About this book

⚠️ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

EdgeInsets: Text set off in this manner provides important supplemental information.
1 Introduction ...................................................................................................................... 1
   What is HP Device Manager? ............................................................................................. 1
   Overview ........................................................................................................................... 2
      HP Management Console ............................................................................................ 2
      HP Management Server .............................................................................................. 3
      HP Management Gateway .......................................................................................... 3
      Device Agent .............................................................................................................. 3
      File Repositories ........................................................................................................ 3
   Concepts ........................................................................................................................... 4
      Agent Mode .................................................................................................................. 4
      Managed Device ........................................................................................................... 4
      Package ....................................................................................................................... 4
      PXE ............................................................................................................................. 4
      Repository ................................................................................................................... 4
      Rules ............................................................................................................................ 5
      Task ............................................................................................................................. 5
      Task Template ............................................................................................................. 5
      Template Sequence ..................................................................................................... 5
      Write Filter .................................................................................................................. 5
   Getting more information ............................................................................................ 5
      The Internet ................................................................................................................ 5
      Technical support ....................................................................................................... 6

2 Getting started with HP Device Manager ........................................................................... 7
   Installing HP Device Manager .......................................................................................... 8
   System requirements ..................................................................................................... 8
      Management Console .................................................................................................. 8
      Management Server .................................................................................................. 9
      Management Gateway .............................................................................................. 9
      Management Agent .................................................................................................. 10
      Master Repository Controller .................................................................................... 11
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per device mapping</td>
<td>134</td>
</tr>
<tr>
<td>9 Security management</td>
<td>136</td>
</tr>
<tr>
<td>User management</td>
<td>136</td>
</tr>
<tr>
<td>Adding users</td>
<td>136</td>
</tr>
<tr>
<td>Deleting users</td>
<td>137</td>
</tr>
<tr>
<td>Assigning users to groups</td>
<td>137</td>
</tr>
<tr>
<td>Changing a user’s password</td>
<td>138</td>
</tr>
<tr>
<td>Assigning Security Filters to Users</td>
<td>139</td>
</tr>
<tr>
<td>Adding a group</td>
<td>141</td>
</tr>
<tr>
<td>Assigning permissions to groups</td>
<td>141</td>
</tr>
<tr>
<td>Assigning users to groups</td>
<td>142</td>
</tr>
<tr>
<td>Assigning security filters to groups</td>
<td>143</td>
</tr>
<tr>
<td>Deleting groups</td>
<td>144</td>
</tr>
<tr>
<td>User authentication with LDAP and Active Directory</td>
<td>144</td>
</tr>
<tr>
<td>Configuration</td>
<td>144</td>
</tr>
<tr>
<td>Importing users and groups</td>
<td>148</td>
</tr>
<tr>
<td>Authentication management</td>
<td>155</td>
</tr>
<tr>
<td>Key management</td>
<td>155</td>
</tr>
<tr>
<td>Gateway access control</td>
<td>158</td>
</tr>
<tr>
<td>10 Report management</td>
<td>160</td>
</tr>
<tr>
<td>Adding a Report template</td>
<td>160</td>
</tr>
<tr>
<td>Importing a report plug-in file</td>
<td>164</td>
</tr>
<tr>
<td>Generating a report using a Report template</td>
<td>165</td>
</tr>
<tr>
<td>Producing reports</td>
<td>167</td>
</tr>
<tr>
<td>Gateway report</td>
<td>167</td>
</tr>
<tr>
<td>Device Information report</td>
<td>167</td>
</tr>
<tr>
<td>Device Task report</td>
<td>168</td>
</tr>
<tr>
<td>Task report</td>
<td>169</td>
</tr>
<tr>
<td>Task Status report</td>
<td>169</td>
</tr>
<tr>
<td>Task Log report</td>
<td>170</td>
</tr>
<tr>
<td>11 Template reference</td>
<td>172</td>
</tr>
<tr>
<td>File and Registry</td>
<td>172</td>
</tr>
<tr>
<td>_File and registry</td>
<td>173</td>
</tr>
<tr>
<td>_Get registry</td>
<td>174</td>
</tr>
<tr>
<td>Agent</td>
<td>174</td>
</tr>
<tr>
<td>_Configure Agent</td>
<td>175</td>
</tr>
<tr>
<td>_Configure Task Deferment</td>
<td>176</td>
</tr>
</tbody>
</table>
12 Backing up and restoring the HPDM Server and database ............................................... 196

Appendix A Network configuration .......................................................................................... 199
  Configuring DHCP servers ................................................................................................. 199
    Management Server installed separately to the DHCP server ........................................ 199
    Management Server installed on DHCP server machine .............................................. 199
  Configuring a Linux DHCP server .................................................................................... 201
  Configuring routers ........................................................................................................... 201

Appendix B Port usage ......................................................................................................... 202
### Appendix C  Agent polling and error logging

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent polling</td>
<td>205</td>
</tr>
<tr>
<td>Error logging</td>
<td>206</td>
</tr>
<tr>
<td>Agent logging</td>
<td>206</td>
</tr>
<tr>
<td>Gateway logging</td>
<td>206</td>
</tr>
<tr>
<td>Server and Console logging</td>
<td>207</td>
</tr>
<tr>
<td>Master Repository Controller logging</td>
<td>207</td>
</tr>
</tbody>
</table>

### Appendix D  Status Walkers

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Walker</td>
<td>208</td>
</tr>
<tr>
<td>Creating a Status Walker</td>
<td>209</td>
</tr>
<tr>
<td>Configuring the Status Walker</td>
<td>214</td>
</tr>
<tr>
<td>Status Snapshot</td>
<td>215</td>
</tr>
</tbody>
</table>

### Appendix E  Easy Update

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
</table>

### Index

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
</table>
1 Introduction

What is HP Device Manager?

HP Device Manager is a server-based application that provides sophisticated centralized administration capabilities for thin client devices running HP software. Features of HP Device Manager include:

- 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

HP Device Manager is structured as a Console–Server–Gateway system.

**Figure 1-1** HP Device Manager overview

![Diagram of HP Device Manager system]


**HP Management Console**

The HP Management Console is the user interface of HP Device Manager. Several HP Management Consoles can interact with an HP Management Server. The console allows system administrators to view details for each controlled device, organize device trees, create and maintain remote job definitions, and monitor tasks sent out to devices.
**HP Management Server**

The HP Management Server controls agents through the HP Management Gateway. Tasks, stored as Task Templates on the server, can be sent to each agent through each agent’s respective gateway to perform commands as required.

**HP Management Gateway**

The HP Management Gateway serves as the link between devices and the HP Management Server. Devices register with the gateway when they are started. The machine installed with the HP Management Gateway also normally contains the PXE Server installed by HP Device Manager. Multiple Gateway systems may be required in order to span several subnets. In a simple single network environment, the Gateway system may be the same system that contains the HP Management Server.

**Device Agent**

The HP Device Management Agent is a software component installed on thin client devices so that HP Device Manager can interact with them. Agents are embedded into the operating system to enable HPDM to manage devices out-of-the-box (agents on older devices may need to be upgraded). Agents receive task commands from an HPDM Gateway, execute the commands and report back to the Gateway with the results.

**File Repositories**

File Repositories are where files are stored in a repository of components, images, etc. that can be uploaded from or downloaded to the agents at the request of the HP Management Server. There are two types of repositories, the Master Repository and the Child Repositories. You can create multiple Child Repositories on different servers.

On the machine where the Master Repository resides, a component named Master Repository Controller is installed along with the Master Repository. The Master Repository Controller manages the content in the Master Repository and synchronizes that content to Child Repositories as requested by the HPDM Server. The supported file transferring protocols for FTP Repositories are FTP, FTPS, SFTP, and Server Message Block (SMB).

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Windows is known as the Shared Folders functionality. The Common Internet File System (CIFS) Protocol is a dialect of SMB.
Concepts

Agent Mode

Agent Mode is the mode of the Management Agent to acquire tasks from the Management Gateway. Through configurations to the Agent mode, the agent can work at the NAT network without Gateway. The Agent mode can be either Push mode or Pull mode. Push mode means the gateway sends the available task to the agent, and Pull mode means the agent would request the task from the gateway at regular intervals.

Managed Device

Managed device, client device, remote device, or device, as mentioned in this guide, means a device managed by HP Device Manager, such as a thin client.

Package

A Package is a basic unit that the system manipulates and that repositories embrace, and which is comprised of a description file and a folder which contains payload files. The package name is identical to the folder name, and the folder name can be any legal string. The name of the description file follows the convention “PackageName-ChecksumString.desc”. The checksum is computed from all payload files in alphabetical sequence of file name or folder name with depth-first traverse.

PXE

Preboot eXecution Environment (PXE) is a network protocol used to boot computers using a network interface independently of data storage devices or installed operating systems.

HP Device Manager utilizes PXE to execute thin-client image extraction and distribution.

Repository

A Repository is a collection of elements which may consist of software components, system images, diagnostic tools, and agent files stored on one or more FTP servers. The accessing protocols DM can support are generic FTP, FTP Secure (FTPS), Secure FTP (SFTP), and SMB (Windows Share-folder / Linux Samba). Repositories with various protocols can co-exist in one DM environment, and multiple protocols are able to be applied to one repository. Repositories may reside across several servers, these being the Master Repository and one or more Child Repositories.

SMB is required by PXE-less imaging tasks for the WES 7 platform. The FileZilla server application or Microsoft IIS is recommended for FTP/FTPS, and the Open SSH Server application is recommended for SFTP.

There is a Master Repository containing all content that resides along with the Master Repository Controller. The consistency of resources in all other repositories is ensured by means of automated synchronization.
Rules

Rules enable you to automate the execution of tasks. 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.

Task

A Task is the scheduled action to 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 thin clients.

Task Template

A Task Template (or Template) is the definition of actions an administrator may use to remotely control devices. Each Task Template is an XML file that defines the configuration change or software update that administrators want the remote devices to perform.

HP Device Manager provides a variety of built-in Task Templates on how to manage remote devices, including device name changes, network settings, home URL changes, ICA connection clones, add/remove software components, and so on.

Task Templates can be imported or exported by using tools on the Management Console. New Task Templates can be downloaded from HP’s FTP site, then imported to your HP Management Server.

Template Sequence

A Template Sequence (or Sequence) is a special kind of task template that enables you to connect several templates together and send them out for execution in one task.

Write Filter

The 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, the Write Filter allows the run-time image to maintain the appearance of a writable run-time image. Additionally, the 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, the traditional partition-based Enhanced Write Filter (EWF) and the File-based Write Filter (FBWF).

Getting more information

The Internet

Current and archival information about HP products, including the latest software updates, is available at:

http://www.hp.com/go/hpdm
— or —
In addition, this user guide and more HP documentation are available at the HP website and FTP site for browsing or downloading.

**Technical support**

Please visit [http://www.hp.com/support](http://www.hp.com/support) and search for HP Device Manager.
2 Getting started with HP Device Manager

In order to begin using HP Device Manager you will need to:

- Perform software installation and configure your network environment
- Understand the management console
- Add client systems to the HPDM asset database

The following sections describe each of these topics.
Installing HP Device Manager

This section will guide you through the installation of HP Device Manager.

System requirements

The following sections describe the minimum system requirements for the installation of each of the product components.

Management Console

The Management Console can be installed on any number of machines. The following environment is required:

- **Operating system**
  
  - Windows Server 2003 with Service Pack 2 (64 bit)
  
  - Windows Server 2003 R2 with Service Pack 2 (32 & 64 bit)
  
  - Windows Server 2008 with Service Pack 2 (32 bit)
  
  - Windows Server 2008 R2 with Service Pack 1 (64 bit)
  
  - Windows XP Professional with Service Pack 3 (32 bit)
  
  - Windows 7 Enterprise with Service Pack 1 (64 bit)

- **Third-party software**

  Java™ Runtime: SUN Java Runtime Environment version 6 update 2

  **NOTE:** Java Runtime is installed with HP Device Manager.

- **Hardware**

  - Pentium® III or greater
  
  - 512 MB RAM
  
  - 256 MB free disk space
Management Server

There must be only one Management Server in the system. The following is the minimal hardware and software requirements for running the Management Server:

- **Operating system**
  - Windows Server 2003 with Service Pack 2 (64 bit)
  - Windows Server 2003 R2 with Service Pack 2 (32 & 64 bit)
  - Windows Server 2008 with Service Pack 2 (32 bit)
  - Windows Server 2008 R2 with Service Pack 1 (64 bit)

- **Third-party software**
  - Java Runtime: SUN Java Runtime Environment version 6 update 2.
  - **NOTE:** Java Runtime is installed with HP Device Manager.
  - DBMS—any of the following are supported: Microsoft SQL Server 2005 or later and PostgreSQL 8.3 or later (bundled with installer).
  - **NOTE:** PostgreSQL is included in the HPDM distribution. If you select PostgreSQL as your database, it will be installed from the installation media.

- **Hardware**
  - Pentium® III or greater
  - 512 MB RAM
  - 512 MB free disk space

Management Gateway

The Management Gateway may be installed on multiple machines. However, only one Gateway should be present on a subnet. The following environment is the minimal hardware and required software for running the Management Gateway:

- **Operating system**
  - Windows Server 2003 with Service Pack 2 (64 bit)
  - Windows Server 2003 R2 with Service Pack 2 (32 & 64 bit)
  - Windows Server 2008 with Service Pack 2 (32 bit)
  - Windows Server 2008 R2 with Service Pack 1 (64 bit)

- **Hardware**
  - Pentium® III or greater
  - 512 MB RAM
Management Agent

The Management Agent should be installed on each thin-client device that will be managed by the system. The following environment is required for running the Management Agent:

- **Operating system**
  - HP XPe*, WES09, WES7E, WES7P
  - HP CE 6*
  - HP ThinPro 3, HP ThinPro 4
  - HP Smart Zero Core

**NOTE:** For the operating systems marked with an asterisk “*” symbol, HP Device Manager 4.5 only provides limited support. The newly added features may or may not work with these operating systems. These operating systems are not under full test by the HP Device Manager Product Development Team. The latest stable HP Device Manager release that has been fully tested with these operating systems is HP Device Manager 4.4 (installer version: 4.4.12440, built on 08/29/2011).

- **Hardware**

Thin-client device supporting one of the operating systems listed above

2 MB free disk space

The following HP thin clients are supported:

- HP XPe*, WES09, WES7E, WES7P
  - t610, t510, t5740, t5740e, t5570, t5570e, t5400, t57720, 6360t, mt40
- HP CE 6*
  - t510, t5550
- HP ThinPro 4
  - t610, t510, t5745, t5565
- HP ThinPro 3
  - t5745, t5565
- HP Smart Zero Core
  - t610, t510, t410, t410 All-in-One, t5565z, t5335z

512 MB free disk space
NOTE: For the operating systems marked with an asterisk “*” symbol, HP Device Manager 4.5 only provides limited support. The newly added features may or may not work with these operating systems. These operating systems are not under full test by the HP Device Manager Product Development Team. The latest stable HP Device Manager release that has been fully tested with these operating systems is HP Device Manager 4.4 (installer version: 4.4.12440, built on 08/29/2011).

**Master Repository Controller**

There must be only one Master Repository in the system. The Master Repository needs to be managed by a Master Repository Controller, which must be installed on the same machine as the Master Repository. The Master Repository Controller may or may not be installed on the same host machine as the Management Server. The Master Repository Controller must be installed on a machine that has installed the service supporting any of the following file transferring protocols: FTP, FTPS, SFTP, or SMB (Share Folder). The following environment is the minimal hardware and required software for running the Master Repository Controller:

- **Operating system**
  - Windows Server 2003 R2 with Service Pack 2 (64 bit)
  - Windows Server 2008 R2 with Service Pack 1 (64 bit)

- **Hardware**
  - Pentium® III or greater
  - 512 MB RAM
  - 2 GB free disk space

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

**File Repositories**

To transfer any files to or from the managed thin clients or to pull or push thin client operating system images, one or more servers that support any of the FTP, FTPS, SFTP, or SMB protocols must be accessible by the Management Console, Management Gateway, or the Management Agent. These are referred to as the File Repositories. HP Device Manager will need to have read and write access and will automatically synchronize content on the FTP Repositories. The FTP, FTPS, SFTP, and SMB protocols are supported.

**Recommended FTP servers—Third-party software**

- Filezilla Server
- Microsoft Internet Information Server (IIS) 6.0 or later
- freeSSHd
Network requirements

The following are further requirements for your network environment:

- HP Device Manager only supports IPv4 networks.
- HP Device Manager can image thin clients using either PXE or PXE-less (preferred) methods. If PXE imaging is desired, then you must ensure that there are no other PXE services running on the network.
- A number of UDP and TCP ports are required for client/server communication. See Port usage on page 202 for a list of standard and custom ports required.
- If you are using a Server behind a firewall, you must add ports 1099 and 40002 to the exception ports in the firewall settings.
- If you are using an ISC DHCP server, it must be running at least version 3.0.

Installation procedure

If the software required to run HP Device Manager is already installed on the local computer, the installation program will detect it and attempt to perform a product upgrade.


**NOTE:** Different operating systems may have slightly different steps and wording for the installation process.

1. Run the Device Manager InstallShield Wizard. The installation’s introductory dialog box will appear.
   
   Click Next>.

2. Review all the terms in the License Agreement.
   
   If you agree to these terms, click Yes.

3. Review the System Requirement information.
   
   If your system meets these requirements, click Next>.

4. In the Choose Destination Location dialog box, select the folder where HP Device Manager will be installed. Accept the default folder or click Browse and navigate to a specific location.
   
   When you have chosen the installation location, click Next>.
5. This step allows you to select a setup type.

- **Complete** - The Management Console, Server, Gateway, and Master Repository Controller will be installed with their default configurations.

- **Custom** - Select the components to install and specify the configuration of each one:
  - **Console**—Does not require any configuration.
  - **Server**—You can choose which database will be used for the Server. The optional databases are PostgreSQL and Microsoft SQL Server.
  - **Gateway**—You should configure DHCP and Gateway settings. 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 gateway, etc.).
  - **Master Repository Controller**—You should configure the root path where the Master Repository will store the necessary HPDM tools and files.

Select the desired setup type and click **Next>**.

6. If you selected **Custom** as the desired setup type you will now have to select the HP Device Manager components that you wish to have installed.

Click **Next>**.

7. If you selected **Custom** as the desired setup type and selected the component **Master Repository Controller**, or if you selected **Complete** as the desired setup type, the **HP Device Manager Master Repository Root Path** dialog box will appear. In this dialog box, select the folder where the Master Repository will be stored. Accept the default root path or click **Browse** and navigate to a specific location. When you have chosen the location, click **Next**.

8. If you wish to review any of the installation settings, click **<Back**.

If you are satisfied with the installation settings, click **Install**.

9. Once you confirm the installation parameters, the installation process proceeds. During the installation, the HPDM Configuration Wizard launches to guide you through the key configuration settings.
The following describes the steps of the HPDM Configuration Wizard. The left-hand pane lists all of the configuration steps that will be performed and indicates which step is the current step. The right-hand pane contains the configuration options for the current step.

a. **Language setting** - Select the desired language and click **Next** to continue.

   **NOTE:** HPDM version 4.5 supports English, German, Japanese, Korean, Chinese (Simplified), French, Chinese (Traditional), and Spanish.

b. **Port Checking** - This step verifies that the system’s ports are correctly configured and that the system is capable of supporting HPDM.

   Clicking **Check** launches a scan of the required network ports to ensure that all of the ports are available.

   The network should permit free communication on ports used by HP Device Manager. When a problem is detected, the HPDM Configuration Wizard port scan flags the problem so you can correct the issue before continuing. You are not required to stop and restart the installation in order to address port issues. When the check detects an issue the corresponding port is flagged as shown below:

   A warning icon is used to indicate that the scan has detected a problem with a port. The **Component** column indicates which HPDM component needs to utilize the port. Use the HPDM port list, see Port usage on page 202 to narrow down the issue.

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

   Click **Check** to rescan after attempting to resolve a problem. Click **Next** to continue after all issues have been resolved.

c. **DHCP Settings for PXE** - This step guides you in setting up DHCP to ensure that all clients that receive their addressing through DHCP also get the information they will need to contact the HPDM PXE server. If the local server is not providing DHCP, you must ensure that there is a network accessible DHCP server available to provide the necessary DHCP options. If you are using a local DHCP service, you configure the options as indicated in the wizard screen.

   Click **Next** to continue.

d. The **HPDM Gateway configuration** wizard step displays the standard **HPDM Gateway configuration** dialog.

   The settings of this dialog that should be reviewed at this time are:

   - **Server Address** - The address for the Management Server to which the Gateway will report. Using **localhost** will work when both the Server and Gateway are on the same system but it is better practice to use the actual address.

   - **Local NIC** - The NIC through which the 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** - Determines whether the PXE service is started along with the Gateway. The PXE service is always installed with the Gateway but can be independently controlled (by changing this setting to NO) if
required. You should set this to YES for most situations so the PXE service starts/stops when the Gateway starts/stops.

Click **Next** to continue.

e. The **Result** wizard step provides a viewable summary of the settings and results from each of the previous wizard steps. The selected settings are not applied until you click **Execute**.

f. The HPDM Configuration Wizard dialog will remain visible after you click **Execute**.

When the setup completes, the **Execute** button changes to a **Finish** button. When the **Finish** button displays, you can click **View** to view the results for the different configuration steps on the **Result** pane to view a report on each configuration task.

Click **Finish** to continue.

10. After the HPDM Configuration Wizard completes the InstallShield process continues. Next the standard HPDM Database dialog displays. Select the desired database option and click **Next** to continue.

**NOTE:** When customers choose MS SQL SERVER as the Device Manager database and use Windows Authentication type, they need to type the account and password. The Server will be started as a Service using the specified account.

11. Enter the database admin credentials and click **Next**.

12. Enter the administrator’s user name and password for HP Device Management Server, then click **Finish**.

13. The installation has completed.

Click **Finish** to exit the installation wizard.

If the Management Console, Server, Gateway, and Master Repository Controller are set up successfully, icons of the Server and Gateway will be displayed in the Systray of your machine as shown below:

**Figure 2-1** HPDM Server and HPDM Gateway—Sys tray icons

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

**NOTE:** You can start/stop services and configure the Gateway server again by using the menu options displayed when you right-click on the Sys tray icons.

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

**Figure 2-2** HPDM Management Console—Desktop icon
In some cases there will be other network configuration changes that may need to be made, see Network configuration on page 199.
Using the HPDM Management Console

Logging in to the HPDM Management Console

To launch the HPDM Management Console:

1. Either double-click the **HP Device Management Console** icon on the Windows desktop, or from the **Start** menu select **Programs > HP > HP Device Manager > HP Device Management Console**

   The **Log in** dialog box will appear.

2. Enter the **Server Address** of your network’s HP Management Server. The address can be entered as an IP address or as a machine name. If the console is on the same machine as the HP Management Server, then enter **localhost**.

3. Enter your **Username** and **Password** in their respective fields.

4. Click **OK** to log in to the Console.

   Once the username and password are verified, the main window of the HP Management Console appears.

Management Console overview

The management 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 discrete operating systems that have been identified on the thin client systems. There is one tab for each thin 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 view tabs produces the following view:

Figure 2-3  HPDM Management Console—Operating system tabs

1. **OS Tabs** - Selects the different categories of terminal operating systems that are controlled by HP Device Manager. Note that only the tabs for the operating system types of the devices currently managed by HP Device Manager 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 OS 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 HP Management 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 gateway.

**Figure 2-4** HPDM Management Console—Gateway tab

1. Tree view of HPDM Gateway systems
2. List of tasks applied to the gateway, such as discover devices.
Discovering client systems

Now that you have installed the HPDM software and you have a basic understanding of the management console, you can proceed to the next step, which is adding client systems to the HPDM asset database. There are two methodologies for adding client systems to the HPDM asset database, from the HPDM Server (discovering client systems) or from the client systems (registering client systems). These processes insert information into the HPDM asset database about client systems which you will be managing.

Normally the HPDM Gateway system will be able to detect most HP thin client systems by listening for a network broadcast message made by an HP thin client when it starts. This solution does require that the HPDM Gateway system is running before the thin client starts. For other methods to add thin clients to the HPDM asset database, see Client discovery on page 24.
Displaying device properties

HPDM stores asset information about each thin client it manages. When a thin client registers with the HPDM Server it passes just enough asset information to uniquely identify the thin client and allow HPDM to communicate with it. Complete asset information can then be retrieved by sending a Get Device Asset Information task to the thin client. The information returned by this task is stored in the HPDM asset database.

Basic asset information

Double-clicking a thin client icon in the 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 thin client views.

<table>
<thead>
<tr>
<th>Table 2-1 Basic asset information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>Device ID</td>
</tr>
<tr>
<td>Host Name</td>
</tr>
<tr>
<td>Device Type</td>
</tr>
<tr>
<td>Device Version</td>
</tr>
<tr>
<td>Device Serial Number</td>
</tr>
<tr>
<td>OS Type</td>
</tr>
<tr>
<td>MAC Address</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet Address</td>
</tr>
<tr>
<td>Agent Version</td>
</tr>
<tr>
<td>HPDM Gateway ID</td>
</tr>
<tr>
<td>Agent Working Mode</td>
</tr>
<tr>
<td>First Contact Time</td>
</tr>
<tr>
<td>Last Time Online</td>
</tr>
<tr>
<td>BIOS Version</td>
</tr>
<tr>
<td>Asset Tag</td>
</tr>
</tbody>
</table>
### Initiating a Get Device Asset Information task

To collect more information about a thin client you must execute an HPDM task—the **Get Device Asset Information** task.

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

1. Right-click the thin 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 thin client’s **Properties** window.

### Displaying complete thin client asset information

After a successful **Get Device Asset Information** task the additional tabs in the thin client’s **Properties** window will be populated:

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

### Keeping the HPDM Agent updated on client systems

HPDM Server has built-in rules to automatically update the HPDM Agent on thin client systems to the latest version. Each operating system type has a system rule with a startup trigger. When thin clients startup and report to the HPDM Server, the rule will compare the thin client’s agent version to the version in the server repository. If the thin client has an older version, the HPDM Server will send a task to the thin client to update its agent.
**NOTE:** This rule is disabled by default.
3 Client discovery

Clients which have the HP Management Agent installed must be discovered (added to the HPDM asset database) by HP Device Manager before they can be managed. There are three approaches to client discovery:

- HP Management Agent broadcast (Automatic Registration)
- Server-side discovery
- Manual Client configuration

Automatic registration

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 Agent works through these methods in order and stops as soon as one is successful. If the Agent loses contact with its current 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 Gateway to use. These settings will only be preset on thin clients that are shipped with a custom factory image and this option must have been included in the specification of the custom image. If the primary Gateway is set the agent will try to contact it. If that fails and a backup Gateway is also set it will then try to contact that. If that also fails the agent will move on to the next method.

2. The 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 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:

   192.168:t - 1.5:t: 192.168; 1.1

   The Agent will attempt to connect to the Gateway 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 Agent will send a request to the broadcast address of its subnet. If a Gateway is present on the subnet it will reply to the broadcast and the Agent will connect to it.
Server-side discovery

HP Device Manager can search a range of IP addresses for agents and gateways. There are two methods: Walking With IP Range and Walking With IP List. Each of these methods begin in the same manner:

▲ In the Management console, click the HPDM Gateway tab, right-click the gateway and select Discover Device in the context menu.

To search using the Walking With IP Range method:

1. Select Walking With IP Range, 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 a manually-specified IP range: deselect the Use Preset IP Scope checkbox and enter a Starting IP Address and an Ending IP Address. Click OK.

   ● To search using an IP scope: Click Use Preset IP Scope then select an IP Search Scope and click OK.

You can check the progress of the Discover Device task by displaying the HPDM Gateways tab and selecting the name of the gateway. The discovery progress will be displayed in the tasks pane at the bottom of the console window.

To configure an IP scope:

a. In the Discover by Range dialog box, select Use Preset IP Scope checkbox, and select the Edit option in the IP Search Scope list box to display the Edit IP Walking Scope dialog box.

b. Select an existing IP scope from the IP Walking Scopes list or click Add to create a new one.

c. Enter a scope name to be used by HPDM to refer to the new search scope, then click OK.

d. Define the IP address range you want HP Device Manager to search for client agents by filling in the Starting IP Address and Ending IP Address. Click Apply to save the settings, then OK to exit.

To search using the Walking With IP List method:

1. Select Walking With IP Range, Click Next >.

2. The Discover by List dialog box is displayed.

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>Button</td>
<td>Function</td>
</tr>
<tr>
<td>--------</td>
<td>----------</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 agents or gateways. Once the search has finished, a report will show the clients detected by HP Device Manager. When devices are found, they are added to the HPDM asset database.

**Manual configuration**

The following methods can be used to manually add a device to the HPDM asset database:

**Manually adding a device from the client**

You can manually register the HPDM Agent from the client device. To do so:

1. Switch to **Administrator** mode (see your thin client operating system documentation for instructions).
2. Open the **HP Agent** applet in the control panel.

**Figure 3-1** HPDM Agent

3. Enter the IP address of the gateway in the **Current Gateway** field (new feature since 4.4).
4. Click **OK**.
NOTE: If your devices are in a NAT environment, they will not be able to automatically discover their
gateway via DHCP. In that case, you should use the above procedure to manually set their current
gateway to the appropriate IP address. They will then connect to that gateway the next time they are
rebooted.

Manually adding a device from the Management Console

1. Using the Management Console, click the HPDM Gateways tab, right-click the gateway you
   wish to have connect to the thin client.

2. From the context-sensitive menu, select Device -> Add.

3. Enter the Device ID, MAC Address and IP Address of the device and click OK.

4. 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.
HP Device Manager performs many of the operations required for client management by the use of tasks. Tasks are individual operations performed on individual client systems. A task operation might be to instruct a client system rename a local file, or change a registry value. A task is the actual execution of the requested operation; an HPDM task may be thought of as the execution of a batch job; it has execution parameters, an effect and a resultant output log.

The vehicle used to define a task’s exact operations is task templates. Task templates contain the logic used to accomplish a specific operation. Task templates are similar to a batch file—the task template contains the commands to execute and the actual execution of a task template is a task. This is analogous to a batch file that contains commands that can be executed as a batch job.

The controlled triggering of a task’s execution can be specified with task rules. Task rules are a way to specify that a particular task should be executed based on specific criteria being met. HPDM and the HPDM client Agent cooperate in watching for task rule trigger conditions.
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
- **Agent**—Used to configure Agent settings and update the 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 so they can be shared between HP Device Manager systems.

To export Task Templates:

1. Right-click the template to export and select **Export**.

**Figure 4-1** Exporting a Task Template

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 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.

   **Figure 4-2** Importing a Task Template

2. Select the XML and/or ZIP files that you want to import. Only XML files and ZIP files exported from HPDM will be accepted.

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.

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**.

   **Figure 4-3** Generating a template from payload

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.

**Figure 4-4** Generating a template from payload

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.

**Figure 4-5** Copying an image to another OS

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 4-1  Task status icons

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The task was executed successfully by the device.</td>
</tr>
<tr>
<td>Sending</td>
<td>The console has sent the task to the device and is waiting for a reply.</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 Console lists tasks in two groups: Manual Tasks and Rules Tasks. Manual Tasks are created directly with the Console and Rules Tasks are created indirectly by the Rules mechanism.

You can specify general task settings by selecting Tools > Configuration from the 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 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**

**Figure 4-6** Task Editor—Valid Time, Timeout & WOL

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

Figure 4-7 Task Editor—Target Device List

This 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.
This 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.
Write Filter and WOL setting

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 left-hand tree pane of the **Configuration Management** dialog box.

   **Figure 4-9** Configuration Management—Write Filter and WOL

2. Choose one of the three policy options.

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

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 46.

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 Agent needs to reboot/shutdown the device normally, it displays either the Reboot Required or the Shutdown Required dialog box.

**Figure 4-10** Task deferment—Reboot required
Figure 4-11  Task deferement—Shutdown required

- 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 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 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 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.

**Figure 4-12** Configuration Management—Task Parameters

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 HP Device Manager will wait for the execution of tasks. You can also specify the start and end time of working hours during which
HP Device Manager 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.

   ![Figure 4-13 Rule Editor](image)

   **Task Template**

   - **OS** HP vWS/XPe
   - **Category** Agent
   - **Template** Configure Agent

   Enabled (This rule will be active and generate tasks)

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.

**Figure 4-14** Rule Editor—Filter Chooser

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.

**Figure 4-15** Rule Editor—Trigger selection
6. Specify the template to use.

**Figure 4-16** Rule Editor—Task Template

![Task Template](image)

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

7. Click **OK** to create the rule.

**Figure 4-17** Rules Management

![Rules Management](image)

8. The new rule will be enabled by default. You can disable it by un-checking its check box in the **Rules Management** window.
All thin clients of the selected folders are displayed in the **Device Pane** of the Management Console window when clients connect to the server. Double-clicking an item in the **Device Tree Pane** or clicking on a folder icon will expand the device group. Clicking on folders will display all thin clients of the selected group in the **Device Pane**.

Select one or more folders from the **Device Tree Pane**, and then right-click to see a menu of applicable commands.

**Figure 5-1**  Folder commands

Select one or more devices from the **Device Pane**, and then right-click to see a menu of applicable commands.
All of these commands are also available in the **Device** menu which is displayed from the Console’s menu bar.

## Device icons

On the **Gateway** tab, a **G** icon indicates a Management Gateway:

- A green **G** icon represents a gateway that is currently active.
- A greyed-out **G** icon represents a gateway that is currently down or disconnected.

On the **OS** tabs, devices are represented by the following icons:

- A folder represents a number of devices that have been grouped together using the grouping schemes function.
- A screen icon with a power symbol over it indicates that currently the status of this device cannot be confirmed because a gateway to the device cannot be found.
- A greyed-out screen icon with an exclamation mark over it indicates the device is currently turned off.
- A screen icon with a curved arrow over it indicates the device is currently in pull mode.
- A screen icon with a curved arrow and padlock over it indicates the device is currently in pull–lock mode (Write Filter is ON).
- A screen icon with a straight arrow over it indicates the device is currently in push mode.
- A screen icon with a straight arrow and padlock over it indicates the device is currently in push–lock mode (Write Filter is ON).
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 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 5-3  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:

\[ P1=\text{"valor"}; P2=\text{"valor"}; P3=\text{"valor"}; P4=\text{"valor"}; P5=\text{"valor"}; P6=\text{"valor"}; MG=\text{"valor"} \]

For example:

\[ P1=\text{"Asia"}; P2=\text{"China"}; P3=\text{"Shanghai"}; MG=\text{"Empresa/Departamento/Grupo"} \]

**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 ensure the **Dynamic Scheme** tab is selected.

**Figure 5-4** Selecting the Dynamic Scheme tab

![Dynamic Scheme tab](image)

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.

**Figure 5-5** Defining a Dynamic Grouping scheme

![Grouping Scheme](image)

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.

Figure 5-6 Device Filter Management dialog
3. Give your new filter a name. Click OK to accept the name.

**Figure 5-7** Naming a new Device Filter

4. Click Add… in the Edit Device Filter dialog box to open the Choose Criteria Key dialog box.

**Figure 5-8** Device Filter Management—Choose Criteria Key dialog

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.

**Figure 5-9** Device Filter Management—Criterion Editor

![Criterion Editor](image)

7. Repeat steps 4–6 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.

**Figure 5-10** Editing a Device Filter

![Edit Device Filter dialog box](image)

3. Click **Add…** in the **Edit Device Filter** dialog box to open the **Choose Criteria Key** dialog box.

**Figure 5-11** Device Filter Management—Choose Criteria Key dialog

![Choose Criteria Key dialog box](image)

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**.

**Figure 5-12** Device Filter Management—Criterion Editor

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.

**Figure 5-13** Device Filter Management—New filter displayed

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 ensure 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 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 and view and control that client from the HP Management Console. This can be achieved either by using the **Shadow Device** template available on the **Operations** tab, or by selecting from the pop-up menu when you right-click on a device as described below.

**NOTE:** Make sure the VNC Server is running on target device(s). For devices that already have an installed VNC Server, send an "Apply Settings" task to enable the VNC Server. For HP XPe/WES devices, please update to 4.4 Agent version which includes a VNC Server in its update/install process.

**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.

**Figure 5-14**  Shadowing devices—Task Editor

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 Management 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.
HP Device Manager 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

HP Device Manager 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. HP Device Manager manages images through the 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 HP Device Manager, and some DHCP server setups may conflict with PXE. Should you experience problems with PXE, see Configuring DHCP servers on page 199.

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 HP Device Manager and store it as a `.dd.gz` file in the 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.

   ![Figure 6-1 PXE Capture default template](image)

2. Input an Image Name and a Description

3. Click **Save as** to save the template.

   ![Figure 6-2 Template Editor—Creating a new PXE Capture template](image)

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 a 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. The UI will look like below.

**Figure 6-3** Task Editor—Resulting template of a PXE Capture task
2. Create a “PXE Deploy” template by importing an image file and then dragging the “PXE Deploy” template to thin clients. From the menu, click **Template > Import > Image Files > to deploy using PXE ...**, and according to the wizard, it will create a “PXE Deploy” template with the import image UI looking like below.

![Figure 6-4 Import Image File dialog (with PXE)](image)

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

**NOTE:** On ThinPro or Python, there is no license check. For example, you can deploy a ThinPro 4 image to an HP Smart Zero Core device or deploy an HP Smart Zero Core image to a 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:

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.

**Figure 6-5** Template Editor—Capture Image template creation (without PXE)

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.

**Figure 6-6** Capture Image template appears in the Task pane (without PXE)
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.

**Figure 6-7** Task Editor—Capture Image task (without PXE)

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 HP Management Agent on the client receives the task, the client will display a warning message indicating that the device will reboot in 30 seconds.

For 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.

**Figure 6-8** Capture Image task progress

10. The client will reboot and enter Maintenance Mode 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 Management 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.

**Figure 6-9** Resulting template of a Capture Image task appears in the Task pane

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.

**Figure 6-10** Template Editor—Resulting template of a Capture Image task

![Template Editor dialog box](image)

This template deploys the image to devices.

- **Image Name**: WINCH9883.iso
- **OS Type**: WES8Q
- **Description**: 

**Advanced Options**

- **Cached Imaging**: Selecting this option will cause the whole image to be transferred to devices prior to deployment.

  **Note**: If this option is selected, the Deploy Image task will fail if the device does not have enough available disk space to store image.

- **Allow Cross Platform Imaging**: By default, HP Device Manager will only deploy images to the same hardware platform type as from which the image was captured. This is because the captured image may not contain necessary drivers for the other platform. Please note that although the standard WES Images from HP contain drivers for multiple platforms, all unnecessary are removed on the first boot to conserve the space. If you have added drivers for the other target device(s), select this option to bypass the platform check.

**Buttons**

- **Save as...**
- **OK**
- **Cancel**

Capturing an image from an HP thin client
Figure 6-11 Template Editor—Viewing details of the resulting template of a Capture Image task

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>W0CH9883</td>
</tr>
<tr>
<td>Create Time</td>
<td>2012/11/07 15:20:22</td>
</tr>
<tr>
<td>Installation Space (bytes)</td>
<td>10000000000</td>
</tr>
<tr>
<td>Architecture</td>
<td>X86</td>
</tr>
<tr>
<td>OS Type</td>
<td>WES09</td>
</tr>
<tr>
<td>Model Type</td>
<td>t510</td>
</tr>
<tr>
<td></td>
<td>t5400</td>
</tr>
<tr>
<td></td>
<td>t5570</td>
</tr>
<tr>
<td></td>
<td>t5570e</td>
</tr>
<tr>
<td></td>
<td>t5740</td>
</tr>
<tr>
<td></td>
<td>t5745</td>
</tr>
<tr>
<td></td>
<td>t610</td>
</tr>
</tbody>
</table>

**NOTE:** An image captured from WES7 or WES09 via HPDM is a file-based image (.ibr). An image captured from ThinPro or Python 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.

**Figure 6-12** WES HPDM Agent warning

System is updating critical components. Please do not operate on this device or shut it down. The device may fail to boot if the update is interrupted.

OK
Deploying images

There is no “Deploy Image” base template, but one can be created by capturing an image.

To deploy an image to one or more devices:

1. In the Management 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.

**Figure 6-13** Template Editor—Resulting template of a Capture Image task

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 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 Thin Client and want to deploy it to a t610 Thin Client, you need to select this option. Otherwise, this Deploy Image task will fail. If you select this option, you need to ensure 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 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.
Renaming devices (hostname)

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

1. Right-click the desired thin client in the 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. HP Device Manager 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 ensure that the connections work on the network where they will be used.

2. Run the Management Console and display the name of the device with the correct connections in the device tree.

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**.

**Figure 7-1**  Templates in the Settings category
Cloning settings

1. Double-click the _Clone Settings_ template to display the Template Editor.

Figure 7-2 Template Editor—Clone Settings

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.

**Figure 7-3** Task Editor—Clone Settings

![Task Editor](image)

This template is used to clone settings through HPDMC tool.

- **Choose settings to clone**
  - [ ] Select All
  - [ ] Display Settings
  - [ ] Network Settings
  - [ ] Time Settings
  - [ ] Keyboard Settings (*)
  - [ ] Mouse Settings (*)
  - [ ] Internet Explorer Settings (*)
  - [ ] Web browser homepage Settings
  - [ ] Region Settings (*)
  - [ ] VNC Settings
  - [ ] Screensaver Settings

*Note: The settings with "(*)" are user-specific.*

Specify username of the account to capture

**Username:** Administrator

Save result as template: **mySettings**

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.

Figure 7-4  Template Editor—Apply Settings template with no settings configured
3. Use the check boxes to indicate which settings to edit.

Figure 7-5 Edit Settings Wizard (Windows GUI)

Figure 7-6 Edit Settings Wizard (HP ThinPro GUI)

4. Click **Next** or click on the settings titles on in the left hand pane to configure individual settings.
5. Once the settings are configured, navigate to the **Summary** page. This lists all settings that will be changed by this template.

**Figure 7-7** Edit Settings Wizard—Summary page
6. If the changes are correct, click **Finish** to go back to the **Template Editor**.

   **Figure 7-8** Template Editor—Apply Settings template with settings configured

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.
Configuring display settings

1. Select the settings to be modified.

Figure 7-9 Edit Settings Wizard—Display Settings

2. Modify the values for each selected setting.
Configuring network settings

1. Select the settings to be modified.

Figure 7-10 Edit Settings Wizard—Network Settings

2. Modify the values for each selected setting.
Configuring time settings

NOTE: The GUIs for Windows and Linux operating systems are different.

1. Select the settings to be modified.

   **Figure 7-11** Edit Settings Wizard—Time Settings (Windows GUI)

   ![Edit Settings Wizard—Time Settings (Windows GUI)](image)

   **NOTE:** The option values for HP WES/XPe are unified with WES7 devices. There are 97 values in all; some might not be supported by WES09 or XPe devices. Also, not all values on WES09 and/or XPe are supported by DM 4.4 settings template/task.

2. Modify the values for each selected setting.

   **Figure 7-12** Edit Settings Wizard—Time Settings (HP ThinPro GUI)

   ![Edit Settings Wizard—Time Settings (HP ThinPro GUI)](image)
Configuring keyboard settings

1. Select the settings to be modified.

   **Figure 7-13** Edit Settings Wizard—Keyboard Settings

2. Modify the values for each selected setting.
Configuring mouse settings

1. Select the settings to be modified.

   **Figure 7-14** Edit Settings Wizard—Mouse Settings

2. Modify the values for each selected setting.
Configuring region settings

1. Select the settings to be modified.

   **Figure 7-15** Edit Settings Wizard—Region Settings

2. Modify the values for each selected setting.
Configuring Internet Explorer settings

**NOTE:** This is available only for HP WES/XPe and HP CE operating systems.

1. Select the settings to be modified.

   **Figure 7-16** Edit Settings Wizard—Internet Explorer Settings

2. Modify the values for each selected setting.
Configuring web browser home page settings

**NOTE:** This is only available for HP ThinPro 4.1 and earlier versions. For ThinPro 4.2 and above, browser settings have been removed. You cannot capture or deploy browser settings for these versions.

1. Select the settings to be modified.
   
   **Figure 7-17** Edit Settings Wizard—Firefox Settings (HP ThinPro 4.1 and earlier)

2. Modify the values for each selected setting.
Configuring VNC settings

**Figure 7-18** Edit Settings Wizard—VNC Settings

![Image of Edit Settings Wizard—VNC Settings]

Configuring screensaver settings

**NOTE:** This is available only with HP ThinPro.

**Figure 7-19** Edit Settings Wizard—Screensaver Settings (HP ThinPro only)

![Image of Edit Settings Wizard—Screensaver Settings (HP ThinPro only)]
Adding devices using MAC addresses

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

You can **Wake On LAN** a device that has not previously been reported to the HP Management Server, and it will therefore report in and be displayed in the proper OS tab.
To add a new device using its MAC address:

1. Select **Device > Add** from the Management Console menu bar.

   **Figure 7-20** Management Console—Device menu

   ![Add Device dialog box](image1)

   The **Add Device** dialog box will appear.

   **Figure 7-21** Adding a new device using a MAC address

2. Enter the **MAC Address** of the device to be added.
3. Select the Management Gateway that will connect with the device from the Neoware Management 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 re-arranging a variety of sub-tasks.

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

   **Figure 7-22** Template Editor—File and Registry
2. Click **Add** to add a variety of sub-tasks. (Refer to the following tables for more information on each sub-task.)

**Figure 7-23** Sub-Task Chooser

![Sub-Task Chooser](image)

Click **Edit** to edit a sub-task.

Click **Delete** to delete the selected sub-task.

Click **Up** and **Down** to rearrange the sub-tasks as required.

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

**Table 7-1** Capture Files sub-task

<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>
</tbody>
</table>

**Table 7-2** Deploy Files sub-task

<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 sub-task

<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 <strong>File Name</strong> recursively in all subdirectories from the given <strong>Path On Device</strong>.</td>
</tr>
</tbody>
</table>
### Table 7-4 Registry sub-task

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Key</td>
<td>(Registry tree) Add a key at the selected location on the tree.</td>
</tr>
<tr>
<td>Add Value</td>
<td>(Registry tree) Add a value on the selected key.</td>
</tr>
<tr>
<td>Rename</td>
<td>(Registry tree) Rename the selected item.</td>
</tr>
<tr>
<td>Delete</td>
<td>(Registry tree) Delete the selected item.</td>
</tr>
<tr>
<td>Action</td>
<td>(Registry settings) The action to be applied to the registry table. Set to <strong>add</strong> to add a key, or <strong>delete key</strong> to delete a key.</td>
</tr>
<tr>
<td>Type</td>
<td>(Registry settings) The type of registry key value.</td>
</tr>
<tr>
<td>Value Name</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</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</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</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 sub-task

<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. 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>
</tr>
<tr>
<td>Execute After Reboot</td>
<td>Set to <strong>Yes</strong> if you want the system to reboot and execute the command when it restarts, or <strong>No</strong> if you want the command to be executed immediately.</td>
</tr>
<tr>
<td>Wait</td>
<td>Set to <strong>Yes</strong> if the given command has to wait for the previous command to finish before processing, or set to <strong>No</strong> for simultaneous execution of commands.</td>
</tr>
</tbody>
</table>

### Table 7-6 Pause sub-task

<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>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------</td>
</tr>
<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 sub-tasks 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.

   **Figure 7-24**  Merge Templates dialog

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.

   **Figure 7-25** Merged Template Name dialog

```
Merged Template Name

Please enter the name of the new template to be created:
Reinstall TeemTalk

OK  Cancel
```

5. A new **File and Registry** template will be created with all of the sub-tasks of the original templates combined.
Changing registry settings

HP Device Manager 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

HP Device Manager 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**.

   **Figure 7-26** Template Editor—Get Registry template
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**.

**Figure 7-27** Add Registry Node dialog

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.

**Figure 7-28** Registry node appears in Template Editor
5. Click **Save as** and enter a name which indicates the purpose of this template (get desktop settings).

   **Figure 7-29** Enter New Template Name dialog

   ![Enter New Template Name dialog](image)

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.

**Figure 7-30** Task Editor—Get Registry task

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.

**Figure 7-31** Resulting template of a Get Registry task in the Task pane
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 Sub-Task box to display the Configure Registry Sub-Task dialog box, then click on the registry node in the Registry Tree panel to display the settings.

Figure 7-32 Configure Registry sub-task
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 Sub-Task box.

Figure 7-33 Template Editor—Resulting template of a Get Registry task
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.

**Figure 7-34** Sub-Task Chooser—Registry

Select *Registry* in the *Sub-Task Chooser*, then click *OK*. 
3. The **Configure Registry Sub-Task** dialog box will be displayed enabling you to edit registry settings.

**Figure 7-35** Configure Registry sub-task

- You can edit the contents of the **Registry Tree** using the four buttons at the bottom of the box.

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

- The **Registry Settings** box will display the current settings of the key selected in the **Registry Tree**. It is divided into the following columns:
| **Action** | Indicates the action to be applied to the registry table: **add** or **delete** a key. Click in the field to change the current setting. |
| **Type** | Indicates the type of registry key value. |
| **Value Name** | Displays the name of the registry key. Double-click in this field to edit it. |
| **Value Data** | Displays the data for the registry key value. Double-click in this field to edit it. |

- 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.
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>Wildcard</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>
<tr>
<td>a*</td>
<td>means all the files that start with the letter a.</td>
</tr>
<tr>
<td>*a</td>
<td>means all the files that end with the letter a.</td>
</tr>
</tbody>
</table>
5. Click **OK** when you have finished specifying the files to capture. A **Capture Files** sub-task will be added to the **Sub-Task** list of the template.

**Figure 7-36** Template Editor—Capture Files sub-task

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

7. 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** sub-task will be added to the **Sub-Task** list of the template.

**Figure 7-37** Template Editor—Deploy Files sub-task

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.

**Figure 7-38** Program Record dialog

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 sub-task will be added to the Sub-Task list of the template.

**Figure 7-39** Template Editor—Program Record sub-task

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

HP Device Manager 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**.

   ![Template Editor—File and Registry](image)

   **Figure 7-40** Template Editor—File and Registry
2. Click the **Add** button and select **Command**.

**Figure 7-41** Sub-Task Chooser—Command

![Sub-Task Chooser](image)

3. Click **OK**.

**Figure 7-42** Execute Command Sub-Task dialog

![Execute Command Sub-Task](image)
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 HP Device Manager, you need to add `wscript` before the script name you want to run. `Wscript.exe` is in the **C:\windows\system32** directory.
HP Device Manager uses one or more file 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 Share Folder.

**Initializing from wizard**

You will be prompted by a wizard to help you initialize the repository system when you start the Console for the first time.
The wizard consists of two pages:

- Protocol Settings
- Master Repository Configuration

**Figure 8-1** Repository Wizard—Protocol Settings

Choose protocol for all repositories. You can also configure Share Folder for each repository as additional access.

- Use FTP-like protocol as main access for repositories.
- Use Share Folder as access for repositories.

Note: Share folders are required for capturing images from or deploying images to WES Thin Clients that do not have enough free space to hold the image file.
Repositories are used to store payloads for all tasks. There is one Master Repository and could be multiple Child Repositories. Payloads on Child Repositories are copies of those on the Master Repository. The Master Repository Controller must reside on the same computer as the Master Repository. Paths specified below must point to the same location you configured for the Master Repository Controller during installation.

If both protocols are used for the repository, they should point to the same location on the server.

**FTP Protocol Settings**

- **Username:**
- **Password:**
- **Path:**

**Share Folder Protocol Settings**

- **Share Folder enabled for this repository**
- **Username:**
- **Password:**
- **Path:** HPDM
Selecting the file protocol to use

To select the file protocol HPDM should use:

1. Select **Tools > Repository Management > Protocol Configuration** from the menu.

   **Figure 8-3**  Protocol Configuration in the Console menu

2. In the **Protocol Configuration** dialog box, establish the protocol and port you wish to use.

   **Figure 8-4**  Protocol Configuration dialog

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.
1. Select **Tools > Repository Management > Repository Configuration** from the menu.

**Figure 8-5** Repository Configuration in the Console menu

<table>
<thead>
<tr>
<th>Tools</th>
<th>Device</th>
<th>Template</th>
<th>Tools</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Management ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repository Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Management ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Management ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status Walker</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status Snapshot</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Password ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Configuration ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repository Configuration ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Management ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repository Mapping ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP ThinPro 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP W</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. In the **Repository Configuration** dialog box, select the **Master Repository** item and click the **Edit** button.

**Figure 8-6** Repository Configuration dialog
3. In the **Repository Editor** dialog box, configure the **Repository Name**, **Server Address**, **Username**, **Password**, and **Path** settings.

**Figure 8-7** Repository Editor—Master Repository

- **Master Repository Basic Information**
  - **Repository Name**: Master Repository
  - **Server Address**: 192.168.1.102

- **FTP Protocol Settings**
  - **Username**: root
  - **Password**: ****
  - **Path**: HPDM

- **Share Folder Protocol Settings**
  - **Username**: Administrator
  - **Password**: ********
  - **Path**: HPDM

**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 Share Folder you access it by `IP\HPDM`, so here you should input **HPDM** for the Path value of the FTP and the Share 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 **Share Folder**.

6. Click the **Save** button to save the settings
Configuring the Child Repositories

1. Select **Tools > Repository Management > Repository Configuration** from the menu.

![Figure 8-8 Repository Configuration in the Console menu](image)

2. In the **Repository Configuration** dialog box, click the **Add** button.

![Figure 8-9 Repository Configuration dialog](image)
3. In the **Repository Editor** dialog box, configure the **Repository Name**, **Server Address**, **Username**, **Password**, and **Path** settings.

**Figure 8-10** Repository Editor—Child Repositories

4. Click the **Test** button if you want to test the connection to the **FTP server** and/or the **Share 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 Child Repository and click the **Remove** button and then **Yes** to confirm.

**Figure 8-11** Repository Configuration—Deleting a Child Repository

---

**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.

![Figure 8-12 Repository synchronization warning](image)

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

1. Select **Tools > Repository Management > Content Management** from the menu.
2. In the **Content Management** dialog box, you can view the all contents of the **Master Repository**.

**Figure 8-13** Content Management dialog
3. Select one category (except File Captured) in the left panel, then double-click one item in the right panel. A dialog box will appear to display detailed payload information.

**Figure 8-14** Properties dialog displaying detailed payload information

<table>
<thead>
<tr>
<th>Title</th>
<th>HP Device Manager Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>HPDM Team</td>
</tr>
<tr>
<td>Create Time</td>
<td>2012-11-08T16:38:55Z</td>
</tr>
<tr>
<td>Version</td>
<td>4.5.3667.15939</td>
</tr>
<tr>
<td>Description</td>
<td>This is the HP Device Manager Agent for Th...</td>
</tr>
<tr>
<td>Installation Space (bytes)</td>
<td>4194304</td>
</tr>
<tr>
<td>OS Type</td>
<td>HP Smart Zero Core</td>
</tr>
</tbody>
</table>

4. Select one 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.

5. Select one item of the **Files Captured** category, then click the **Download** button. Browse to the location where you want to save it, and the content will be downloaded to the local machine.

6. Click the **Sync All** button, and all the contents will be synchronized to the **Child Repositories**.

**Repository mapping**

HPDM automatically maps each and every client device to the nearest and most convenient repository. This allows the administrator to send tasks to a large number of 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.

**Figure 8-15** Repository Mapping in the Console menu

<table>
<thead>
<tr>
<th>Tools</th>
<th>Device</th>
<th>Template</th>
<th>Task</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Management ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Repository Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Management ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Configuration ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repository Configuration ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Management ...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Repository Mapping ...</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Batch mapping**

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

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

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

**Figure 8-16** Repository Mapping dialog—Batch Mapping by Gateway
**Figure 8-17** Repository Mapping dialog—Batch Mapping by subnet

An administrator can change the mapping settings of a device or a Gateway/subnet at any time.

HP Device Manager 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 55 for details about filters.

**Figure 8-18** Repository Mapping dialog—Per Device Mapping
There are two forms of security management in HP Device Manager, 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.

**Adding users**

1. Display the **Tools** menu from the Console’s menu bar and select **User Management**.

   ![User Management dialog—Users](image)
   
   **Figure 9-1**  User Management dialog—Users
2. Click **Add** to add a new user. The **Create New User** dialog box will appear.

**Figure 9-2** Create New User dialog

![Create New User dialog box](image)

3. Enter a **Username** for the new user and specify a **Password**. Click **OK** to create the new user.

4. Refer to the relevant section below in order to add the new user to a user group. Note that the user must be added to a group before it has any permissions to use HP Device Manager.

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

**NOTE:** Multiple Consoles cannot logon to the Management Server with the same username at the same time.

### Deleting users

1. Display the **Tools** menu from the menu bar and select **User Management**.
2. Select a user in the **User Management** dialog box.
3. Click **Delete** then **Yes** to confirm that you want to delete the selected user from the list.

### Assigning users to groups

1. In the **User Management** dialog box, double-click a user name in the **Users** list to edit the user.
2. Select the **Member Of** tab.

   **Figure 9-3** User Properties dialog—Member Of

3. Click **Add** to add the user to a new group, or **Delete** to remove the user from the selected group.

**Changing a user's password**

1. In the **User Management** dialog box, right-click on the name of the user whose password needs to be changed.
2. Select **Change Password** from the pop-up menu.

   ![Figure 9-4 Change Password dialog](image)

3. Enter the **New Password** for the user, 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 name in the **Users** list to edit the user.
2. Select the Filter tab.

Figure 9-5  User Properties dialog—Filter

3. Click Add to add the filter to this user, or Remove to remove the security filter from this user.
Adding a group

Groups can be used to control user permissions in HP Device Manager.

1. Display the Tools menu from the Console’s menu bar and select User Management.

![Figure 9-6 User Management dialog—Groups](image)

2. Select the Groups tab.

3. 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 All Groups list, right-click the group you wish to modify.

2. Select Properties in the pop-up menu.
3. Select the Privileges tab.

**Figure 9-7** Group Properties dialog—Privilege

4. Select the permissions you wish to assign to the group.

5. Click OK to finish.

**Assigning users to groups**

1. Right-click the group you wish to modify in the Groups tab of the User Management dialog box.

2. Select Properties in the pop-up menu.
3. Select the **Users** tab.

**Figure 9-8** Group Properties dialog—Users

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 **Group Management** dialog box, double-click a group name in the **Groups** list to edit the group.

2. Select the **Filter** tab.

**Figure 9-9** Group Properties dialog—Filter

3. Click **Add** to add the filter to this group, or **Remove** to remove the security filter from this group.
Deleting groups

1. Select the name of the group to be deleted in the All Groups list on the Groups tab.

   Figure 9-10  User Management dialog—Deleting a group

2. Click the Delete button then Yes to confirm that you want to delete the selected group from the list.

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 HP Device Manager. This allows reuse of existing login accounts and also simplifies the management of who has administrative privileges with Device Manager.

Configuration

To configure a connection to a LDAP Server:

1. Display the Tools menu from the Console menu bar and select Configuration.
2. In the **Configuration Management** dialog box, select **User Authentication** in the left pane.

**Figure 9-11** Configuration Management dialog—User Authentication with Active Directory

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](http://<your-ldap-server>/certsrv/certcarc.asp).

   - Java Keystore: A hpdmcert.key file from a previous HP Device Manager 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**:

   **Figure 9-12** Configuration Management dialog—User Authentication with LDAP

   ![Configuration Management dialog](image)

   - 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:
     
     - dc=testnet,dc=com
     - o=company,c=US

   - Specify the **RDN Attribute**. The RDN (Relative Distinguished Name) attribute is the LDAP attribute that specifies the login name of the user. Common values for this include **sAMAccountName** (Active Directory), **UID**, and **CN**.
8. Configure a **Search User**. This Search User will be used in two situations: by the **Import Users and Groups** dialog box to browse the LDAP Server, and to dynamically determine the members of an imported Group. Unless the LDAP supports anonymous search, a search user must be specified. Leave the Username and Password blank to use the anonymous user.

This **Username** should be specified as a **Distinguished Name**.

**Active Directory Note**: The Distinguished Name uses the LDAP CN attribute instead of the regular login name. To determine the LDAP CN, on the Domain Controller, open **Active Directory Users and Computers**, and double-click the **search user**. On the **General** tab of this **Properties** window is shown the **Display Name**. This **Display Name** is the LDAP CN.

**Figure 9-13** Searching user properties

![Searching user properties](image)

In the example shown above, for 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 Device Manager which LDAP users are permitted to log in, and what their privileges are once they do so.

To open the Import Tool:

1. Display the Tools menu from the Console menu bar and select User Management.

   **Figure 9-14** User Management dialog
2. Click the **Import from LDAP** button.

**Figure 9-15** Import Users and Groups dialog

![Image of Import Users and Groups dialog](image.png)

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.

**Figure 9-16** Import Users and Groups dialog—Expanding directories
To search for a User or Group:

1. Click the **Search** tab in the upper left of the **Import Users and Groups** dialog box.

   ![Figure 9-17 Import Users and Groups dialog—Search tab](image)

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, \( \leq \), will similarly find LDAP objects with an attribute value that is numerically smaller than the search value.

- The **Similar to** comparison, \( \sim \), permits searching for attribute values that are similar to the search value.

- Finally, the **Not Equals** comparison, \( \neq \), 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.

**Figure 9-18** User or group Properties dialog

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 141.
Authentication management

Since the HP Management Server can discover and manage all HP Device Manager gateways and agents on the network, a security problem may occur due to the improper usage of the Management Server. To overcome this, HP Device Manager provides an authentication capability for the gateways and the agents to recognize a secure Management Server.

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

Key management

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

To update the current Authentication Key:

1. Select Tools > Authentication Management > Key Management in the Console’s menu bar to display the Authentication dialog box.

   Figure 9-19 Authentication dialog
2. Enter your user **Password** then click **OK**. The **Key Management** window will appear.

   **Figure 9-20** Key Management dialog

3. Click the **Update Current Key** button to display the **Update Key** dialog box.

   **Figure 9-21** Update Key dialog

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 agent cannot contact a gateway for key information before a specified time (Expiration Interval), the Key will expire, (i.e., no longer in use) and the 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.

   ![Create KeyStore Password dialog](image)

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.

   **Figure 9-23** Authenticate KeyStore Password dialog

![Authenticate KeyStore Password dialog](image)

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.

   **Figure 9-24** Key Update Log

![Key Update Log](image)

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.

**Gateway access control**

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

To control Gateway access manually:

1. Select **Tools > Authentication Management > Device Management Gateway Access Control** from the Console's menu bar to display the Authentication dialog box.

   **Figure 9-25** Authentication dialog

   ![Authentication dialog](image1)

2. Enter your password then click **OK**. The Device Management Gateway Access Control window will appear.

   **Figure 9-26** Device Management Gateway Access Control dialog

   ![Device Management Gateway Access Control dialog](image2)

3. Select a gateway from the **Gateway Access Control List**, then click the **Acknowledge** or **Ban** button to recognize or ban the selected gateway.

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

To add a Report template:

1. Select Tools > Report Management from the Console’s menu bar to display the Report Management window.

Figure 10-1 Report Management dialog
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.

Figure 10-2 Set New Report Template Name dialog
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**.

**Figure 10-3** Choose Criteria Key dialog

![Choose Criteria Key dialog](image)

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.

**Figure 10-4** Edit Report Template dialog

![Edit Report Template dialog](image)
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.

**Figure 10-5**  Edit Report Template dialog

![Edit Report Template dialog]

6. Define operator and value for each criterion.

**Figure 10-6**  Criterion Editor

![Criterion Editor]

**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.

![Figure 10-7 Report Management dialog—Report Template appears](image)

**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.

   Figure 10-8 Report Management dialog

2. Select a template from the list then click Edit, or double-click on the template to view the template’s content.

   Figure 10-9 Edit Report Template dialog
3. Click **Generate Report** to preview the report.

**Figure 10-10** Device Report preview
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.

Gateway report

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

To create a Gateway report:

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

![Gateway report](image)

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** ...

**Figure 10-12** Device Information report

---

**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** ...

**Figure 10-13** Device Task report
3. Select the appropriate options in the **Device Task Report** dialog and click **Next >**.

**Figure 10-14** Device Task Report dialog

![Device Task Report dialog]

### Task report

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

To create a Task report:

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

**Figure 10-15** Task report

![Task report]

### 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** ....

**Figure 10-16** Task Status report

---

**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 ...**

**Figure 10-17** Task Log report
11 Template reference

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

**File and Registry**

*Figure 11-1 File and Registry templates*

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Base Template Name</th>
<th>Category</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>_Configure Agent</td>
<td>Configure Agent Mode.</td>
<td>_Configure Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>_Configure Task Deferment</td>
<td>Configure Task Deferment</td>
<td>_Configure Task Deferment</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>_Update Agent</td>
<td>Update the version of Agent</td>
<td>_Update Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>_Pull Connection Configuration</td>
<td>Pull Connection Settings from a device.</td>
<td>_Pull Connection Configuration</td>
<td>Connections</td>
<td></td>
</tr>
<tr>
<td>_File and Registry</td>
<td>Perform customized file, registry and command sub-tasks</td>
<td>_File and Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>_Get Registry</td>
<td>Get Registry Setting from a device.</td>
<td>_Get Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>_Capture Image</td>
<td>Capture the image from a device.</td>
<td>_Capture Image</td>
<td>Imaging</td>
<td></td>
</tr>
<tr>
<td>_PXE Capture</td>
<td>Capture the image from a device with PXE service.</td>
<td>_PXE Capture</td>
<td>Imaging</td>
<td></td>
</tr>
<tr>
<td>_Get Asset Information</td>
<td>Get asset information of device.</td>
<td>_Get Asset Information</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>_Reboot Device</td>
<td>Reboot device.</td>
<td>_Reboot Device</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>_Reverse Shadow Device</td>
<td>Remote control device by Reverse VNC.</td>
<td>_Reverse Shadow Device</td>
<td>Operations</td>
<td></td>
</tr>
</tbody>
</table>
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

Figure 11-3 Template Editor—Get Registry

This template is used to get the registry settings on a device.

- Get all registry entries.

Save result as template:

This template enables you to upload one or more keys from a thin clients registry.

Agent

Figure 11-4 Agent templates

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Base Template Name</th>
<th>Category</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Agent</td>
<td>Configure Agent Mode.</td>
<td>Configure Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Configure Task Deferent</td>
<td>Configure Task Deferent</td>
<td>Configure Task Deferent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Update Agent</td>
<td>Update the version of Agent</td>
<td>Update Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Pull Connection Configuration</td>
<td>Pull Connection Settings from a device.</td>
<td>Pull Connection Configuration</td>
<td>Connections</td>
<td></td>
</tr>
<tr>
<td>File and Registry</td>
<td>Perform customized file, registry and command sub-tasks</td>
<td>File and Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>Get Registry</td>
<td>Get Registry Setting from a device.</td>
<td>Get Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>Capture Image</td>
<td>Capture the image from a device.</td>
<td>Capture Image</td>
<td>Imaging</td>
<td></td>
</tr>
<tr>
<td>PXE Capture</td>
<td>Capture the image from a device with PXE service.</td>
<td>PXE Capture</td>
<td>Imaging</td>
<td></td>
</tr>
<tr>
<td>Get Asset Information</td>
<td>Get asset information of device.</td>
<td>Get Asset Information</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Reboot Device</td>
<td>Reboot device.</td>
<td>Reboot Device</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Reverse Shadow Device</td>
<td>Remote Control device by Reverse VNC.</td>
<td>Reverse Shadow Device</td>
<td>Operations</td>
<td></td>
</tr>
</tbody>
</table>
This template enables you to configure the HPDM Agent on the target thin clients.

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

Figure 11-6 Template Editor—Configure Task Deferment

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

**Figure 11-7** Template Editor—Update Agent

This template updates the version of the Agent on devices.

Connections

**Figure 11-8** Connections templates

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Base Template Name</th>
<th>Category</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Agent</td>
<td>Configure Agent Mode.</td>
<td>Configure Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Configure Task Deferment</td>
<td>Configure Task Deferment</td>
<td>Configure Task Deferment</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Update Agent</td>
<td>Update the version of Agent.</td>
<td>Update Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Pull Connection Configuration</td>
<td>Pull Connection Settings from a device.</td>
<td>Pull Connection Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File and Registry</td>
<td>Perform customized file, registry and command sub-tasks.</td>
<td>File and Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>Get Registry</td>
<td>Get Registry Setting from a device.</td>
<td>Get Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>Capture Image</td>
<td>Capture the image from a device.</td>
<td>Capture Image</td>
<td>Imaging</td>
<td></td>
</tr>
<tr>
<td>PXE Capture</td>
<td>Capture the image from a device with PXE service.</td>
<td>PXE Capture</td>
<td>Imaging</td>
<td></td>
</tr>
</tbody>
</table>
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.
Figure 11-10 Template Editor—Pull Connection Information

![Template Editor - Connections](image)

This template is used to push connections through HPJCT tool.

- **Summary of connections to push**
  - Team Talk (Remove existing)
    - TT1

---

**Imaging**

Figure 11-11 Imaging templates

![Imaging templates](image)

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
<th>Base Template Name</th>
<th>Category</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Agent</td>
<td>Configure Agent Mode.</td>
<td>_Configure Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Configure Task Deferral</td>
<td>Configure Task Deferral</td>
<td>_Configure Task Deferral</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Update Agent</td>
<td>Update the version of Agent.</td>
<td>_Update Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Pull Connection Config</td>
<td>Pull Connection Settings from a device.</td>
<td>_Pull Connection Configuration</td>
<td>Connections</td>
<td></td>
</tr>
<tr>
<td>File and Registry</td>
<td>Perform customized file, registry and command sub-tasks.</td>
<td>_File and Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>Get Registry</td>
<td>Get Registry Setting from a device.</td>
<td>_Get Registry</td>
<td>File and Registry</td>
<td></td>
</tr>
<tr>
<td>Capture Image</td>
<td>Capture the image from a device.</td>
<td>_Capture Image</td>
<td>Imaging</td>
<td></td>
</tr>
<tr>
<td>PXE Capture</td>
<td>Capture the image from a device with PXE service.</td>
<td>_PXE Capture</td>
<td>Imaging</td>
<td></td>
</tr>
<tr>
<td>Get Asset Information</td>
<td>Get asset information of device.</td>
<td>_Get Asset Information</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Reboot Device</td>
<td>Reboot device.</td>
<td>_Reboot Device</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Reverse Shadow Device</td>
<td>Remote control device by Reverse VNIC.</td>
<td>_Reverse Shadow Device</td>
<td>Operations</td>
<td></td>
</tr>
</tbody>
</table>
This template will capture a full disk 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

**Figure 11-13** Template Editor—PXE Capture

This template is used to capture the image from a device, and generate a template to deploy that image.

Image

- **Image Name**

*Note:* You do not need to add extension (.img, .ibr, etc) to the end of image name.

Description

Save result as template:

This template will capture a full disk 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**

**Figure 11-14** Operations templates
_Factory Reset

**Figure 11-15** Template Editor—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

**Figure 11-16** Template Editor—Get Asset Information

This template extracts a full asset report from the targeted thin clients.
**Reboot Device**

*Figure 11-17* Template Editor—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**

*Figure 11-18* Template Editor—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. This template can only be sent to a single thin client at a time and is not available for the HPCE thin clients.
**Send Message**

*Figure 11-19 Template Editor—Send Message*

This template sends a customized message to target thin clients. This template is not available for ThinPro thin clients.

**Shadow Device**

*Figure 11-20 Template Editor—Shadow Device*

This template causes VNC viewer bundled with the HPDM Console to connect to the VNC service on a targeted thin client. This template can only be sent to a single thin client at a time.
**Shutdown Device**

Figure 11-21 Template Editor—Shutdown 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**

Figure 11-22 Template Editor—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 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

Figure 11-24 Template Editor—Wake Up Device

Note: Execution Timeout value is an essential parameter of this task, please set it to an appropriate value. Especially some devices are behind NAT, please confirm Execution Timeout is bigger than Agent Pull Interval.

This template will cause the 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 Gateway, but also for devices that are not in the same subnet of Gateway, if the subnet has at least one online Agent. We can wake up devices behind NAT, if the subnet has at least one online Agent. During timeout, Gateway reports the unfinished part as failure.

Settings

Figure 11-25 Settings templates
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, refer to [Changing device settings on page 79](#).
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

**Figure 11-28** Template Editor—Hostname and IP (Modify specified devices)

![Template Editor—Hostname and IP (Modify specified devices)](image)

**Figure 11-29** Template Editor—Hostname and IP (Set with pattern)

![Template Editor—Hostname and IP (Set with pattern)](image)
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**

Figure 11-30  Template Editor—Set Password

This template is used to 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 it to show the password.
_Write Filter Settings_

**Figure 11-31  Template Editor—Write Filter Settings**

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

_Take TPM Ownership_

**Figure 11-32  Template Editor—Take TPM Ownership**

This operation will enable/activate TPM and set the TPM owner password to take the TPM ownership of the selected devices. Meanwhile, a BIOS Setup password is required to protect TPM configuration. If the BIOS Setup password has been set on devices, please provide the correct password. Otherwise, please input a new BIOS Setup password.

The credential information is critical. Please keep it safe.
This template enables/activates TPM and sets the TPM owner password and BIOS setup password to take the TPM ownership of the selected devices.

**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>
<thead>
<tr>
<th>Icon</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="anyway" /></td>
<td>anyway</td>
<td>Execute the template regardless of any previous template execution success or failure.</td>
</tr>
<tr>
<td><img src="image" alt="success" /></td>
<td>success</td>
<td>Execute the template only if the previous template completed successfully.</td>
</tr>
<tr>
<td><img src="image" alt="failure" /></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.

**Figure 11-33** Template Sequence default template

---

**_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 where you can specify a different conditions to control the execution of each template of the sequence.
Basic template sequences

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

**Figure 11-34** Template Editor—Template Sequence (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 if 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 11-35** 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.
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 > HP Device Manager > 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 Server backup location**

The **Backup** 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 **Backup** 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, which must be done manually as shown in the following screen shot. The prompt will NOT show up again if the HPDM Server is not actually stopped.

**Figure 12-3** Server backup—Stop server prompt

![Server backup—Stop server prompt](image)

**NOTE:** If the HPDM Server is not stopped, the tool cannot ensure 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 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.
This chapter contains information necessary to configure some networks in order to utilize HP Device Manager:

**Configuring DHCP servers**

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

**Management Server installed separately to 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 gateway, etc.).

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

**Configuring the DHCP Server**

1. Ensure 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 Device Manager 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.

**Management Server installed on DHCP server machine**

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

The Management 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 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 Management Server.

1. If **DHCP option 43** is set, remove it. (This is due to the fact that Management Server 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.
   
   *Either:*
   
   a. From the main Windows 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:*

   a. Enter **server <ip_address>** (using the IP address of the server.). A “**dhcp server >**” prompt appears in the command window.
   
   b. Enter **add optiondef 60** (name of your choice) **STRING 0** then press the **Enter** key.
   
   c. Enter **set optionvalue 60** **STRING “PXEClient”** then press the **Enter** key.
   
   d. To confirm that the settings are correct, enter **show optionvalue all** then press the **Enter** key.

3. Add **option 201**, and set the value to “`Management_Gateway_IP_Address’ ‘40003’”
   
   a. Type in **add optiondef 201** (name of your choice) **STRING 0** then press the **Enter** key.
   
   b. Type in **set optionvalue 201** **STRING ‘Management_Gateway_IP_Address’ ‘40003’** then press the **Enter** key. (**Note:** The **Management_Gateway_IP_Address** is the address of the server running the Management 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, ‘Management_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;
   Option vendor-class-identifier “PXEClient”;
   Option NDM “‘Management_Gateway_IP_Address’ ‘40003’”;
   ```

2. Restart `dhcpd` to use the new configuration.

3. The HP Device Manager config string should be:

   ‘Management_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 Management Gateway.

**Example (Cisco Router):**

1. Go to **Global Configuration** mode.
2. Type `ip forward-protocol udp 67` and press Enter.
3. Type `ip forward-protocol udp 68` and press Enter.
4. Go to 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 <Management Gateway IP address>` and press Enter.

**NOTE:** The above IP addresses should be entered without the < or > characters.
The following standard and custom ports are used by HP Device Manager. The ports are categorized by HPDM components as the receiver. This is to facilitate the firewall configuration if the HPDM components are installed separately on different host machines.

### Table B-1 Console

<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>VNC Server (thin client side)</td>
<td>VNC Viewer (bundled with HPDM Console)</td>
<td>TCP</td>
<td>VNC Viewer in Listen Mode (reverse VNC)</td>
</tr>
</tbody>
</table>

### Table B-2 Server

<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>Console queries the RMI Registry</td>
</tr>
<tr>
<td>40002</td>
<td>HPDM Console</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Console calls the remote objects on Server by RMI</td>
</tr>
<tr>
<td>40005</td>
<td>HPDM Gateway</td>
<td>HPDM Server</td>
<td>TCP</td>
<td>Gateway sends report to Server</td>
</tr>
<tr>
<td>40006</td>
<td>HPDM Server</td>
<td>PostgreSQL (bundled with HPDM Server)</td>
<td>TCP</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>Agent sends resource information (CPU, RAM, Disk IO, Network IO, Processes, etc.) to Server, and Server sends stop process command to Agent</td>
</tr>
</tbody>
</table>

### Table B-3 Gateway

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</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>
</tbody>
</table>
### Table B-3  Gateway (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>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</td>
<td>HPDM Gateway</td>
<td>UDP</td>
<td>Server/Agent polls Gateway</td>
</tr>
<tr>
<td></td>
<td>HPDM Agent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40003</td>
<td>HPDM Server</td>
<td>HPDM Gateway</td>
<td>TCP</td>
<td>Server sends task to Gateway</td>
</tr>
<tr>
<td></td>
<td>HPDM Agent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40008</td>
<td>HPDM Gateway</td>
<td>HPDM Gateway Controller</td>
<td>TCP</td>
<td>Gateway notifies Gateway Controller there are other gateways running in the same subnet</td>
</tr>
</tbody>
</table>

### Table B-4  Agent

<table>
<thead>
<tr>
<th>Receiver port</th>
<th>Sender</th>
<th>Receiver</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>OpenSSH Client (bundled with HPDM Console)</td>
<td>OpenSSH Server (bundled with HPDM WES Agent)</td>
<td>TCP</td>
<td>OpenSSH port for secure VNC connection (only for WES Agent).</td>
</tr>
<tr>
<td>67</td>
<td>HPDM Agent</td>
<td>DHCP Server</td>
<td>UDP</td>
<td>Send DHCP option requests</td>
</tr>
<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 (thin client side)</td>
<td>UDP</td>
<td>PXE – Bootstrap</td>
</tr>
<tr>
<td>5900</td>
<td>VNC Viewer (bundled with HPDM Console)</td>
<td>VNC Server (thin client side)</td>
<td>TCP</td>
<td>VNC Server</td>
</tr>
<tr>
<td>40001</td>
<td>HPDM Gateway</td>
<td>HPDM Agent</td>
<td>TCP</td>
<td>Gateway sends task to Agent</td>
</tr>
<tr>
<td>40001</td>
<td>HPDM Gateway</td>
<td>HPDM Agent</td>
<td>UDP</td>
<td>Receive replies of broadcasting Gateway</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>20 &amp; 21</td>
<td>HPDM Console</td>
<td>FTP Server (third-party software)</td>
<td>TCP</td>
<td>The default ports for FTP (used for HPDM Repository). Port 20 is for data transfer and port 21 is for listening to commands. FTP port can be configured on HPDM Console. If you do not use the default ports for your FTP, 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>The default port for SFTP (used for HPDM Repository). SFTP port can be configured on HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.</td>
</tr>
<tr>
<td>989 &amp; 990</td>
<td>HPDM Console</td>
<td>FTPS Server (third-party software)</td>
<td>TCP</td>
<td>The default ports for FTPS (used for HPDM Repository). Port 989 is for data transfer and port 990 is for listening to commands. FTPS port can be configured on HPDM Console. If you do not use the default ports for your FTPS, please configure the firewall appropriately.</td>
</tr>
<tr>
<td>40012</td>
<td>HPDM Server</td>
<td>Master Repository Controller</td>
<td>TCP</td>
<td>Server talks to Master Repository Controller to manage Master Repository</td>
</tr>
</tbody>
</table>
This chapter describes the agent polling and error logging capabilities of HP Device Manager.

Agent polling

HPDM Gateway can be set to communicate with Agent periodically and update device status (on/off) to HPDM Server. The default interval is 0 which means do not do this to save net traffic. Detailed description of its two parameters can be found on configuration GUI by stopping mouse cursor on relevant text field.

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

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

HP Device Manager 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.

**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 Agent, either set the log level through the Configure Agent dialog on the device or send a Configure Agent task to the target device(s).

**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>
<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 a Gateway, use one of the following methods:

- Use the Gateway configuration dialog, which can be accessed from right-clicking the HPDM Gateway tray icon.
- Send a Configure HPDM Gateway task from the Console. Choose an HPDM Gateway in the **HPDM Gateways** tab and click **Configure** or right-click the Gateway and select **Configure HPDM Gateway**.
Server and 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 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 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.
HP Device Manager 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 Console’s menu bar and select Status Walker to display the following dialog box.

**Figure D-1** Status Walker dialog
2. Click **Add** to create a new walking schedule, or **Edit** to modify an existing one. The **Schedule Editor** dialog box will appear.

**Figure D-2** Schedule Editor
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.

**Figure D-3** Scope Management dialog
4. Click the **Add** button and enter a name for the new scope.

**Figure D-4** Add New Scope dialog

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

**Figure D-5** Scope Editor

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.

**Figure D-6** Status Walker dialog with tasks

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

**Figure D-7** Status Results dialog
Configuring the Status Walker

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

1. Select Tools > Configuration from the Console’s menu bar to open the Configuration Management window.

2. Select the Status Walker Configuration item in the left-hand tree pane.

   **Figure D-8** Configuration Management dialog—Status Walker Configuration

   ![Configuration Management dialog—Status Walker Configuration](image)

   **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 Console’s menu bar and select **Status Snapshot**. The **Status Snapshot** dialog box will appear.

   **Figure D-9** Status Snapshot dialog
2. Click **Add** to create a new status snapshot schedule, or **Edit** to modify an existing one. The **Schedule Editor** dialog box will appear.

   **Figure D-10** Schedule Editor

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.

**Figure D-11**  Status Snapshot dialog with schedule snapshots

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

**Figure D-12**  Status Results dialog
Easy Update 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 Easy Update 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 Easy Update:

1. Start the Console and from the menu, select Template > Import > HP FTP Software Component Browser.

Figure E-1  HP FTP Software Component Browser in the Console menu
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.

**Figure E-2** HP FTP Software Component Browser
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.

**Figure E-3** Package Description Editor

![Package Description Editor](image)

**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.

**Figure E-4** Thin Client Models dialog

![Thin Client Models](image)
4. Select the OS to generate templates to, and click **OK**. A template will be generated in the specified OS.

**Figure E-5** Select OS dialog

![Select OS dialog](image)

**Figure E-6** Generate Templates confirmation

![Generate Templates confirmation](image)

**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.

**Figure E-7** Template status—Transferring

![Template status—Transferring](image)
6. After the transfer completes successfully, the template will become valid. You can then send the generated template to the specified thin client.

**Figure E-8** Template status—Complete
Index

A
Activity Directory 144
adding
  group 141
  report template 160
  users 136
agents
  configuration for client
discovery 26
device 3
discover 25
mode 4
asset database 21
assigning
  permissions to groups 141
  users to groups 137
authentication key
  export 157
  import 157
  update 155
  view 158
authentication management 155

B
backup 196

C
changing
  connection settings 78
device settings 79
  registry settings 103
  user password 138
Child Repositories
  configuring 127
deleting 128
client BIOS settings, PXE 64
client discovery 24
discover agent 25
manual configuration 26
walking with IP list 25
walking with IP range 25
client, discovering 24
cloning
device settings 80
command execution, remote 118
configuration
display settings 86
  Internet Explorer settings 92
  keyboard settings 89
  LDAP server connection 144
  mouse settings 90
  network 199
  network settings 87
  region settings 91
  status walker 214
time settings 88
  web browser home page
  settings 93
connection settings, changing 78
console management 2
copying files 113
devices
  adding using MAC addresses 95
  applying tasks to 39
  changing settings 79
deleting 52
  grouping 52
  printing information 60
  shadowing 61
DHCP
  installing management server 199
  Linux server 201
  management server 199
  server, configuring for PXE 199
DHCP tag 53
tag 202 24
tag 203 52, 54
discover agent 25
discovering clients 24
display, configuring settings 86

E
Easy Update 218
editing settings 109
export authentication key 157

F
file and registry 103, 109
file and registry templates
capture files sub-task 99
command sub-task 100
delete files sub-task 99
deploy files sub-task 99
merging 101
pause sub-task 100
registry sub-task 100
using 98
File Repositories
requirements 11
file repositories 121
files, copying 113
filter
device, editing 57
security 60
firewall settings 12
FTP 121
mappings 132
FTP server 3
FTPS 121
G
gateway
access control 158
management 3
generating report using template
165
getting settings 103
grouping
devices 52
groups
adding 141
assigning permissions to 141
assigning users to 137, 142
deleting 144
import 148
H
HPDM Agent
Agent 21, 24, 174, 183
HPDM Configuration Wizard 13
HPDM Server 21, 24, 48
I
icon, management console 15
icons
device tree 51
in systray 15
images
capture from client with PXE 65
capturing from thin client without PXE 68
pushing to client 66
updating 75
import
authentication key 157
report plug-in file 164
users and groups 148
installation
procedure 12
system requirements 8
Internet Explorer, configuring settings 92
IP scope, configuring 25
ISC DHCP 12
K
key management 155
keyboard, configuring settings 89
L
LDAP server 144
log in, management console 17
M
MAC addresses, using to add devices 95
managed device 4
management
agent, system requirements 10
authentication 155
gateway 3
gateway icon in systray 15
gateway, system requirements 9
key 155
power 63
report 160
repository 121
security 136
server 3, 199
server icon in systray 15
server, system requirements 9
task 34
task template 29
users 136
management console 2, 28
device pane 18
device tree pane 18
gateway tab 19
icon on desktop 15
log in 17
operating system tabs 18
OS tabs 18
overview 17
status bar 18
system requirements 8
task pane 18
template pane 18
mappings, FTP 132
Master Repository
configuring 125
mouse, configuring settings 90
N
Neoware, legacy client BIOS settings 64
network
checking connection status 60
configuration 199
configuring settings 87
requirements 12
O
opening VNC viewer 45
operations
agent 174
file and registry 172
general 181
get connection information 177
imaging 179
settings 187
template sequencing 193, 195
overview 1
overview, system structure 2
P
parameters
task 35
permissions, assigning to groups 141
persistent write operation, performing 202
plugin
template, removing 30
policy setting, write filter 39
ports
required 12
power management 63
properties
displaying task 41
pushing PXE image to client 66
PXE 4
capture image from client 65
client BIOS settings 64
configuring DHCP server 199
configuring routers 201
pushing image to client 66
configuring Internet Explorer 92
configuring keyboard 89
configuring mouse 90
configuring network 87
configuring region 91
configuring time 88
configuring web browser home page 93
editing file and registry 109
getting file and registry 103
write filter policy 39
SFTP 121
shadowing 45
shadowing devices 61
Share Folder 121
status checking network connection 60
status snapshot 215
status walker 208
configuring 214
support internet 5
technical 6
system requirements 8
systray icons 15

R
region, configuring settings 91
registry changing settings 103
editing settings 109
getting settings 103
remote command execution 118
execution of Windows scripts 120
report adding template 160
generating using 165
importing plug-in file 164
management 160
Reporting 167
repositories content management 130
exporting 129
importing 129
synchronizing 130
repository 4
repository management 121
requirements firewall ports 12
FTP 11
IPv4 12
ISC DHCP version 12
network 12
PXE 12
restore 196
result template, opening 45
router, configuring for PXE 201
rules 5

classification
authentication management 155
filter 60
gateway access control 158
key management 155
management 136
user authentication 144
server management 3
settings applying 82
changing file and registry 103
cloning 80
configuring display 86
tasks 28
operating system 77
parameters 35
settings 35
TCP ports required 12
technical support 6
template opening a result 45
removing plugin 30
sequence 31
task 5
template sequences advanced 195
basic 194
thin client asset information 21
defining rules 46
defining tasks 35
grouping 52
imaging 64
reporting 167
time, configuring settings 88
troubleshooting 5

U
UDP ports required 12
updating authentication key 155
user management 136
users adding 136
assigning to groups 137, 142
authentication 144
changing password 138
deleting 137
import 148

V
view authentication key 158

W
walking with IP list 25
with IP range 25
web browser home page, configuring settings 93
write filter 5
write filter policy setting 39