td>The program name.</td>
</tr>
<tr>
<td>Action</td>
<td>Add or remove program action type.</td>
</tr>
<tr>
<td>Publisher</td>
<td>The program publisher.</td>
</tr>
<tr>
<td>Version</td>
<td>The program version.</td>
</tr>
<tr>
<td>Comments</td>
<td>The program comments.</td>
</tr>
</tbody>
</table>

**Merging File and Registry templates**

Two or more **File and Registry** templates can be merged together to form a new **File and Registry** template with the combined subtasks of all of them.

1. Select one of the **File and Registry** templates that you wish to merge.
2. Right-click on it and select **Merge** from the pop-up menu.
3. Select another template to merge the selected template with, then click **OK** to merge the templates.
4. Enter a name for the new template when prompted.
5. A new **File and Registry** template will be created with all of the subtasks of the original templates combined.
Changing registry settings

HPDM can add, delete, and change registry keys and their values on thin client devices using File and Registry templates. Additionally, the existing settings can be cloned from a device using the Get Registry template and then modified.

Getting registry settings

HPDM can clone the system registry of a thin client device. The procedure is as follows:

1. Select the OS tab corresponding to the operating system of the device from which you want to get registry settings.
2. Double-click on the _Get Registry template to display the Template Editor.
3. Click the Add button and enter the name of the registry node from which you want to retrieve settings (e.g. desktop for desktop settings), then click OK.
   
The name of the new node will appear on the Registry tab of the Template Editor.
4. In the Save result as template field, enter a name for the template which will be created to store the result.
5. Click Save as and enter a name which indicates the purpose of this template (get desktop settings).
6. Click OK and the new template will appear in the Task Templates pane.
7. Drag and drop this template on the device in the Device Tree from which you want to get registry settings. The Task Editor dialog box will appear.
8. Click OK to apply the task to the device immediately.
   
The registry settings will be retrieved from the device and stored in a new template in the Task Templates pane. Its name will be the one which you specified in step 4.
9. To view the retrieved registry settings, double-click on the result template to display the Template Editor, double-click on the Registry entry in the Subtask box to display the Configure Registry Subtask dialog box, then click on the registry node in the Registry Tree panel to display the settings.

Editing registry settings

1. If you are editing a previously generated _Get Registry task result template, double-click the name of that template, then double-click Registry in the Subtask box.
2. If you need to create a new template, double-click the _File and Registry template to display the Template Editor, then click the Add button.
   
Select Registry in the Subtask Chooser, then click OK.
3. The Configure Registry Subtask dialog box will be displayed enabling you to edit registry settings.
   
   - You can edit the contents of the Registry Tree using the four buttons at the bottom of the box.

<table>
<thead>
<tr>
<th>Add Key</th>
<th>This enables you to add a new key under the currently selected item.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Value</td>
<td>This enables you to add a value to the selected key.</td>
</tr>
</tbody>
</table>
Rename This enables you to rename the selected item.

Delete This enables you to remove the selected item.

- The **Registry Settings** box will display the current settings of the key selected in the Registry Tree. It is divided into the following columns:

<table>
<thead>
<tr>
<th>Action</th>
<th>Indicates the action to be applied to the registry table: add or delete a key. Click in the field to change the current setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Indicates the type of registry key value.</td>
</tr>
<tr>
<td>Value Name</td>
<td>Displays the name of the registry key. Double-click in this field to edit it.</td>
</tr>
<tr>
<td>Value Data</td>
<td>Displays the data for the registry key value. Double-click in this field to edit it.</td>
</tr>
</tbody>
</table>

- The **Action to Perform** options determine whether the key is added or deleted. If **Add Key** is selected, the selected key will be added to the registry even if the key is empty. If **Delete Key and Value** is selected, the selected key and all values under it will be deleted. Note that there must not be any values under the specified key.

4. When you have finished modifying the template, click the **Save as** button and enter a name for the new template.

5. Click **OK**. The new template will be created and its name will appear in the **Template Pane**.

6. You can now apply the new registry settings to one or more devices by dragging the template from the **Template Pane** and dropping it on to the device(s) in the **Device Tree**.

**Copying files**

You can capture files from a device to the Master Repository, or you can deploy files to devices through repositories. Both are achieved using the **_File and Registry** template.

**Capturing files**

1. Double-click the **_File and Registry** template to display the Template Editor.
2. Click the **Add** button and select **Capture Files**.
3. Click **OK**. The Capture Files Editor dialog box will appear.
4. Specify the **Files to Transfer** by clicking in the field and entering the file or folder name with the full path. Additional lines can be added by clicking the **Add** button.

The **File or Folder Name** field supports the use of the wildcards * and ?. For example:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>means zero or more characters.</td>
</tr>
<tr>
<td>?</td>
<td>means one character.</td>
</tr>
<tr>
<td>com.jar</td>
<td>means the file is named com.jar.</td>
</tr>
<tr>
<td>c:\abc*</td>
<td>all mean the same thing, that is, all the files under directory c:\abc.</td>
</tr>
<tr>
<td>c:\abc\</td>
<td></td>
</tr>
<tr>
<td>c:\abc</td>
<td></td>
</tr>
</tbody>
</table>
a* means all the files that start with the letter a.

*a means all the files that end with the letter a.

NOTE: Wildcards are only accepted in the last level path or file name.

5. Specify the target path to store captured items on the Master Repository. The target path accepts parameters making it possible to send one task to multiple devices and have same name files captured to different folders (since version 4.5 Service Pack 1)

6. Select the Overwrite if exists option.

7. Click OK when you have finished capture editing. A Capture Files subtask will be added to the Subtask list of the template.

8. Click Save as to save the template with a new name.

9. Drag and drop the template onto the device you want to capture files from.

Deploying files

1. Double-click the _File and Registry template to display the Template Editor.
2. Click the Add button and select Deploy Files.
3. Click OK.
4. Add Files to Transfer by clicking the Add from local button or the Choose upload button.
5. Click OK when you have finished specifying files to be deployed. A Deploy Files subtask will be added to the Subtask list of the template.
6. Click Save as to save the template with a new name.
7. Drag and drop the template onto the device you want to deploy files to.

Program Record

To add/remove program records to thin clients using the _File and Registry template:

1. Double-click the _File and Registry template to display the Template Editor.
2. Click the Add button and select Program Record.
3. Click OK. The Program Record Editor dialog will appear.
4. Click the Add… button to add a record.
5. Choose the Action type.
6. Input the Publisher, Version, and Comments if needed.
7. Click OK. A Program Record subtask will be added to the Subtask list of the template.
8. Click Save as ..., to save the template with a new name.
9. Drag and drop the template onto the device you want to add/remove a program record to.
Remote command execution

HPDM can remotely execute commands on a device using File and Registry templates. In this context, a command is anything executable on the device’s operating system. It can be applications, DOS batch files, Windows scripts, etc. You can enter any command, however it is recommended that these commands are tested on a client device first.

**NOTE:** DOS commands cannot be executed directly on a Windows XP Embedded OS. To execute DOS commands you need to write them to a batch file saved with the suffix .bat, then execute the batch file.

The Windows environment variable PATH may be different on each device, so it is important to enter the full path to each command to make sure it can be found on the device. For example, to execute an executable file named xxx.exe in a directory named C:\Program Files, enter the command as C:\Program Files\xxx.exe.

To execute commands:

1. Double-click the _File and Registry_ template to display the Template Editor.
2. Click the Add button and select Command.
3. Click OK.
4. Specify the command to be executed by clicking in the Command column and entering the appropriate information.
5. In the Execute After Reboot column, select Yes if the device should reboot before executing the command you specify. Select No if you want the command to execute without the need to reboot the device.
6. In the Wait column, select Yes if the given command has to wait for the previous command to finish before processing, or set to No for simultaneous execution of commands.
7. If you want to specify more commands, click Add to continue.
8. Click OK when you have finished.
9. Click Save As to save the template under a new name.
10. Drag and drop the template on the devices where you want the commands to run.

Remote execution of Windows scripts

Windows Scripting Host is a comprehensive scripting infrastructure for the Microsoft Windows platform, provides script engines, Visual Basic Scripting Edition and Microsoft JScript, which can be embedded into Windows applications and an extensive array of supporting technologies that make it easier for script users to script Windows applications.

For more information on how to write Windows scripts, see:

http://www.msdn.microsoft.com

Enter “windows script” as search keywords.

To run windows scripts as a command from HPDM, you need to add wscript before the script name you want to run. Wscript.exe is in the C:\windows\system32 directory.
8 Repository management

HPDM uses one or more repositories to store the files needed for its tasks. 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.

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:

2. 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 > Repository Configuration from the menu.
2. In the Repository Configuration dialog box, select the Master Repository item and click the Edit button.
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 the Connect button if you want to test the connection to Master Repository Controller.
5. Click the Test button if you want to test the connection to the FTP server and/or the Shared Folder.
6. Click the Save button to save the settings.
Configuring the Child Repositories

1. Select Tools > Repository Management > Repository Configuration from the menu.
2. In the Repository Configuration dialog box, click the Add button.
3. In the Repository Editor dialog box, configure the Repository Name, Server Address, Username, Password, and Path settings.
4. Click the Test button if you want to test the connection to the FTP server and/or the Shared Folder.
5. Click the Save button to save the settings

Deleting Child Repositories

1. Select Tools > Repository Management > Repository Configuration from the menu.
2. In the Repository Configuration dialog box, select the HPDM Child Repository and click the Remove button and then Yes to confirm.

Exporting repositories

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

Importing repositories

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

Synchronizing repositories

1. Select Tools > Repository Management > Repository Configuration from the menu.
2. In the Repository Configuration dialog box, click the Sync All button.
3. A warning message appears. Click Yes to confirm.
4. The synchronization will be done in the background. After finishing, the Last Time Synchronized column in the Repository Configuration dialog box will be updated.

Content management

To view the contents of the Master Repository:

Select Tools > Repository Management > Content Management from the menu.
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.

Syncing content to the child repositories

To sync content to the HPDM Child Repositories:

▲ In the Content Management dialog box, click the Sync All button. All the contents will be synced to the HPDM Child Repositories.

Repository mapping

HPDM automatically maps each client 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 configure the Repository Mappings, select Tools > Repository Management > Repository Mapping to open the Repository Mapping dialog.

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 thin clients on page 32](#) for details about filters.
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 54 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 DNs:
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 by either:
   - Double-clicking 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 55**.

---

**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.
10 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 thin clients 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 thin clients.

To create a Device Information report:

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

### Device Task report

This report is only available when a single thin client 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 thin client system for which you want a report.
2. Right-click on the selection and select **Print Device Task Report** ....
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:

1. 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 ....
HPDM separates templates into several categories. Most of the standard templates are available for every operating system.

**File and Registry**

*File and registry*

This template enables you to create a sequence using these sub-templates:

- Set a registry key.
- Capture a file from a thin client.
- Deploy a file to a thin client.
- Execute a command on a thin client.
- Delete files on a thin client.
- Pause a sequence.
- Add or remove a program record on a device.

*Get registry*

This template enables you to upload one or more keys from a thin client’s registry.

**HPDM Agent**

*Configure Agent*

This template enables you to configure the HPDM Agent on the target thin clients.

*NOTE:* You can no longer set the current HPDM Gateway by type ‘cur-gateway, back-gateway’ in the **Backup HPDM Gateway** field.

*Configure Task Deferment*

This template enables you to configure task deferment settings on target thin clients.

*Update Agent*

This template updates HPDM Agent on the target thin clients 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

_Pull Connection Information

This template will extract the specified connection settings from a thin client and create a new template to push those connections to other thin clients.

Imaging

_Capture Image

This template will capture an image from the target thin client and upload it to the Master Repository. It will also create a new Deploy Image template to install the image to other thin clients. This template can only be sent to a single thin client at a time.

_PXE Capture

This template will capture an image with PXE service from the thin client and upload it to the Master Repository. It will also create a new PXE deploy template to install the image to other thin clients. This template can only be sent to a single thin client at a time.

Operations

_Factory Reset

This template resets the targeted thin clients to their original configuration. The effects of this differ according to the operating system of the thin client. 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 thin clients.

_Reboot Device

This template reboots the targeted thin clients. A warning message will be displayed on the thin clients’ screen for 15 seconds before the reboot actually takes place.

_Reverse Shadow Device

This template causes the HPDM Agent on a targeted thin client 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 target thin clients. 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 thin client by SSL tunnel.
Shut down Device

This template shuts down the targeted thin clients. A warning message will be displayed on the thin clients’ screen for 15 seconds before the reboot actually takes place.

Start Resource Monitor

This template starts the Resource Monitor for the target thin client. This template can only be sent to a single thin client at a time and is not available for HP ThinPro thin clients.

When this template is sent to a thin client successfully, a Resource Monitor dialog will pop up. You can monitor Process, Performance, and Network Disk information.

Wake Up Device

This template will cause the HPDM Gateway associated with the targeted thin clients 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

Apply Settings

This template enables you to create a set of custom settings and deploy them to one or more thin clients. Click Edit ... to launch a wizard which will assist you. For more information, see Changing device settings on page 41.

Clone Settings

This template enables you to copy a selection of custom settings from one thin client and deploy them to other thin clients.

Hostname and IP

This template enables you to change the hostname and IP address of one or more thin clients. There are two options:

- 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 Password

This template enables you to set a password for one or more users on one or more thin clients. You can check hide password check box to hide the password, or clear the check box if to show the password.

Write Filter Settings

This template enables you to change the Write Filter settings for a thin client.
_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.

:Set Domain

The _Set Domain template allows devices to join a domain or a workgroup.

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 11-1  Template sequence conditions

<table>
<thead>
<tr>
<th>Icon</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![icon]</td>
<td>anyway</td>
<td>Execute the template regardless of any previous template execution success or failure.</td>
</tr>
<tr>
<td>![icon]</td>
<td>success</td>
<td>Execute the template only if the previous template completed successfully.</td>
</tr>
<tr>
<td>![icon]</td>
<td>failure</td>
<td>Execute the template only if the previous template completed with a failure.</td>
</tr>
</tbody>
</table>

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 condition 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 11-1  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.
12 Backing up and restoring the HPDM Server and database

The HPDM Server Backup and Restore Tool can back up or 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

**NOTE:** The tool can be used to restore an HPDM backup to another HPDM server running version 4.5 or later.

1. To start the tool, select Start > All Programs > Hewlett-Packard > HPDM > HPDM Server Backup and Restore Tool.
2. The following dialog will be shown:

![Figure 12-1 HPDM Server Backup & Restore Tool]

In this dialog, the values of Database Type, Host, Port, and Database are shared with the HPDM Server's configuration and cannot be edited. The value of Database Type can be either PostgreSQL or Microsoft SQL Server, depending on what database server the HPDM server connects to. The value of Authentication is set as Database Authentication when the Database Type is PostgreSQL, and it can be either Database Authentication or Windows Authentication when the Database Type is Microsoft SQL Server.

**NOTE:** The database owner privilege is required to perform a backup or restore.

**NOTE:** The values of Authentication, Username, and Password are NOT going to be recorded anywhere, neither database nor local disk.

The HPDM Server backup is a folder with a name like DMBackup20121107145359, which contains the database schema and data and some HPDM Server files.

![Figure 12-2 HPDM Server backup location]

The **Back up** button is enabled when the Backup Folder value is set to a folder that already exists and is not the folder of an existing backup (such as DMBackup20121107145359). The **Restore** button is enabled when the Backup Folder value is set to an existing HPDM Server backup. For example, in the above screen shot, the value C:\HPDMBackup enables the **Back up** button and leaves the **Restore** button disabled, while the value C:\HPDMBackup\DMBackup20121107145359 does the opposite.

3. When either **Back up** or **Restore** is clicked, you are prompted to stop the HPDM Server. This must be done manually by right-clicking the HPDM Server icon in the system tray and selecting...
Stop HPDM Server. The prompt will NOT show up again if the HPDM Server is not actually stopped.

NOTE: If the HPDM Server is not stopped, the tool cannot make sure the success of a backup or restore, even though the process may continue and be finished with a message that says it’s successful.

4. Progress and results will be shown in the Messages pane on the right side of the main dialog. The tool will back up or restore the database and then the HPDM Server files sequentially.

   The back up or restore process will fail and stop when the database manipulation or the file copying fails. A warning will be shown when the source files/folders are missing or the deletion of the target files/folders fails, but the process will continue.

   On a successful backup, the Backup Folder value will be locally saved and will be restored the next time the tool starts up.

5. The HPDM Server needs to be manually restarted after a backup/restore operation. The HPDM Server will NOT be able to restart correctly if the database restore operation fails or terminates in the middle of the process. In this case, another restore from the same or a different backup should follow as needed.
A Network configuration

This chapter contains information necessary to configure some networks in order to use HPDM:

Configuring DHCP servers

This section describes how to configure the DHCP server for use with PXE.

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

Should problems occur when using PXE, the DHCP servers may need to be checked for certain settings that may conflict with PXE. However, on most networks, these issues should not occur.

The DHCP server is used by the PXE boot ROM to get an IP address as well as other basic networking information (subnet mask, default HPDM Gateway, etc.).

**NOTE:** Note: The network must be configured using DHCP to use the PXE service.

Configuring the DHCP Server

1. Be sure the DHCP server has not been previously configured for a PXE bootstrap.
2. If the DHCP options 43 & 60 are set, remove them.

   **NOTE:** The HPDM PXE service will detect the DHCP packets sent by any PXE BootROMs and will offer PXE network parameters without disturbing the standard DHCP negotiation process. This is called DHCP Proxy.

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

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

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

The HPDM Server installation process installs the HP PXE Service. This service provides the PXE remote-imaging function. The service is automatically started and stopped with the operating system.

The DHCP server is used by the PXE boot ROM to get an IP address as well as other basic networking information (subnet mask, default HPDM Gateway, etc.).

The following instructions assume that:

- 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.

Configuring the DHCP Server:

By default options 60 and 201 are not set under Windows 2000. These options will have to be added in order to tell PXE clients where to find the HPDM Server.

To configure the DHCP server:
1. If DHCP option 43 is set, remove it. (This is due to the fact that the HPDM Gateway is installed on the same machine as the DHCP server.)

2. Add option 60, and set value to PXEClient. If option 60 does not exist, see the following instructions on setting this option.
   a. From the Windows Start menu, select Start > Run.
   b. Enter Cmd in the Open: field. A Command shell appears.
   c. Enter netsh then press the Enter key.
   d. Enter dhcp then press the Enter key.
   e. Enter server \servername (using the UNC name for the server).
      —or—
   f. Enter server <ip_address> (using the IP address of the server).
      A “dhcp server >” prompt appears in the command window.
   g. Enter add optiondef 60 <name of your choice> STRING 0 then press the Enter key.
   h. Enter set optionvalue 60 STRING “PXEClient” then press the Enter key.
   i. To confirm that the settings are correct, enter show optionvalue all then press the Enter key.

3. Add option 201 by following these steps:
   a. Type in add optiondef 201 <name of your choice> STRING 0 then press the Enter key.
   b. Type in set optionvalue 201 STRING ‘HPDM_Gateway_IP_Address’ ‘40003’ then press the Enter key.
      
      **NOTE:** The HPDM_Gateway_IP_Address is the address of the server running the HPDM Gateway service.
      
      c. To confirm that the settings are correct, type in show optionvalue all then press the Enter key.
      
      **NOTE:** When setting optionvalue 201,’HPDM Gateway_IP_Address’ ‘40003’ must be written exactly as shown above, including the single quotes and separated by a single space, otherwise errors will occur.

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

### Configuring a Linux DHCP server

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;
   ```

   **Configuring DHCP servers**
Option vendor-class-identifier “PXEClient”;
Option NDM “’HPDM_Gateway_IP_Address’ ‘40003’”;

2. Restart dhcpd to use the new configuration.
3. The HPDM config string should be:
   ‘HPDM_Gateway_IP_Address’ ‘40003’

### Configuring routers

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

**Example (Cisco Router):**

1. See Global Configuration mode.
2. Type `ip forward-protocol udp 67` and press Enter.
3. Type `ip forward-protocol udp 68` and press Enter.
4. See the LAN interface(s) that serves the PXE workstations.
5. Type `ip helper-address <DHCP Server IP address>` and press Enter.
6. Type `ip helper-address <HPDM Gateway IP address>` and press Enter.

**NOTE:** The above IP addresses should be entered without the `< or >` characters.
The following tables list the standard and custom ports used by HPDM. The ports are categorized by HPDM components to facilitate the firewall configuration if the HPDM components are installed separately on different host machines.

### Table B-1  HPDM Console ports (inbound)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5500</td>
<td>SSL VNC Proxy</td>
<td>VNC Viewer (bundled with HPDM Console)</td>
<td>TCP (loopback)</td>
<td>VNC Viewer in Listen Mode (reverse VNC)</td>
</tr>
<tr>
<td>5900</td>
<td>VNC Viewer (bundled with HPDM Console)</td>
<td>SSL VNC Proxy (bundled with HPDM Console)</td>
<td>TCP (loopback)</td>
<td>VNC Viewer in Listen Mode (reverse VNC)</td>
</tr>
<tr>
<td>40004</td>
<td>SSL VNC Proxy (bundled with HPDM Agent)</td>
<td>VNC Proxy (bundled with HPDM Console)</td>
<td>TCP</td>
<td>SSL VNC Proxy in Listen Mode (reverse VNC)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 &amp; 21</td>
<td>HPDM Console</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>22</td>
<td>HPDM Console</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>137</td>
<td>HPDM Console</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td>Allows NetBIOS Name Resolution</td>
</tr>
<tr>
<td>138</td>
<td>HPDM Console</td>
<td>NetBIOS Datagram Service</td>
<td>UDP</td>
<td>Allows NetBIOS Datagram transmission and reception</td>
</tr>
<tr>
<td>139</td>
<td>HPDM Console</td>
<td>NetBIOS Session Service</td>
<td>TCP</td>
<td>Allows NetBIOS Session Services connections</td>
</tr>
<tr>
<td>445</td>
<td>HPDM Console</td>
<td>Microsoft Directory Services</td>
<td>TCP</td>
<td>For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes</td>
</tr>
<tr>
<td>989 &amp; 990</td>
<td>HPDM Console</td>
<td>FTPS server (third-party software)</td>
<td>TCP</td>
<td>These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening</td>
</tr>
</tbody>
</table>
### Table B-2  HPDM Console ports (outbound) (continued)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1099</td>
<td>HPDM Console</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Allows the HPDM Console to query the RMI Registry</td>
</tr>
<tr>
<td>5500</td>
<td>SSL VNC Proxy (bundled with HPDM Console)</td>
<td>VNC View (bundled with HPDM Console)</td>
<td>TCP (loopback)</td>
<td>VNC Viewer in Listen Mode (reverse VNC)</td>
</tr>
<tr>
<td>5900</td>
<td>VNC Viewer (bundled with HPDM Console)</td>
<td>VNC Proxy (bundled with HPDM Console)</td>
<td>TCP (loopback)</td>
<td>VNC Shadow</td>
</tr>
<tr>
<td>40002</td>
<td>HPDM Console</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Allows the HPDM Console to call remote objects on the HPDM Server by RMI</td>
</tr>
<tr>
<td>40004</td>
<td>SSL VNC Proxy (bundled with HPDM Console)</td>
<td>VNC Proxy (bundled with HPDM Agent)</td>
<td>TCP</td>
<td>Port for SSL VNC connection</td>
</tr>
</tbody>
</table>

### Table B-3  HPDM Server ports (inbound)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1099</td>
<td>HPDM Console</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Allows the HPDM Console to query the RMI Registry</td>
</tr>
<tr>
<td>40002</td>
<td>HPDM Console</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Allows the HPDM Console to call remote objects on the HPDM Server by RMI</td>
</tr>
<tr>
<td>40005</td>
<td>HPDM Gateway</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Allows the HPDM Gateway to send reports to the HPDM Server</td>
</tr>
<tr>
<td>40006</td>
<td>HPDM Server</td>
<td>PostgreSQL (bundled with HPDM Server)</td>
<td>TCP (loopback)</td>
<td>The default database PostgreSQL listening port (only needed when PostgreSQL is used)</td>
</tr>
<tr>
<td>40009</td>
<td>HPDM Agent</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table B-4  HPDM Server ports (outbound)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>40000</td>
<td>HPDM Server</td>
<td>HPDM Gateway</td>
<td>UDP</td>
<td>Allows the HPDM Server to poll the HPDM Gateway</td>
</tr>
<tr>
<td>40003</td>
<td>HPDM Server</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Allows the HPDM Server to send tasks to the HPDM Gateway</td>
</tr>
</tbody>
</table>
### Table B-4  HPDM Server ports (outbound) (continued)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver Description</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>40006</td>
<td>HPDM Server</td>
<td>PostgreSQL (bundled with HPDM Server)</td>
<td>TCP (loopback)</td>
<td>The default database PostgreSQL listening port (only needed when PostgreSQL is used)</td>
</tr>
<tr>
<td>40012</td>
<td>HPDM Server</td>
<td>Master Repository Controller</td>
<td>TCP</td>
<td>Allows the HPDM Server to talk to the Master Repository Controller to manage the Master Repository</td>
</tr>
</tbody>
</table>

### Table B-5  HPDM Gateway ports (inbound)

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

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

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver Description</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 &amp; 21</td>
<td>HPDM Gateway</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>22</td>
<td>HPDM Gateway</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table B-6  HPDM Gateway ports (outbound) (continued)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>HPDM PXE Server (bundled with HPDM Gateway)</td>
<td>HPDM Imaging Mini Linux Tool (client-side)</td>
<td>UDP</td>
<td>PXE bootstrap</td>
</tr>
<tr>
<td>137</td>
<td>HPDM Gateway</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td>Allows NetBIOS Name Resolution</td>
</tr>
<tr>
<td>138</td>
<td>HPDM Gateway</td>
<td>NetBIOS Datagram Service</td>
<td>UDP</td>
<td>Allows NetBIOS Datagram transmission and reception</td>
</tr>
<tr>
<td>139</td>
<td>HPDM Gateway</td>
<td>NetBIOS Session Service</td>
<td>TCP</td>
<td>Allows NetBIOS Session Services connections</td>
</tr>
<tr>
<td>445</td>
<td>HPDM Gateway</td>
<td>Microsoft Directory Services</td>
<td>TCP</td>
<td>For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes</td>
</tr>
<tr>
<td>989 &amp; 990</td>
<td>HPDM Gateway</td>
<td>FTPS server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>40001</td>
<td>HPDM Gateway</td>
<td>HPDM Agent</td>
<td>TCP</td>
<td>Allows the HPDM Gateway to send tasks to the HPDM Agent</td>
</tr>
<tr>
<td>40001</td>
<td>HPDM Gateway</td>
<td>HPDM Agent</td>
<td>UDP</td>
<td>Allows the HPDM Agent to receive replies of broadcasting from the HPDM Gateway</td>
</tr>
<tr>
<td>40005</td>
<td>HPDM Gateway</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Allows the HPDM Gateway to send reports to the HPDM Server</td>
</tr>
<tr>
<td>40008</td>
<td>HPDM Gateway</td>
<td>HPDM Gateway Controller (loopback)</td>
<td>TCP</td>
<td>Allows the HPDM Gateway to notify the HPDM Gateway Controller there are other gateways running in the same subnet</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>DHCP Server</td>
<td>HPDM Agent</td>
<td>UDP</td>
<td>Receive replies for DHCP options</td>
</tr>
<tr>
<td>68</td>
<td>HPDM PXE Server (bundled with HPDM Gateway)</td>
<td>HPDM Imaging Mini Linux Tool (client-side)</td>
<td>UDP</td>
<td>PXE bootstrap</td>
</tr>
<tr>
<td>5500</td>
<td>Windows platform: VNC Server (client-side)</td>
<td>Windows platform: SSL VNC Proxy (bundled with HPDM Agent) (loopback)</td>
<td>TCP</td>
<td>SSL VNC Proxy in Listen Mode (reverse VNC)</td>
</tr>
<tr>
<td>5900</td>
<td>SSL VNC Proxy (bundled with HPDM Console)</td>
<td>VNC Server (client-side)</td>
<td>TCP</td>
<td>VNC Shadow</td>
</tr>
<tr>
<td>40001</td>
<td>HPDM Gateway</td>
<td>HPDM Agent</td>
<td>TCP</td>
<td>Allows the HPDM Gateway to send tasks to the HPDM Agent</td>
</tr>
</tbody>
</table>
Table B-7  HPDM Agent ports (inbound) (continued)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>40001</td>
<td>HPDM Gateway</td>
<td>HPDM Agent</td>
<td>UDP</td>
<td>Allows the HPDM Agent to receive replies of broadcasting from the HPDM Gateway</td>
</tr>
<tr>
<td>40004</td>
<td>SSL VNC Proxy (bundled with HPDM Console)</td>
<td>SSL VNC Proxy (bundled with HPDM Agent)</td>
<td>TCP</td>
<td>VNC SSL Proxy in Listen Mode on the HPDM Agent</td>
</tr>
</tbody>
</table>

Table B-8  HPDM Agent ports (outbound)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 &amp; 21</td>
<td>HPDM Agent</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>22</td>
<td>HPDM Agent</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>67</td>
<td>PXE client (client-side)</td>
<td>HPDM PXE server (bundled with HPDM Gateway)</td>
<td>UDP</td>
<td>PXE bootstrap</td>
</tr>
<tr>
<td>67</td>
<td>HPDM Agent</td>
<td>DHCP server</td>
<td>UDP</td>
<td>Allows the HPDM Agent to send DHCP option requests</td>
</tr>
<tr>
<td>69</td>
<td>PXE client (client-side)</td>
<td>HPDM PXE server (bundled with HPDM Gateway)</td>
<td>UDP</td>
<td>TFTP (Trivial File Transfer Protocol)</td>
</tr>
<tr>
<td>137</td>
<td>HPDM Agent</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td>Allows NetBIOS Name Resolution</td>
</tr>
<tr>
<td>138</td>
<td>HPDM Agent</td>
<td>NetBIOS Datagram Service</td>
<td>UDP</td>
<td>Allows NetBIOS Datagram transmission and reception</td>
</tr>
<tr>
<td>139</td>
<td>HPDM Agent</td>
<td>NetBIOS Session Service</td>
<td>TCP</td>
<td>Allows NetBIOS Session Services connections</td>
</tr>
<tr>
<td>445</td>
<td>HPDM Agent</td>
<td>Microsoft Directory Services</td>
<td>TCP</td>
<td>For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes</td>
</tr>
<tr>
<td>5500</td>
<td>Windows platform: VNC Server (client-side)</td>
<td>Windows platform : SSL VNC Proxy (bundled with HPDM Agent)</td>
<td>TCP (loopback)</td>
<td>SSL VNC Viewer in Listen Mode (reverse VNC)</td>
</tr>
<tr>
<td>5900</td>
<td>SSL VNC Viewer (bundled with HPDM Console)</td>
<td>VNC Proxy (client-side)</td>
<td>TCP (loopback)</td>
<td>VNC Shadow</td>
</tr>
</tbody>
</table>
### Table B-8 HPDM Agent ports (outbound) (continued)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>989 &amp; 990</td>
<td>HPDM Console</td>
<td>FTPS server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>4011</td>
<td>PXE client (client-side)</td>
<td>Proxy DHCP service (third-party software)</td>
<td>UDP</td>
<td>Proxy DHCP service (an alternative to port 67 if port 67 is not available)</td>
</tr>
<tr>
<td>40000</td>
<td>HPDM Agent</td>
<td>HPDM Gateway</td>
<td>UDP</td>
<td>Allows the HPDM Agent to poll the HPDM Gateway</td>
</tr>
<tr>
<td>40003</td>
<td>HPDM Agent</td>
<td>HPDM Gateway</td>
<td>TCP</td>
<td>Allows the HPDM Agent to send reports to the HPDM Gateway</td>
</tr>
<tr>
<td>40004</td>
<td>Windows: SSL VNC Proxy (bundled with HPDM Agent); HP ThinPro: X11VNC (bundled with platform)</td>
<td>SSL VNC Proxy (bundled with HPDM Console)</td>
<td>TCP</td>
<td>SSL VNC Proxy in Listen Mode (reverse VNC)</td>
</tr>
<tr>
<td>40009</td>
<td>HPDM Agent</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>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 command to the HPDM Agent.</td>
</tr>
</tbody>
</table>

### Table B-9 Repositories ports (inbound)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 &amp; 21</td>
<td>HPDM Console</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>HPDM Gateway</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HPDM Agent</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Master Repository Controller</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>HPDM Console</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>HPDM Gateway</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HPDM Agent</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Master Repository Controller</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>137</td>
<td>HPDM Console</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td>For File and Printer Sharing to allow NetBIOS Name Resolution</td>
</tr>
<tr>
<td></td>
<td>HPDM Gateway</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HPDM Agent</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Master Repository Controller</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td></td>
</tr>
</tbody>
</table>
### Table B-9 Repositories ports (inbound) (continued)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>138</td>
<td>HPDM Console</td>
<td>NetBIOS Datagram Service</td>
<td>UDP</td>
<td>For File and Printer Sharing to allow NetBIOS Datagram transmission and reception</td>
</tr>
<tr>
<td>139</td>
<td>HPDM Console</td>
<td>NetBIOS Session Service</td>
<td>TCP</td>
<td>For File and Printer Sharing to allow NetBIOS Session Service connections</td>
</tr>
<tr>
<td>445</td>
<td>HPDM Console</td>
<td>Microsoft Directory Services</td>
<td>TCP</td>
<td>For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes</td>
</tr>
<tr>
<td>989 &amp; 990</td>
<td>HPDM Console</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>40012</td>
<td>HPDM Server</td>
<td>Master Repository Controller</td>
<td>TCP</td>
<td>Allows the HPDM Server to talk to the Master Repository Controller to manage the Master Repository (this port is for the Master Repository only)</td>
</tr>
</tbody>
</table>

### Table B-10 Repositories ports (outbound)

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 &amp; 21</td>
<td>Master Repository Controller</td>
<td>FTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>22</td>
<td>Master Repository Controller</td>
<td>SFTP server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>Receiver port</td>
<td>Sender</td>
<td>Receiver</td>
<td>Protocol</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>137</td>
<td>Master Repository Controller</td>
<td>NetBIOS Name Service</td>
<td>UDP</td>
<td>For File and Printer Sharing to allow NetBIOS Name Resolution.</td>
</tr>
<tr>
<td>138</td>
<td>Master Repository Controller</td>
<td>NetBIOS Datagram Service</td>
<td>UDP</td>
<td>For File and Printer Sharing to allow NetBIOS Datagram transmission and reception.</td>
</tr>
<tr>
<td>139</td>
<td>Master Repository Controller</td>
<td>NetBIOS Session Service</td>
<td>TCP</td>
<td>For File and Printer Sharing to allow NetBIOS Session Service connections.</td>
</tr>
<tr>
<td>445</td>
<td>Master Repository Controller</td>
<td>Microsoft Directory Services</td>
<td>TCP</td>
<td>For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes.</td>
</tr>
<tr>
<td>989 &amp; 990</td>
<td>Master Repository Controller</td>
<td>FTPS server (third-party software)</td>
<td>TCP</td>
<td>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.</td>
</tr>
</tbody>
</table>
C 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>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMATION</td>
<td>Logs of running information, contains no errors</td>
</tr>
<tr>
<td>WARNING</td>
<td>Low-level error</td>
</tr>
<tr>
<td>ERROR</td>
<td>Significant errors</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE</td>
<td>Some trace logs; for example, number of HPDM Agents</td>
</tr>
<tr>
<td>DEBUG</td>
<td>Internal debug logging</td>
</tr>
<tr>
<td>INFO</td>
<td>Log of some report content</td>
</tr>
</tbody>
</table>
Table C-2  HPDM Gateway logging (continued)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARN</td>
<td>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</td>
</tr>
<tr>
<td>ERROR</td>
<td>Significant errors</td>
</tr>
<tr>
<td>FATAL</td>
<td>High-level error; the error will usually prevent HPDM Gateway from running normally</td>
</tr>
</tbody>
</table>

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 C-3  HPDM Server and HPDM Console logging

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEBUG</td>
<td>Low-level debugging information</td>
</tr>
<tr>
<td>INFO</td>
<td>Logs of running information, contains no errors</td>
</tr>
<tr>
<td>WARN</td>
<td>Logs with warning, means something unexpected happened</td>
</tr>
<tr>
<td>FATAL</td>
<td>Fatal errors</td>
</tr>
</tbody>
</table>

To change the logging level for the HPDM Server, change the value of the hpdm.log.level in the file /Server/conf/server.conf in the install folder.

To change the logging level for the HPDM Console, change the value of the hpdm.log.level in the file /Console/conf/console.conf in the install folder.

**Master Repository Controller logging**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMATION</td>
<td>Logs of running information, contains no errors</td>
</tr>
<tr>
<td>WARNING</td>
<td>Low-level error</td>
</tr>
<tr>
<td>ERROR</td>
<td>Significant errors</td>
</tr>
</tbody>
</table>

To change the logging level for the Master Repository Controller, change the value of Loglevel in the file Controller.conf in the install folder.
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.
HP FTP Software Component Browser provides a means to automate the process of leveraging software components from the HP public FTP site.

Currently, there are two kinds of components:

- Image file
- Application file

You can use HP FTP Software Component Browser to generate specified templates by downloading the component file. An image file will be generated as a **Deploy Image** template, while an application file will be generated as a **File and Registry** template.

To use HP FTP Software Component Browser:

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 under the **Task Templates** view. 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 HPDM 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 thin client.
Index

A
Activity Directory 56
adding
  group 55
  report template 61
  users 54
assigning
  permissions to groups 55
  users to groups 54
authentication key
  export 59
  import 60
  update 59
  view 60
authentication management 59

B
backup 69

C
changing
  connection settings 41
  device settings 41
  registry settings 46
  user password 54
Child Repositories
  configuring 51
  deleting 51
  description 4
client BIOS settings, PXE 36
client discovery 16
  manual registration 18
  server-side 17
  walking with IP list 17
  walking with IP range 17
client, discovering 16
cloning
  device settings 42
command execution, remote 49
configuration
  LDAP server connection 56
  network 72
  status walker 85
connection settings, changing 41
copying files 47

D
deleting
  groups 56
  users 54
deploying
  images 39
device filters
  creating 32
  editing 33
device management 30
devices
  adding using MAC addresses 43
  applying tasks to 25
  changing settings 41
  definition 5
  deleting 31
  grouping 31
  icons 30
  printing information 34
  properties, displaying 14
  shadowing 34
DHCP
  Linux server 73
  server, configuring for PXE 72
tag 202 16
DHCP tag 32
tag 203 31, 32
discovering clients 16

E
Easy Update 87
editing settings 46
export authentication key 59

F
file and registry 46
file and registry templates
  capture files sub-task 43
  command sub-task 44
  delete files sub-task 44
  deploy files sub-task 44
  merging 45
  pause sub-task 45
  registry sub-task 44
  using 43
files, copying 47
filter
  device, editing 33
  security 33
FTP 50
  mappings 52
FTPS 50

generating report using template 61
getting settings 46
grouping
  devices 31
groups
  adding 55
  assigning permissions to 55
  assigning users to 54, 55
  deleting 56
  import 57

H
HPDM
  task 23
HPDM Agent
  Agent 14, 64, 65
  description 3
  system requirements 8
HPDM Console
  description 3
  HPDM Gateway tab 13
  system requirements 7
HPDM Gateway
  access control 60
HPDM installation 10
HPDM overview 2
HPDM Server 29
description 3
system requirements 7

images
capture from client with PXE 36
capturing from thin client without PXE 37
pushing to client 37
updating 39
import
authentication key 60
report plug-in file 61
users and groups 57
IP scope, configuring 17

key management 59

LDAP server 56
log in, HPDM console 11

MAC addresses, using to add devices 43
mappings, FTP 52
Master Repository
configuring 50
description 4
Master Repository Controller
system requirements 8

Neoware, legacy client BIOS settings 36
network
checking connection status 34
configuration 72
network requirements 9

opening VNC viewer 28
operations
agent 64

packages
definition 5
parameters
task 24
permissions, assigning to groups 55
ports 75
power management 35
properties
displaying task 26
pushing PXE image to client 37
PXE
capture image from client 36
client BIOS settings 36
configuring DHCP server 72
configuring routers 74
definition 5
pushing image to client 37

registry
changing settings 46
editing settings 46
getting settings 46
remote
command execution 49
execution of Windows scripts 49
report
adding template 61
generating using 61
importing plug-in file 61
management 61
Reporting 62
repositories 50
content management 51
description 4
exporting 51
importing 51
management 50

requirements 9
synchronizing 51
restore 69
result template, opening 28
router, configuring for PXE 74
rules
definition 5

security
authentication management 59
filter 33
HPDM Gateway access control 60
key management 59
management 54
user authentication 56
settings
applying 42
changing file and registry 46
cloning 42
ingoing file and registry 46
getting file and registry 46
SFTP 50
shadowing 28
shadowing devices 34
Share Folder 50
status
checking network connection 34
status snapshot 86
status walker 85
configuring 85
system requirements
HPDM Agent 8
HPDM Console 7
HPDM Gateway 8
HPDM Server 7
Master Repository Controller 8
network 9
repositories 9

task templates
adding to favorites 20
creating/editing 20
definition 5
importing/exporting 21
management 19
removing a plugin 20
sequencing 20
tasks 19
applying to devices 25
configuring parameters 26
continuing 27
deferment 26
definition 5
deleting 27
displaying logs 28
displaying properties 26
icons 23
management 23
operating system 41
parameters 24
pausing 27
performing 23
resending 27
settings 24
status icons 23
template sequences
advanced 68
basic 67
definition 5
using 20
terms and definitions 5
thin client
defining rules 28
defining tasks 24
grouping 31
imaging 36
reporting 62
U
updates
documentation 5
software 5
updating
authentication key 59
user management 54
users
adding 54
assigning to groups 54, 55
authentication 56
changing password 54
deleting 54
import 57
V
view
authentication key 60
W
walking
with IP list 17
with IP range 17
write filters 5