Administrator Guide

HP Device Manager 4.7

Fourth Edition: July 2017

First Edition: August 2015

Document Part Number: 834476-004

User input syntax key

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

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

Table of contents

1   Getting started

To find the latest HPDM software, administrator guide (this document), white papers, and release notes:

Go to ftp://ftp.hp.com/pub/hpdm.

Terms and definitions

Term	Definition
Device	An HP thin client managed by HPDM
HPDM Agent	The software component installed on each device to enable device management
HPDM Console	The software component that is the primary GUI for administrators, allowing them to manage devices and perform other administrative activities
HPDM Gateway	The software component that links HPDM Server and each device's HPDM Agent
HPDM Server	The software component that is the central server, which controls all management activities and hosts the HPDM database
HPDM Master Repository Controller	The software that manages the HPDM repository system
HPDM Master Repository	The primary storage location for payload (contains all payload files)
HPDM Child Repository	One or more optional secondary storage locations for payload (each can contain all or a subset of payload files)
HPDM database	The storage location for the information that defines all the HPDM assets, such as devices, HPDM Gateway servers, repositories, task templates, and rules
Package	Contains a description file and a folder that contains payload files
Payload	Files, such as operating system images and software packages, that are stored in the HPDM Master Repository (and optionally one or more HPDM Child Repository) and are distributed to devices via tasks
PXE	Preboot eXecution Environment, a network protocol that starts up computers using a network interface that is independent of data storage devices or installed operating systems
Rule	Allows you to automate the execution of tasks
Task	A scheduled action that is based on a task template and applies configuration changes to a device or group of devices
Task template	Defines the configuration changes you want to make to a device or group of devices
Template sequence	A special kind of task template that allows you to combine multiple task templates and execute them as a single task
HPDM Archive Tool	A software tool included with HPDM that allows you to archive outdated tasks and logs from both the HPDM database and file system
HPDM Automatic Device Importer	A different mode of HPDM Console that only imports devices **NOTE:** For more information, see the white paper titled *HPDM Automatic Device Importer*.

Term	Definition
HPDM Port Check Tool	A software tool included with HPDM that allows you to check network connectivity and firewall port allowance between different components of HPDM
HPDM Server Backup and Restore Tool	A software tool included with HPDM that allows you to back up and restore the files and database from HPDM Server

Repository protocols

Repositories are standard file servers and support the following protocols:

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

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

A repository can use either one or multiple protocols with the following guidelines:

- If using only one protocol, it can be any of the supported protocols.
- If using multiple protocols, all accesses need to be configured to point to the same directory on the file system.
- SMB is required for non-cached Windows imaging.
- SMB is not supported for non-cached imaging of HP ThinPro or HP Smart Zero Core because SMB is not well-supported for those operating systems.
- HTTPS is not supported for HP thin clients based on Windows Embedded Standard 2009, Windows XP Embedded, Windows Embedded CE 6.0, HP ThinPro 3, HP ThinPro 4, or HP Smart Zero Core.
- HP ThinPro 6.0 and later supports HTTPS for non-cached imaging.

> **NOTE:** If multiple protocols are configured for a repository and you send a task other than a non-cached Windows imaging task, HPDM attempts the connection in the following protocol order: HTTPS, FTP/FTPS, SFTP, SMB.

Deployment example
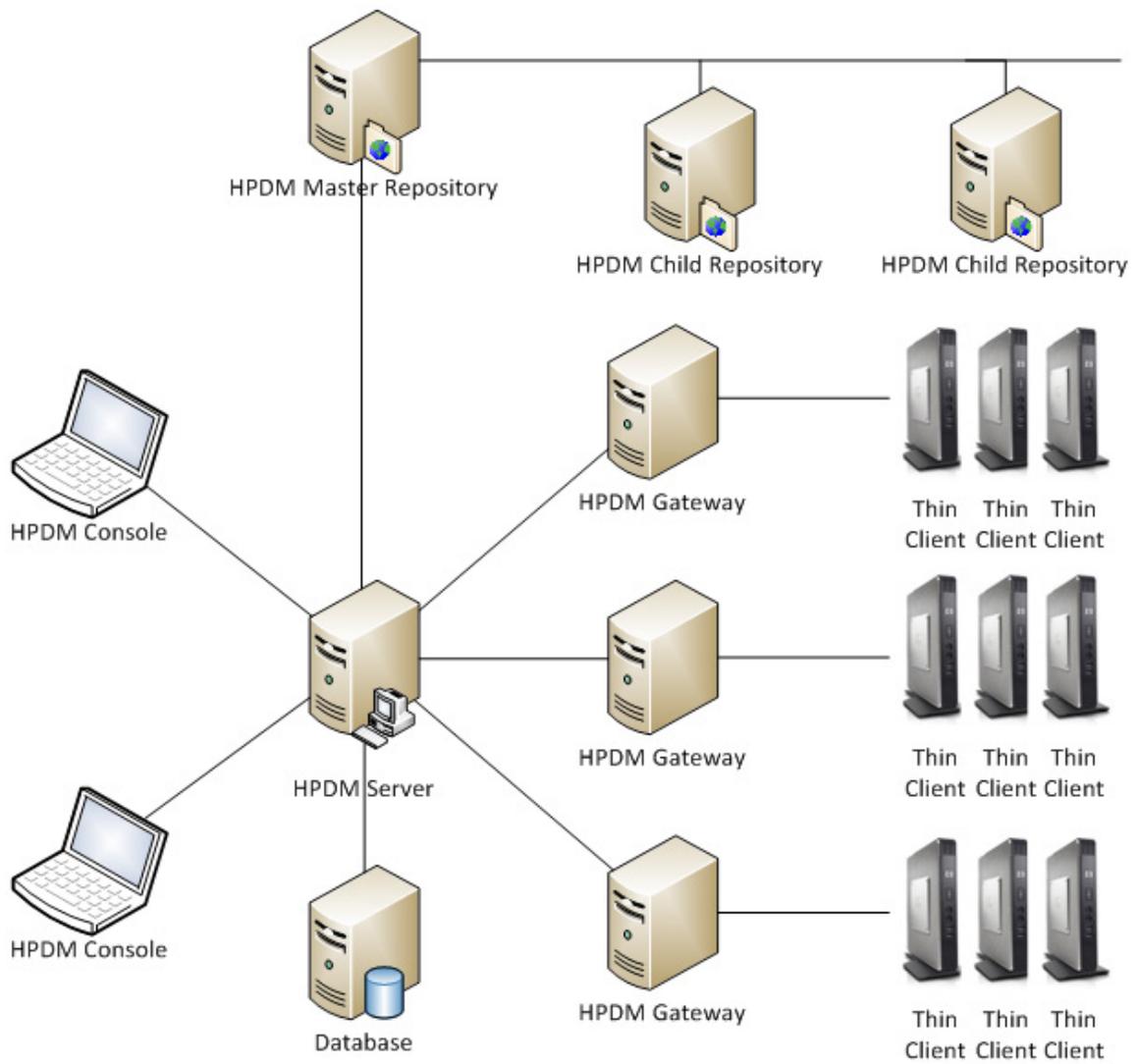
NOTE: HPDM deployment is very flexible. For more information, see the white paper titled *HPDM Deployment Guide*.

For system requirements, see the *Release Notes* for your version of HPDM or HPDM Service Pack.

For installation procedures and information, see the white paper titled *HPDM Installation and Update Guide*.

HPDM uses SSL/TLS for communication security. For enhanced security, SSLv2 and SSLv3 are disabled. For more information, see the white paper titled *HPDM Security Mechanism*.

2 HPDM Console overview

Logging in to HPDM Console

To launch HPDM Console:

1. Double-click the shortcut for HPDM Console on the Windows desktop.

    – or –

    Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, and then select **HP Device Manager Console**.

2. In the dialog box that opens, enter the hostname or IP address for HPDM Server.

    NOTE: If HPDM Console is installed on the same system as HPDM Server, enter `localhost.`

3. Enter your user name and password, and then select **OK**.

Device tabs

Item	Description
1	**Device tabs**—Allow you to manage devices by operating system
	TIP: You can hover the mouse cursor over a tab to view the full name of the operating system.
	NOTE: A particular device tab is available only if that operating system is detected on at least one device. A tab labeled Unidentified is available if the operating system of one or more devices has not been identified by HPDM.
2	**Device list**—Shows some basic information about each of the devices belonging to the group or groups selected in the device tree
3	**Status bar**—Shows the total number of active devices and some context-sensitive information
4	**Task pane**—Allows you to create tasks from task templates, manage existing tasks, and monitor task status
5	**Device tree**—Shows a hierarchical list of devices that are sorted into groups based on a grouping scheme that you can customize
6	**Toolbar**—Allows you to send tasks, discover new HPDM gateways and devices, and find a specific device in the device list using various search criteria

HPDM Gateway tab
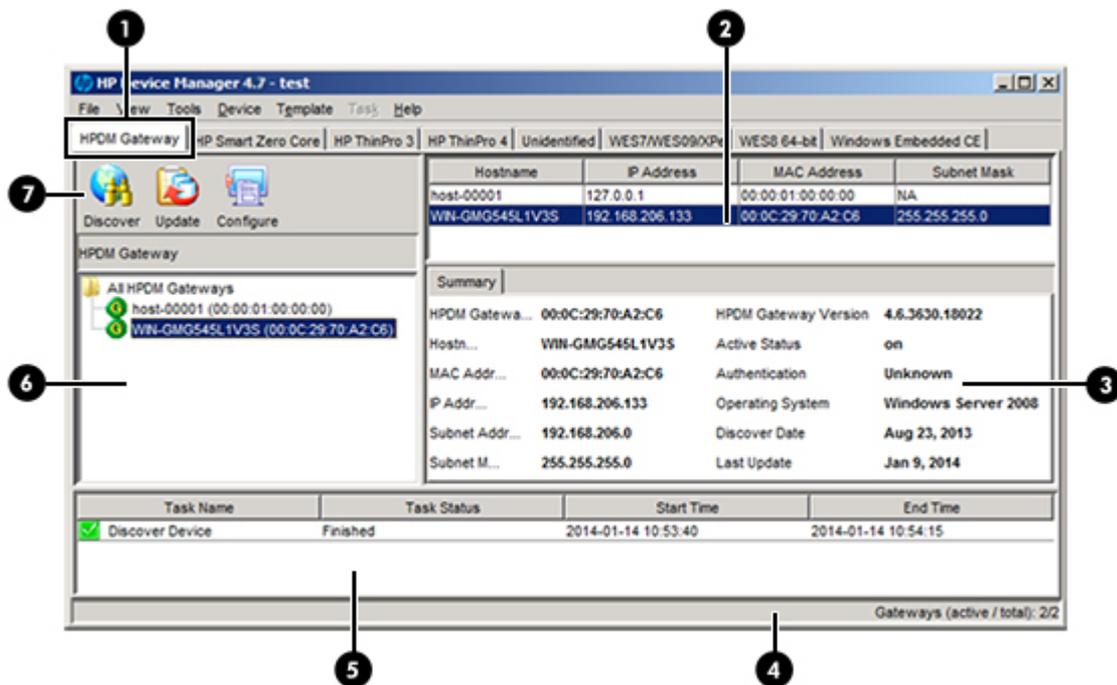
Item	Description
1	**HPDM Gateway tab**—Allows you to manage HPDM gateways
2	**Gateway list**—Shows some basic information about each HPDM gateway
3	**Summary panel**—Shows additional information about an HPDM gateway if only one is selected
4	**Status bar**—Shows the total number of active HPDM gateways
5	**Task pane**—Displays the status of tasks assigned to an HPDM gateway if only one is selected
6	**Gateway tree**—Lists all HPDM gateways
7	**Toolbar**—Allows you to discover new HPDM gateways and devices, update the software for an HPDM gateway to the latest version, and configure an HPDM gateway

Displaying device properties

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

Basic asset information

To display a device's basic asset information:

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

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

Basic asset information can be used to filter and group your devices. You can define custom grouping information on the Grouping page. You can also clear grouping values from the Grouping page, which must be done to accept new values from a device report.

The following table describes the basic asset information available on the General page.

Item	Description
Device ID	The unique ID that HPDM assigns to the device. The device ID is the first MAC address found on the device.
Hostname	The hostname of the device.
Device Type	The model name of the device.
Device Serial Number	The hardware serial number of the device.
OS Type	The name of the device's operating system.
Image Version	The image version of the device's operating system.
OS Configuration	Indicates the configuration of the device's operating system. For example, it displays **Smart Zero** in Smart Zero mode and **ThinPro** in ThinPro mode (if you are using an HP ThinPro 5 device).
BIOS Version	The BIOS version of the device.
Asset Tag	The asset tag of the device.
Have TPM Module	Indicates whether the device has a Trusted Platform Module (TPM). A TPM is a secure crypto-processor that can store cryptographic keys that protect information and is often called the TPM chip or TPM Security Device. Software can use a TPM to authenticate hardware devices. Currently, some HP thin client models, such as the t610, have a TPM chip built in.
TPM Owned	Indicates whether a TPM is owned. A TPM must be owned before it can be used to secure a computer. The ownership of a TPM is set by assigning a password to it so that only the authorized TPM owner can access and manage the TPM. Only one password exists per TPM, so anyone who knows that password is effectively the TPM owner. Once an owner is set, no other user or software can claim ownership of the TPM.
Base Snapshot	Indicates the base snapshot of the device (if you are using an HP ThinPro 5 device).

The following table describes the basic asset information available on the Agent page.

Item	Description
Agent Version	The version of HPDM Agent on the device.
HPDM Gateway ID	The MAC address of the HPDM Gateway that is being used to communicate with the device.

Item	Description
Agent Working Mode	Indicates whether HPDM Gateway is able to push tasks to the device or if it has to wait for HPDM Agent to pull tasks from HPDM Gateway. In some environments, for example where the devices are separated from their HPDM Gateway by a NAT, a device is not addressable by its HPDM Gateway and its HPDM Agent must pull tasks.
Agent Pull Interval	Indicates how often HPDM Agent attempts to pull tasks from HPDM Gateway.
First Contact Time	The date and time when the device registered with HPDM.
Last Time Online	The date and time of the last time HPDM communicated with HPDM Agent on the device.

Collecting complete asset information

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

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

1. Right-click the devcie about which you wish to gather information and select **Get Device Asset Information**.

2. Select **OK** when the task creation window appears.

3. Once the task has completed, you can see the extra asset information in the device's **Properties** window.

Displaying complete device asset information

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

- **Software**—Lists software packages installed on the device.

- **Hardware**—Lists CPU, memory, and storage details.

- **Network**—Lists configuration information for each network adapter present on the device.

- **Configuration**—Lists time zone and display settings.

- **Microsoft Hotfix**—Lists Microsoft Hotfix Information (this page is only available if the device is Windows-based).

- **Extended Properties**—Lists the device's extended properties.

3 Device discovery

In a standard deployment, HPDM Gateway automatically discovers most devices and adds them to the HPDM database by listening for a network broadcast message made by a device when it starts up, but this method requires that the gateway is running before the device starts up. This chapter discusses other methods to add devices to the HPDM database.

Automatic registration (normal thin clients)

When you connect a device to your network, its HPDM Agent automatically tries to connect to an HPDM gateway via the following methods, one by one, in the following order until a connection is successful:

1. Current gateway

2. Backup gateway

3. The gateway listed by DHCP tag 202

4. The gateway listed by the DNS server

5. The gateway or gateways listed in DNS service records

6. The gateway that responds to the broadcast from the device

NOTE: On HP ThinPro only, if the value of the option **DHCPOverrideCurrentGateway** is **1**, HPDM Agent registers itself via HPDM Gateway at DHCP tag 202 first. The default value is **0**.

If HPDM Agent loses contact with its current gateway or the device is restarted, the automatic registration process restarts and runs at regular intervals until it is successful.

DNS service records

Most device discovery methods assign only one HPDM gateway to each device. You can assign multiple gateways with different priority values using DNS service records. The benefit is that HPDM Agent will try the gateways one by one until it connects to one successfully, allowing you to set backup gateways.

Prerequisite: HPDM Agent must have either a static domain name or access to a DHCP server to get the domain name via DHCP option 15.

NOTE: Currently, the version of HPDM Agent for HP ThinPro does not support static domain names. If a device uses a static IP address, this feature is not supported.

Creating a DNS service record

1. Open the DNS console.

2. Right-click the domain, and then select **Other New Records**.

3. Select **Service Location (SRV).**

4. Select the **Create Record** button.

5. Set the service as **_hpdm-gatewy**.

6. Set the protocol as **_tcp**.

7. Optional: Set the priority to a numerical value (lower values indicate a higher priority).

8. Set the host as the fully qualified domain name (FQDN) of the gateway.

9. Select **OK**.

10. Optional: Repeat steps 4–9 to add additional records.

11. Select **Done**.

Troubleshooting

1. Verify the network information (including the IPv4 address and domains) of the device.

2. Use the following command to make sure the device can get DNS service records:

   - Windows:

     ```
     nslookup —timeout=30 —type=SRV _hpdm-gateway._tcp.<domain name>.com
     ```

   - HP ThinPro:

     ```
     host —t SRV _hpdm-gateway._tcp.<domain name>.com
     ```

Setting a static domain name (Windows only)

1. Open the Network Connections dialog via Control Panel or the network notification icon.

2. Right-click the network adapter and select **Properties**.

3. Left-click the **Internet Protocol Version 4 (TCP/IPv4)** item in the list, and then select the **Properties** button.

4. Select the **Advanced** button.

5. Select **DNS** tab.

6. Select **Append these DNS suffixes (in order)**, and then add the DNS domain to the list.

7. Select **OK**.

Automatic registration (PCoIP zero clients)

Using a DNS service record

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

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

To create a DNS service record:

1. Open the DNS console, and select the zone containing PCoIP zero clients.

2. Right-click to display the menu, and then select **Other New Records** to display the Resource Record Type dialog.

3. Select **Service Location (SRV)** and select the **Create Record** button to display the New Resource Record dialog.

4. Set the Service value to **_pcoip-broker** (recommended) or **_pcoip-tool**. Set the Protocol value to **_tcp**, set the Host offering this service to the fully qualified domain name (FQDN) of HPDM Gateway, and then select **OK**. Select **Done**.

5. Restart the PCoIP zero clients. They will report to HPDM automatically.

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

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

To troubleshoot this method:

1. Verify the network information, including the IPv4 address and domains, of the PCoIP zero clients.

2. The PCoIP zero clients have an embedded diagnostic tool. Use it to ping HPDM Gateway at the address in the DNS service record.

Using a DHCP vendor class option

To create a vendor class:

1. Open the DHCP console, and then select the DHCP server that the PCoIP zero clients are in.

2. Right-click to display the menu, and then select **Define Vendor Classes** to display the DHCP Vendor Classes dialog.

3. Select the **Add** button to display the New Class dialog.

4. Set the Display Name to **PCoIP Endpoint**, set the value to **PCoIP Endpoint**, and then select **OK**.

To set a vendor class option:

1. Right-click the DHCP server to display the menu, and then select **Set Predefined Options** to display the Predefined Options and Values dialog.

2. Set the option class to **PCoIP Endpoint**, and then select **Add**.

3. In the Option Type dialog box, enter `MC Address` in the Name field, set the data type to **String**, set the code to **1**, and then select **OK**.

4. Set the value of MC Address to the IP address of HPDM Gateway, and then select **OK**.

To enable a vendor class option:

1. Select the **Scope Options** of the Scope that the PCoIP zero clients are in.

2. Right-click to display the menu, and then select **Configure Options** to display the Scope Options dialog.

3. Select the **Advanced** tab.

4. Set the vendor class to **PCoIP Endpoint**, enable the **MC Address** option, and then select **OK**.

5. Restart the PCoIP zero clients. They will report to HPDM automatically.

To troubleshoot this method:

1. Verify the network information, including the IPv4 address and domains, of the PCoIP zero clients.

2. The PCoIP zero clients have an embedded diagnostic tool. Use it to ping HPDM Gateway at the MC Address.

Searching for devices

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

1. In HPDM Console, select the **HPDM Gateway** tab.

2. Right-click the desired HPDM Gateway and select **Discover Device** in the menu.

3. Select the device type (normal thin client or PCoIP zero client).

4. Proceed to Using the Walking With IP Range method on page 12 or Using the Walking With IP List method on page 12, depending on the method you wish to use.

Using the Walking With IP Range method

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

1. Select **Walking With IP Range**, and then select **Next**.

2. You can specify the range of IP addresses to search by using either an IP scope or by manually specifying an IP range. An IP scope is a range of IP addresses that you have built and saved for future scans.

   To search using an IP scope:

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

   To search using a manually-specified IP range:

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

> ☼ **TIP:** You can display information about the discovery progress in the task pane by selecting a gateway in the gateway tree.

Configuring an IP scope

To configure an IP scope:

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

2. Select an existing IP scope from the **IP Walking Scopes** list or select **Add** to create a new one.

3. Enter a scope name to be used by HPDM to refer to the new search scope, and then select **OK**.

4. Define the IP address range in which you want HPDM to search for devices by filling in the **Starting IP Address** and **Ending IP Address**. Select **Apply** to save the settings, and then select **OK** to exit.

Using the Walking With IP List method

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

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

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

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

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

3. Select **OK**. Once the search has finished, a report shows the devices detected by HPDM. When devices are found, they are added to the HPDM database.

Manually registering a device

To manually register a device:

1. In HPDM Console, select the **HPDM Gateway** tab.

2. Right-click the desired HPDM Gateway, select **Device**, and then select **Add**.

3. Enter the device ID, MAC address, and IP address of the device.

4. Select an operating system from the dropdown list, and then select **OK**.

If you selected **Unidentified** for the operating system, the device is initially added under the Unidentified device tab. When the device first reports to HPDM Server and the operating system is detected, the device is then moved to the appropriate device tab.

Manually registering multiple devices

To manually register multiple devices:

1. In HPDM Console, select **File**, and then select **Import Devices**.

2. Select the **Select** button, and then choose a folder that contains text files that describe the devices to import.

> **NOTE:** For more information, see the white paper titled *HPDM Automated Device Importer*.

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

Each device is added under the appropriate device tab, as specified in the text files. If the operating system is not specified, the device is initially added under the **Unidentified** device tab. When the device first reports to HPDM and the operating system is detected, the device is then moved to the appropriate device tab.

4 Tasks and task templates

Task templates

Select the **Task Templates** tab in the task pane to display a list of the available task templates with the following sortable columns:

- **Icon**—Indicates whether the template is a base template, a custom task template, or a favorite custom task template

- **Template Name**—Indicates the name of the template

- **Description**—Shows the description text of the template

- **Base Template Name**—Indicates the base template name of the template

- **Category**—Indicates which category the template belongs to

  There are seven categories in HPDM:

  - **File and Registry**—A generic template consisting of a customizable combination of tasks for managing device operating systems (see Managing files and registry settings on page 29 for more information)

  - **Connections**—Used to get or set the connection settings of a device

  - **Agent**—Used to configure HPDM Agent settings and update HPDM Agent

  - **Imaging**—Used to capture or deploy flash-memory images of devices

  - **Operations**—Used to perform various operations on a device, such as restart, shadow, shut down, 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 changes 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 a task template

Preset task templates are available in the Task Templates list and begin with the _ (underscore) character, like in the following example: **_File and Registry**.

To create or edit a task template:

1. Double-click a task template.

   – or –

   Right-click a task template and select **Properties** from the context 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, select the **Save as** button and enter a name for the new template.

4. Select **OK**. The new template is created and added to the Task Templates list.

Adding a task template to the Favorites list

To add a task template to the **Favorites** list for quicker access:

▲ Right-click the task template and select **Add to Favorites** from the context menu.

The icon for the task template changes to the Favorites icon shown below.

You can sort the columns by icon to have your favorite templates listed above other templates. To perform a quick search, select a column header to show your favorite templates only.

Exporting task templates

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

2. If one or more of the selected templates utilizes payload files, you are asked if the payload files should also be exported. If you choose to export payload files, they are downloaded from the HPDM Master Repository.

3. Enter the name of the template.

4. Select the destination of the exported file.

5. Select **Export** to export the template(s). Templates with payload files are exported as ZIP files; otherwise the exported template is an XML file.

Importing task templates

1. In HPDM Console, select **Template**, select **Import**, and then select **Exported Templates**.

2. Select the XML file, ZIP file, or both to import. Only XML files and ZIP files exported from HPDM are accepted. Templates created using a version of HPDM earlier than HPDM 4.4 might not be recognized or be compatible.

3. Select **Import**. The file is added as a new template. Payload files in ZIP format are uploaded to the HPDM Master Repository automatically.

Generating a template from payload

1. In HPDM Console, select **Template**, select **Import**, and then select one of the following menu items:

   - **Image Files** (.ibr, .img, .hpimg, .dd, .dd.gz)

   - **PCoIP firmware** (.all)

   - **Easy Tools Configuration** (.hpcfg)

   - **Easy Tools Settings** (.hpset)

2. Select the file that you want to import.

3. Select **Import**. Then add payload information in the **Package Description Editor** dialog box.

4. Select **Generate**.

   The file is added as a new template. Payload files are uploaded to the HPDM Master Repository automatically.

Copying a Deploy Image template for use with a different OS type

1. Right-click on a **Deploy Image** or **PXE Deploy Image** task template.

2. Select **Copy to other OS** from the menu.

3. Select the OS type and enter a name for the new template.

4. Select **OK**.

Template sequences

A template sequence can contain up to 50 task templates. The tasks are executed in a specified order, and a condition is evaluated before the execution of each task to determine if the task should be executed.

The following table describes the possible conditions.

Icon	Condition	Description
	Anyway	Execute the task regardless of if the previous task completed successfully.
	Success	Execute the task only if the previous task completed successfully.
	Failure	Execute the task only if the previous task failed.

To create a template sequence:

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

Basic template sequences

A basic template sequence uses the same condition between every task and can be defined by selecting the **Content** tab and then selecting **Basic**.

If you select the **Stop sequence on error** option, the template sequence will not continue if a single task fails.

Advanced template sequences

An advanced template sequence allows you to specify a different condition between every task and can be defined by selecting the **Content** tab and then selecting **Advanced**.

If you select the **Stop sequence on error** option, the template sequence will not continue if a single task fails.
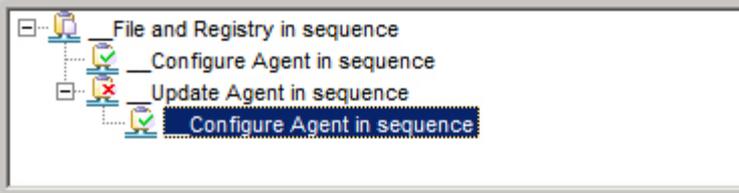
This example shows four tasks to be executed as follows:

- Unconditionally execute the File and Registry task.

- If the previous task completed successfully, execute the first Configure Agent task and exit the sequence.

- If the initial task fails, execute the Update Agent task.

- If the Update Agent task completes successfully, execute the final Configure Agent task and exit the sequence.

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 one of the following:

- One **anyway** condition

    –or–

- One **success** condition and one **failure** condition

Tasks

A task is a combination of a task template, an execution schedule, and a list of target devices. HPDM Console lists tasks in two groups:

- **Manual Tasks**—Created directly using HPDM Console (see Performing a task on page 18)

- **Rule Tasks**—Created indirectly using rules (see Task rules on page 21)

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

The task list consists of the following columns:

- **Task ID**—Indicates the ID of the task.

- **Task Name**—Indicates the name of task template used to send this task.

- **Progress and Status**—Indicates the progress and status of the task.

- **Target Device Number**—Indicates the number of devices to which the task was assigned.

- **Create Time**—Indicates when the task was created.

- **Sender**—Indicates the sender of the task.

Performing a task

1. Drag a task template from the task pane and drop it onto a device or group.

   – or –

   Right-click a device in the device pane or a folder in the device tree, and then select **Send Task** from the context menu to open the Template Chooser. Select a category, select a task template, and then select **Next**.

2. The **Task Editor** dialog box appears. 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 is applied to the device as soon as you select the **OK** button.

3. Select **OK** to apply the task to the device.

Task status icons

The following table describes the icons used in the Device Task View window.

Icon	Description
	Success The task was executed successfully by the device.
	Sending The task is being sending from HPDM Server through HPDM Gateway to the device and is waiting for a reply.
	Failed / Timeout The task has failed or timed out.
	Ready The task is executed and waiting for the user's operation.
	Paused The task has been paused.
	Cancelled The task has been cancelled.
	Waiting The task has been scheduled for sending at a later time, and has not been sent yet.
	Cached The task and its payload has been cached on the device and can be processed later.
	Processing The task has been accepted by the device and is being processed.

Task parameters

You can set default values for some task parameters via the Configuration Management dialog box. In HPDM Console, select **Tools**, select **Configuration**, and then expand the **Task Parameters** tree in the left-hand pane.

The Task Parameters tree consists of the following items:

- **Valid Time and Timeout**—Allows you to configure the following default parameters:
  - Valid time—Sets the duration HPDM waits for the execution of a task
  - Execution timeout—If a task processes longer than this value, it enters a timeout status, and HPDM Server tries to determine if the task is dead on the target device
  - Batch control—Controls how many devices are sent a task simultaneously and the interval between each batch (allowing you to have some control over network traffic)
  - Exclude working hours—Delays a task until the time is outside the specified working hours
- **Write Filter, WOL and Task Deferment**—Allows you to configure the following default parameters:
  - Write filter policy—Specifies how to handle the task if the write filter is on (applies to Windows only)
  - Wake On LAN—Specifies if HPDM should attempt to wake a device before sending the task
  - Task deferment—Specifies if a task can be deferred on the device side before a mandatory restart or shutdown (to give users a chance to save their work). For more information, see Task deferment on page 19.
- **Cached Updates**—Allows you to cache a task and payload on the device instead of executing the task immediately (send an **_Execute Cached Tasks** task later to execute the task)

You can set parameters for an individual task using the Task Editor after applying a task template to one or more devices. The Task Editor consists of the following tabs:

- **Content**—Allows you to specify parameters specific to the type of task
- **Schedule & Batch Control**—Allows you to set the task schedule and modify parameters for write filter policy, batch control, and task deferment for the specific task
- **Valid Time, Timeout & WOL**—Allows you to modify parameters for valid time, timeout, and Wake On LAN for the specific task
- **Cached Updates**—Allows you to cache a task and payload on the device instead of executing the task immediately (send an **_Execute Cached Tasks** task later to execute the task)
- **Target Device List**—Lists the devices the task is applied to, and allows you to add or remove devices

Task deferment

Task deferment allows users to save their work before an HPDM-initiated restart or shutdown of the device. Prior to the restart/shutdown, a dialog box is displayed to the user allowing them to postpone the restart/shutdown or initiate it immediately. The user can postpone the restart/shutdown a maximum of three times.

You must send a _Configure Task Deferment task to the device before any tasks can be deferred. This task also allows you to customize the title and message of the dialog box displayed to the user.

NOTE: If the device needs to forcibly restart, the dialog box 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 displays showing detailed information about the assigned task.

Pausing a task

NOTE: This operation is only available for tasks that have a status of Waiting.

To pause a task:

1. Select a task in the task pane.

2. Right-click and select **Pause** from the pop-up menu.

   The status of the task is changed to **Paused**.

Continuing a task

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 changes to **Waiting**.

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

Resending a task

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 a task

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

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

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

📝 **NOTE:** You cannot delete a cached task. A warning message prompts you to either execute or clear a cached task before you can delete it.

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 appears.

2. Select the target device to show the task log.

   📝 **NOTE:** To refresh the task log, press F5. To export the task log, right-click on the target device and select **Export Task Log**.

3. Select **Close** to close the log viewer when you have finished.

Displaying a task's success rate

To display a task's success rate:

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

Opening VNC Viewer for shadowing

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

Opening a Result Template

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

Viewing tasks from all users

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

Task rules

Rules allow you to automate the execution of tasks. Each rule has three parts: a filter to define to which devices the rule applies, a trigger that defines when the rule is executed, and a template which defines what operation the rules should perform on to the devices.

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

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

Adding a new rule

1. Select the **Add** button to open the **Rule Editor** window.

2. Each rule must be given a unique name.

3. Each rule must also have a filter defined. Select the **Choose** button to the right of the filter to open the **Filter Chooser** window.

4. You can then select a pre-existing filter or create a new one by selecting **Add**.

5. Once the name and filter are set you can select your trigger. There are three options:

    ● **First Contact**—The rule executes for each device that matches its filter criteria once when the device first registers itself with HPDM Server, or after completing a Factory Reset task.

    ● **Startup**—The rule executes for each device that matches its filter criteria every time the device restarts.

    ● **Scheduled**—This option expands the 'Rule Editor' window to enable you to specify a time and date for when the rule is executed and also the frequency at which it is repeated.

6. Specify the template to use.

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

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

8. The new rule is enabled by default. You can disable it by unchecking its check box in the **Rules Management** window.

NOTE: HPDM includes predefined **_Automatic Update Agents** rules that check the version of HPDM Agent when a startup report is received from a device. If the version on the device is older than the version in the rule, a task is sent to that device to update HPDM Agent. These rules are disabled by default.

5   Device management

Viewing devices

To view the currently managed devices in the device pane:

▲   Select a folder in the device tree.

To customize the columns of a device displayed in the device pane:

1.   In HPDM Console, select **View**, select **Device Columns**, and then select **More**.

     – or –

     Right-click a device column header, and then select **More**.

2.   In the resulting dialog, select whether to show or hide columns and order the columns.

To see a menu of applicable commands:

▲   Right-click a folder in the device tree.

     – or –

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

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

The following icons are used in the gateway tree of HPDM Console:

Icon	Description
	Represents a gateway that is currently active
	Represents a gateway that is currently down or disconnected

Deleting devices

To delete a device from the device tree:

1.   Right-click the folder in the device tree.

2.   Select **Delete** from the menu.

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

To delete a device from the device pane:

1.   Right-click the device in the device pane.

2.   Select **Delete** from the menu.

     The selected device is removed from the device pane.

Grouping devices

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

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

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

Setting group information using a DHCP tag

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

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

For example, if the path is set to Company/Department/Group the device tree shows:
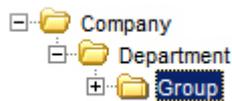
The format that is used by HPDM for tag 203 is as follows:

```
P1='<value>';P2='<value>';P3='<value>';P4='<value>';P5='<value>';P6='<value>';MG='<value>'
```

> **NOTE:** All of the parameters are optional, but any that are specified must be assigned a value.

For example:

```
P1='Asia';P2='China';P3='Shanghai';MG='Company/Department/Group'
```

Switch to Manual Grouping

1. Select the **Group by** button.
2. Select **Manual Group**, and then select **_global (system)**.
3. Any **Manual Groups** specified with the DHCP tag appear automatically.

Adding a new Manual Group

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

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

Dynamic Grouping

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

Creating a new Dynamic Grouping scheme

1. Select the **Group by** button.

2. Select **Edit Scheme** and be sure the **Dynamic Scheme** tab is selected.

3. Select **Add** and give the new scheme a name. Select **OK** to accept the new name.

4. Select and order the criteria you want to define in the scheme. **Extension Properties 1-6** correspond to the P1-P6 grouping items you can set with the DHCP tag 203.

5. Select **OK** to exit the **Edit Grouping Scheme** window.

Switching to a Dynamic Group

1. Select the **Group by** button.

2. Select **Dynamic Group**.

3. Select the scheme you wish to use.

Quick search

HPDM enables you to search quickly among currently listed devices. You can select any column header in the device table to add a search criteria or sort. All criteria are automatically cleared after switching to another folder.

Filtering devices

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

Creating a new Device Filter

1. Select **View** on the main menu then **Device Filter**

2. Select **Add** in the **Device Filter Management** window.

3. Give your new filter a name. Select **OK** to accept the name.

4. Select **Add...** in the **Edit Device Filter** dialog box to open the **Choose Criteria Key** dialog box.

5. In the **Choose Criteria Key List** dialog box, select the criteria according to your needs. Select **OK** to open the **Criterion Editor** dialog box for the chosen criterion.

6. Define the operator and value for the new criterion.

7. Repeat steps 4 through 6 to load more criteria, select **Save**, and then select **Close**.

8. Select the new filter from the **Filter** drop down list.

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

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

Editing a Device Filter

To edit a Device Filter:

1. Select **Device Filter** from the **View** menu.

2. Double-click an existing filter or choose an existing filter and then select **Edit...** to open the **Edit Device Filter** dialog box.

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

4. In the **Candidate Criteria Key List**, select the criteria according to your needs. Select **OK** to open the **Criterion Editor** dialog box for the chosen criterion.

5. Select the arrow button in the **Edit Criteria** section to select conditions in the drop-down menus. For example: **OS Type = HP ThinPro**.

6. If multiple filters exist in the **Criteria List**, you can select **Satisfy all criteria** or **Satisfy any criteria**. Then, select **Save** to return to the **Device Filter Management** dialog box.

7. In the **Device Filter Management** dialog box you can edit or remove the selected filter according to your requirements.

8. Select 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 or a group can see by assigning a filter to that user or group as a security filter. The procedure is as follows:

1. Select the **Tools** menu, and then select **User Management**.

2. Select the name of the user from the **Users** panel, and then select **Edit**.

3. Select the **Filter** tab.

4. Select the filter to use from the **Security Filter** list.

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

Checking network connection status

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

1. In the device pane, select one or more devices, right-click and select **Check Connection Status** from the context menu.

2. Select the utility you want to use to check the connection status of the device. You can choose from:

   - **Ping**—A basic Internet program that lets you verify that a particular Internet address exists and can accept requests. Pinging is diagnostically used to make sure that a host computer, which you are trying to reach, actually operates.

   - **Trace Route**—This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer.

A window displaying the network connection status of the device appears.

3. Select **Close**.

Shadowing devices

Shadowing enables you to connect to a remote device by SSL tunnel and view and control that device from HPDM Console. This can be achieved either via the **_Shadow Device** task template or via the context menu when you right-click a device as described in the following procedures.

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

To shadow a device:

1. Select a group of devices in the device pane or a device in the device tree.

2. Right-click and select **Shadow** from the pop-up menu. The **Task Editor** dialog box appears.

3. Select **OK**. When the Shadow processing task is complete, the remote desktop of the terminal is displayed in a separate window.

To Open VNC Viewer for Shadowing:

1. Select a completed **Shadow Device** task in the task pane.

2. Right-click and select **Open VNC Viewer for Shadowing**, or display the **Task** menu and select **Open VNC Viewer for Shadowing**.

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

Power management

HPDM Console enables you to restart, shut down, and wake a device remotely. This can be achieved either via task templates or via the context menu when you right-click a device as described in the following procedures.

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

To shut down, restart, or wake a device:

1. Right-click a device in the device pane, select **Power Management**, and then select **Reboot**, **Wake On LAN** or **Shutdown** from the context menu.

2. The **Task Editor** dialog box appears. Select **OK** to perform the task.

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

Managing normal thin clients

Changing a device's hostname

To change a device's hostname:

1. Right-click the desired device in HPDM Console and select **Rename**.

2. Edit the hostname value and select **OK** to automatically initiate a task.

3. Adjust the task settings as needed in the Task Editor (e.g. Write Filter Policy Setting).

4. Select **OK**.

Capturing and deploying connections

To capture connections:

1. Double-click the **_Pull Connection Configuration** template to open the Template Editor.

2. Use the check boxes to indicate which connection settings to capture.

3. In the **Save result as template** field, enter a name for the result template that will be created to store the captured connections.

4. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

5. Drag and drop the template onto the desired device.

6. Select **OK** to apply the task to the device.

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

To deploy captured connections:

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

Cloning and deploying settings

To clone settings:

1. Double-click the **_Clone Settings** template to open the Template Editor.

2. Use the check boxes to indicate which settings to clone.

3. In the **Save result as template** field, enter a name for the result template that will be created to store the cloned settings.

4. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

5. Drag and drop the template onto the desired device.

6. Select **OK** to apply the task to the device.

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

To deploy cloned settings:

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

Applying custom settings

To apply custom settings:

1. Double-click the **_Apply Settings** template to open the Template Editor.

2. Select the **Edit** button.

3. Use the check boxes to indicate which settings to edit.

4. Configure individual settings as desired.

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

    📝 **NOTE:** When configuring Time Settings, the available time zone values for all Windows-based devices are unified with those available for Windows Embedded Standard 7 devices. Some of the values might not be supported by Windows Embedded 2009 or Windows XP Embedded. Also, not all values on Windows Embedded 2009 and Windows XP Embedded are supported by HPDM templates and tasks.

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

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

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

    ● When the **Type** value is **Network**, **Address** and **Port** can be edited.

    ● When the **Type** value is **LPT** or **COM**, **Port** can be edited.

    ● When the **Type** value is **USB**, nothing can be edited.

5. Once the settings are configured, navigate to the **Summary** page. This page lists all settings that will be changed by this template.

6. If the changes are correct, select **Finish** to go back to the Template Editor.

7. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

8. Drag and drop the template onto the desired devices.

9. Select **OK** to apply the task to the devices.

Managing files and registry settings

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

The following subtasks are available:

● **Capture Files**—See Capturing files on page 30.

● **Deploy Files**—See Deploying files on page 30.

● **Delete Files**—See Deleting files on page 31.

● **Registry**—See Managing device registry settings on page 31.

● **Command**—See Remotely executing commands on page 32.

● **Pause**—See Pausing a _File and Registry task on page 33.

● **Program Record**—See Adding or removing program records on page 33.

● **Script**—See Running a script on page 34.

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

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

2. **Add**, **Edit**, **Delete**, and rearrange subtasks **Up** and **Down** as necessary.

3. Select **Save as** to name and save the template for later use.

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

To merge **_File and Registry** templates:

1. Right-click on a **_File and Registry** template, and select **Merge**.

2. Select another **_File and Registry** template, and then select **OK**.

3. Enter a name for the merged template when prompted.

Capturing files

To capture files from a device and save them to the HPDM Master Repository:

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

2. Select **Add**, select the **Capture Files** subtask, and then select **OK**.

3. In the Capture Files Editor, specify the path of the file or folder to transfer. Additional lines can be added by selecting **Add**.

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

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

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

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

5. Select the **Overwrite if exists** option if desired.

6. Select **OK** when you are finished specifying files.

7. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

8. Drag and drop the template onto the desired devices.

9. Select **OK** to apply the task to the devices.

Deploying files

To deploy files to devices:

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

2. Select **Add**, select the **Deploy Files** subtask, and then select **OK**.

3. Add files to transfer by selecting **Add from local** or **Choose upload**.

4. Select **OK** when you are finished specifying files.

5. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

6. Drag and drop the template onto the desired devices.

7. Select **OK** to apply the task to the devices.

Deleting files

To delete files from devices:

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

2. Select **Add**, select the **Delete Files** subtask, and then select **OK**.

3. Add files or folders to delete. Each line has the following options:

   ● **File or Folder Name**—Enter the file or folder name to delete. The wildcards * and ? are also supported.

   ● **Path On Device**—Enter the path on the device where the file or folder is located.

   ● **Delete Recursively**—Set this option to **Yes** if you want to delete all files or folders that match the pattern entered in **File or Folder Name** in all subdirectories under the **Path On Device**. If set to **No**, subdirectories will not be affected.

4. Select **OK** when you are finished specifying files.

5. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

6. Drag and drop the template onto the desired devices.

7. Select **OK** to apply the task to the devices.

Managing device registry settings

You can manage device registry settings in the following ways:

● Cloning registry settings on page 31

● Adding, editing, and deleting registry settings on page 32

Cloning registry settings

To clone registry settings from a device:

1. Double-click the **_Get Registry** template to open the Template Editor.

2. Select **Add**, enter the name of the registry node from which you want to clone settings (such as `desktop` for desktop settings), and then select **OK**. The node appears in the **Registry** panel of the Template Editor.

3. In the **Save result as template** field, enter a name for the result template that will be created to store the cloned registry settings.

4. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

5. Drag and drop the template onto the desired device.

6. Select **OK** to apply the task to the device.

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

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

Adding, editing, and deleting registry settings

To add, edit, or delete registry settings:

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

   If you want to create a new template, double-click the **_File and Registry** template to open the Template Editor, and then select **Add**. Select the **Registry** subtask, and then select **OK**.

2.   Configure the registry settings in the editor as necessary using the following methods:

   ●   Use the **Registry Tree** to navigate the registry node and add, rename, or delete registry keys and values.

   ●   Use the **Registry Settings** pane to add or delete values from the selected registry key.

   ●   Use the **Action to Perform** pane to add or delete a registry key. If you have modified the key's values individually in the Registry Settings pane, the options in this pane are greyed out.

   ●   Select **Import Registry File** to import registry settings.

3.   Select **OK** when you are finished editing registry settings.

4.   Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

5.   Drag and drop the template onto the desired devices.

6.   Select **OK** to apply the task to the devices.

Remotely executing commands

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

●   Applications

●   DOS batch files

●   Windows scripts

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

To remotely execute commands on a device:

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

2.   Select **Add**, select the **Command** subtask, and then select **OK**.

3.   In the editor, enter the command in the **Command** column.

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

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

5. In the **Wait** column, select **Yes** if the command has to wait for the previous command to finish before executing.

6. If you want to add more commands, select **Add**.

7. Select **OK** when you are finished editing registry settings.

8. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

9. Drag and drop the template onto the desired devices.

10. Select **OK** to apply the task to the devices.

Remotely executing Windows scripts

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

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

To run Windows scripts as a command using HPDM:

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

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

Pausing a _File and Registry task

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

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

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

2. Specify the pause duration, and then select **OK**.

Adding or removing program records

To add or remove program records:

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

2. Select **Add**, select the **Program Record** subtask, and then select **OK**.

3. In the Program Record Editor, select **Add**.

4. Specify the action type (add or remove).

5. Input the publisher, version, and comments if necessary.

6. Select **OK** when you are finished editing program records.

7. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

8. Drag and drop the template onto the desired devices.

9. Select **OK** to apply the task to the devices.

Running a script

To run a script on a device:

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

2. Select **Add**, select the **Script** subtask, and then select **OK**.

3. In the editor, enter the script content.

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

4. For Windows platforms only, specify the path to start the script in if necessary.

5. For Windows platforms only, specify the user account to run the script for if necessary.

6. Select **OK** when you are finished editing the script.

7. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

8. Drag and drop the template onto the desired devices.

9. Select **OK** to apply the task to the devices.

Enrolling certificates with SCEP

To enroll certificates with SCEP:

1. Double-click the **_Enroll Certificate with SCEP** template to open the Template Editor.

2. Enter the URL for enrollment and the challenge password.

3. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

4. Drag and drop the template onto the desired device.

5. Select **OK** to apply the task to the device.

Managing PCoIP zero clients

Capturing connections

To capture connections from a PCoIP zero client:

1. Double-click the **_Capture Connections** template to open the Template Editor.

2. In the **Save result as template** field, enter a name for the result template that will be created to store the captured connections.

3. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

4. Drag and drop the template onto the desired device.

5. Select **OK** to apply the task to the device.

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

Deploying connections

To deploy connections to PCoIP zero clients:

1. Double-click the **_Deploy Connections** template or the result template of a **_Capture Connections** task to open the Template Editor.

2. If necessary, select the connection type and set the values.

3. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.

4. Drag and drop the template onto the desired devices.

5. Select **OK** to apply the task to the devices.

Updating firmware

To update firmware on PCoIP zero clients:

1. In HPDM Console, select **Template**, select **Import**, and then select **PCoIP firmware**.

2. Select **Browse** to choose a firmware file (.all), and then select **Import**.

3. Select **Generate**, and then wait until the template is created successfully. The template is added to the Task Templates list.

4. Drag and drop the template onto the desired devices.

5. Select **OK** to apply the task to the devices.

6 Imaging operations

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

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

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

For information about imaging support for each specific operating system, see the *Release Notes* for your version of HPDM or HPDM Service Pack.

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

- Imaging without PXE on page 36 (recommended)

- Imaging with PXE on page 39

NOTE: For information about supported thin clients and imaging support for specific thin-client models, see the release notes for your version of HPDM.

Imaging without PXE

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

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

Capturing an image without PXE

To capture an image without PXE:

1. Select the **Task Templates** tab in the task pane, and then double-click the **_Capture Image** template.

2. In the **Template Editor – Imaging** dialog box, enter information into the **Image Name** and **Description** fields.

3. If the device uses a wireless network, select **Cache captured image file on thin client before uploading to Master Repository**.

   NOTE: If the **Cache captured image file on thin client before uploading to Master Repository** option is selected, it requires enough free disk space on the device to cache the captured image.

4. Select the **Save as** button, enter a name for this template, and then select **OK**. A new template appears in the task pane.

5. Drag and drop this template onto a device in the device pane. The **Task Editor** dialog box appears.

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

7. Select **OK** to apply the task to the device immediately. When the task is sent, a result template is created with the name you designated. Its initial status is "Transferring."

8. When HPDM Agent receives the task, the device displays a warning message indicating that a restart will occur in 30 seconds. After the device restarts, the image is captured to the HPDM Master Repository.

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

9. The device restarts after capturing has completed.

    IMPORTANT: Do not turn off the device during this procedure.

    The device restarts again.

10. The task pane in HPDM Console will continue to indicate that the task is processing. The captured image is being compressed. After the task is finished and the checksum of the captured image is verified, a new template appears in the Task Templates list with the name you specified.

11. You can now use this template to apply the captured image to other devices by dragging and dropping it onto devices in the device pane or folders in the device tree.

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

Preserved settings during an image capture without PXE

Operating system	Preserved settings
Windows 10 IoT Enterprise Windows Embedded 8.1 Industry Pro Windows Embedded 8 Standard Windows Embedded Standard 7 Windows Embedded Standard 2009	All settings from the source device are preserved on both the source device and the captured image except the hostname, network settings, domain settings, and write filter status.
HP ThinPro HP Smart Zero Core	All settings from the source device are preserved on both the source device and the captured image except the hostname and network settings.

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

Deploying an image without PXE

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

To deploy an image without PXE:

1. Create a deployment template by capturing an image without PXE (see <u>Capturing an image without PXE on page 36</u>).

   – or –

   From the menu, select **Template**, select **Import**, select **Image Files**, and then select **to deploy without PXE**. The wizard then automatically creates a deployment template.

2. Double-click on the deployment template to open the **Template Editor**.

3. Select the **View Details** button to view detailed information about the image package.

4. 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**. If this option is selected, you need to make sure the image can work well on the target device.

5. Select the **Save as** button to save the template with a new name.

6. Drag and drop the template onto the devices to which you want to deploy the image. The **Task Editor** dialog box appears, allowing you to edit the same options you were presented with in the Template Editor.

7. If the device uses a wireless network or if you want to deploy an image with cached updates, select the **Cached Updates** tab, and then select **Cache task and payload on device instead of executing task immediately**.

   NOTE: If the **Cached Updates** option is selected when sending a task, the task is cached after the image file is cached on the device. You need to send the **_Execute Cached Tasks** task to the device to execute the cached imaging task.

   This option requires enough free disk space on the device to cache the image file.

   NOTE: In cached updates mode, HPDM only supports deploying .ibr images to Windows-based devices or .dd.gz images to HP ThinPro-based devices.

8. Select **OK** to deploy the image to the devices.

NOTE: There is an automatic BIOS update during a **_Deploy Image** task to install Windows Embedded Standard 7 SP1 on the t5740 or t5740e. The factory BIOS version is 1.03 on the t5740 and t5740e, and Windows Embedded Standard 7 SP1 requires version 1.04.

Preserved settings during an image deployment without PXE

Operating system	Preserved settings
Windows 10 IoT Enterprise	● Write filter status
Windows Embedded 8.1 Industry Pro	● Hostname
Windows Embedded 8 Standard	● Network settings
Windows Embedded Standard 7	● Terminal Services license
Windows Embedded Standard 2009	● Windows activation license (select operating systems only)
HP ThinPro	● Hostname
HP Smart Zero Core	● Network settings

Imaging with PXE

PXE is an optional imaging method that is best for remote system recovery. HPDM Gateway includes a PXE service that is disabled by default but can be configured to start and stop at the same time as the HPDM Gateway service.

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

☼ **TIP:** Some additional configurations might be required for PXE imaging. If you experience problems with PXE imaging, see Configuring your environment for PXE imaging on page 40.

Creating a PXE Deploy template

There is no PXE Deploy template by default, but there are three ways to create a PXE Deploy template:

- Import an image file

- Convert a Deploy Image template to a PXE Deploy template

- Copy an existing PXE Deploy template to use for a different OS

Importing an image file

1. From the HPDM Console menu bar, select **Template > Import > Image Files > to deploy using PXE**.

2. In the **Import Image File** dialog box, select **Browse** to choose an image file to import.

3. Select **Import**.

4. In the **Package Description Editor**, enter the necessary information about this image file.

   📝 **NOTE:** Select **OS Type** of the image itself.

5. Select **Generate** to begin uploading the image file to the repository.

6. After the upload is complete, select **OK** in the confirmation dialog box.

Converting a Deploy Image template to a PXE Deploy template

1. Select a **Deploy Image** template, and then from the **HPDM Console** menu bar, select **Template > Create template for PXE Deploy**.

   – or –

   Right-click a **Deploy Image** template in the task pane and select **Create template for PXE Deploy**.

2. In the dialog box that appears, select the operating system type to convert the template to, and then select **OK**. The new PXE Deploy template is now listed in the task pane.

Copying an existing PXE Deploy template to use for a different OS

1. Right-click a **Deploy Image** template in the task pane and select **Copy to other OS**.

2. In the dialog box that appears, select the operating system type to copy the template to, and then select **OK**.

Deploying an image with PXE

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

To deploy an image with PXE:

1. From the menu, select **Template**, select **Import**, select **Image Files**, and then select **to deploy using PXE**. The wizard automatically creates a deployment template.

2. Drag the deployment template onto a device.

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

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

Configuring your environment for PXE imaging

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

● Configuring a device to boot from PXE

● Configuring a DHCP server for PXE imaging

● Configuring routers for PXE imaging

● Configuring BIOS settings on legacy Neoware devices for PXE imaging

Configuring a device to boot from PXE

The boot order can be changed locally (on the device side) or remotely. HP recommends that you change the boot order locally.

Changing the boot order locally

1. Turn on or restart the device.

2. Press F10 during startup to access the BIOS settings.

3. Locate the boot order settings, and set the PXE network controller as the first legacy boot source.

Changing the boot order remotely

Windows

This example uses a t520 based on Windows Embedded Standard 7P (64-bit).

1. Download the HP BIOS Configuration Utility (BCU) from http://ftp.hp.com/pub/caps-softpaq/cmit/HP_BCU.html.

2. Install BCU on the same computer as HPDM Console.

3. In HPDM Console, create a **File and Registry** template with the following subtasks in order:

   a. Deploy Files (to deploy **BiosConfigUtility64.exe** to the device).

   b. Script (to execute a BCU command that gets the BIOS settings of the device and writes them to a file). See the following table for an example script.

Field	User input
Start in	`c:\temp`
Content	`cd c:\temp`
	`BiosConfigUtility64.exe /set "c:\temp\t520_BiosConfig.txt"`

    c. Capture Files (to capture the file from **d:\temp\t520_BiosConfig.txt** to the master repository).

4. Send the File and Registry task to the target device.

After the task is complete, the captured file should be located in the master repository at \Repository\Files\Captured\.

5. Create a copy of t520_BiosConfig.txt, and then rename the new file to **set_bootOrder_t520.txt**.

6. Open **set_bootOrder_t250.txt** in Notepad.

7. Delete all of the file contents except for the file heading and the two boot source sections.

8. Move the PXE network controller to be the first legacy boot source, and then save and close the file.

9. In HPDM Console, create a **File and Registry** template with the following subtasks in order:

    a. Deploy Files (to deploy **BiosConfigUtility64.exe** and **set_bootOrder_t520.txt** to the device)

    b. Script (to execute a BCU command that applies the new settings, in this case, the boot order) See the following for an example script.

Field	User input
Start in	`c:\temp`
Content	`cd c:\temp`
	`BiosConfigUtility64.exe /set "c:\temp\t520_BiosConfig.txt"`

10. Send the File and Registry task to the target devices.

NOTE: The hardware platform of the target devices must be the same as the device that you got the BIOS settings from.

Before changing the boot order on multiple devices, you should test the task on a single device.

HP ThinPro

This example uses a t630 based on HP ThinPro 6.

NOTE: This procedure requires Notepad++ and only works for the t628, t630, and t730. If you want to remotely change the boot order on other platforms, contact HP for support.

1. In HPDM Console, create a **File and Registry** template with the following subtasks in order:

    a. Script (to get the BIOS settings of the device and write them to a file)

    For example:

```
hptc-bios-cfg —G /tmp/t630_BiosConfig.txt
```

    b. Capture Files (to capture the file from **/tmp/t630_BiosConfig.txt** to the master repository).

2. Send the File and Registry task to the target device.

After the task is complete, the captured file should be located in the master repository at \Repository \Files\Captured\.

3. Create a copy of t630_BiosConfig.txt, and then rename the new file to **set_bootOrder_t630.txt**.

4. Open set_bootOrder_t630.txt in Notepad++.

5. Select **Edit > EOL Conversion**, and then select the item for **Windows** (the name depends on your version of Notepad++).

6. If not already enabled, enable the **Show End of Line** option under **View > Show Symbol**.

7. Delete all of the file contents except for the Legacy Boot Source seciton.

8. Move the PXE network controller to be the first legacy boot source, and then save and close the file.

9. In HPDM Console, create a File and Registry template with the following subtasks in order:

    a. Deploy Files (to deploy **set_bootOrder_t630.txt** to the device).

    b. Script (to execute a BCU command that applies the new settings, in this case, the boot order).

    For example:

```
hptc-bios-cfg —S /tmp/set_bootOrder_t630.txt
```

10. Send the File and Registry task to the target devices.

> 📝 **NOTE:** The hardware platform of the target devices must be the same as the device that you got the BIOS settings from. Before changing the boot order on multiple devices, you should test the task on a single device.

11. Send a Reboot Device task to reboot the target devices.

Configuring a DHCP server for PXE imaging

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

The DHCP server is installed on a different physical server from HPDM Server

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

To configure the DHCP server:

1. Make sure that the DHCP server has not been previously configured for a PXE bootstrap.

2. Make sure that DHCP options 43 and 60 are not set.

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

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

These instructions assume the following:

- The network is already configured using DHCP.

- The DHCP server has not been previously configured for a PXE bootstrap.

- There are no other TFTP servers running on the same network.

To configure the DHCP server:

1. Make sure that DHCP option 43 is not set.

2. Add DHCP option 60 by doing the following:

   a. In Windows, select **Start**, and then select **Run**.

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

   b. Enter `cmd`, and then select **OK** to open Command Prompt.

   c. Enter `netsh`.

   d. Enter `dhcp`.

   e. Enter one of the following commands:

      ```
      server \\<hostname>
      ```

      – or –

      ```
      server <IP address>
      ```

   f. At the **dhcp server>** prompt, enter the following command (replace `<name>` with any custom name):

      ```
      add optiondef 60 <name> STRING 0
      ```

   g. Enter the following command:

      ```
      set optionvalue 60 STRING "PXEClient"
      ```

   h. To confirm that the settings are correct, enter `show optionvalue all`.

3. Add DHCP option 201 by doing the following:

   a. At the **dhcp server>** prompt, enter the following command (replace `<name>` with any custom name):

      ```
      add optiondef 201 <name> STRING 0
      ```

   b. Enter the following command:

      ```
      set optionvalue 201 STRING '<HPDM Gateway IP address>' '40003'
      ```

   📝 **NOTE:** See the following example:

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

   c. To confirm that the settings are correct, enter `show optionvalue all`.

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

Configuring a Linux DHCP server for PXE imaging

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

```
ddns-update-style ad-hoc;
Authoritative;
Option NDM code 201 =string;
Option vendor-class-identifier "PXEClient";
Option NDM "'<HPDM Puerta de enlace IP address>' '40003'";
```

📝 **NOTE:** See the following example:

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

2. Restart dhcpd to use the new configuration.

Configuring routers for PXE imaging

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

The following example uses a Cisco router in global configuration mode:

1. Enter the following command:

```
ip forward-protocol udp 67
```

2. Enter the following command:

```
ip forward-protocol udp 68
```

3. Enter the following command:

```
ip helper-address <DHCP server IP address>
```

4. Enter the following command:

```
ip helper-address <HPDM Gateway IP address>
```

Configuring BIOS settings on legacy Neoware devices for PXE imaging

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

To configure BIOS settings on legacy Neoware devices for PXE:

1. Turn on the device and hold down the Delete key to display the **CMOS Setup Utility** screen.

2. Select **Advanced BIOS Features** and set the following:

```
 First Boot Device [LAN]
Second Boot Device [HDD-0]
```

3. Press the Esc key to return to the initial screen, select **Integrated Peripherals**, and then select **VIA OnChip PCI Device**.

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

5. Press the F10 key, press the Y key, and then press Enter to save the settings.

Deploying the image

If the device has no operating system or is turned off, in HPDM Console, drag a PXE Deploy template onto the device, and then select **OK** to send the task.

This method does not work if the operating system is Windows Embedded 8 Standard or Windows 10 loT Enterprise. Use the following method instead.

If the device has an operating system and is turned on, do the following:

1. In HPDM Console, drag a PXE Deploy template onto the device, and then select **OK** to send the task.

    If the device's current operating system is not Windows Embedded 8 Standard or Windows 10 loT Enterprise, the device automatically restarts and boots to PXE, and you can skip the rest of this procedure.

    If the device's current operating system is Windows Embedded 8 Standard or Windows 10 loT Enterprise, continue this procedure.

2. Restart the device manually and press F9 during startup to access the **Please select boot device** menu.

3. Press Enter to select the PXE network controller as the boot device.

Troubleshooting

-   Verify that the device supports imaging using PXE (see the HPDM release notes).

-   Verify that all HPDM components are 4.7 SP6 or newer.

-   Verify that the device is set to boot from PXE

-   Verify that there is only one PXE service running in your network.

-   If the image file is Windows-based, verify that the devices can connect to the Shared Folder.

-   If using Shared Folder, verify that its password is simple enough. Do not include the following characters: ~!@#$%^&*()/.

-   Verify that the device is not connected via a wireless network (HPDM does not support PXE deployment to a device connected via a wireless network).

-   If a turned-off device does not boot from PXE upon receiving the PXE Deploy task, verify that the **Remote Wakeup Boot Source** setting in the BIOS is set to **Remote Server** or **Wake On LAN** (the name depends on the device's BIOS version).

7   Repository management

Configuring the HPDM Master Repository

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select the HPDM Master Repository and select **Edit**.

3. In the Repository Configuration Wizard, enter a repository name and the server address.

4. Select the protocols to use.

5. Configure the user name, password, and path for each protocol.

    NOTE: Paths must point to the same location you configured for HPDM Master Repository Controller during installation. For example, if you entered `c:\ftproot\HPDM` during installation, for FTP you access this folder via `ftp://IP/HPDM`, and for Shared Folder you access it via `\\IP\HPDM`. You should enter **HPDM** for the Path value of the FTP and the Shared Folder.

6. Select **Test** to test the connections you've configured and display results on-screen.

7. Select **Finish**.

    NOTE: If you changed the repository path, HPDM Server needs time to establish the new connection. Wait for a while before doing repository-related operations.

Configuring an HPDM Child Repository

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select **Add**.

3. In the Repository Configuration Wizard, enter a repository name and the server address.

4. Select the protocols to use.

5. Configure the user name, password, and path for each protocol.

6. Select **Test** to test the connections you've configured and display results on-screen.

7. Select **Finish**.

Deleting an HPDM Child Repository

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select an HPDM Child Repository.

3. Select **Remove**, and then select **Yes** to confirm.

Exporting repositories

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select **Export**.

3. Browse to the location where you want to save the repositories.

4. Select the **Export** button. All repositories are exported to an XML file.

Importing repositories

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select **Import**.

3. Browse to the location where the repositories you want to import are located.

4. Select the **Import** button.

Synchronizing repositories

When a task that requires repository content starts, the content is automatically synced from the HPDM Master Repository to each appropriate HPDM Child Repository.

If you want to synchronize all content to every HPDM Child Repository (which is not required), use either of the following methods:

- Manually start a synchronization

- Schedule synchronizations to automatically occur at times you specify

To manually start a synchronization of all content to every HPDM Child Repository:

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select **Sync**.

3. In the **Synchronization** dialog box, select **Sync**.

4. Select **Yes**.

To schedule synchronizations to automatically occur at times you specify:

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select **Sync**.

3. In the **Synchronization** dialog box, select the **Enable schedule synchronization** option.

4. Configure the schedule settings.

5. Select **Save**.

Content management

To view the contents of the HPDM Master Repository:

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. In the **Repository Management** dialog box, select **Content**.

Viewing detailed payload information

To view detailed payload information:

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

Deleting contents from the HPDM Master Repository

To delete contents from the HPDM Master Repository:

▲ In the Content Management dialog box, select an item in the right panel, and then select the **Delete** button. A confirmation message appears. Select **Yes**, and the payload is deleted.

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

Downloading contents from the Files Captured category

To download contents from the HPDM Master Repository:

1. In the Content Management dialog box, select an item in the **Files Captured** category, and then select the **Download** button.

2. Browse to the location where you want to save it. The content is downloaded to the local machine.

Repository mapping

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

To access the Repository Mapping dialog box:

1. In HPDM Console, select **Tools**, and then select **Repository Management**.

2. Select **Mapping**.

Batch mapping

You can map devices to repositories according to each device's HPDM Gateway or subnet address. To change the mapping for a particular item, right-click the item, and then select one of the following options:

● **Auto Map**—HPDM Server assigns a repository to each HPDM Gateway or subnet address.

● **Use Master**—Uses the HPDM Master Repository.

● **Use Specified**—Allows you to choose a repository from a list for the specified HPDM Gateway or subnet address.

> **NOTE:** You can view all mapping results by clearing the **Show exceptions only** option. HPDM automatically maps any new devices in 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 for details about filters.

8 Security management

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

User management

Each user account can have customized privileges, according to their level of need. Privileges are assigned based on the groups a user is added to.

To view the User Management dialog box:

▲ In HPDM Console, select **Tools**, and then select **User Management**.

Adding users

1. In the User Management dialog box, select **Add** to add a new user. The **Create New User** dialog box appears.

2. Enter a **Username** for the new user and specify a **Password**. Select **OK** to create the new user.

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

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

> 📝 **NOTE:** Multiple instances of HPDM Console cannot log on to HPDM Server with the same username at the same time.

Deleting users

1. In the User Management dialog box, select a user from the list in the **Users** panel.

2. Select **Delete**, and then select **Yes** to confirm.

Assigning users to groups

1. In the User Management dialog box, double-click a user from the list in the **Users** panel.

2. Select the **Member Of** tab.

3. Select **Add** to add the user to a new group, or select **Remove** to remove the user from the selected group.

Changing a user's password

1. In the User Management dialog box, right-click on a user from the list in the **Users** panel.

2. Select **Change Password** from the pop-up menu.

3. Enter the **New Password** for the user, and then re-enter it in the **Confirm Password** field.

4. Select **OK** to finish.

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

Assigning security filters to users

1. In the User Management dialog box, double-click a user from the list in the **Users** panel.

2. Select the **Filter** tab.

3. Select **Add** to add the filter to this user, or select **Remove** to remove the security filter from this user.

    📝 **NOTE:** The added security filter is a copy of a device filter. Modifying the device filter will not affect the security filter.

Adding a group

Groups can be used to control user privileges in HPDM.

1. In the User Management dialog box, select the **Groups** tab.

2. Select **Add** to add a new group. This group can now be assigned a set of privileges, and then users can be assigned to this group.

Assigning privileges to groups

1. In the User Management dialog box, right-click on a group from the list in the **Groups** panel.

2. Select **Properties** in the pop-up menu.

3. Select the **Privileges** tab.

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

5. Select **OK** to finish.

    📝 **NOTE:** Aside from the group privilege to control the common operations in HPDM, there is an additional template privilege to control each template, including viewing, modifying, and executing operations.

Assigning users to groups

1. In the User Management dialog box, right-click on a group from the list in the **Groups** panel.

2. Select **Properties** in the pop-up menu.

3. Select the **Users** tab.

4. Use the **Add** and **Delete** buttons to modify the members of this group.

5. Select **OK** to finish.

Assigning security filters to groups

1. In the User Management dialog box, double-click on a group from the list in the **Groups** panel.

2. Select the **Filter** tab.

3. Select **Add** to add the filter to this group, or select **Remove** to remove the security filter from this group.

    📝 **NOTE:** The added security filter is a copy of a device filter. Modifying the device filter will not affect the security filter.

Deleting groups

1. In the User Management dialog box, select a group from the list in the **Groups** panel.

2. Select the **Delete** button, and then select **Yes** to confirm.

User authentication with LDAP and Active Directory

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

Configuration

You can configure more than one LDAP server for user authentication. To configure a connection to an LDAP server:

1. In HPDM Console, select **Tools**, and then select **Configuration**.

2. In the **Configuration Management** dialog box, select **LDAP Settings** in the left pane.

3. Click **Add** to create a new LDAP setting.

4. Enter the name of the LDAP setting, and click **OK**.

5. In the **Host** field, type the LDAP server hostname or IP address. If an encrypted connection is used, the LDAP server must be specified by the hostname.

6. 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.

7. Select an **Encryption** type.

8. If a TLS or SSL encryption is in use, a **Host Key** must be specified. Do one of the following:

   ▲ Select **Get Key From Host**. A connection is created to the LDAP server, and the host key is saved.

   − or −

   ▲ Select **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 file can be obtained from the following location:

     `http://<LDAP server address>/certsrv/certcarc.asp`

   - Java KeyStore: An hpdmcert.key file from a previous HPDM installation or another Java KeyStore file can be imported.

9. In the **Server Type** section, choose a LDAP server type from the **Type** menu.

   a. **Active Directory**: Specify the Active Directory **Domain**. Only a single Domain is supported.

   b. **Generic LDAP**:

   - Specify the **Base DN**. A Base DN (Distinguished Name) is required to connect to the LDAP Server. Please refer to your LDAP server documentation for further details about the Base DN.

     Examples of Base DNs:

- 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**.

10. Configure a **Search User**. This Search User is 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**. The Display Name is shown on the General panel of the Properties window and is the LDAP CN.

    For example, a Display Name of "HPDM search user" in the Users directory of the domain "testnet.com", the DN is:

    CN=hpdm search user,CN=Users,DC=testnet,DC=com

11. Finally, test the configuration by selecting the **Test** button. When the configuration for the LDAP server has been completed successfully, this test will pass.

📝 **NOTE:** HPDM supports both single domain authentication and multiple trusted domains authentication.

Importing users and groups

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

To open the Import Tool:

1. In HPDM Console, select **Tools**, and then select **User Management**.

2. Select the **LDAP Settings** button.

3. Select one LDAP setting from the left pane, and then select **Import users and groups**.

– or –

▲ In HPDM Console, select **Tools**, select **Configuration**, select **LDAP Settings**, select one of the LDAP settings from the left pane, and then select **Import users and groups**.

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 selecting 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. Select **Show 20 more** to show more results.

To search for a user or group:

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

2. The **Base DN** is the starting point from which the search runs. All searches are 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, **=**, finds LDAP objects that are equivalent to the search value.

      ● The **Greater than or Equals** comparison, **>=**, finds LDAP objects with an attribute value that is numerically larger than the search value.

      ● The **Less than or Equals** comparison, **<=**, similarly finds LDAP objects with an attribute value that is numerically smaller than the search value.

      ● The **Similar to** comparison, **~=**, permits searching for attribute values that are similar to the search value.

      ● Finally, the **Not Equals** comparison, **!=**, permits searching for attribute values that are not equivalent to the search value.

4. Finally, press the **Search** button. Results appear in the **Search** tree to the left.

To add a user or group to the import list:

1. Locate the user or group, either by **Browse** or **Search**.

2. Add the user or group using one of the following methods:

   ● Double-click the user or group.

      – or –

   ● Select the user or group, and then select **Add**.

3. The user or group should now be on the right side.

📝 **NOTE:** The users and groups are not imported until you select the **Import** button in the bottom-right corner. After importing a group, the privileges of the group must be assigned (see Assigning privileges to groups on page 50).

To remove a user or group from the import list:

1. Select a user or group on the right side of the **Import Users and Groups** dialog box.

2. Select the **Remove** button.

To examine a user or group:

1. Select a user or group.

2. Select the **Show Attributes** button.

3. If desired, this object can be added to the import list by selecting the **Add** button.

Authentication management

Because HPDM Server can discover and manage all instances of HPDM Gateway and HPDM Agent on the network, a security issue could occur due to improper usage of HPDM Server. To overcome this issue, HPDM has an authentication function that allows HPDM Gateway and HPDM Agent to recognize a secure HPDM Server.

There are two tools for providing authentication: **Key Management** and **HPDM Gateway Access Control**. To find these tools, in HPDM Console, select **Tools**, and then select **Authentication Management**.

Key management

An Authentication Key is a plain text password that is entered via HPDM Console. The key is passed to the devices during the key update process. The devices will check the key passed by HPDM Server when executing tasks.

To update the current Authentication Key:

1. In HPDM Console, select **Tools**, select **Authentication Management**, and then select **Key Management**.

2. Enter your user **Password**, and then select **OK**.

3. Select **Update Current Key**.

4. Enter the new **Password** (the authentication key) and specify a value for **Expire Interval** (number of days).

    NOTE: This value is the time that the key stays valid. If a device cannot contact HPDM Gateway for key information before the specified time, the key will expire and HPDM Agent will revert to its initial key.

5. Select **OK**.

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. Select 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, and then select the **Export** button.

3. The system prompts you to create and confirm the KeyStore password.

4. In the **Create KeyStore Password** dialog box, enter a KeyStore **Password** and confirm the password in the **Re-enter Password** field.

5. Select the **OK** button.

To import Authentication Key(s):

1.	Select the **Import Key(s)** button in the **Key Management** window to display the Import dialog box.

2.	Browse for the exported ***.ks** file, and then select the **Import** button.

3.	The system prompts you to enter the KeyStore password.

4.	Enter the KeyStore **Password** then select the **OK** button.

Viewing the Key Update Log

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

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

HPDM Gateway access control

HPDM Server communicates with HPDM gateways that have a status of Acknowledged (safe) and does not communicate with HPDM gateways that have a status of Banned (unsafe). When an HPDM Gateway is discovered by HPDM Server, the status of that HPDM Gateway is set to Unknown. By default, an HPDM Gateway with a status of Unknown is automatically regarded as Acknowledged (safe) by HPDM Server. You can change this behavior, as well as manually acknowledge or ban an HPDM Gateway, via the HPDM Gateway Access Control window.

To open the HPDM Gateway Access Control window:

1.	In HPDM Console, select **Tools**, select **Authentication Management**, and then select **HPDM Gateway Access Control**.

2.	In the authentication dialog box that opens, enter your password, and then select **OK**.

To acknowledge or ban an HPDM Gateway manually:

▲	In the HPDM Gateway Access Control window, select an HPDM Gateway from the list, and then select the **Acknowledge** or **Ban** button.

To set all HPDM gateways that have a status of Unknown to be automatically regarded as Banned (unsafe) by HPDM Server:

▲	In the HPDM Gateway Access Control window, select the option **Manually control HPDM Gateway access**.

9 Report management

Adding a report

To add a report:

1. In HPDM Console, select **File**, and then select **Manage Report**.

2. Select one report type from the **Report Types** buttons, and then select the **Add** button. A **Set New Report Name** dialog box prompts you to enter a report template name.

3. Select **OK** to open the **Report Wizard** dialog. In the **Set Filter** page, either select **Add** to add criteria to the **Criteria List** or select an existing criteria and then select **Edit** to renew the restricted condition. Choose a criteria relation by selecting either **Satisfy all criteria** or **Satisfy any criteria**.

   NOTE: The report can contain several criteria that work together with the selected criteria relation. Either option can be used to generate a report, or you can define a report without any criteria to include all devices and tasks.

4. Select **Choose Columns** to select the columns to display in the report, and then select **Next**.

   NOTE: The **Next** button is disabled until you select at least one column. For column values with multiple records, the subcolumns are combined into a single row with comments.

5. Optionally, select **Summary** to see a summary of the report. Then, select **Next**.

6. Select **Finish**. A prompt asks if you would like to preview the report.

Editing a report

To edit an existing report:

1. In HPDM Console, select **File**, and then select **Manage Report**.

2. From the **Report List**, select a report and then select **Edit**.

3. To edit the report's filter, use the options under **Set Filter**. To edit the report's columns, use the options under **Choose Columns**. To see a summary, select **Summary**.

4. After editing, select **Finish**. A prompt asks if you would like to preview the report.

Deleting a report

To delete a report:

1. In HPDM Console, select **File**, and then select **Manage Report**.

2. From the **Report List**, select a report and then select **Delete**.

3. In the pop-up window, select **Yes**.

Generating a report preview

To generate report preview using an existing report:

1. In HPDM Console, select **File**, and then select **Manage Report**.

2. Select a report from the list, and then select **Generate Report Preview**.

3. In the resulting window, select either **Export selected** or **Export all**.

10 HP Update Center

The HP Update Center allows you to leverage software components from the HP FTP server for use as payload.

IMPORTANT: This feature requires Internet access. If the system running HPDM Console or HPDM Master Repository Controller cannot access the Internet directly, you must first configure proxy settings. See for more information.

You can use the HP Update Center to generate task templates. The following software component types are available:

- Operating system images—Generate **_Deploy Image** templates

- Applications—Generate **_File and Registry** templates

Generating task templates

To use the HP Update Center to generate task templates:

1. In HPDM Console, select **Template**, select **Import**, and then select **HP Update Center**.

2. Select an item, and then select the **Generate Template** button.

   TIP: You can use the **Search** function to filter the components.

   NOTE: If HPDM Console or HPDM Master Repository Controller does not have direct access to the HP FTP server, select the **Proxy Settings** link to configure proxy settings.

   Once set, the proxy settings are stored in the HPDM database. HPDM Master Repository Controller and all instances of HPDM Console use the same proxy settings when connecting to the HP FTP server.

3. The Package Description Editor dialog shows the default information about the software component. You can use the default information or modify it, and then select the **Generate** button.

   NOTE: If you select the **Thin Client Models** field, a dialog allows you to select thin client models.

4. Select one or more operating systems to generate a template for, and then select **OK**. Each generated template is added to the Task Templates list for the appropriate operating system, but the template is invalid until the software component transfer from the HP FTP server to the HPDM Master Repository is complete.

   NOTE: If you selected more than one item to generate the template, those download requests are queued instead of simultaneous.

5. After the transfer completes successfully, the template becomes valid. You can then send the generated template to the specified device.

Configuring HP Update Center proxy settings

1. In HPDM Console, select **Tools**, and then select **Configuration**.

2. In the **Configuration Management** window, select the **HP Update Center Proxy** page.

3. Select one of the following options:

- **Use automatic configuration script**—Use this option to specify the path to a proxy settings auto-configuration file.

- **Use manual configuration**—Use this option to manually specify proxy settings.

4. Select **Test** if you want to test the proxy settings.

5. Select **OK**.

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

11 HPDM Server Backup and Restore Tool

HPDM Server Backup and Restore Tool allows you to back up and restore the files and database from HPDM Server, including the following items:

- Database schema and data
- The following subfolders under the HPDM root folder:
    - `\Server\task`
    - `\Server\template`
    - `\Server\template_plugins`

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

- This tool requires the credentials of a user account that has the database owner privilege.
- HPDM Server and HPDM Server Backup and Restore Tool must be from the same version of HPDM.

To open HPDM Server Backup and Restore Tool:

▲ Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Tools**, and then select **HPDM Server Backup and Restore Tool**.

☆ **TIP:** In Windows Server 2012, you can also open HPDM Server Backup and Restore Tool by selecting its tile on the Start screen.

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

Field	Description
Database Type	Displays the database type, either PostgreSQL or MS SQL Server (cannot be edited)
Host	Displays the hostname or IP address of HPDM Server (cannot be edited)
Port	Displays the database's listening port (cannot be edited)
Database	Displays the database name (cannot be edited)
Authentication	Allows the user to select the authentication type, depending on the database type, as follows: • PostgreSQL—**Database Authentication** • MS SQL Server—**Database Authentication** or **Windows Authentication**
Username	Allows the user to enter the username for an account that has the database owner privilege
Password	Allows the user to enter the password for an account that has the database owner privilege
Backup Folder	Allows the user to specify an already-existing folder in which the backups will be stored

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

Backing up HPDM Server

To back up HPDM Server:

1. In HPDM Server Backup and Restore Tool, select the authentication type and enter the credentials of a user account that has the database owner privilege.

2. Specify an already-existing folder in which the backup will be stored.

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

3. Select the **Back up** button.

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

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

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

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

To back up HPDM Server silently, run `br.cmd` on the command line using the following syntax:

▲ `br.cmd -withoutUI "-backupfolder=<path>"`

   NOTE: Replace `<path>` with the path of an existing folder in the file system, like the following example:

   `br.cmd -withoutUI "-backupfolder=c:\backup`

   Each backup creates a new subfolder named with the date and time of the backup.

Restoring HPDM Server

To restore HPDM Server:

1. In HPDM Server Backup and Restore Tool, select the authentication type and enter the credentials of a user account that has the database owner privilege.

2. Specify the folder of an existing backup (such as `DMBackup20121107145359`).

3. Select the **Restore** button.

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

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

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

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

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

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

12 HPDM Port Check Tool

HPDM Port Check Tool allows you to check network and service connectivity and firewall port allowance between different components of HPDM. The tool is located at the following path:

`<HPDM root folder>\Console\bin\HPDMPortCheck`

For quick access to that folder, do the following:

▲ Select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Tools**, and then select **HPDM Port Check Tool**.

To check a particular line of communication between HPDM components, copy the `HPDMPortCheck` folder to the side that initiates the connection, and then run the tool using Command Prompt. For example, to check if HPDM Gateway is reachable from HPDM Agent on a particular device, copy the folder to that device.

The command line syntax is as follows:

`HPDMPortCheck <target> [<flags>]`

The target can be a hostname or IP address, and valid flags are described in the following table. If no flags are specified, all ports in the following table are checked.

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

See the following examples.

To check if HPDM Gateway on a server with an IP address of 192.168.1.1 is reachable from HPDM Agent on a particular device, run the tool on that device and execute the following command:

`HPDMPortCheck 192.168.1.1 -g`

To check if HPDM Agent on a device with an IP address of 192.168.1.100 is reachable from HPDM Gateway, run the tool on the server hosting HPDM Gateway and execute the following command:

`HPDMPortCheck 192.168.1.100 -a`

To check the ports of HPDM Gateway, HPDM Server, and HPDM Master Repository Controller if all are hosted on a single server with an IP address of 192.168.1.1, run the tool from any device managed by HPDM and execute the following command:

`HPDMPortCheck 192.168.1.1 -gsm`

For more information about specific ports, see .

13 HPDM Archive Tool

HPDM Archive Tool allows you to archive outdated tasks and logs from both the HPDM database and the file system of the server hosting HPDM Server. This is a good solution if you have restricted disk space.

To use HPDM Archive Tool:

1. In Windows, select **Start**, select **All Programs**, select **HP**, select **HP Device Manager**, select **HP Device Manager Tools**, and then select **HPDM Archive Tool**.

2. On the command line, enter the following:

   ```
   archive.cmd –config:archive.conf
   ```

3. You can change the configuration of `archive.conf` under `\Server\conf`. See the following default configuration:

   - Type—By default, the **Archive** option deletes tasks and archives database tables and task files. Select **Delete** to delete tasks without archiving any files.

   - Tasks—By default, tasks over three months old are outdated. The value of an outdated month must be a natural number. All dates must be in the same format as the configuration file.

   - Archive folder—By default, the folder where archived task data is stored is `C:\HPDM_Archived`.

   📝 **NOTE:** If you change this configuration, follow the format instructions to prevent failure or errors. For example, if you include multiple Type items, only the final one is used for the configuration.

4. Under `\Server\logs`, there is the archive tool log: `hpdm-archive.log`. This shows the process information.

To use Task Scheduler in Windows to schedule HPDM Archive Tool:

1. In Windows, select **Start**, select **Control Panel**, select **System and Security**, select **Administrative Tools**, and then select **Schedule tasks**.

2. Select **Action**.

3. For **Program/script**, enter the full path to `\Server\bin\archive.cmd`, like in the following example:

   ```
   C:\Program Files\HP\HP Device Manager\Server\bin\archive.cmd
   ```

4. For **Add arguments**, enter the following:

   ```
   -config:archive.conf
   ```

5. For **Start in**, enter the full path to `\Server\bin`, like in the following example:

   ```
   C:\Program Files\HP\HP Device Manager\Server\bin
   ```

6. Select **Create Basic Task**, and then schedule the task.

14 Grouping tool

Using a custom script and the HPDM Agent-side tool **groupingtoolex**, you can remotely collect custom data from the thin client to assign to grouping keys P1–P6 and MG. HPDM Agent automatically sends the new properties to HPDM Server so they can be used in HPDM Console.

Using groupingtoolex commands in a custom script

Use the following command in a custom script to invoke groupingtoolex:

```
groupingtoolex <command>
```

The following table lists the valid commands (replace <key> with P1, P2 … P6, or MG).

Command	Description
`set <key> <value>`	Sets a grouping property, overriding the original one
`unset <key>`	Removes a grouping property

NOTE: The file extendedgp.ini is generated by the tool when updating grouping properties. You should not modify it.

Example commands

- Set P1 as an empty string:

  ```
  groupingtoolex set P1 ""
  ```

- Set MG as a string:

  ```
  groupingtoolex set MG "China/Shanghai"
  ```

- Remove P1:

  ```
  groupingtoolex unset P1
  ```

  NOTE: HPDM Agent can still get a P1 value via DHCP or registry.

- Remove all grouping properties:

  ```
  groupingtoolex unset
  ```

Invoking a custom script periodically

In Windows, you can use the **schtasks** tool to create periodic tasks to invoke a custom script:

```
schtasks /create /tn <task name> /tr <script file> /sc hourly /ru
SYSTEM /rp <password>
```

For example:

```
schtasks /create /tn DailyUpdateNIC /tr UpdateNIC.bat /sc hourly /ru
SYSTEM /rp MyPassword
```

In HP ThinPro, you can use the **crontab** command to create a periodic task.

Example procedure

The following example describes how to group devices by NIC card:

1. Remotely execute a script on the thin client that retrieves the NIC card type and assigns it to grouping key (P3 for this example).

2. In HPDM Console, select **Group by**, and then select **Edit scheme**.

3. In the **Edit Grouping Schemes** dialog box, select **Add**, enter `NIC Type` (or any custom name) for the grouping scheme name, and then select **OK**.

4. Select extension properties 1–3, select **Add**, and then select **OK**.

5. In HPDM Console, select **Group by**, select **Dynamic Group**, and then select **NIC Type**.

   Devices are now grouped by NIC type, such as BNC.

   NOTE: It might take some time for the new grouping properties to display in HPDM Console after being sent by HPDM Agent to HPDM Server. If you can't see the change in HPDM Console after some time, try reducing the **Pull Interval** setting in HPDM Agent on the device side, or try restarting the thin client.

15 HPDM Agent polling and error logging

HPDM Agent polling

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

You can use either of the following methods to change HPDM Agent polling settings:

- Use the HPDM Gateway Configuration window, which can be opened via the HPDM Gateway notification icon.

- Send a Configure HPDM Gateway task via HPDM Console.

Error logging

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

HPDM Agent logging

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

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

HPDM Gateway logging

Level	Description
TRACE	Some trace logs; for example, number of HPDM Agent instances
DEBUG	Internal debug logging
INFO	Log of some report content
WARN	Low-level error; for example, HPDM Gateway failed to connect to Console/Server at this time, maybe Server is not ready, but HPDM Gateway will retry later
ERROR	Significant errors
FATAL	High-level error; the error will usually prevent HPDM Gateway from running normally

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

- Use the HPDM Gateway Configuration window, which can be opened via the HPDM Gateway notification icon.
- Send a Configure HPDM Gateway task via HPDM Console.

HPDM Server and HPDM Console logging

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

To change the logging level of HPDM Server:

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

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

To change the logging level of HPDM Console:

▲ Change the value of `hpdm.log.level` in the file `/Console/conf/console.conf`, which is located at `<program data folder>/HP/HP Device Manager`.

☼ **TIP:** `<program data folder>` is either `C:\ProgramData` or `C:\Documents and Settings\All Users\Application Data`, depending on the operating system.

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

HPDM Master Repository Controller logging

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

To change the logging level of HPDM Master Repository Controller:

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

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

A   Task template reference

File and Registry

Template	Description
_File and Registry	This template enables you to create a sequence using these sub-templates: • Set a registry key. • Capture a file from a device. • Deploy a file to a device. • Execute a command on a device. • Delete files on a device. • Pause a sequence. • Add or remove a program record on a device. • Execute a script on a device.
_Get Registry	This template enables you to upload one or more keys from a device's registry.

Agent

Template	Description
_Configure Agent	This template enables you to configure HPDM Agent on the target device. **NOTE:** You can no longer set the current HPDM Gateway by typing 'cur-gateway, back-gateway' in the **Backup HPDM Gateway** field.
_Configure Task Deferment	This template enables you to configure task deferment settings on target devices.
_Update Agent	This template updates HPDM Agent on the target devices to the version stored in your repository. The payload is synchronized to the mapped repository automatically before the task is sent to the target devices.

Connections

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

Imaging

Template	Description
_Capture Image	This template, which can be sent to only one device at a time, captures an image from the target device and uploads it to the HPDM Master Repository. It also creates a new Deploy Image template.
_Update Firmware	This template updates the firmware of PCoIP zero clients. You need to import a firmware file to generate this template.

Operations

Template	Description
_Factory Reset	This template resets the targeted devices to their original configuration. The effects of this differ according to the operating system of the device. The reset to **Current Profile** option is unique to the HP ThinPro operating system.
_Get Asset Information	This template extracts a full asset report from the targeted devices.
_Reboot Device	This template restarts the targeted devices. A warning message displays on the devices' screen for 15 seconds before the restart actually takes place.
_Reverse Shadow Device	This template causes HPDM Agent on a target device to connect to the VNC viewer bundled with HPDM Console by SSL tunnel. This template is not available for the HPCE thin clients.
_Send Message	This template sends a customized message to targeted devices. This template is not available for HP ThinPro thin clients.
_Execute Cached Tasks	This template executes all cached tasks on the target devices.
_Clear Cached Tasks	This template removes all cached tasks on the target devices. The status of each cached task changes to "failed."
_Shadow Device	This template causes the VNC viewer bundled with HPDM Console to connect to the VNC service on a targeted device via an SSL tunnel.
_Shutdown Device	This template shuts down the targeted devices. A warning message displays on the devices' screen for 15 seconds before the restart actually takes place.
_Start Resource Monitor	This template starts the Resource Monitor for the target device. This template can only be sent to a single device at a time and is not available for HP ThinPro thin clients. When this template is sent to a device successfully, a Resource Monitor dialog pops up. You can monitor Process, Performance, and Network Disk information.
_Wake Up Device	This template causes the HPDM Gateway associated with the targeted devices to send them a Wake On LAN message. The Wake device works not only for devices in the same subnet with HPDM Gateway, but also for devices that are not in the same subnet of HPDM Gateway, if the subnet has at least one online HPDM Agent. We can wake up devices behind NAT, if the subnet has at least one online HPDM Agent. During timeout, HPDM Gateway reports the unfinished part as failure.

Settings

Template	Description
_Apply Settings	This template enables you to create a set of custom settings and deploy them to one or more devices.
_Capture Profile	This template captures a profile from a device running HP ThinPro 5.
_Capture Snapshot List	This template captures a snapshot list from a device running HP ThinPro 5.
_Capture Write Filter Exclusion List	This template captures the FBWF/UWF exclusion list from a device running a Windows operating system with FBWF or UWF.
_Clone Settings	This template enables you to copy a selection of custom settings from one device and deploy them to other devices.
_Deploy Profile	This template is used to configure a profile and deploy it to devices running HP Smart Zero Core or HP ThinPro 5.
_Deploy Write Filter Exclusion List	This template deploys the write filter exclusion list to devices running a Windows operating system with FBWF or UWF.
_Enroll Certificate With SCEP	This template enables you to enroll certificates with SCEP on normal thin clients.
_Hostname and IP	This template enables you to change the hostname and IP address of one or more devices. 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.
_Manage Snapshot	This template manages snapshots on devices running HP ThinPro 5.
_Set Domain	This template allows devices to join a domain or a workgroup.
_Set OS Configuration	This template switches the target device's operating system configuration on devices running HP ThinPro 5. **NOTE:** This template does not set the default connection if switching to Smart Zero. You can use a connection template to implement that change.
_Set Password	This template enables you to set a password for one or more users on one or more devices. You can select the **Hide password** check box to hide the password, or clear the check box it to show the password. **NOTE:** This template is not available for thin clients running HP Smart Zero Core.
_Take TPM Ownership	This template enables/activates TPM and sets the TPM owner password and BIOS setup password to take the TPM ownership of the selected devices.
_Write Filter Settings	This template enables you to change the Write Filter settings for a device.

Template Sequence

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

B   Port reference

HPDM Console ports (inbound)

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

HPDM Console ports (outbound)

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

Receiver port	Sender	Receiver	Protocol	Purpose
1099	HPDM Console	HPDM Server	TCP	Allows HPDM Console to query the RMI Registry
5500	SSL VNC Proxy (bundled with HPDM Console)	VNC Viewer (bundled with HPDM Console)	TCP (loopback)	VNC Viewer in Listen Mode (reverse VNC)
5900	VNC Viewer (bundled with HPDM Console)	SSL VNC Proxy (bundled with HPDM Console)	TCP (loopback)	VNC Shadow
40002	HPDM Console	HPDM Server	TCP	Allows HPDM Console to call remote objects from HPDM Server via RMI
40004	SSL VNC Proxy (bundled with HPDM Console)	SSL VNC Proxy (bundled with HPDM Agent)	TCP	Port for SSL VNC connection

HPDM Server ports (inbound)

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

HPDM Server ports (outbound)

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

HPDM Gateway ports (inbound)

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

HPDM Gateway ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Gateway	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	HPDM Gateway	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
68	HPDM PXE Server (bundled with HPDM Gateway)	HPDM Imaging Mini Linux Tool (client-side)	UDP	PXE bootstrap
137	HPDM Gateway	NetBIOS Name Service	UDP	Allows NetBIOS Name Resolution
138	HPDM Gateway	NetBIOS Datagram Service	UDP	Allows NetBIOS Datagram transmission and reception
139	HPDM Gateway	NetBIOS Session Service	TCP	Allows NetBIOS Session Services connections
443	HPDM Gateway	HPDM Embedded HTTPS Server	TCP	This is the default port for HTTPS (used for repositories). HTTPS ports can be configured via HPDM Console. If you do not use the default port, configure the firewall appropriately.

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

HPDM Agent ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
68	DHCP Server	HPDM Agent	UDP	Receive replies for DHCP options
68	HPDM PXE Server (bundled with HPDM Gateway)	HPDM Imaging Mini Linux Tool (client-side)	UDP	PXE bootstrap
5500	VNC Server on the thin client Windows: TightVNC (bundled with HPDM Agent) HP ThinPro: X11VNC (bundled with platform)	SSL VNC Proxy (bundled with HPDM Agent)	TCP (loopback)	SSL VNC Proxy in Listen Mode (reverse VNC)
5900	SSL VNC Proxy (bundled with HPDM Agent)	VNC Server on the thin client Windows: TightVNC (bundled with HPDM Agent) HP ThinPro: X11VNC (bundled with platform)	TCP (loopback)	VNC Shadow
40001	HPDM Gateway	HPDM Agent	TCP	Allows HPDM Gateway to send tasks to HPDM Agent

Receiver port	Sender	Receiver	Protocol	Purpose
40001	HPDM Gateway	HPDM Agent	UDP	Allows HPDM Agent to receive replies of broadcasting from HPDM Gateway
40004	SSL VNC Proxy (bundled with HPDM Console)	SSL VNC Proxy (bundled with HPDM Agent)	TCP	SSL VNC Proxy in Listen Mode (reverse VNC)

HPDM Agent ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Agent	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	HPDM Agent	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
67	PXE client (client-side)	HPDM PXE server (bundled with HPDM Gateway)	UDP	PXE bootstrap
67	HPDM Agent	DHCP server	UDP	Allows HPDM Agent to send DHCP option requests
69	PXE client (client-side)	HPDM PXE server (bundled with HPDM Gateway)	UDP	TFTP (Trivial File Transfer Protocol)
137	HPDM Agent	NetBIOS Name Service	UDP	Allows NetBIOS Name Resolution
138	HPDM Agent	NetBIOS Datagram Service	UDP	Allows NetBIOS Datagram transmission and reception
139	HPDM Agent	NetBIOS Session Service	TCP	Allows NetBIOS Session Services connections
443	HPDM Agent	HPDM Embedded HTTPS Server	TCP	This is the default port for HTTPS (used for repositories). HTTPS ports can be configured via HPDM Console. If you do not use the default port, configure the firewall appropriately.
445	HPDM Agent	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
5500	VNC Server on the thin client Windows: TightVNC (bundled with HPDM Agent) HP ThinPro: X11VNC (bundled with platform)	SSL VNC Proxy (bundled with HPDM Agent)	TCP (loopback)	SSL VNC Proxy in Listen Mode (reverse VNC)
5900	SSL VNC Proxy (bundled with HPDM Agent)	VNC Server on the thin client	TCP (loopback)	VNC Shadow

Receiver port	Sender	Receiver	Protocol	Purpose
		Windows: TightVNC (bundled with HPDM Agent)		
		HP ThinPro: X11VNC (bundled with platform)		
989 & 990	HPDM Agent	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.
4011	PXE client (client-side)	Proxy DHCP service (third-party software)	UDP	Proxy DHCP service (an alternative to port 67 if port 67 is not available)
40000	HPDM Agent	HPDM Gateway	UDP	Allows HPDM Agent to poll HPDM Gateway
40003	HPDM Agent	HPDM Gateway	TCP	Allows HPDM Agent to send reports to HPDM Gateway
40004	SSL VNC Proxy (bundled with HPDM Agent)	SSL VNC Proxy (bundled with HPDM Console)	TCP	SSL VNC Proxy in Listen Mode (reverse VNC)
40009	HPDM Agent	HPDM Server	TCP	Allows HPDM Agent to send resource information (CPU, RAM, disk I/O, network I/O, processes, etc.) to HPDM Server. HPDM Server sends a stop process command to HPDM Agent.

Repository ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
137	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	NetBIOS Name Service	UDP	For File and Printer Sharing to allow NetBIOS Name Resolution This is required for Shared Folder.

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

Repository ports (outbound)

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

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

Index