

HP Device Manager 5.0.14

Administrator's Guide



Table of contents

- Overview 4
 - Terminology 4
- Installation 5
 - Installation requirements 5
 - Product Support Matrix 8
 - Server preparation 9
 - Installation options 11
 - HPDM component installers 18
- Deployment 21
 - Overview 21
 - Typical Device Manager topology 21
 - Figure 3. Port usage in HPDM 27
 - Deployment factors 35
 - Ports between networks 41
 - Cloud deployments 46
 - HPDM HTTPS Repository 57
 - FTP Repositories 66
 - Mutual authentication between console and server 83
- Operation 84
 - Management Console 84
 - Device Discovery 100
 - Device Management 107
- Templates and rules 125
 - Task Templates 125
 - Templates folder 130
 - Task rules 131
- Tasks & Reports 134
 - Tasks 134
 - Cached tasks 142
 - Using cached updates 143

Task template reference.....	147
Connections	151
Imaging Devices	153
Reporting tools.....	174
Gateways and repositories	175
Page layout	175
Managing Repositories.....	176
Users and Groups.....	181
Page Layout.....	181
Users.....	182
Groups	183
Directory Services	184
Privilege System.....	191
Administrative Functions.....	196
Page Layout.....	196
Security Controls.....	196
HP Update Center.....	199
Configuration Center	201
Disaster Recovery	221
Troubleshooting.....	229
Log files	229
Collecting useful log information.....	231
Collect all HPDM component logs.....	234
General Troubleshooting	235
Database Issues	237
Network Issues.....	240
Duplicated Devices.....	246
Appendix A: Database Schema.....	247
Device Tables.....	247
Grouping Tables	253
Rule and filter Tables.....	254
Template Tables	258
Task Tables.....	259
Gateway Tables	262
Repository Tables	263
Privilege System Tables.....	264
Configuration Tables	267
Auditlog Tables.....	268
Deprecated tables.....	268

Accessing the database.....	268
Appendix B: Additional Configuration Options	270
Configuring HPDM Console	270
Configuring HPDM Server	270
Resetting Device State	273
Configuring HPDM Gateway.....	274
Configuring HPDM Agent.....	275
SQL Server Always-on Support.....	280
Appendix C: Configuring DHCP tags	280
Configuring a DHCP server for use with PXE	280
Configuring options 202 and 203	280
Configuring options for scopes (scope options)	281
Appendix D: Configuring a device to boot from PXE.....	281
Changing the boot order locally.....	281
Changing the boot order remotely	281
Appendix E: Configuring HPDM Master Repository Controller Certificate.....	284
Appendix F: Agent Device ID Filter Policy	287
Background.....	287
Mechanism.....	288
Usage.....	288

Overview

HP Device Manager (HPDM) is an enterprise-class application for managing and administering thin client devices on large- and small-scale networks. The system consists of the following major components:

- **HPDM Server**—The central management service, which monitors all states and controls all device management activities.
- **HPDM Gateway**—The software component that links the HPDM Server and HPDM Agents on each thin client.
- **HPDM Master Repository Controller**—The software component that manages the software payloads and package content in the Master Repository and synchronizes that content to other child repositories as requested by the HPDM Server.
- **HPDM HTTPS Repository**—The software component that provides the ability to set up an HPDM repository using the HTTPS protocol.
- **HPDM Console**—The software component that is the primary user interface for administrators, allowing the inventory and management of devices and other administrative activities.
- **HPDM Console Web Bridge**—The component that provides access to HPDM Console content through a web browser.
- **HPDM Configuration Center**—The graphical application used to configure settings of various HPDM components.
- **HPDM Agent**—The software component installed on each device to enable device management capabilities.

Terminology

The following table defines common terminology used when working with HP Device Manager.

Table 1. Common terminology

Term	Definition
HPDM Server	The central management service, which monitors all states and controls all device management activities.
HPDM Gateway	The software component that links the HPDM Server and HPDM Agents on each thin client.
HPDM Master Repository Controller	The software component that manages the software payloads and package content in the Master Repository and synchronizes that content to other child repositories as requested by the HPDM Server.
HPDM Master Repository	The primary storage location for payload contents (contains all payload files).
HPDM Child Repository	One or more optional secondary storage locations for payload contents used as distribution points within the management environment (each HPDM Child Repository can contain all or a subset of payload files).
HPDM HTTPS Repository	The software component that provides the ability to set up an HPDM repository using the HTTPS protocol.
HPDM Console	The software component that is the primary GUI for administrators, allowing the inventory and management of devices and other administrative activities.
HPDM Console Web Bridge	The software component that provides access to HPDM Console content through a web browser.
HPDM Configuration Center	The graphical application used to configure settings of various HPDM components.
HPDM Agent	The software component installed on each device to enable device management capabilities.
HPDM database	The storage location for the information that defines all the HPDM managed assets, such as devices, HPDM Gateway servers, repositories, task templates, and rules.
Device	A computing endpoint, such as an HP Thin Client that is managed by HPDM.

Package	A container object comprised of the description file and a folder which contains payload files.
Payload	Files, such as operating system images and software updates, that are stored in the HPDM Master Repository (and optionally one or more HPDM Child Repositories) and are distributed to managed devices via tasks.
PXE	Preboot eXecution Environment, a network server and accompanying protocol that enables devices to boot from a remote operating system image using the endpoint device network.
Rule	A declarative construct which allows for the automation of tasks based on certain matching criteria or system events.
Task	A scheduled action that is based on a task template and is used to apply 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 utility included with HPDM that allows you to archive retired devices, outdated tasks and logs from both the HPDM database and file system.
HPDM Automatic Device Importer	A specialized tool that only imports devices into the HPDM database.
HPDM Port Check Tool	A software utility included with HPDM that allows you to check network connectivity and firewall port permissions between different components of HPDM.
HPDM Server Backup and Restore Tool	A software utility included with HPDM that allows you to back up and restore database, templates, tasks, and the configuration files from an HPDM Server installation.

Installation

This section describes the installation requirements and procedures required to install HP Device Manager in various customer scenarios.

Installation requirements

Table 2. HPDM Server requirements

Component	Requirements
Operating system	Windows Server 2016 Windows Server 2019 Windows Server 2022
Third-party software	OpenJDK (bundled with installer) One of the following database management systems (DBMS): Microsoft® SQL Server 2016 or later PostgreSQL (bundled with installer)
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 4GB RAM (Recommend: 4 CPU cores and 6 GB RAM) 2 GB free disk space

Table 3. HPDM Gateway requirements

Component	Requirements
Operating system	Windows Server 2016

	Windows Server 2019 Windows Server 2022
Hardware	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 2 GB free disk space

Table 4. HPDM Master Repository Controller requirements

Component	Requirements
Operating system	Windows Server 2016 Windows Server 2019 Windows Server 2022
Hardware	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 4 GB free disk space NOTE: The above hardware is the minimum required for the Master Repository. If there will be many imaging or file-copying operations, then HP recommends using a more powerful system with additional free disk space.
Protocols	HTTPS, FTP, FTPS, SFTP, or SMB
Recommended third-party FTP servers	Apache HTTP Server (An embedded version of Apache HTTP Server is bundled with the installer.) FileZilla Microsoft Internet Information Server (IIS) freeSSHd

Table 5. HPDM HTTPS Repository requirements

Component	Requirements
Operating system	Windows Server 2016 Windows Server 2019 Windows Server 2022
Hardware	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 2 GB free disk space 7200 RPM disk NOTE: The above hardware is the minimum required for the Master Repository. If there will be many imaging or file-copying operations, then HP recommends using a more powerful system with additional free disk space.
Protocol	HTTPS

Table 6. HPDM Console requirements

Component	Requirements
-----------	--------------

Operating system	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11
Third-party software	OpenJDK (bundled with installer)
Hardware	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM (<u>Recommended: 4 CPU cores and 6 GB RAM</u>) 1 GB free disk space

Table 7. HPDM Console Web Bridge requirements

Component	Requirements
Operating system	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11
Prerequisite	HPDM Console
Hardware	Intel compatible 64-bit processor supporting 2 or more CPU cores 5 GB RAM (<u>Recommended: 4 CPU cores and 7 GB RAM</u>) (For 1 Console instance and Console Web Bridge server. Add 1 GB for each additional Console) 2 GB free disk space

Table 8. HPDM Configuration Center requirements

Component	Requirements
Operating system	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11
Hardware	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 1 GB free disk space

Table 9. Network requirements

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

Port requirements

See the **Port Usage** section for a list of standard and custom ports required.

Product Support Matrix

HPDM provides full support for all HP thin clients within EOL (end-of-life) + 3 years and partial support for all HP thin clients within EOL + 5 years. Each thin client should have a minimum of 10 MB of free disk space.

In the following matrix, full support (●) indicates that all existing and new features in HPDM 5.0 are supported. Partial support (○) indicates that not all task templates are available for a given device platform and operating system.

Table 10. Product support matrix

Thin client model	Windows 10 IoT Enterprise LTSC (64-bit)	Windows 10	Windows 11	Windows 11 IoT Enterprise LTSC 2024	HP ThinPro 8.1	HP ThinPro 8	HP ThinPro 7.2
HP t755 Thin Client	●			●	●		
HP t740 Thin Client	●				●	●	●
HP t730 Thin Client	●				●	●	●
HP Elite t660 Thin Client				●			
HP Elite t655 Thin Client	●			●	●	●	
HP t640 Thin Client	●				●	●	●
HP t638 Thin Client	●					●	●
HP t630 Thin Client	●				●	●	●
HP t628 Thin Client	●						●
HP Pro t550 Thin Client	●			●	●	●	
HP t540 Thin Client	●				●	●	●
HP t530 Thin Client	●				●	●	●
HP t430-R Thin Client	●				●	●	
HP t430 Thin Client	●					●	●
HP t420 Thin Client							●
HP t240 Thin Client							●
HP Elite mt645 G8 Mobile Thin Client	●			●	●		
HP Elite mt645 G7 Mobile Thin Client	●				●	●	

HP Pro mt440 G3 Mobile Thin Client	●	●	●	●
HP mt46 Mobile Thin Client	●		●	●
HP mt45 Mobile Thin Client	●		●	●
HP mt44 Mobile Thin Client	●			
HP mt32 Mobile Thin Client	●		●	●
HP mt31 Mobile Thin Client	●			
HP mt22 Mobile Thin Client	●		●	●
HP mt21 Mobile Thin Client	●		●	●
HP ThinPro PC Converter			○	○
Windows PC Converter	●	●		

Server preparation

This setup requires Windows Server 2016 or later running on either a physical or virtual machine. Allocate a minimum of 10 GB of storage for the operating system and the HPDM components. Full server recommendations are available in the **HPDM Server requirements** section.

This assumes that HPDM Server will use a standard installation without any additional services running.

This section focuses on the post-installation steps of installing HPDM onto Windows Server 2016. The example assumes a complete HPDM installation has already been performed on HPDM Server and that a user account for the FTP transactions has already been created.

Selecting a database management system

HPDM supports both PostgreSQL and Microsoft SQL Server databases. PostgreSQL is integrated in the HPDM installation package and can be used directly without extra installation or configuration. However, PostgreSQL within the HPDM installation package cannot be upgraded or replaced by a higher version as some files are customized by the HPDM installation. If you want to view the data in the PostgreSQL database, you need to install a third-party database admin tool such as pgAdmin or Navicat. If you choose to use Microsoft SQL Server with HPDM, you need to install the Microsoft SQL Server separately. PostgreSQL is a free database management system, while Microsoft SQL Server is a commercial database management system. For HPDM, there is no difference in capabilities or performance between the two database solutions.

Table 11. Database management system

	Microsoft SQL Server	PostgreSQL
Type	Commercial database	Free database
Authentication	Username-password authentication Windows authentication	Username-password authentication
Installation	User-defined installation Note: Interaction with the HPDM server is affected by network latency when installed on a different machine.	In HPDM server installation package
Upgrade	Support	Not support
Visualization tool	Built-in	Third-part tool
Port	1433 (Default)	40006 (Default)

Choosing repository protocols

HPDM supports the HTTPS, FTP/FTPS, SFTP, and SMBv2 (Shared Folder, Samba) as file transfer protocols. HTTPS protocol support is provided by the HPDM HTTPS Repository component, FTP family protocols are supported through third-party FTP servers, and

SMBv2 is provided through Windows operating system support. You can choose any single protocol or combination of protocols within a single repository. However, there are two limitations, as follows:

-
- SMBv2 must be selected for Windows non-cached file-based imaging.

If multiple protocols are used within a single repository, they should all point to the same folder location on the computer system.

Windows firewall settings

In Windows Server 2016, the built-in firewall service helps secure your server from network threats and is enabled by default. If you use the built-in Windows Firewall, you need to configure your settings so that the HPDM, HTTPS and FTP traffic can pass through the firewall. Note that you need to be logged on as Administrator or as a user that has administrator privileges to configure the firewall. If not logged on as Administrator, be sure to right-click **Start Menu** button, and then select **Command Prompt (Admin)**. This is required because User Account Control (UAC) in the Windows Server 2016 operating system prevents non-Administrator accounts access to the operating system firewall policy settings.

Firewall settings for HP Device Manager

The basic ports used by HPDM for management traffic between HPDM Server, HPDM Gateway, and HPDM Agent are in the range of 40000 to 40009, and 40012.

To configure the necessary exceptions:

1. Right-click **Start Menu** button, and then select **Command Prompt**. If not logged on as Administrator, be sure to select **Command Prompt (Admin)**.
 - To add an inbound rule to allow UDP traffic on port 40000, type the following command, and then press **Enter**:

```
netsh advfirewall firewall add rule name="HP Device Manager UDP IN" action=allow protocol=UDP dir=in localport=40000
```
 - To add an outbound rule to allow UDP traffic on port 40000, type the following command, and then press **Enter**:

```
netsh advfirewall firewall add rule name="HP Device Manager UDP OUT" action=allow protocol=UDP dir=out localport=40000
```
 - To add an inbound rule to allow TCP traffic on ports 40001 to 40009, and 40012, type the following command, and then press **Enter**:

```
netsh advfirewall firewall add rule name="HP Device Manager TCP IN" action=allow protocol=TCP dir=in localport=40001-40009,40012
```
 - To add an outbound rule to allow TCP traffic on ports 40001–40009, and 40012, type the following command, and then press **Enter**:

```
netsh advfirewall firewall add rule name="HP Device Manager TCP OUT" action=allow protocol=TCP dir=out localport=40001-40009,40012
```

These steps allow HPDM Server, HPDM Gateway and HPDM Agents to connect to each other. The ports used for HPDM traffic are open on the Windows Firewall. Other ports might be needed for other specific tasks. See the **Port Usage section** of this guide for a complete list of ports used by HPDM.

Firewall settings for HPDM HTTPS repository

The default port used by HPDM HTTPS Repository is 443. If you changed the listen port of HPDM HTTPS Repository via HPDM Configuration Center, be sure to replace 443 with the new port number in following command lines.

To configure the Windows Firewall setting for HPDM HTTPS Repository using the command line:

1. Right-click **Start Menu** button, and then select **Command Prompt**. If not logged on as Administrator, be sure to select **Command Prompt (Admin)**.
 - To add an inbound rule to allow TCP traffic on port 443, type the following command, and then press **Enter**:

```
netsh advfirewall firewall add rule name="HPDM HTTPS TCP IN" action=allow protocol=TCP dir=in localport=443
```
 - To add an outbound rule to allow TCP traffic on port 443, type the following command, and then press **Enter**:

```
netsh advfirewall firewall add rule name="HPDM HTTPS TCP OUT" action=allow protocol=TCP dir=out localport=443
```

Firewall settings for FTP Repositories

You must configure an exception for both the control channel (port 21) and the port range for the passive data channel. While it is easier to add these rules from the command line, you can also use the user interface for the Windows Firewall.

To configure the Windows Firewall setting for FTP using the command line:

1. Right-click **Start Menu button**, and then select **Command Prompt**. If not logged on as Administrator, be sure to select **Command Prompt (Admin)**.
2. To add an inbound rule for the command channel and to allow connections to port 21, type the following command, and then press **Enter**:

```
netsh advfirewall firewall add rule name="FTP (non-SSL)" action=allow protocol=TCP dir=in localport=21
```
3. Activate firewall application filter for FTP (aka Stateful FTP) that will dynamically open ports for data connections, type the following command, and then press **Enter**:

```
netsh advfirewall set global StatefulFtp enable
```
4. You do not have to enable the port range for the passive data channel in the windows firewall due to the FTP filter. For routers, you can manually configure the port changes in the routers' firewall.

Note:

For FTPS, enable the control channel (usually port 990) and the port range for the passive data channels. Disable the FTP filter, because FTPS data connections are encrypted, so standard firewalls cannot recognize the protocol.

Installation options

The HP Device Manager installer consists of Device Manager Component installers. Each component has its own standalone installer, and the HP Device Manager installer is the global application that installs all HPDM components.

Before installing HPDM, copy the installation file to the server. If a version prior to 5.0 of HPDM is installed, see [Upgrading a Previous Installation](#).

Server-side components

The server-side components of the system are installed using the HP Device Manager installer (`HP_Device_Manager-revision.exe`).

There are two setup types: Complete Setup and Custom Setup.

Complete setup

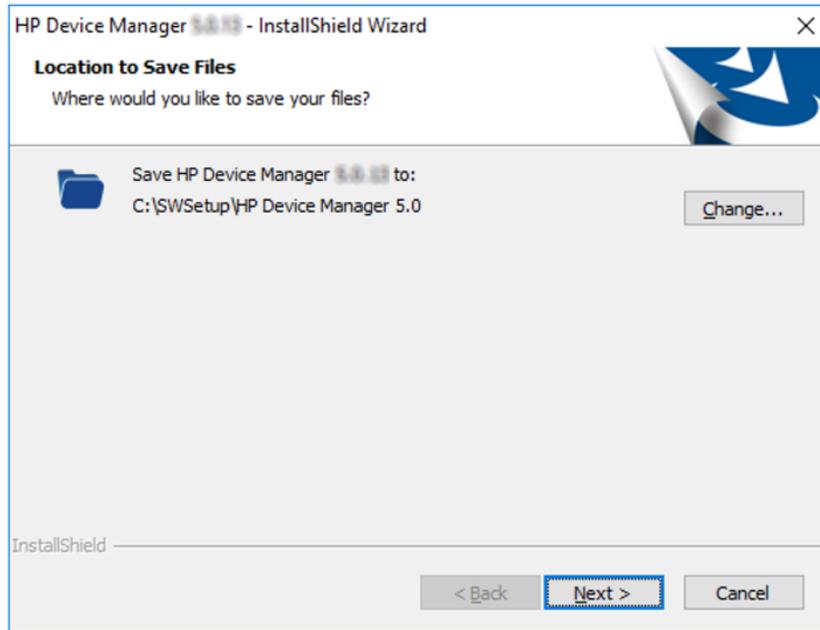
This process installs all HPDM server-side components. No configuration is necessary during installation. You can use most HPDM functions after installation, such as update agent, capture/deploy files, and so on.

The following lists provides the default settings for complete setup:

- HTTPS Repository is installed as the default repository server, and a random user and password are created during installation.
- A clean PostgreSQL database is created and initialized for HPDM Server if there is no database for the HPDM. A random password is created for the root user when initializing the database, which must be changed at first logon.
- HPDM Server uses the local HTTPS Repository as its master repository and automatically imports a randomly created user and password to the database.

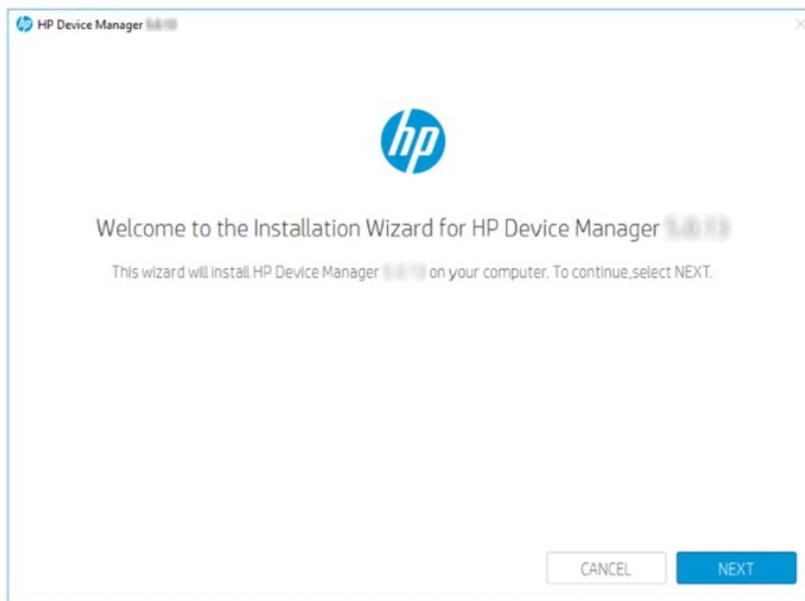
Custom setup

1. Select the HPDM setup file. If the User Account Control dialog is displayed, select **Yes**.
2. Select the **Location to Save Files**, and then select **Next**. The following image shows the location to save the extracted files from the installation package.

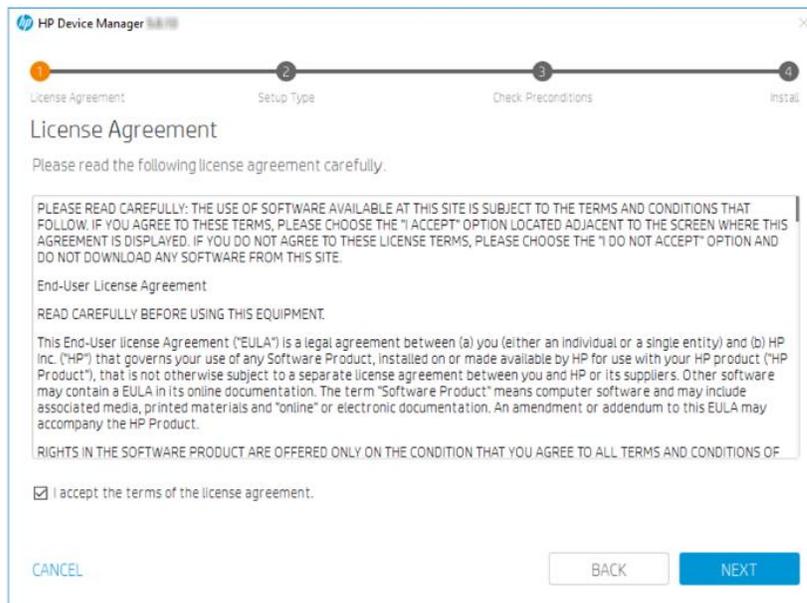


3. If the Overwrite Protection dialog is displayed when extracting files, select **Yes to All**.

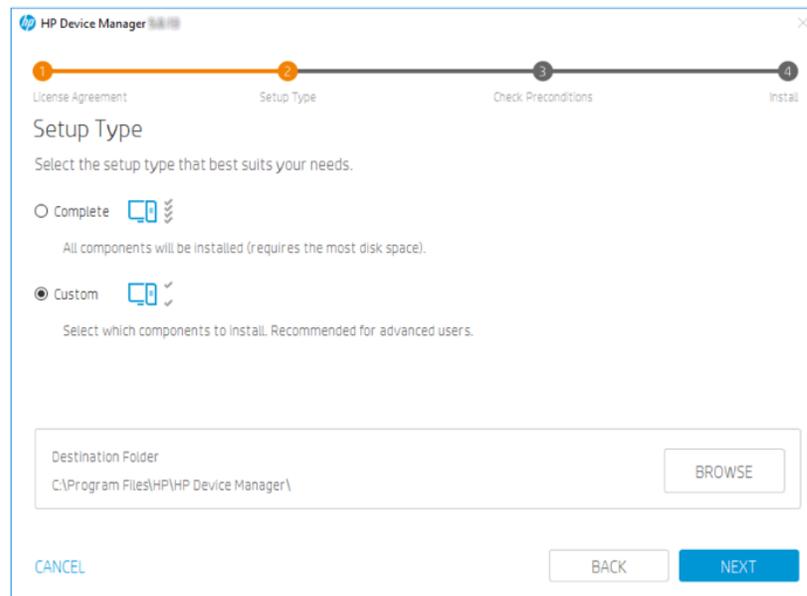
4. Select **Next**.



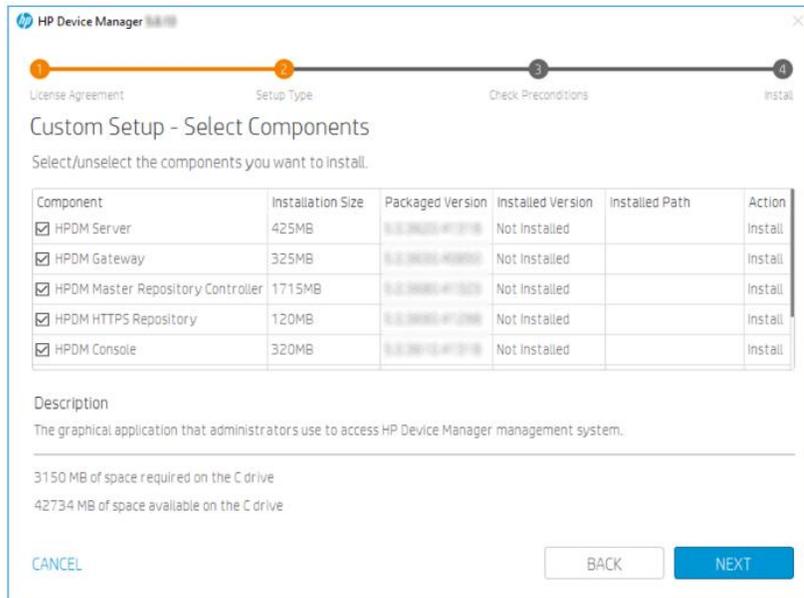
5. Select **I accept the terms of the license agreement**, and then select **Next**.



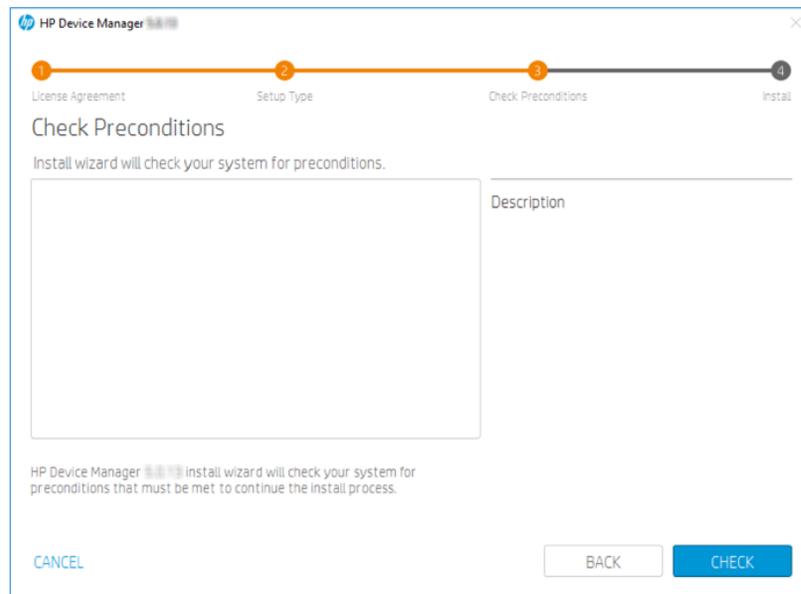
- Under **Setup Type**, select **Custom**, and then navigate to the installation path of HP Device Manager.



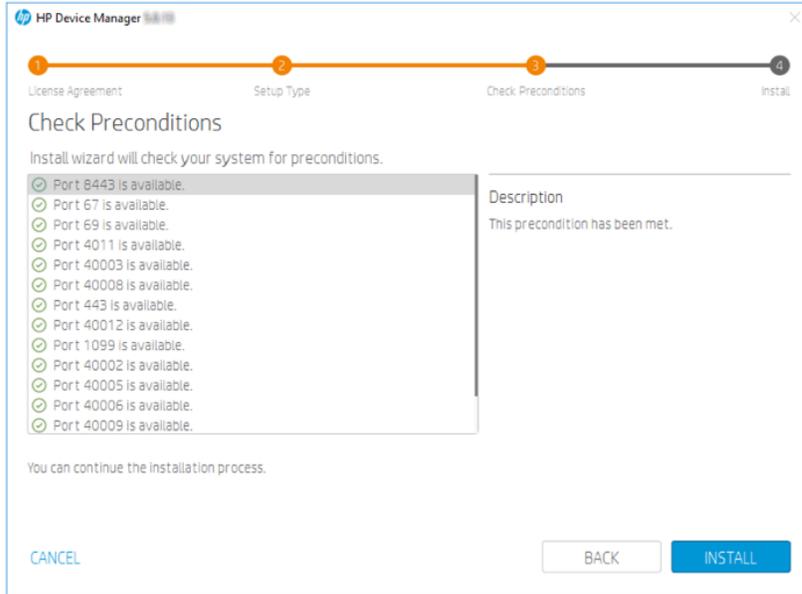
- Select the components you want to install, and then select **Next**. Note that the dependent components are selected automatically when you select a primary component. You cannot clear a primary component if a dependent component is selected and the dependent component depends on the primary component.



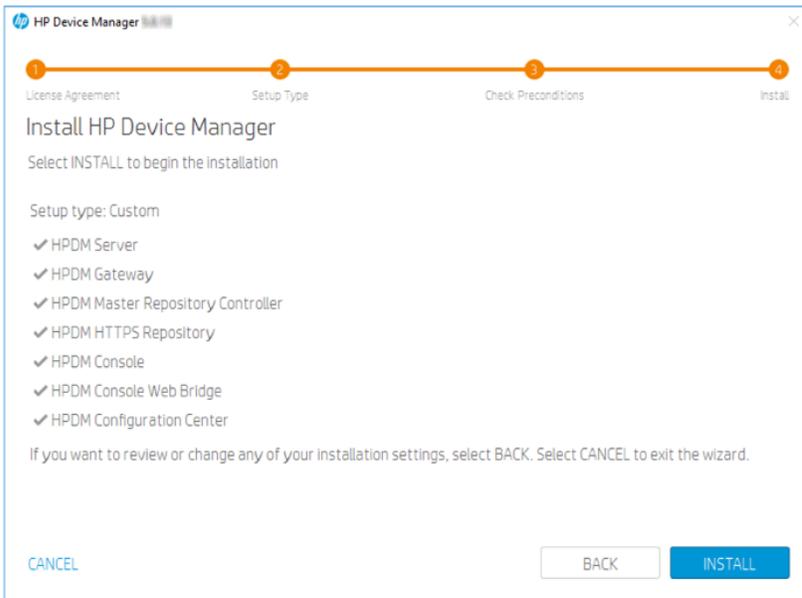
8. Select **Check** to check preconditions.



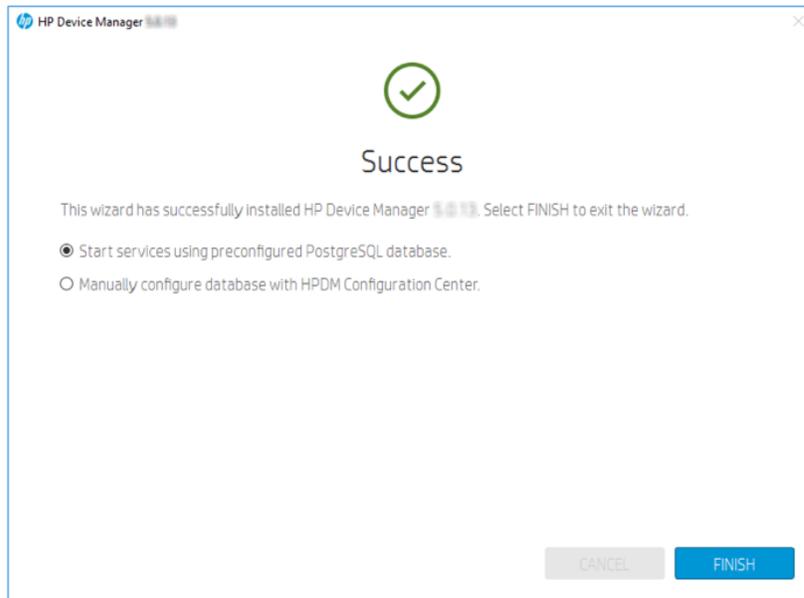
9. If all preconditions are met, select **Next**. If preconditions are not met, review the description, and resolve them manually. Select **Check** to continue.



10. View your installation settings summary, and then select **Install**.



11. When installation is complete, select **Finish**. If you want to use SQL Server database, select **Manually configure database with HPDM Configuration Center** to open HPDM Configuration Center. See the **HPDM Configuration Center** section to view how to configure HPDM components.



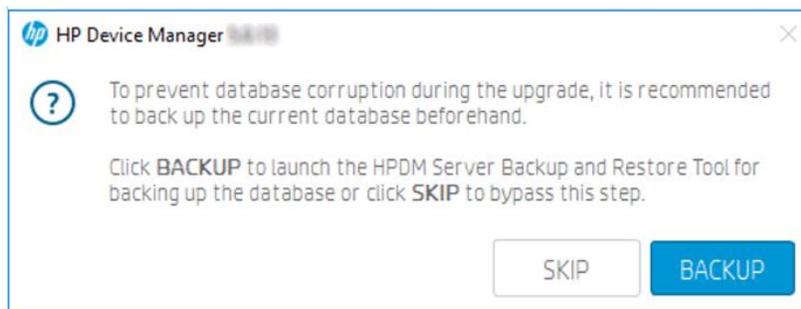
Note

- If the HPDM Server, HPDM Master Repository Controller, and HPDM HTTPS Repository are not installed on the same machine, reset the user account of HPDM HTTPS Repository and its password using HPDM Configuration Center.
 - If the HPDM Server and HPDM Console are not installed on the same machine, reset the password of HPDM root user using HPDM Configuration Center before logging into HPDM Console.
-

Updating an existing installation

There are two updating setup types: Upgrade Setup and Custom Setup. Upgrade Setup is used to upgrade all installed HPDM components directly. Custom Setup is used to upgrade installed components, as well as install new components. You can view detailed information of both components in the installer package and in the installed components. If you want to add new HPDM components into the current machine, use Custom Setup.

If the HPDM Server needs to be upgraded, a prompt dialog will ask the user to back up the database.

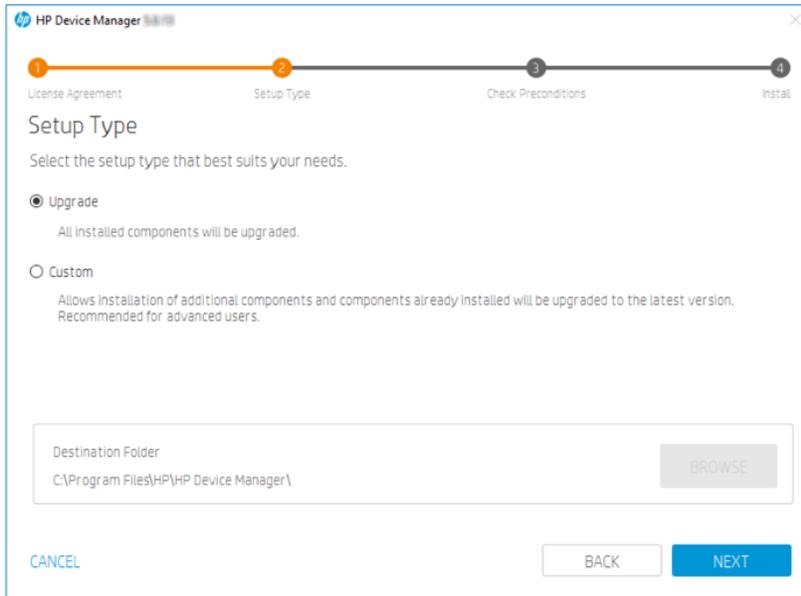


Note

The installation process doesn't restore the backup database automatically, you need to restore it manually if you met the database problem after the upgrade.

Upgrade

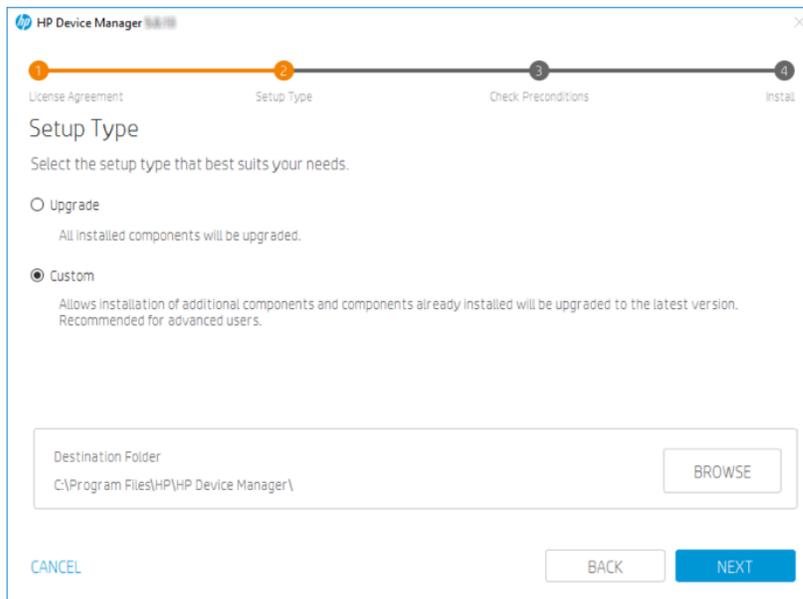
To upgrade all installed HPDM components, follow the procedure for a new installation until the Setup Type window, and then select **Upgrade**.



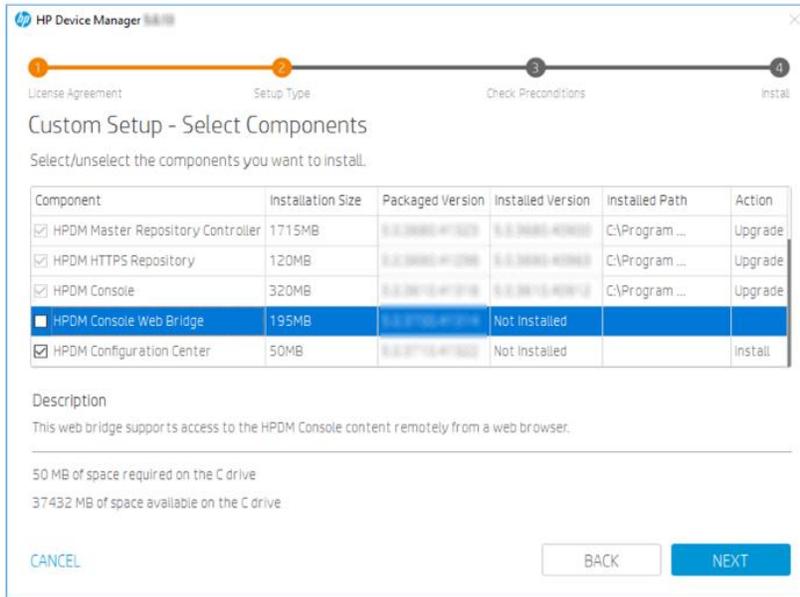
Custom setup

To perform a custom setup, follow the procedure for a new installation until the Setup Type window, and then use the following steps:

1. Select **Custom**, and then navigate to the destination folder. The installation location does not affect installed components.



2. To install new components or upgrade installed components, select the components to add, and then select **Next**.



Note

The HP Device Manager upgrade process upgrades all installed components at the same time. You cannot clear installed components on this page.

3. The following steps are same with the new installation.

Uninstalling HP Device Manager

To uninstall all installed HP Device Manager components:

1. If the HPDM Configuration Center is installed, run **Start > HP > Uninstall HP Device Manager**.

If the HPDM Configuration Center isn't installed, go to the HPDM installation location. By default, the location is "C:\SWSetup\HP Device Manager 5.0\". Then run the **uninstall.cmd** script as administrator. To run as administrator, right-click the file and select **Run as administrator**.

3. To uninstall an individual component:

- a. Go to **Control Panel > Programs and Features**.
- b. Select the component that you want to uninstall.

HPDM component installers

The HP Device Manager 5.0 installer is composed of individual component installers. Each component has a separate installer, and the HP Device Manager installer is a bootstrap application that launches individual component installers to install each component individually.

The HP Device Manager installer is composed of the following component installers:

- **HPDMServer.exe** – the component installer of HPDM Server
- **HPMDGateway.exe** – the component installer of HPDM Gateway
- **HPDMMasterRepositoryController.exe** – the component installer of HPDM Master Repository Controller
- **HPDMHTTPSRepository.exe** – the component installer of HPDM HTTPS Repository
- **HPDMConsole.exe** – the component installer of HPDM Console
- **HPDMConsoleWebBridge.exe** – the component installer of HPDM Console Web Bridge
- **HPDMConfigurationCenter.exe** – the component installer of HPDM Configuration Center

Preparation

Get the component installers

Only the HP Device Manger installer is available on the HP website. Component installers are available only after installing or extracting the HP Device Manager installer. All component installers are located at the location that you selected during HP Device manager installation. The default location is C:\SWSetup\HP Device Manager 5.0\.

Note

This location is not the installation path of HP Device Manager.

If you want only the component installers, you extract the HP Device Manager installer without installing.

To extract the HP Device Manager installer:

1. Run the HP Device Manager installer.
2. Select **Location to Save Files**, and then select **Next**.
3. After the Welcome to the install wizard for HP Device Manager 5.0 dialog is displayed, select **Cancel**.

Installing HPDM Component with component installer

Component installers support only silent installation - there is no user interface. You can install a component with the default installation path and configuration by selecting the component installer or using a command line. For detailed command line parameters, see following sections.

Note

Make sure the **Microsoft Visual C++ 2015-2022 Redistributable (x64)** is installed on the target machine before installing a component. The installer file is included with the HP Device Manager installer at the same location as the component installer and is named **VC_redist.x64.exe**.

If you want to configure an installed component, install HPDM Configuration Center after you install the component.

HPDM Server Component Installer

Installation command:

```
HPDMServer.exe /hide_progress /v"INSTALLDIR="C:\Program Files\HP\HP Device Manager\"  
START=1 ""
```

Parameters:

INSTALLDIR: The target installation path. The default path is C:\Program Files\HP\HP Device Manager.

START: Starts the HPDM Server service after installation. Values are 1 = start, 0 = do not start. The default is 1.

Note

An initial database is created but not configured when the HPDM Server service starts. In this scenario, a random password is created for the root user. Be sure to reset the password or recreate a new database via HPDM Configuration Center.

HPDM Gateway for Windows® Component Installer

Installation command:

```
HPDMGateway.exe /hide_progress /v"INSTALLDIR="C:\Program Files\HP\HP Device Manager\"  
START=1 ""
```

Parameters:

INSTALLDIR: The target installation path. The default installation path is C:\Program Files\HP\HP Device Manager.

START: Starts HPDM Gateway service after installation. Values are 1 = start, 0 = do not start. The default is 1.

HPDM Master Repository Controller Component Installer

Installation command:

```
HPDMMasterRepositoryController.exe /hide_progress /v"INSTALLDIR="C:\Program  
Files\HP\HP Device Manager\ ""
```

Parameters:

INSTALLDIR: The target installation path. The default installation path is C:\Program Files\HP\HP Device Manager.

Note

The default location of the repository is %ProgramData%\HP\HP Device Manager\HPDM. You can only change this path using HPDM Configuration Center.

HPDM HTTPS Repository Component Installer

Installation command:

```
HPDMHTTPSRepository.exe /hide_progress /v"PORT=443 INSTALLDIR=\"C:\Program Files\HP\HP Device Manager\""
```

Parameters:

PORT: The listening port of the HPDM HTTPS Repository service. The default value is 443.

INSTALLDIR: The target installation path. The default installation path is C:\Program Files\HP\HP Device Manager.

Note

If the HPDM Master Repository Controller is installed, the installation process sets the location of the repository as the root path of HTTPS Repository. Otherwise, the default root path is %ProgramData%\HP\HP Device Manager\HPDM.

A random user and password are created during installation. Be sure to reset them after installation using HPDM Configuration Center.

You can use this component installer to upgrade the older HPDM HTTPS Repository when no other HPDM component is installed. Select HPDMHTTPSRepository.exe or run the following command:

```
HPDMHTTPSRepository.exe /hide_progress
```

All configurations are restored after upgrading.

HPDM Console Component Installer

Installation command:

```
HPDMConsole.exe /hide_progress /v"INSTALLDIR=\"C:\Program Files\HP\HP Device Manager\""
```

Parameters:

INSTALLDIR: The target installation path. The default installation path is C:\Program Files\HP\HP Device Manager.

HPDM Console Web Bridge Component Installer

Installation command:

```
HPDMConsoleWebBridge.exe /hide_progress
```

Note

You can install this component only on the computer where HPDM Console is installed. Its installation path is same as the installed HPDM Console component. The installation process stops if it detects that the HPDM Console is not installed.

HPDM Configuration Center

Installation command:

```
HPDMConfigurationCenter.exe /hide_progress /v"INSTALLDIR=\"C:\Program Files\HP\HP Device Manager\""
```

Parameters:

INSTALLDIR: The target installation path. The default installation path is C:\Program Files\HP\HP Device Manager.

Note

You must install this component if you want to configure other components after installation.

Deployment

Overview

The following sections provide information for planning the setup and configuration of HP Device Manager (HPDM), including managing larger device deployments with HPDM, as well as tips to fine tune performance.

HPDM is divided into the following components:

- HPDM Console
- HPDM Server
- Database (Here it means MS SQL Server, PostgreSQL is taken as an inner part of Server)
- HPDM Gateway
- Master Repository
- Child Repository (not necessary)
- HPDM Agent (pre-installed on device)
- HPDM Console Web Bridge

Typical Device Manager topology

The following illustrations show the topology of a typical HPDM deployment.

Figure 1. Topology of a typical HPDM deployment

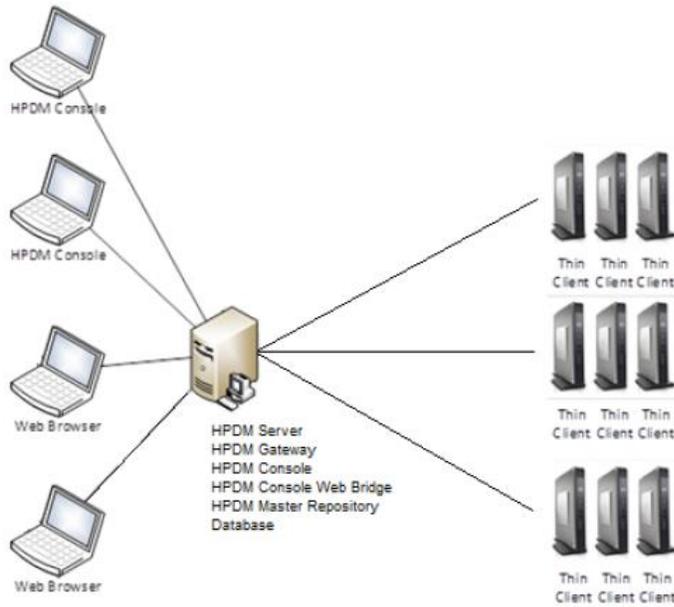
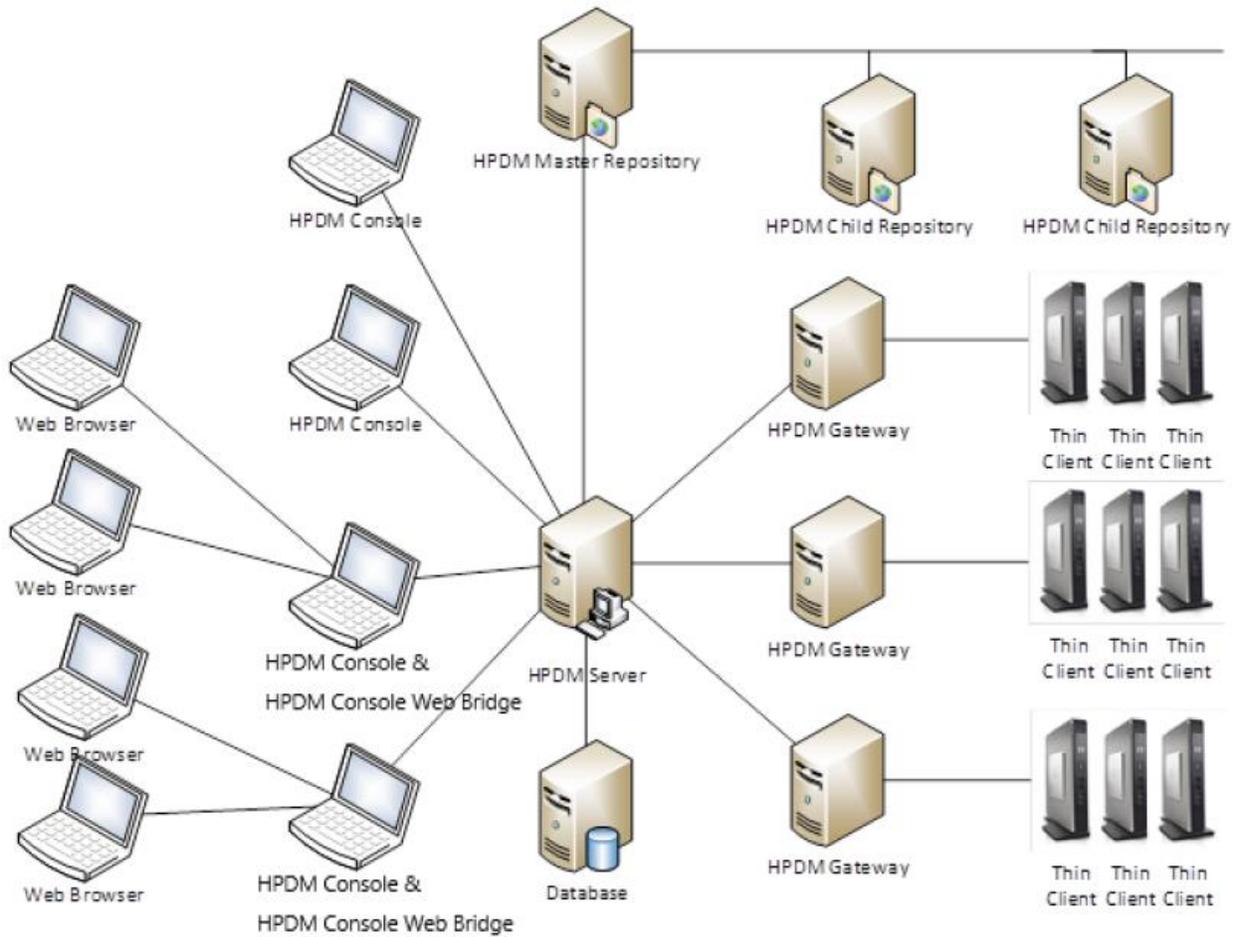


Figure 2. Topology of a typical HPDM deployment



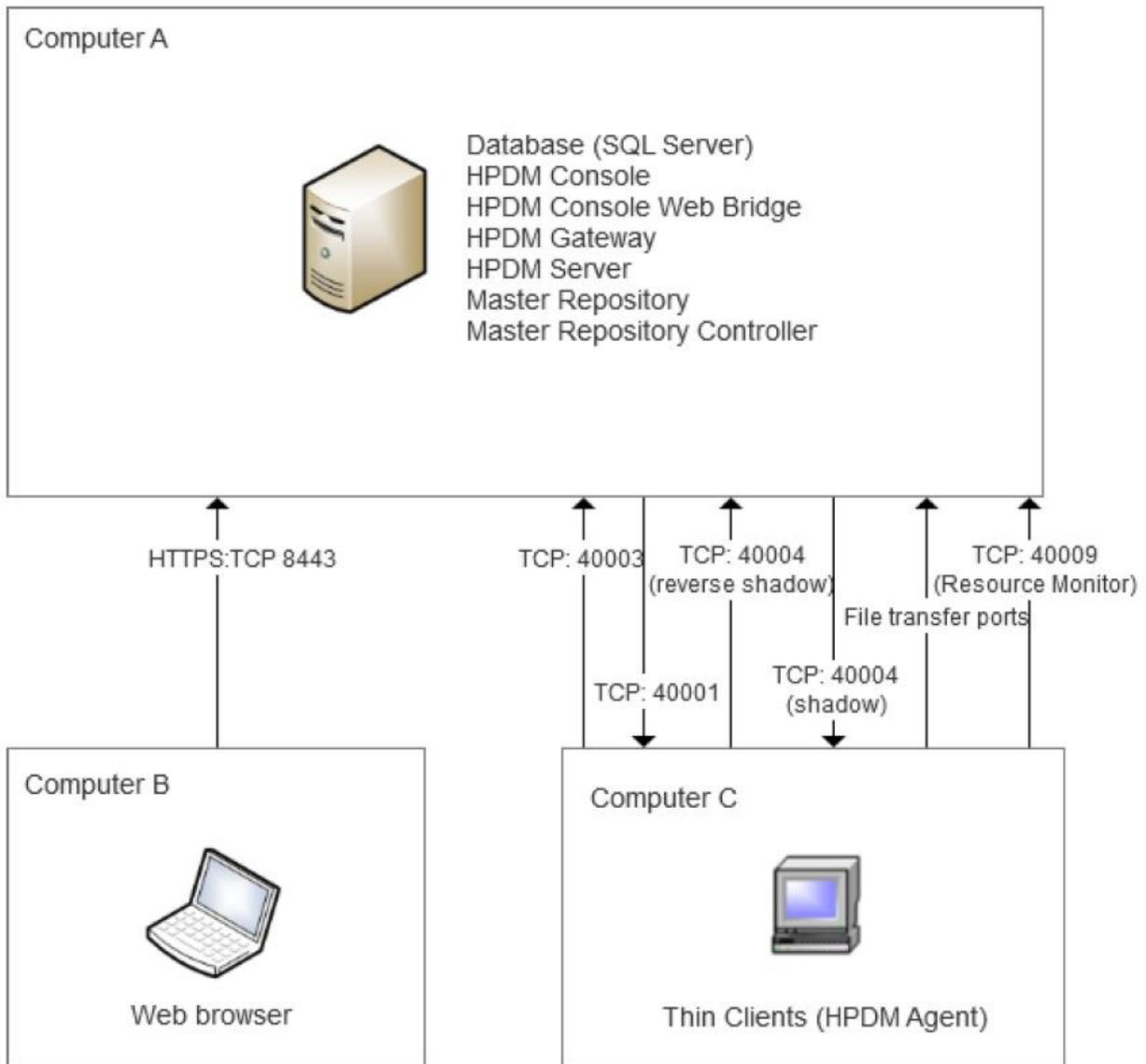
Note

If you want to generate templates using the HP Update Center, make sure that the HPDM Console and the Master Repository Controller can reach to HP File Server, either through direct connection or a proxy configuration.

Port usage

The following two scenarios shows two typical deployments with the enabled ports:

Scenario 1: All components are installed together



Firewall configuration:

Table 12. File Transfer ports

Protocol	TCP Port(s)	UDP Port(s)
FTP	20, 21	
FTPS	989, 990	
SFTP	22	
Shared Folder	139, 445	137, 138
HTTPS	443	

Note: Not all file transfer ports are essentials. They are enabled on demand. For more details, please refer to **Choosing repository protocols**.

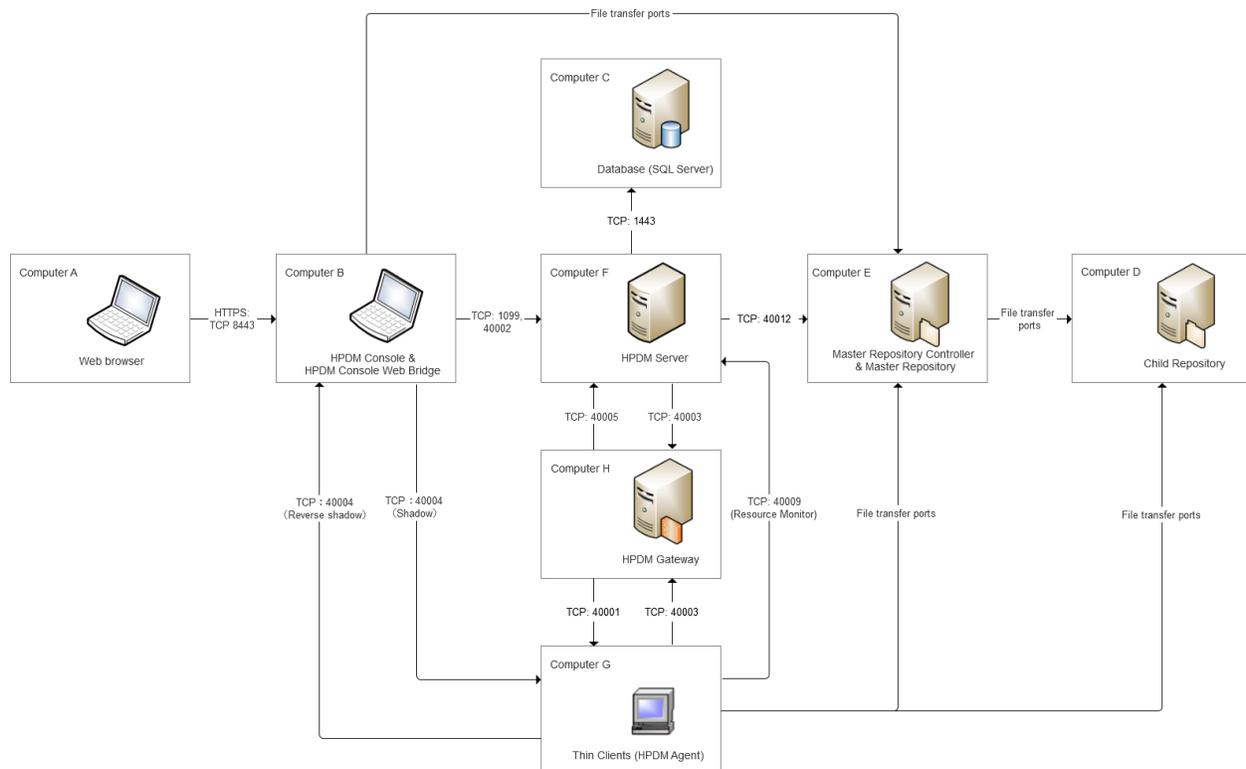
Table 13. Components installed on machines

Computer	Components
Computer A	HPDM Console & HPDM Console Web Bridge, HPDM server, HPDM Gateway, SQL Server, Master repository controller & Master repository
Computer B	Web Browser
Computer C	Thin Clients (HPDM Agent)

Table 14. Ports for each machine

Computer	Firewall	Ports	On-demand ports
Computer A	Inbound	8443, 40003, 40005, File transfer ports	40004(Reverse shadow) 40009(Resource monitor)
Computer A	Outbound	40001, 40003	40004(Shadow)
Computer B	Inbound	40003	
Computer B	Outbound	40001	
Computer B	Inbound	40001	40004(Shadow)
Computer B	Outbound	40003, File transfer ports	40009(Resource monitor), 40004(Reverse Shadow)

Scenario 2: All components are installed on different machines.



Firewall configuration:

Table 15. File Transfer ports

Protocol	TCP Port(s)	UDP Port(s)
FTP	20, 21	
FTPS	989, 990	
SFTP	22	
Shared Folder	139, 445	137, 138
HTTPS	443	

Note: Not all file transfer ports are essentials. They are enabled on demand. For more details, please refer to **Choosing repository protocols**.

Table 16. Ports for each machine

Computer	Component	Firewall	Required Ports	On-demand ports
Computer A	Web browser	Outbound	8443	
Computer B	HPDM Console & HPDM Console Web Bridge	Inbound	8443	40004(Reverse shadow)
Computer B	HPDM Console and HPDM Console Web Bridge	Outbound	40002, File transfer ports	40004(Shadow)
Computer C	SQL Server	Inbound	1443	
Computer D	Child Repository	Inbound	File transfer ports	
Computer E	Master Repository Controller & Master Repository	Inbound	40012, File transfer ports	
Computer E	Master Repository Controller & Master Repository	Outbound	File transfer ports	
Computer F	HPDM Server	Inbound	1099, 40002, 40005	40009(Resource monitor)
Computer F	HPDM Server	Outbound	1443, 40003, 40012	
Computer G	Thin Client (HPDM Agent)	Inbound	40001	40004(Shadow)
Computer G	Thin Client (HPDM Agent)	Outbound	40003, File transfer ports	40009(Resource monitor), 40004(Reverse Shadow)
Computer H	HPDM Gateway	Inbound	40003	
Computer H	HPDM Gateway	Outbound	40001, 40005	

Table 17. Purposes for each port

Port	Protocol	Purpose
20 & 21	TCP	Default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. You can configure FTP ports via HPDM Console. If you do not use the default ports for your FTP server, be sure to configure the firewall appropriately.

22	TCP	Default port for SFTP (used for repositories). You can configure SFTP ports via HPDM Console. If you do not use the default port for your SFTP, be sure to configure the firewall appropriately.
137	UDP	Allows NetBIOS Name Resolution
138	UDP	Allows NetBIOS Datagram transmission and reception
139	TCP	Allows NetBIOS Session Services connections
443	TCP	Default port for HTTPS (used for repositories). You can configure HTTPS ports via HPDM Console. If you do not use the default port, be sure to configure the firewall appropriately.
445	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
989 & 990	TCP	Default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. You can configure FTPS ports via HPDM Console. If you do not use the default ports for your FTPS server, be sure to configure the firewall appropriately.
1099	TCP	Allows HPDM Console to query the RMI Registry.
1443	TCP	Default port for remote connections to SQL Server.
8443	TCP	Allow access to the console via a browser, you can modify this port in the configuration center.
40001	TCP UDP	Allows HPDM Gateway to send tasks to HPDM Agent Allows HPDM Agent to receive replies of broadcasting from HPDM Gateway
40002	TCP	Allows HPDM Console to call remote objects from HPDM Server via RMI.
40003	TCP	Allows HPDM Server to send tasks to HPDM Gateway
40004(Reverse Shadow)	TCP	SSL VNC Proxy in Listen Mode (reverse VNC)
40004(Shadow)	TCP	Port for SSL VNC connection
40005	TCP	Allows HPDM Gateway to send reports to HPDM Server
40009(Resource monitor)	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.

40012	TCP	Allows HPDM Server to communicate with HPDM Master Repository Controller to manage the HPDM Master Repository
-------	-----	---

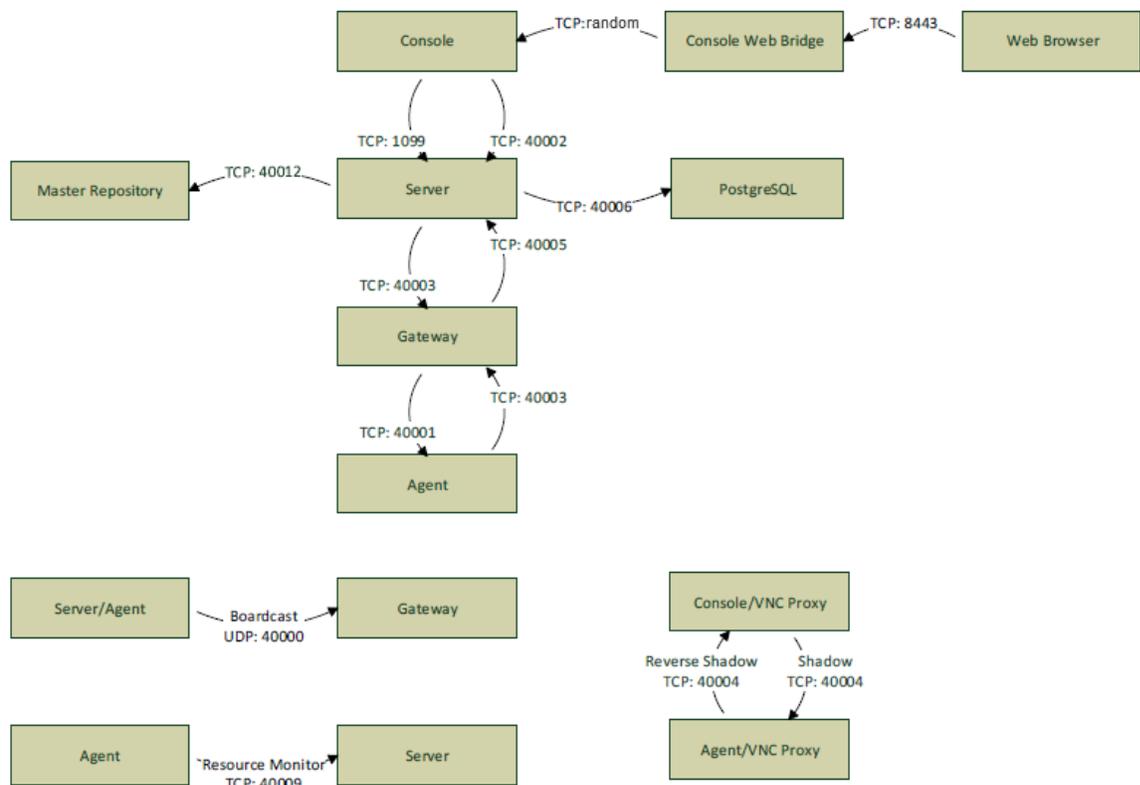
Windows Firewall Rules

A rule will be created to enable ports by default if a component is installed.

Table 18, Default Firewall Rules

Rule name	Default state	Default port
HPDM Console TCP - In	Enable	5500,5900,34455,40004
HPDM Console Web Bridge TCP In	Enable	8443
HPDM Gateway TCP - In	Enable	40003
HPDM Gateway UDP - In	Enable	67,69,4011,40000
HPDM HTTPS Repository TCP - In	Enable	443
HPDM Master Repository TCP - In	Enable	40012
HPDM Server TCP - In	Enable	1099,40002,40005,40006,40009

Figure 3. Port usage in HPDM



Note

This chart lists only the basic ports created by HPDM.

Make sure that the ports are not blocked by a firewall or used by other processes.

Table 19. 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
8443	Web Browser	HPDM Console Web Bridge (bundled with HPDM Console)	TCP	Allow access to the console via a browser. YThankou can modify this port in the configuration center
random	HPDM Console Web Bridge (bundled with HPDM Console)	HPDM Console	TCP	Java Message Service, used to transfer information between the Console Web Bridge and the console
40004	SSL VNC Proxy (bundled with HPDM Agent)	SSL VNC Proxy (bundled with HPDM Console)	TCP	SSL VNC Proxy in Listen Mode (reverse VNC)

Table 20. Console ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Console	FTP server (third-party software)	TCP	Default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. You can configure FTP ports with HPDM Console. If you do not use the default ports for your FTP server, be sure to 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 HTTPS Repository	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.

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

Table 21. 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.

Table 22. 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

Table 23. 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

Table 24. Gateway ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Gateway	FTP server (third-party software)	TCP	Default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. You can configure FTP ports via HPDM Console. If you do not use the default ports for your FTP server, be sure to configure the firewall appropriately.
22	HPDM Gateway	SFTP server (third-party software)	TCP	Default port for SFTP (used for repositories). You can configure SFTP ports via HPDM Console. If you do not use the default port for your SFTP, be sure to 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 HTTPS Repository	TCP	Default port for HTTPS (used for repositories). You can configure HTTPS ports via HPDM Console. If you do not use the default port, be sure to configure the firewall appropriately.
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	Default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. You can configure FTPS ports via HPDM Console. If you do not use the default ports for your FTPS server, be sure to 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

Table 25. 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
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)

Table 26. Agent ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
---------------	--------	----------	----------	---------

20 & 21	HPDM Agent	FTP server (third-party software)	TCP	Default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. You can configure FTP ports via HPDM Console. If you do not use the default ports for your FTP server, be sure to configure the firewall appropriately.
22	HPDM Agent	SFTP server (third-party software)	TCP	Default port for SFTP (used for repositories). You can configure SFTP ports via HPDM Console. If you do not use the default port for your SFTP, be sure to 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 HTTPS Repository	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 Windows: TightVNC (bundled with HPDM Agent) HP ThinPro: X11VNC (bundled with platform)	TCP (loopback)	VNC Shadow

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.

Table 27. 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	Default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. You can configure FTP ports via HPDM Console. If you do not use the default ports for your FTP server, be sure to configure the firewall appropriately.
22	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	SFTP server (third-party software)	TCP	Default port for SFTP (used for repositories). You can configure SFTP ports via HPDM Console. If you do not use the default port for your SFTP, be sure to 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.

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 HTTPS Repository	TCP	Default port for HTTPS (used for repositories). You can configure HTTPS ports 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	Default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. You can configure FTPS ports via HPDM Console. If you do not use the default ports for your FTPS server, be sure to 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)

Table 28. Repository ports (outbound)

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

22	HPDM Master Repository Controller	SFTP server (third-party software)	TCP	Default port for SFTP (used for repositories). You can configure SFTP ports via HPDM Console. If you do not use the default port for your SFTP, be sure to 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 HTTPS Repository	TCP	Default port for HTTPS (used for repositories). You can configure HTTPS ports via HPDM Console. If you do not use the default port, be sure to 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	Default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. You can configure FTPS ports via HPDM Console. If you do not use the default ports for your FTPS server, be sure to configure the firewall appropriately.

Deployment factors

This section lists the primary factors that might influence an HPDM deployment and provides deployment recommendations. The main factors are as follows:

- Hardware environment
- Network environment
- Number of devices
- HPDM logic

Hardware environment

The following table provides the minimum hardware requirements of HPDM components.

Table 29. System requirements

HPDM component	Operating system	Suggested minimum hardware
HPDM Console	Windows Server 2016	Intel® compatible 64-bit processor supporting 2 or more CPU cores
	Windows Server 2019	4 GB RAM (Recommended: 4 CPU cores and 6 GB RAM)
	Windows Server 2022	1 GB free disk space
	Windows 10	
	Windows 11	

HPDM Console Web Bridge	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11	Intel® compatible 64-bit processor supporting 2 or more CPU cores 5 GB RAM (<u>Recommended: 4 CPU cores and 7 GB RAM</u>) (For 1 console instance and Console Web Bridge server. Add 1 GB for each additional console) 2 GB free disk space
HPDM Server	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM (<u>Recommended: 4 CPU cores and 6 GB RAM</u>) 2 GB free disk space
HPDM Configuration Center	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 1 GB free disk space
HPDM Gateway	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 2 GB free disk space
HPDM Master Repository Controller	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 4 GB free disk space Note: This is the minimum required hardware for the Master Repository. If there are more than 50 imaging or file-copying operations, then HP recommends using a more powerful system that has free available disk space.
HPDM HTTPS Repository	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 10 Windows 11	Intel compatible 64-bit processor supporting 2 or more CPU cores 4 GB RAM 2 GB free disk space 7200 RPM disk Note: This is the minimum required hardware for HPDM HTTPSRepository. If there are more than 50 imaging or file transfer-operations, then HP recommends using a more powerful system that has free available disk space.

Database storage

The disk space usage of the database grows with the total device and task amounts. Calculate the required disk space with the following pattern:

- The initial disk space is less than 50 MB.
- Add an additional 100 MB for every 1,000 devices.
- Add an additional 1 MB for every 100 tasks.

Repository capacity

The disk space usage of the repositories grows with the size of payload contents; especially with images of a device operating system. Make sure that the disk space is enough to hold all payloads and tools.

Table 30. Recommended size reserved for repository

Device Operating System	Minimum Recommended Size
Windows 10 IoT Enterprise LTSC	8 GB
HP ThinPro 8.1	2 GB
HP ThinPro 8	2 GB
HP ThinPro 7.2	2 GB

Network infrastructure

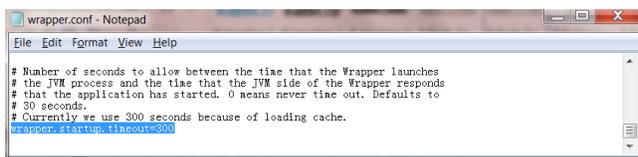
There are many network factors that might influence the deployment of HPDM, such as the network bandwidth or whether HPDM components are deployed on one or more subnets. Some companies might have different network strategies, such as devices that are required to be in a NAT environment, or devices that are required to be deployed in different regions, or that HPDM components cannot connect to directly to the internet. You can deploy HPDM based on your specifications.

To manage large-scale deployments, HP recommends installing the HPDM Server and the HPDM Gateway services on the same subnet as the database. A server-type operating system is needed because of the half-open connection limit on client operating systems.

HP recommends deploying the HPDM Server as close to the database server as possible, because the network latency between these two components has a significant impact on Device Manger performance. Network latency between the HPDM Server and database that is more than 30 milliseconds causes obvious delays for HPDM Console users. In addition, HP recommends deploying a Child Repository as close to its related devices as possible.

Note

If latency is unavoidable, go to ... \Server \conf \wrapper . conf, and increase the value of `wrapper.startup.timeout` in `wrapper . conf` on the HPDM Server side. The default value is 300 seconds, which makes the HPDM Server more tolerant to database latency.



Network address translation (NAT)

The physical network where HPDM is deployed might be complex. When allocating components between two networks, such as a public network and private network, you can separate different NAT cases as shown in the following model. There is a single HPDM component within the public, or outer, network, and other HPDM components within the a single private, or inner, network. Within this model, it is assumed that without additional configuration, applications on the private network can connect to the public network and that applications on the public network cannot connect to the private network.

Figure 4. Topographical model of NAT environment

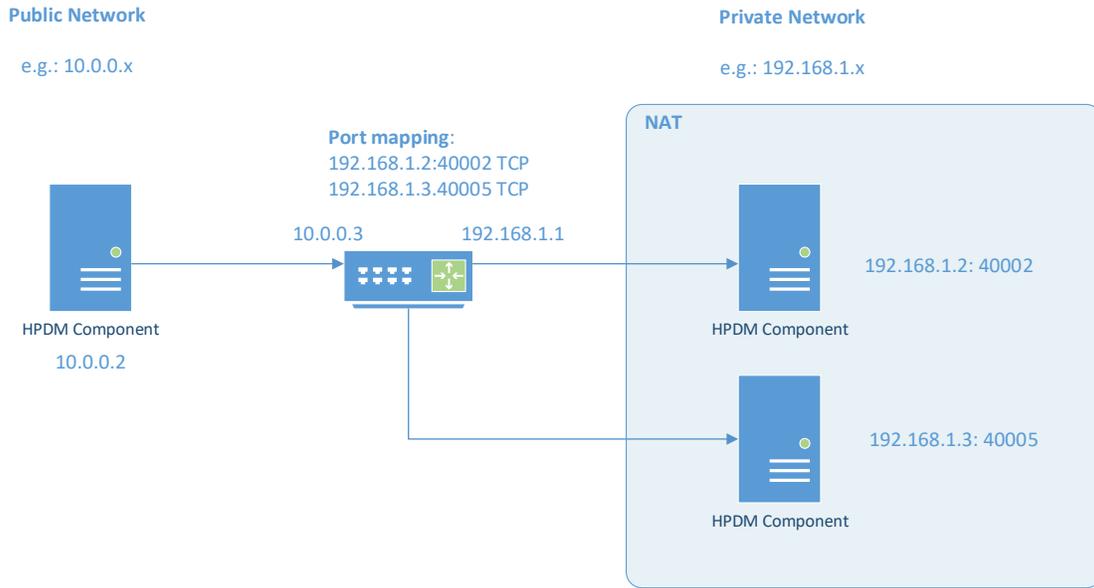


Table 31. Evaluated NAT scenarios

				With outer router ports mapped to inner ports ⁵	Without outer router ports mapped to inner ports	
HPDM Server	HPDM Gateway	40000	UDP	Passed	N/A ⁴	
	HDPM Gateway	40003	TCP	Passed		
	Master Repository Controller	40012	TCP	Passed	N/A	
HPDM Console	HPDM Server	1099	TCP	Failed ²	N/A	
		40002	TCP			
	HPDM Agent	40004	TCP	Failed ²		
HPDM Gateway	HPDM Agent	40001	TCP	Passed	N/A ³	
	HPDM Server	40005	TCP	Passed	N/A ³	
	PCoIP Zero Client	50000	TCP	Failed	N/A	Only PCoIP-related tasks fail.
HPDM Agent	HPDM Gateway	40000	UDP	Passed	N/A ⁴	
	HPDM Gateway	40003	TCP	Passed	N/A	
	HPDM Console (Reverse Shadow)	40004	TCP	Failed	N/A	Only Reverse Shadow tasks fail.
	HPDM Server (Resource Monitor)	40009	TCP	Failed	N/A	Only Resource Monitor tasks fail.

¹ Passes if the HPDM Console can connect to the HPDM Server successfully, perform operations, send tasks to devices, and update device status correctly.

² To connect the HPDM Console to the HPDM Server successfully, perform the following steps on the HPDM Server side:
Stop the HPDM Server.

Open the following file for editing: `\Server\conf\wrapper.conf`

Add the following parameter to the file, where <IPAddress> is the outer IP address of the private network router:

```
wrapper.java.additional.2=-Djava.rmi.server.hostname=<IPAddress>
```

4. On 5.0 and 5.0 SP1, run `\Server\bin\HPDMServer.exe` to add the following parameter to JVM Options to the HPDM Server service:

```
-Djava.rmi.server.hostname=<IPAddress>
```

HP Device Manager Server Service Properties

General Log On Logging **Java** Startup Shutdown

Use default

Java Virtual Machine:
 ...

Java Classpath:

Java Options:

Since 5.0 SP2, run \Server\bin\service_update.bat to update the HPDM Server service

5. Restart the HPDM Server.

³ HPDM supports a poll mode in which ports 40001 and 40005 can be replaced by port 40000.

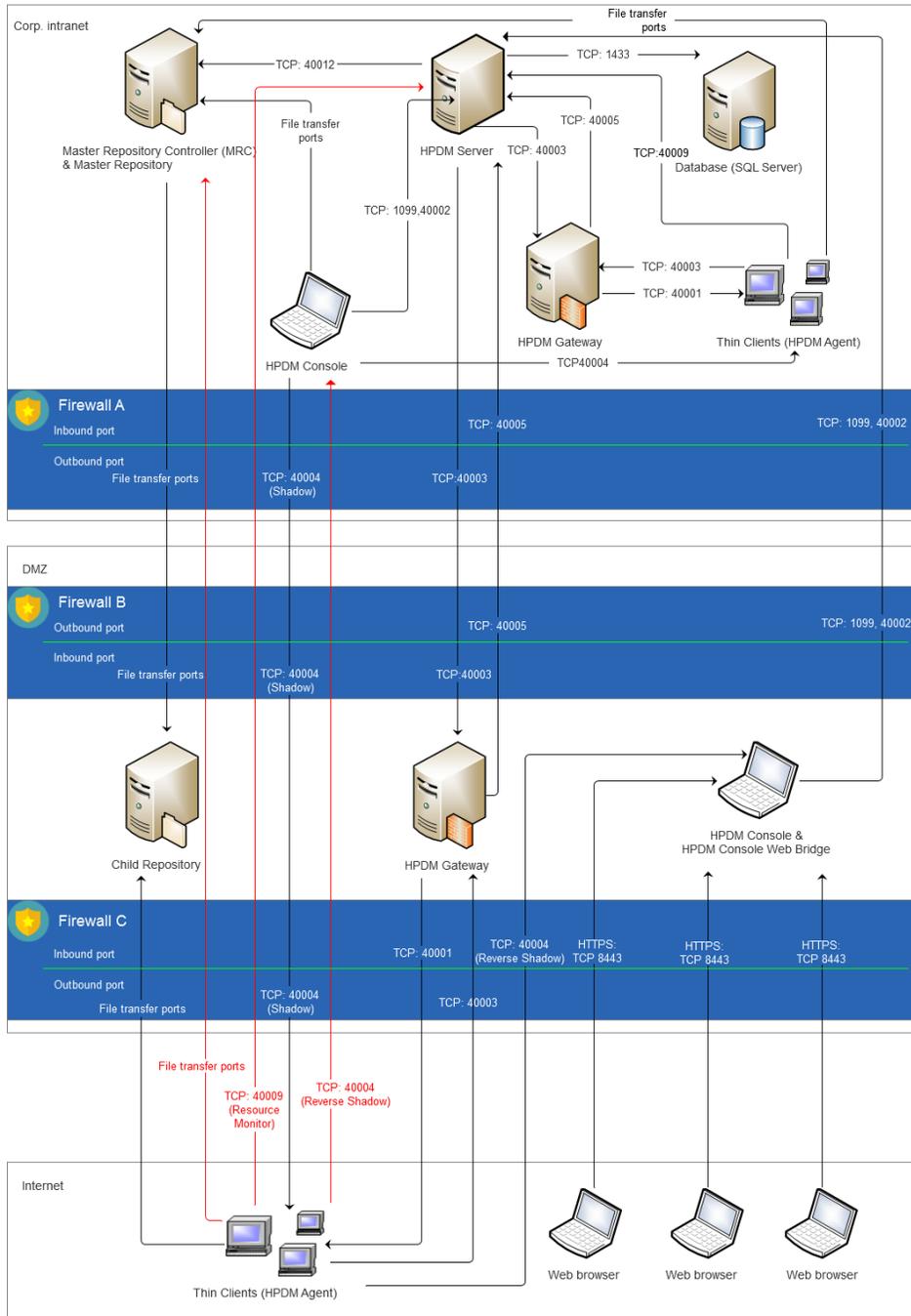
⁴ Port 40000 is for HPDM poll mode only, and can be replaced by ports 40001 and 40005.

⁵ In this setup, the router maps the inner (private network) IP address and port to the outer (public network) IP address and port. Based on these results, you can connect from a private network IP address and port from a public network.

DMZ considerations

If you want to use HPDM to manage devices located in both the corporate (intranet) network and the internet, you must place an HPDM Gateway, an HPDM repository and an HPDM Console in the corporate network’s DMZ environment to manage the devices outside the corporate network.

Figure 5. Typical HPDM topology in a DMZ environment



Note:

If you use the window system firewall, HP configures it by default.

For detailed information about HPDM ports, see **Port usage** in the **Port Reference** chapter of this guide.

Figure 5 provides an example of how to deploy HPDM within a DMZ environment. In this example, each component is installed on a single computer. You can install more than one component, such as HPDM Gateway A and HPDM Server, on one computer. You must install HPDM Console Web Bridge and HPDM Console on one computer.

Installing all HPDM Server-side components in the DMZ environment usually makes the topology simpler; however, most companies have a strict security policy against this configuration.

Selecting a file transfer protocol

- If you are using FTP protocol, use ports 20 (in PORT mode) and 21. If you want to use PASV mode, set a port range for PASV mode in the FTP server and be sure that your firewall does not block the selected ports.
- If you are using FTPS protocol, use ports 989 (in PORT mode) and 990. If you want to use PASV mode, set a port range for PASV mode in the FTP server and be sure that your firewall does not block the selected ports.
- If you are using SFTP protocol, use port 22.
- If you are using Shared Folder protocol, use ports TCP 139 and 445 and UDP 137 and 138.
- If you are using HTTPS protocol, use port 443.

Resolving child repository addresses

Both the Master Repository Controller located in the corporate intranet and the devices located within the internet need access the child repository. However, you can only set one address for a repository location from the HPDM Console. If you set an intranet address, devices in the internet cannot access the repository. If you set an outside (internet) address, the Master Repository Controller might not be able to access the repository.

There are two possible solutions, as follows:

- Configure the network to make sure that the Master Repository Controller can access the outside address.
- On the Master Repository Controller, modify the Windows HOSTS file (in %systemroot%\system32\drivers\etc\) to map the outside address (hostname or FQDN) to the internal IP address of the child repository.

For example, the child repository address is `hpdm-dmz.hp.com`, and corp. network cannot access it. Add the line `192.168.10.20 hpdm-dmz.hp.com` to the HOSTS file of the Master Repository Controller. The Master Repository Controller can then go to 192.168.10.20 to access the child repository.

You can set the outside address as the child repository address in HPDM Console

Using PASV mode with FTP or FTPS

When an FTP or FTPS server receives a PASV command, it replies with an IP address and a port using an `xx,xx,xx,xx,yy,yy` string to the FTP or FTPS client. `xx,xx,xx,xx` is the IP address and `yy,yy` is the port. Then, the client connects to `xx.xx.xx.xx:yyyy`. Both the Master Repository Controller and outside devices need access to the FTP or FTPS server. This is similar to the child repository address issue; however, the FTP or FTPS server only can be set to IP address in PASV mode.

The HPDM file client library can resolve this issue. The HPDM file client does not use `xx.xx.xx.xx` in reply to a PASV command but does use the original address for the control socket.

For example, if an HPDM file client connects to `hpdm-dmz.hp.com:21` and sends `PASV`, it receives the reply `192,168,10,20,10,01`. Then, its data socket connects to `hpdm-dmz.hp.com:2561` ($10*256 + 01 = 2561$).

Limitations

The three red lines in Figure 5 represent connections that cannot be easily resolved. See the following list for details:

- Protocols for file transfer between the HPDM Agents and the Master Repository Controller.
A Capture File task always capture files to the Master Repository. If the Master Repository is in the corporate intranet, outside devices cannot connect to the Master Repository.
- Using Reverse Shadow on port TCP 40004 between the HPDM Agents and HPDM Console.
If the HPDM Console is in the corporate intranet, outside devices cannot connect to the HPDM Console.
- Using Resource Monitor on port TCP 40009 between the HPDM Agents and HPDM Console.
- If the HPDM Console is in the corporate intranet, outside devices cannot connect to the HPDM Console.

Moving all HPDM Server-side components to the DMZ environment can resolve these issues. Your security policy determines whether you can use this configuration.

Ports between networks

Table 32. Ports between networks

Network	Peer	Direction	Type	Port
Corporate intranet	DMZ	Inbound	TCP	20, 989, 1099, 40002, 40005
		Outbound	TCP	21, 22, 139, 443, 445, 40003

			UDP	137, 138
DMZ	Corporate intranet	Inbound	TCP	21, 22, 139, 443, 445, 40003
			UDP	137, 138
		Outbound	TCP	20, 989, 1099, 40002, 40005
	Internet	Inbound	TCP	21, 22, 139, 443, 445, 8443, 40003
			UDP	137, 138
		Outbound	TCP	40001, 40004
Internet	DMZ	Inbound	TCP	40001, 40004
		Outbound	TCP	21, 22, 139, 443, 445, 8443, 40003
			UDP	137, 138

Note

There is no requirement to allow all file transfer ports in your firewall. For details on required ports, see **Selecting a file transfer protocol**.

Failover redundancy

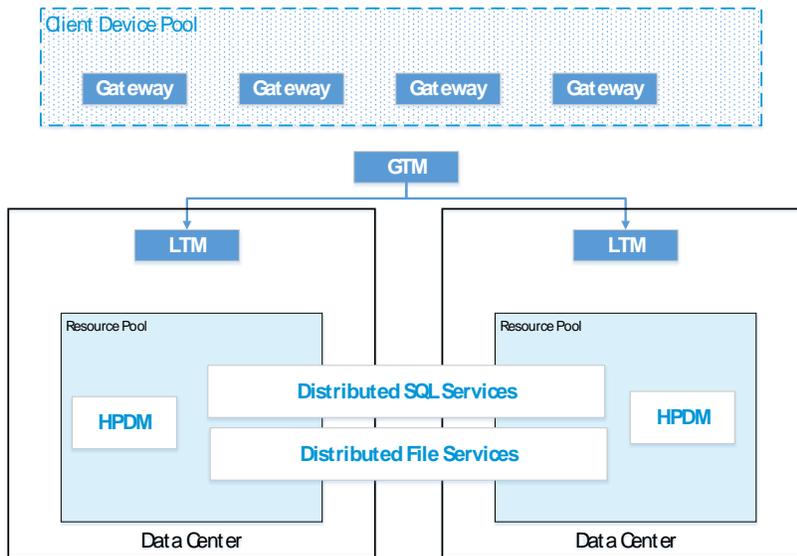
This section provides high-level guidance for implementing failover redundancy of HP Device. The HPDM management solution provides an easy-to-use interface and workflows that are streamlined for the management of HP thin clients. HPDM is a highly scalable management solution for thin clients. HPDM can scale from managing thousands to more than 100,000 devices, all on a single management server. However, scalability is not enough to cover all unforeseen failures. Diligent planning and built-in redundancy can help ensure that HPDM remains available and resilient despite infrastructure failures or other catastrophic events.

Redundancy scenario

One approach to high availability that covers a wide range of issues is the creation of redundant data centers. You can create mirrors of the resources within your network to make these resources instantly available if the origin service goes offline. This approach is consistent with the current architecture of HPDM, because HPDM is designed to have a single point of operation with gateways and repositories feeding from the single-server service layer in a hub-and-spoke pattern.

The following diagram provides a high-level depiction of an example environment with redundant data centers. The active infrastructure in this model is F5 Network’s BIG-IP; however, the concepts demonstrated can also apply to other software-defined networking solutions.

Figure 6. Example environment with redundant data centers



In this model, the global traffic manager is used to mask and route traffic between data center implementations, keeping client devices unaware of the redundancy model that has been put in place. In addition, local traffic managers monitor the availability of and provide access to resources within each data center. The local traffic manager does this by managing the resources available, the HP Device Manager server itself, the HP Device Manager Master Repository Controller (hosted within the same VM as our server), the SQL database service, and the distributed file system service used to store master repository content.

Implementing redundancy

Ideally, your redundant HPDM configuration looks identical to your regular configuration. If you can provide consistent addressing for SQL database services and for master repository file system services, configure the same for the VM housing HPDM Server and the Master Repository Controller agent. You can also use this VM to create local redundancy within each data center by supporting multiple VM hosts behind Local Traffic Manager. In this example, that level of redundancy is unnecessary. Depending on your own data center configuration, Local Traffic Manager can manage both multiple VMs and multiple VM pools containing the HPDM resources.

Some key things to consider when implementing redundancy of your HPDM Server environment:

- Choose a database solution that provides availability across data centers. HPDM interoperates with a wide selection of databases that you can configure for high availability.
- Be sure that both data centers have access to the same user level; typically, you can configure this access through Active Directory replication. HPDM uses user-level permissions to communicate with the file service layer. Additionally, HPDM uses Active Directory users and groups to provide privilege access controls to various management tasks.
- Do not try to load balance HPDM traffic across multiple VMs. HPDM is not designed to operate in a coordinated effort with multiple servers either servicing the same device or leveraging the same database tables. If you have reached the scalability limits of HPDM within your installation environment, consider segmenting traffic by location and routing that traffic through your available data centers.

Local traffic management

To monitor the availability of HPDM resources, add HPDM as a virtual server resource to manage within each of your data center Local Traffic Managers. Identically configure each Local Traffic Manager per data center.

Inbound traffic from HPDM Gateways to HPDM Server is on TCP port 40005. Outbound traffic to HPDM Gateways is on TCP port 40003.

Inbound connections to HPDM Server from management consoles use TCP ports 1099 and 40002.

Global traffic management

To the client network, there is one and only one instance of HPDM. To implement redundancy, be sure that to the client network still perceives one and only one instance of HPDM.

This example Global Traffic Manager uses a well-known DNS entry HPDM. This address is routed to the appropriate virtual HPDM Server based on availability. Global Traffic Manager asks each Local Traffic Manager that manages virtual server resources for availability information.

In this example, one virtual resource pool (Local Traffic Manager) is designated as the primary HPDM resource. Any other Local Traffic Managers are used as failover sources, if the primary Local Traffic Manager becomes unavailable.

Summary

This scenario demonstrates where additional fault tolerance and disaster recovery support for HPDM can be achieved through data center redundancy using corporate infrastructure. While this example does not consider all environments or implementations, it does demonstrate the basic requirements for implementing redundancy with HPDM.

Number of devices

As the total number of managed devices increases, you should use more powerful, server-level hardware configurations such as RAID. The recommended maximum number of devices in one HPDM deployment is 100,000. Lab testing shows that HPDM performs most efficiently up to this number.

You can successfully use HPDM to manage up to 100,000 devices with a single HPDM Server using the following considerations:

- Use of networks faster than 1000 Mbps
- Efficient placement of gateways and repositories to maximize the use of LAN-based communications
- Use of scheduled tasks to execute tasks during non-peak hours of operation
- Use of cached tasks and bandwidth throttling to minimize network impact of large payloads

Note

HPDM is a very flexible system and supports the use of any number of HPDM Servers, HPDM Gateways, and repositories to match the customer's existing network architecture.

Deployment options

There are many factors in which Device Manager's implementation logic might influence the deployment, as included in the following list:

- HPDM does not support clustering or synchronization. Only one HPDM Server can manage a single device at any given time. While you can deploy as many HPDM Servers within your environment as necessary according to your requirements, under a single HPDM Server, you can deploy the following:
 - Multiple HPDM Consoles
 - One database
 - Multiple HPDM Gateways
 - One Master Repository
 - Multiple Child Repositories
- PXE imaging
 - To use PXE imaging, deploy an HPDM Gateway in the same subnet as the devices.
 - If the subnet is a NAT subnet, configure port mapping on NAT to make sure that HPDM Server can talk to HPDM Gateway directly.

Multiple HPDM Consoles

Currently, HPDM does not limit the number of HPDM Consoles connected to an HPDM server. Based on the results of extreme performance testing (using 50,000/100,000 devices, one HPDM Gateway, and one HPDM Server), sending tasks from HPDM Consoles to all devices at the same time, HP recommends sending a task from less than five HPDM Consoles at the same time.

Multiple HPDM Gateways

HPDM does not limit the number of HPDM Gateways connected to an HPDM Server. One HPDM Gateway has verified good performance from the performance testing (using 50,000/100,000 devices, one HPDM Gateway, and one HPDM Server), so HP recommends not using too many HPDM Gateways in under one HPDM Server. For some core centers and regions, multiple HPDM Gateways are preferred for the following reasons:

- Required for PXE imaging tasks
- Consolidated communication between branch offices and DMZ
- Accelerated task delivery speed when there is a NAT Gateway in branch offices

Advantages of additional repositories

As the volume of transferred files increases, add more Child Repositories for the following reasons:

- Move software payloads closer to distribution points with target devices
- Reduced traffic between branch offices and DMZ
- Faster software updates and image deployment

Determining number of repositories

To determine the number of Child Repositories required, use the following formula:

Number of repositories = (transferred data ÷ bandwidth) ÷ expected time spent

For example, if you have 20,000 units to be reimaged, and each image is 1 GB, you have 20,000 GB (20 TB) of data to transfer. With a connection of 100 Mbps from one repository to a device, it takes 444.4 hours to transfer all data.

$20,000 \text{ GB} \div (100 \text{ Mbps} \div 8 \text{ bits per byte} \div 1000 \times 3600 \text{ seconds per hour}) \approx 444.4 \text{ hours}$

To reduce the data transfer time to 48 hours, you need 10 repositories ($444.4 \div 48$). Keep in mind that there is some overhead to synchronize from the Master Repository to the Child Repositories.

Replacing certificates for HPDM Console Web Bridge

If you need to use different certificates, follow these instructions to replace certificates:

For example, if you have the server.key and server.crt signed by end_entity.crt, and you have a certificate chain: root.crt -> intermediate.crt -> end_entity.crt

Generate ConsoleWebBridgeKeystore.jks and ConsoleWebBridgeTruststore.jks:

- Perform the following command to generate a pfx format file:
`openssl pkcs12 -export -clcerts -in server.crt -inkey server.key -out server.pfx`
Once prompted, enter the required passwords.
- Perform the following command to generate ConsoleWebBridgeKeystore.jks
`keytool -importkeystore -destkeystore "ConsoleWebBridgeKeystore.jks" -srckeystore server.pfx -srcstoretype PKCS12`
Once prompted, enter the required passwords.
Note: keytool can be found in the <installation folder>\Console \JVM\bin
- Perform the following commands to generate ConsoleWebBridgeTruststore.jks:
`keytool -import -trustcacerts -alias end_entity -file end_entity.crt -keystore ConsoleWebBridgeTruststore.jks`
`keytool -import -trustcacerts -alias intermediate -file intermediate.crt -keystore ConsoleWebBridgeTruststore.jks`
`keytool -import -trustcacerts -alias root -file root.crt -keystore ConsoleWebBridgeTruststore.jks`

Deploy ConsoleWebBridgeKeystore.jks and ConsoleWebBridgeTruststore.jks:

- Put two file into the folder <installation folder>\ConsoleWebBridge\webswing\ssl. If the folder already has two files, overwrite them.
- Perform the following command to put passwords:
`"<insallation folder>\ConsoleWebBridge\bin\booter.cmd" -pass`
Once prompted, enter the required passwords.

Deployment scenarios

The following examples provide typical scenarios.

Note

The following table introduces the minimum requirements of some typical scenarios, but you must deploy your environment according to your network situation and company strategies, such as whether devices are in a NAT environment or distributed in different places.

Table 33. Minimum requirements for various deployment sizes

Number of devices	HPDM Servers	HPDM Gateways	Database implementation
1 – 5,000	1	1	PostgreSQL
5,000 – 20,000	1	1	PostgreSQL or MS SQL
20,000 – 100,000	1	1+	MS SQL
100,000+	1+ per 100,000 devices	3+	M1S SQL

Small-scale deployment

Device number: < 5,000

Deployment: 1 HPDM Server, 1 HPDM Gateway, PostgreSQL (or MS SQL Server), 1 Master Repository

This is a small-scale deployment, so the minimum requirement is that you can deploy all HPDM components on one computer.

Typical deployment

Device number: 25,000

Deployment: 1 HPDM Server, MS SQL Server, 3 HPDM Gateways, 1 Master Repository, 2 Child Repositories.

HP recommends that you deploy each HPDM component on its respective computer. In the case that the Master Repository overloads, there are two Child Repositories to divide the file transmission pressure. There are three HPDM Gateways to separate all devices into three groups. Note that one device group is behind a NAT environment. Use the HPDM poll function to manage those devices.

Note

See **Deployment factors** for hardware and other requirements.

Large-scale deployments

Device number: > 100,000

Deployment: Because one HPDM Server supports up to 100,000 devices with verified performance, deployments of greater than 100,000 devices may require multiple instances of HPDM. You might view as multiple normal scale deployments to deploy.

Cloud deployments

Deploying to Amazon EC2

HP Device Manager (HPDM) can work in many different complicated environments. You can configure your firewall to enable deployment of HPDM in a cloud, and then use HPDM in the cloud to manage HP devices. This section covers deploying HPDM in Amazon Elastic Compute Cloud (EC2).

Note

Make sure that your Amazon account has the necessary privileges, and that you have created your Amazon EC2 instance before deploying HPDM. For more information on creating an Amazon account, see Amazon documentation.

To deploy HPDM in Amazon EC2 and manage HP devices:

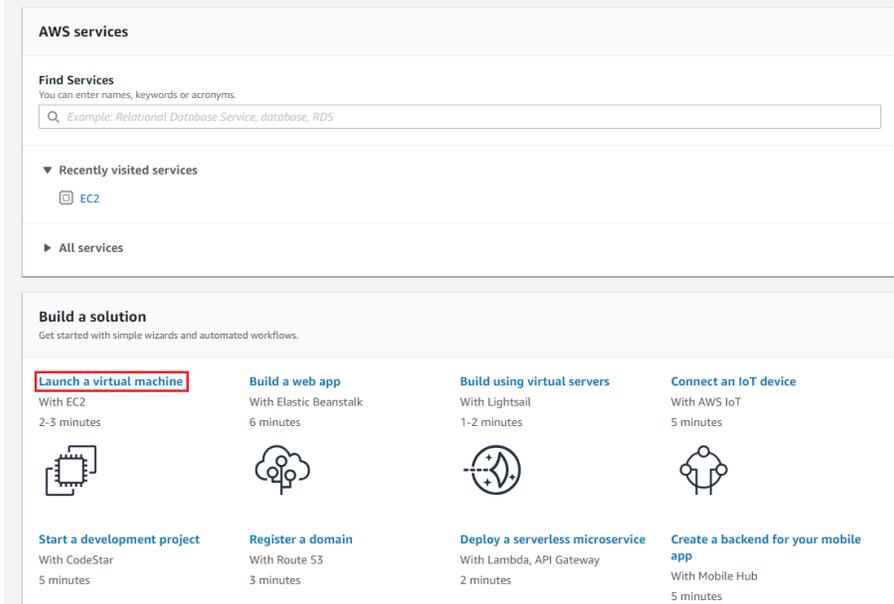
- Create an Amazon EC2 instance. See Amazon documentation. See [Creating an Amazon EC2 instance](#).
- Install HPDM.
- Configure the security groups. See [Error! Reference source not found.](#)
- Launch the Amazon EC2 instance.

Creating an Amazon EC2 instance

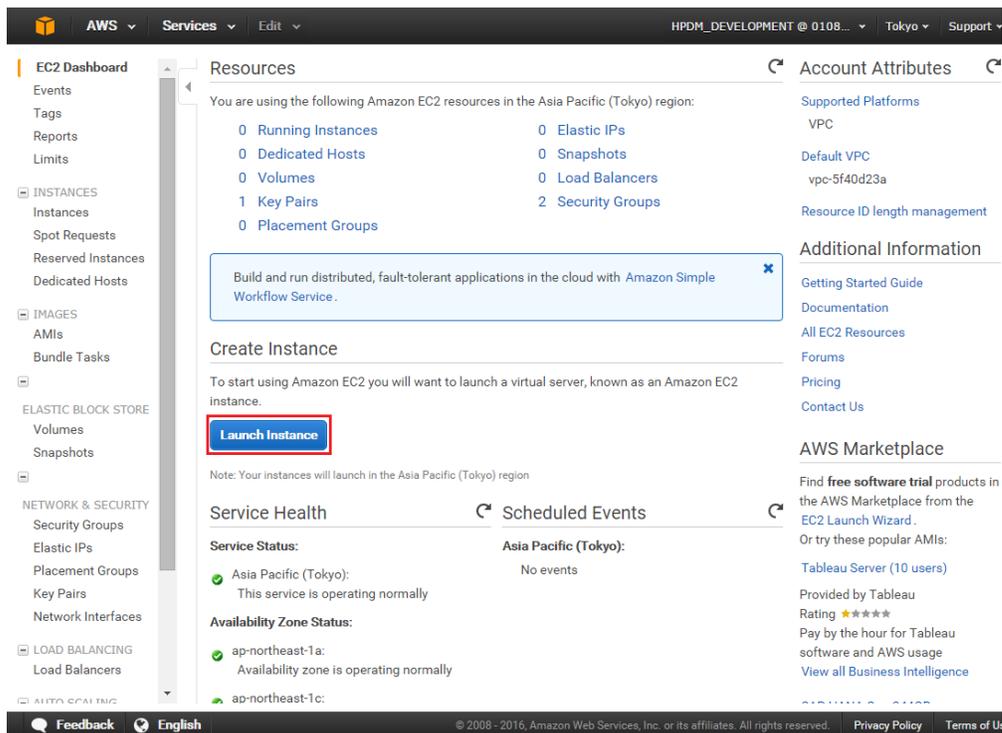
To create an Amazon EC2 instance:

1. Go to <http://aws.amazon.com/> and log on to your Amazon account.
2. On the AWS Management Console, select Launch a virtual machine

AWS Management Console



3. In the EC2 Dashboard, select **Launch Instance**.



4. Choose an available Amazon Machine Image (AMI), and then select **Select**.

AWS Services Edit HPDM_DEVELOPMENT @ 0108... Tokyo Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

Root device type: ebs Virtualization type: hvm

	Microsoft Windows Server 2012 Base - ami-7f799e1e	Select
Windows	Microsoft Windows 2012 Standard edition with 64-bit architecture. [English]	64-bit
Free tier eligible	Root device type: ebs Virtualization type: hvm	
	Microsoft Windows Server 2012 with SQL Server Express - ami-7d799e1c	Select
Windows	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Express. [English]	64-bit
	Root device type: ebs Virtualization type: hvm	
	Microsoft Windows Server 2012 with SQL Server Web - ami-6c47a00d	Select
Windows	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Web edition. [English]	64-bit
	Root device type: ebs Virtualization type: hvm	
	Microsoft Windows Server 2012 with SQL Server Standard - ami-eb7a9d8a	Select
Windows	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Standard edition. [English]	64-bit
	Root device type: ebs Virtualization type: hvm	
	Microsoft Windows Server 2008 R2 Base - ami-857e99e4	Select
Windows	Microsoft Windows 2008 R2 SP1 Datacenter edition and 64-bit architecture. [English]	64-bit

Feedback English © 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

5. Choose an instance type, and then select **Review and Launch**.

Note

Before completing step 6, configure the security groups. See [Error! Reference source not found.](#)

AWS Services Edit HPDM_DEVELOPMENT @ 0108... Tokyo Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High

Cancel Previous **Review and Launch** Next: Configure Instance Details

Feedback English © 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

6. After you configure the security groups, select **Launch**.

Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Warning: Improve your instances' security. Your security group, launch-wizard-2, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)
Microsoft Windows Server 2012 Base - ami-7f799e1e
Free tier eligible
Microsoft Windows 2012 Standard edition with 64-bit architecture. [English]
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name	Description
launch-wizard-2	launch-wizard-2 created 2016-05-26T08:26:16.756+08:00

[Cancel](#) [Previous](#) [Launch](#)

After the instance is created, you can launch it with your Amazon account. Then you can install HPDM in it.

Installing HP Device Manager 5.0

1. In the EC2 Dashboard, select **Running Instances**.

Resources
You are using the following Amazon EC2 resources in the Asia Pacific (Tokyo) region:

1 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
1 Volumes	0 Load Balancers
1 Key Pairs	3 Security Groups
0 Placement Groups	

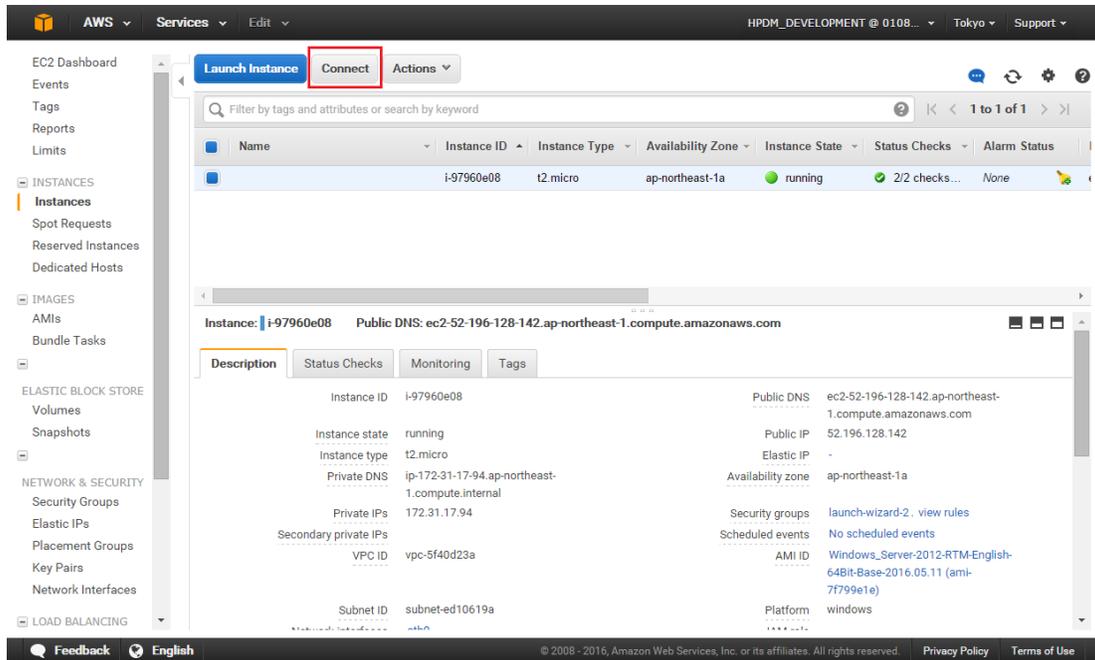
Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.
[Launch Instance](#)

Note: Your instances will launch in the Asia Pacific (Tokyo) region

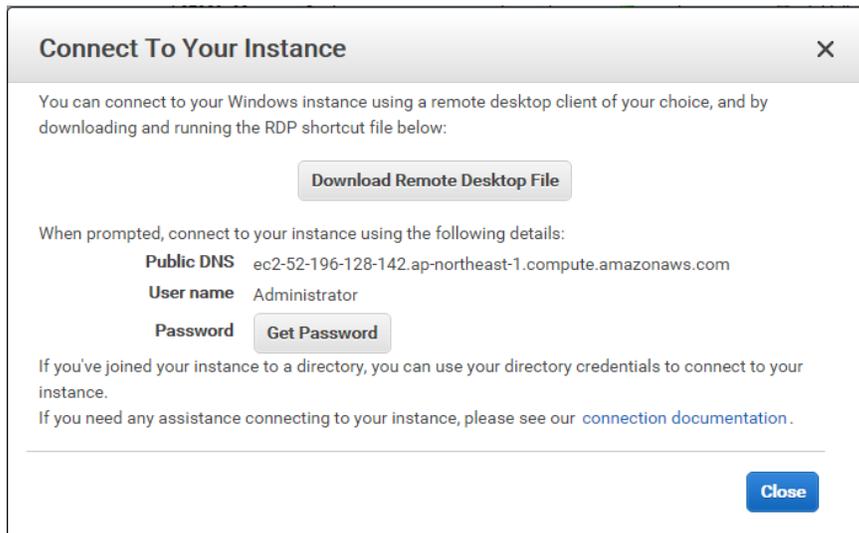
Service Health
Service Status: Asia Pacific (Tokyo): This service is operating normally
Availability Zone Status: ap-northeast-1a: Availability zone is operating normally

Scheduled Events
Asia Pacific (Tokyo): No events

2. Select **Connect**.



3. Select **Download Remote Desktop File** and save it to your local system.
4. Select **Get Password**.



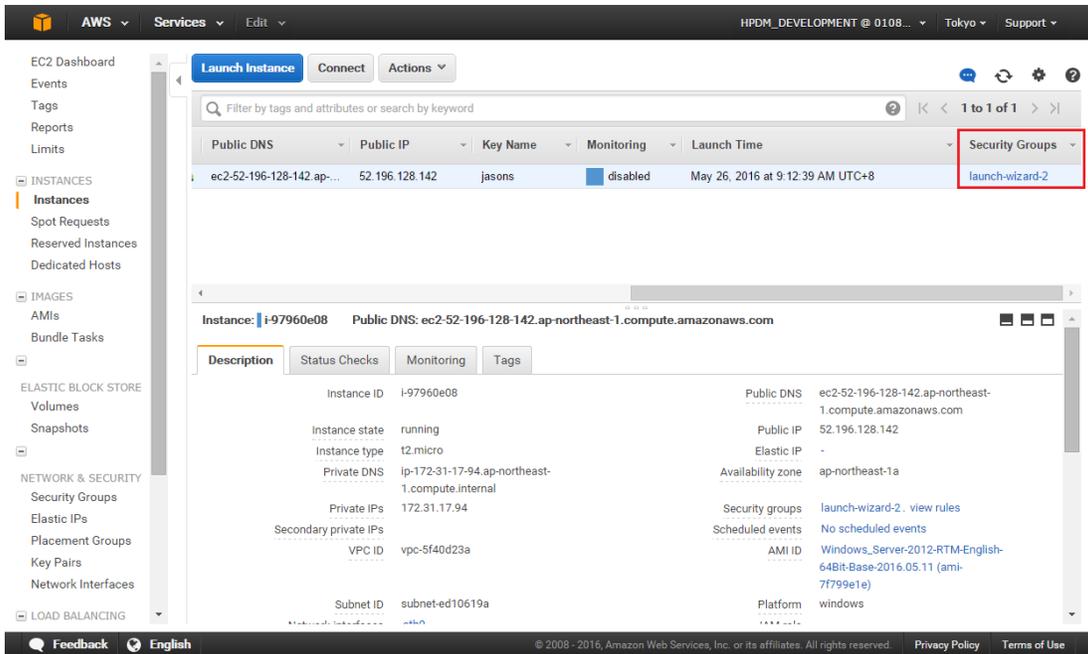
5. Use this password and file to connect to your instance.
6. Upload the HPDM package to the instance, and then install it. For instructions on installing HPDM, refer to the installation section of the guide.

Configuring the security groups

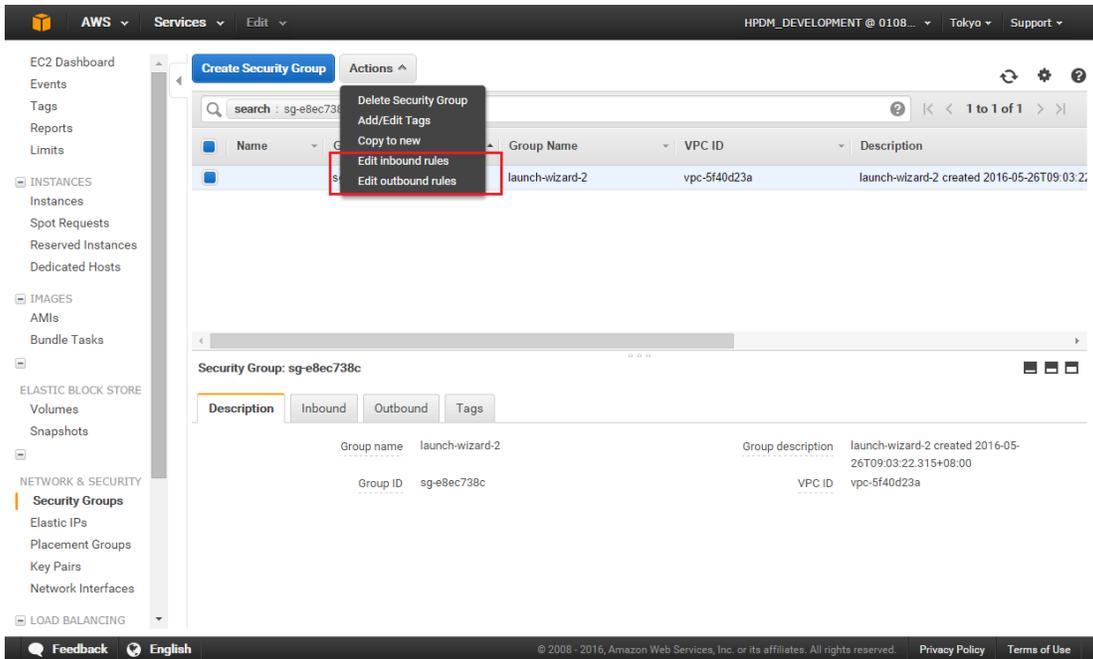
By default, an Amazon EC2 instance opens only the RDP connection through port 3389. You must map the ports corresponding to HPDM to manage your device over the Internet.

To add a port to your firewall:

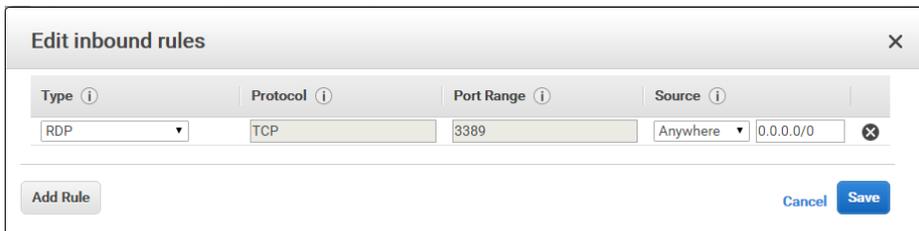
1. Select the instance where HPDM was installed, and then select the **Security Groups** column value.



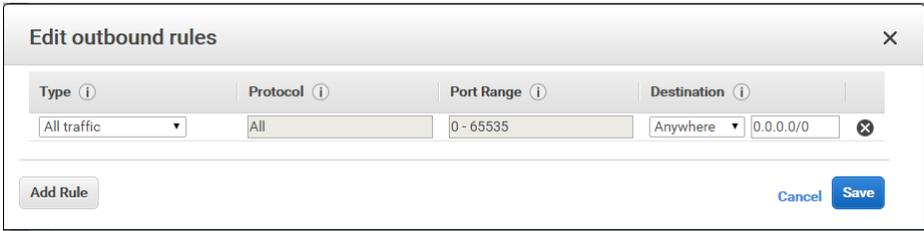
2. Select **Actions** to configure this security group as necessary.



• **Edit inbound rules**—Specifies which ports of the Amazon EC2 instance can be accessed and by which computers.



- **Edit outbound rule**—Specifies which ports on the selected computers can be accessed by the Amazon EC2 instance. By default, **All traffic** is selected.



Repeat this procedure for every port used by HPDM in your production environment. For more information about which ports HPDM uses, see the Port reference section in the *Administrator Guide* for HP Device Manager 5.0.

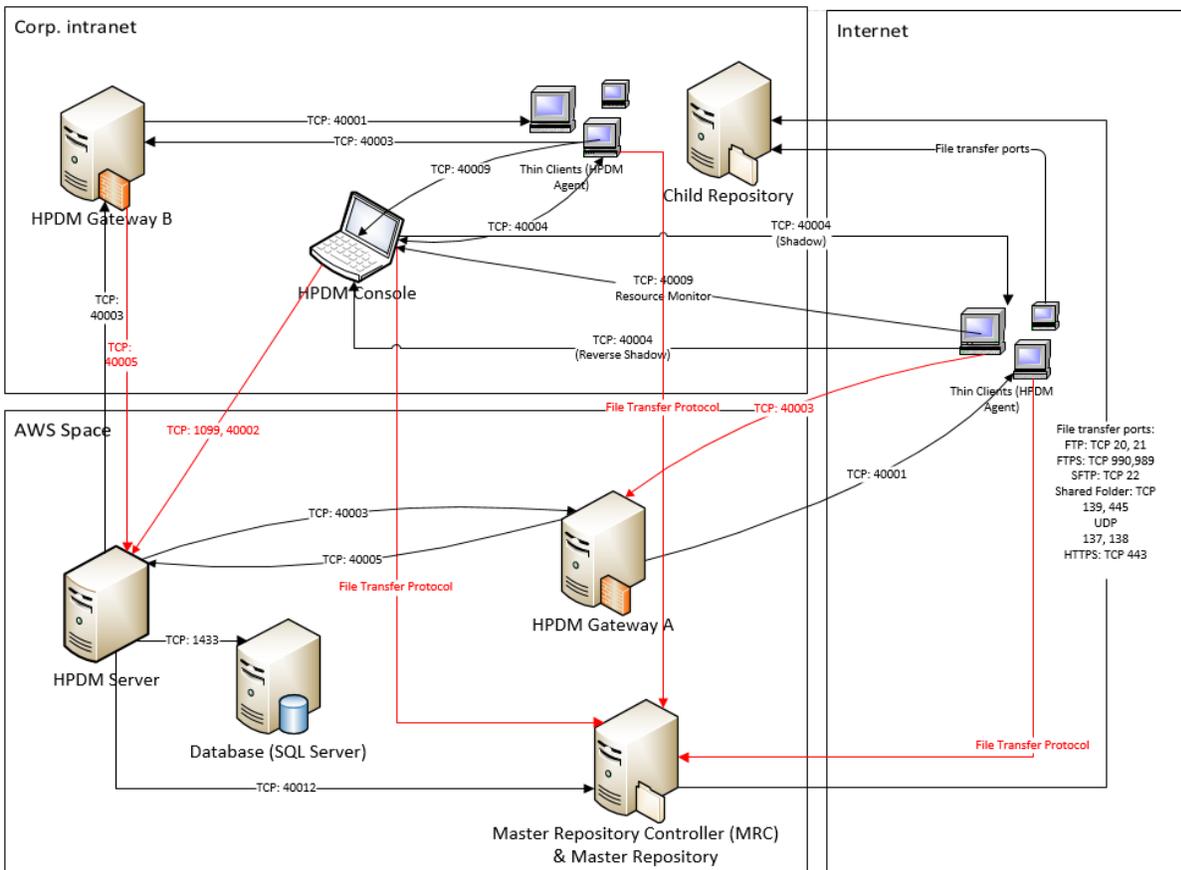
Sample scenario

Production environments are complex, diversified, and flexible. Use the following example to better understand port configuration in the cloud. This is a typical model with detailed configurations for reference.

Note

There might be firewalls between the internet or intranet and Amazon EC2. Make sure that you have completed the procedure in **Configuring the security groups** to allow communication between your devices and the cloud.

Figure 6. Typical topography



All ports in red in previous illustration must be added to the endpoint firewall.

Table 27. Endpoints rule in Amazon EC2

Name	Protocol	Public port	Private port
------	----------	-------------	--------------

HPDM Gateway B to HPDM Server	TCP	40005	40005
HPDM Console to HPDM Server	TCP	1099	1099
HPDM Console to HPDM Server	TCP	40002	40002
HPDM Agent to Master Repository Controller	TCP/UDP	File Transfer Port	File Transfer Port
HPDM Console to Master Repository Controller	TCP/UDP	File Transfer Port	File Transfer Port
HPDM Agent to HPDM Gateway A	TCP	40003	40003

Deploying to Microsoft Azure

HP Device Manager (HPDM) is a device management tool capable of working in many different complicated environments. If you configure your firewall, you can deploy HPDM in a cloud and use it to manage HP devices. This section covers deploying HPDM in Microsoft® Azure.

Note:

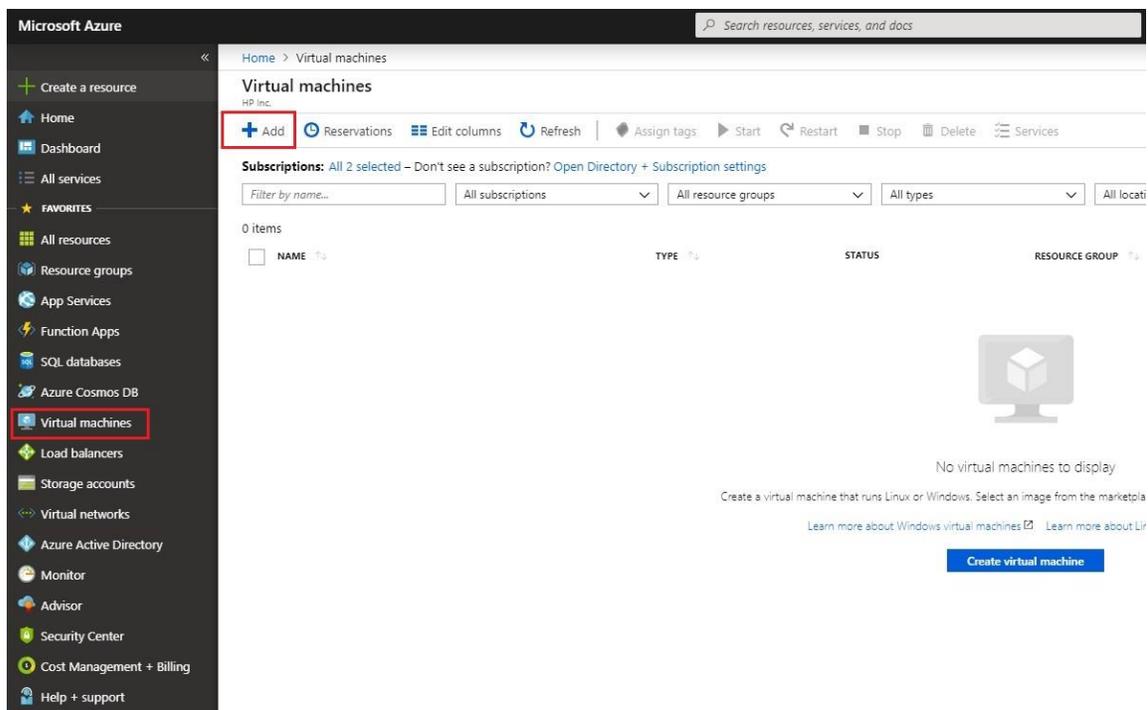
Make sure your Azure account has the necessary privileges, and that you have created your Azure workspace before deploying HPDM. For more information of creating an Azure account, contact Microsoft.

To deploy HPDM in Azure and manage HP devices:

- Create virtual machines in your Azure workspace.
- Install HPDM.
- Configure the firewall.

Creating virtual machines in your Azure workspace

1. Go to <https://manage.windowsazure.com> and log on using your Azure account.
2. In the VIRTUAL MACHINES tab, select **Add**.



3. Provide necessary info and select the **Review + create** button to create the virtual machine

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription ⓘ

* Resource group ⓘ
[Create new](#)

INSTANCE DETAILS

* Virtual machine name ⓘ

* Region ⓘ

Availability options ⓘ

* Image ⓘ
[Browse all images](#)

* Size ⓘ **Standard D2s v3**
2 vcpus, 8 GB memory
[Change size](#)

ADMINISTRATOR ACCOUNT

Authentication type ⓘ Password SSH public key

* Username ⓘ

* SSH public key ⓘ

Login with Azure Active Directory (Preview) On Off ⓘ

[Review + create](#) [Previous](#) [Next : Disks >](#)

When the virtual machine status changes from Starting (Provisioning) to Running, you can install HPDM.

[+](#) Add [🕒](#) Reservations [☰](#) Edit columns [🔄](#) Refresh | [🏷️](#) Assign tags [▶](#) Start [↺](#) Restart [■](#) Stop [🗑️](#) Delete [☰](#) Ser

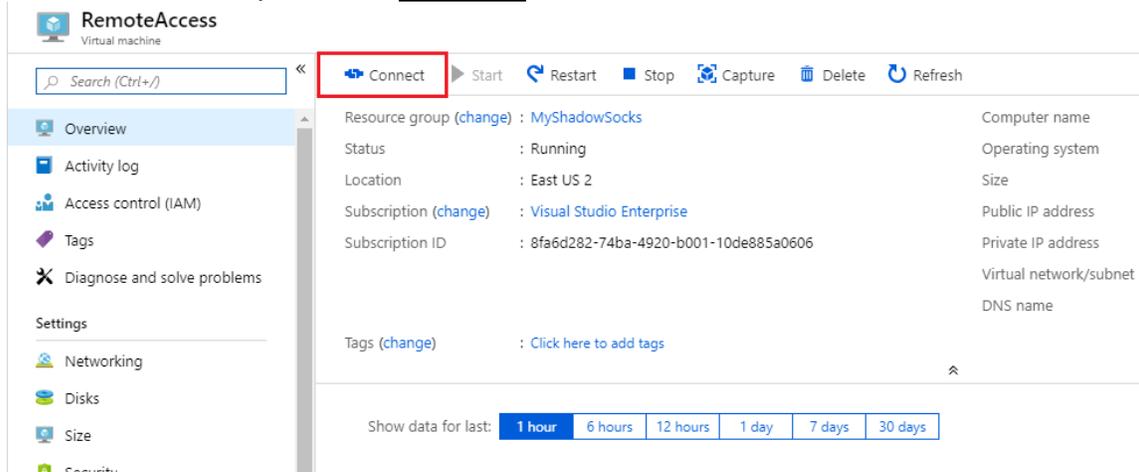
Subscriptions: Visual Studio Enterprise – Don't see a subscription? [Open Directory + Subscription settings](#)

1 items

<input type="checkbox"/>	NAME ↑↓	TYPE ↑↓	STATUS
<input type="checkbox"/>	RemoteAccess	Virtual machine	Running

Installing HP Device Manager 5.0

1. Select the virtual machine you created in [Creating an A](#), and then select **CONNECT**.



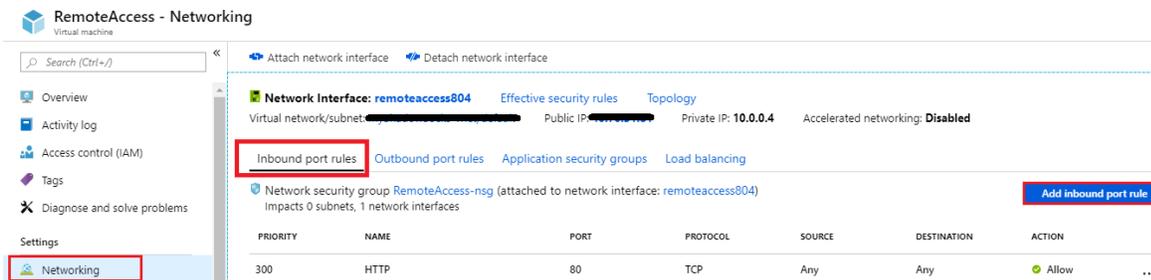
2. Save the RDP file your local system, and then use it to connect.
3. Upload the HPDM package to the virtual machine, and then install it. For instructions on installing HPDM, see the Installation section of this guide.

Configuring the firewall rules

By default, a virtual machine created in Azure is protected by the endpoint firewall. You must map the ports corresponding to HPDM to manage your device over the Internet.

To add a port to your firewall:

1. Select a virtual machine with HPDM installed to open the virtual machine properties page.
2. Navigate to **Networking** page, select **Inbound port rules** tab and select **Add inbound port rule**.



In the page that is displayed, input the name of your HPDM component, enter the **Destination port ranges** it uses, select **TCP** as **Protocol**, and then select **Add** to add the firewall rule

Add inbound security rule
✕

RemoteAccess-nsg

Basic

*** Source** ⓘ

Any

*** Source port ranges** ⓘ

*

*** Destination** ⓘ

Any

*** Destination port ranges** ⓘ

40000 ✓

*** Protocol**

Any

TCP

UDP

*** Action**

Allow

Deny

*** Priority** ⓘ

380

*** Name**

HPDM_Gateway ✓

Description

Add

3. Navigate to **Networking** page, select **Outbound port rules** tab and select **Add outbound port rule**. Follow step 2 to add outbound port rule.

RemoteAccess - Networking
⋮

Virtual machine

Attach network interface
Detach network interface

Network Interface: remoteaccess804 Effective security rules Topology

Virtual network/subnet: [redacted] Public IP: [redacted] Private IP: **10.0.0.4** Accelerated networking: **Disabled**

Inbound port rules
Outbound port rules
Application security groups
Load balancing

Network security group **RemoteAccess-nsg** (attached to network interface: **remoteaccess804**)

Impacts 0 subnets, 1 network interfaces

Add outbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow	...

Repeat step 2 and step 3 for every port that HPDM uses in your production environment. For more information about which ports HPDM uses, see the HP Device Manager 5.0 Admin Guide

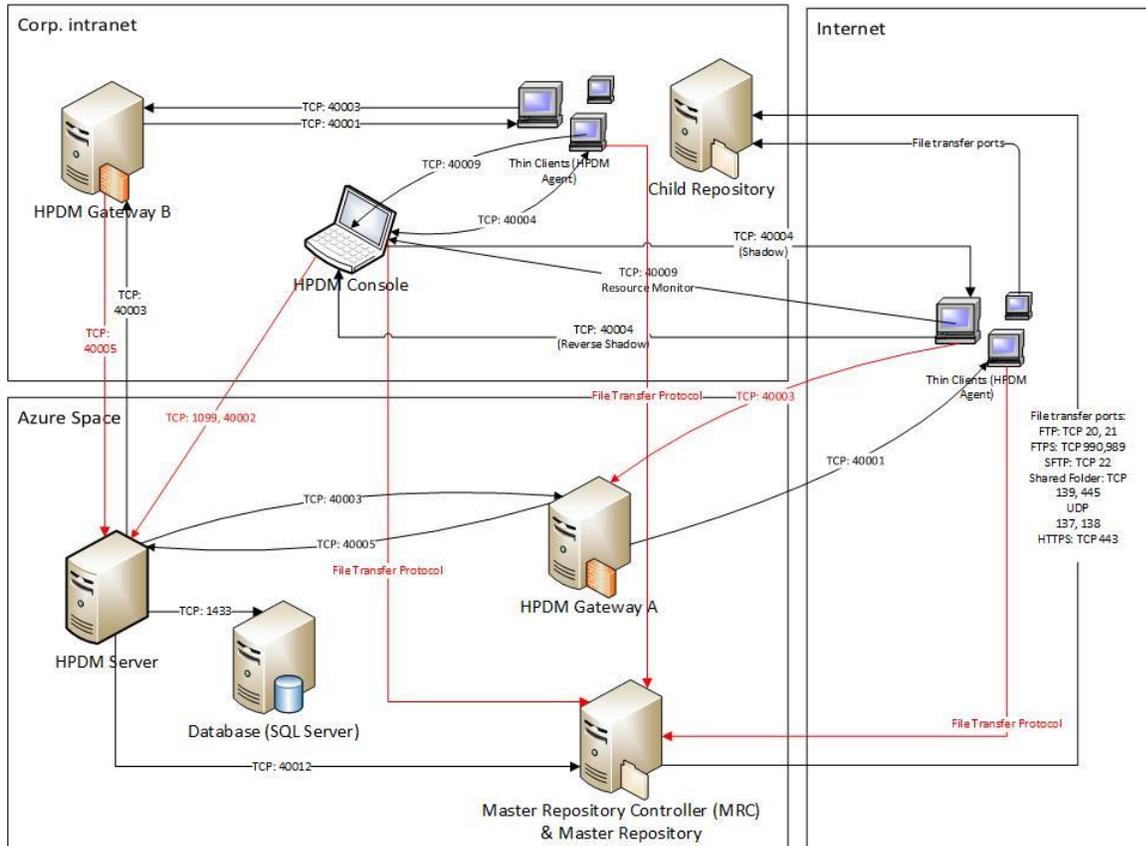
Sample scenario

Production environments are complex, diversified, and flexible. Use the following example to better understand port configuration in the cloud. This is a typical model with detailed configurations for reference.

Note

There might be firewalls between internet/intranet and Azure. Make sure that you have completed the procedure in **Configuring the firewall rules** to allow communication between your devices and the cloud.

Figure 7. Typical topography



All ports in red in the previous illustration must be added to the endpoint firewall.

HPDM HTTPS Repository

This section covers the installation and configuration of the HPDM HTTPS Repository, a component of the HP Device Manager (HPDM) solution. It also includes useful tips to fine-tune the performance of HPDM HTTPS Repository, such as how to implement bandwidth throttling.

Installation

Hardware environment

The following table provides the supported operating systems and both the minimum and recommended hardware requirements of HPDM HTTPS Repository.

Table 28. Supported operating systems

Operating system	Minimum hardware	Recommended hardware
Windows Server 2016 Windows Server 2019	Intel Core™ 2 or AMD Athlon 64 processor 2 GHz	Intel Core i5 quad-core processor 2.5 GHz or higher

Windows Server 2022	<ul style="list-style-type: none"> - 4 GB RAM - 2 GB free disk space - 100 Mbps NIC 	<ul style="list-style-type: none"> - 8 GB RAM - 20 GB free disk space - 1000 Mbps NIC
---------------------	--	--

Network environment

Many network factors might influence the deployment of the HPDM HTTPS Repository, such as network bandwidth or whether related devices are deployed on a subnet. HPDM HTTPS Repository must be deployed on the same system as either the HPDM Master Repository or a HPDM Child Repository. HP recommends deploying a HPDM Child Repository that has HTTPS support as close to its target devices as possible.

Installing HPDM HTTPS Repository

There are two ways to install HPDM HTTPS Repository, HP Device Manager installer and HPDM HTTPS Repository component installer. For detailed steps, see the **Installation** section. For the configuration about user, port and root path, see the section Configuration Center > HPDM HTTPS Repository.

Certificate configuration

HPDM HTTPS Repository and all HPDM components support only Privacy Enhanced Mail (PEM) format certificates and keys. For other certificate formats, such as .pfx and .der, you can use the openssl tool to convert the certificate to PEM format.

To use the openssl tool, go to <HPDM install path>\HP Device Manager\HTTPSRepository\Apache24\bin.

CA Certificate Trust List

In HPDM, the CA Certificate Trust List (CTL) is a file containing multiple certificates in PEM format. This file is used to verify peer certificates. The following is an example of a CTL file.



To verify a certificate, the CTL file must contain its CA certificates.

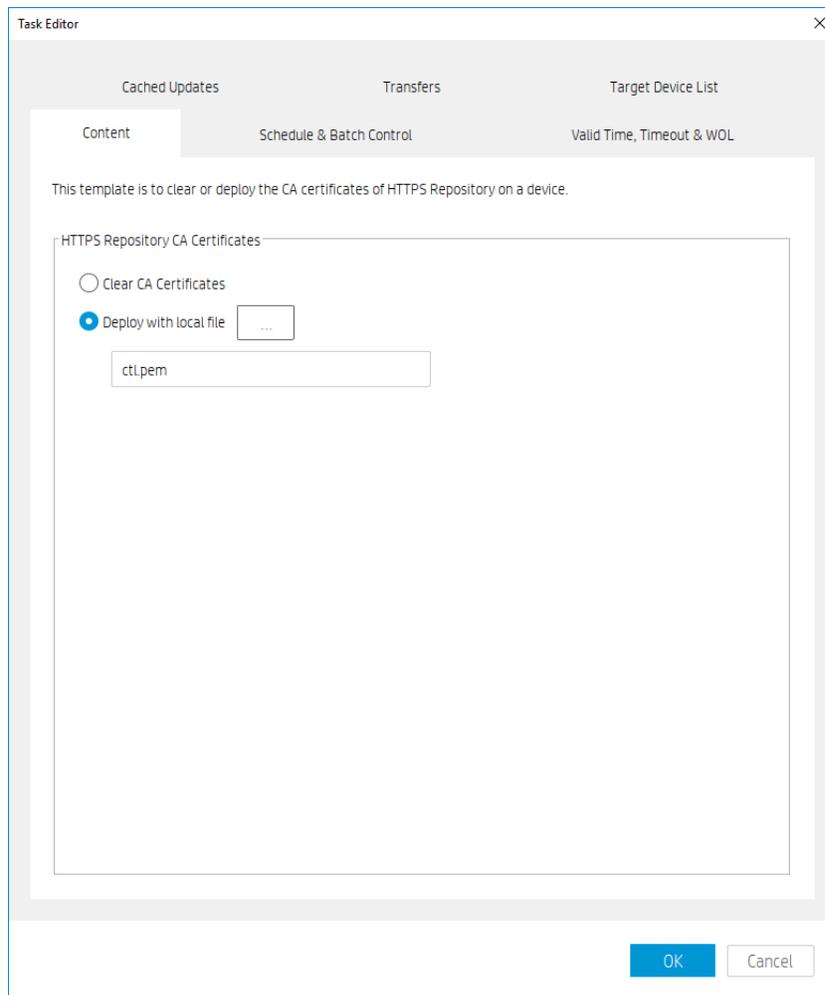
To create a CTL file:

1. If the certificate is a self-signed certificate, copy its PEM-format certificate content to the CTL file.
2. If the certificate is available in a CA chain, copy all CA certificates on the CA chain to the CTL file.
3. If you want to verify several certificates with one CTL file, repeat steps 1 and 2 to copy all CA certificates to one CTL file.

Deploying the CA CTL to HPDM

To verify the server certificate when HPDM components connect to HPDM HTTPS Repository, you must create a CTL file for your server certificate first, and then deploy this CTL file to HPDM components. Otherwise, HPDM does not authenticate the server certificate and accepts the connection automatically. In HPDM, the name of this CTL file is **ctl.pem** and cannot be changed.

1. For HPDM Console, HPDM Gateway, and HPDM Master Repository Controller, manually copy the **ctl.pem** file to %HPDMInstallPath%\Certificates\repos_certs\https\.
2. If the components are installed on separate machines, you need to copy it several to each system.
3. From HPDM Agent, send a **Set CA Certificates** template to each thin client. Select **Deploy with local file**, and then select the file **ctl.pem**.



Server certificate management

For server certificate management, refer to Configuration Center > HPDM HTTPS Repository .

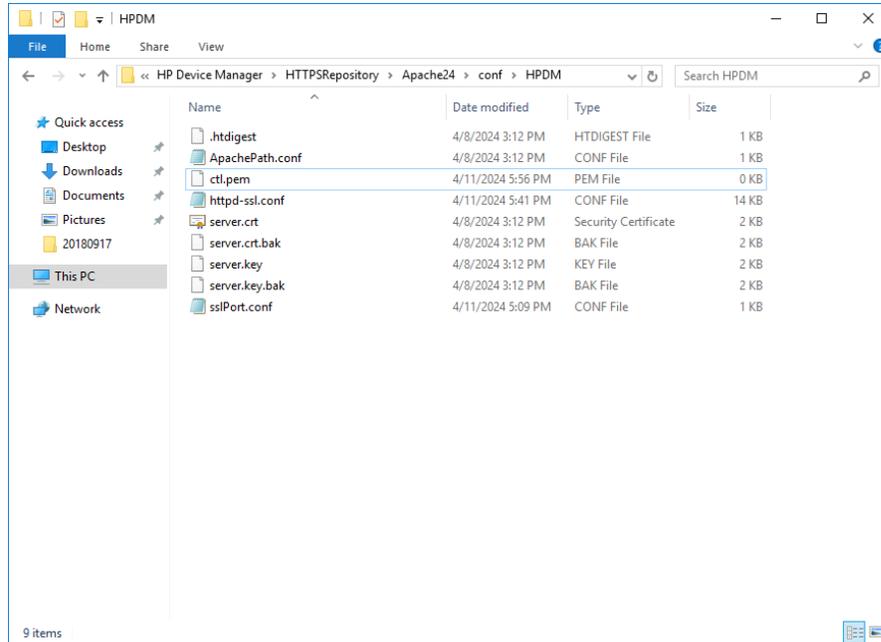
Client certificate management

There is no client certificate or key on the client side, by default. That means the client connects the HPDM HTTPS Repository directly.

Configuring client authentication on the HPDM HTTPS Repository side

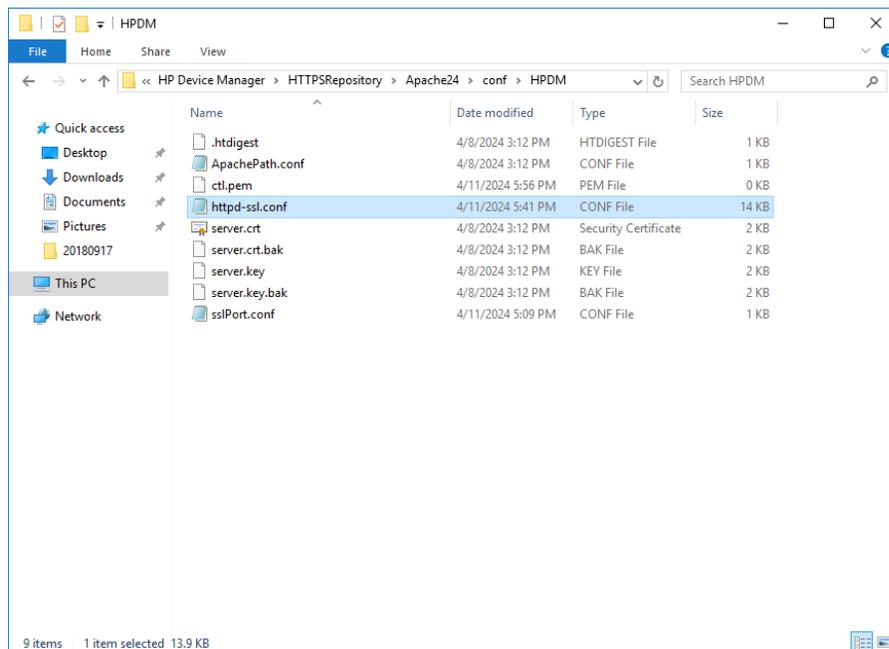
If your deployment requires to the server to verify the client certificate, use the following procedure:

1. Create a CTL file for the client certificate and copy it to <HPDM install path>\HP Device Manager\HTTPSRepository\Apache24\conf\HPDM. The CTL file name must be named **ctl.pem**.

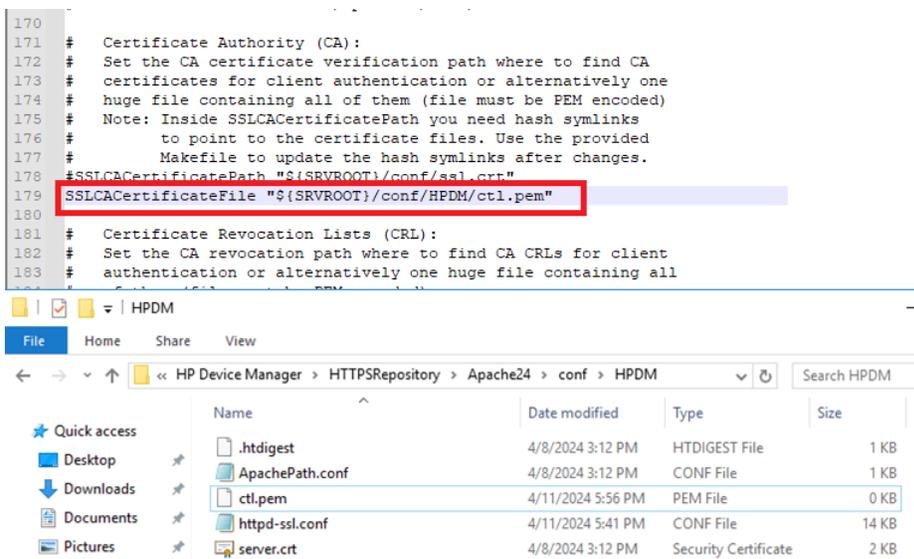


2. To configure the certificate authentication of HTTPS client, modify the SSL configuration on HPDM HTTPS Repository.

- a. Locate the file httpd-ssl.conf. By default, this file is saved in the following location:
<HPDM install path>\HP Device Manager\HTTPSRepository\Apache24\conf\HPDM



- b. Edit the configuration file. By default, the line SSLCACertificateFile is a comment. Modify so it is not a comment, and then save the file.



3. Restart the HPDM HTTPS Repository service.

Deploying a client certificate to HPDM components

1. Verify that the client certificate name is client.pem and the private key name is client.key.

Note

Currently, HPDM supports only PEM format certificates and keys. For other certificate formats, such as .pfx and .der, you can use the openssl tool to transfer them to PEM format.

2. To deploy the files to HPDM Console, HPDM Gateway and HPDM Master Repository Controller:

a. Copy client.pem and client.key to the folder %HPDMInstallPath%\Certificates\repos_certs\https\.

b. To deploy the password for the client key, open a command prompt, change the current path to %HPDMInstallPath%\Certificates\, and then run the command **dmenc <password> -h** where <password> is the password of the private key.

For example, if the password is HPDM, run the command **dmenc HPDM -h**.

3. To deploy the files to HPDM Agents running a Windows operating system:

a. Copy client.pem and client.key to the folder c:\windows\xpeagent\repos_certs\https\.

b. To deploy the password for the private key, send the following script task to the devices via HPDM:

```
c:\windows\xpeagent\dmenc <password> -h
```

4. To deploy the files to HPDM Agents running HP ThinPro:

a. Copy client.pem and client.key to the folder /etc/hpdmagent/repos_certs/https/.

b. To deploy the password for the private key, send the following script task to the devices via HPDM:

```
/usr/sbin/dmenc <password> -h
```

Performance

Many factors impact performance, such as disk, CPU, RAM size, and so on. The suggested minimum hardware only ensures HPDM HTTPS Repository can run on the computer, but minimum hardware might cause poor performance. HP recommends that you deploy HPDM HTTPS Repository on a computer with the recommended hardware requirement or higher. The following sections describe the performance with the recommended hardware and how to tune the configuration or hardware to achieve maximum performance.

Recommended performance data

The following performance data was obtained from a system running the recommended hardware configuration: 4 GB RAM, quad-core CPU, 1000 Mbps NIC, and 7200 RPM disk. The operating system used during testing was Windows Server 2012 R2.

Maximum number of connections

By default, the maximum number of connections is 64. This is an ideal value. The performance of HPDM HTTPS Repository degrades, if this number is raised too high for the supporting hardware configuration. For most configurations, HP recommends setting the number of concurrent connections to no more than 50.

Capturing large files and images

Due to the I/O speed of the storage device (hard disk), performance can be compromised when capturing large files or images from multiple thin clients at the same time. The following are the recommended usage parameters when capturing large files or images.

- The total upload speed must not exceed 10 MBps.
- The recommended maximum concurrent connections are 5, and the upload bandwidth for each connection must not exceed 2 MBps.

For example, if you want to capture images from 10 devices, you can send the capturing image task to 5 devices at first with the upload bandwidth set to 2 MBps. After those 5 tasks are finished, send the task to other 5 devices with the upload bandwidth set to 2 MBps.

For information about how to configure the bandwidth, see **Bandwidth throttling**.

Deploying large files and images

The following list provides the recommended usage parameters for deploying large files and images.

If you are deploying the same file, folder, or image file to multiple devices, do the following:

- If the number of target devices does not exceed 50, deploy the same file, folder, or image file to all devices at the same time.
- If the number of target devices exceed 50, divide the target devices into batches, with the number of devices in each batch fewer than 50. Then, send the task to the devices batch by batch. Do not send the task to next batch until all tasks in the previous batch are finished.

If you are deploying different files, folders, or image files to different devices, do the following:

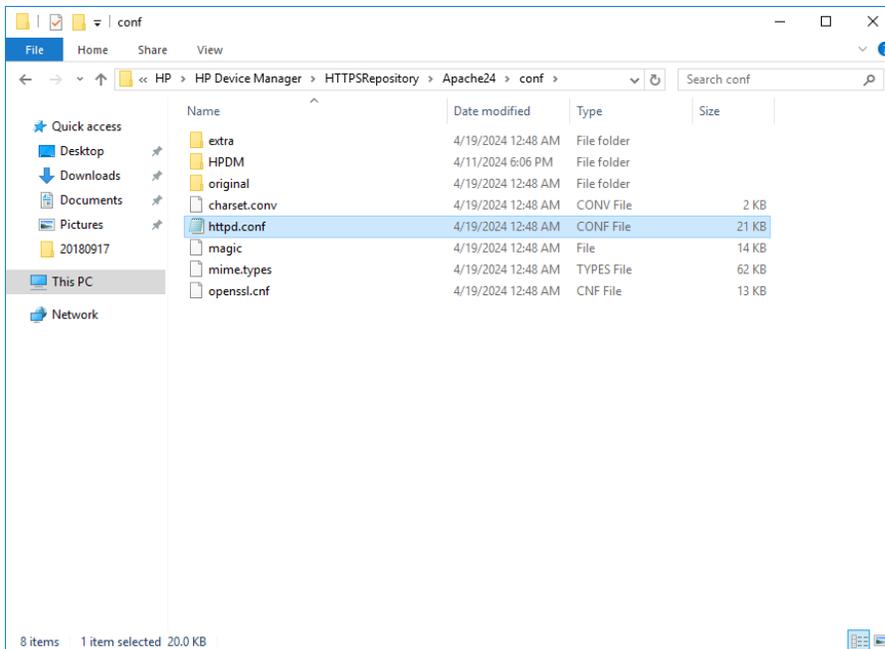
- Divide the target devices into different scenarios that would be used for targeting a single device. Execute each scenario one by one following the previous steps.

Managing the maximum number of connections

By default, the maximum number of connections is 64. If you installed HPDM HTTPS Repository on a more powerful machine, such as a workstation or server with greater disk I/O performance, you can modify this number to achieve the maximum performance of the hardware.

1. Locate the file `httpd.conf`. By default, it is saved in the following location:

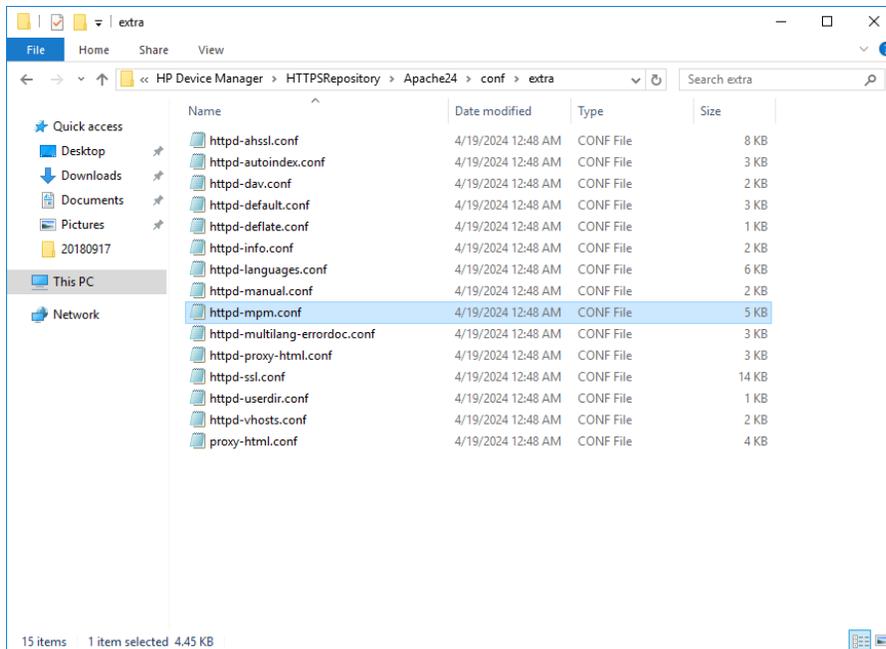
<HPDM install path>\HP Device Manager\HTTPSRepository\Apache24\conf



2. Edit the configuration file.
 - a. Locate the comment line `#Include conf/extra/httpd-mpm.conf`.
 - b. Remove the `#` so that the line is `Include conf/extra/httpd-mpm.conf`.
 - c. Save the file.

```
481 # Supplemental configuration
482 #
483 # The configuration files in the conf/extra/ directory
484 # included to add extra features or to modify the default
485 # the server, or you may simply copy their contents to
486 # necessary.
487
488 # Server-pool management (MPM specific)
489 Include conf/extra/httpd-mpm.conf
490
491 # Multi-language error messages
492 #Include conf/extra/httpd-multilang-errordoc.conf
493
494 # Fancy directory listings
495 Include conf/extra/httpd-autoindex.conf
496
```

3. Locate the file `httpd-mpm.conf`. By default, this file is saved in the following location:
<HPDM install path>\HP Device Manager\HTTPSRepository\Apache24\conf\extra



4. Edit the configuration file.

- a. Find the section WinNT MPM, and then go to the ThreadsPerChild command. By default, the value of ThreadsPerChild is 150. The reasonable value scope is 100–500. Enter a reasonable value for your hardware configuration.
- b. Save the file.

```

101
102 # WinNT MPM
103 # ThreadsPerChild: constant number of worker threads in the server process
104 # MaxConnectionsPerChild: maximum number of connections a server process serves
105 <IfModule mpm_winnt module>
106     ThreadsPerChild      250
107     MaxConnectionsPerChild  0
108 </IfModule>
109

```

5. Restart the HPDM HTTPS Repository service.

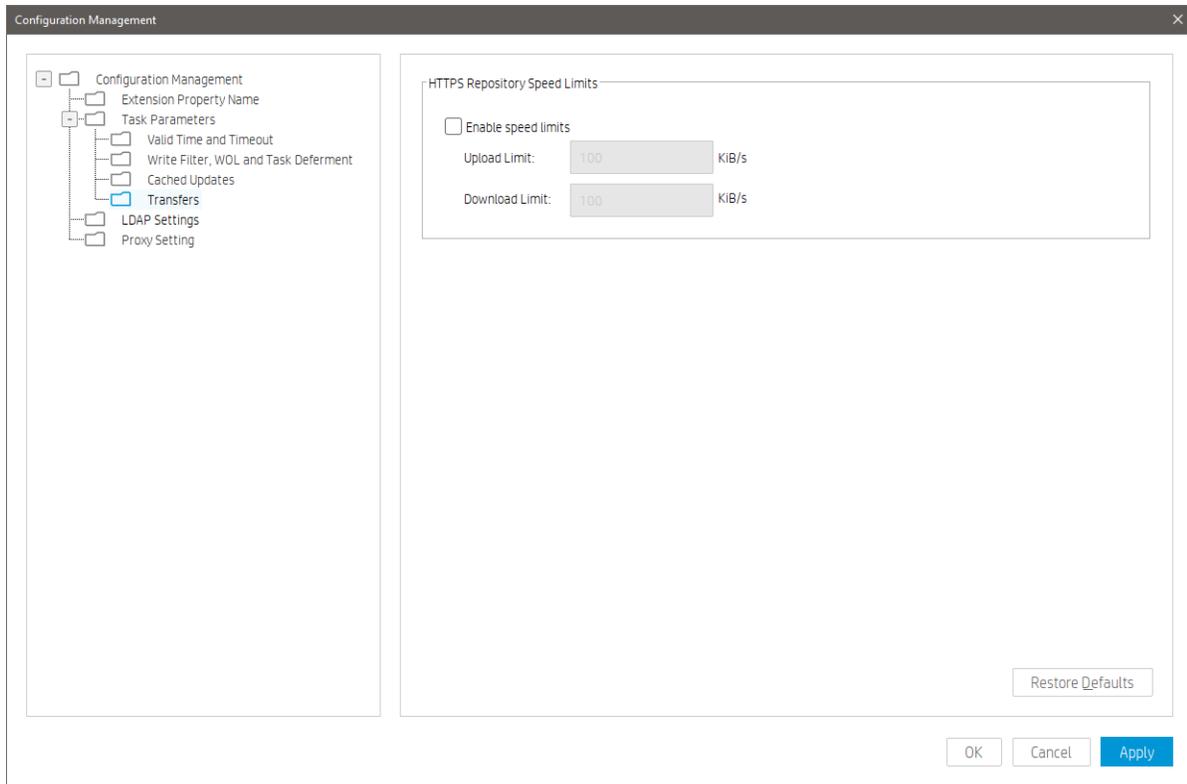
Hardware performance

The performance of the disk I/O is the key factor that impacts performance of the HPDM HTTPS Repository service. If the disk is a mechanical hard disk, the performance degrades when multiple clients are connected to the server and uploading and/or downloading large files simultaneously. In that scenario, the CPU usage generally shows high use and the file transfer speed decreases. To improve the performance, HP recommends using SDD or RAID disk storage.

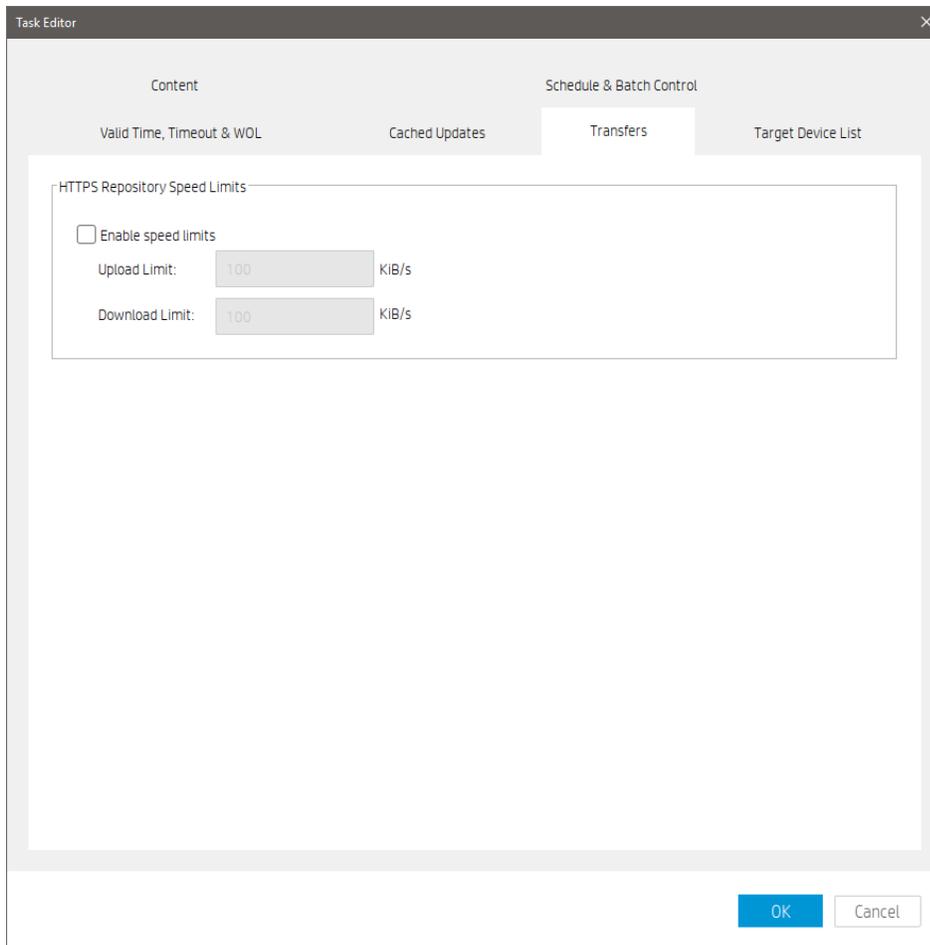
Bandwidth throttling

Administrators can configure bandwidth throttling for the HTTPS file transfer protocol. When logged in as the administrator, you can enable or disable the throttling feature, and you can set upload and/or download limits.

By default, the throttling function is disabled. After you enable the throttling function, the default value for the upload and download limits is 100 KiB/s each. You can set the upload and download limits to any value between 1 and 999999999 KiB/s.



For every task within HPDM related to payload transferring you can customize the bandwidth throttling parameters based on the global configuration.



Configuring the bandwidth throttling parameters

If you need to configure the bandwidth throttling parameters for all tasks, use the following procedure:

1. To open the Configuration Management dialog box, switch to **Administration** page, and then select **Configure System**.
2. Select **Task Parameters**, and then select **Transfers**.
3. Configure the bandwidth throttling parameters for global settings.

To configure bandwidth throttling for a single task related to payload transferring:

1. Right-click the template, and then select **Send Task**.
2. On the **Transfers** tab in the Task Editor dialog box, configure the bandwidth throttling parameters for a single task.

Automated update Apache, PHP, and OpenSSL

Please refer to [Security Updates](#).

FTP Repositories

Overview

This document contains the following parts:

- Configuration of an IIS FTP server
- Configuration of FTP over SSL
- Configuration of a FileZilla FTP server

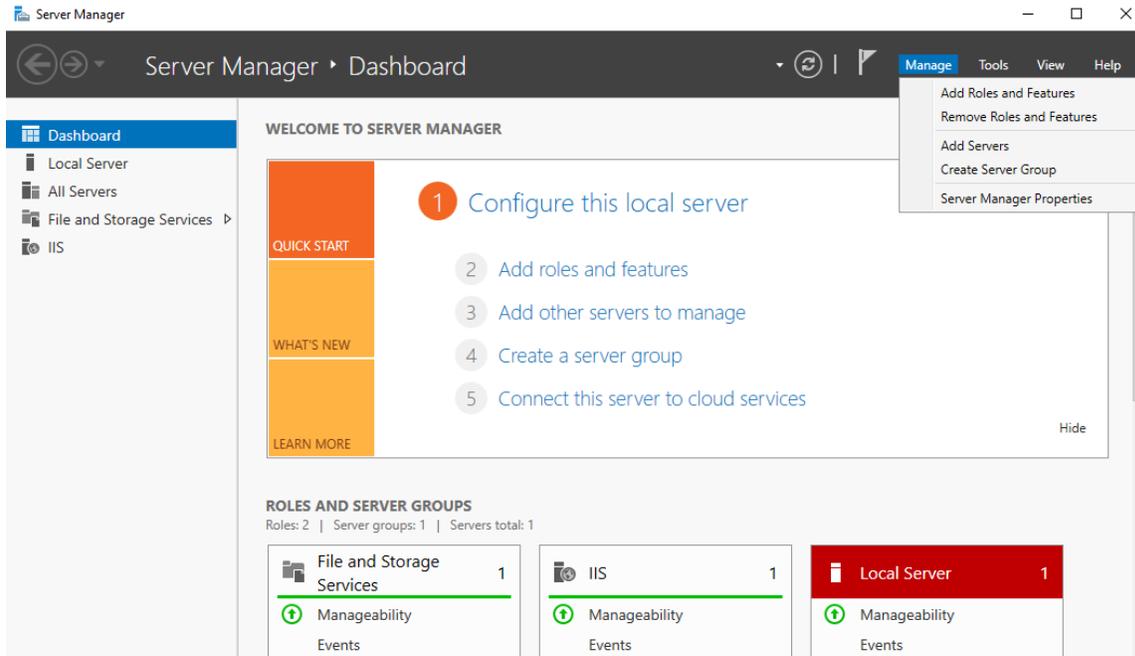
IIS FTP server configuration

Installing FTP for IIS

If the FTP service is not already installed on the server, follow these steps to add the service. Otherwise, see [Creating an FTP site with basic authentication](#).

Select **Start > Windows Administrative Tools > Server Manager**.

In the Server Manager, select **Manage**, and then select **Add Roles and Features** to open the Add Roles Wizard.



3. Select **Server Roles**, select **Web Server (IIS)**, and then select **Next**.
4. Select **Next**.
5. On the Select Role Services page, expand the **FTP Server** option. Then, select **FTP Service**.
6. Select **Next**.
7. On the Confirm Installation Selections page, select **Install**.
8. On the Results page, select **Close**.

Creating an FTP site with basic authentication

This section details how to create a new FTP site to which the HP Device Management (HPDM) Server, as well as the HPDM Agents, can connect for read and write access using basic authentication. Before creating this site, ensure that you create a user account from which the FTP service can authenticate. This example uses a local user account with the username `hpdmdm`.

To create the FTP site:

1. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the Connections pane of the IIS Manager, expand the root server node, and then select the **Sites** node.
3. In the Actions pane, select **Add FTP Site**. Or, right-click the **Sites** node in the Connections pane and select **Add FTP Site** from the pop-up menu. The Add FTP Site wizard opens.
4. On the Site Information page, enter a name for the FTP site, and select a path on the local system to use as the content (or root) directory. This example uses the site name `HPDM-Repository` and the root path `C:\inetpub\ftproot`.

**Site Information**

FTP site name:

Content Directory

Physical path:

Note

Ensure that the user account used for HPDM FTP transactions has sufficient rights to allow reading, writing, and directory listing on the folder selected for the content (or root) directory.

5. Select **Next**.
6. On the Binding and SSL Settings page, enter or modify the details for your configuration. This example uses the default values for IP Address and Port, All Unassigned and 21 respectively.

**Binding and SSL Settings**

Binding

IP Address: Port:

Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

Start FTP site automatically

SSL

No SSL

Allow SSL

Require SSL

SSL Certificate:

Note

For information about configuring a Secure Sockets Layer (SSL) FTP, see **Error! Reference source not found.**

7. Select **Next**.
8. On the Authentication and Authorization Information page, select the **Basic authentication** option. Under Allow access to, select **Specified users** and enter the username of the account that you created for HPDM FTP transactions. Under Permissions, select both **Read** and **Write**.

**Authentication and Authorization Information**

Authentication

Anonymous

Basic

Authorization

Allow access to:

Specified users

hpdmadmin

Permissions

Read

Write

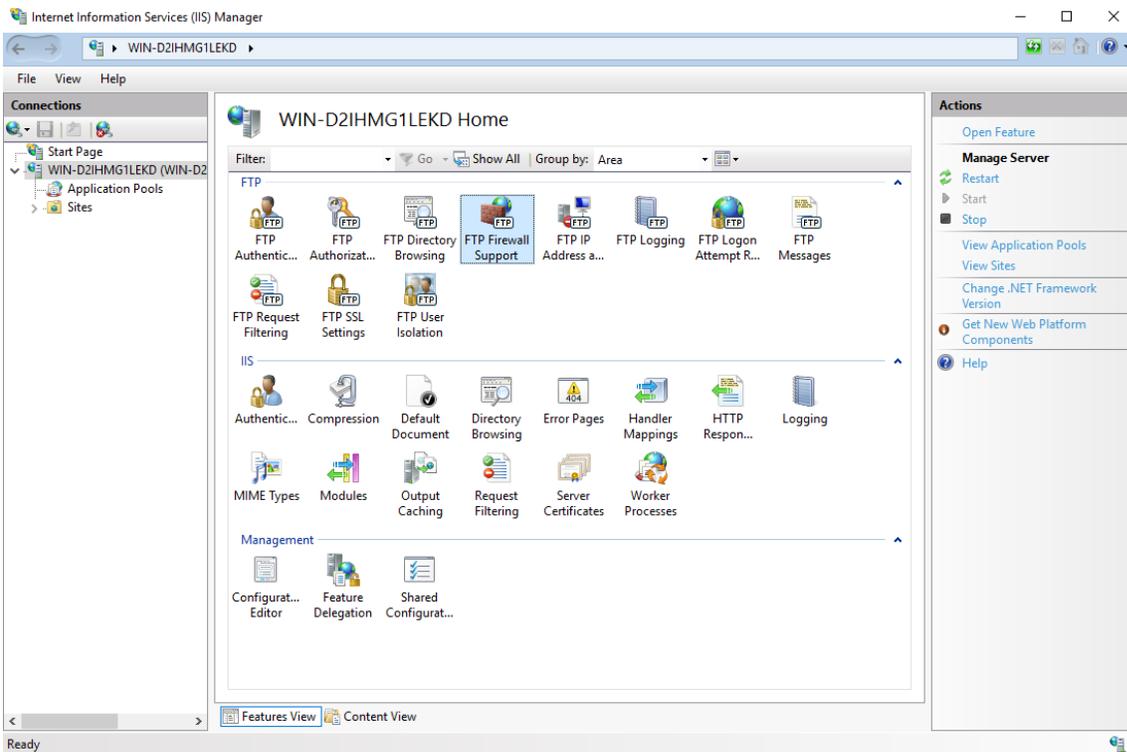
Previous Next Finish Cancel

9. Select **Finish**.*Configuring the passive port range for the FTP service*

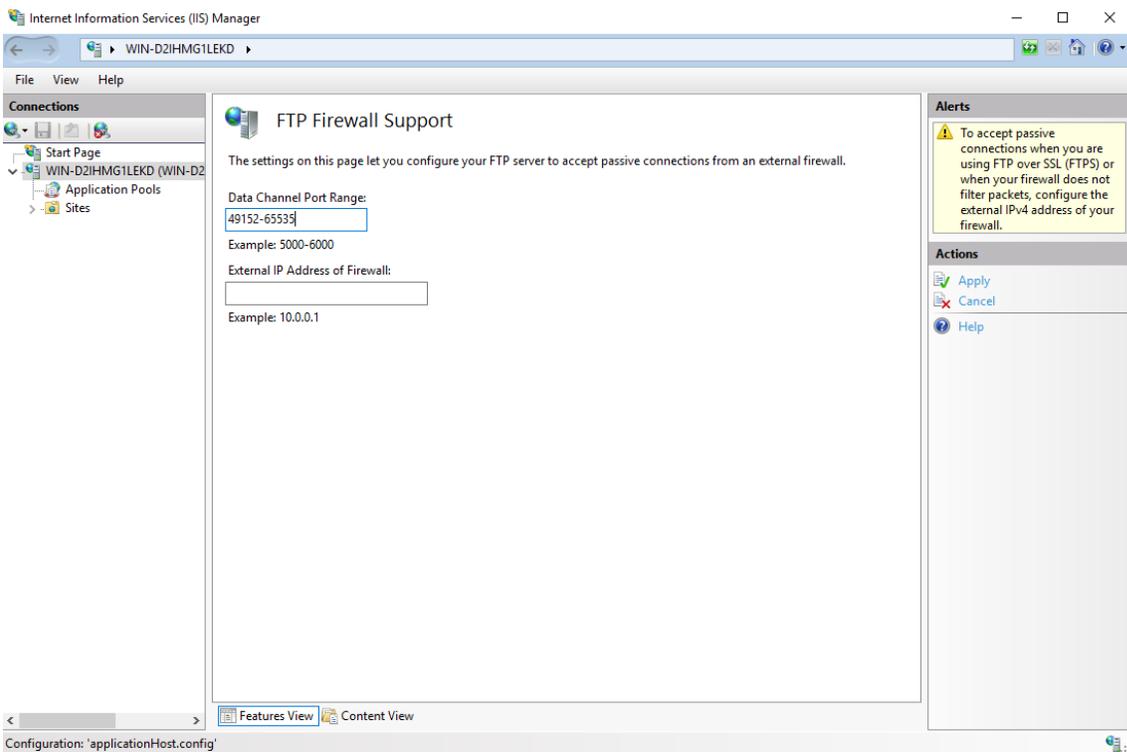
This section details how to configure the server-level port range for passive connections for the data channel from devices. Although the FTP client used by the HPDM Agent on the devices supports both active and passive modes for the data channel, the passive mode enables the device to initiate both control and data connections to the server, preventing a firewall from filtering the incoming data port connection to the device from the server. However, to support a firewall on the server, a passive port range needs to be specified, and the server's firewall must be configured to allow traffic on this port range.

To configure the passive port range:

1. Select **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the Connections pane, select the server-level node, and then select the **FTP Firewall Support** icon.



3. Enter a range of values in the **Data Channel Port Range** box. The valid range for ports is 1024 through 65535. Ports from 1 through 1023 are reserved for use by system services. This example uses the port range of 49152–65535.



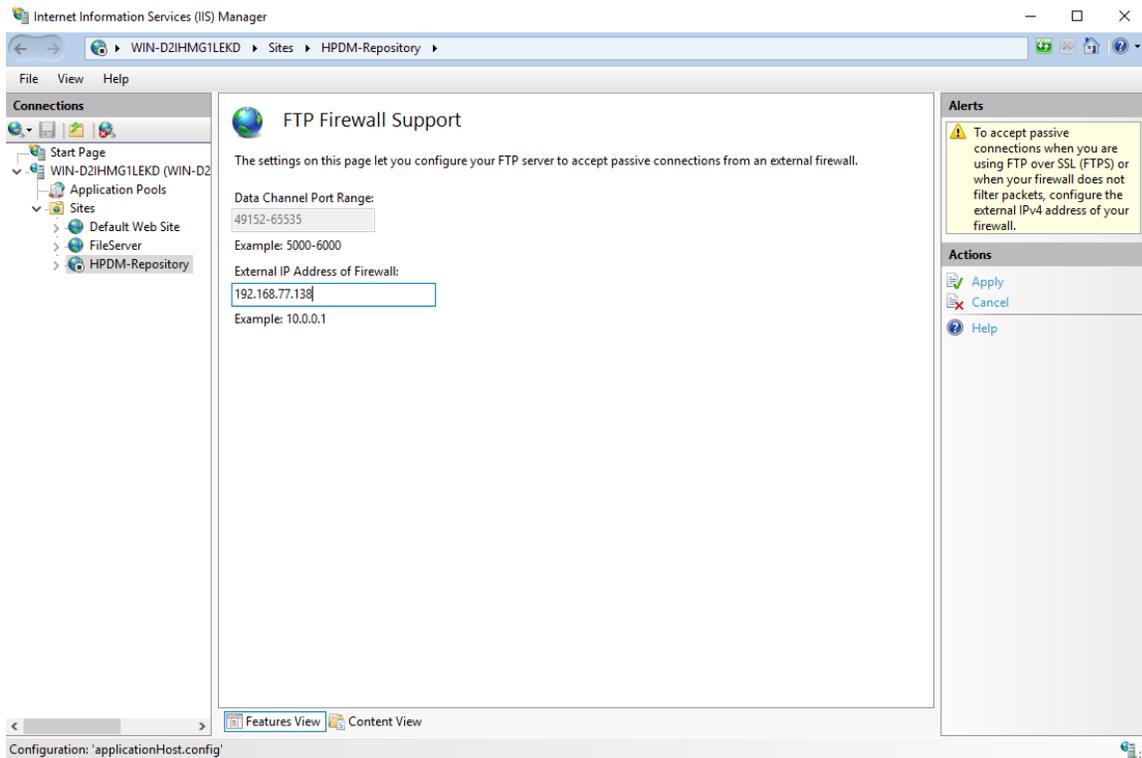
4. In the Actions pane, select **Apply**.
5. A warning message indicating that the ports need to be added to the server firewall might appear. For information on how to add the ports, see **Error! Reference source not found.** Select **OK**.

Configuring the external IPv4 address for the FTP site

You must specify the external address of the firewall (in most cases, this is just the IP address of the server itself) in the FTP site configuration to accept passive connections when the Windows Firewall is enabled.

To configure the external IPv4 address for the FTP site:

1. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the Connections pane, expand the **Sites** node, select the FTP site you created earlier, and then select the **FTP Firewall Support** icon.
3. Enter an IP address in the **External IP Address of Firewall** box. In this example, the IP address is the address of the server itself.



4. In the Actions pane, select **Apply**.

Windows Firewall settings for FTP

In Windows Server 2016, the built-in firewall service helps secure your server from network threats and is enabled by default. If you use the built-in Windows Firewall, you need to configure your settings so that the HPDM and FTP traffic can pass through the firewall. Note that you need to be logged on as Administrator or as a user that has administrator privileges to configure the firewall.

You must configure an exception for both the control channel (port 21) and the port range for the passive data channel. This can be done in the GUI for the Windows Firewall, but it is easier to add these rules from the command line.

To configure the Windows Firewall setting for FTP using the command line:

1. Select **Start > All Programs > Accessories > Command Prompt**. If not logged on as Administrator, be sure to right-click **Command Prompt** and select **Run as Administrator**. This is required because User Account Control (UAC) in the Windows Server 2016 operating system prevents non-Administrator account access to the firewall settings.
2. To add an inbound rule for the command channel and to allow connections to port 21, enter the following command and then press **Enter**:

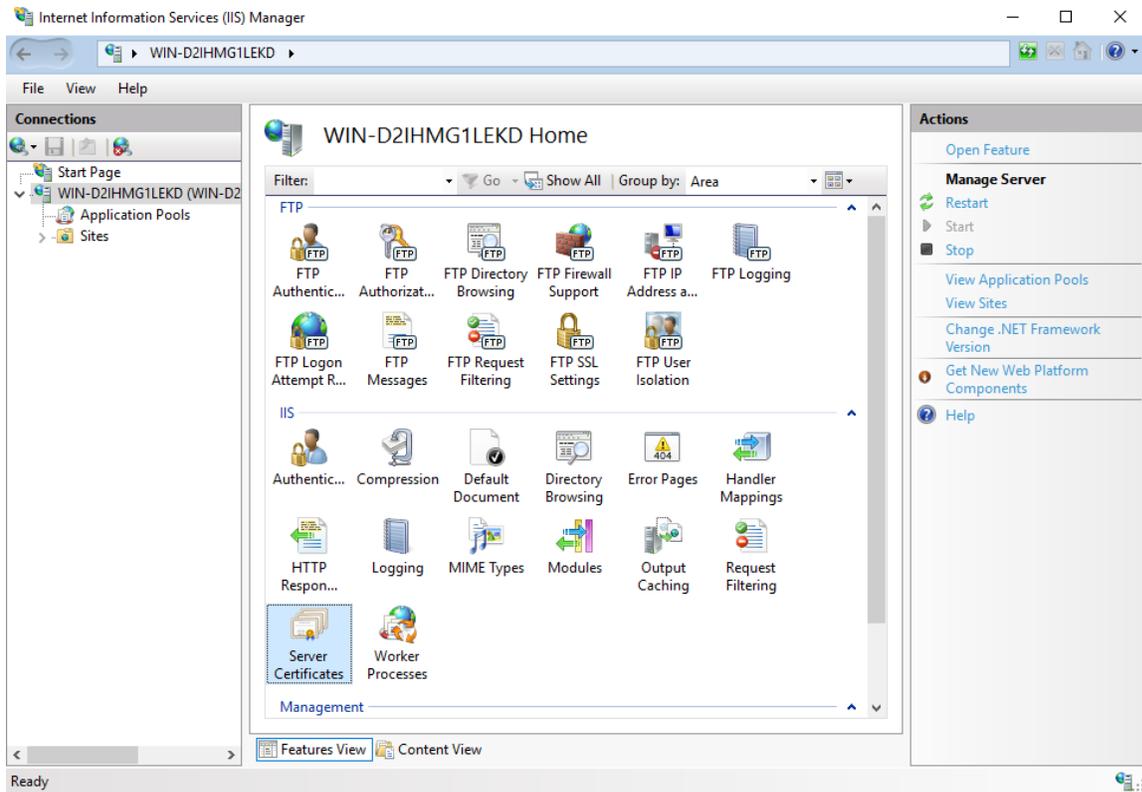
```
netsh advfirewall firewall add rule name="FTP (non-SSL)" action=allow protocol=TCP dir=in localport=21
```
3. To disable stateful FTP filtering so that Windows Firewall does not block FTP traffic to the passive port range, enter the following command and then press **Enter**:

```
netsh advfirewall set global StatefulFtp disable
```

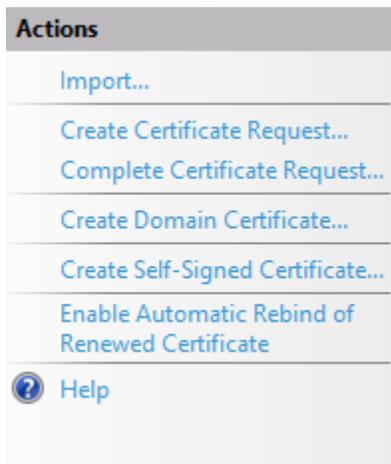
Configuring HPDM to use FTPS

Configuring Microsoft IIS & FTP

1. Open **IIS Manager** on Windows Server 2016 (IIS 10).
2. In the Server Manager, select your server, and then select **Server Certificates**.



3. Select **Create Self-Signed Certificate**.



4. Enter the common name for the certificate and select **OK**.



Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

Select a certificate store for the new certificate:

OK

Cancel

5. Enter the **FTP site name** and select the **Physical path**. Select **Next**.

6. Select **Require SSL** and then select the **SSL Certificate** you created. Enter 990 in the **Port** box. Select **Next**.

**Binding and SSL Settings**

Binding

IP Address: Port:

Enable Virtual Host Names:
Virtual Host (example: ftp.contoso.com):

Start FTP site automatically

SSL

No SSL
 Allow SSL
 Require SSL

SSL Certificate:

7. Select **Basic**. Under Allow access to, select **Specified users** and enter the name of the FTP user group. Under Permissions, select both **Read** and **Write**. Select **Finish**.



Authentication and Authorization Information

Authentication

Anonymous

Basic

Authorization

Allow access to:

Specified users

hpdmadmin

Permissions

Read

Write

Previous Next Finish Cancel

Configuring HPDM FTPS

1. Log on to the HPDM Console.
2. Select **Gateways & Repositories** Page and navigate to **Repositories** panel
3. Add new repository or select existing repository to open the **Repository Configuration Wizard**
4. In the **Protocol Settings** page, check **FTP/FTPS** option

Initialization Steps

- Basic Information
- Protocol Settings**
- HTTPS
- FTP/FTPS
- Summary

Protocol Settings

Please select at least one protocol below for the current repository:

- HTTPS
- FTP/FTPS**
- SFTP
- SMB v2

i Note: SMB v2 is required for capturing images from or deploying images to Windows device that do not have enough available space to hold the image file.

< Back **Next >** Finish Cancel

5. Select **Enable FTP over TLS support (FTPS)** in the **FTP/TPS Protocol Setting** page and select **Next**.

Repository Configuration Wizard

Initialization Steps

- Basic Information
- Protocol Settings
- HTTPS
- FTP/FTPS**
- Summary

FTP/FTPS Protocol Settings

During installation of the Master Repository a "Repository" folder is created. You should see a "Repository" directory in the URL below if the Master Repository is configured correctly.

- Enable FTP over TLS support (FTPS)**

Port: 990

Username: test

Password: ****

URL: ftps://192.168.77.132/

< Back **Next >** Finish Cancel

6. Select **Test Repository** in the **Summary** page to verify that it connects over FTPS.

Initialization Steps

- Basic Information
- Protocol Settings
 - HTTPS
 - FTP/FTPS
 - Summary

Summary

Use the Test Repository button below to validate the protocol settings for this Repository. Test results will be reflected on this page.

Protocol	Port	URL	Username
HTTPS	443	https://192.168.77.1	admin
FTPS	990	ftp://192.168.77.1	test

Test Result

Test Repository

< Back
Next >
Finish
Cancel

7. Send an **Update Agent** task to ensure that FTPS is working properly.

FileZilla FTP server configuration

FileZilla is free, open-source, cross-platform FTP software, consisting of FileZilla Client and FileZilla Server. You only need to download, install, and configure FileZilla Server.

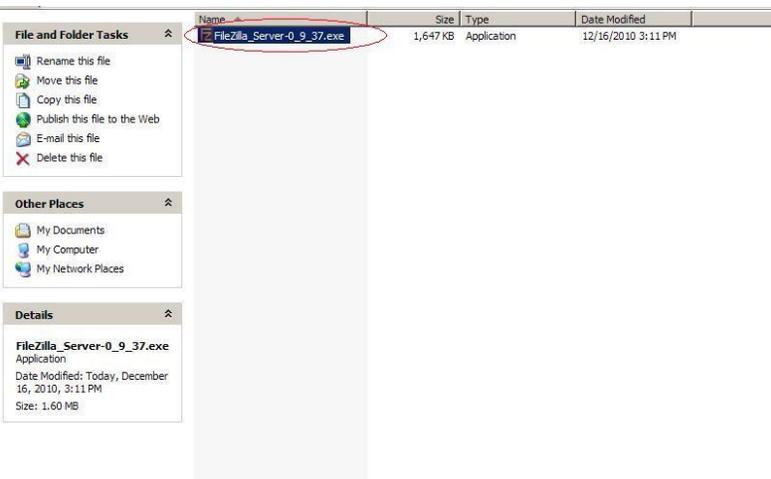
1. Go to <http://filezilla-project.org/>. Select **Download FileZilla Server**.

The screenshot shows the FileZilla website homepage. The main heading is "FileZilla The free FTP solution". Below the navigation menu, there is an "Overview" section with a welcome message and support information. The "Quick download links" section contains two buttons: "Download FileZilla Client" (All platforms) and "Download FileZilla Server" (Windows only). A red arrow points to the "Download FileZilla Server" button. Below this, there is a "News" section with a link to "2010-11-21 - FileZilla Client 3.3.5.1 released" and a "Bugfixes and minor changes:" section.

2. Select your Windows platform.



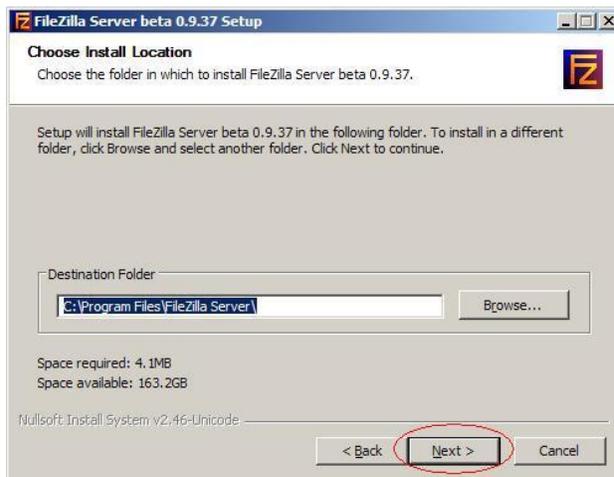
3. Download this file to the specified location of the server system, and then select this file to install it.



4. Select **I Agree**.

5. Select **Next**.

6. Select the **Destination Folder**, and then select **Next**.

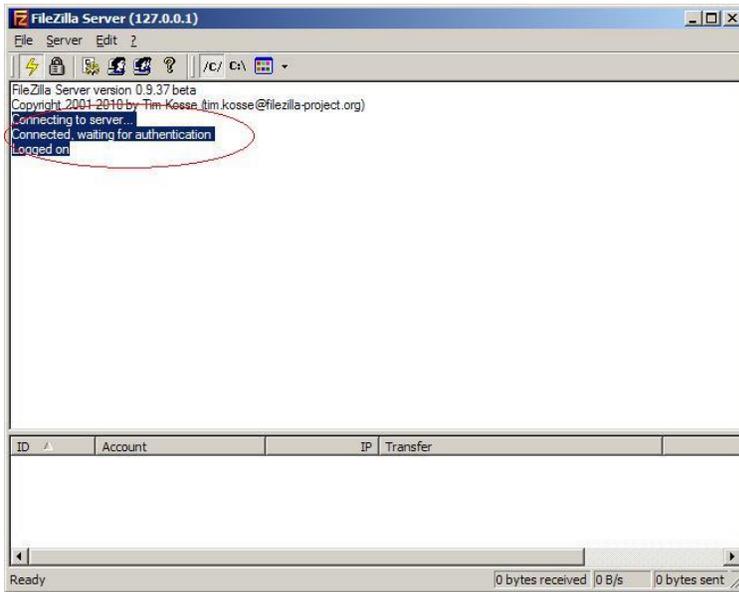


7. Select **Next**.

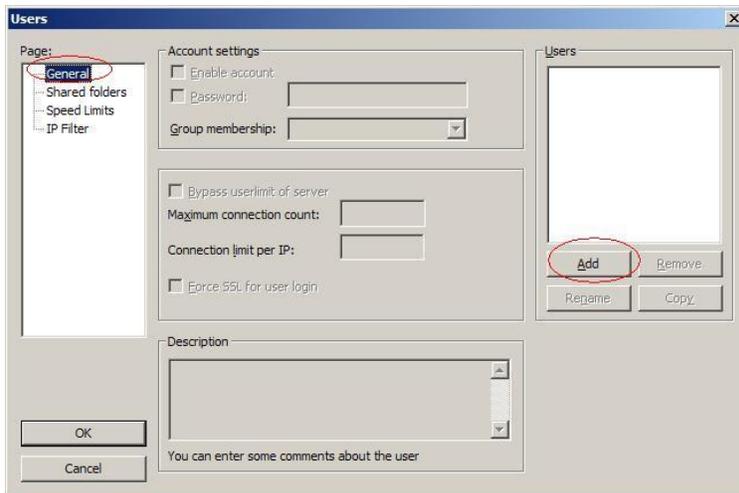
8. Select **Install**.

9. After the installation is complete, select **Close**.

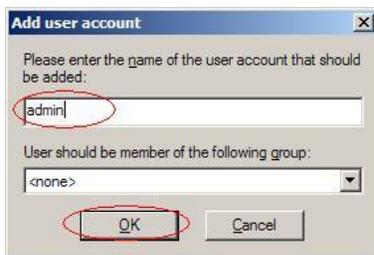
10. Open the FileZilla Server dialog.



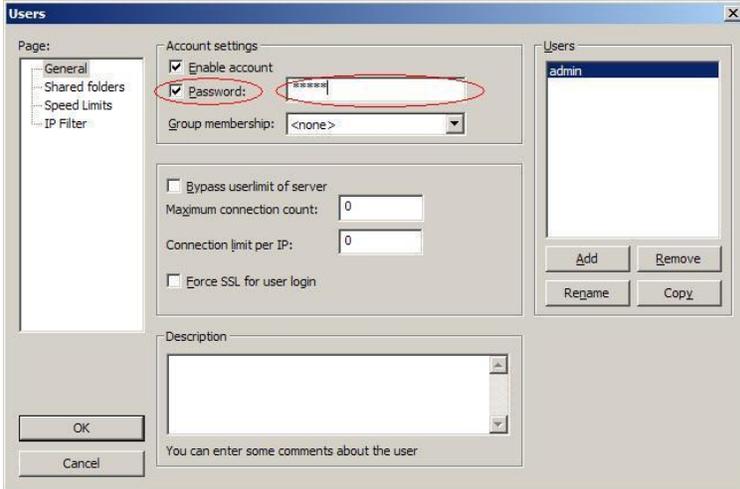
11. Select **Edit > Users** to open the Users dialog. Select the **General** page, and then select the **Add** button to add a user.



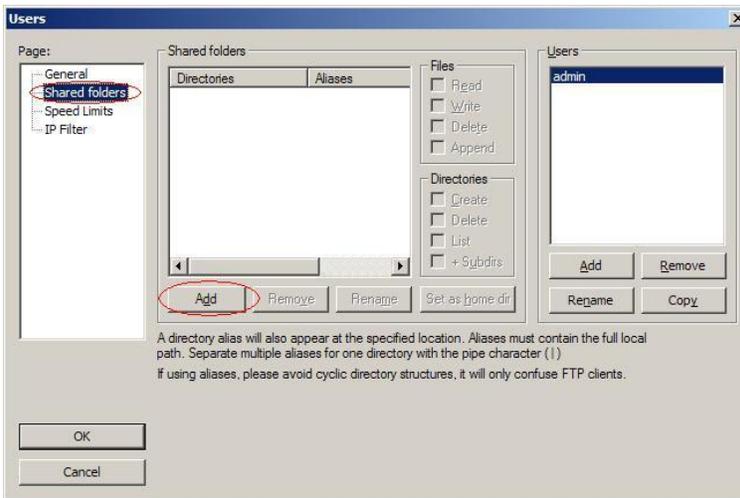
12. Enter a username, and then select **OK**.



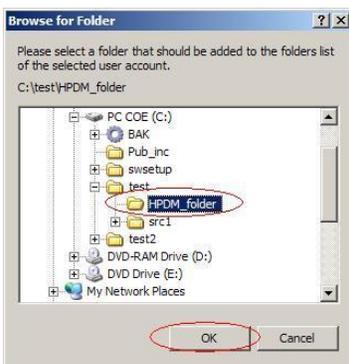
13. Select the **Password** option, and then enter a password.



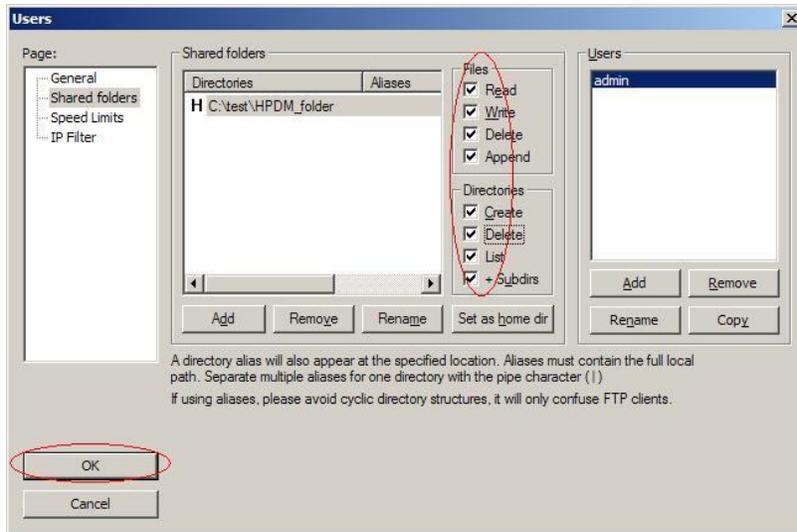
14. Select the **Shared folders** page, and then select the **Add** button to add a shared folder.



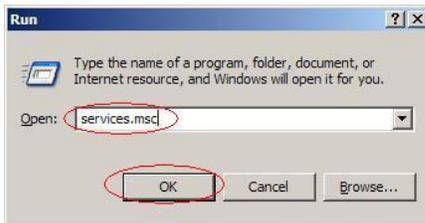
15. Select the Shared Folder, and then select **OK**.



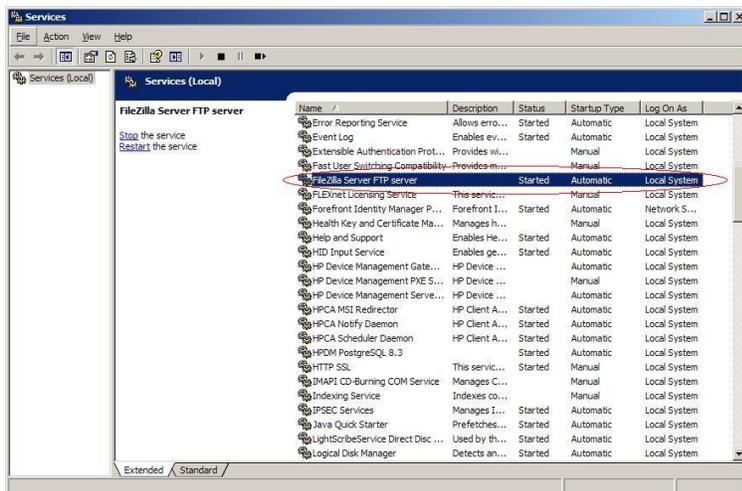
16. In the User dialog, select the **Read**, **Write**, **Delete**, and **Append** options in Files panel, select the **Create**, **Delete**, **List**, and **+ Subdirs** options in Directories panel, and then select **OK**.



17. The FTP server is now created. Verify this FTP service by entering `services.msc` in the Windows Run dialog.



The FileZilla Server FTP server is started.



For more information

To read more about installing and configuring FTP on IIS, go to <http://www.iis.net/learn/install/installing-publishing-technologies/installing-and-configuring-ftp-7-on-iis-7>.

For more information about using FTP Over SSL, go to <http://www.iis.net/learn/publish/using-the-ftp-service/using-ftp-over-ssl-in-iis-7>.

Mutual authentication between console and server

Before HPDM 5.0.4, communication between console and server did not require client authentication. Since HPDM 5.0.4, mutual authentication between console and server has been introduced to enhance the security for the RMI communication over SSL. The mutual authentication requires console to get **rmiclient.jks** generated on server side for client authentication. Otherwise, connection between console and server cannot be established. HPDM Server generates **rmiserver.jks** and **rmiclient.jks** on first start.

Connecting to a remote server

Before you login, copy **rmiclient.jks** from the remote server (under the folder “<HPDM installation folder>\Server\bin”) to the console’s folder “<HPDM installation folder>\Console\lib”.

Note1: If there already exists “<HPDM installation folder>\Console\lib\rmiclient.jks”, it should be overwritten during copying because the existing one does not work.

Note2: If the local server is installed, please either delete **rmiclient.jks**, **rmiserver.jks** generated the local server or overwrite them with those from the remote server.

Note3: Restarting the console is required to make the copied file take effect.

Connecting to the local server

Console will automatically fetch **rmiclient.jks** from the server’s folder on login.

Note1: Use “run as administrator” to run console to log in for once to write **rmiclient.jks** under its folder, in case that console does not have enough write privilege under non-admin accounts.

Note2: Please make sure console and server are in the same installation location. If they are installed separately, console will fail to automatically fetch **rmiclient.jks**. In this case, manually copying the file from the server’s folder is required.

Reset **rmiclient.jks** and **rmiserver.jks**

For any security concern, these two files can be reset easily by deleting them under the server’s folder “<HPDM installation folder>\Server\bin”. After restarting server, new **rmiclient.jks** and **rmiserver.jks** will be generated. Please refer to **Connecting to a remote server** to refresh **rmiclient.jks** on console side.

Use the same pair of **rmiclient.jks** and **rmiserver.jks** for multiple servers

If multiple servers are used, please generate **rmiclient.jks** and **rmiserver.jks** by one server and copy them to the folder “<HPDM installation folder>\Server\bin” of the rest servers. Therefore, all servers and consoles can use the same pair of **rmiclient.jks** and **rmiserver.jks** for mutual authentication.

Use one-way authentication

HPDM 5.0.4 is still compatible with the old authentication method before HPDM 5.0.4. Before HPDM 5.0.4, authentication was not required. Therefore, console does not need to get **rmiclient.jks** generated on server side. To disable client authentication and use one-way authentication, please follow the below steps:

1. Modify “<HPDM installation folder>\Server\conf\server.conf”. At the last line of the file, append “**hpdm.rmi.needClientAuth=false**”. Then restart the HPDM Server service.
2. Use console to log in to server as before.

Operation

Management Console

The Device Manager Console acts as the focal point for device management orchestration within your environment. Multiple administrators can be connected simultaneously to a single HPDM Server through local console interfaces, each observing a customizable and tailored view of the device management framework.

Logging into the Console

To launch the HPDM Console:

Select 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**.

The different installation options create different first-time login experiences:

- For Complete Installation:
The first log in to the Console requires a password. After the Console initializes, the system prompts you to change the password.

Note

The first Console initialization might require extra time.

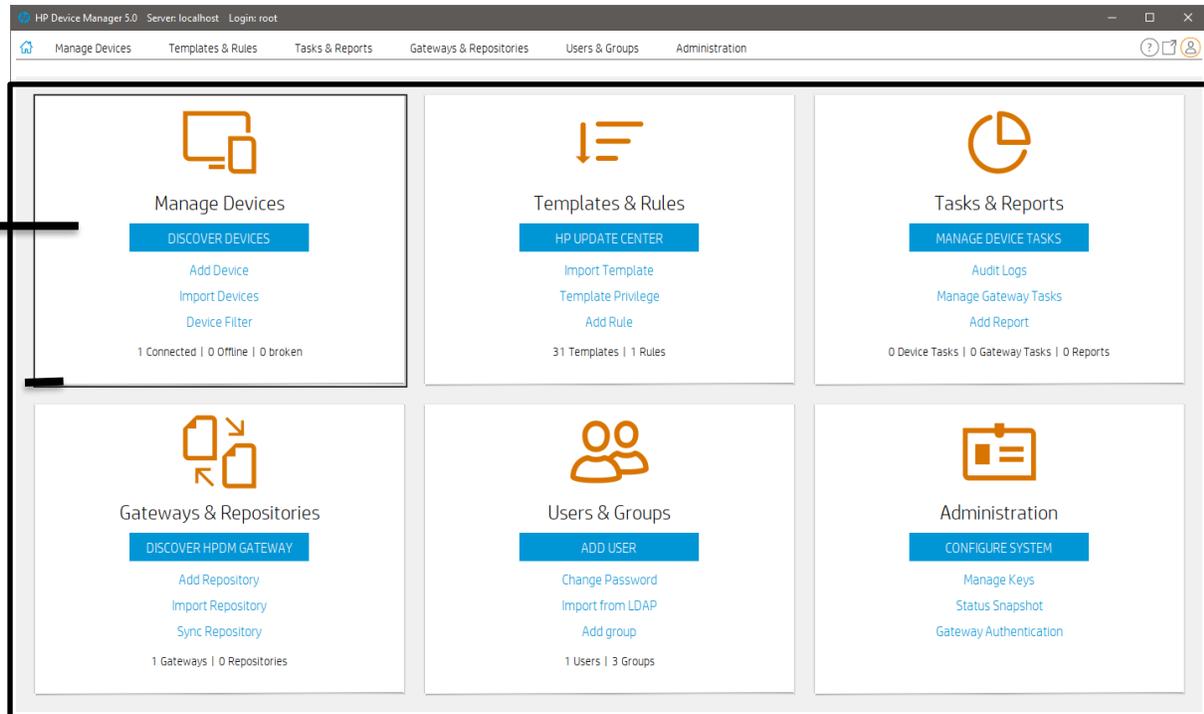
- For Custom Installation:

Type the host name or IP address, type the user name and password for HPDM Server, and then select **OK**.

Note

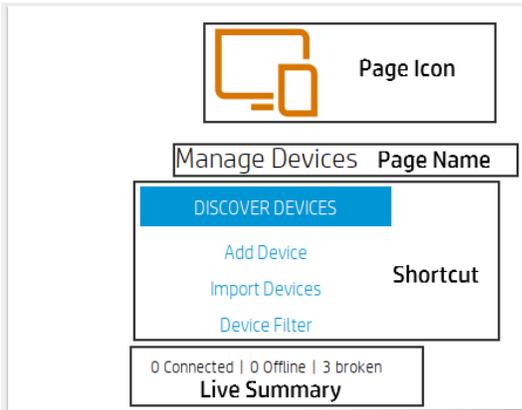
If HPDM Console is installed on the same system as HPDM Server, enter localhost.

The homepage



1. Homepage—Summary view of all management pages within the HPDM Console.

2. Tile—Each tile maps to a management page and contains an icon, name, shortcuts within each management page, and contextual live summary information.



Page Icon and Page Name—After selecting a tile’s icon or name, the console locates and maximizes the specified page.

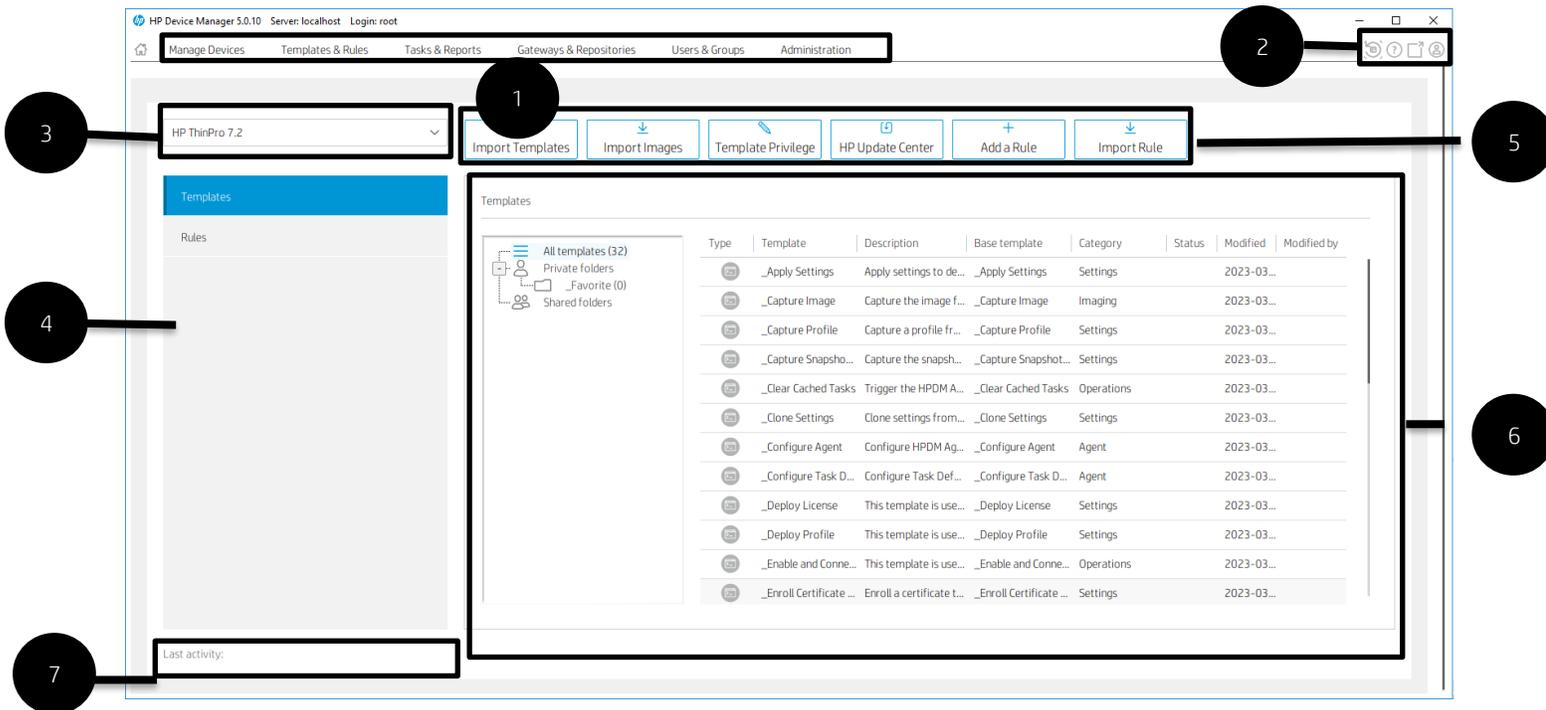
Shortcuts—Commonly used features within the Page tile. The tile contains one main shortcut and several secondary shortcuts. After the shortcut is selected, the console transitions to the related management page, navigates to the management page’s Detail View, and then performs the action defined by the shortcut.

Live Summary—Provides a real-time summary of the main content of each page.

Console layout

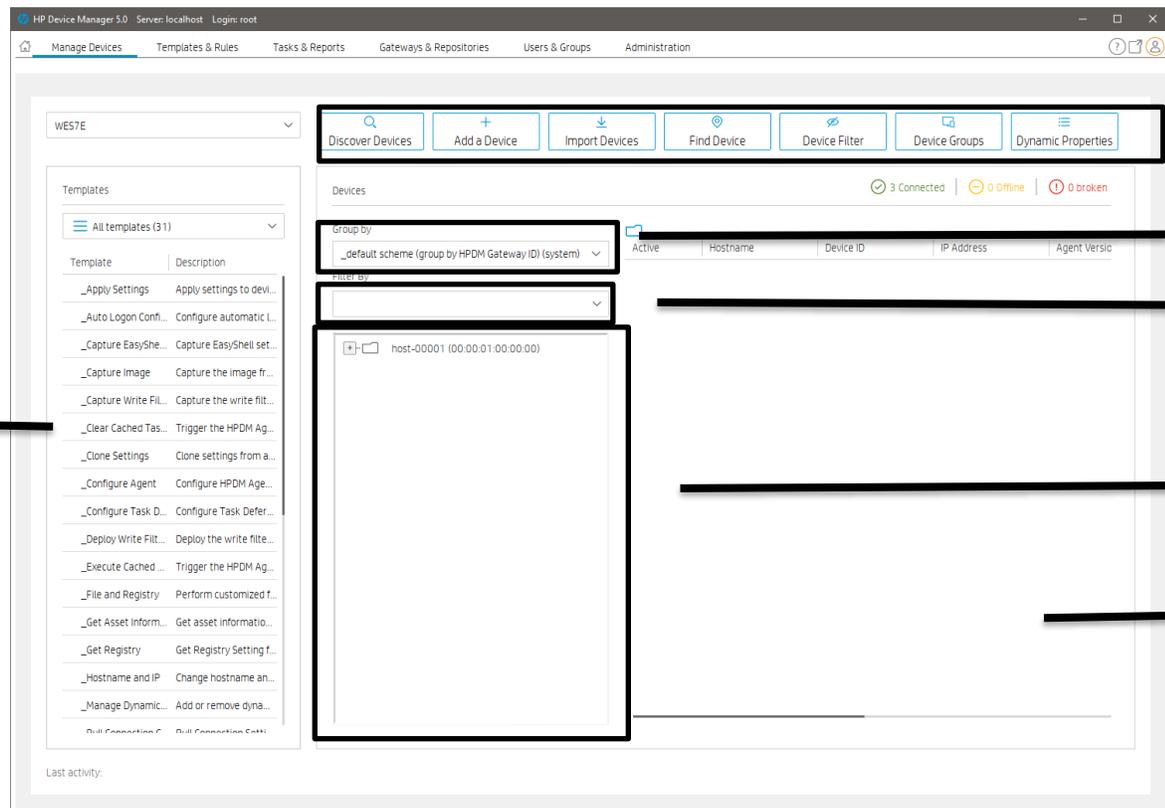
General diagrams of the main activity window layout include the following:

- Manage Devices
- Templates & Rules
- Tasks & Reports
- Gateways & Repositories
- Users & Groups
- Administration



1. Page—Summary of features and navigators.
2. Global shortcuts—Includes Reset layout, Help, Docking and Profile.
3. OS family selector—Used to change the operating system, which changes the contents of the Manage Devices page.
4. Navigation view—Sorts features.
5. Toolbar—An enumeration of common operations.
6. Detail view—Corresponds to the content under the navigator.
7. Last activity— Displays the last operation associated with the current user.

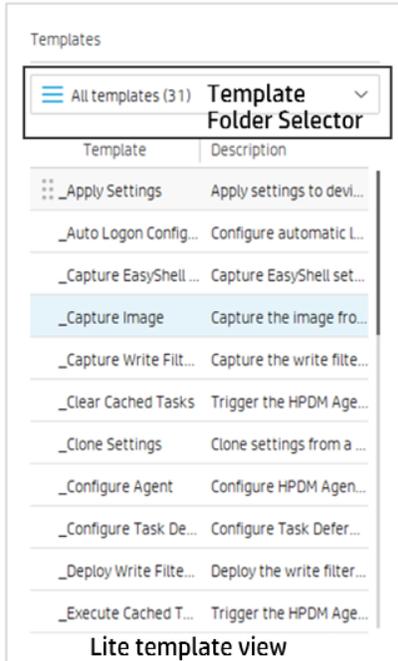
Manage Devices



1. Toolbar—An enumeration of common operations.



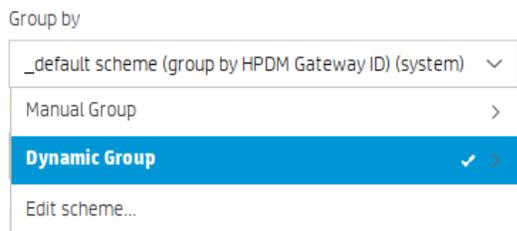
- Discover Devices—HPDM Gateway automatically discovers most devices and adds them to the HPDM database by listening for a network broadcast message made by a device when it starts up, but this method requires that the gateway is running before the device starts up.
 - Add Device—Manually register a device.
 - Import Devices—Manually register multiple devices.
 - Find Device— Find registered devices by condition. The default option is Hostname.
 - Device Filter—Device Filter management
 - Device Groups—Device group management
 - Dynamic Properties— Management of custom extended properties of device.
2. Navigation View—Brief information of template.



2.1 Template folder Selector—Switch between different template folders.

2.2 Lite Template View—Display the template under the current template folder.

3. Device Grouping Selector—HPDM enables you to create one or more grouping schemes. Each grouping scheme creates a tree structure based on the criteria selected.

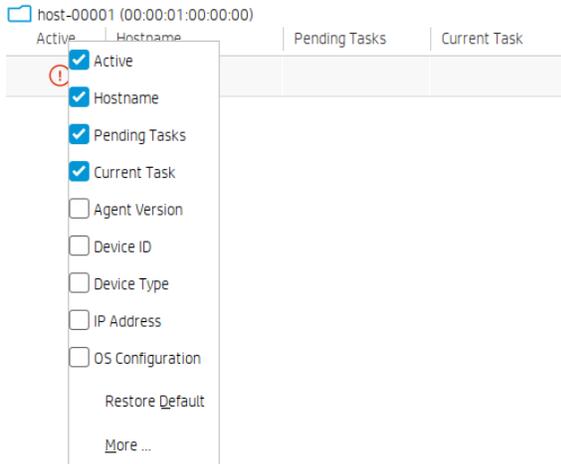


4. Device Filter Selector—Filtering enables you to work with a subset of your devices. Combine with User Privileges to divide the management of your devices between different administrators.



5. Device Tree—Display the device tree under the device scheme.

6. Device Table—Display the devices under the device tree node. If the device filter is not empty, the selected filter is used to filter the device.



Device columns—Show or hide the column of the device.

87

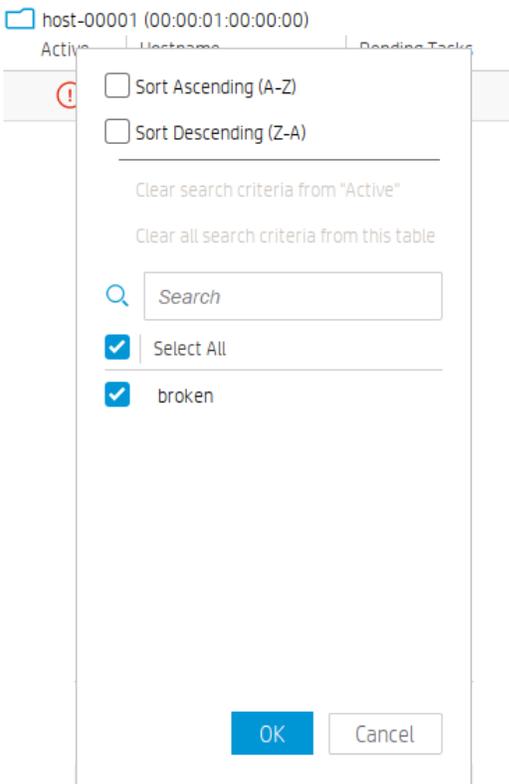


Table quick search—HPDM enables you to search quickly among listed devices. You can select any column header in the device table to add a search criteria or sort. All criteria are automatically cleared after switching to another folder.

Templates & Rules

HP ThinPro 8

Import Templ... Import Images Template Privi... HP Update Ce... HPCEM Add a Rule Import Rule

Templates

Rules

All templates (33)
Private folders
_Favorite (0)
Shared folders

Type	Template	Description	Base template	Category	Status	Modified	Modified by
	._Apply Settin...	Apply settings_Apply Settings	Settings		2024-0...	
	._Capture Ima...	Capture the im...	._Capture Image	Imaging		2024-0...	
	._Capture Pro...	Capture a profi...	._Capture Profile	Settings		2024-0...	
	._Capture Sna...	Capture the sn...	._Capture Snaps...	Settings		2024-0...	
	._Clear Cache...	Trigger the HP...	._Clear Cached T...	Operations		2024-0...	
	._Clone Settin...	Clone settings_Clone Settings	Settings		2024-0...	
	._Configure A...	Configure HPD...	._Configure Agent	Agent		2024-0...	
	._Configure T...	Configure Task...	._Configure Task...	Agent		2024-0...	
	._Deploy Lice...	This template i...	._Deploy License	Settings		2024-0...	
	._Deploy Prof...	This template i...	._Deploy Profile	Settings		2024-0...	
	._Enable and ...	This template i...	._Enable and Con...	Operations		2024-0...	
	._Enroll Certif...	Enroll a certific...	._Enroll Certifica...	Settings		2024-0...	
	._Execute Cac...	Trigger the HP...	._Execute Cache...	Operations		2024-0...	
	._Factory Res...	Factory reset.	._Factory Reset	Operations		2024-0...	

Last activity:

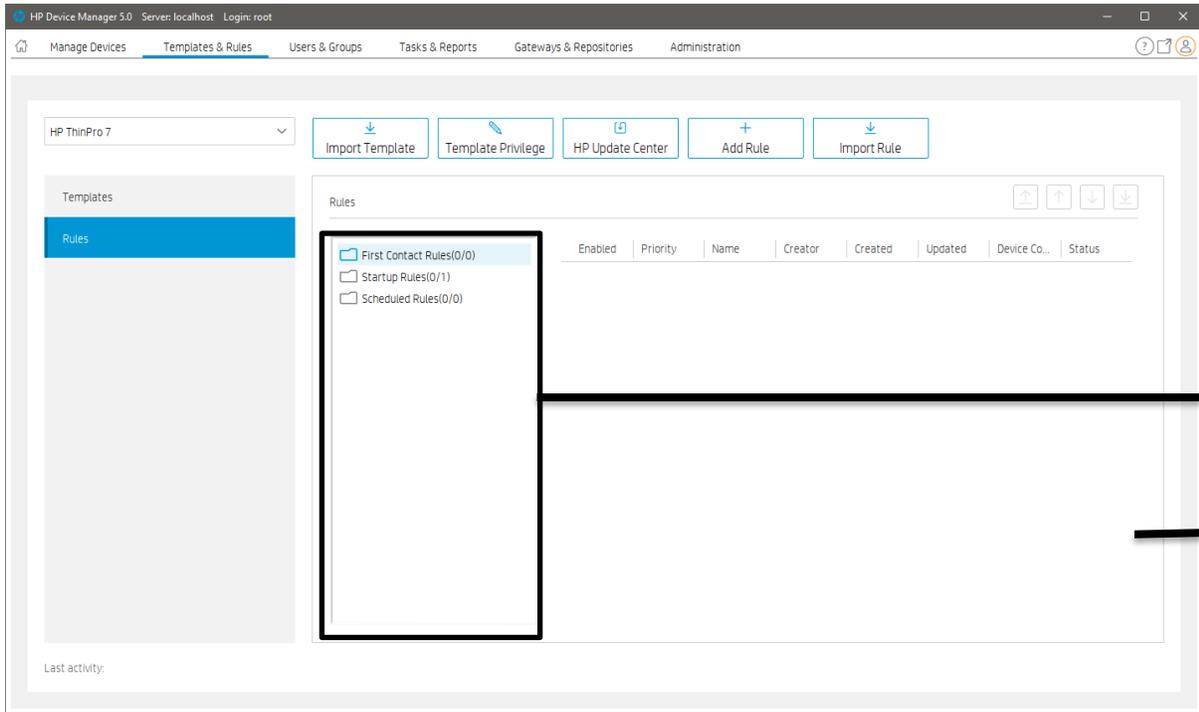
1. Toolbar— An enumeration of common operations.



- Import Template—Import templates from a file (xml, zip).
- Import Images—Generate a template with selected image file to deploy the image.
- Template Privilege— Control each template using an additional template privilege, including viewing, modifying, and executing operations.
- HP Update Center—Leverage software components from the HP FTP server for use as payload.
- HPCEM—Generate templates with selected HPCEM installation packages to deploy HPCEM.
- Add Rule—Create a new rule.
- Import Rule—Import rule from a rule file.

2. Template Folder View—View a collection of template folders.

3. Template View—List all the templates under the corresponding template folder.

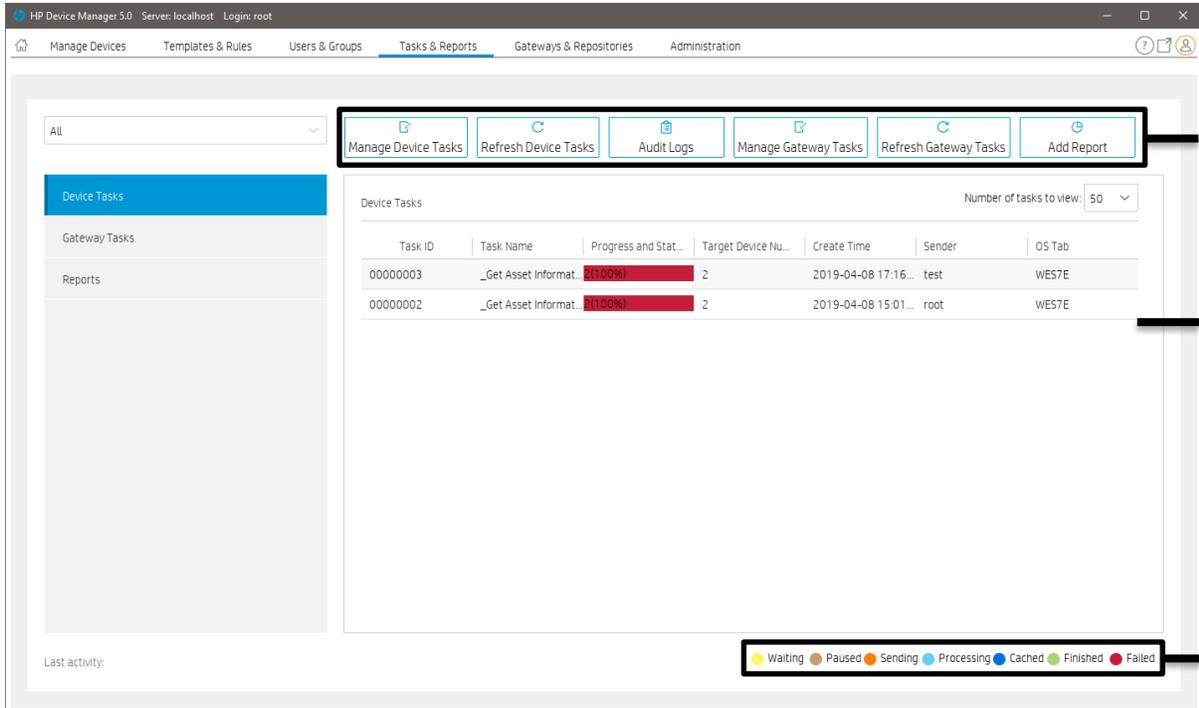


1

2

1. Rule Type List—Assort for rules.
2. Rule View—List all the rules for the corresponding rule type.

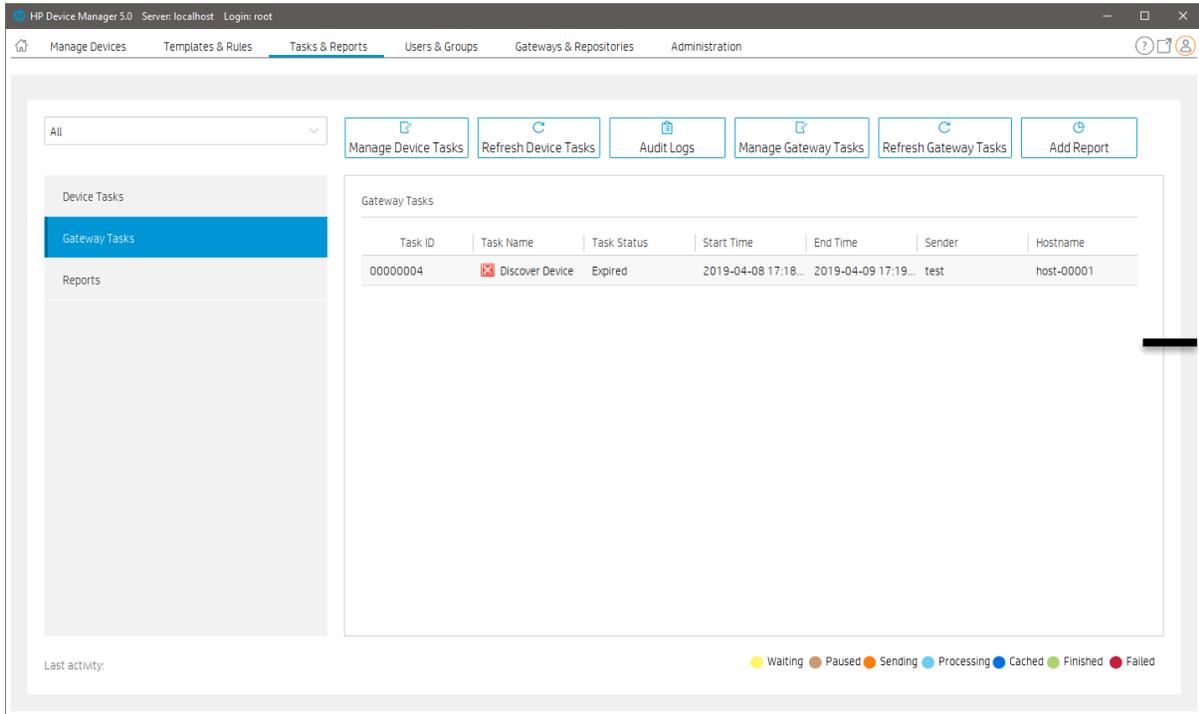
Tasks & Reports



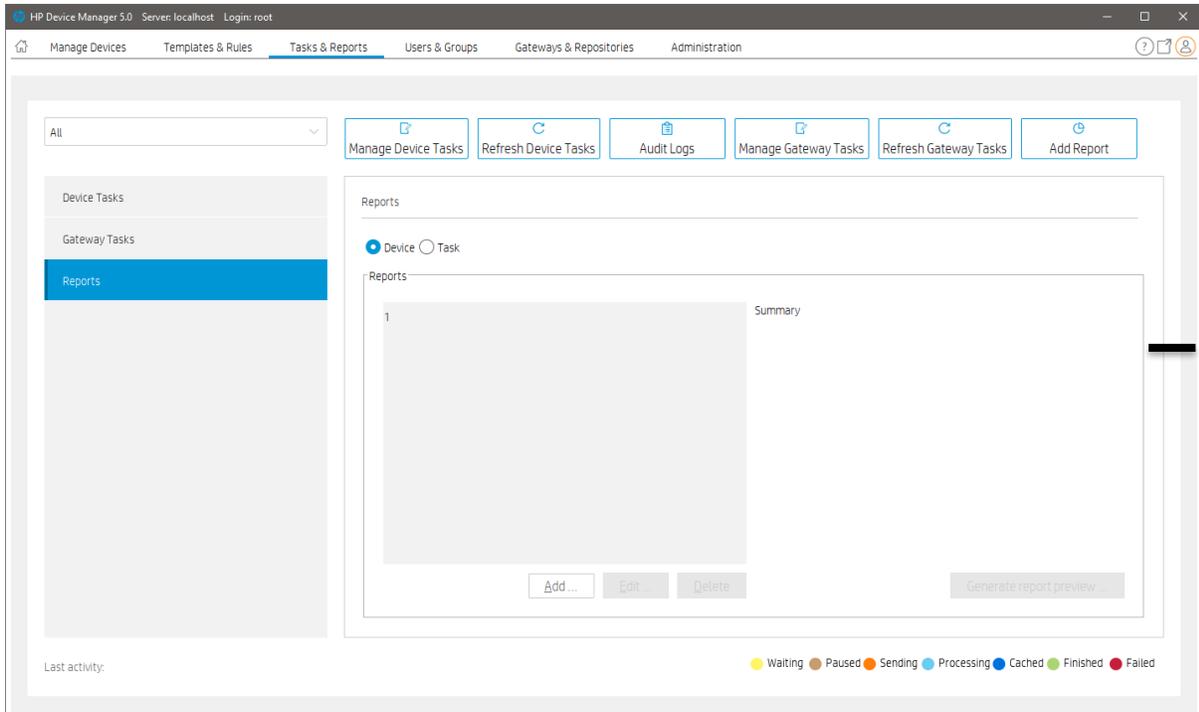
1

2

3



4



5

1. Toolbar— An enumeration of common operations



- Manage Device Tasks—Go to the device task view.
 - Refresh Device Tasks—Refresh all device task status.
 - Audit logs—Open audit log view.
 - Manage Gateway Tasks—Go to the gateway task view.
 - Refresh Gateway Tasks—Refresh all gateway task status.
 - Add Report—Create a new report.
2. Device Tasks View—Display all device tasks visible to the current user.
-

Note

The device filter shows the devices in the task. **Number of tasks to view** sets the maximum number of tasks visible to the user.

3. Task status legend

The following list describes the icons used in the Device Task View window:



Waiting

The task is scheduled or queued to send at a later time and has not yet been sent.



Paused

The task is paused.



Sending

The task is being sent from HPDM Server through HPDM Gateway to the device and is waiting for a reply.



Processing

The device accepted and is processing the task.



Cached

The task and its payload are cached on the device to be processed later.



Finished

The task was executed successfully by the device.



Failed

The task has failed or timed out.

4. Gateway Tasks View—Lists all gateway tasks.

5. Report View—Displays report management.

Users & Groups

HP Device Manager 5.0 Server: localhost Login: root

Manage Devices Templates & Rules Tasks & Reports **Users & Groups** Gateways & Repositories Administration

All

Users

Groups

Users

Username	Description	Type	DN
root		Local	
test		Local	

Last activity:

HP Device Manager 5.0 Server: localhost Login: root

Manage Devices Templates & Rules Tasks & Reports **Users & Groups** Gateways & Repositories Administration

All

Users

Groups

Groups

Group name	Description	Type	DN
Administrators		Local	
Power Users		Local	
Users		Local	

Last activity:

1. Toolbar— An enumeration of common operations.



- Add User—Create a new user.
- Change Password—Change current user password. The password should be between 12 and 36 characters in length and must include uppercase letters, lowercase letters, numbers, and special characters..

- Import from LDAP—Import users from LDAP server.
 - Add group—Create a new group.
2. User View—View all user information.
 3. Group View—View all Group information.

Gateways & Repositories

HP Device Manager 5.0.10 Server: localhost Login: root

Manage Devices Templates & Rules Tasks & Reports **Gateways & Repositories** Users & Groups Administration

All

Discover HPD... Find HPDM Ga... Add a Reposit... Import Reposi... Sync Repository Mapping Policy Master Reposi...

Gateways

Active Status	Hostname	HPDM Gateway ID	IP Address	HPDM Gateway Version	Last Update	Subnet Mask	Subnet Address
on	WIN-C89P80QGMV8	00:0C:29:0E:D4:00	192.168.23.144	5.0.3630.40158	Apr 3, 2023	255.255.255.0	192.168.23.0

Last activity: System added HPDM Gateway WIN-C89P80QGMV8.

HP Device Manager 5.0.10 Server: localhost Login: root

Manage Devices Templates & Rules Tasks & Reports **Gateways & Repositories** Users & Groups Administration

All

Discover HPD... Find HPDM Ga... Add a Reposit... Import Reposi... Sync Repository Mapping Policy Master Reposi...

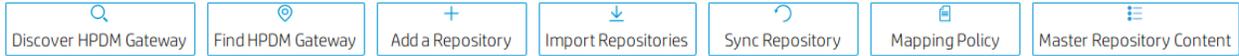
Gateways

Repositories

Name	Server Address	HTTPS	FTP/FTPS	SFTP	Shared Folder	Last Time Synchronized
Master Repository	192.168.23.144	Enabled				Master

Last activity: System added HPDM Gateway WIN-C89P80QGMV8.

1. Toolbar— An enumeration of common operations.



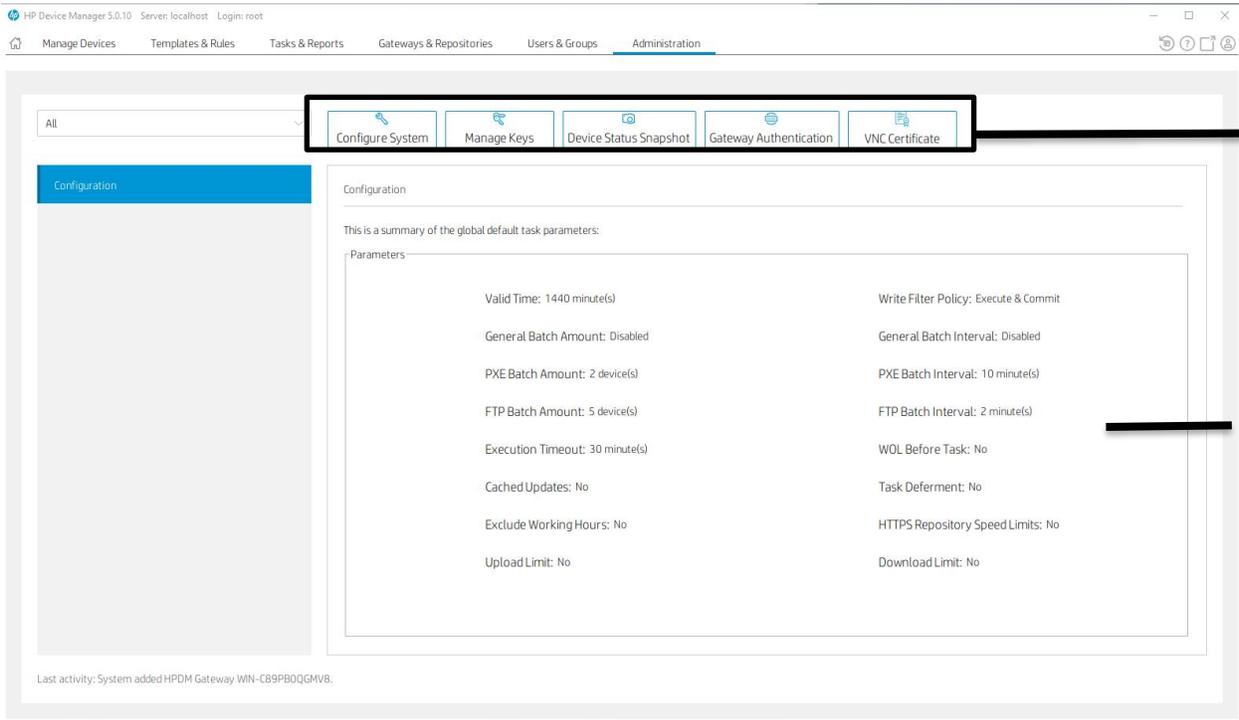
- Discover HPDM Gateway—Discover a gateway by IP range to register.
- Find HPDM Gateway—Find a registered gateway by condition.
- Add Repository—Create a new repository.
- Import Repository—Import repositories from a file.
- Sync Repository—Synchronize content from the master repository to child repositories. Synchronization can be performed immediately or scheduled.

Note

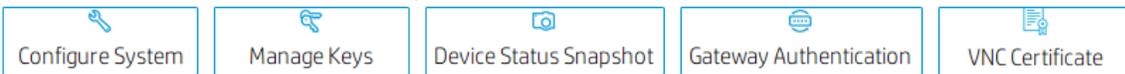
When a task that requires repository content starts, the content is automatically synced from the HPDM Master Repository to each appropriate HPDM Child Repository.

- Mapping Policy—View mapping devices to repositories according to each device’s HPDM Gateway or subnet address.
 - Master Repository Content—Manage content in Master Repository
2. Gateway View—View all gateway information.
 3. Repository View—View all repository information.

Administration



1. Toolbar— An enumeration of common operations.



- Configure System—Manage system configuration.
- Manage Keys— Update, import, or export the keys that the agent uses to verify the server. The key is passed to the devices during the key update process. The devices check the key passed by HPDM Server before executing tasks.
- Status Snapshot—View status snapshot schedule.
- Gateway Authentication—Set access control to the HPDM Gateway.
- VNC Certificate—Import or generate certificate and private key for VNC connections.

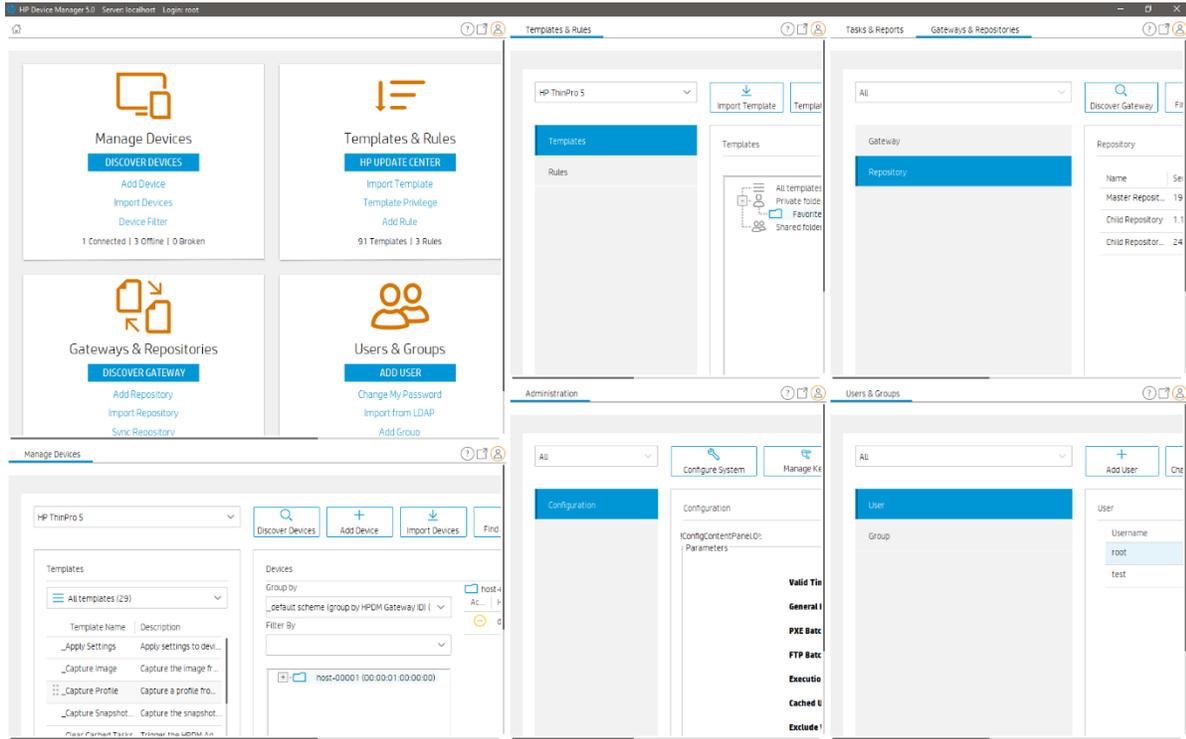
2. Configuration View—View a summary of the global default task parameters.

Console management

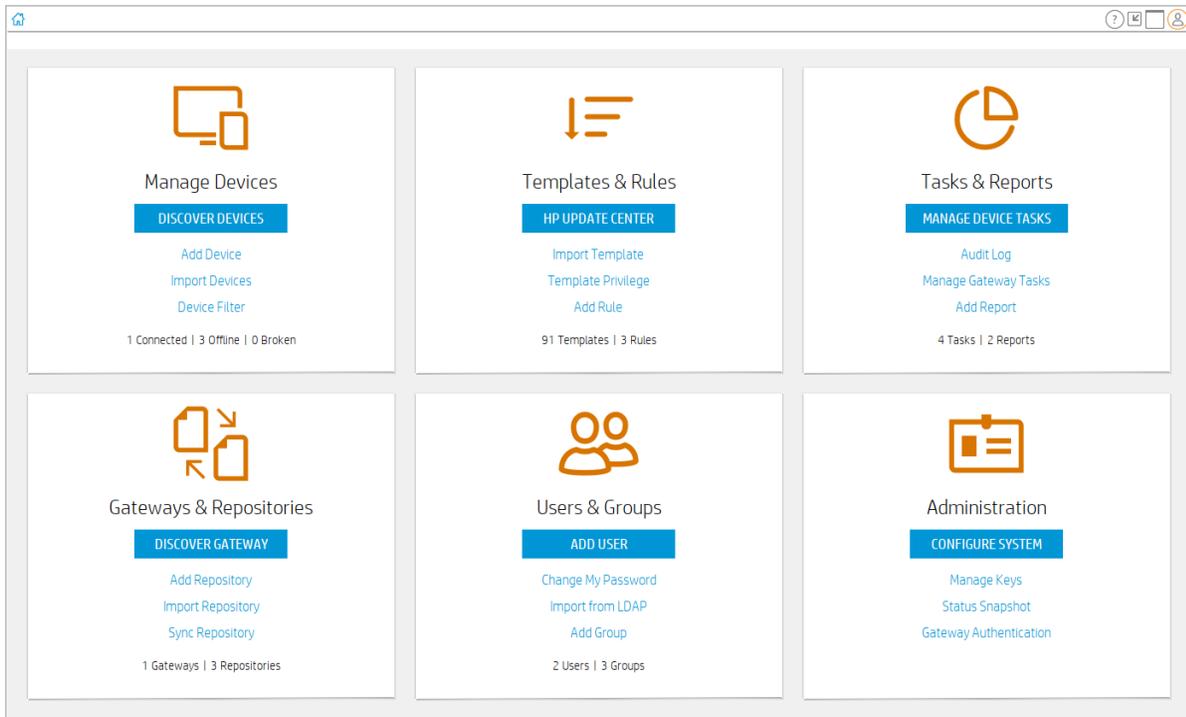
Docking Controls

You can personalize the layout of console and unlock tabbed pages to utilize multiple displays.

All page support personalized layout.

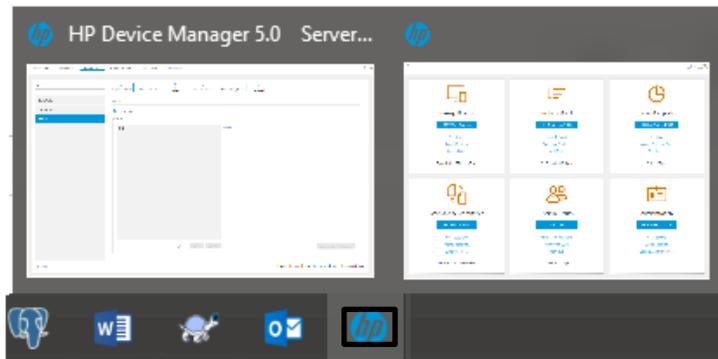


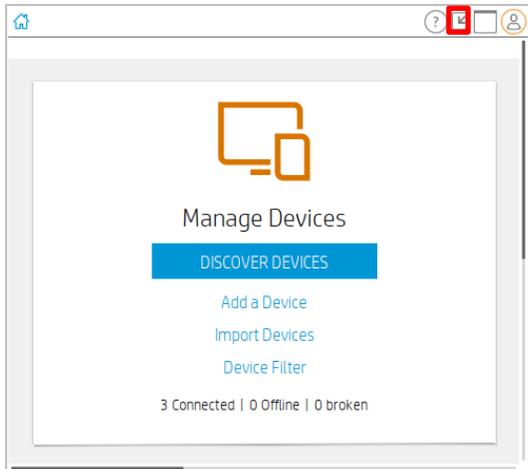
You can drag and maximize all page out of the main window.



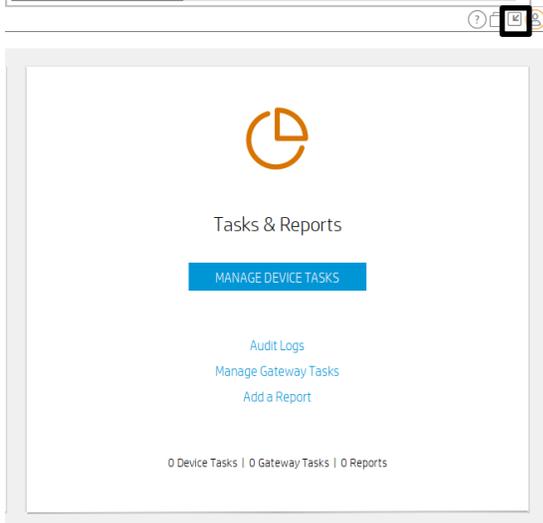
- You can separately resize and position each window.
- Can you merge an independent window with other independent windows.

A detached window is displayed in the Windows taskbar. When the main window is closed from the taskbar, the console is closed. When a detached window is closed from the taskbar, the pages are displayed in the main window again.





Detach/Back to controller window
Maximize the current window



The current window back to the size and position
before the maximized operation.

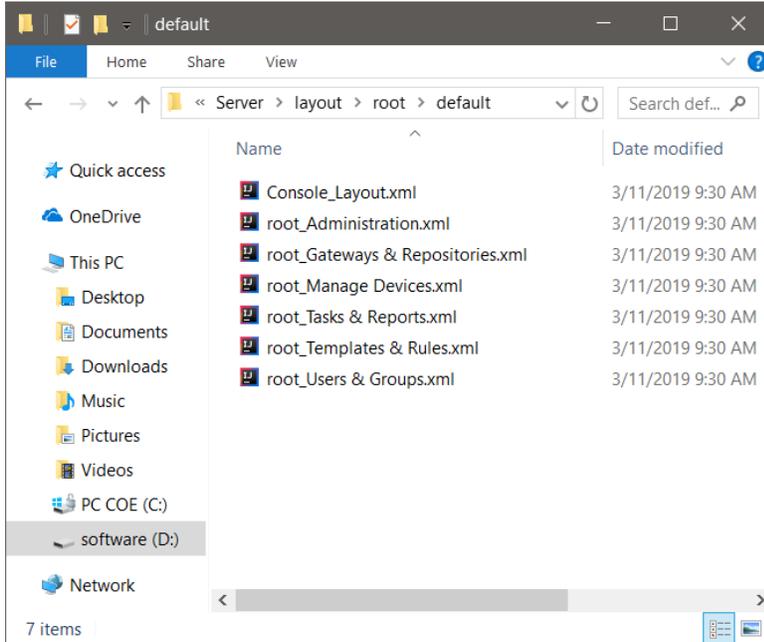
Layout Management

Console layout information is saved on the server when a user logs out. It is automatically restored when the same user logs in.

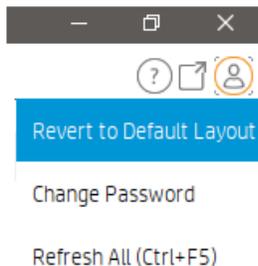
Note

Abnormal exit from the console (such as ending the console through task manager, the computer suddenly losing power) does not save the console layout and content to the server.

All documents are saved in the **Server/layout/root/default** folder:

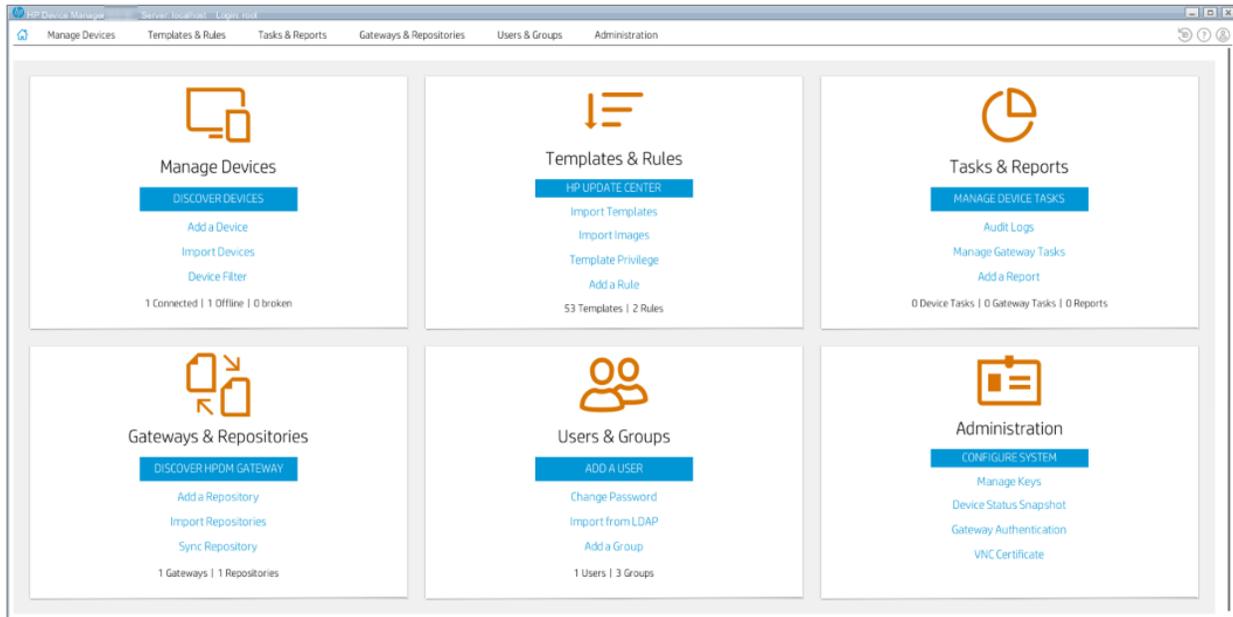


The user profile menu includes **Revert to default layout**, which restores to the default layout and clear all changeable items of the console



Console Web Bridge

To start a web console, go to <https://server-address:8443/hpdm> or <https://server-address:8443>. The user interface of a web console is similar to the HPDM console.



Functionality comparison with HPDM Console

The HPDM Console Web Bridge provides convenient access to HPDM Console users. The bridge is not designed to replace HPDM Console. For daily use, use HPDM Console.

Due to system security, some features of HPDM console are not supported in the HPDM Console Web Bridge.

Table. Feature compatibility

Features	HPDM Console	HPDM Console Web Bridge
Web access		✓
Dock/undock	✓	
Shadow	✓	
Reverse shadow	✓	
Enable and connect with SSH	✓	
Deploy profile	✓	
Features utilizing file chooser	✓	
VNC certificate management	✓	

Note

File chooser exposes the file system to any web user, jeopardizing safety of the server.

Starting from HPDM 5.0.13, export functionality for task/device reports is now available. Upon initiating the export, reports are automatically downloaded.

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 section discusses other methods to add devices to the HPDM database.

Automatic registration

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

For an 802.1x EAP-TLS protected network, if thin clients do not have other available network connections, the agent launches the Automatic Registration process after 802.1x is built up. Otherwise (if devices have other available network connections), the agent launches the Automatic Registration before 802.1x is built up.

HP ThinPro only: If the value of the option `Tag202OverrideCurrentGateway` is 1, HPDM Agent registers itself first via HPDM Gateway at DHCP tag 202. The default value is 0.

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

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

If the primary HPDM Gateway is set, the HPDM Agent tries to contact it. If that fails and a backup HPDM Gateway is also set, the agent then tries to contact the backup. If that also fails, the HPDM Agent moves on to the next method.

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

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

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

DHCP tag 202

Option 202 is used to set the IP address for the HPDM Server and HPDM Gateway.

To set option 202:

1. Select **Start > Run**.
2. Type `cmd` in the box. A command shell is displayed.
3. Type `netsh`, and then press **Enter**.
4. Type `dhcp`, and then press **Enter**.
5. Type `server \\<server_name>` (using the UNC name for the DHCP server).
-or-
Type `server <IP_address>` (using the IP address of the DHCP server).
A `<dhcp server>` prompt displays in the command window.
6. Type `add optiondef 202 <custom_option_name> STRING 0`, and then press **Enter**.
7. Type `set optionvalue 202 STRING "<HPDM_Server_IP> <HPDM_Gateway_IP>"`, and then press **Enter**.
For example: `set optionvalue 202 STRING "192.168.1.100 192.168.1.200"`
8. To confirm that the settings are correct, type `show optionvalue all`, and then press **Enter**.

Note

Replace the items in brackets with the appropriate value.

When setting optionvalue 202, the syntax must be written exactly as shown above, separated by a single space, otherwise errors occur. See the following example: `192.168.1.100 192.168.1.200`

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.

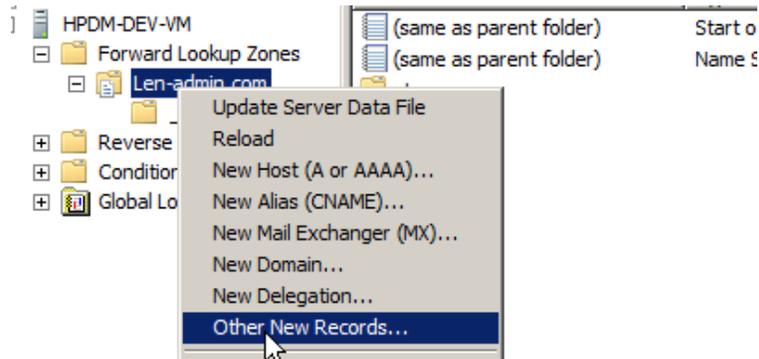
Prerequisite: HPDM Agent must have either a static domain name or access to a DHCP server to get the domain name via DHCP option 15.

Note

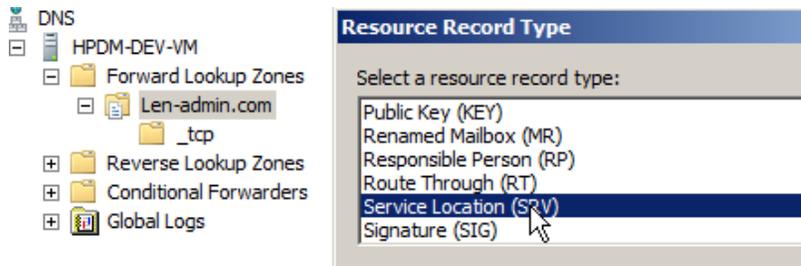
Currently, the version of HPDM Agent for HP ThinPro does not support static domain names. If a device uses a static IP address, this feature is not supported.

Creating a DNS service record

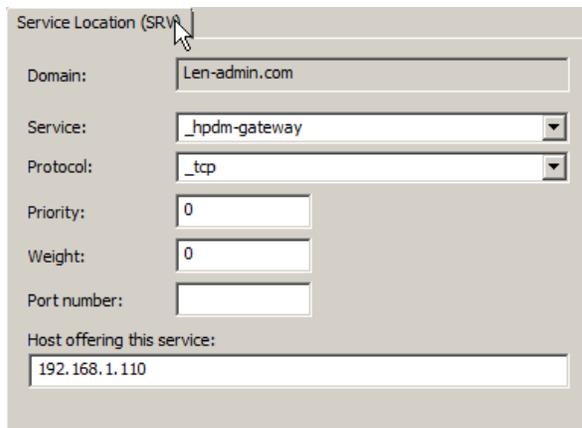
1. Open the DNS console, select your domain name.
2. Right-click to display the menu, and then select **Other New Records** to display the Resource Record Type dialog.



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



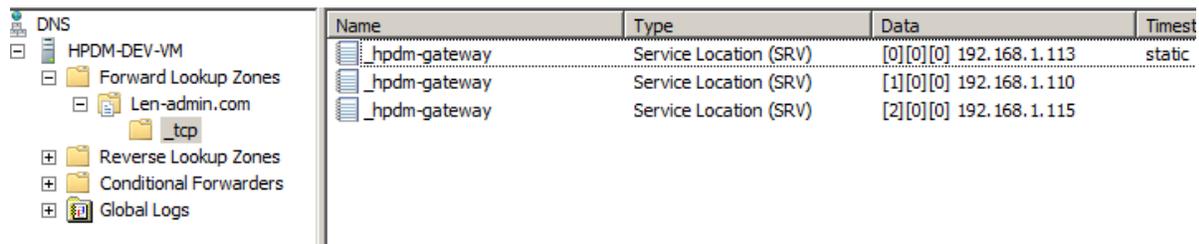
4. Set the Service value to **_hpdm-gateway**. Set the Protocol value to **_tcp**, set the Host offering this service to the fully qualified domain name (FQDN) of the HPDM Gateway, and then select **OK**. Select **Done**.



5. The agent can retrieve the gateway address from the DNS service record automatically when it starts.

Multiple DNS Service Records

The following image provides a sample multiple DNS Service Records:



Name	Type	Data	Time
_hpdm-gateway	Service Location (SRV)	[0][0][0] 192.168.1.113	static
_hpdm-gateway	Service Location (SRV)	[1][0][0] 192.168.1.110	
_hpdm-gateway	Service Location (SRV)	[2][0][0] 192.168.1.115	

If you want to set one or more backup HPDM Gateways, add the same service records with different priority values. A lower value means more preferred. Each record points to one HPDM Gateway. Setting multiple gateways in a DNS service record causes HPDM Agent to try the gateways one by one until it connects to one successfully.

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

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:

Microsoft 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 then select **Properties**.
3. Left-click Internet Protocol Version 4 (TCP/IPv4), and then select Properties.
4. Select **Advanced**.
5. Select the **DNS** tab.
6. Select **Append these DNS suffixes (in order)**, and then add the DNS domain to the list.
7. Select **OK**.

Searching for devices

HPDM can search a range of IP addresses for instances of HPDM Agent and HPDM Gateway. There are three methods: Scan using IP Range, Scan using IP List, and Scan using subnet of the specified gateway. Each of these methods begin in the same manner:

1. In HPDM Console, open the Gateways & Repositories page.
2. Select **Gateways** in navigator view. All gateways are listed in the details view.
3. Right-click the HPDM Gateway, and then select **Discover Device**.
4. Go to the section for the method you want to use.

-or-

1. In HPDM Console, select the Homepage or the Manage Devices page.
2. Select **Discover Devices**.
3. Select the HPDM Gateway.
4. Go to the section for the method you want to use.

Using the Scan using IP Range method

To search using the **Scan using IP Range** method:

1. Select **Scan using IP Range**, and then select **Next**.

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.

2. 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, clear **Use Preset IP Scope**, 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 Gateway Tasks panel on the **Tasks & Reports** tab.

Configuring an IP scope

To configure an IP scope:

1. In the **Discover by Range** dialog box, select **Use Preset IP Scope**, and then select **Edit** 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 where 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 Scan using IP List method

To search using the **Scan using IP List** method:

1. Select **Scan using IP Range**, and select **Next**.

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

2. You can customize the IP addresses in the list according to your specific needs. See the following table 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**. When the search has finished, a report shows the devices detected by HPDM. Discovered devices are added to the HPDM database.

Using the Scan using subnet of specified Gateway method

To search using the **Scan using subnet of specified Gateway** method:

1. Select **Scan using subnet of specified Gateway**, and then select **Next**.

The **Discover Device** dialog box is displayed. The IP range is automatically set according to the selected gateway.

2. Select **OK**. When the search has finished, a report shows the devices detected by HPDM. Discovered devices are added to the HPDM database.

Manually registering a device

To manually register a device:

1. In HPDM Console, open the Gateways & Repositories page.
2. Select **Gateways** in navigator view. All gateways are listed in the details view.
3. Right-click the HPDM Gateway, select **Device**, and then select **Add**.
4. Enter the device ID, MAC address, and IP address of the device.
5. Select an operating system from the list, and then select **OK**.

-or-

1. In HPDM Console, open the homepage or the Manage Devices page.
2. Select **Add Device**.
3. Enter the device ID, MAC address, and IP address of the device.
4. Select an operating system from the list.
5. Select a HPDM Gateway from the list, and then select **OK**.

If you selected **Unidentified** for the operating system, the device is initially added under the **Unidentified OS** family. 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

The Automated Device Importer is a special feature integrated within the HPDM Console. The importer parses all files in a specified folder to find all devices and to import them into HPDM.

Input file preparation

1. Create a folder containing text files.
2. The file names are used as manual group folder, up to three levels. A file name that does not contain a “_” leads devices to the default manual group, or others.
 - a. For example, A_B_C_D.txt adds devices to the manual group B/C/D.
 - b. Book1.csv adds devices to the default manual group (others).
3. Split the columns with either “;” or a “,”.
4. The columns must be in the following order:

hostname	Mac	Type	sn	OS	gw	IP
----------	-----	------	----	----	----	----

5. The hostname and MAC columns are required.
 - a. MAC is used as unique device ID. Entries in the formats AABCCDDEEFF or AA:BB:CC:DD:EE:FF are accepted.
 - b. HPDM can send a task to rename a device if the host name of the registered device in the database differs from the host name assigned to the device in the input file. You can disable this function by clearing the check box in the options panel.
6. The other columns are optional. They are updated as soon as a device reports to the HPDM Server.
 - Type**—The device type, such as HP t550.
 - sn** – The device serial number
 - OS**—The device operating system family, such as Win10/11 IoT 64bit or HP ThinPro 8. If the operating system family is not specified, the device is added as Unidentified. The device moves to the correct tab when it reports to the HPDM Server.
 - gw**—The HPDM Gateway ID for the HPDM Gateway that manages the device. If a HPDM Gateway ID is not specified or is not a valid ID in the system, the device is added to a random, known HPDM Gateway. You can find the known HPDM Gateway IDs in the HPDM Gateway tab in the HPDM Console.
 - IP** – The device IP address
7. The following is an example of valid content in txt:

```
#hostname;mac;type;sn;os;gateway_mac;ip
hostname5;000000000005;HP t610;;;192.168.1.123
hostname6;000000000006;HP t620;;;
hostname7;000000000007;HP t630;;;
hostname8;000000000008;HP t630;;;
newhostname9;000000000009;HP t5545;SNABCDEF;HP ThinPro 4;AA:BB:CC:DD:EE:FF;
hostnameA;00000000000A;HP t630;;;
hostnameB;00000000000b;HP t630;;;
HP000c29c8ee17;000C29C8EE17;;;;
001e331021d3;001e331021d3;;;;
```

8. The following is an example of qualified content in csv:

hostname	MAC	type	SN	OS	gw	IP
sampleWES7E	AA:88:99:EE:BB:11	HP t610	ABCDE22222	WES7E/WES7P/WES2009/XPE	AA:BB:CC:DD:EE:FF	192.168.1.123
sampleWES2009	AA:88:99:EE:BB:12		ABCDE22223	HPXPe		
sampleWin10IoT	AA:88:99:EE:BB:13		ABCDE22224	WE8.1IP-64/WE8S-64/Win10IoT-64		
sampleWE8S	AA:88:99:EE:BB:14			HPWE8_64		
sampleWES7P	AA:88:99:EE:BB:15			WES7P-64		
sampleWES7P-2	AA:88:99:EE:BB:16			HPWES7_64		
sampleThinPro6	AA:88:99:EE:BB:17			HP ThinPro 6-64		192.168.1.124
sampleTP6	AA:88:99:EE:BB:18		ABCDE22225	HPThinPro6_64		
sampleThinPro5	AA:88:99:EE:BB:19		ABCDE22226	HP ThinPro 5	AA:BB:CC:DD:EE:FF	
sampleTP5	AA:88:99:EE:BB:1A			HPThinPro5		

9. The expected behavior is as follows:

All new devices are imported.

The First Contact Rules for new devices are not triggered until they report to the HPDM Server.

All known devices are ignored unless there is hostname change.

Importing devices

To manually register multiple devices:

1. In HPDM Console, open the homepage or the Manage Devices page.
2. Select **Import Devices**.
3. Select **Select**, and then choose a folder that contains text files that describe the devices to import.
4. 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 OS** family. When the device first reports to HPDM and the operating system is detected, the device is then moved to the appropriate device tab.

Alternatively, to import devices using the Automated Device Importer:

1. Run the HPDM Console with the parameter `-DeviceImporter`. The Automated Device Importer starts at login. This user interface allows only the importing of devices.
2. Enter your username and password to log in to the HPDM Server.
3. Select the folder containing the import device list.
4. View the progress and results from the user interface.

Maintaining the device importer

You can modify the configuration file (%ProgramData%\HP\HP Device Manager\Console\conf\importer.conf) to change the user, path, or auto-close options.

The following image provides an example of the content of importer.conf:

```

1 #Device Management Console Profile Proerties
2 #Fri May 31 09:12:36 CST 2013
3 hpdm.logon.password=B1BCF159F7A6DDDD793E628A5A977904
4 hpdm.logon.server=localhost
5 hpdm.import.path=C:\testImporter
6 hpdm.discoverDevice.endIP=
7 hpdm.discoverDevice.startIP=
8 hpdm.discoverDevice.isPreset=true
9 hpdm.noPromptWhenClosed=true
10 hppdm.window.width=1220
11 hppdm.window.maximize=false
12 hppdm.window.height=728
13 hpdm.logon.user=Importer
14 hppdm.sequence.flat=true

```

Remove this line to disable auto-login and change user on next run

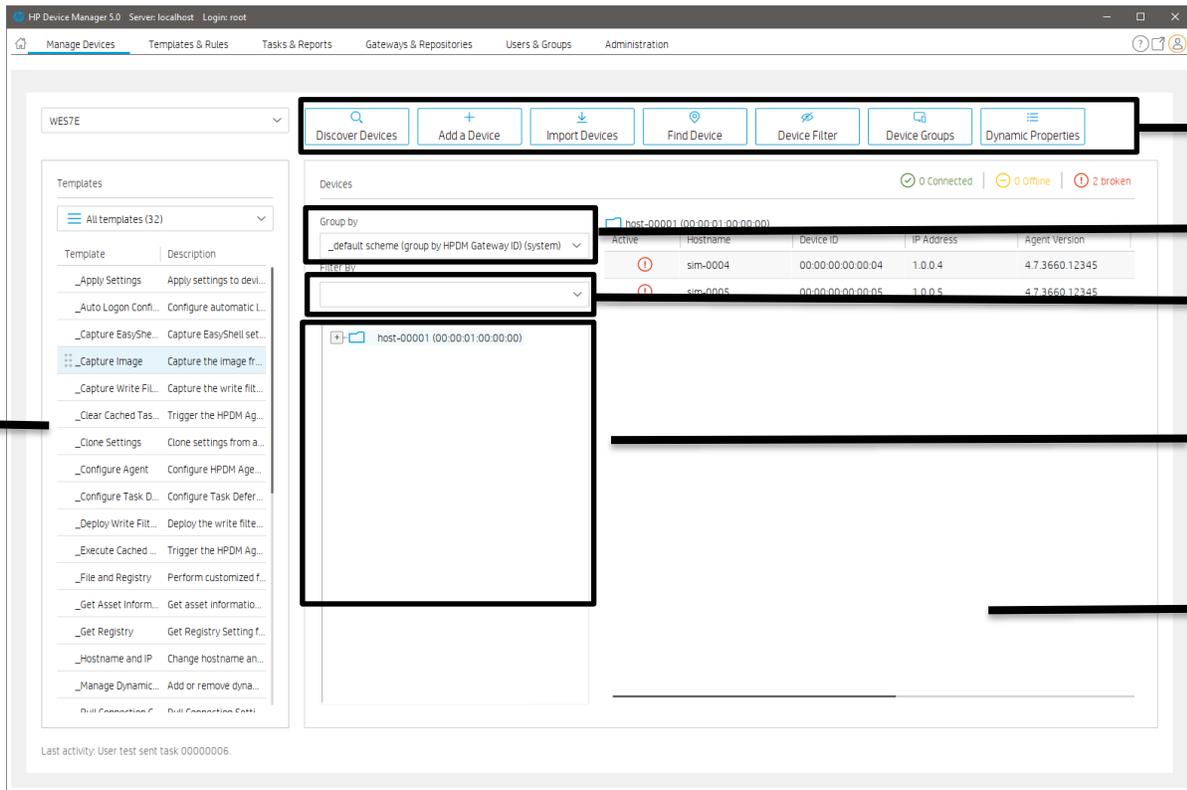
Remove this line to select import path on next run

Remove this line to avoid auto-closing the Automated Device Importer

You can create a Scheduled Task to run this importer periodically. Go to [http://technet.microsoft.com/en-us/library/cc786711\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc786711(WS.10).aspx) for more information.

Device Management

Page Layout



1. Toolbar—An enumeration of the Device most commonly operations.



- Discover Devices—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.
- Add Device—Manually register a device.
- Import Devices—Manually register multiple devices.
- Find Device—Find device by condition. The default option is Hostname.
- Device Filter—Device Filter management.
- Device Groups—Device group management.
- Dynamic Properties—Management of custom extended properties of device.

2. Navigation View—Brief information of template.

3. Device Grouping Selector—HPDM enables you to create one or more grouping schemes. Each grouping scheme creates a tree structure based on the criteria selected.

4. Device Filter Selector—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.

5. Device tree—Display the device tree under the device scheme.

6. Device Table—Display the devices under the device tree node, if the device filter is not empty, the selected filter will be used to filter the device.

Viewing devices

To view the currently managed devices in Console, go to **Manage Devices**, and then select a folder in the device tree.

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

1. In HPDM Console, go to **Manage Devices**, right-click a device table column header, and then select **More**.
2. In the resulting dialog, select whether to show or hide columns and order the columns.

On the top of Device table, there are three icons and texts to represent device status: Connected, Offline, Broken.

Deleting devices

To delete devices from the device tree:

1. Right-click the folder in the device tree.
2. Select **Delete**. All devices under this folder are removed from the device tree.

To delete a device from the device table:

1. Right-click the device in the device table.
2. Select **Delete**. The selected device is removed from the device table.

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)

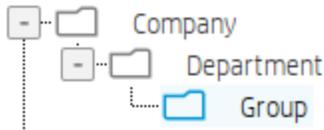
In addition, you can use the device asset information to filter the devices. This enables you to divide your devices into sets and then assign those sets to specific administrators.

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, 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 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**.

You can drag and drop devices between manual groups. You can also rename or delete manual groups.

You can utilize the 'purge' or 'purge all' functionality in the 'manual group' within the context to clear groups without associated devices.

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 **Group by**.
2. Select **Edit Scheme**, and then select the **Dynamic Scheme** tab.
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.

Switching to a Dynamic Group

1. Select **Group by**.
2. Select **Dynamic Group**.
3. Select the scheme you want to use.

Quick search

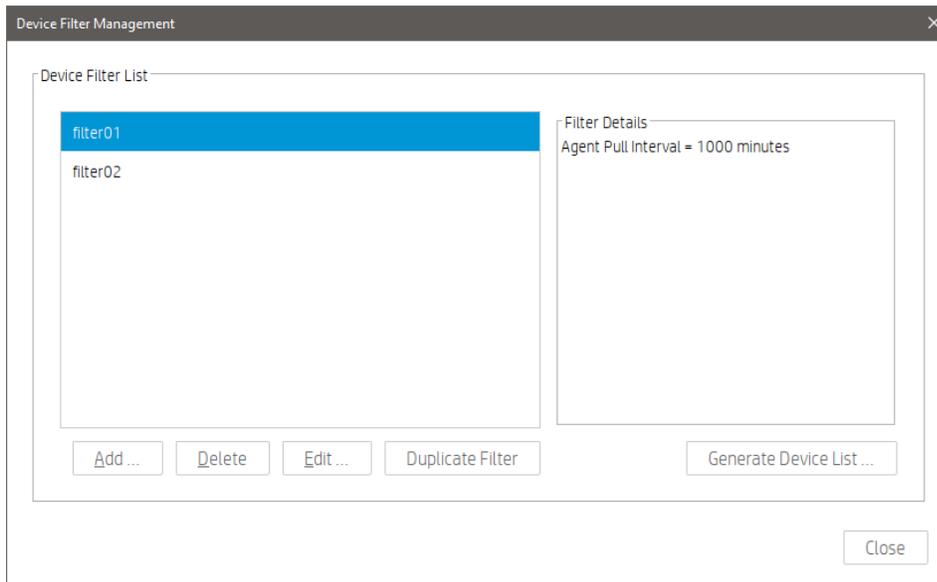
HPDM enables you to search quickly among currently listed devices. You can select any column header in the device table to add a search criteria or sort. All criteria are automatically cleared after switching to another folder.

Filtering devices

Filtering enables you to work with a subset of your devices. You can combine filtering with user privileges to divide the management of your devices between different administrators.

Create a new Device Filter

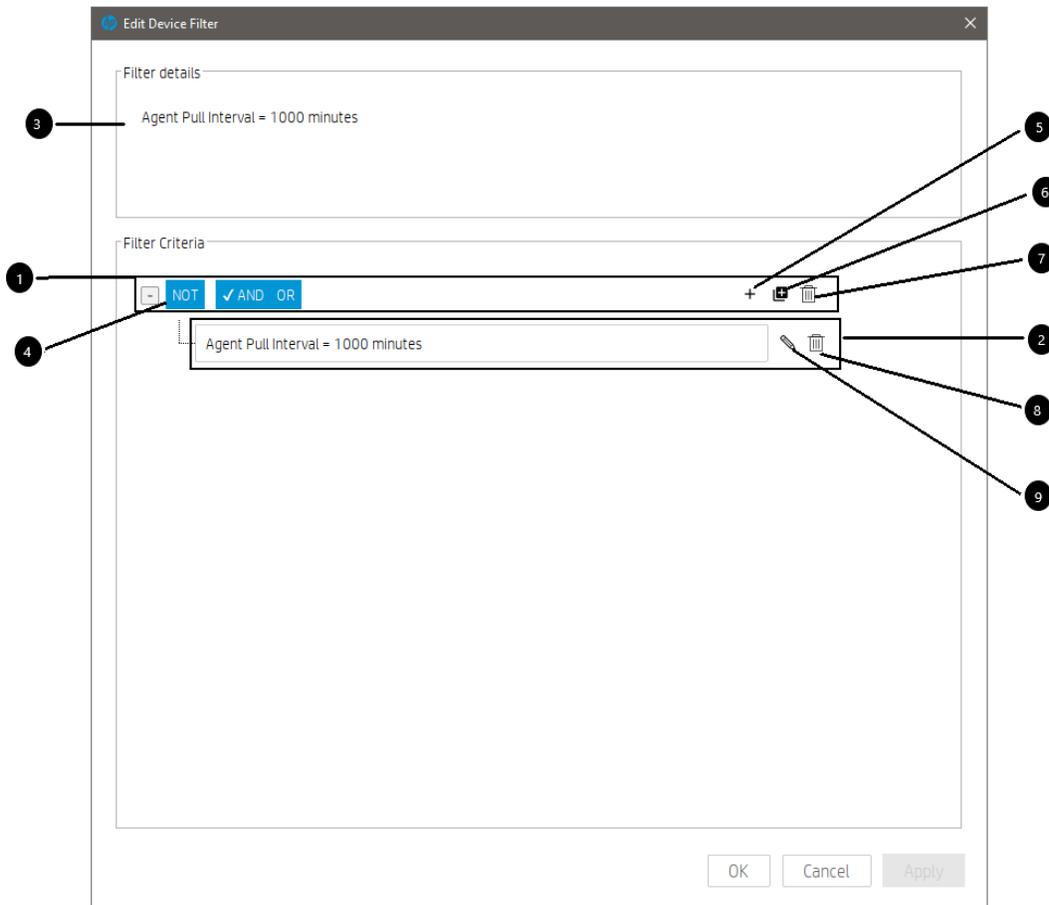
1. Open the Manage Devices page, and then select the **Device Filter toolbar** button.



Generate Device List: Shows all matched devices.

Duplicate Filter: Copies a selected filter to create a new filter.

2. Select **Add**.
3. Name the new filter, and then select **OK**.



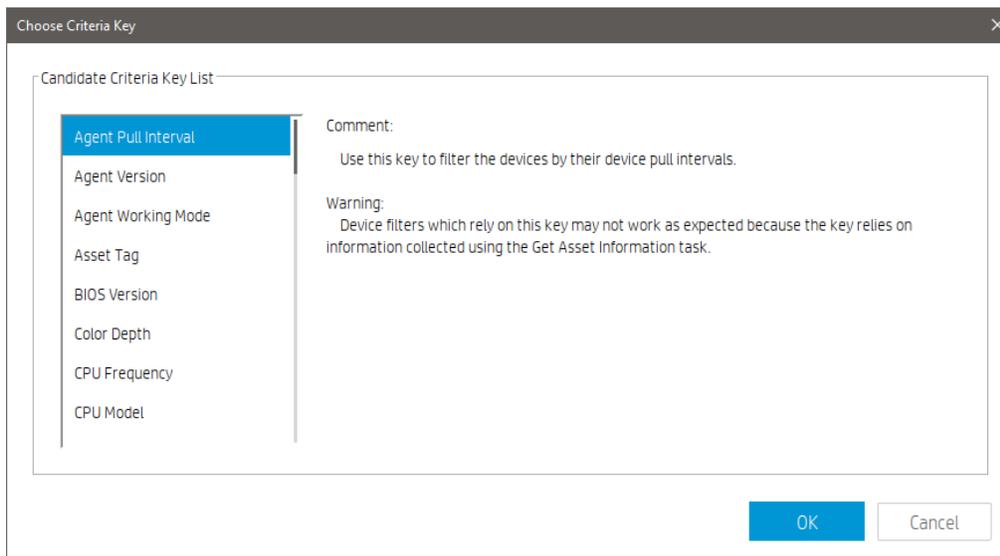
(1) **Filter Group**

(2) **Filter Criteria**

(3) **Filter details** shows expression of this filter.

(4) The **Relationship** button used to control the relation of child group or child criterion.

(5) The **Add Criteria** button used to add a child criterion under the selected group.



Select a criteria key from the list, and then select **OK**.

Criteria Editor

Choose operator and value for this criteria.

Agent Pull Interval = 1000 minutes

OK Cancel

You can choose operator and value for this criterion, select OK, this criterion will be shown under the selected group.

(6) The **Add Group** button adds a new child group under the selected group.

(7) Delete the selected group.

(8) Edit selected criteria.

(9) Delete selected criteria.

6. Select **OK**.

Edit a Device Filter

1. Open the Device Filter Management window.

2. Select an existing filter, and then select **Edit**.

3. Edit **Filter Group** and **Filter Criteria**.

4. Select **OK**.

Filter Security

You can limit the device a group can see by assigning a filter to that group as a security filter as follows:

1. Open the User & Groups page - Groups navigation view.

2. Select a group and open group properties.

3. Select the **Security Filter** panel.

4. Select **Add**.

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

When the users in this group log on, only the devices allowed by the selected filter are displayed.

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 HPDM can uniquely identify and communicate with it. You can both view and export this information.

Standard Properties

Basic asset information

To display a device's basic asset information, select 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 have content. You can use basic asset information to filter and group your devices.

The following list describes the basic asset information available on the General page:

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 ThinPro in ThinPro mode.

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 t740, 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.

License Status—The certificate status of the device.

License Expiration—The validity period of the device certificate.

License Description—The description of the device certificate.

The basic asset information available on the Agent page is as follows:

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.

Agent Working Mode— Indicates whether HPDM Gateway can push tasks to the device or if it must 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.

Asset information on the Other page lists the following information:

- Software—Software packages installed on the device.
- Hardware—CPU, memory, and storage details.
- Network—Configuration information for each network adapter present on the device.
- Configuration—Time zone and display settings.
- Microsoft Hotfix—Microsoft Hotfix Information (this page is only available if the device is Windows-based).
- Grouping—The device's extended properties.

Extension Properties

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.

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.

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.

`groupingtoolex` is located at the following path:

- Windows—C:\Windows\xpeagent

- HP ThinPro—/usr/sbin

Using groupingtoolex commands

Use the following command in your script to invoke groupingtoolex:

```
groupingtoolex <command>
```

The following table lists the valid commands (replace <key> with P1, P2 ... P6, or MG).

Table 30. Valid commands

Command	Description
set <key> <value>	Sets a grouping property, overriding the original
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 the script periodically

In Windows, you can use the **schtasks** tool to create periodic tasks to invoke the script:

```
schtasks /create /tn <task name> /tr <script file> /sc hourly /ru SYSTEM /rp <password>
```

For example:

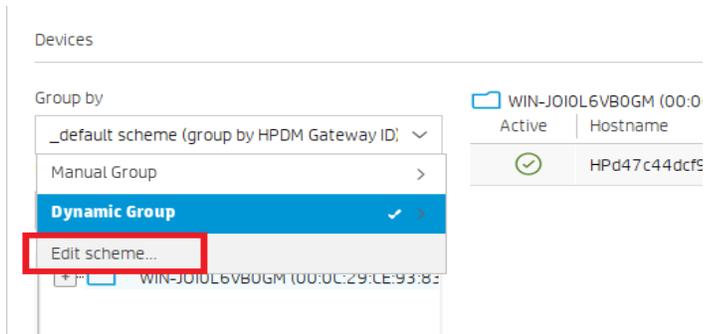
```
schtasks /create /tn DailyUpdateNIC /tr UpdateNIC.bat /sc hourly /ru SYSTEM /rp MyPassword
```

In HP ThinPro, you can use the **crontab** command to create a periodic task.

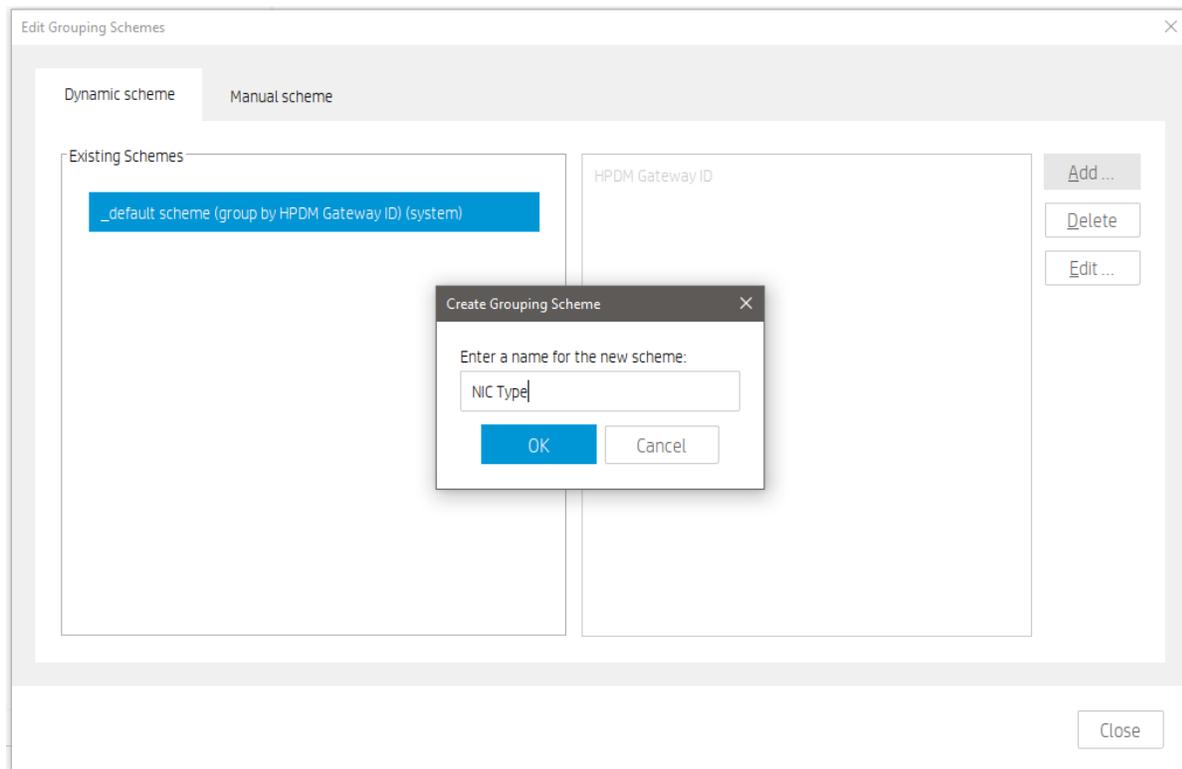
Example procedure

The following example describes how to group devices by NIC card:

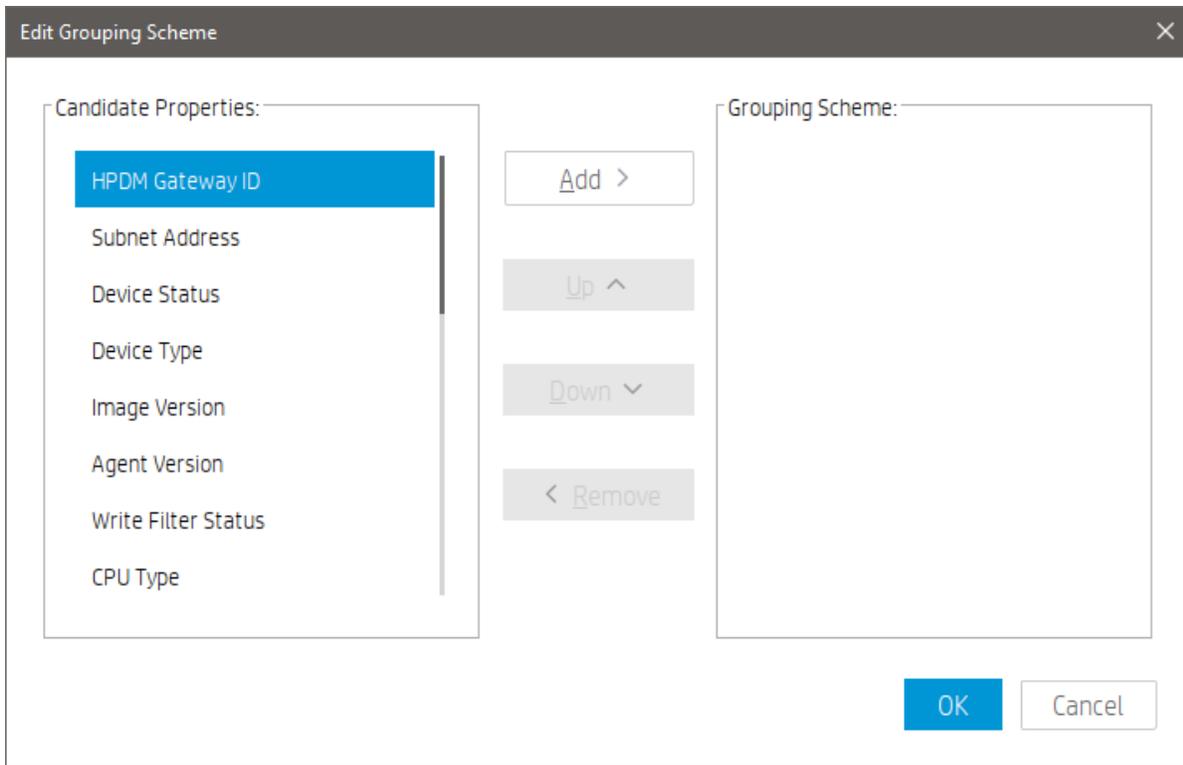
1. Remotely execute a script on the thin client that retrieves the NIC card type and assigns it to grouping key (P3 for this example).
2. In HPDM Console, select **Group by**, and then select **Edit scheme**.



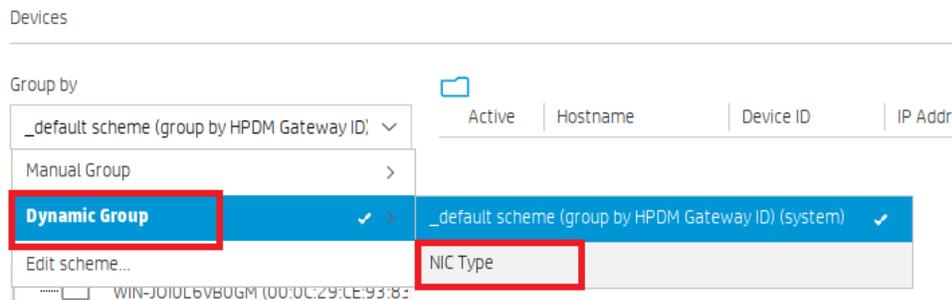
3. In the **Edit Grouping Schemes** box, select **Add**, enter NIC Type (or any custom name) for the grouping scheme name, and then select **OK**.



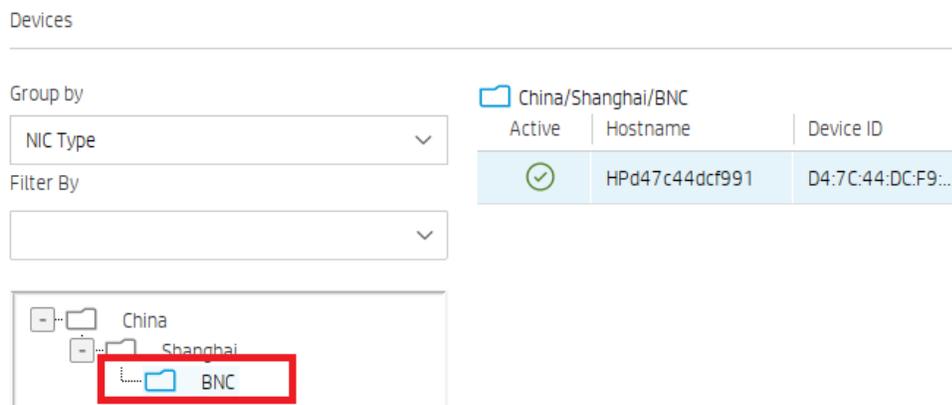
4. Select extension properties 1–3, select **Add**, and then select **OK**.



5. In HPDM Console, select **Group by**, select **Dynamic Group**, and then select **NIC Type**.

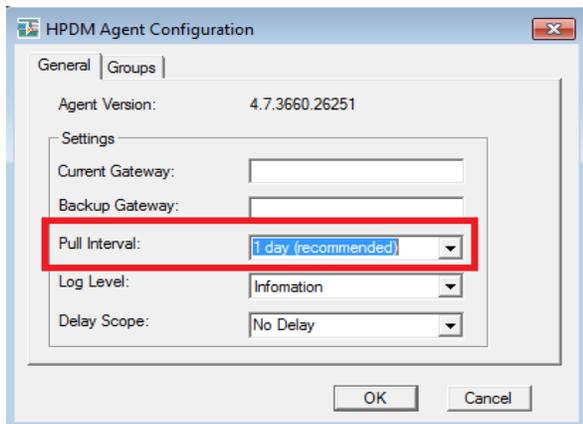


Devices are now grouped by NIC type, such as BNC.



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 cannot 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.

**Dynamic Properties**

Dynamic properties are designed for HPDM administrator to use as many properties as they are interested in. Currently there are three types of dynamic properties:

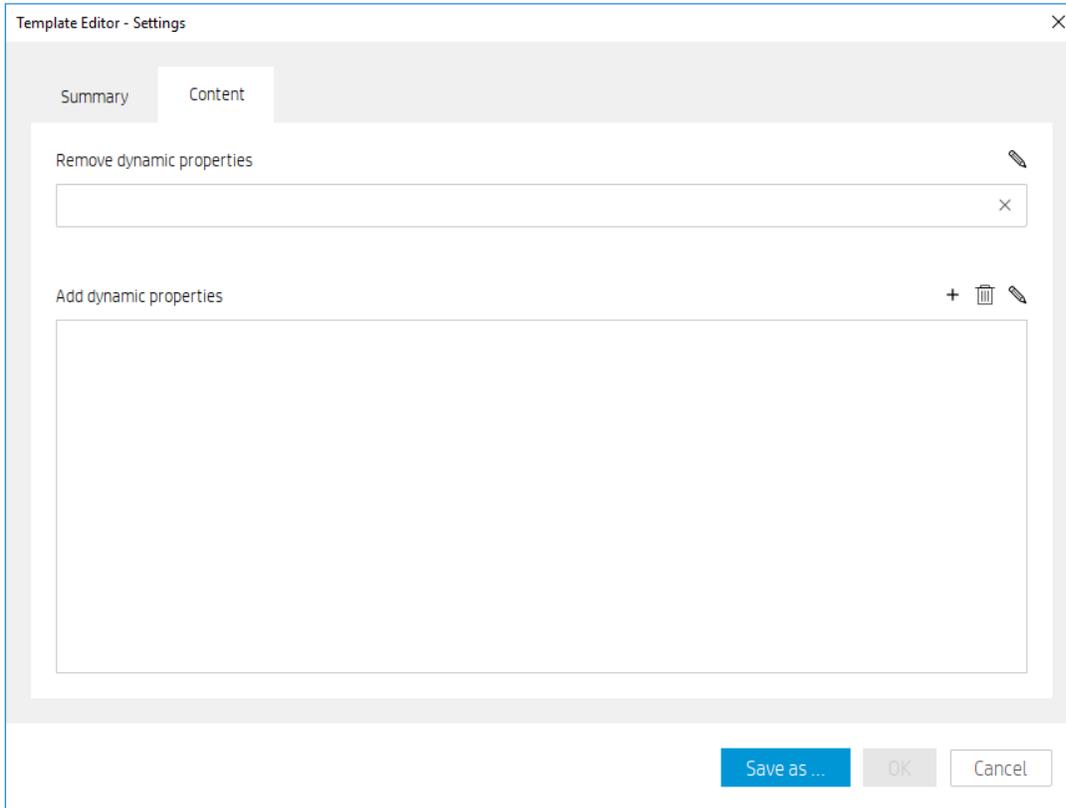
Software version: The property which displays the version of software installed in devices. The property name starts with "sw_ver_".

Microsoft hotfix: The property which displays the Microsoft hotfix installed in devices. The property name starts with "ms_hf_".

Customized script: The property which displays value of the running script in devices.

Manage Dynamic Properties

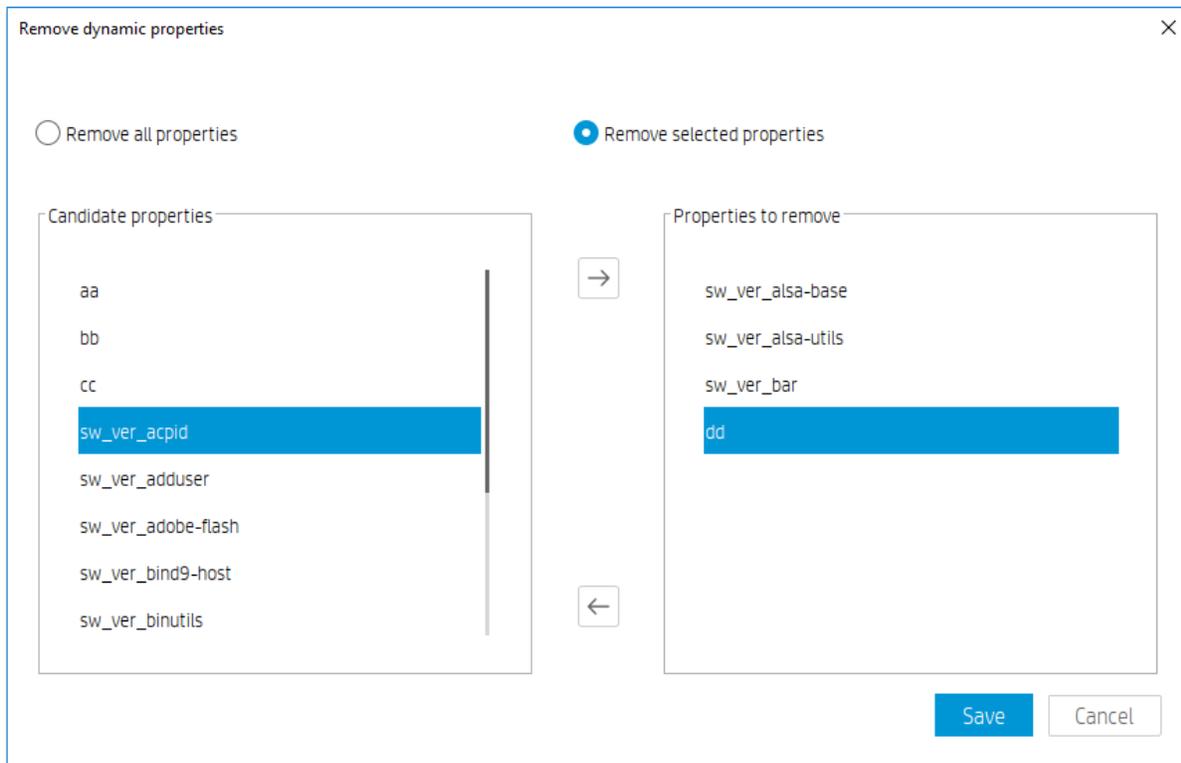
A template **_Manage Dynamic Properties** is designed for adding or removing dynamic properties. It consists of two parts: **Remove dynamic properties** section and **Add dynamic properties** section.



If both sections are defined in the task template, **Remove dynamic properties** action is always performed before **Add dynamic properties** action since HPDM administrator may clean up old properties before adding new properties.

Remove dynamic properties

Remove dynamic properties consists of two options: **Remove all properties** or **Remove selected properties**. **Remove all properties** is a special instruction. Agent will search all the dynamic properties defined in the target device and remove them all, while **Remove selected properties** make agent search and remove the listed properties in the task. If the target device does not have specified properties. Agent will do nothing and return a success code.



To remove dynamic properties from the target device:

1. Open the template editor of **_Manage Dynamic Properties**. Select  in the **Remove dynamic properties** section to open the dialog editor of **Remove dynamic properties**.
2. Select **Remove all properties** or **Remove selected properties**.
3. If **Remove selected properties** is selected, move properties from **Candidates properties** to **Properties** to remove list.
4. Select **Save** to save properties to be removed and back to the template editor.
5. The text box lists properties to be removed. Click X to reset text box if you want to abandon your previous selections.

Figure 13. Remove dynamic properties section



Note

Dynamic properties in candidates' properties are the set of all properties of a specific operating system instead of those of the target devices on which tasks are performed.

Add dynamic properties

Add dynamic properties consists of two parts: Schedule and Properties.

Schedule requires a number for check interval. Agent checks the value of property in device at this interval. If the value changes, it is reported. Otherwise, no value is reported.

Properties defines type, name and content of a dynamic property. Microsoft Hotfix is not visible in non-windows operating system.

Add dynamic properties
✕

Schedule

Check interval

minutes

Properties

Software version
 Microsoft Hotfix
 Customized script

Property Name

Software Name

✕
▼

Save
Cancel

To add dynamic properties

1. Open the template editor of **_Manage Dynamic Properties**. Click + in the **Add dynamic properties** section to open the dialog editor of **Add dynamic properties**.
2. Input a number to assign a check interval.
3. Select one of three types: **Software version**, **Microsoft Hotfix**, or **Customized Script**.
4. If **Software version** or **Microsoft Hotfix** is selected, select a software name of Microsoft hotfix from the list. Property name is automatically created.
5. If **Customized script** is selected, input property name and script content in the corresponding text boxes.
6. You can access provided **Sample Scripts** by hovering the cursor. A text editor lists all sample scripts. Click  or  to navigate and  to use the sample script.
7. Select **Save** to save one custom property. The property name is added the list.
8. Select the saved property name. Click  to edit and  to delete.

Note

Do not set the check interval number too small if you want to add many properties. Otherwise the CPU usage will show high use in device.

Schedule

Check interval

30

Properties

- Software version
 Microsoft Hotfix
 Customized script

Property Name

loginName

Script

[Sample Scripts](#)

```
for /f "tokens=2 delims=\" %%i in ('wmic computersystem get username ^| findstr "\\") do set loginName=%%i

echo value=%loginName%
```

```
for /f "tokens=2 delims=\" %%i in ('wmic computersystem get username ^| findstr "\\") do set loginName=%%i

echo value=%loginName%
```

Note

If the Property Name or Microsoft Hotfix list is empty, you can retrieve the content after performing the Get Asset Information command on devices.

```
loginName
ms_hf_KB1234567
sw_ver_citrix
```

Collect dynamic properties

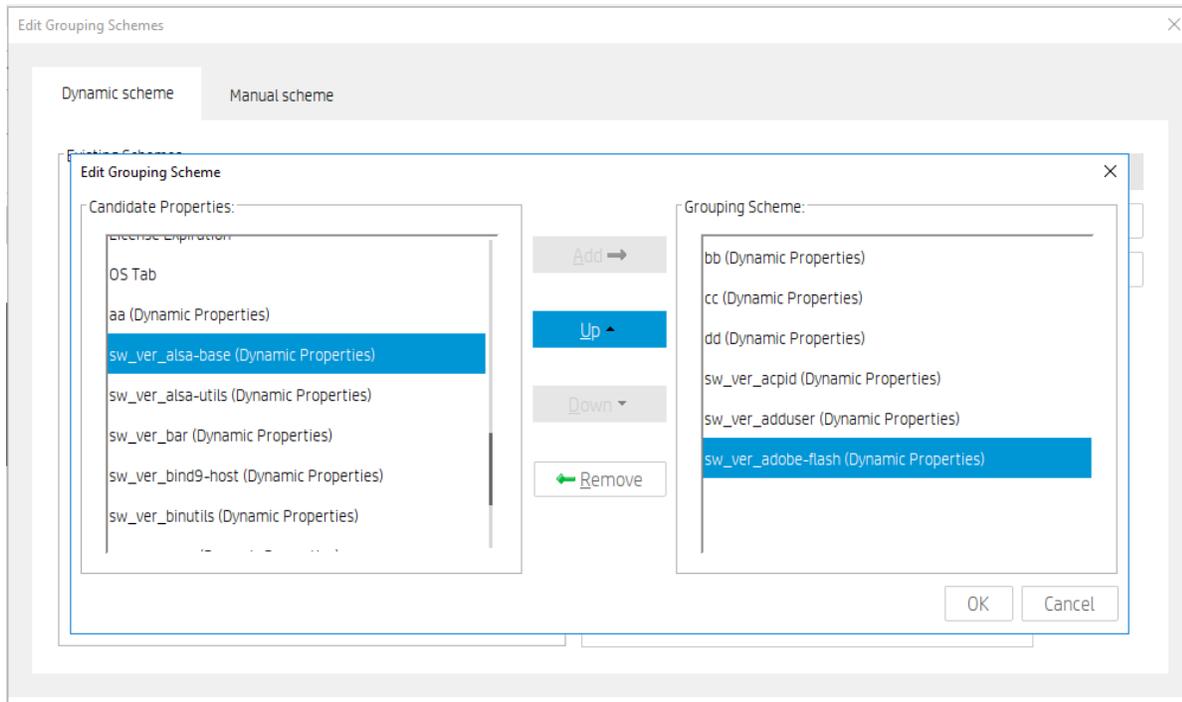
There are two ways to collect dynamic properties:

- Perform a Get Asset Information task to retrieve all dynamic properties from devices. View dynamic properties in the Dynamic Properties page of the Device Properties window.
- Perform a Manage Dynamic Properties task to add multiple dynamic properties. Agent immediately reports the values and checks values at an interval and reports if values change.

Manage Devices with Dynamic Properties

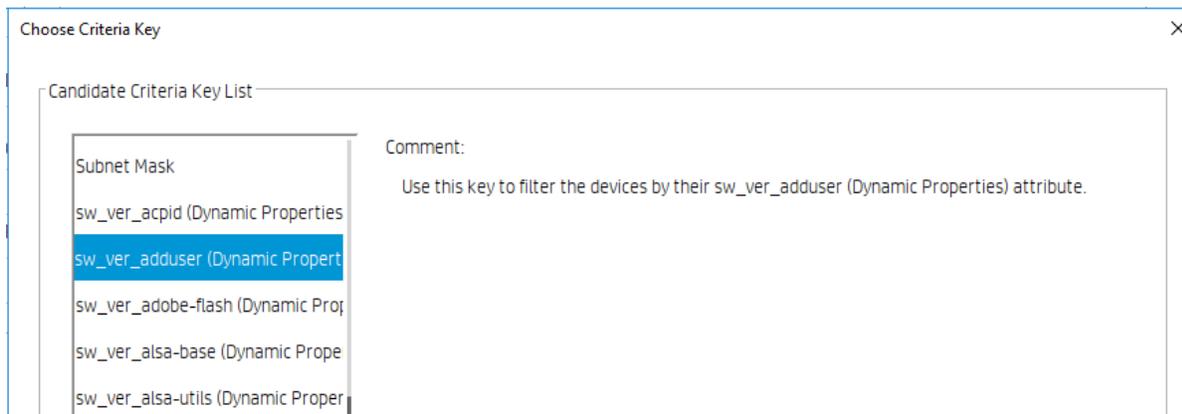
Device Groups

HPDM administrator can group device by dynamic properties. When creating or editing grouping scheme, you can identify dynamic properties by an indicator (Dynamic Properties).



Device Filter

HPDM administrator can filter device by dynamic properties. When creating or editing criteria key, you can identify dynamic properties by an indicator (Dynamic Properties).

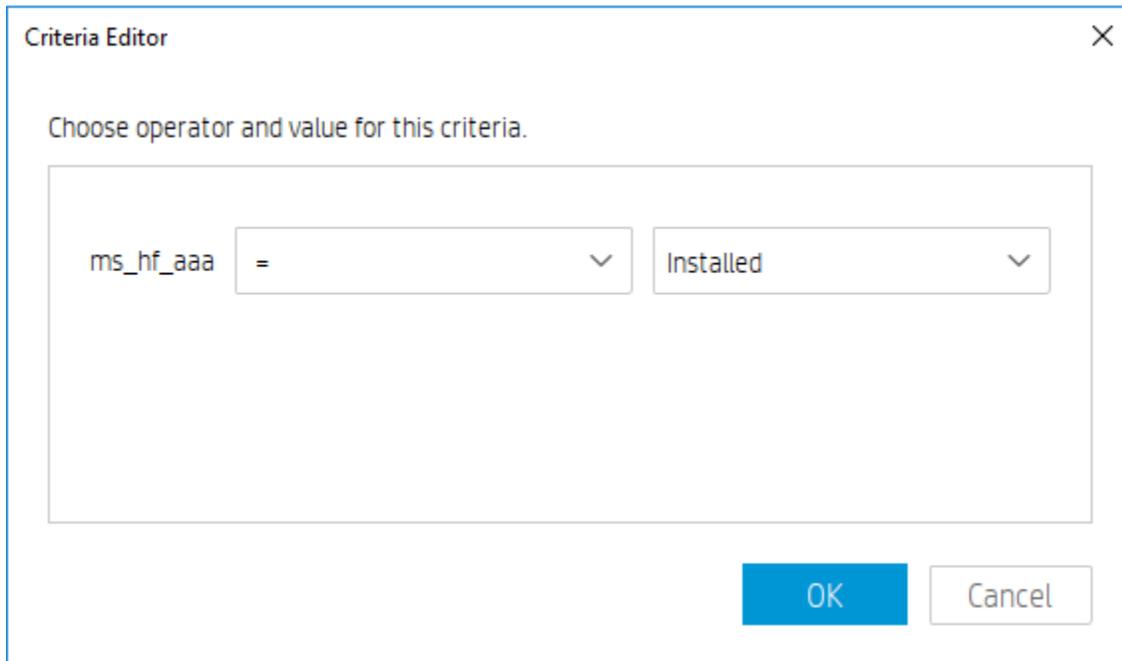
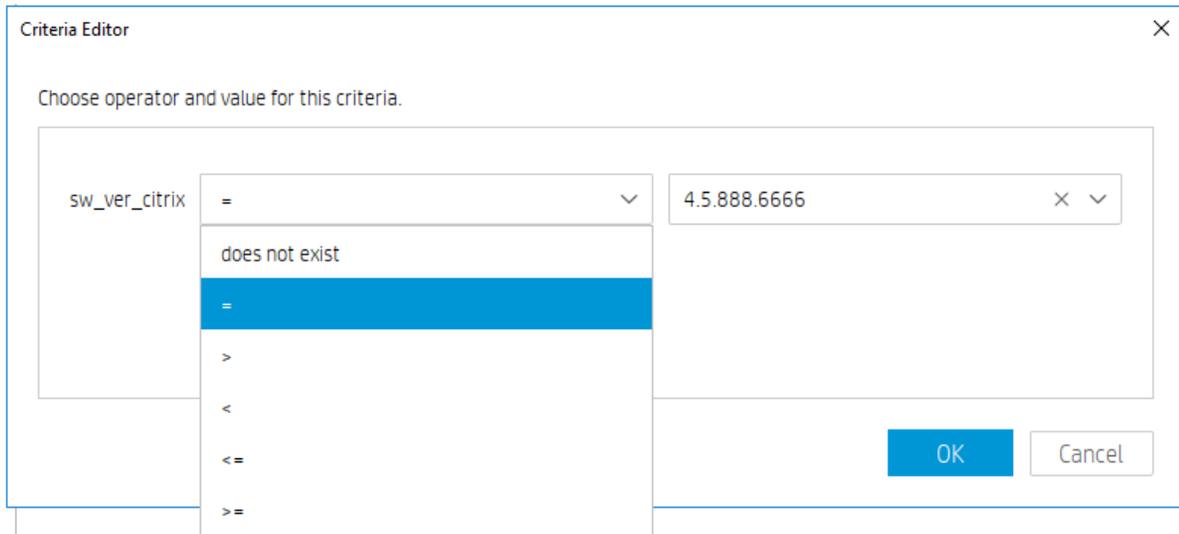


There are two sets of operators applied to dynamic properties.

For software versions and customized scripts, the set of operators includes: does not exist, =, >, <, <=, >=.

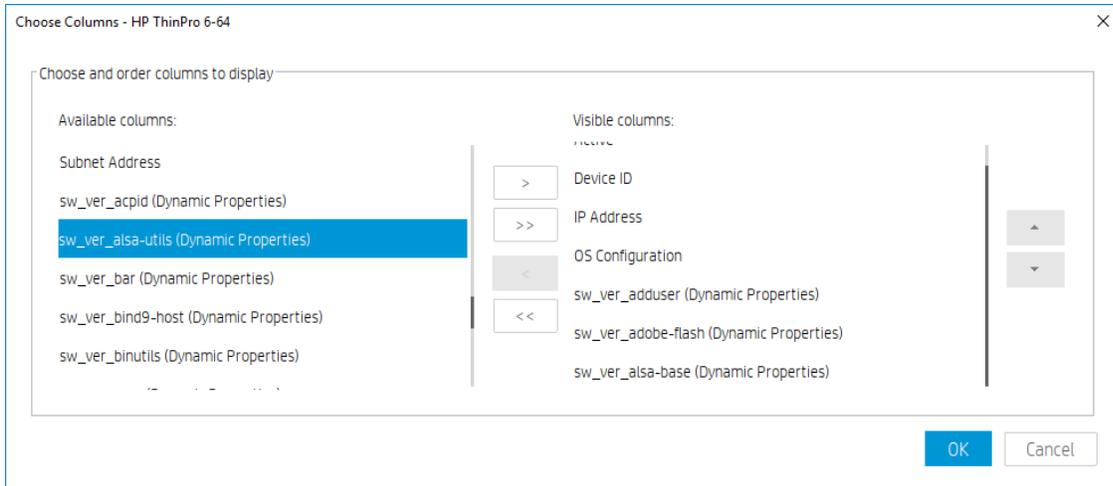
Note: When filtering based on user-defined attributes starting with 'sw_ver,' the results are obtained through version number comparison methods.

For Microsoft hotfix, the set of operators includes: does not exist =. The value is either **Installed** or **Not Installed**.



Device Table

HPDM administrator can view devices with dynamic properties. When choosing columns, you can identify dynamic properties by an indicator (Dynamic Properties). Choose and order columns so you can view dynamic properties of devices under the selected operating system.



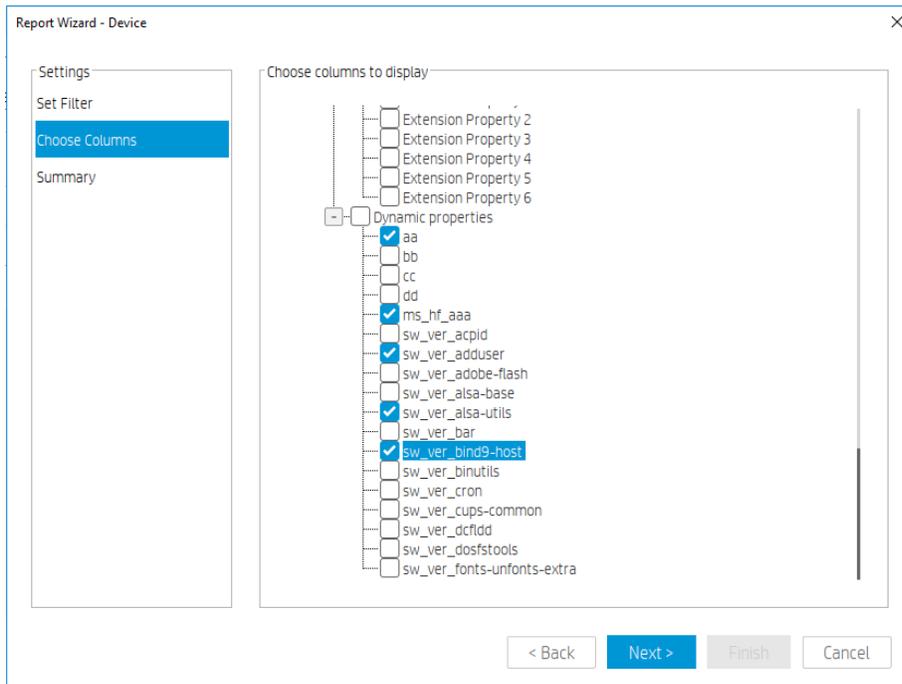
WIN-C89PB0QGMV8 (00:0C:29:4E:2E:3F)	Active	Device ID	IP Address	OS Configuration	sw_ver_adduser	sw_ver_adobe-f...	sw_ver_alsa-ba...
		08:50:56:3B:AC:D5	192.168.153.130	ThinPro	3.113+nmu3hp3	11.2.202.491	1.0.25+dfsg-0hp4

Device Report

HPDM administrator now can generate device reports with dynamic properties.

To generate a device report with dynamic properties:

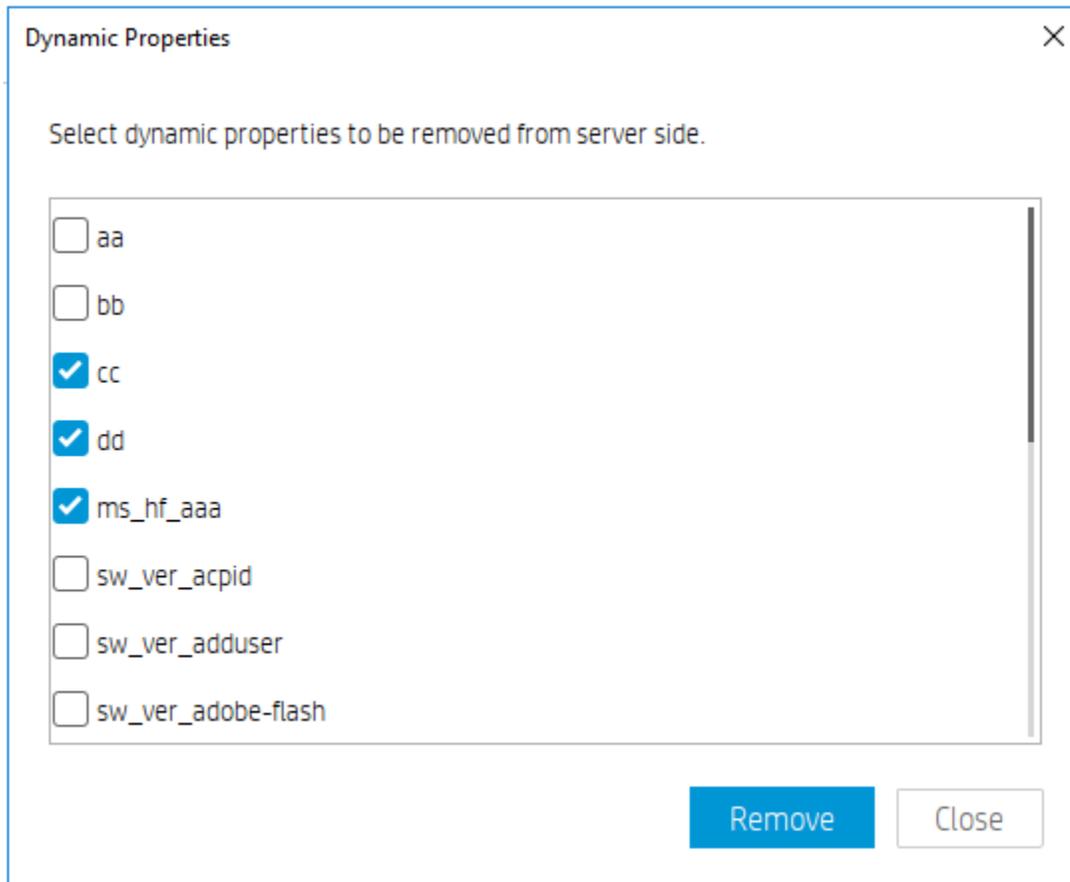
1. Go to the **Tasks & Reports** tab.
2. Choose **Reports** in the left panel, and then select **Device for report type**.
3. Select **Add** to open Report Wizard – Device.
4. Select several properties in the **Dynamic Properties** section.
5. Complete the remaining steps and generate a report.



Delete dynamic properties from server side

In some situations, some dynamic properties will no longer be updated by devices. For example, some devices are removed from the network. Dynamic properties of those devices have been stored in server, but will not be updated by any devices. These dynamic properties are supposed to be purged. To delete dynamic properties from server side

1. Select **Dynamic Properties** on the tool bar of the **Manage Devices** page to open the custom properties editor.
2. Check the custom properties that need to be purged from the list.
3. Select **Remove** to remove the custom properties from the server side.
4. Select **Close** to close the editor.



Checking device connection status

You can check the network connection status of a device (if it is connected to the network).

1. In the device table, select one or more devices, and then 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 the following:
 - **Ping**—A basic Internet program that lets you verify that an Internet address exists and can accept requests. Pinging is diagnostically used to make sure that a host computer you are trying to reach is operational.
 - **Trace Route**—Diagnostic tool that 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**.

Template Navigator

The Manage Devices page is a centralized location to manipulate and inspect devices. In addition, the page provides easy access to templates through the through the Template Navigator. Templates from Template Navigator can be dragged to selected devices to send tasks directly.

NOTE:

Templates in Template Navigator are not editable.

Templates and rules

HP Device Manager centrally controls and monitors devices. Templates, Tasks, and Rules are the primary mechanisms to drive configuration changes and updates to devices.

- Templates represent an executable plan or set of instructions that administrators can edit, organize, and share.
- Tasks represent the manifestation of a given template on a managed device that you can track through the stages of execution all the way to completion.
- Rules provide a mechanism to automate tasks based on certain preconditions within the Device Manager system.

Task Templates

HP Device Manager 5.0.14 Server: localhost Login: root

Manage Devices Templates & Rules Tasks & Reports Gateways & Repositories Users & Groups Administration

HP ThinPro 8

Import Templ... Import Images Template Privi... HP Update Ce... HPCEM Add a Rule Import Rule

Templates

Rules

All templates (33)
Private folders
_Favorite (0)
Shared folders

Type	Template	Description	Base template	Category	Status	Modified	Modified by
Settings	._Apply Settin...	Apply settings_Apply Settings	Settings		2024-0...	
Imaging	._Capture Ima...	Capture the im...	._Capture Image	Imaging		2024-0...	
Settings	._Capture Pro...	Capture a profi...	._Capture Profile	Settings		2024-0...	
Settings	._Capture Sna...	Capture the sn...	._Capture Snaps...	Settings		2024-0...	
Operations	._Clear Cache...	Trigger the HP...	._Clear Cached T...	Operations		2024-0...	
Settings	._Clone Settin...	Clone settings_Clone Settings	Settings		2024-0...	
Agent	._Configure A...	Configure HPD...	._Configure Agent	Agent		2024-0...	
Agent	._Configure T...	Configure Task...	._Configure Task...	Agent		2024-0...	
Settings	._Deploy Lice...	This template i...	._Deploy License	Settings		2024-0...	
Settings	._Deploy Prof...	This template i...	._Deploy Profile	Settings		2024-0...	
Operations	._Enable and ...	This template i...	._Enable and Con...	Operations		2024-0...	
Settings	._Enroll Certif...	Enroll a certifi...	._Enroll Certifica...	Settings		2024-0...	
Operations	._Execute Cac...	Trigger the HP...	._Execute Cache...	Operations		2024-0...	
Operations	._Factory Res...	Factory reset.	._Factory Reset	Operations		2024-0...	

Last activity:

1. Toolbar— An enumeration of the Template & Rules most commonly operations.



- Import Template—Import templates from a file (xml, zip).
- Import Images—Generate a template with selected image file to deploy the image.
- Template Privilege— Control each template, including viewing, modifying, and executing operations.

- HP Update Center—Leverage software components from the HP FTP server for use as payload.
 - HPCEM—Generate templates with selected HPCEM installation packages to deploy HPCEM.
 - Add Rule—Create a new rule.
 - Import Rule—Import a rule from a rule file.
2. Template Folder View—A collection of template folders.
3. Template View—List all the templates under the corresponding template folder.

Working with Task Templates

Select the templates navigation view in the Templates & Rules page 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—Displays the name of the template.

Description—Shows the description text of the template.

Base Template—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—Shows a generic template consisting of a customizable combination of tasks for managing device operating systems.
- Connections—Get or set the connection settings of a device.
- Agent—Configure HPDM Agent settings and update HPDM Agent.
- Imaging—Capture or deploy flash-memory images of devices.
- Operations—Perform various operations on a device, such as restart, shadow, shut down, and wake up.
- Settings—Change various settings on the device, such as display, network, time, and write filter.
- Template Sequence—Define sequences in which tasks are performed.

Status—Indicates the status of each template. The status can 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.

Modified—Creation or modification time of template.

Modified by—The creator or modifier of the template. The base template is created by the system, so this property is empty.

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, for example: **_File and Registry**.

To create or edit a task template:

1. Select 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 **Save as** and type a name for the new template.

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

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. Type the name of the template.
4. Select the destination of the exported file.
5. Select **Export** to export the templates. Templates with payload files are exported as ZIP files; otherwise the exported template is an XML file.

Importing task templates

1. In HPDM Console, right-click any template, select **Import**, and then select **Exported Templates**.

-or-

Select **Import Template**.

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 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.

NOTE:

If you want to import and export the template sequence, the deploy image subtask of this template sequence can only be performed once.

Importing templates across operating system versions

Overview

Each template is associated with a specific operating system tab in the HPDM system. Because multiple operating systems are supported so therefore there are more operating system tabs, some templates can be useful for devices under similar but different operating system tabs.

Templates might work on similar operating systems, according to the environment and tools on the target operating system. In this situation, you can make a copy for another operating system; however, you still need to verify the templates case by case.

The term similar operating systems indicates that both operating systems are Windows or both operating systems are Linux.

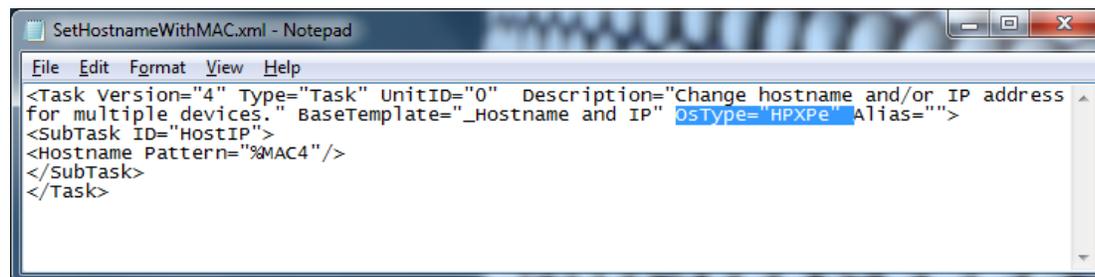
Preparation

Template preparation

1. Log in the HPDM Console.
2. Modify the template you want to copy across operating system tabs to remove operating-system-dependency content.
3. Save the template.
4. Export the template.

Modifying an Exported XML Template

1. Open the exported XML file with any text editor.
2. Find the **OsType** attribute.



3. Change the value of this attribute to the operating system type into which you want to import the template. For example, if you want to copy the template to Windows 10 IoT Enterprise LTSC (64-bit), enter `OsType="HPWE8_64"`.

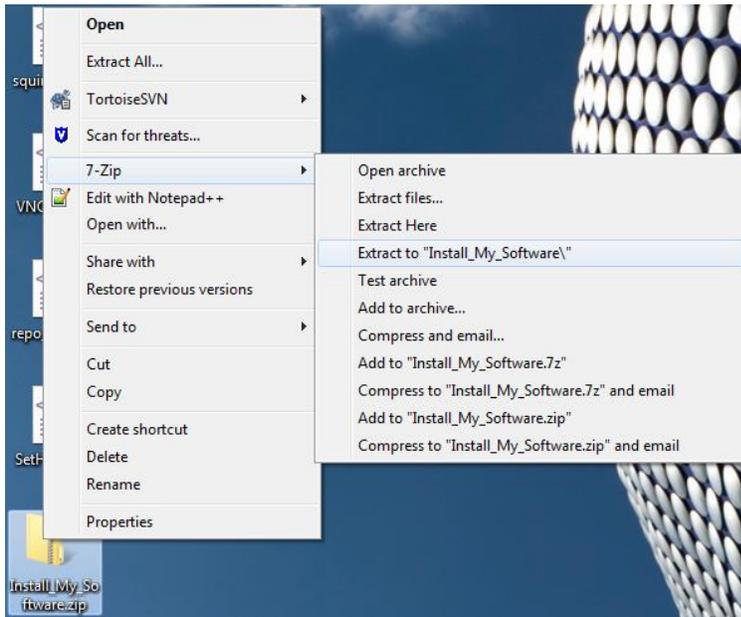
Table 1. Operating system name and database value

Operating system name in HPDM Console	OsType value in database
Windows 10/11 IoT Enterprise (64-bit)	HPWE8_64
Windows (64-bit)	Win64
HP ThinPro 7.2	HPThinPro7-2
HP ThinPro 8	HPThinPro8
HP ThinPro 8.1	HPThinPro8.1

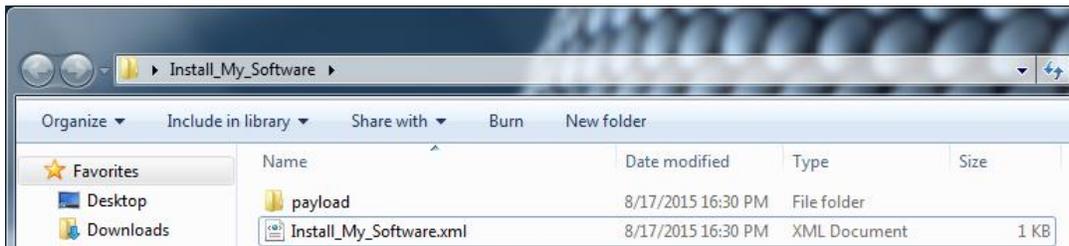
4. Save the exported XML file.

Modifying an Exported ZIP Template

1. Extract the exported .zip that contains the XML file to a folder with the same name.



2. Open the extracted folder, which includes a folder named payload and an XML file.



3. Open the XML file with any text editor.

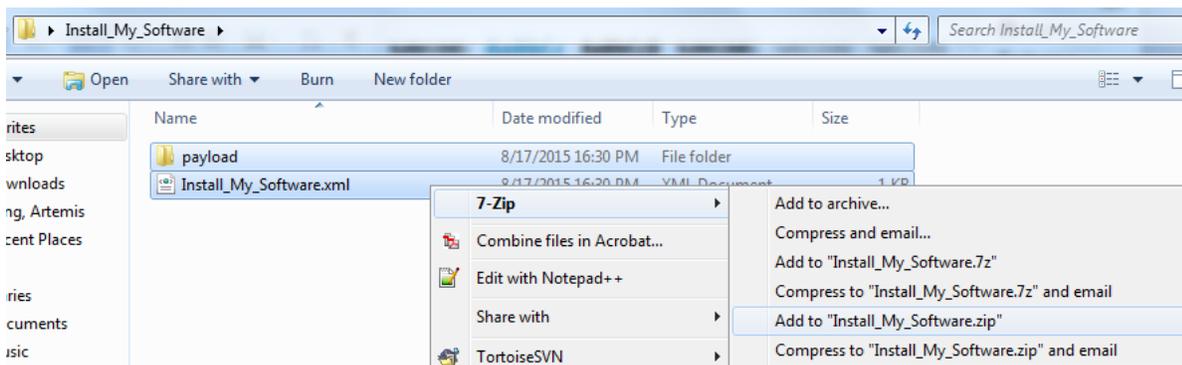
4. Find the OsType attribute.

```

<Task version="4" Type="Task" UnitID="0" Description="Perform customized file, registry and command
sub-tasks." BaseTemplate="_File and Registry" OsType="HPXPe" Alias="">
  <SubTask ID="DeployFiles">
    <FileTransfer Overwrite="true">
      <Directory Direction="download" Path="/Repository/Files/ToDeploy/Install_My_Software">
        <FileItem PathOnAgent="c:\temp" FileName="clone.jpg" IsRecursively="Yes"></FileItem>
      </Directory>
    </FileTransfer>
  </SubTask>
  <SubTask ID="Script">
    <Content type="batch" encrypt="aes_128_cbc" convert="base64">QA5AL5M+agFA446NkoamtD0Q
+Fs8jIky2vGhPGw72lM=</Content><StartIn encrypt="aes_128_cbc" convert="base64">T1IRv4SLK0c1K
+FWqW4DlQ==</StartIn><RunAs><User encrypt="aes_128_cbc" convert="base64">FL
+02upp4VjtI196tmn1gw==</User><Password encrypt="aes_128_cbc"
convert="base64">D0djByuqdiP2jToR79306w==</Password></RunAs>
  </SubTask>
  <SubTask ID="Reboot"></SubTask>
</Task>

```

5. Change the value of this attribute to the operating system type into which you want to import the template. For example, if you want to copy the template to Win10/11 IoT 64bit, enter `OsType=HPWE8_64`.
6. Save the XML file.
7. Select both the folder and the XML file and add them to a new ZIP file with the same name.



Importing Modified Templates

Importing an XML Template

1. On the template page, right-click on any template, and then select **Import > Exported Templates (*.xml, *.zip)**. Or select the **Import Template** toolbar button on the template page.
2. Select the modified XML files and then select **Import**.

Importing a ZIP Template

1. On the template page, right-click on any template, and then select **Import > Exported Templates (*.xml, *.zip)**. Or select the **Import Template** toolbar button on the template page.
2. Select the ZIP file you created in Modifying an exported ZIP file template, and then select **Import**.

Generating a template from payload

1. In HPDM Console, right-click on any template, select **Import**, and then select one of the following menu items:

Image Files

2. Select the file that you want to import.
3. Select **Import**. Then add payload information in the **Package Description Editor** 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 another 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.

Table 38. 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, select the default **_Template Sequence** template to open the Template Editor.

Basic template sequences

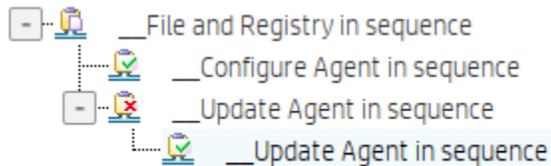
A basic template sequence uses the same condition between every task and can be defined by selecting the **Content** tab, and then selecting **Basic**.

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

Templates folder

The template folder is a collection of task templates for managing task templates. Template folder is divided into three types:

- All templates—List of all task templates.
- Private folders—Private folder that only the current user can see and operate. There is a built-in folder in the private folder called “_Favorite”, which lists all the favorite task templates of the user. There can only be one favorite folder.

- Shared folders—Shared folder that all users can see. Only users with Template Shared Folder Management privileges can operate the shared folder.

Adding a folder

1. Right-click on **Private folders** or **Shared folders**, and then select **Add Folder**.

– or –

Right-click a folder and select **Add Private/Shared Folder**.

2. A template folder named “New Folder” is added. You can change the folder name.
3. Save the folder by pressing **Enter** or clicking on the blank.

NOTE:

A folder cannot create a child folder.

Deleting a folder

Right-click the folder and select **Delete** from the pop-up menu.

NOTE:

You cannot delete “_Favorite”, “All templates”, “Private folders” and “Shared folders”.

Renaming a folder

1. Right-click the folder, and then select **Rename**.
 2. Type the name, and then press **Enter** or click on the blank to save.
-

NOTE:

“_Favorite”, “All templates”, “Private folders” and “Shared folders” cannot be renamed.

Adding a template to a folder

- Right-click the task template and select **Copy to** or **Move to**, then click on the folder name.
- Drag the task template to the target folder.
- Save the template in the folder. The template is added to the folder.

Removing a template from the folder

- Select the target folder, right-click the task template, and then select **Remove from folder**.
 - When the template is deleted, the template is also removed from all folders.
-

NOTE:

Other than “All templates,” any template can be removed in the folder. The template under “All templates” can only be deleted.

Task rules

Rules allow you to automate the execution of tasks. Each rule has four parts: a folder to define to which devices the rule applies, a filter to determine if devices under target folder need to take action, a trigger that defines when the rule is executed, and a template which defines what operation to perform on to the devices.

- All rules are shown on the Templates & Rules page under **Rule** navigation view— **Rule detail** view. You can execute operations in this view that include edit, delete, import, export, run a rule immediately, and sort (only Startup rules and First Contact rules can be sorted).
- All rules for a selected folder and device are shown under **Properties – Rule panel**.

Trigger type

Trigger type rules execute as follows:

- First Contact - 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 - Executes for each device that matches its filter criteria every time the device restarts.
- Schedule - Specifies time and date when the rule is executed and the frequency at which it repeats, as follows:

- Only once
- Daily
- Weekly

Target folder

After you select a folder (manual group folder or dynamic group folder), all devices under the folder are target devices of this rule.

Rule compliance

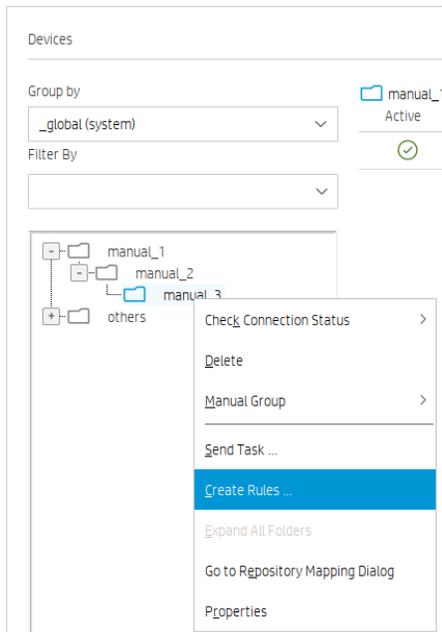
When in compliance, image version, software, and other settings or configurations on a device match the expected value/state.

You can view the Compliance of rule at:

- Templates & Rules page – Rule navigation view– Rule detail view.
- Device Properties - Rule panel.
- Folder Properties – Rule panel.

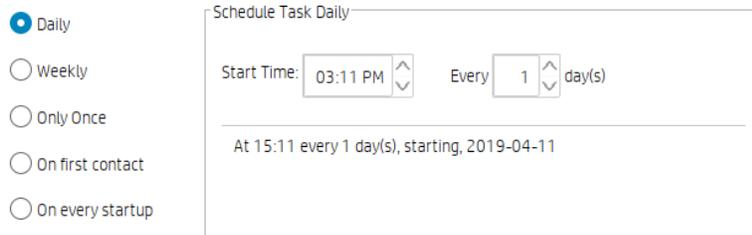
Adding a new rule

- Entrance to create a rule:
 - Right-click on a folder (manual group folder or dynamic group folder), and then select **Create Rule**.



- Select **Add Rule**.

- In **Rule Wizard**, type a rule name and description for the General page.
- Specify **OS Type** and **Target devices** (All devices or devices in the specified folder).
- Specify any device properties you want to use to constrain this rule. For Startup rules, devices matching below criteria display as **Noncompliant**. Be sure the action changes device properties so that this rule does not fall into an endless loop.
- Select a rule trigger.

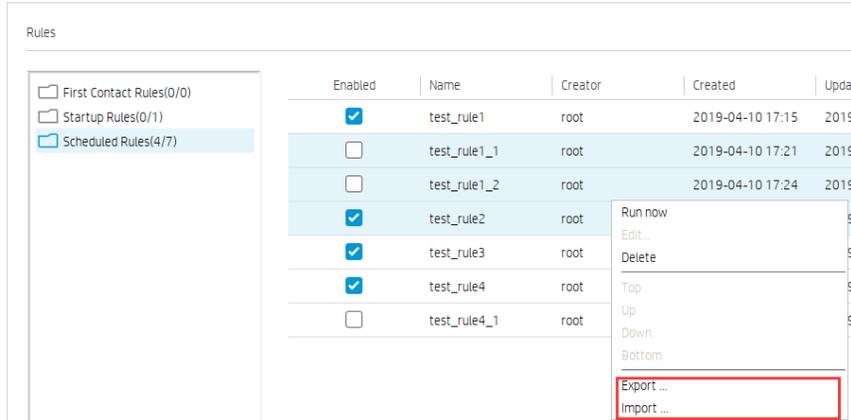


- Specify the template to use.

7. Edit task parameters.
8. Use the **Show devices** button to view all target devices.
9. Select **Finish** to end the process. The rule runs immediately if you selected **Run now**. All rules are shown on the **Templates & Rules** page in **Rule navigation** view > **Rule detail** view.

Export and import rules

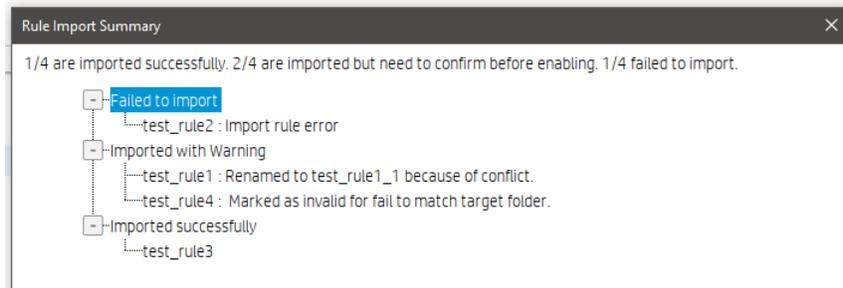
1. Entrance to export or import rule is shown on the Templates & Rules page in **Rule navigation** view. Right-click the rule table, and then select **Export** or **Import**.



- **Import Rule** toolbar button:



3. When importing rules, provide a summary dialog to show all imported rules and import result. You can export or import multiple rules at once.



4. Imported rules are disabled by default. You can manually enable.
5. Rules without a matched folder are marked as invalid and cannot be triggered and enabled. You can edit them and set a new target folder.

Tasks & Reports

Tasks

Tasks Interface

The screenshot shows the HP Device Manager 5.0 interface with the 'Tasks & Reports' tab selected. The left sidebar has 'Device Tasks' highlighted. The main content area displays a table of Device Tasks. A toolbar above the table includes buttons for 'Manage Device Tasks', 'Refresh Device Tasks', 'Audit Logs', 'Manage Gateway Tasks', 'Refresh Gateway Tasks', and 'Add Report'. A legend at the bottom right shows task statuses: Waiting (yellow), Paused (brown), Sending (orange), Processing (light blue), Cached (blue), Finished (green), and Failed (red).

Task ID	Task Name	Progress and Stat...	Target Device Nu...	Create Time	Sender	OS Tab
00000003	_Get Asset Informat...	2 (100%)	2	2019-04-08 17:16...	test	WES7E
00000002	_Get Asset Informat...	2 (100%)	2	2019-04-08 15:01...	root	WES7E

1

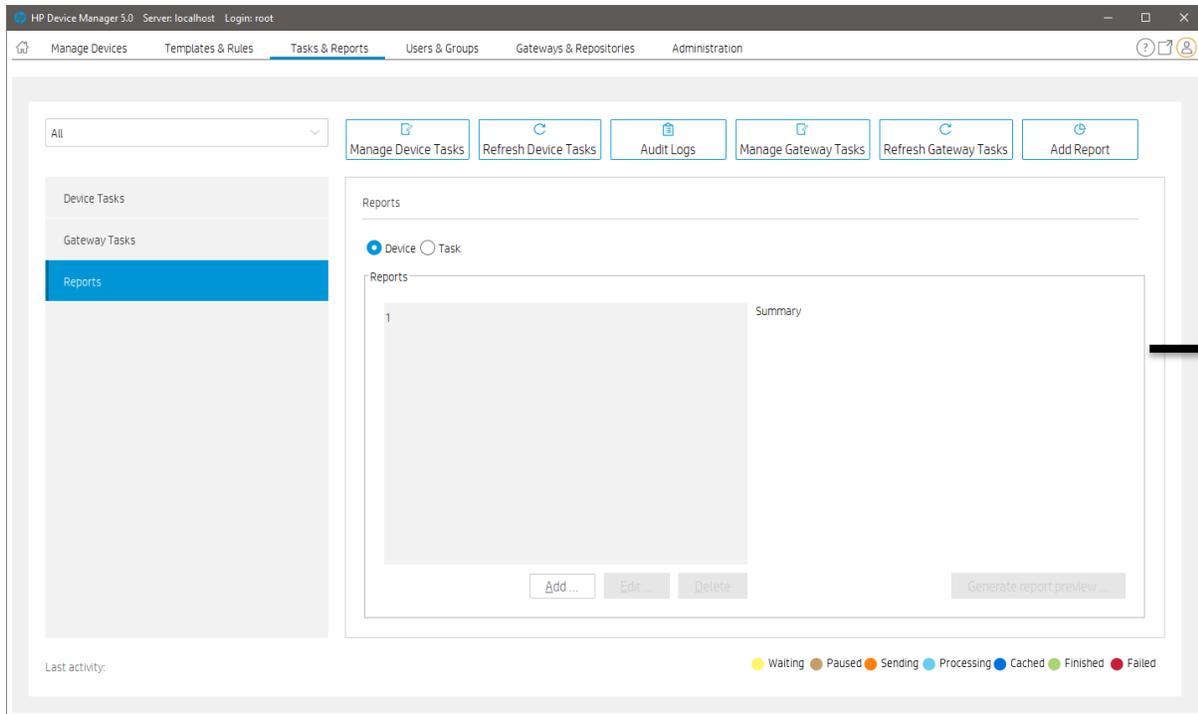
2

3

The screenshot shows the HP Device Manager 5.0 interface with the 'Tasks & Reports' tab selected. The left sidebar has 'Gateway Tasks' highlighted. The main content area displays a table of Gateway Tasks. The toolbar and legend are the same as in the previous screenshot.

Task ID	Task Name	Task Status	Start Time	End Time	Sender	Hostname
00000004	Discover Device	Expired	2019-04-08 17:18...	2019-04-09 17:19...	test	host-00001

4



1. Toolbar— An enumeration of the Tasks & Reports most commonly operations.



- Manage Device Tasks—Go to the device task view.
- Refresh Device Tasks—Refresh all device task status.
- Audit logs—Open audit log view.
- Manage Gateway Tasks—Go to the gateway task view.
- Refresh Gateway Tasks—Refresh all gateway task status.
- Add Report—Create a new report.

2. Device Tasks View—All device tasks visible to the current user.

NOTE:

The device filter operates here. **Number of tasks to view** sets the maximum number of tasks visible to the user.

3. Task status legend—See **Task Status** for more information.

4. Gateway Tasks View—List all gateway tasks.

5. Report View—Displays report management.

Working with Tasks

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

- Manual Tasks—Created directly using HPDM Console.
- Rule Tasks—Created indirectly using rules.

All sent tasks 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—The ID of the task.
- Task Name—The name of task template used to send this task.
- Progress and Status—The progress and status of the task.

- Target Device Number—The number of devices to which the task was assigned.
- Create Time—When the task was created.
- Sender—The sender of the task.
- OS Family—The operating system family it belongs to.

Performing a task

1. Drag a task template from the template 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** to open the Template Chooser. Select a category, select a task template, and then select **Next**.

2. The **Task Editor** box is displayed. Select the **Schedule & Batch Control** tab and specify when and how to perform the task defined in the template. 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 **OK**.

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

Task status

Task statuses are as follows:



- Waiting: The task is scheduled to send at a later time.
- Paused: The task is paused.
- Sending: The task is currently sending from HPDM Server through HPDM Gateway to the device and is waiting for a reply.
- Processing: The task was accepted by the device and is being processed.
- Cached: The task and its payload are cached on the device and can be processed later.
- Finished: The task was executed successfully by the device.
- Failed: The task has failed or timed out.

Task parameters

You can set default values for some task parameters using the Configuration Management dialog. In HPDM Console, go to **Administration > Configure System**, and then expand the **Task Parameters** tree in the left pane.

The Task Parameters tree consists of the following items:

- Valid Time and Timeout—Allows you to configure the following default parameters:
 - Valid time—Defines the upper limit for the duration between task dispatch to the gateway and its retrieval by the agent. If the HPDM agent fails to respond to HPDM GW during this interval, the task will be canceled or failed.
 - Execution timeout—Defines the processing time limit after a task is retrieved from HPDM GW by agent. If the task surpasses this limit, it will be marked as timeout, denoting an intermediate status. Subsequently, the task will eventually transition to a final status such as failure or success.
 - 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).
 - Automatically cancel tasks after Execution Timeout – Enables automatic task cancellation once a task reaches to Execution Timeout limit.
 - 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 (Windows only).

Ephemeral mode policy – Specifies how to handle the task if the On Boot Snapshot is set (ThinPro 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).

- 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).

- **Transfers**—Allows you to define the HTTP Repository Speed Limits for payload related tasks.

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

- **Content**—Allows you to specify parameters specific to the type of task.
 - **Target Device List**—Lists the devices the task is applied to and allows you to add or remove devices.
-

Note

When you configure a rule, there is a step to configure rule task parameters.

Task deferment

Task deferment allows users to save their work before an HPDM-initiated restart or shutdown of the device. Before restart or shutdown, a dialog box displays that allows users to postpone or initiate immediately the restart or shutdown. The user can postpone the restart or shutdown a maximum of three times.

You must send a **_Configure Task Deferment** task to the device before you can defer any tasks. 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 does not display.

Viewing task properties

To display the properties of a task: right-click a task and select **View Task Contents**.

Pausing a task

To pause a task:

1. Select a task in the task pane.
 2. Right-click the task, and then select **Pause**.
-

NOTE:

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

Resuming a task

To continue a paused task:

1. Select a paused task in the task pane.
2. Right-click the task, and then select **Continue**.

The status of the paused task changes to Waiting.

NOTE:

You can only resume paused tasks (tasks that have not been sent).

Resending a task

If a task has completed, you can resend the task to the device:

1. Select the finished task in the task pane.
2. Right-click the task, and then select **Resend**.

Canceling a task

To cancel an active task, right-click the task and select **Cancel**.

NOTE:

You can cancel only ongoing tasks (tasks in the Sending or Processing state). You cannot cancel all tasks on the device side. For example, a task might complete before the system delivers the cancel request. Unsuccessfully canceled tasks are listed on reports.

Deleting a task

To delete a task, right-click the task and select **Delete**.

WARNING!

Deleting a task (such as updating and upgrading tasks, image deployment tasks, and so on) that is in progress may damage the operating system image.

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.

Viewing 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** or double-click a task in the task panel.
 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.

Viewing task status and device details (Device Properties)

To display the task status of each device in a task:

1. Right-click a task in the task pane and select **View device tasks and logs** or double-click a task in the task panel.
2. Check the **task status** table.
3. Double-click an entry in the table to open **Device Properties Dialog** to check the device details.
4. Right-click an entry in the table to open the context menu with the **Copy Hostname** option to get device hostname.
5. Select **Close** to close the viewer.

Viewing task success ratio

To display a task's success rate, right-click the 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.

Device shadowing

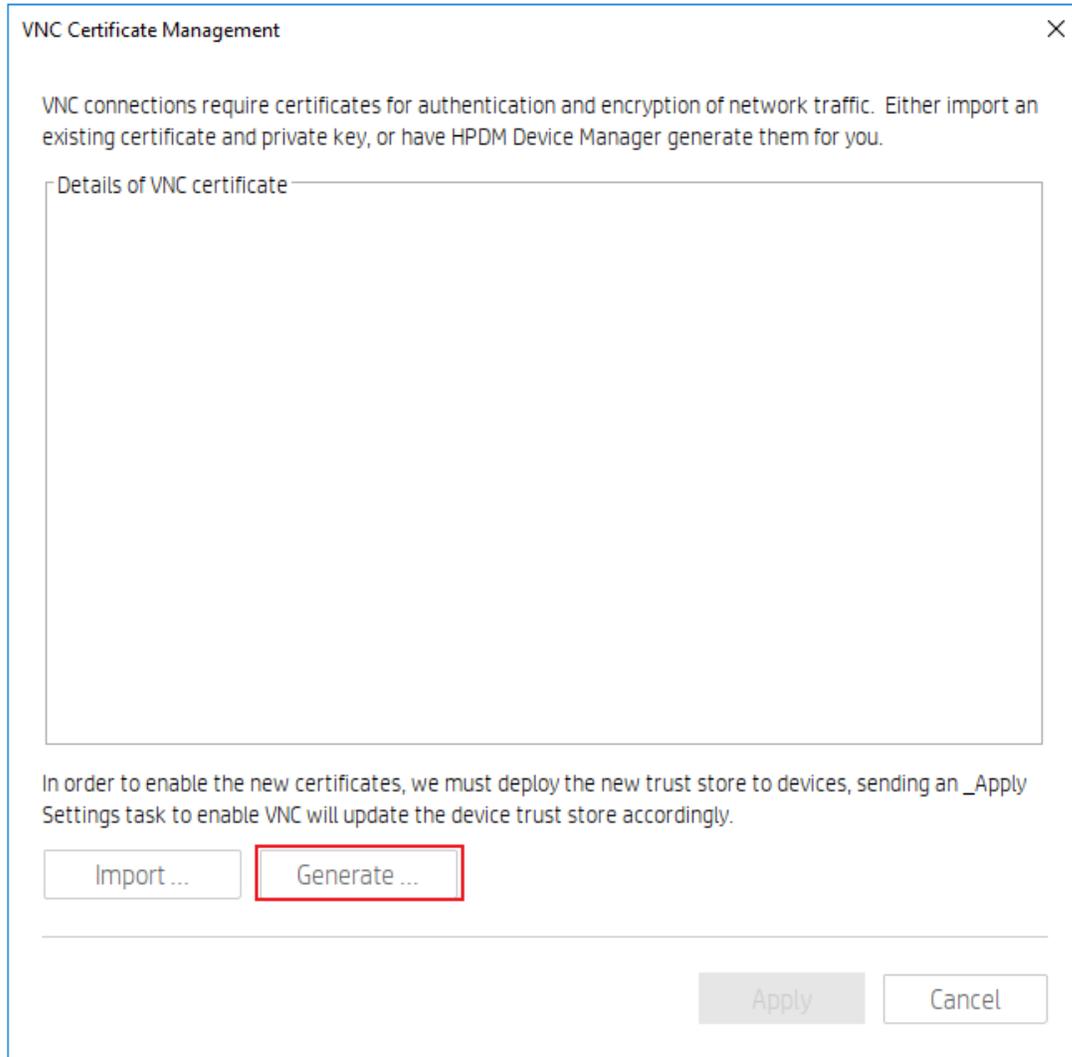
You can remotely control a device with VNC using the **_Shadow** or the **_Reverse Shadow** templates. Certificate authentication for VNC connections is enabled beginning with HP Device Manager 5.0.1. Use the following steps to prepare your Console and devices before shadowing.

1. Configure VNC certificates on Console

Go to “**Administration**” page, click “**VNC Certificate**” toolbar button

The available options allow you to use an HPDM-generated certificate or import your own certificate.

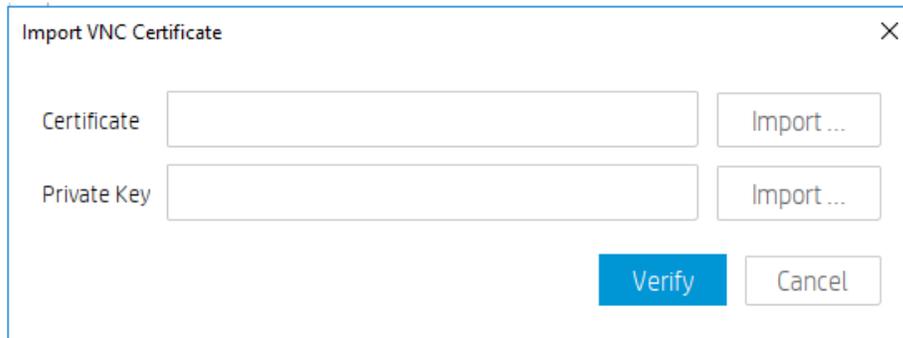
- Using the certificate generated by HPDM, as followed:



Click the “**Generate ...**” button to generate a new certificate. The “**Details of VNC certificate**” panel will display the certificate details. Then click the “**Apply**” button to save the certificate to the server.

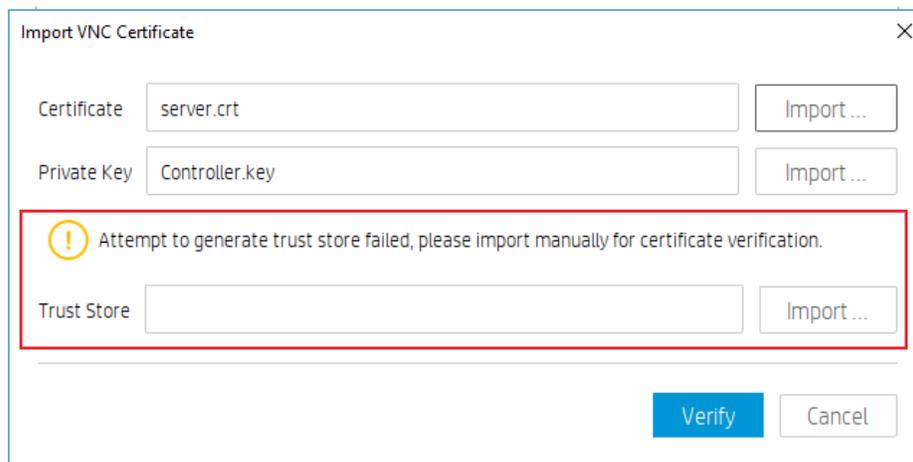
- Using your own certificate

Click the “**Import ...**” button above to import your own certificate. As followed:



Import the paired certificate and private key.

HPDM will look from the Windows system for the root certificate and all intermediate certificates used for generating the trust store. If any of the certificates are missing, the generation will fail. In that case, you will need to import the trust store manually. As followed:



The Trust Store contains all intermediate certificates and the root certificate.

There are two solutions for reference:

- You can install all intermediate certificates and root certificates, reopen the above dialog and import again.
- Ask your certificate provider for a trust store containing all certificates in the chain.

Click the “**Verify**” button to verify the certificate. If the verification is successful, you will see the details of the certificate. If it fails, an error prompt will be displayed.

Note: If the attribute of the certificate for Enhanced Key Usage exists, it must include both **Server Authentication** and **Client Authentication**. **Server Authentication** is required for the reverse shadowing. **Client Authentication** is required for direct shadowing.

2. Update HPDM Agent on target devices to 5.0.1 or higher version.

Note: If the shadow / reverse shadow task execution result shows an error that the trust store is missing, it means the HPDM agent needs to be upgraded.

3. Deploy certificates to devices.

Create a new “**_Apply Settings**” task with VNC Settings. Send this task to the target devices.

The configuration of VNC Shadow needs to be set to **Enable**. Other configurations are optional.

The screenshot shows the 'Edit Settings Wizard' window. On the left is a 'Page List' with 'Settings Choice', 'VNC Settings' (highlighted), and 'Summary'. The main area is titled 'This template is used to changes the VNC settings on device.' and contains the following settings:

- VNC Shadow: Enable (dropdown)
- Trust Store: Imported (text field) with a [Manage Certificate ...](#) link.
- VNC Use Password: Unchecked. Below it are two text input fields: 'Enter Password: (1 - 8 characters)' and 'Retype Password:'.
- Auto-Accept: Disable (dropdown)
- VNC show timeout for notification: 0 (spin box)

At the bottom right are buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

The successful execution of this task ensures the deployment of the certificate to the target devices.

Note: If the trust store displays "not imported", you can also click the "Manage Certificate ..." link to enter the certificate management dialog.

Once the certificate has been deployed, you can send a task with the **_Shadow** or **_Reverse Shadow** template to remotely control the managed devices.

Result Template

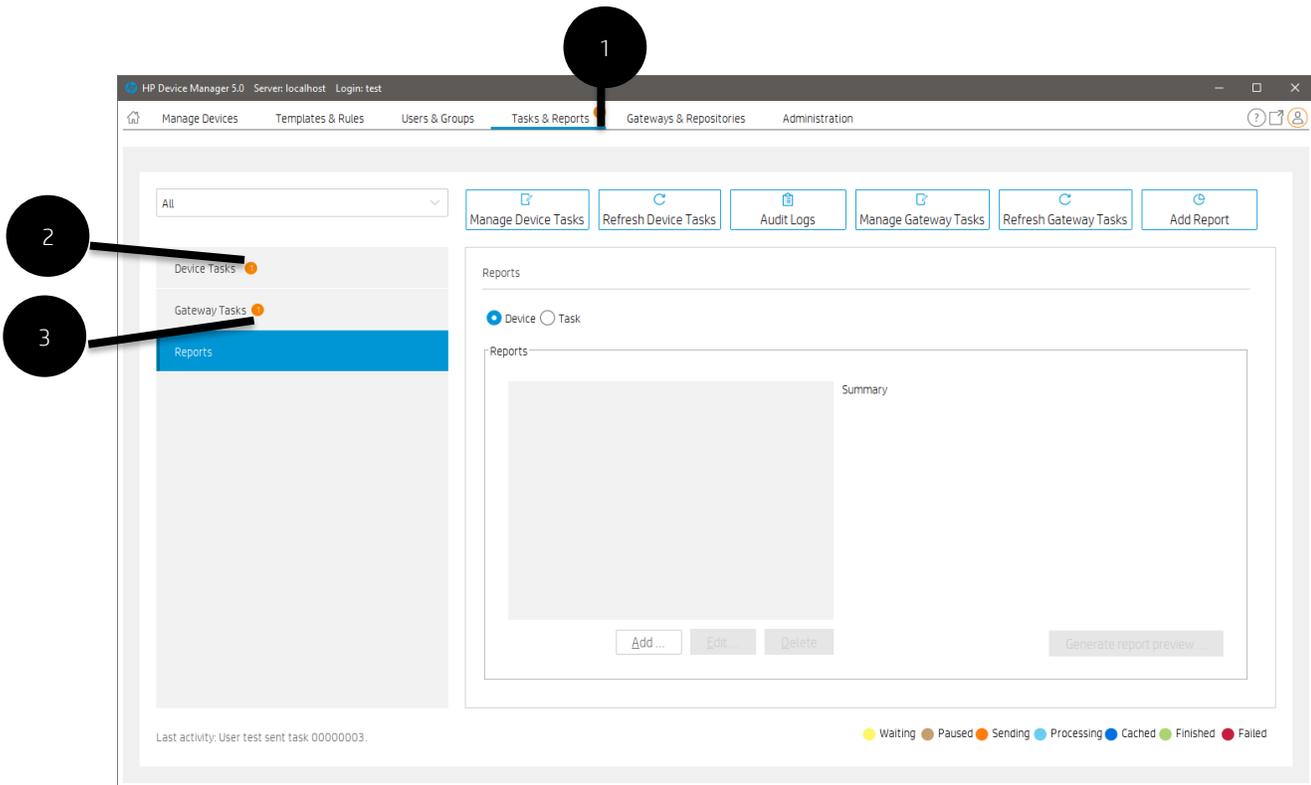
Right-click a ready task and select **Open Results Template** to open the results of some tasks such as Get Registry, Pull Connection Configuration, and Capture.

Displaying tasks from all users

If you have the View Tasks from All Users privilege, you can view all tasks sent by all users. You can also resend, pause, continue, cancel, and delete any task sent by any user.

Task Notifications

When the console receives a new task notification, the notification is displayed.



The notification of the Tasks & Reports page informs only the sum of the device task and the gateway task. Samples are shown in previous screenshot as 1-3.

The notification is cleared when the item on navigation view is selected.

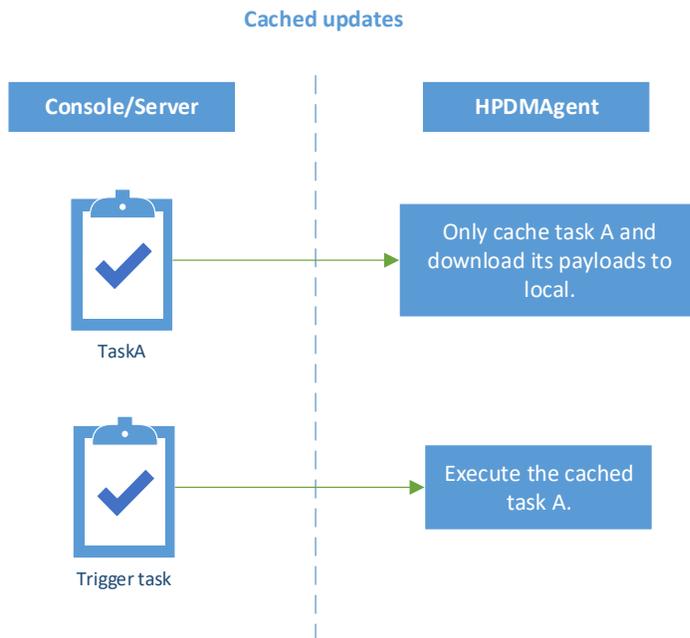
Cached tasks

Cached updates provide a solution if which one task is separated into two distinct steps: caching and execution. This document introduces cached updates, details some usage scenarios, explains how to use this feature, and provides instructions for configuring cached updates.

Cached updates

The following workflow demonstrates the cached update feature.

Figure 8. Cached updates



When the HPDM Agent receives a task, the Agent caches task content and downloads its payloads (if necessary) to a local cache. The HPDM Agent then notifies HPDM Server to update the task status to Cached. If you want the HPDM Agent to execute this cached task, send a trigger task to the target device. The HPDM Agent executes the cached task and sends reports to the HPDM Server.

Note

(ThinPro) The cached update features is also unavailable when the On Boot Snapshot is set. Please disable the On Boot Snapshot on the device before using Cached Updates.

Usage scenarios

Cached updates enhance the flexibility of HPDM. It solves issues that exist in many complex network environments, and is useful in the following scenarios:

- You are using a complex network, such as VPN or 802.1x.
 - For most of the tasks, because of the limitations of write filters on Windows operating systems, the HPDM Agent needs to reboot to disable the write filter to execute the tasks.
 - In these network environments, if the Writer Filter is enabled, some tasks cannot be finished without help from a local user.
- You want to download the payloads or updates during working hours, and then install those updates after working hours.
For example, you want to update 10,000 devices over the weekend. With cached updates, the devices can download the payloads throughout the previous week, and you can then trigger all 10,000 devices to update at midnight Saturday.
- You do not want to interrupt the current local user's operation when performing tasks.

Using cached updates

If you want the HPDM Agent to execute a task in cached updates mode, you need to send the task with cached updates to the device first, and then send an `_Execute Cached Tasks` task to the device. This tells the HPDM Agent to execute the cached task. If you want to remove tasks cached on a device, send a `_Clear Cached Tasks` task to the device.

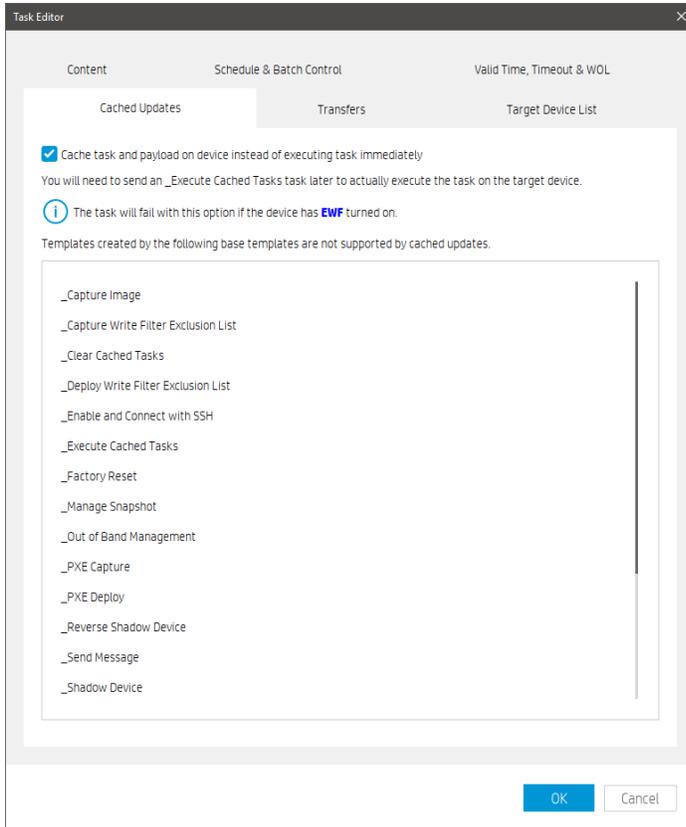
Sending a task in cached updates mode

1. Open the Task Editor and select the **Cached Updates** tab.
2. Select **Cache task and payload on device instead of executing task immediately**, and then select **OK**.

Note:

The default value of the Cache task and payload on device instead of executing task immediately option is set to false.

If the **Cache task and payload on device instead of executing task immediately** option is grayed out in the Task Editor, the task is not supported by cached updates. For more information, see Blacklist.



When the status of the task is Cached, the task has been cached on the device.

Note:

The Cached task status does not block follow-up task. Any tasks following this task can be sent to the device after the task is cached locally. You can send multiple tasks in cached updates mode to a device, one by one. All cached tasks on the HPDM Agent are triggered when an **_Execute Cached Tasks** task is received.

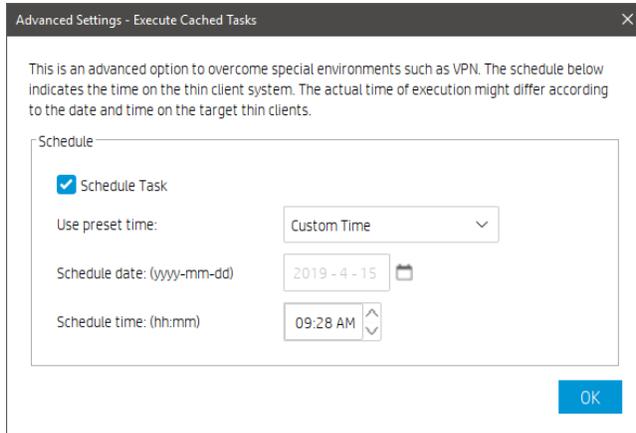
Task ID	Task Name	Progress and Status	Target Devic...
00000006	_Get Asset Information	1(100%)	1
00000005	_Get Asset Information	1(100%)	1
00000004	_Reboot Device	1(100%)	1
00000003	_Get Asset Information	1(100%)	1
00000002	_Automatic Update Agents HPThinPro6...	1(100%)	1

4. After the task is cached on the device, send an **_Execute Cached Tasks** task to the device to execute this cached task.

Executing tasks cached on a device

To execute the cached tasks, send an **_Execute Cached Tasks** task, or trigger task, to the device.

1. Select the **_Execute Cached Tasks** template and drop it on the target device.
2. Select a failure option.
3. Optionally, if you want the HPDM Agent to execute the cached tasks at a specific time, configure the schedule parameter of this template. If you do not configure the schedule parameter, the HPDM Agent executes the cached tasks immediately after receiving the trigger task.
 - a. Select **Advanced**.
 - b. Select **Schedule Task**, select a preset time or a schedule date and time, and then select **OK**. The schedule time uses the device local time.



– or –

Set the **_Execute Cached Tasks** task as a schedule task.

Note:

The differences between using the schedule parameter of the **_Execute Cached Tasks** task or setting the **_Execute Cached Tasks** task as a general schedule task are as follows.

Behavior	Schedule parameter	Schedule task
Schedule control	HPDM Agent	HPDM Server
Time basis	Device local time	HPDM Server local time
Blocking follow-up tasks	Yes	No
Requires network connection when schedule hits	No	Yes

A general scheduled task is not sent by the HPDM Server before its scheduled time. At that time, the HPDM Server sends the task through HPDM Gateway to the HPDM Agent. If there are multiple target devices for the task, they receive the task at the same time. Until the task is sent, its status is Waiting. Any tasks sent before this scheduled time are not blocked by the scheduled task.

The schedule parameter in the **_Execute Cached Tasks** task uses the device local time. The HPDM Server sends the task to the target device immediately. When the HPDM Agent receives the task, its status is Processing. The HPDM Agent does not execute the **_Execute Cached Tasks** task until the scheduled time on its local system.

HP recommends that you configure the schedule parameter of the **_Execute Cached Tasks** task instead of setting it as a schedule task, especially if you are using a complex network.

4. Select **OK**. After the cached task is executed, its status becomes either Finished or Failed.

Removing cached tasks from a device

To remove cached tasks that you do not want to execute from a device, you can send a **_Clear Cached Tasks** task to the target device. The HPDM Agent removes all cached tasks and their payloads after receiving this task, and then sends reports to HPDM Server. After receiving the reports, the HPDM Server updates the task status of original cached tasks to Failed.

Note:

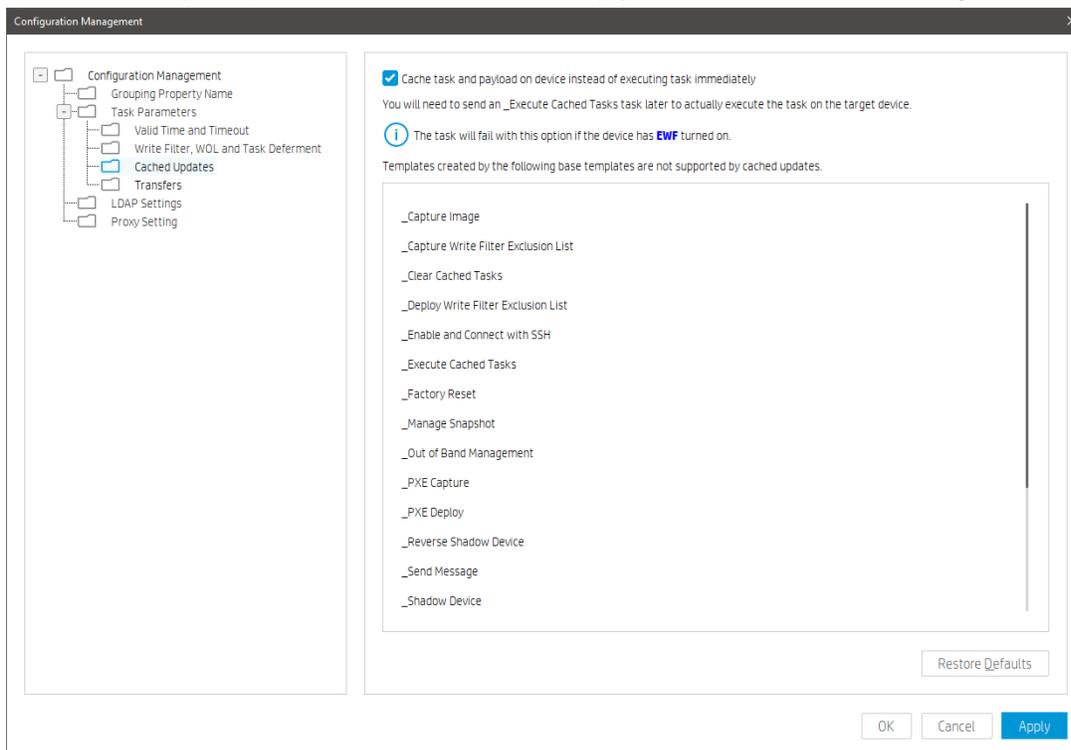
HPDM does not support removing a single cached task when multiple tasks are cached on a device.

Configuring cached updates*Configuring the task parameter of a cached update on the HPDM Console*

The default value of the Cache task and payload on device instead of executing task immediately option is false. If you set this value to true, all tasks supported by cached updates are sent in cached updates mode.

To set this value to true:

1. In the HPDM Console, select **Administration > Configure System**.
2. Expand **Task Parameters**.
3. Select **Cached Updates**, and then select the **Cache task and payload on device instead of executing task immediately** option.



4. Select **OK** or **Apply**.

Blacklist

The blacklist is a list of base templates. Templates created by base templates in the blacklist are not supported by cached updates. Whether the value of the Cache task and payload on device instead of executing task immediately option is true, these templates are never sent cached updates mode.

To view which base template included in the blacklist:

1. In the HPDM Console, select **Administration > Configure System**.
2. Select **Task Parameters > Cached Updates**.

Disabling the lock screen option

For devices running a Windows operating system, the screen is locked while cached tasks are executing, and by default the local user cannot operate the system.

To disable this option:

1. Open the HPDM Server configuration file serverconf.xml.
2. Locate the following line:

```
<Attribute Name="hpdm.lockscreen.showtime" Value="10" Enabled="yes"
SN="0"></Attribute>
```

3. Change the value of **Enabled** to **no**.

```
<Attribute Name="hpdm.lockscreen.showtime" Value="10" Enabled="no"
SN="0"></Attribute>
```

4. Restart the HPDM Server.

Cached update limitations

-
- Because of the limitations of the Unified Write Filter (UWF), deploy image tasks in cached updates mode are not supported when the UWF is enabled.
- Because of the limitations of the UWF, deploying a file larger than 1 GB with cached updates might fail when the UWF is enabled.
- Because of the limitations of the Ephemeral Mode, cached update is not supported when the On Boot Snapshot is set.

Task template reference

Table 32. File and registry

Template	Description
_File and Registry	A multi-purpose template that allows the execution of general-purpose scripts to collect or set values on a given device.
_Get Registry	Enables the retrieval of registry attributes from a given device.

_File and Registry

This template enables you to create a sequence using these subtasks:

Capture Files

This subtemplate allows you to capture files from devices.

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

1. Select 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. Select **Add** to create additional lines.

The wildcards * and ? are supported in the lowest level of the path or file name, as follows:

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.

The subtemplate supports five parameters (macros) to allow you to put captured files from different devices in different folders. You can select the button after **Files\Captured** to set them into the target path. You can also input them manually. The parameters are:

- a) %ID% - Device ID
- b) %SN% - Device serial number
- c) %HOSTNAME% - Device host name
- d) %DATE% - Device local date

e) %TIME% - Device local time

You can set multiple macros at a time. The Sample string tells you the format of the folders.

For example, if you want to capture a file daily, you can set %ID%_%DATE%.

5. (Optional) Select **Overwrite if exists**.
6. Select **OK** when you have completed 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 devices.
9. Select **OK** to apply the task to the devices.

Deploy Files

The subtemplate allows you to deploy files to devices.

To deploy files to devices:

1. Select the **_File and Registry** template to open the Template Editor.
2. Select **Add**, select the **Deploy Files** subtask, and then select **OK**.
3. Select **Add from local** to choose files from the local machine. If you want to deploy a selected file or folder to another path, you can use the Choose Upload button.
4. Edit the **Path On Device** to set the path on devices.
5. Select **OK** when you have completed specifying files.
6. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the **Task Templates** list.
7. Edit the contents in the **Package Description Editor**.
8. Select **Generate** to generate HPDM Package and the template.
9. Drag and drop the template onto the devices.
10. Select **OK** to apply the task to the devices.

Delete Files

The subtemplate allows you to delete files in devices.

To delete files from devices:

1. Select 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 are not 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.

Script

The subtemplate allows you to run a script in devices.

To run a script on a device:

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

When enabled, the Script option **Wait for the script to finish executing**, causes Agent to wait for the exit of process, captures outputs and the exit code, and then reports execution result to HPDM Server. When disabled, Agent only executes the script and reports successful to HPDM Server immediately. This value is enabled by default.

This option is for the cases that the script reboots devices, where Agents have no chance to report the executing result, so they repeatedly retrieve the task. If you assume the script will reboot the device, please clear the option and add several seconds sleep to make sure Agent can report the result correctly.

For example, you can add `sleep 2` before the formal ThinPro shell script or add `ping localhost` before the formal Windows batch script.

Registry

This subtemplate allows you to set registry values to devices.

To add, edit, or delete registry settings:

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

If you want to create a new template, select to open the **_File and Registry** 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 devices.
6. Select **OK** to apply the task to the devices.

Program record:

The subtemplate allows you to add or remove a program record in devices.

After you install some patches, if you want to tag that some patches are installed, you can use this sub-template to tag it.

To add or remove program records:

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

Command (deprecated)

The subtemplate allows you to execute commands. It is deprecated. HP recommends that you use the **Script** subtask.

Pause

You can pause a **_File and Registry** task to wait for certain events such as the previous Script subtask needs extra time to do something after it returns.

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**.

_Get Registry

The template enables you to retrieve one or more keys from a device registry.

To retrieve registry settings from a device:

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

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 selecting the new template, selecting the Registry subtask, and then expanding the registry node in the Registry Tree.

Table 33. Agent

Template	Description
_Configure Agent	Enables the configuration of Agent parameters on a given device or devices.
_Configure Task Deferment	Allows an administrator to define conditions where the device user may be able to defer the application of management updates (Tasks) that would otherwise interrupt their productivity on the device.
_Update Agent	Allows you to update the Agent version on an existing device with the Agent version supplied within the template payload.

_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.

The Contents show the configurations you can configure.

Current Gateway - Set Current Gateway: Agent retrieves the current gateway value and tries to connect when Agent starts.

Backup Gateway - Set Backup Gateway: When the current gateway value is empty, Agent retrieves backup gateway value and tries to connect.

Pull Interval - Set Pull Interval: Defines the frequency at which HPDM Agent sends a startup reports to HPDM Gateway to retrieve tasks.

Delay Scope - Set Delay Scope: After started, HPDM Agent sends a startup report at a randomly chosen time between 0 and the selected Delay Scope.

Log Level - Set Log Level: You can select the log level in the comboBox. After configuring Agent options, select **OK**.

Auto-set Gateway - Set Auto-set Gateway: Indicates if Agent will change the Current Gateway address automatically when it receives a task from a Gateway successfully. You can select Yes or No in the comboBox. If No, HPDM Agent will not change the Current Gateway address.

_Configure Task Deferment

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

Task deferment allows users to save their work before an HPDM-initiated restart or shutdown of the device. Prior to the restart or shutdown, the user can postpone or immediately initiate the restart or shutdown. The user can postpone the restart or shutdown up to three times.

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

1. Move **_Configure Task Deferment** template to the device to open the Task Editor.
2. In the Content panel, configure options in the Task deferment parameters dialog. You can customize the Title and Message in the Prompt Information dialog.
3. In the Task deferment parameters dialog you can define the following parameters:
 - Maximum chances to postpone. You can define value in 0-65535 in this line edit.
 - Maximum postponement time. You can define value in 0-65535 in this line edit.
 - Default postponement time. You can define value in 0-65535 in this line edit (in minutes).
 - Remind before reboot/shutdown: defines the time that remind before reboot/shutdown in seconds. You can define value in 0-65535 in this line edit.

After configuring Task Deferment, select **OK**.

Note:

If the device needs to forcibly restart, the dialog box does not display.

_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.

1. Move the **_Update Agent** template to the device to open the Task Editor.
2. Select **OK**.

Connections

Table 34. Imaging

Template	Description
_Capture Image	This template captures an image from the target device and upload it to the Master Repository. It also creates a new Deploy Image template to install the image to other devices. This template can only be sent to a single device at a time.

Table 35. 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 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.
_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 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 displays. 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 for devices in the same subnet with HPDM Gateway, as well as for devices that are not in the same subnet of HPDM Gateway, if the subnet has at least one online HPDM Agent. Devices behind NAT can wake up if the subnet has at least one online HPDM Agent. During timeout, HPDM Gateway reports the unfinished part as failure.

Table 36. Settings

Template	Description
_Apply Settings	Creates a set of custom settings and deploy them to one or more devices.
_Auto Logon Configuration	Configures automatic logon settings on devices.
_Capture EasyShell Settings	Captures EasyShell settings from a device.
_Capture Profile	Captures a profile from a device.
_Capture Snapshot List	Captures a snapshot list from a device.
_Capture Write Filter Exclusion List	Captures the HPWF/UWF exclusion list from a device running a Windows operating system with HPWF or UWF.
_Clone Settings	Lets you copy a selection of custom settings from one device and deploy them to other devices.
_Deploy License	Deploys licenses to devices.
_Deploy Profile	Configures a profile and deploy it to devices.
_Deploy Write Filter Exclusion List	Deploys the write filter exclusion list to devices running a Windows operating system with HPWF or UWF.
_Enroll Certificate With SCEP	Lets you enroll certificates with SCEP on normal thin clients.

_Hostname and IP	Lets you to change the hostname and IP address of one or more devices. Two options include: 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 Dynamic Properties	Lets you add or remove dynamic properties to collect from devices.
_Manage Snapshot	Manages snapshots on devices.
_Set CA Certificates	Lets you clear or deploy CA certificates to devices.
_Set Domain	Allows devices to join a domain or a workgroup.
_Set OS Configuration	Switches the target device's operating system configuration on devices.
_Set Password	Lets you set a password for one or more users on one or more devices. You can hide or show the password with Hide password .
_Take TPM Ownership	Enables or activates TPM and sets the TPM owner password and BIOS setup password to take the TPM ownership of the selected devices.
_Write Filter Settings	Lets you change the Write Filter settings on devices
_Apply Restart Plan Settings	Lets you change the Restart Plan settings on devices.
_Apply Snapshots Settings	Lets you change the Factory snapshot and the On Boot Snapshot on devices.
_Clone Restart Plan Settings	Lets you copy the Restart Plan settings from one device to generate an Apply Restart Plan Settings result template.
_Clone Snapshots Settings	Lets you copy the Facotry snapshot and the On Boot Snapshot from one device to generate an Apply Snapshots Settings result template.

Table 37. 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.

Imaging Devices

One of the routine tasks often facing administrators is the need to capture and deploy operating system and software images across their fleet of devices. Device Manager supports many types of image capture and deployment across the entire range of HP devices and supported operating systems.

Note

Before capturing images from and deploying images to thin clients, make sure that the repository is configured. See the “Repository management” chapter of the *Administrator Guide* for HP Device Manager for more information.

Imaging support matrix

For information about imaging support for specific thin client platforms, see the Release Notes for your current HPDM version.

Capturing an image

HPDM supports two modes to capture an image without PXE: non-cached mode and cached mode. If the thin client uses an advanced network, such as wireless or 802.1x, use the Cached Imaging mode to capture an image.

The following table shows which formats are supported when capturing images from thin clients.

Operating system	Imaging method	Captured image format
Windows 10 IoT Enterprise LTSC	File-based	.ibr
HP ThinPro 8	Disk-based	.dd.gz
HP ThinPro 8.1	Disk-based	.dd.gz

Capturing an image using the non-cached mode

Note

Capturing images from Windows-based thin clients using the non-cached mode requires a Shared Folder.

You cannot capture images using the non-cached mode when using a wireless connection.

Capturing an image from a Windows 10 IoT Enterprise-based device requires at least 300 MB of free disk space on the thin client.

Capturing an image from the Windows 11 IoT device via HPDM is unsupported since a critical issue. If you want to deploy an image to devices via HPDM, please capture the image via ThinUpdate and then import the captured image into HPDM template via HPDM Console.

1. Go to the Manage Devices page. Drag the **_Capture Image** template from the Templates pane onto the device in the Devices pane whose image you want to capture.

Task Editor

Valid Time, Timeout & WOL Cached Updates Transfers Target Device List

Content Schedule & Batch Control

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

Image

Image Name

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

Description

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:

OK Cancel

2. In the **Task Editor** dialog box, type a name in the **Image Name** field for the captured image, and then enter a description of the captured image in the **Description** field.

Task Editor

Valid Time, Timeout & WOL Cached Updates Transfers Target Device List

Content Schedule & Batch Control

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

Image

Image Name:

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

Description:

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:

OK Cancel

Note

Do not select the option Cache captured image file on thin client before uploading to Master Repository.

3. In the **Save result as template** field, enter a name for the resulting template.

Task Editor

Valid Time, Timeout & WOL Cached Updates Transfers Target Device List

Content Schedule & Batch Control

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

Image

Image Name: ImageTP7.1

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

Description

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template: ImageTP7.1

OK Cancel

4. Select **OK** to immediately apply the task to the device.

After you send the task, you can find there is a notification on the **Tasks & Report** page of HPDM Console. Go to the **Task & Report** page and select **Device Tasks** in the navigator to confirm if the task is processing. The captured image is being compressed. When the task is sent, a new template appears in the **Templates & Rules** page with the name you specified for the resulting template. It appears disabled with a status of transferring. If the task fails to finish, the status changes to failed. If the task finishes successfully, the status changes to enabled.

Templates

All templates (34)

- Private folders
- Favorite (0)
- Shared folders

Type	Template	Description	Base template	Category	Sta...	Modifi...	Modifi...
	_Manage Snapshot	Manage snapshot...	_Manage Snaps...	Settings		2019-0...	
	_Pull Connection ...	Pull Connection Se...	_Pull Connectio...	Connections		2019-0...	
	_Reboot Device	Reboot device.	_Reboot Device	Operations		2019-0...	
	_Reverse Shado...	Remote control d...	_Reverse Shad...	Operations		2019-0...	
	_Set CA Certificat...	Clear or deploy CA...	_Set CA Certific...	Settings		2019-0...	
	_Set Domain	Device domain set...	_Set Domain	Settings		2019-0...	
	_Set OS Configur...	Switch the OS con...	_Set OS Configu...	Settings		2019-0...	
	_Set Password	Set user passwor...	_Set Password	Settings		2019-0...	
	_Shadow Device	Remote control d...	_Shadow Device	Operations		2019-0...	
	_Shutdown Device	Shutdown device.	_Shutdown Dev...	Operations		2019-0...	
	_Template Seque...	The Sequential Te...	_Template Seq...	Template Sequ...		2019-0...	
	_Update Agent	Update the versio...	_Update Agent	Agent		2019-0...	
	_Wake Up Device	Wake device on L...	_Wake Up Device	Operations		2019-0...	
	Deploy License1	This template is u...	_Deploy License	Settings		2019-0...	root
	ImageTP7.1	Deploy an image o...	_Deploy Image	Imaging		2019-0...	root

5. You can now use this template to apply the captured image to other devices by performing a drag-and-drop operation on devices in the device pane or folders in the device tree.

Capturing an image using the cached mode

Note

HPDM does not support Cached Imaging on devices running the HP ThinPro 7.2, HP ThinPro 8, HP ThinPro 8.1.

When capturing an image from a Windows-based device, free disk space must be at least 70% of total file system size. When capturing an image from an HP ThinPro device, free disk space must be at least 50% of total disk size, and the available RAM needs to be at least 1 GB.

1. Go to the **Manage Devices** page. Drag the **_Capture Image** template from Templates pane onto the device in the Device pane whose image you want to capture.

Task Editor

Valid Time, Timeout & WOL Cached Updates Transfers Target Device List

Content Schedule & Batch Control

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

Image

Image Name

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

Description

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:

OK Cancel

2. In the Task Editor dialog box, type a name in the **Image Name** field, and then enter a description for the captured image in the **Description** field.

X

Task Editor

Cached UpdatesTransfersTarget Device List

ContentSchedule & Batch ControlValid Time, Timeout & WOL

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

Image

Image Name

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

Description

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:

OKCancel

Task Editor ✕

Cached Updates Transfers Target Device List

Content Schedule & Batch Control Valid Time, Timeout & WOL

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

Image

Image Name

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

Description

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:



3. Select the option **Cache captured image file on thin client before uploading to Master Repository**. This option is needed if the thin client uses an advanced network, such as wireless or 802.1x.

Task Editor ✕

Cached Updates Transfers Target Device List

Content Schedule & Batch Control Valid Time, Timeout & WOL

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

Image

Image Name:

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

Description:

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:

4. In the **Save result as template** field, enter a name for the resulting template.

Task Editor✕

Cached UpdatesTransfersTarget Device List

ContentSchedule & Batch ControlValid Time, Timeout & WOL

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

Image

Image Name

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

Description

Advanced Options

Cache captured image file on thin client before uploading to Master Repository

Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:

OK Cancel

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

After you send the task, a notification displays on the **Tasks & Reports** page of HPDM Console. Go to the Tasks & Reports page and select **Device Tasks** in the navigator to determine if the task is processing. The captured image is being compressed. When the task is sent, a new template displays in the Templates & Rules page with the name you specified for the resulting template. The task is disabled with a status of transferring. If the task fails to finish, the status changes to **failed**. If the task finishes successfully, the status changes to **enabled**.

Type	Template	Description	Base template	Category	Status	Modified	Modified by
	__Factory Reset	Factory reset.	__Factory Reset	Operations		2019-05-23 14:...	
	__File and Registry	Perform customized file, regis...	__File and Registry	File and Registry		2019-05-23 14:...	
	__Get Asset Information	Get asset information of device.	__Get Asset Information	Operations		2019-05-23 14:...	
	__Get Registry	Get Registry Setting from a d...	__Get Registry	File and Registry		2019-05-23 14:...	
	__Hostname and IP	Change hostname and/or IP a...	__Hostname and IP	Settings		2019-05-23 14:...	
	__Manage Dynamic Properties	Add or remove dynamic prop...	__Manage Dynamic Propert...	Settings		2019-05-23 14:...	
	__Manage Snapshot	Manage snapshots on devices.	__Manage Snapshot	Settings		2019-05-23 14:...	
	__Pull Connection Configuration	Pull Connection Settings from...	__Pull Connection Configura...	Connections		2019-05-23 14:...	
	__Reboot Device	Reboot device.	__Reboot Device	Operations		2019-05-23 14:...	
	__Reverse Shadow Device	Remote control device by Rev...	__Reverse Shadow Device	Operations		2019-05-23 14:...	
	__Set CA Certificates	Clear or deploy CA certificates...	__Set CA Certificates	Settings		2019-05-23 14:...	
	__Set Domain	Device domain settings.	__Set Domain	Settings		2019-05-23 14:...	
	__Set OS Configuration	Switch the OS configuration.	__Set OS Configuration	Settings		2019-05-23 14:...	
	__Set Password	Set user password of device(s).	__Set Password	Settings		2019-05-23 14:...	
	__Shadow Device	Remote control device by VNC.	__Shadow Device	Operations		2019-05-23 14:...	
	__Shutdown Device	Shutdown device.	__Shutdown Device	Operations		2019-05-23 14:...	
	__Template Sequence	The Sequential Template.	__Template Sequence	Template Sequence		2019-05-23 14:...	
	__Update Agent	Update the version of Agent.	__Update Agent	Agent		2019-05-23 14:...	
	__Wake Up Device	Wake device on LAN.	__Wake Up Device	Operations		2019-05-23 14:...	
	ImageWE57P	Deploy an image onto devices...	__Deploy Image	Imaging		2019-05-23 16:...	root

6. You can now use this template to apply the captured image to other devices by performing a drag-and-drop operation on devices in the device pane or folders in the device tree.

Deploying an image

There is no **Deploy Image** or **PXE Deploy Image** base template. However, you can create a Deploy Image or PXE Deploy Image template by capturing and importing an image.

Importing an image file for deployment without PXE

1. Go to the Templates and Rules page of HPDM Console, and then right-click in the **Templates** pane. Select **Import > Imaging Files**, unselect **Deploy using PXE**.

Note

This step is used only to import an image file to generate a Deploy Image template. If you want to generate a PXE Deploy Image template, select **Import > Image Files**, select **Deploy using PXE**. The other steps are the same.

2. In the **Import Image File** dialog box, select **Browse** to select the image file that you want to import.

Import Image File

Generate a template with selected image file to deploy the image onto devices.

Deploy using PXE

File

OS family for devices

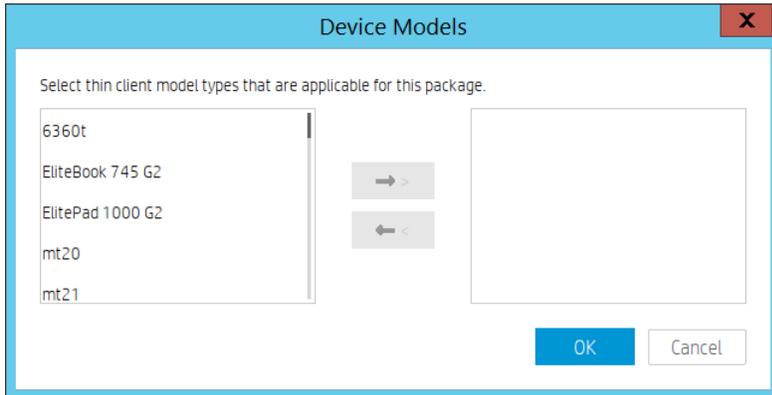
Template name

3. After selecting the desired image file, select **Import**.
4. In the Package Description Editor, enter the necessary information about this image file.
 - a. Enter a title for this package in the **Title** field.

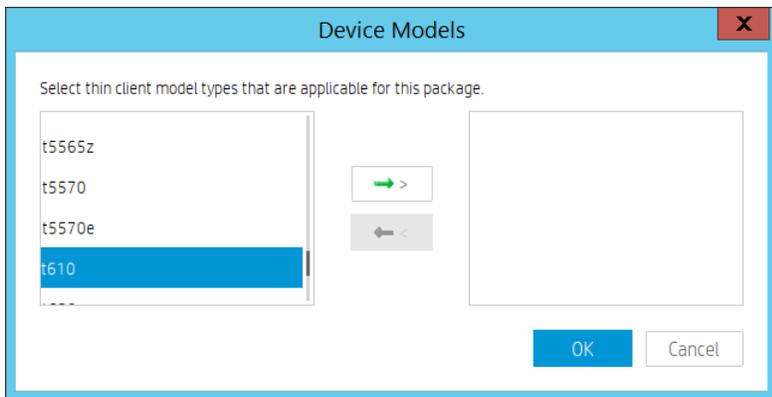
- b. Enter the **Installation Space** in bytes. This is the minimum disk size required to install this image. Usually HPDM can retrieve the space requirement for image files and input it correctly.
- c. Select the **Architecture**. For example: ThinPro 7.2 should be x64.
- d. Select the **OS type of the image**. This is the image file's operating system. You can select the operating system from the supported operating system list.

e. Select the **Thin Client Models** that the image supports. You can select the thin client models using the following steps:

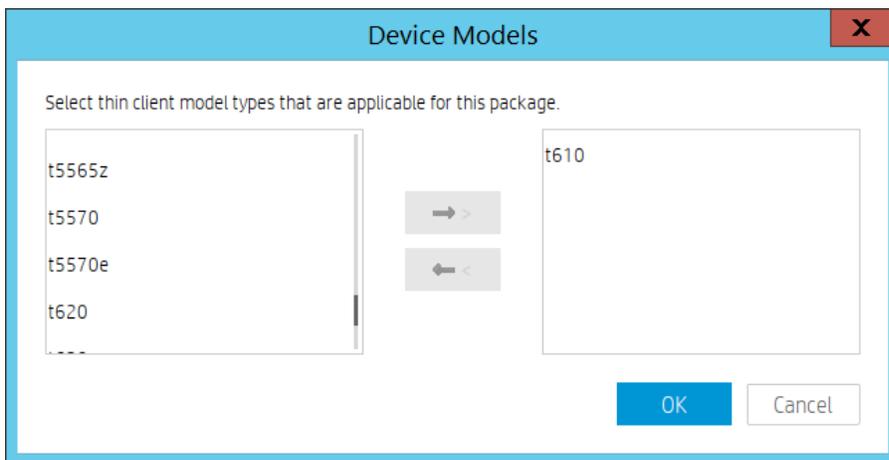
i. Select the **Thin Client Models** field.



ii. Select the thin client model from the left pane, such as t610, and then select ->.



iii. Select **OK** to return to the Package Description Editor.



Package Description Editor - Images

Type: image

Title: ThinPro7.1 image_1

Installation Space (bytes): 2,048,385,024

For images, Installation Space refers to the minimum disk space require to hold the image. For other packages, Installation Space refers to the minimum free space required to install the package.

Architecture: x64

OS type of the image: HP ThinPro 7

Device Models: (Click here to select Device Models)

Description:

Generate Cancel

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

Transfer In Progress

Transferring data:80805888 bytes of 1026199972 bytes transfe...

7%

6. After the upload is complete, a confirmation message displays. Select **OK** to finish this operation.

Import Image File

Successfully generated template "ThinPro7.1 image_1" with file "ImageTP7.1.dd.gz".

OK

If the image file imported successfully, a new Deploy Image template is displayed in the Templates pane.

	_Update Agent	Update the versio...	_Update Agent	Agent	2019-0...
	_Wake Up Device	Wake device on L...	_Wake Up Device	Operations	2019-0...
	_Write Filter Sett...	Configure Write Fil...	_Write Filter Se...	Settings	2019-0...
	File and Registry	Perform customiz...	_File and Regist...	File and Registry	2019-0... root
	ThinPro7.1 imag...	Deploy an image o...	_Deploy Image	Imaging	2019-0... root

Deploying an image without PXE

HPDM supports two modes to deploy an image: noncached mode and cached updates mode. If the thin client uses an advanced network, such as wireless or 802.1x, use the cached updates mode to capture an image. For more information about cached updates, see the **Cached Task** section.

The following table shows which formats are supported when deploying images to thin clients.

Table 38. Supported formats

Operating system	Image format (non-cached mode)	Image format (cached updates mode)
Windows 10 IoT Enterprise LTSC	.ibr	.ibr
HP ThinPro 8.1	.dd.gz	.dd.gz
HP ThinPro 8	.dd.gz	.dd.gz
HP ThinPro 7.2	.dd.gz	.dd.gz

Deploying an image using the non-cached mode

Note the following requirements for deploying an image using noncached mode:

- A shared folder is required to deploy an .ibr image to a Windows-based thin client
- Deployment cannot be performed via a wireless connection.
- When deploying an .ibr image to a Windows 10 IoT Enterprise device, there must be at least 300 MB of free disk space on the thin client.

To deploy an image using the non-cached mode:

1. In HPDM Console, go to the Manage Devices page.
2. Select the Deploy Image template you created by capturing or importing an image from the **Templates** pane.
3. Drag and drop the template onto the devices where you want to deploy the image. The Task Editor displays detailed information about the image.

Task Editor

Cached Updates Transfers Target Device List

Content Schedule & Batch Control Valid Time, Timeout & WOL

Image Name: ImageTP7.1.dd.gz

OS Type: HP ThinPro 7;

Description:

Details

Title	ThinPro7.1 image_1
Create Time	2019/04/10 14:50:09
Installation Space (bytes)	2048385024
Architecture	x64
OS Type	HP ThinPro 7
Model Type	t610

Advanced Options

Allow Cross-Platform Imaging

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

Retain HP ThinPro Configuration

OK Cancel

4. To deploy the image to a device with a different hardware platform than the source device, select **Allow Cross-Platform Imaging**.

Note

For example, select this option if you captured an image from an HP t740 and want to deploy it to an HP t755. Otherwise, this Deploy Image task will fail. If you select this option, be sure that the captured image works on the target device.

5. **Retain HP ThinPro Configuration** is a special option only for ThinPro imaging. Agent restores the ThinPro profile after image deployment. Note that some options are not restored perfectly due to profile compatibility.

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

Deploying an image using the cached updates mode

Note the following requirements for deploying an image using cached updates mode:

- When deploying an image to a Windows-based device, the free disk space must be greater than the image file size.

- When deploying an image to an HP ThinPro device, the free disk space must be greater than the image file size, and the total RAM must be greater than the image file size + the imaging operating system.
-

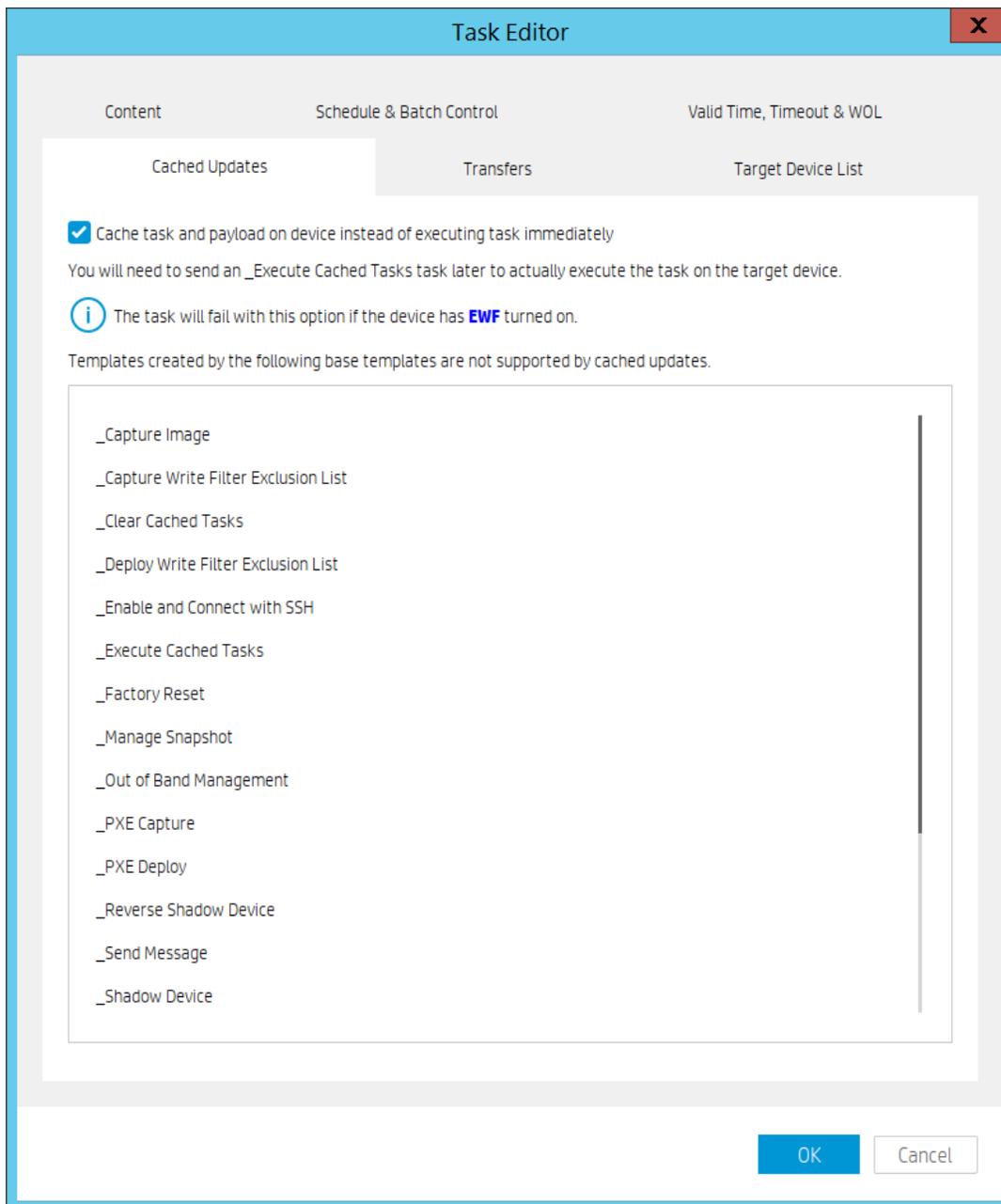
Note

4 GB is the recommended memory size for ThinPro series cached image deployment.

- To deploy an image to a device that uses a wireless network, be sure that the image file contains wireless network credentials and can connect to the wireless network after the image is deployed.

To deploy an image using the cached updates mode:

1. In HPDM Console, go to the Manage Devices page.
2. Select the Deploy Image template you created by capturing or importing an image from the **Templates** pane.
3. Drag and drop the template onto the devices where you want to deploy the image. The **Task Editor** dialog box displays detailed information about the image.
4. On the **Cached Updates** tab, select **Cache task and payload on device instead of executing task immediately**. This option is needed if the thin client uses an advanced network, such as wireless or 802.1x, or if you want to deploy an image with cached updates.



5. To deploy the image to a device with a different hardware platform than the source device, select **Allow Cross-Platform Imaging**.

Note

For example, if you captured an image from an HP t740 and want to deploy it to an HP t755, you need to select this option. Otherwise, this Deploy Image task will fail. If you select this option, you need to ensure that the captured image will work well on the target device.

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

7. Send the **_Execute Cached Tasks** task to the device to execute this cached imaging task.

Deploying an image with PXE

You can generate a PXE Deploy template by importing an image from the Template and Rule page, and then right-clicking in the Templates pane to select **Import > Image Files**, select **Deploy using PXE**.

The other importing steps are same with importing for Importing an image file for deployment without PXE.

The steps of sending the imported PXE image template are also same.

1. In HPDM Console, go to the **Manage Devices** page.
2. Select the imported PXE Image template you created by importing.
3. Drag and drop the template onto the devices to which you want to deploy the image. The **Task Editor** dialog box appears and displays detailed information about the image.
4. Select **OK** to apply the PXE Image task to the devices.

Note

HPDM Agent does not change the boot order before PXE imaging. Be sure to manually set legacy PXE boot as the default one to improve the success rate.

This operation does not preserve any settings on the target device, which is usually used to deploy an image to a crashed device. A PXE Deploy task fails when using a wireless connection.

Preserved settings during imaging

- Source device—The device from which the image is captured.
- Target device—The device to which the captured image is deployed.

Settings preserved when capturing an image

Windows 10 IoT Enterprise LTSC:

All settings from the source device are preserved on both the source device and the captured image, except the host name, network settings, domain settings, and Write Filter status.

HP ThinPro:

All settings from the source device are preserved on both the source device and the captured image, except the host name and network settings.

Settings preserved when deploying an image

When deploying an image, the following settings on the target device are preserved and restored after image deployment.

Windows 10 IoT Enterprise LTSC:

- Write Filter status
- Hostname
- Network
- Terminal Service License
- Windows Activation License (select operating systems only)

HP ThinPro:

- Hostname
- Network

Retain HP ThinPro Configuration

This is a special option only for ThinPro imaging. Agent restores the ThinPro profile after image deployment.

Note

Some options might not restore perfectly due to ThinPro profile compatibility.

Imaging task performance

This section introduces the time spent on imaging tasks. HP gathered this data from the HP test environment for reference only. The time spent on imaging tasks depends on the network environment, protocol, and hardware. The HP data was retrieved using the following environment:

- Network bandwidth: 100 MB bandwidth
- File Transfer Protocol: FTP and Shared Folder

Table 39. HP Win10 IOT imaging task performance

Operating system	Connection type	Mode	Device model	Disk size (GB)	Image clone duration (minutes)	Deploy Image duration for image cloned via HPDM (minutes)	Deploy Image duration for image downloaded from HP.com (minutes)
Win10Iot	Wireless	Cached	t430				
			t530	256	56	31+22	
			t630				
			t730				
	Wired	Cached	t430	32	34	7+29	
			t530	128	46	23+28	
			t630	512+64	35	9+17	
			t730	64	28	7+20	
		Non-cached	t430	32	34	29	
			t530	128	30	28	
			t630	512+64	24	26	
			t730(fiber)	128	44	27	

Table 40. HP ThinPro imaging task performance

Operating system	Connection type	Mode	Device model	Disk size (GB)	File system size (GB)	Image clone-zero duration (minutes)	Image clone-clone duration (minutes)	Image deploy-deploy duration (minutes)	Image deploy-resize duration (minutes)
HP ThinPro	Wired	Non-cached	t610	4	1	0.33	3	4	1
				4	4	2	4	15	0.03
				16	1	0.13	2.5	2.5	13.5
				16	16	28.5	8.5	13	0.03

Known issues

- When deploying an image using PXE, if a device is shut down and not set to **Network boot first**, the device receives the reboot task circularly.
Workaround:
1. Go into the BIOS and enable **Network boot first**.
2. Cancel the task from HPDM Console.
- In Windows, if the source thin client was joined to a domain prior to a Capture Image task, the domain membership is lost after cloning the image. HP recommends removing the source device from any domain before a Capture Image task.
- The group policy that controls the domain password complexity affects local user accounts, resulting in a requirement to change the password to meet stricter criteria.
- HPDM does not support deploying an image file downloaded from HP.com to a thin client that uses a wireless network.
Workaround:
1. Deploy this image to a device using a local image tool, such as HP ThinUpdate.
– or –
Configure the device to use a wired network, and then deploy the image to this device via HPDM.
1. Configure the wireless network settings after deploying the image.
2. Capture the image from this device via HPDM.

3. Deploy the newly captured image to other devices that use a wireless network.

Reporting tools

Adding a report

To add a report:

1. In HPDM Console, go to **Tasks & Reports**, then navigate to **Reports**.
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 criterion 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. You can use either option 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, and then, select **Next**.
 6. Select **Finish**. A prompt asks if you want to preview the report.

Editing a report

To edit an existing report:

1. Navigate to **Reports**.
2. From the **Report List**, select a report and then select **Edit**.
3. To edit the report filter, use the options under **Set Filter**. To edit report columns, use the options under **Choose Columns**. To see a summary, select **Summary**.
4. After editing, select **Finish**. A prompt asks if you want to preview the report.

Deleting a report

To delete a report:

1. Navigate to **Reports**.
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:

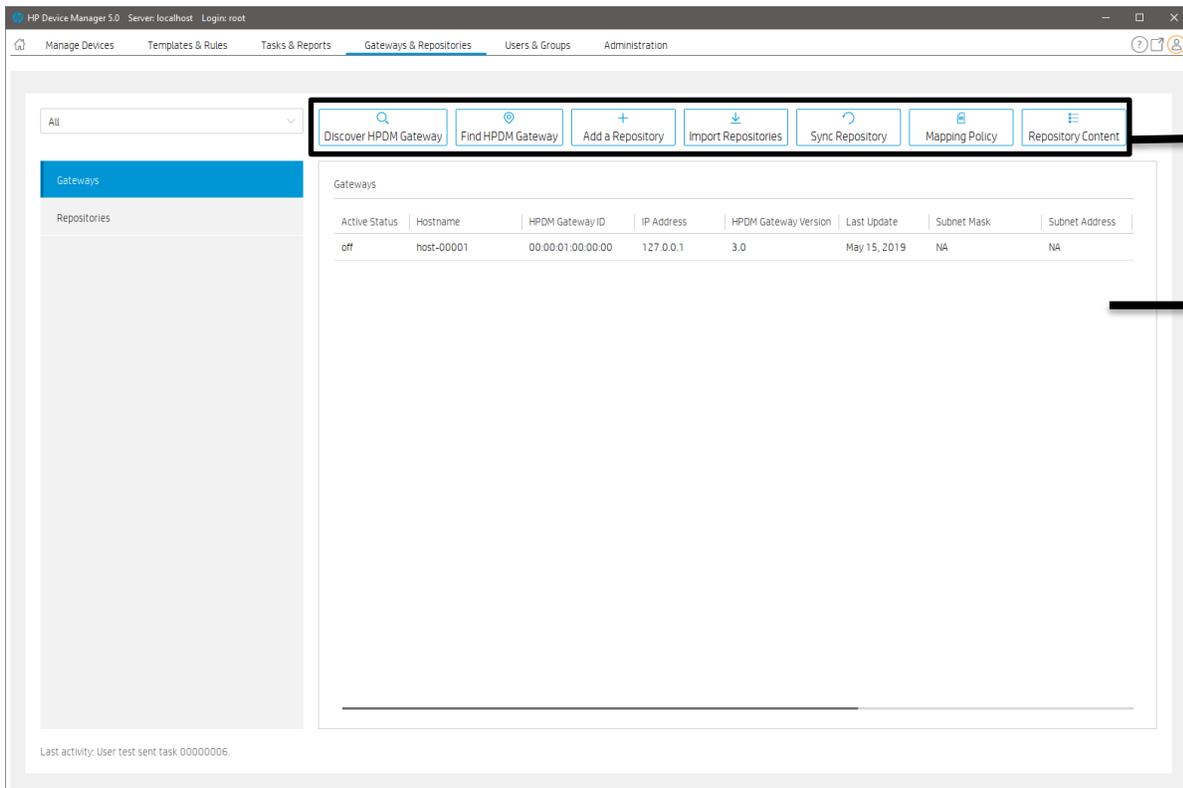
1. Navigate to **Reports**.
2. Select a report from the list, and then select **Generate Report Preview**.
3. In the resulting window, select either **Export selected** or **Export all**.

NOTE:

Reports can be also exported from web console. Upon clicking the export button, the report will be automatically downloaded.

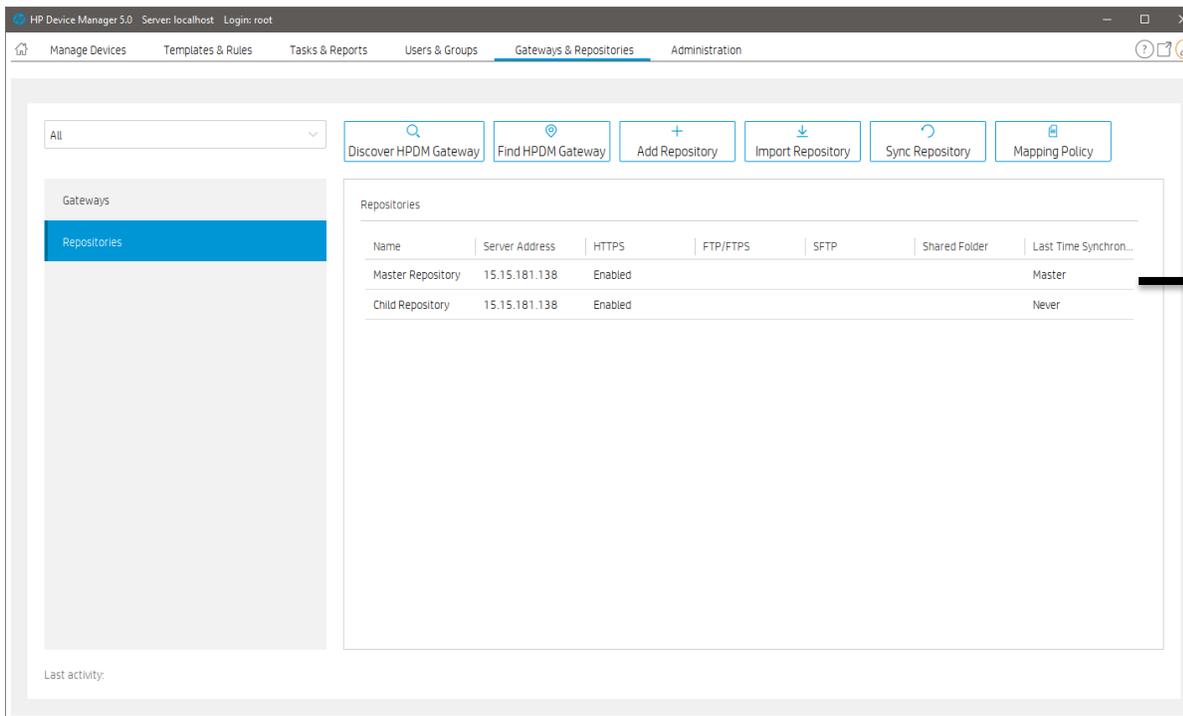
Gateways and repositories

Page layout



1

2



3

1. Toolbar— An enumeration of the Gateways & Repositories most commonly operations.



- Discover HPDM Gateway—Discover gateway by IP range.
 - Find HPDM Gateway—Find gateway by condition.
 - Add Repository—Create a new repository.
 - Import Repository—Import repository from a file.
 - Sync Repository—When a task that requires repository content starts, the content is automatically synced from the HPDM Master Repository to each appropriate HPDM Child Repository.
 - Mapping Policy—Mapping devices to repositories according to each device’s HPDM Gateway or subnet address.
2. Gateway View—All gateways information.
 3. Repository View—All repositories information.

Managing Repositories

Automated Repository Management improves the efficiency of HPDM and ensures the consistency of resources in all repositories through automated synchronization. Automated Repository Management makes it easier to associate a payload with templates, manage multiple Child Repositories, synchronize content between repositories, and remove content from repositories.

A repository is a file server that stores payloads used in HPDM tasks, like software components, system images, tools, and agent files. There can be multiple repositories in an HPDM setup. One repository contains the master copy of the payloads and is called the Master Repository. The other repositories replicate the contents of the Master Repository and are called Child Repositories.

The following tasks need to transfer payloads through repositories:

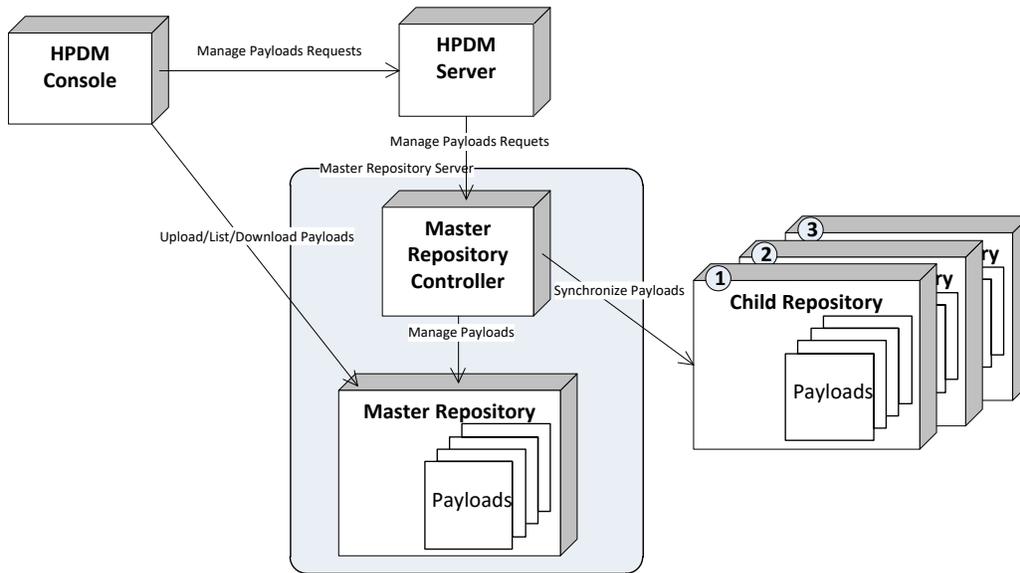
- Agent
 - _Update Agent
- File and Registry
 - _File and Registry > Capture Files, Deploy Files
- Settings
 - _Apply Easy Tools Configurations
 - _Apply Easy Tools Settings
- Imaging
 - _Capture Image
 - _Deploy Image
 - _PXE Deploy

Mechanics

On the Master Repository, a component named the Master Repository Controller manages the content in the Master Repository and synchronizes that content to the Child Repositories as requested by the HPDM Server. The HPDM Server works with the Master Repository Controller to prepare the payload for tasks

The overall structure of the Automated Repository Management feature is shown in the following diagram.

Figure 9. Overall structure



To use this feature, users must set up the file servers and configure them as either the Master Repository or a Child Repository before introducing the payload to the system and using it.

Protocols

HPDM supports the following kinds of protocol: HTTPS, FTP/FTPS, SFTP and SMB (Shared Folder, Samba). You can use a single protocol or multiple protocols in one repository. See the following limitations:

- FTP family protocols must be chosen for Linux noncached imaging.
- SMB must be chosen for Windows non-cached file-based imaging.

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

Modifying Repository settings within HPDM Console

1. Open HPDM Console to add the FTP setting into Master Repository.
 - a. Go to the Gateways & Repositories page of HPDM Console.
 - b. Select the repositories in the **Navigator** pane.
 - c. Select the Repository you want to modify.
 - d. Follow the Repository Configuration Wizard to modify settings:
 - i. In the Basic Information page, you can change the **Repository Name** and the **Server address**.
 - ii. In the Protocol Settings page, you can add or remove file transfer protocols.
 - iii. Change the settings for each selected protocol.
 - iv. In the last Summary page, select the **Test Repository** button. The test report is output in the **Test Result** pane.
 - v. If the test is successful, you can select **Finish** to save the changes. If the test is not successful, modify the settings and test again.

Configuring the Master Repository

Installing HPDM Master Repository with the HPDM 5.0 installer requires HPDM Master Repository Controller and HPDMHTTPSRepository.

HPDM Master Repository Controller

The HPDM Master Repository Controller installer installs the Master Repository at %ProgramData%\HP\HP Device Manager\HPDM.

If you want to move the Master Repository path, install HPDM Configuration Center. After you move the Master Repository path, be sure to modify the root path of the file servers to point to the new Master Repository Path.

For more details, see **HPDM Configuration Center**.

HPDM Embedded HTTPS Server

HPDM 5.0 supports only HPDM Embedded HTTPS Server. When installing, it generates a random user and password. The default root path is also %ProgramData%\HP\HP Device Manager\HPDM.

For a typical installation: If you install the Master Repository and HPDM Server in the same computer with the HPDM 5.0 installer, the full installer intelligently sends the HTTPS Server to HPDM Server. The Repository setting is automatically configured.

If you want to change the random user and password, install HPDM Configuration Center. After you change the user or the password, be sure to modify the **Repository** setting in HPDM Console.

For more information, see **HPDM HTTPS Repository Deployment**.

Add other protocols

Configuring FTP

1. Install an FTP server.
2. Point to the root path to the Master Repository folder.
3. Follow the steps in **How to modify Repository settings in HPDM Console** to add the FTP setting. Be sure to notice the URL setting of FTP/FTPS, such as if you install the Master Repository in the default path:

If you set %ProgramData%\HP\HP Device Manager\HPDM as the FTP root path, you can keep the URL blank after ftp://<ip address>.

If you set %ProgramData%\HP\HP Device Manager as the FTP root path, set HPDM in the URL setting.

Configuring SMBv2

1. Configure the HPDM directory you created as an SMB shared folder with full control permissions.
2. Follow the steps in **Modifying Repository settings** within **HPDM Console** to add the shared folder setting.

Configuring SFTP

1. Install and configure a proper SFTP server.
2. Follow the steps in **Modifying Repository settings** within **HPDM Console** to add the SFTP setting.

Child Repository configuration

The only difference between a Child Repository and the Master Repository is the Master Repository Controller does not need to be installed with a Child Repository.

Configuring an HPDM Child Repository

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the Repositories view, select **Add Repository**.
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 configured connections and display the results.
7. Select **Finish**.

Deleting an HPDM Child Repository

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the Repositories view, select an **HPDM Child Repository**.
3. Select **Remove**, and then select **Yes** to confirm.

Exporting repositories

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the **Repositories** view, right-click on a repository, and then select **Export**.
3. Browse to the location where you want to save the repositories.
4. Select **Export**. All repositories are exported to an XML file.

Importing repositories

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the **Repositories** view, select **Import Repository**.

3. Browse to the location where the repositories you want to import are located.
4. Select **Import**.

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, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. Select **Mapping Policy**.

Batch mapping

You can map devices to repositories according to each device's HPDM Gateway or subnet address. To change the mapping, right-click and 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.

Synchronizing repositories

On-Demand Synchronization

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.

Manual Synchronization

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

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the Repositories view, select **Sync Repository**.
3. In the Synchronization dialog box, select **Sync**.
4. Select **Yes**.

Scheduled Synchronization

To schedule synchronizations to automatically occur at times you specify:

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the Repositories view, select **Sync Repository**.
3. In the Synchronization dialog box, select **Enable schedule synchronization**.
4. Configure the schedule settings.
5. Select **Save**.

Content management

To view the contents of the HPDM Master Repository:

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.

2. In the Repositories, right-click a repository, and then 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 select an item in the right panel. A dialog box displays 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 **Delete**. Select **Yes** to confirm.

NOTE:

You cannot delete built-in content provided by HP

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

Customized Packages

HPDM package

An HPDM package contains two required parts: payload files and a description file. For example, there might be a package called Test, in which there are the following folder and file. The folder contains the payload files.

- Folder: Test
- File: Test-2EFFEB25C7779780C5165292BEE322521A4EBCC08EE19B0FBC6C0274A0B79491.desc

The description file is named by combining the payload name and the SHA256 hash value for the payload, separated by "-". The content of the description file includes detailed information about the package, such as payload size, operating system type, and device models that the package can be applied to. The information comes from either the Package Description Editor user interface input or other sources such as imported HP FTP components.

To Capture Image task:

1. Send a Capture Image task to a device. For details about the Capture Image task, see **Imaging Devices/Capturing an image**.
2. After the Capture Image task completes, an image template is generated and the package uploads to the Master Repository automatically.

Importing a file to generate a package

Importing a local file or folder

1. Go to the Templates & Rules page of HPDM Console.
2. In the Templates pane, select the **_File and Registry** template.
3. Select **Add** in the Template Editor.
4. Choose **Deploy Files** in the Sub-Task Chooser, and then select **OK**.
5. Select **Add from local** to add a file or a folder. Modify **Path On Device** to set the path to deployed on devices, and then select **OK**.
6. Select **Save as**, enter a name for the new template, and then select **OK**.
7. Enter the payload information in the **Package Description Editor** dialog.
8. Select **Generate**. The file is added as a new template. Payload files are automatically uploaded to the Master Repository

Importing an imaging file

1. Go to the Templates & Rules page of HPDM Console.
2. Right-click on the Templates pane, and then select **Import > Image Files**
3. Select the image file that you want to import.
4. Select **Import**, and then enter the payload information in the **Package Description Editor** dialog.
5. Select **Generate**. The imaging file is added as a new template. Payload files are uploaded to the Master Repository automatically.

For more details about Imaging, see **Imaging**.

Importing an update from an HP Update Center

1. Go to the Templates & Rules page of HPDM Console.
 2. Right-click on the Templates pane, and then select **Import > HP Update Center**.
- For more details, see **HP Update Center**.

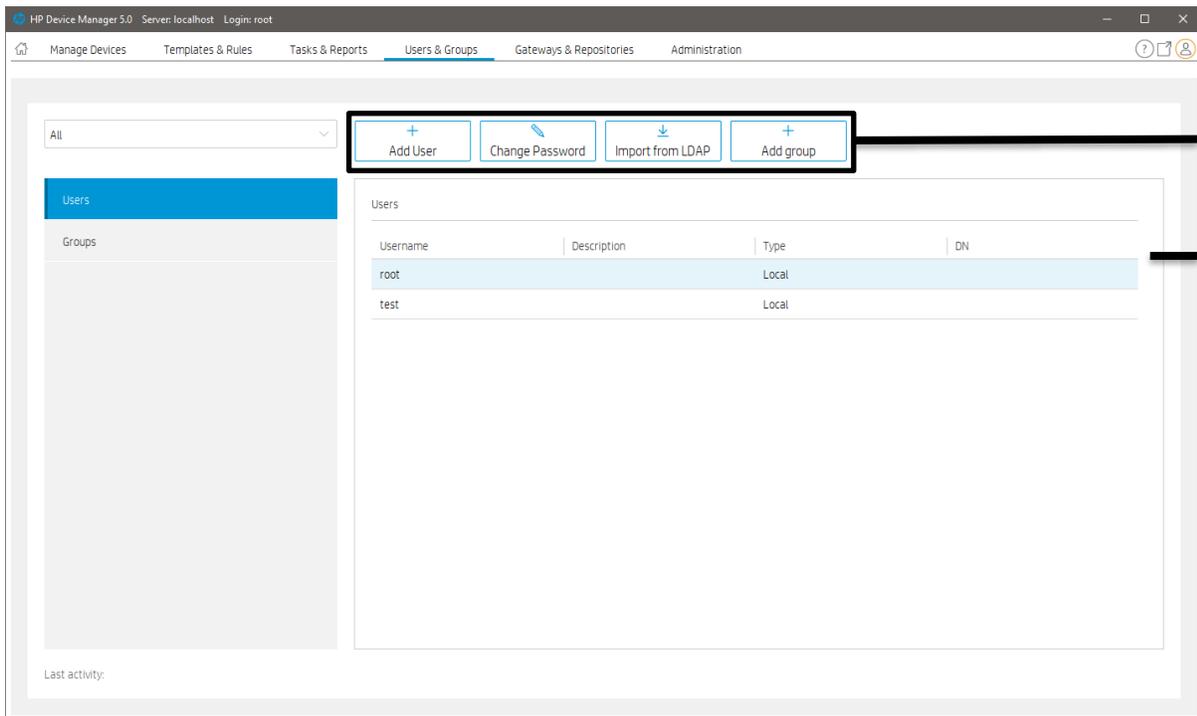
Users and Groups

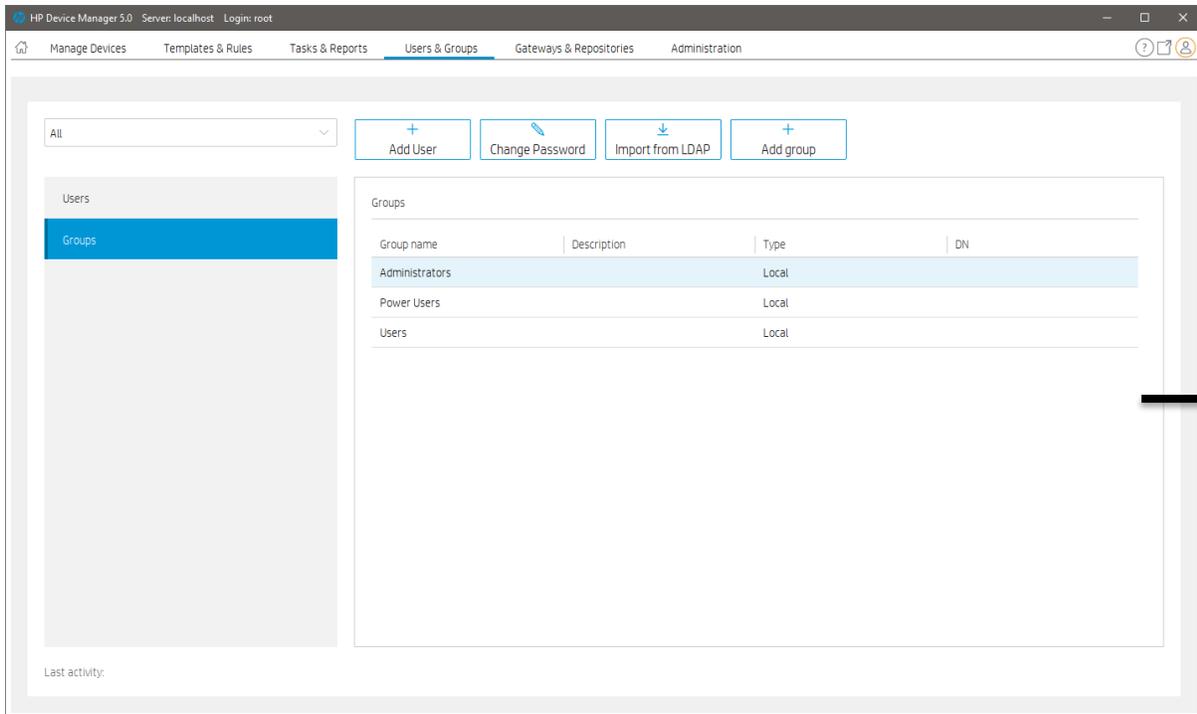
The controls within Users and Groups in HP Device Manager allow you to dictate fine-grained responsibilities within your organization.

In HPDM Console, select the **Users & Groups** page to see all users and groups.

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.

Page Layout





1. Toolbar— An enumeration of the Users and Groups most common operations.



- Add User—Create a new user
- Change Password—Change current user’s password
- Import from LDAP—Import users from LDAP server
- Add group—Create a new group

2. User View—All user information.

3. Group View—All group information.

Users

Add users

1. Select **Add User** in the toolbar.
2. Enter a Username for the new user, **New Password** and then re-enter it in the **Confirm Password**. Select **OK** to create the new user.
3. You can use this user name to log in to HPDM Console the next time it starts.

NOTE:

The password should be between 12 and 36 characters in length and must include uppercase letters, lowercase letters, numbers, and special characters.

The user must be added to a group before it has any privileges to use HPDM.

This user will be added to the Power Users group by default.

Multiple instances of HPDM Console cannot log on to HPDM Server with the same user name at the same time.

Deleting users

1. Right-click a user from the list in the **Users** table.

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

Assigning users to groups

1. Select a user from the list in the **Users** table.
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. Right-click a user from the list in the **Users** table.
2. Select **Change Password**.
3. Enter the **New Password** for the user, and then reenter it in the **Confirm Password** field.
5. Select **OK** to finish.

NOTE:

The password should be between 12 and 36 characters in length and must include uppercase letters, lowercase letters, numbers, and special characters.

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

Change Password in Toolbar can only change your user password.

Viewing privileges and template access

1. Select a user from the list in the **Users** table.
2. Select the **View general privileges** tab. You can see **Action based privilege**.
3. Select the **View template privileges** tab. You can see **Object based privilege**.

NOTE:

Action based privilege, or role-based privilege, assigns privileges to a group, and then users within the group inherit those privileges.

Object based privilege controls each user group's access to the view, modify, and execute operations for each template.

Groups

Adding a group

Groups can be used to control user privileges in HPDM.

1. Select **Groups** in Navigation View.
2. Right-click in the **Groups** table. Select **Add Group**. You can assign this group a set of privileges, and then you can assign users to this group.

NOTE:

The newly added group has the same privileges as the Power Users group.

Assigning privileges to groups

1. Right-click on a group from the list in the **Groups** table.
2. Select **Properties**.
3. Select the **Privileges** tab.
4. Select the privileges you wish to assign to the group.
5. Select **OK**.

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. Right-click on a group from the list in the **Groups** table.

2. Select **Properties**.
3. Select the **Users** tab.
4. Use the **Add** and **Delete** buttons to modify the members of this group.
5. Select **OK**.

Assigning security filters to groups

1. Select a group from the list in the **Groups** table.
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.

Policy

Allow the user who has User Management privilege to limit the maximum number of devices when group users sending a task. Take the maximum limit if a user belongs to multiple groups, send task failed when this limitation is exceeded.

1. Go to the User & Group page, and then **Groups** navigation view.
2. Select a group, and then open group properties.
3. Select the **Policy** category.
4. Select the check box and enter a number in the text area.
5. Select **OK**

Viewing privileges and template access

1. In the HPDM Console, open the Users & Groups page, and then select **Groups** in Navigation View.
2. On the **Groups** table, select a group.
3. Select the Privileges page to view **System-level privileges**.
4. In the privileges tree, select **Template Access Management**.
5. Open the Templates & Rules page, and then select **Template Privilege** in Toolbar to view template access privileges.

Deleting groups

1. Select a group from the list in the **Groups** table.
2. Select **Delete Group**, and then select **Yes**.

Directory Services

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.

The LDAP server configuration information, including User Authentication, needs to be set in HPDM (see **LDAP settings**). HPDM will use the configuration information to connect to the specified LDAP server. The LDAP users and groups need to be imported into HPDM (see **Importing users and groups**).

The LDAP server configuration and basic imported user and group information is stored in the database of HPDM. HPDM does not store the LDAP user's password. (It is only transported to the LDAP server when the user logs in to HPDM.)

After the import is completed, you can log in to HPDM as an LDAP user or group.

- HPDM supports logging in using a full domain account name such as "domain\account".
- HPDM supports multiple trusted domains.
- HPDM supports a universal group.
- HPDM supports subgroups.

For HPDM internal users, HPDM authenticates by itself. When you use an LDAP account to log in to HPDM, the LDAP server is responsible for authentication and returns the result to HPDM.

LDAP settings

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

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

2. Select **Add** to create a new LDAP setting.
3. Enter the name of the LDAP setting, and select **OK**.
4. In the **Host** field, type the LDAP server hostname or IP address. If an encrypted connection is used, make sure the server certificate has IP address in its Subject Alternative Name. Otherwise, the LDAP server must be specified by the host name.
5. 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.
6. Select an **Encryption** type.

7. 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.

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

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

Generic LDAP:

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

Examples of Base DN's:

`dc=testnet,dc=com`

`o=company,c=US`

- Specify the **RDN Attribute**. The RDN (Relative Distinguished Name) attribute is the LDAP attribute that specifies the login name of the user. Common values for this include `sAMAccountName` (Active Directory), `UID`, and `CN`.

9. 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 select 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`

10. 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

Once the LDAP server is configured, Users and Groups must be imported. The 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:

Select one LDAP setting 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 multiple results, for which **Show 20 more** is displayed. Select 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 performed recursively from this origin.
3. The **Query** allows the specification of what to search for. It contains 3 parts: Attribute, Search Value, and Comparison between the two.
 - a. The **Attribute**, on the left side of the query, offers several common attributes to search on. If the needed 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 searched for. You can use an asterisk (*) as part of Search Value. This allows searching when the full **Search Value** is unknown. For example: Searching Attribute UID with an Equals comparison for value = *.smith@testnet.com matches all users with a UID that ends 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 (<=) finds LDAP objects with an attribute value that is numerically smaller than the search value.
 - The **Similar to** comparison (~=) searches for attribute values that are similar to the search value.
 - The **Not Equals** comparison (!=) searches for attribute values that are not equivalent to the search value.
4. Select **Search**. 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:
 - Select the user or group.
 - or –
 - Select the user or group, and then select **Add**.
3. The user or group is now 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**).

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 **Remove**.

To examine a user or group:

1. Select a user or group.
2. Select **Show Attributes**.
3. Select **Add** to add this object to the import list.

Multiple trusted domains login

If you have parent domain and multiple trusted child domains, you can log in to HPDM with different child domain accounts by configuring a single parent domain to use for user authentication.

Environment:

Parent domain

- Domain: hpdm.com
- Host: 192.168.231.150
- User Authentication Account: CN=Administrator,CN=Users,DC=hpdm,DC=com

Child domain

- Domain: test.hpdm.com
- Host: 192.168.231.152
- User Authentication Account: CN=Administrator,CN=Users,DC=test,DC=hpdm,DC=com
- Imported user: CN=tester,CN=Users,DC=test,DC=hpdm,DC=com

HPDM Server

- Host: 192.168.231.138

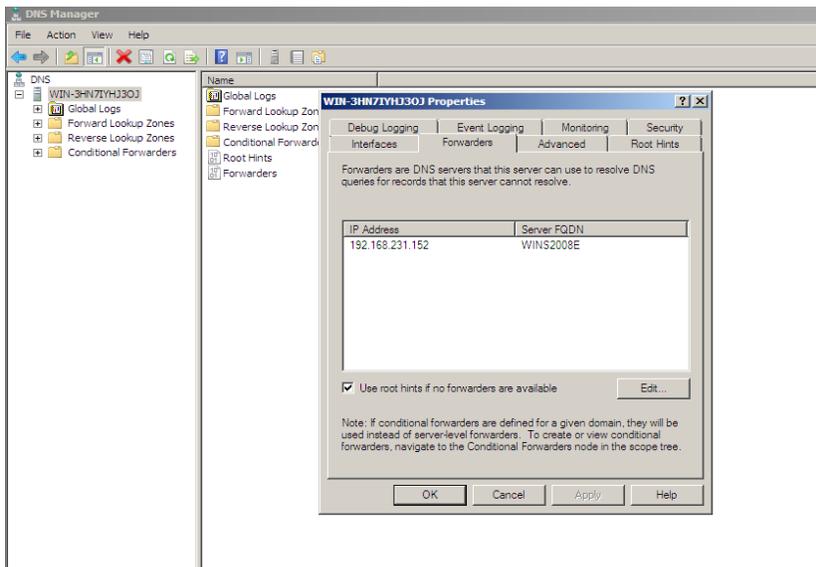
DNS Server

You must set up a DNS Server strategy so that the HPDM Server can communicate with both the parent and child domain servers using the domain name.

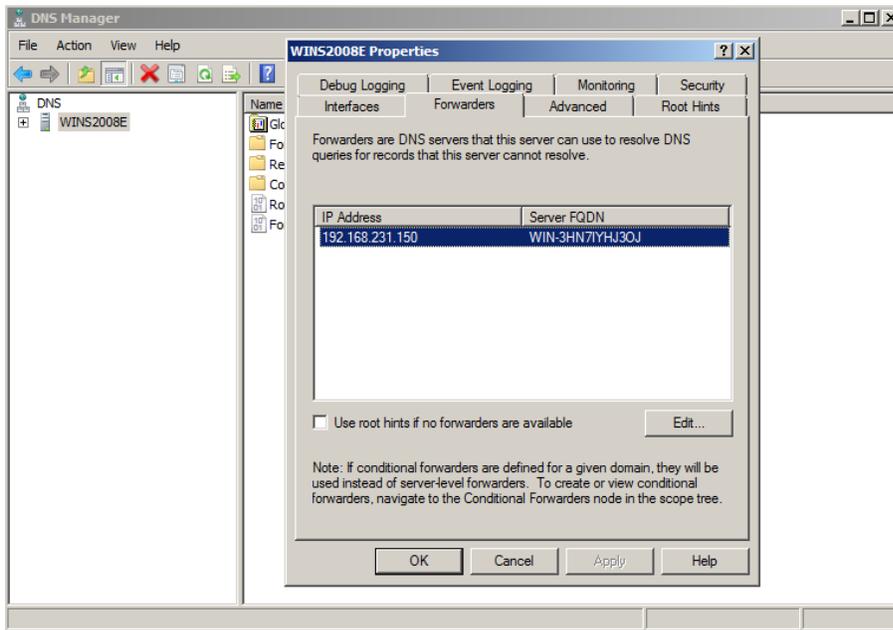
1. If the parent domain and child domain use the same DNS Server, the DNS of the HPDM Server needs to point to this DNS Server.
2. If the parent domain and child domain use different DNS Servers, be sure the **Forwarders** of both the parent domain and child domain DNS Server point to each other. Then make the DNS of HPDM Server point to the DNS Server of the parent domain.

To make the forwarders of the parent domain and child domain point to each other:

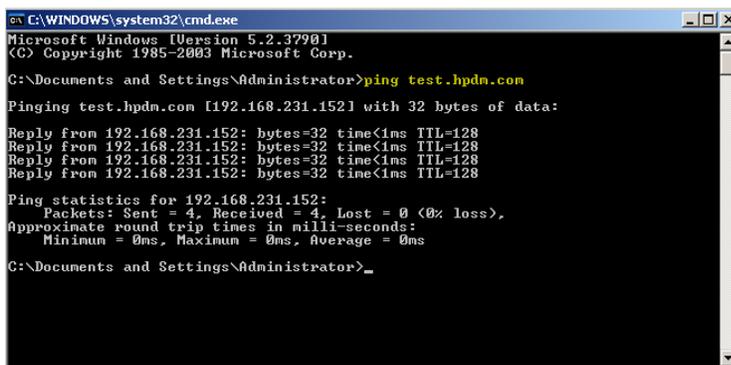
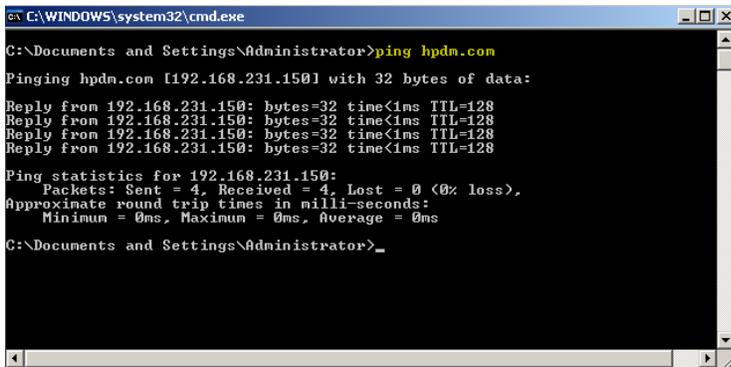
- a. In the DNS Server of the parent domain, select the **Forwarders** tab and then select **Edit**. Enter the IP address of the DNS Server of the child domain.



- b. In the DNS Server of the child domain, select the **Forwarders** tab and then select **Edit**. Enter the IP address of the DNS Server of the parent domain.



To verify that the DNS Server strategy is correctly configured, enter either `ping hpdm.com` or `ping test.hpdm.com` on the command line.

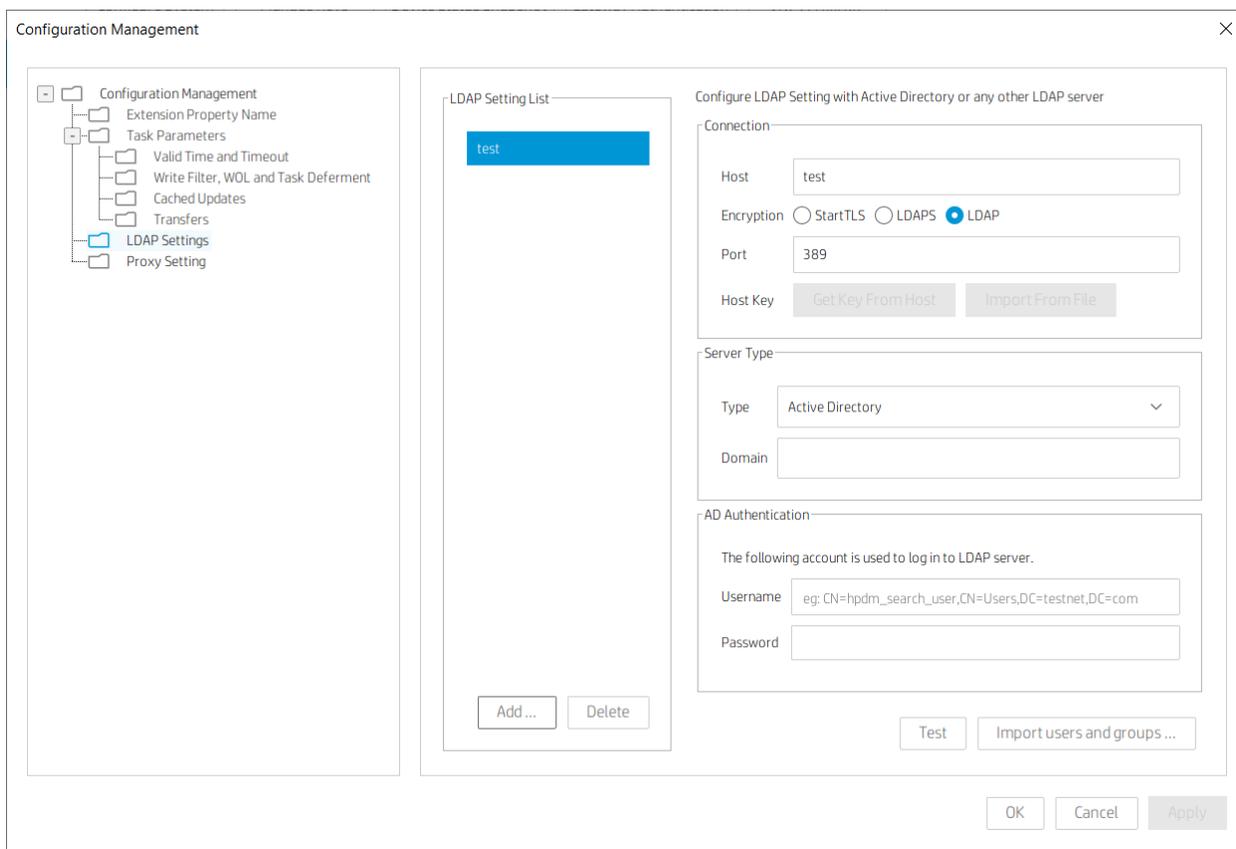


Multiple trusted domains support

User authentication with hpdm.com

To log in to HPDM with a child domain account using parent user authentication:

1. From the HPDM Console, go to **Administration > Configure Systems > LDAP Settings**.
2. Use the user account for hpdm.com.



Note

If you use **SSL** encryption in LDAP authentication, be sure to get a key from the parent domain and any other trusted domains (that you want to use to log in to HPDM).

To get a key:

In the **Host** field, enter the IP or hostname of the domain.

Select **Get Key From Host**.

Repeat steps A and B for each trusted domain that you want to use.

If you select **None** under encryption, do nothing.

Support HPDM login of test.hpdm.com

1. In the HPDM Console, select **Tools > User Management > Import from LDAP**.
2. On the **Search** tab, enter DC=test,DC=hpdm,DC=com in the **Base DN** field.
3. In the **Query** field, select **cn, =, and t1**.
4. Select **Search** to find this user in the domain **DC=test,DC=hpdm,DC=com**.

NOTE:

You can refine the UI by setting CN as the selected item.

5. Select **Add** to import this user account into HPDM.
6. Log in to HPDM using this **test\t1** account.

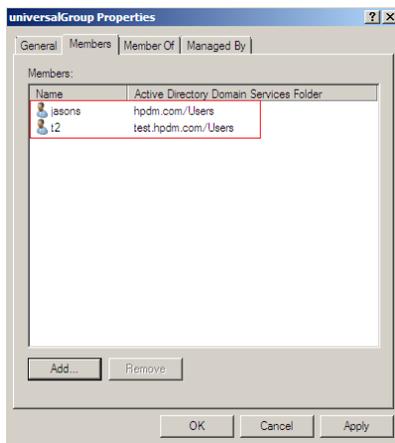
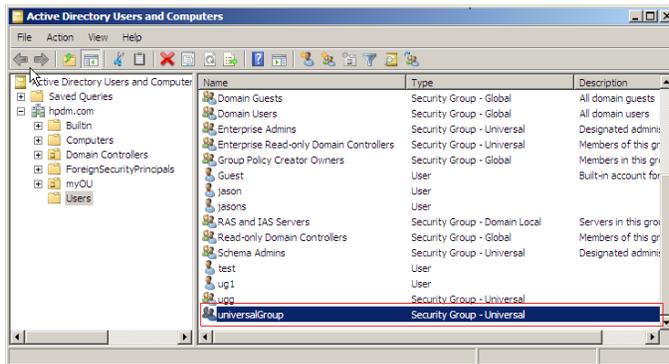
Universal group login

A universal group is a group that can contain accounts from the current domain and other trusted domains. The advantage of using a universal group is that you can import the group into HPDM. You only need to add accounts from different domains into it.

To import a universal group:

This example uses a universal group in the domain hpdm.com that contains two accounts.

- jasons is an account in the domain hpdm.com.
- t2 is an account in the domain test.hpdm.com.



1. In the HPDM Console, Go to **Users & Groups > Users > Import from LDAP**.
2. Select this universal group, and then select **Import**.
3. To verify that the universal group has been imported, log in to HPDM as both jasons (from hpdm.com) and t2 (from test.hpdm.com).

Note

To support multiple domains, the following conditions must be met:

- The DNS server of each server should work well, which means that the HPDM Server and each domain server can reach each other by domain name.
- All domains must trust each other so that they all have the right to communicate with each other.

HPDM must support multiple domains when it is supporting universal group login.

LDAP subgroup login

HPDM supports the login of each user of LDAP subgroup.

Consider the following LDAP server:

- Group: G1
 - It contains group G2.
 - It contains user account t1.

- Group: G2,
 - It contains user account t2

If you import user group G1 into HPDM, user accounts t1 and t2 can both log in to HPDM.

To import an LDAP subgroup:

1. Under **Groups to Import**, select the group name.
2. In the Console, select **Groups > Edit**, and then verify that t1 and t2 are both listed under **Users**.
3. Verify that the group has imported correctly by logging in to HPDM as both t1 and t2.

Privilege System

This section describes the privilege management system in HP Device Manager (HPDM) 5.0. HPDM 5.0 has a more detailed system for privilege classification. HPDM provides not only traditional action-based privilege, but also provides object level privilege that can control each individual template.

This document also covers privilege-related operations and several examples.

In addition to privilege management, HPDM provides another function called a security filter. Depending on customized filter conditions, it can filter the qualified devices and tasks for specified users or groups.

Action based privilege

Action based privilege, has been available in previous HPDM versions. It assigns privileges to a group, and then users within the group inherit those privileges.

To see the privilege as user interface:

1. In the HPDM Console, select **Users & Groups** page, select Groups in **Navigation View**.
2. On the **Groups** table, select a group.
3. In the group properties dialog, select the **Privileges** page.

In this tab, you can see all available privileges and the three default groups: Administrators, Power Users, and Users. None of the default groups can be deleted. The privileges for Administrators cannot be edited. For all other groups, the privileges can be edited. For more information, see **Privilege-related operations**.

Note

Since rules require Template Viewing privilege, when selecting **Rule Management**, **Template Viewing** is selected by default. When **Template Viewing** is cleared, **Rule Management** is automatically cleared.

If you do not have the privilege to perform an operation, an HPDM Console error message is displayed.

This function differs for the Template View and User Management operation. If you do not have Template View privilege, the **Templates & Rules** do not display on the HPDM Console. If you do not have User Management privilege, the **Users & Groups** does not display.

Object based privilege

Object based privilege controls each user group's access to the view, modify, and execute operations for each template.

To configure template-level privileges:

1. In the HPDM Console, select **Template > Set Access Privileges**.
 - or–
 - Right-click a template and select **Set Access Privileges**.
2. If necessary, to configure the default privileges, select a group, and then select **Edit** to change the group's system-level privileges.
3. To see all current templates, select **List all templates**.
4. If you can give a group privilege to access a template's operations, the value under Inherited from group is **Yes**. To enable a group to inherit privileges to templates, select **View**, **Execute**, and/or **Modify** next to the templates' names, and then select **Inherit**.

Note

The group inherits privileges to the selected operations only.

Verify that the template privilege has changed. If so, the template name becomes longer.

HPDM behavior under privilege management system

In HPDM, there are three default groups:

- **Administrators**—Has all privileges and cannot be edited.
- **Power Users**—Has basic privileges. New users are assigned to this group by default.
- **Users**—Has only the template execute privilege and other read-only privileges.

You can create and customize new groups. By default, these groups have the same privileges as power users.

Note

In HPDM, there is a default super user created during the HPDM installation process. By default, the user name is root. You can change the password, but you cannot delete user, because it belongs to the Administrators group.

HPDM privileges use the following rules:

- Users only get privileges through groups. A user can belong to either one or multiple groups and receives all privileges assigned to those groups.
- For system-level privilege operations, if a user has no right to operate, a message displays to notify the user. Exceptions include Template View and User Management.
- If a template's privileges are inherited from a group, the privileges change when group privileges change. If a template has its own privileges, template privileges do not change with group privileges.
- A newly generated template has the following privileges:
 - It inherits privileges from its parent template (the template from which the “name becomes bigger”).
 - If there is no parent template, it inherits its privileges from its basic template.
 - The privileges for a sequence template are the minimum intersection of the template's privileges and its subtemplates' privileges. After a sequence template has been created, the subtemplates inherit privileges from it as the parent template. (An imported sequence template has the minimum intersection of privileges from the base sequence template and its subtemplates.)
 - For a rule template, if the template does not have the execute privilege, the template cannot be added into a rule.
- If a user does not have the necessary privileges to perform an operation, one of the following occurs:
 - If the user does not have the **Template View** privilege, **Templates & Rules** does not display in the HPDM Console.
 - If the user does not have the **User Management** privilege, **Users & Groups** does not display in the HPDM Console.
 - If the user does not have the **View Tasks from All Users** privilege, the tasks belonging to other users and rule tasks do not appear in the HPDM Console.
 - For other privileges the user might not have, if the user tries to access or modify that privilege, the HPDM Server sends a message to the HPDM Console that the action is not allowed.
- If the privileges of a specified group change, the users in the group are logged out from any live sessions to the HPDM Server. The users must log in to HPDM again.

In the 5.0 SP1 version, some template privilege adjustments were made, as follows:

- Template privilege is the minimum privilege of action privilege and object privilege.
 - Templates without template execute privilege will not appear in the template chooser of the send task. And these templates will not appear on the rule action page.
 - In the merge template page, a template without template modify privilege does not appear in the merge template list.
-

Note

When HPDM 5.0 is upgraded to 5.0 SP1 and later, if the template in some lists disappears, please check if it is related to the above privilege changes.

Security filter

A security filter is a special type of device filter that must be assigned to users or groups. Its purpose is to limit what kinds of devices and tasks can be seen by the specified users or groups.

A security filter uses the following rules:

- It is system-level setting. After a user has been assigned to a filter, all HPDM Console behavior when this user is logged in will be the same.
- It is a copy of a device filter. After it is assigned, the original device filter no longer affects it. If the original device filter changes, the security filter does not change.

Note

If a user and the groups it belongs to have multiple security filters, the user's filter results use the minimum intersection of all security filters from the user and its groups.

Privilege-related operations

The following diagrams provide information about privilege-related operations.

Category	Subcategory	Atom privilege	Comment	Power Users	Users
Administration	Configuration management	Set configuration parameters		√	X
	HPDM Gateway access control	Acknowledge		√	X
		Ban			
		Manually control device management access			
	Key management	Update current key		X	X
		Import key			
		Clear key log			
	Status snapshot	Add status snapshot		√	X
		Edit status snapshot			
		Delete status snapshot			

Category	Subcategory	Atom privilege	Comment	Power Users	Users
Gateways&Repositories	Gateway Task Execution	Discover device		√	X
		Discover Gateway			
	Gateway Modification	Configure Gateway		√	X
		Update Gateway			
		Delete Gateway			
	Repository management	Add repository		√	X
		Import repository			
		Remove repository			

	Edit repository			
	View repository			
	Mapping			
	Sync			

Category	Subcategory	Atom privilege	Comment	Power Users	Users
Manage Devices	Device Modification	Add device		√	X
		Delete device			
	Device Filter Management	Add device filter Delete device filter Edit device filter		√	X

Category	Subcategory	Atom privilege	Comment	Power Users	Users	
Tasks&Reports	Audit Logs Management	View		X	X	
		Export				
	View task from all users	View task from all users		X	X	
	Report management	Add report				
		Edit report				
		Delete report			X	X
		Preview report				
	Export report					

Category	Subcategory	Atom privilege	Comment	Power Users	Users	
Templates&Rules	Rules management	Add rule				
		Edit rule				
		Delete rule		√	X	
		Order rule				
		View rule				
	Template Execution	Send task			√	√
		Resend task				
		Configure template in rule				
	Template Modification	Sava as template		If no modify privilege, the template will not be editable.	√	
Import template						
Delete template					X	

		Update template			
		Rename template			
		Merge templates			
	Template Viewing	View	Make template visible or not	√	√
	Template Shared folder Management	Create			
		Rename			
		Delete		√	X
		Copy			
		Move			
	Remove				

Category	Subcategory	Subcategory	Atom privilege	Comment	Power Users	Users
Users&Groups	Template Access Privileges management		Set privileges for single or multiple templates		X	X
	User management	User	Add user		X	X
			Delete user			
			Edit user			
			Change password			
		Group	Add group			
			Delete group			
			Edit group			
		LDAP	Import from LDAP			
		Security Filter	Add security			
			Remove security			

Note

All privileges are independent and do not influence other privileges.

Sample Scenarios

The following example scenarios demonstrate how HP Device Manager's privilege system works.

Example 1

There are two user groups and the **_Capture Image** template is visible to group1, but not visible to group2.

Save this template to generate the new template **my_Capture_Image**. This new template inherits its template-oriented privileges from the **parent _Capture Image** template.

The new template **my_Capture_Image** is also visible to group1, but not visible to group2.

Example 2

This example uses the same scenario as Example 1, and **_Deploy Image** template is visible to group1, but not visible to group2.

Use the **_Capture Image** template to generate a new deploy image template named **my_Deploy_Image**. This new template inherits the privileges of the base template **_Deploy Image**, not **_Capture Image**.

The new template **my_Deploy_Image** is visible to group1, but not visible to group2.

Example 3

There are two user groups.

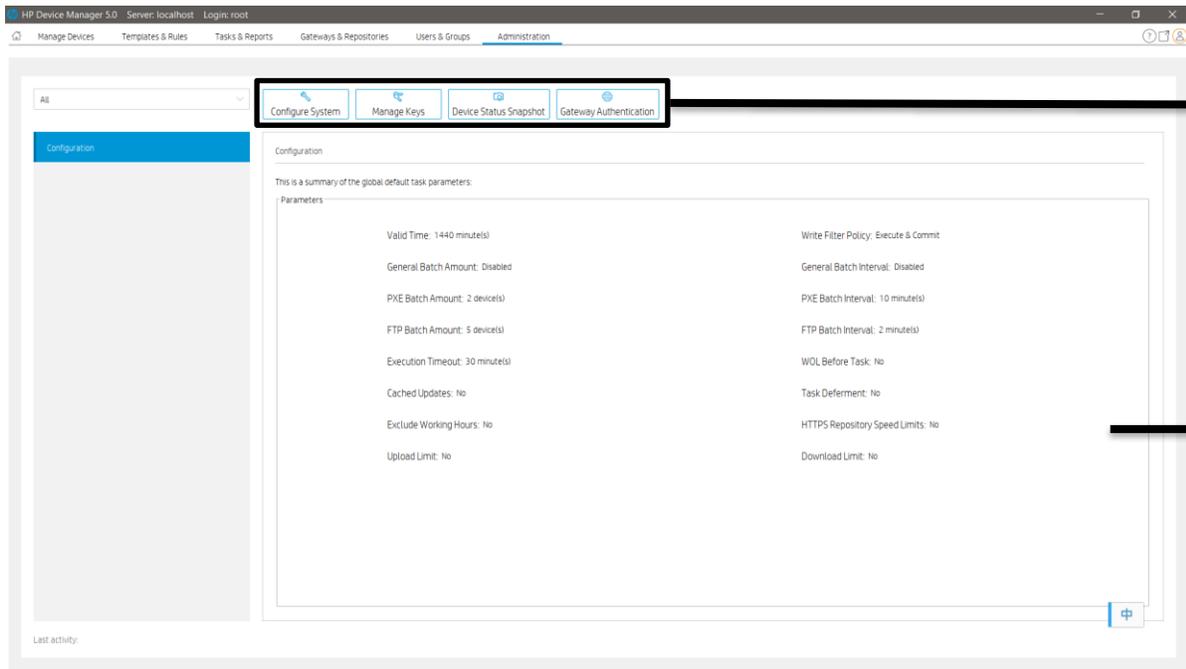
- Group1 includes **_Update Agent** privilege only (view, modify).
- Group2 includes **_Get Asset Info** privilege only (view, execute).

Create a new sequence template based on the **_Update Agent** and **_Get Asset Info** templates. This new template has the minimum intersection of the **_Update Agent template**, **_Get Asset Info** template, and all subtemplates.

The new template has only view privilege.

Administrative Functions

Page Layout



1. Toolbar— An enumeration of the Administration most commonly operations.



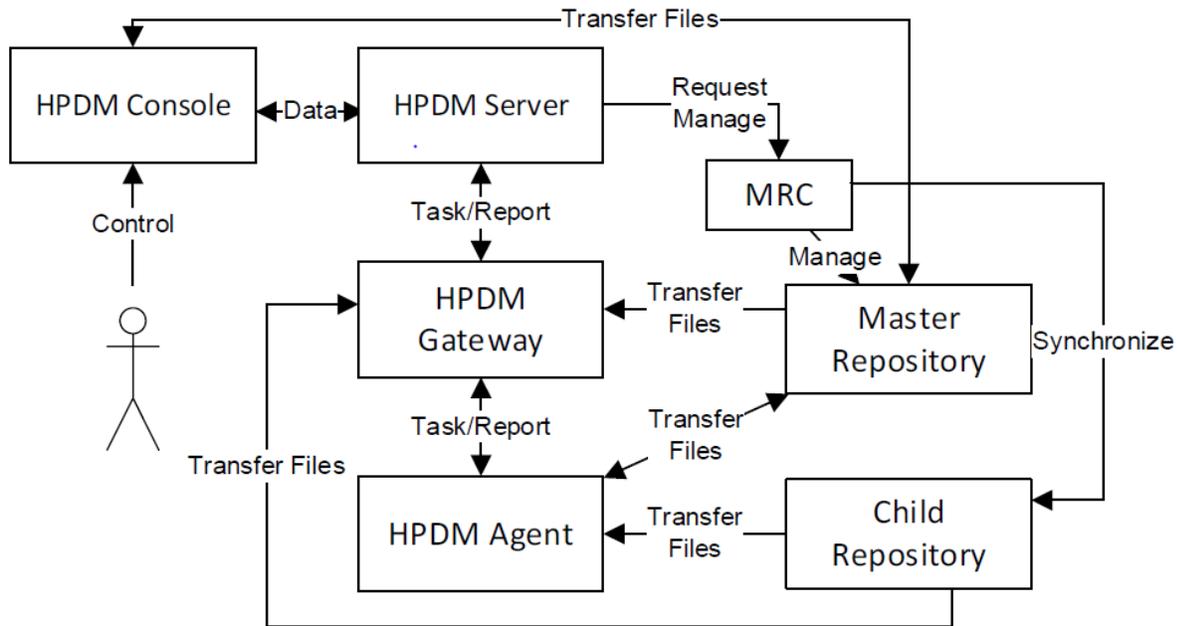
- **Configure System**—Configuration management.
- **Manage Keys**—The key is passed to the devices during the key update process. The devices check the key passed by HPDM Server when executing tasks.
- **Status Snapshot**—Status snapshot schedule.
- **Gateway Authentication**—HPDM Gateway access control.

2. Configuration View—Summary of the global default task parameters.

Security Controls

HP Device Manager (HPDM) is a solution designed to help the IT administrators manage and control remote HP thin clients. The solution consists of the HPDM Console, HPDM Server, HPDM Gateway, HPDM Agent, Master Repository Controller, and file repositories. A standard setup is shown in Figure 18. The solution needs to store highly sensitive data, such as the passwords of the database and file repositories and transfer it over the network. To protect the data, the solution introduces several security measures to authenticate devices and encrypt sensitive data locally. The solution also provides other measures to protect the client devices from misoperation.

Figure 10. HP Device Manager setup



Database confidentiality

In the solution, only the HPDM Server needs to access the database. The HPDM Server stores database account information on the local storage of the server and encrypts the password with a DES algorithm.

File repository confidentiality

HPDM stores file repository information in the database and encrypts the password with an AES algorithm.

HPDM logon authentication

When HPDM is installed, it will prompt you to set a password for the super administrator account. The HPDM Administrators' usernames and the passwords are encrypted by AES256. When storing passwords in database, we compute SHA256 hash values and then apply AES256 to encrypt the hash values. When an HPDM Administrator tries to log on to the HPDM Console, the HPDM Server compares the input (username and SHA256 hash value of the password) to the data in the database to determine whether to allow or deny access. HPDM only saves the encrypted SHA256 hash value of the password, which is unlikely to reveal the original password to a hacker, because SHA256 is a hash cryptographic algorithm.

Confidential data in log files

Each part of HPDM supports different log levels. Set different log levels to trace errors or detail information. If you set the log level to the most detailed level, then the log messages might contain sensitive data, such as passwords in tasks. To protect this sensitive data, HPDM automatically hides it with an asterisk sequence. For example, an FTP password such as P@ssw0rd would be written in the log file as *****.

User management

HPDM supports the following user account and user group management tools to avoid any misoperation and make sure that the system is stable.

- One user is classified as the super administrator and others are classified as ordinary administrators.
- Each ordinary administrator can be put into or removed from a group. All administrators in the same group have the same privileges.
- Each ordinary administrator or group can be granted certain privileges, such as managing specific thin client devices or executing specific operations. The super administrator always has full control to the system.

Authentication management

HPDM provides an authentication capability that allows the HPDM Gateways and the HPDM Agents to recognize a secure management server. There are three features for providing authentication: Key Management, Master Repository Controller Access Control, and Gateway Access Control.

Key management

The authentication key enables the HPDM Agents to verify if the HPDM Server has the privilege to manage them. By default, the HPDM Agents and HPDM Server have the same original key. For security, you can use Key Management to create a new key, and then the HPDM Agents will update their keys automatically. After updating their keys, the HPDM Agents reject tasks sent by servers that do not have the correct key.

An HPDM Agent saves the keys in the files key0.key and key1.key. The file key0.key is the default key and the file key1.key is the current key. The key files are encrypted with DES in CBC mode. When the current key expires, the HPDM Agent uses the default key to overwrite the current key.

To update an HPDM Agent key:

1. In the HPDM Console, select **Manage Keys** from the **Administration Page**. Add a new key.
2. The HPDM Server sends the new key to the HPDM Gateway because the HPDM Gateway keeps the key list in its memory.
3. When an HPDM Agent sends a startup report or tries to receive tasks, the HPDM Gateway will check the HPDM Agent key's SHA256 hash value.
 - a. If the agent key's SHA256 cannot be recognized, the gateway will refuse the connection.
 - b. If the agent key's SHA256 belongs to an old key, the gateway will generate an update key task for the device. The new key will be encrypted with the old one via a AES256 algorithm before being sent to the agent.
 - c. If the agent key's SHA256 is the same as the new one, the gateway will not do any additional operations.
4. The HPDM Agent receives the update key task, decrypts the new key using the old key, and updates the old key to the new one.

Master Repository Controller access control

In the HPDM hierarchy, only the HPDM Server connects to the Master Repository Controller to manage the Master Repository and Child Repositories. When the HPDM Server connects to the Master Repository Controller successfully, both the HPDM Server and the MRC create an RSA key and an X.509 certificate. Then, they exchange the certificates, enroll them, and start a TLS 1.2 connection for security. After the Master Repository Controller enrolls a certificate from an HPDM Server, it rejects connections that either do not have a certificate or have a different certificate.

Gateway access control

The HPDM Server maintains the acknowledged status of a gateway, which is specified by the user from the HPDM Console. When a gateway is discovered by the HPDM Server, the gateway is set to unknown status. You can either acknowledge the gateway or ban it. The HPDM Server will neither establish a connection with a banned gateway nor receive any messages sent from it unless it is later acknowledged.

By default, any gateway with an unknown status is treated like it is safe. HP recommends banning any unexpected gateways that join the HPDM Server. Use the Gateway Access Control dialog to manually control access. Enable the option to treat any gateways with an unknown status as unsafe unless they are later acknowledged.

Network communication

The connections between the HPDM components (Console, Server, Gateway, Agent, and Master Repository Controller) are secure. The components communicate through TLS 1.2 connections created with OpenSSL (www.openssl.org). This prevents data from leaking during network communication.

The crypto algorithms in SSL/TLS use an RSA-created key pair of length 2048 and an X.509-created certificate.

The cipher suites for TLS 1.2 connections: TLS_AES_256_GCM_SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384.

Secure file server

To perform some tasks or operations, the HPDM Console, Gateway, and Agent need to access a repository, or file server, to download or upload files to perform some tasks or operations. To protect this data, HPDM 5.0 supports two types of secure file servers: File Transfer Protocol over SSL (FTPS), Secure File Transfer Protocol (SFTP) and Hypertext Transfer Protocol Secure (HTTPS). FTPS is an extension of the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols. SFTP is a network protocol that provides file access, file transfer, and file management over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) 2.0 to provide secure file transfer capability. Hypertext Transfer Protocol Secure

(HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS).

Task verification

To protect thin clients, an HPDM Agent accepts only the tasks that pass task verification. Task verification is based on Key Authentication. The HPDM Gateway stores the whole key list, which is synchronized from the HPDM Server. The following procedure details how an HPDM Agent receives a task from the HPDM Gateway:

1. The HPDM Gateway connects to the HPDM Agent.
2. The HPDM Agent accepts the connection.
3. The HPDM Gateway sends an encryption request message and creates an SSL-Server instance with OpenSSL.
4. When the HPDM Agent gets the encryption request message, it creates an SSL-Client instance with OpenSSL and connects to the SSL Server.
5. The HPDM Gateway accepts the SSL connection and sends a task request message to the HPDM Agent.
6. The HPDM Agent sends a challenge message to the HPDM Gateway when it receives the task request message. A challenge message includes two parts:
 - a. SHA256 checksum of the HPDM Agent's current key.
 - b. 128-byte randomly generated string.
7. When the HPDM Gateway receives the challenge message, it searches the SHA256 hash values of the keys from the key list. If it finds the key, it calculates the SHA256 hash value of the key plus the random string and signs the result to the task for the HPDM Agent. Then, the HPDM Gateway sends the task to the HPDM Agent.
8. When the HPDM Agent receives the task, it verifies the signature first. The HPDM Agent uses its current key and the random string to calculate the SHA256 hash value. If the SHA256 hash value is not same as the task signature, it will reject the task. Otherwise, it accepts the task and adds the task to the execution queue.

Compatibility with Older Components

HPDM security has been updated to the latest version (1.1.0j of OpenSSL). By default, only TLSv1.2 is enabled and weak ciphers, such as RC4, DES, 3DES, and SEED, have been removed. This prevents vulnerabilities of older versions of SSL/TLS from being exploited.

However, some HPDM Agents and HPDM Gateways might only support older SSL/TLS protocols. You can open HPDM Configuration Center to change SSL/TLS policy to make HPDM 5.0 be compatible with the old Agents and the old Gateways. You can find "SSL/TLS 1.0 support" from the HPDM Server page and the advanced options of the HPDM Gateway page. Set it to "YES" to support old Agents and old Gateways. After all of old Agents and old Gateways are upgraded, please set it to NO to improve security level.

Note

HPDM 5.0 only guarantees you can upgrade Agents and Gateways from 4.7 to 5.0. If your Agents or Gateways are not 4.7, first install HPDM 4.7 to upgrade them.

HP Update Center

The HP Update Center allows you to leverage software components from the HP file 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 **Configuring HP Update Center proxy settings** 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, BIOS Update, Windows Update, Others—Generate **_File and Registry** templates

HP Update Center

Title	Category	Device Model	OS Type	Disk Space	Version
AmazonWorkSpace...	Application	t430/t540/t550/t6...	Win10IoT-64	212.13 MB	5.0.0
AmazonWorkSpace...	Application	t430/t540/t550/t6...	Win10IoT-64	351.56 MB	5.6.2
AVDWindows365Cli...	Application	t638/mt22/mt32/t...	Win10IoT-64	22.40 MB	1.2.3130
AVDWindows365Cli...	Application	mt22/mt32/t655/t...	Win10IoT-64	23.25 MB	
AVDWindows365Cli...	Application	t430/t540/t550/t6...	Win10IoT-64	31.27 MB	1.2.3770
CitrixWorkspaceApp...	Application	t430/t630/t740/t5...	Win10IoT-64	70.30 MB	19.12.0
CitrixWorkspaceApp...	Application	t430/t540/t630/t7...	Win10IoT-64	71.50 MB	1912.4000.19
CitrixWorkspaceApp...	Application	t430/t540/t630/t7...	Win10IoT-64	192.19 MB	19.12.6000.9
CitrixWorkspaceApp...	Application	t430/t540/t630/t7...	Win10IoT-64	128.45 MB	20.6.0.38
CitrixWorkspaceApp...	Application	t430/t540/t630/t7...	Win10IoT-64	134.95 MB	20.9.5.30
CitrixWorkspaceApp...	Application	t430/t540/t630/t7...	Win10IoT-64	138.74 MB	20.12.0.39
CitrixWorkspaceApp...	Application	t430/t540/t630/t7...	Win10IoT-64	142.41 MB	21.3.1.25

[Proxy Settings...](#) Generate Templates Properties Close

Generating task templates

To use the HP Update Center to generate task templates:

1. In HPDM Console, right-click on any template, select **Import**, and then select **HP Update Center**.

-or-

Select **HP Update Center** toolbar button in **Template & Rules** page.

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

TIP: You can use the table quick search function to filter the components.

Note

If HPDM Console or HPDM Master Repository Controller does not have direct access to the HP file 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 file server.

Use the test function on the proxy interface to test the connectivity of the configured proxy. 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 **Configure System** on the **Administration** page.
2. In the Configuration Management window, select the **Proxy Settings** 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.

Documentation and software updates

The documentation lists all documents for the current and previous versions of HPDM, including the admin guide, white paper, and release notes. The software updates list all versions of HPDM.

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 **Configuring HP Update Center proxy settings** for more information.

Access documentation

1. Select  in the upper right corner of the console, and then select **Documentation**.
2. Select on the document hyperlink. The default browser opens a link to this document.

Access software updates

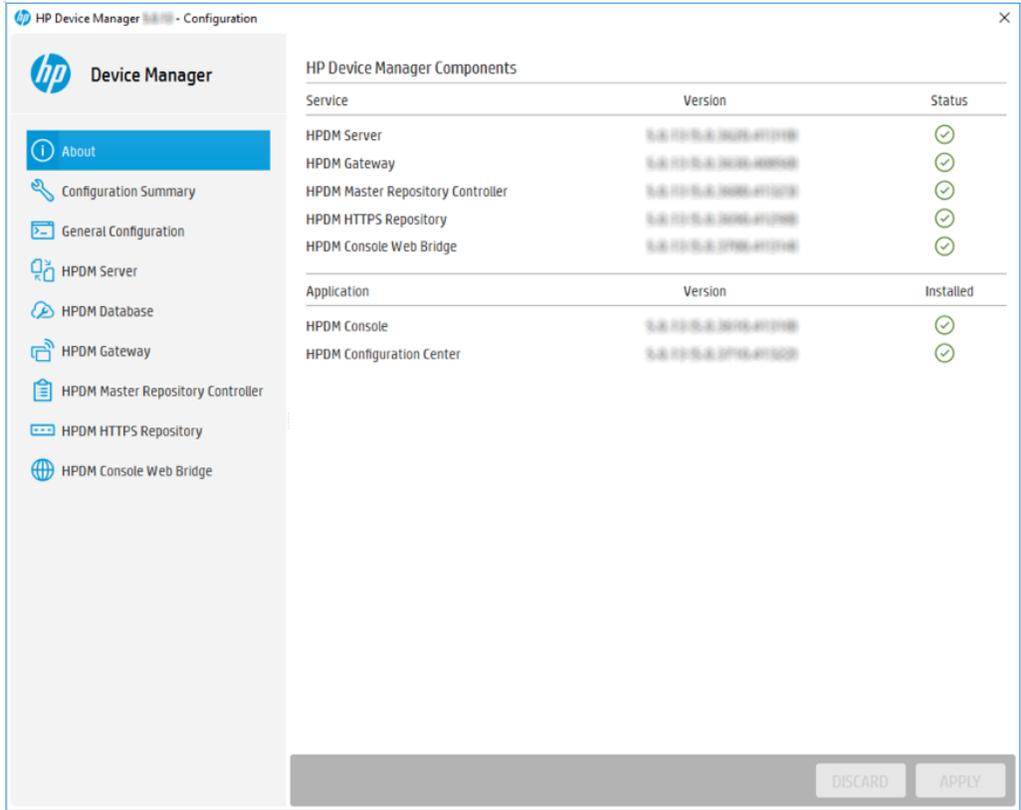
1. Select  in the upper right corner of the console, and then select **Software Updates**.
 2. Select the software hyperlink. The default browser opens a link to this software.
-

Note:

Because access to these files is opened by the default browser, if the proxy is set, the browser should also set the proxy.

Configuration Center

An HPDM Configuration Center Wizard appears after HPDM is installed. If you choose complete installation, you will see all the HPDM components in the About page.



Component: Lists all installed HPDM Components.

Version: The version of HPDM Component.

Status: The status of HPDM Component service. If there is not an HPDM Component service, “N/A” is displayed.

Configuration Summary

On the Configuration Summary page, you can see the detailed configuration about the HPDM Components you have installed.

HP Device Manager - Configuration

Device Manager

- About
- Configuration Summary
- General Configuration
- HPDM Server
- HPDM Database
- HPDM Gateway
- HPDM Master Repository Controller
- HPDM HTTPS Repository
- HPDM Console Web Bridge

Configuration Summary

General

Language: English (United states)

HPDM Server

Log level: DEBUG
 SSL/TLS 1.0 support: NO

HPDM Database

Database provider: PostgreSQL
 Database name: hpdmdb
 Server address: localhost:40006
 User name: postgres

HPDM Gateway

Server address: localhost
 Gateway ID: 00:0C:29:38:8E:3B
 Local NIC: any NIC
 Log level: TRACE
 Poll batch: 50
 Poll Interval: 0s
 Allow Multiple Gateways per Subnet: Yes
 Start HPDM PXE service when HPDM Gateway is started: No
 TLS 1.0 compatibility: No
 Ignore network address translation: No

HPDM Master Repository Controller

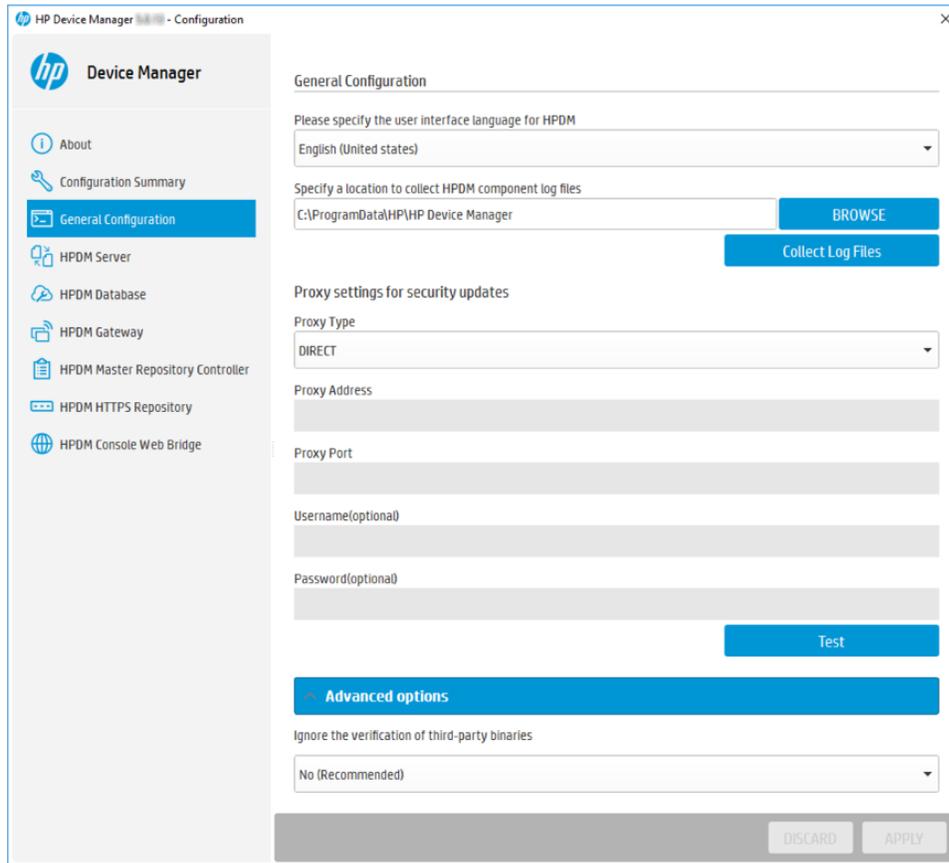
Repository path: C:\ProgramData\HP\HP Device Manager\HPDM
 Log level: Error

HPDM HTTDC Repository

DISCARD APPLY

General Configuration

In General Configuration page, you can specify the operating language for HPDM, collect all HPDM component log files, configure the proxy settings for security update, or configure the advanced options



The screenshot shows the HP Device Manager Configuration window. The left sidebar contains a navigation menu with the following items: About, Configuration Summary, General Configuration (highlighted), HPDM Server, HPDM Database, HPDM Gateway, HPDM Master Repository Controller, HPDM HTTPS Repository, and HPDM Console Web Bridge. The main content area is titled 'General Configuration' and includes the following sections:

- Language:** A dropdown menu labeled 'Please specify the user interface language for HPDM' with 'English (United states)' selected.
- Log Files:** A text field for 'Specify a location to collect HPDM component log files' containing 'C:\ProgramData\HP\HP Device Manager', a 'BROWSE' button, and a 'Collect Log Files' button.
- Proxy settings for security updates:**
 - 'Proxy Type' dropdown menu with 'DIRECT' selected.
 - 'Proxy Address' text field.
 - 'Proxy Port' text field.
 - 'Username(optional)' text field.
 - 'Password(optional)' text field.
 - 'Test' button.
- Advanced options:** A blue header bar with a chevron icon.
- Ignore the verification of third-party binaries:** A dropdown menu with 'No (Recommended)' selected.

At the bottom right of the window are 'DISCARD' and 'APPLY' buttons.

The language you want to use with HPDM takes effect in the HPDM Server and this Configuration Tool. If you change the language, you have to restart other components.

Collect log: Select **Browse** to select a location to save the HPDM components log, and then select **Collect Log Files**.

Proxy settings for security updates

Allows you to configure the proxy settings for downloading security update packages. It is for both HPDM HTTPS Repository and HPDM Console Web Bridge security updates. By default, this tool downloads the package without utilizing any proxy servers.

Important

Security update requires Internet access. If the system running HPDM Configuration Center cannot access the Internet directly, you must configure proxy settings first.

Proxy Type: Choose the proxy type. Currently HPDM only supports HTTP/1.1 (connect method) and SOCK5.

Proxy Address: The address of the proxy server.

Proxy Port: The port of the proxy server.

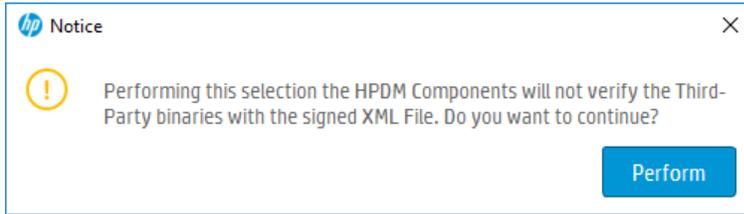
Username & Password: They are optional, and they depend on the proxy server's configuration.

Test: Allows you to test the proxy settings.

Advanced Options

Ignore the verification of the third-party binaries: Allows you to specify the option about the verification of the third-party binaries. By default, all HPDM components verify the third-party binaries upon startup. The HPDM component and service exits if the

verification fails. If a HPDM component or service fails to start, please check the component log. If it is caused by the verification failure, please change the option to “Yes”. The following message box pops up when changing it to “Yes”.



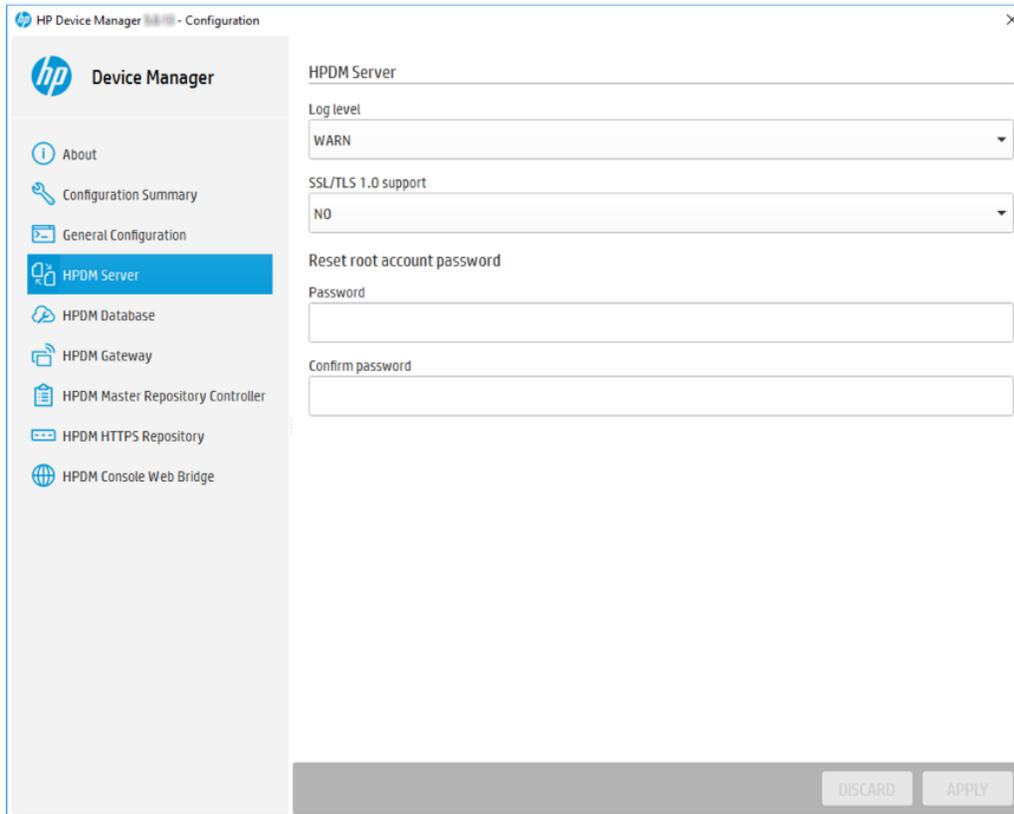
Important

Enabling this option carries the risk of potential security issues, please proceed with caution.

If you update the third-party library manually, please enable the “**Ignore the verification of the third-party binaries**” option.

HPDM Server

In HPDM Server page, you can see the detailed configuration of HPDM server.



Log level: Configure the log level of the HPDM Server component.

SSL/TLS 1.0 support: If you want to use the SSL/TLS 1.0 support, select **YES**.

Reset root account password: Change the root account password by using HPDM Configuration Center on the HPDM Server page. The password should be between 12 and 36 characters in length and must include uppercase letters, lowercase letters, numbers, and special characters.

HPDM Database

In HPDM Database, you can see the detailed configuration of HPDM Database Components.

HP Device Manager 5.0.14 - Configuration

Device Manager

- About
- Configuration Summary
- General Configuration
- HPDM Server
- HPDM Database**
- HPDM Gateway
- HPDM Master Repository Controller
- HPDM HTTPS Repository
- HPDM Console Web Bridge

HPDM Database

PostgreSQL update

Status	Update available	Download
--------	------------------	--------------------------

General

Database provider	PostgreSQL
Database name	hpdmdb
Server address	localhost:40006
User name	postgres

[Manage Database](#)

PostgreSQL Server Access Management

This is a specific account to allow read/write access the database. This will not impact HPDM Server service.

User name

Password

Confirm password

[DISCARD](#) [APPLY](#)

Note:

If you are not initializing the HPDM Database, 'NA' is displayed for the four properties.

PostgreSQL update: this option is support for the minor psql update, when the HPDM Server updates its psql version, custom can use the HPDM Configuration Center to update the psql version, **this update supports only minor version updates (e.g. from 16.1 to 16.2). Major version updates (e.g. from 16.3 to 17.0) are not supported.**

5. Click the Download button to download the new package.
6. After you have successfully downloaded the package, click the Update button to update the Postgresql.
7. Once the update is completed, a notice indicating the Postgresql has been successfully updated will appear.

HP Device Manager 5.0.14 - Configuration

HP Device Manager

- About
- Configuration Summary
- General Configuration
- HPDM Server
- HPDM Database**
- HPDM Gateway
- HPDM Master Repository Controller
- HPDM HTTPS Repository
- HPDM Console Web Bridge

HPDM Database

PostgreSQL update

Status: Update downloaded Update

General

Database provider	PostgreSQL
Database name	hpdmdb
Server address	localhost:40006
User name	postgres

PostgreSQL Update

To prevent database corruption during the update, it is recommended to back up the current database beforehand.

Click **BACKUP** to launch the HPDM Server Backup and Restore Tool for backing up the database or click **SKIP** to bypass this step.

SKIP BACKUP

Password:

Confirm password:

DISCARD APPLY

HPDM Database

HPDM Gateway

HPDM Master Repository Controller

HPDM HTTPS Repository

HPDM Console Web Bridge

Manage Database

Upgrading postgresql...

Impact HPDM Server service.

User name

dm_postgres

HP Device Manager 5.0.14 - Configuration

hp Device Manager

About

Configuration Summary

General Configuration

HPDM Server

HPDM Database

HPDM Gateway

HPDM Master Repository Controller

HPDM HTTPS Repository

HPDM Console Web Bridge

HPDM Database

PostgreSQL update

Status Up to date [Check for update](#)

General

Database provider	PostgreSQL
Database name	hpdmdb
Server address	localhost:40006
User name	postgres

Manage Database

PostgreSQL Server Access Management

This is a specific account to allow read/write access the database. This will not impact HPDM Server service.

User name

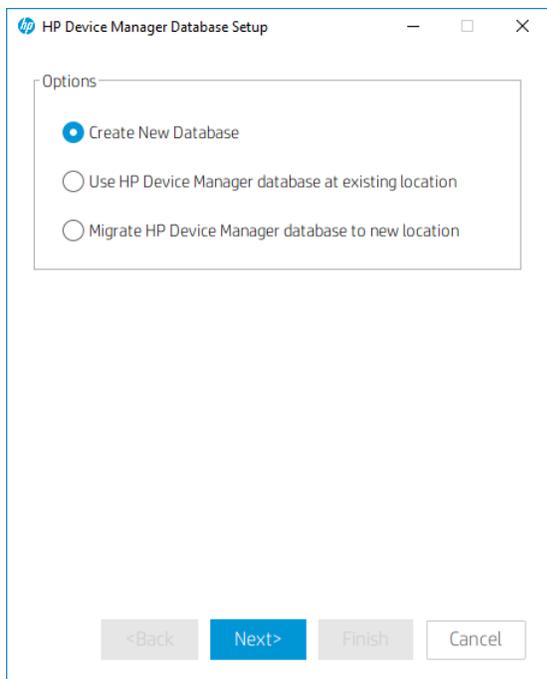
dm_postgres

Password

Confirm password

HPDM Database has been updated. [DISCARD](#) [APPLY](#)

You can select **Manage Database** to operate the HPDM Database.



Create New Database

1. Select **Create New Database**, and then select **Next**.

HP Device Manager supports two database types:

- **PostgreSQL**—If you choose PostgreSQL, you need not perform any other database configuration as it is configured in HPDM.
- **MS SQL Server**—If you choose MS SQL, you must first create an independent MS SQL Server instance to connect to (see MS SQL Server documentation).

Note:

If you choose MS SQL Server as your HPDM database, the authentication type in the HP Device Manager Database Setup dialog must correspond to the MS SQL Server configuration, and you must be authorized to create the database.

If you choose Windows Authentication during the database engine configuration, you must choose **Window Authentication** when configuring the HPDM database.

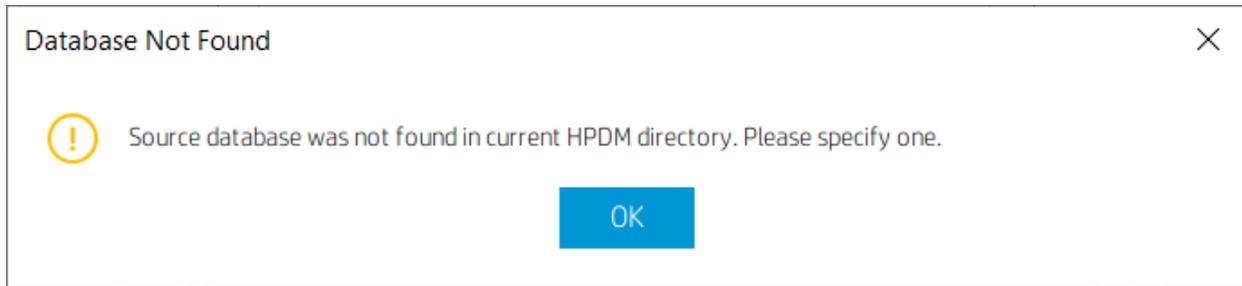
If you choose mixed mode during the database engine configuration, you can choose either **Window Authentication** or **SQL Server Authentication** when configuring the HPDM database.

2. Choose your database type, and then select **Next**.
 - a. If you choose PostgreSQL, you must set a password.
 - b. If you choose MS SQL Server, you must manually input the database information.
3. A progress bar displays. When database creation is complete, enter and confirm the password for the root Administrator account, and then select **Finish**.
4. Select **OK**. The database is created.

Using an existing database

The option **Use HP Device Manager database at existing location** means that HPDM uses the existing database instead of creating a new one. For example, you can use the existing version 5.0 database.

1. Select **Use HP Device Manager database at existing location**, and then select **Next**. A processing dialog box is displayed while a connection is made to the existing database. A dialog displays notifying you that the connection was successful. HPDM is now upgraded.
2. If a dialog box appears notifying you that there was a problem connection to the existing database, select **OK** to specify the database manually.



3. Select a configuration mode:
 - a. **Import**—You can import an existing database configuration file: for example: hibernate.properties.
 - b. **Setting Database**—You configure the database manually.
4. Select **Import**, and then select **Browse**.
5. Go to the HPDM directory .../Server/conf, select the **hibernate.properties** file, and then select **Open**.
 - a. If the existing database is PostgreSQL with a default password, a dialog box prompts you to set new password for PostgreSQL. Enter your **Password**, enter the same password in **Confirm Password**, and then select **OK**.
After you reset your password, the database information automatically populates the **Database Settings** fields.
 - b. If you need to enter the Database Settings information manually, select **Setting Database**, select the database type, and then enter the database information under **Database Settings**.
6. Select **Browse**, select the installation path of the last installed HPDM, and then select **Next**.
7. Enter and confirm the password for the root Administrator account, and then select **Finish**.
8. Select **OK**. The existing database is now used.

Migrate an existing database to a new location

If you select **Migrate HP Device Manager database to new location**, perform the following task:

1. Select **Migrate HP Device Manager database to new location**, then select **Next**.
2. Specify the source database. Select the last installed HPDM directory, and then select the database type. The database settings (stored in a hibernate. Properties file), except for the password, are automatically loaded into Database Settings.
3. The password is automatically loaded.
4. Select **Next**.
5. Specify the destination database, choose the database type, and then select **Next**. The source database and destination database cannot both be PostgreSQL.
6. After the database is migrated, enter and confirm the password for the root Administrator account, and then select **Finish**.
7. Select **OK**. The database is migrated.

HPDM Gateway

In HPDM Gateway page, you can see the detailed configuration of HPDM Gateway component.

The screenshot shows the HP Device Manager Configuration window for the HPDM Gateway component. The window has a sidebar on the left with the HP logo and the text 'Device Manager'. The sidebar contains several menu items: 'About', 'Configuration Summary', 'General Configuration', 'HPDM Server', 'HPDM Database', 'HPDM Gateway', 'HPDM Master Repository Controller', 'HPDM HTTPS Repository', and 'HPDM Console Web Bridge'. The main area of the window is titled 'HPDM Gateway' and contains the following configuration fields:

- HPDM Server address:** localhost
- Gateway ID:** 00:0C:29:38:8E:3B
- Local NIC:** any NIC
- Log level:** TRACE
- Poll batch:** 50
- Poll interval(seconds):** 0
- Allow Multiple Gateways per Subnet:** Yes
- Start HPDM PXE service when HPDM Gateway is started:** No

Below these fields is a blue button labeled 'Advanced options'. Underneath this button are two more configuration fields:

- TLS 1.0 compatibility:** No
- Ignore network address translation:** No

At the bottom right of the configuration area are two buttons: 'DISCARD' and 'APPLY'.

HPDM Server address: Allows you to configure the address of HPDM Server so that the HPDM components are able to interact with this address.

Gateway ID: The mac address of HPDM Gateway. If there are multiple NICs, select one mac address as the Gateway ID.

Local NIC: The IP address of HPDM Gateway. If there are multiple NICs, select the IP address as **Local NIC**.

Log level: Allows you to configure the log level of HPDM Gateway Component.

Poll batch: Defines the maximum number of HPDM Agents that will be queried at a time. Possible values range from 3 to 50. The default value is 50.

Poll interval: Defines whether HPDM Agent polling is enabled. This also defines the delay between HPDM Gateway query requests to give HPDM Agents. The value can be 0 or not less than 60. The default value is 0 seconds, which means polling is disabled.

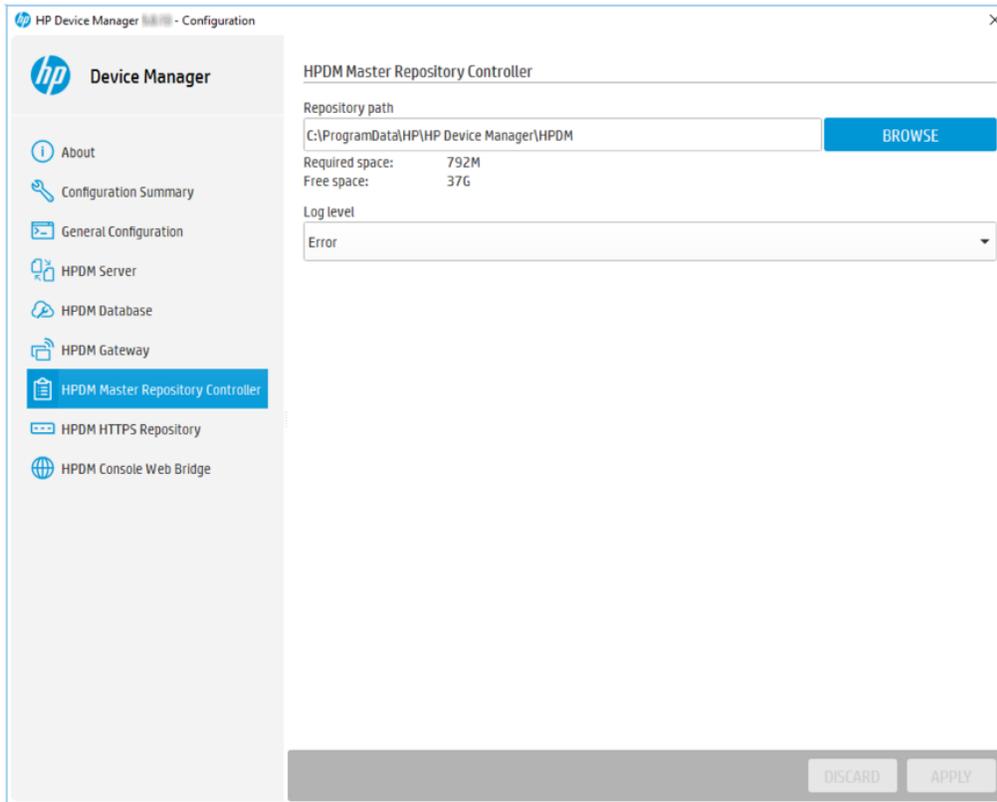
Allow Multiple Gateways per Subnet: Forcibly start gateway even if other gateways are detected in the same subnet.

Start HPDM PXE service when HPDM Gateway is started: PXE service is always started when Gateway is started.

Ignore network address translation: By default, HPDM Gateway treats devices with network address translation as not reachable and marks them as working in PULL mode. Select **Yes** to disable this function if the devices behind NAT are reachable.

HPDM Master Repository Controller

On the HPDM Master Repository Controller page, you can see the detailed configuration of HPDM Master Repository Controller component.



Repository path: Allows you to move the repository root path. Changes take effect after the HPDM Master Repository is restarted.

Log level: Allows you to configure the log level of HPDM Master Repository.

Note

To use a customized certificate, please refer to Appendix E: Configuring HPDM Master Repository Controller Certificate.

HPDM HTTPS Repository

In HPDM HTTPS Repository page, you can see the detailed configuration of HPDM HTTPS Repository component.

Security update: Allows you to check and update Apache, PHP, and OpenSSL for the HPDM HTTPS Repository. If any security updates are available, they will be noted on the page when opening the HPDM Configuration Center. Or you can click the **Check for Update** to check it manually.

- Click the **Download** button to download the new package.
- After you have successfully downloaded the package, click the **Update** button to update the HTTPS Repository.
- Once the update is completed, a notice indicating the HTTPS Repository has been successfully updated will appear.

HP Device Manager - Configuration

Device Manager

- About
- Configuration Summary
- General Configuration
- HPDM Server
- HPDM Database
- HPDM HTTPS Repository**
- HPDM Console Web Bridge

HPDM HTTPS Repository

Security update

Status: Update available [Download](#)

General

Port: 443

Root path: C:\ProgramData\HP\HP Device Manager\HPDM [BROWSE](#)

User Management

User name: 4Wn0RQYz

Password:

Confirm password:

Certificate Management

Certificate: Program Files\HP\HP Device Manager\HTTPSRepository\Apache24\conf\HPDM\server.crt [BROWSE](#)

[DISCARD](#) [APPLY](#)

Downloading HPDM HTTPS Repository packages...

HP Device Manager - Configuration

Device Manager

- About
- Configuration Summary
- General Configuration
- HPDM Server
- HPDM Database
- HPDM HTTPS Repository**
- HPDM Console Web Bridge

HPDM HTTPS Repository

Security update

Status: Update downloaded Update

General

Port: 443

Root path: C:\ProgramData\HP\HP Device Manager\HPDM BROWSE

User Management

User name: 4WnORQYz

Password:

Confirm password:

Certificate Management

Certificate: Program Files\HP\HP Device Manager\HTTPSRepository\Apache24\conf\HPDM\server.crt BROWSE

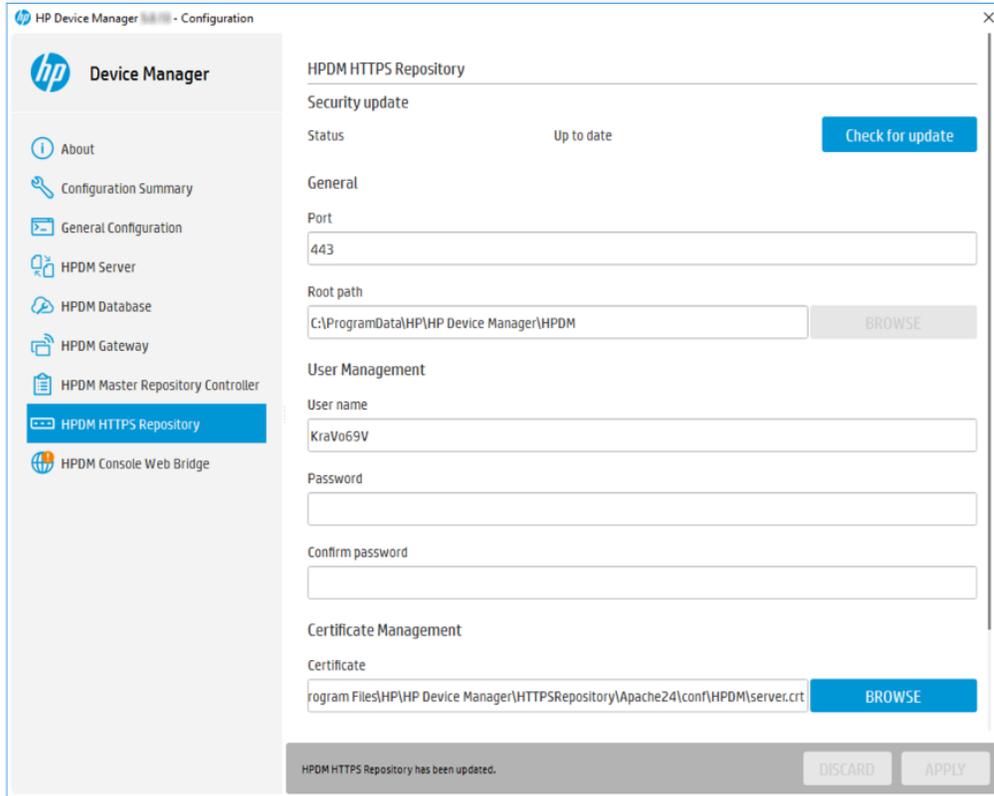
The update package has been successfully downloaded. DISCARD APPLY

HPDM HTTPS Repository Update

Performing this update will restart the HPDM HTTPS Repository. Do you want to continue?

YES NO

Upgrading HPDM HTTPS Repository...



Port: Allows you to configure the occupied port of the HPDM HTTPS Repository Component.

Root path: Display the root path of the HPDM HTTPS Repository. The **BROWSE** button is enabled when the install paths of HPDM Master Repository Controller and HPDM HTTPS Repository are not the same.

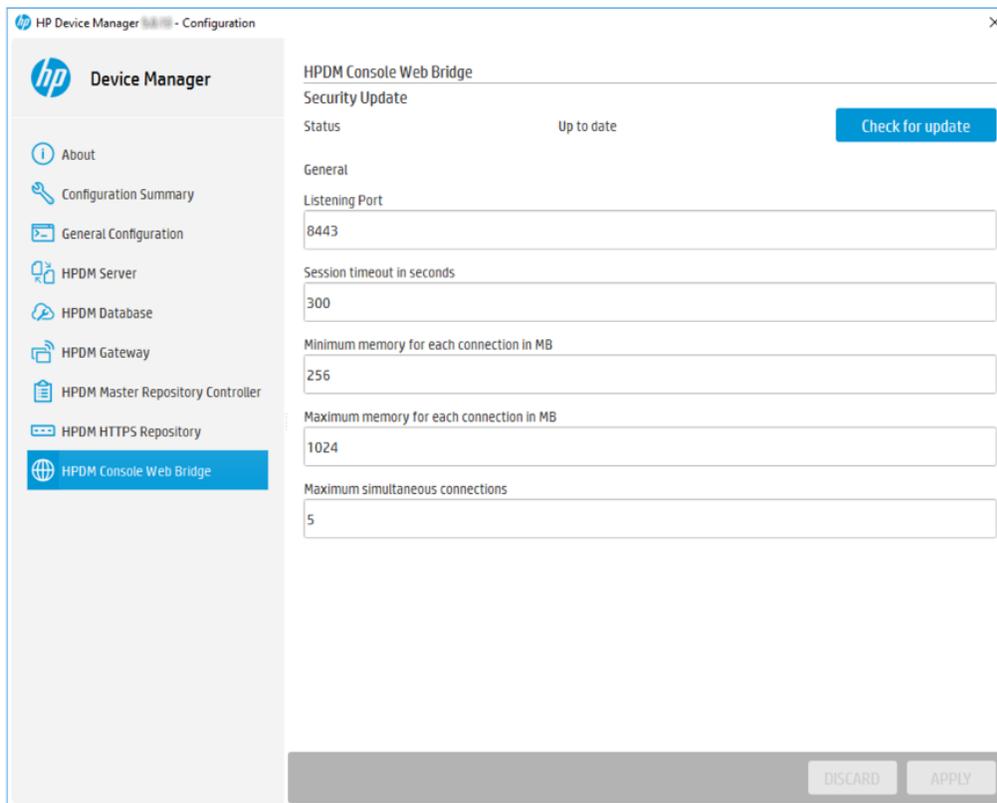
User name: Allows you to configure the HTTPS user name based on detailed rule when you configure HPDM Master Repository use HTTPS protocol

Password: Allows you to reset HTTPS account password in the HPDM HTTPS Repository page when you configure HPDM Master Repository use HTTPS protocol.

Certificate Management: Allows you to change the Certificate and Private key by configuring the Certificate and Private key line Edit.

HPDM Console Web Bridge

In the HPDM Console Web Bridge, you can see the detailed Configuration of the HPDM Console Web Bridge component.



Security update: Allows you to check and update Tomcat for the HPDPM Console Web Bridge. If any security updates are available, they will be noted on the page when opening the HPDPM Configuration Center. Or you can click the **Check for Update** to check it manually.

- a. Click the **Download** button to download the new package.
- b. After you have successfully downloaded the package, click the **Update** button to update the Console Web Bridge.
- c. Once the update is completed, a notice indicating the Console Web Bridge has been successfully updated will appear.

HP Device Manager - Configuration

hp Device Manager

- About
- Configuration Summary
- General Configuration
- HPDM Server
- HPDM Database
- HPDM Gateway
- HPDM Master Repository Controller
- HPDM HTTPS Repository
- HPDM Console Web Bridge**

HPDM Console Web Bridge

Security Update

Status: Update available [Download](#)

General

Listening Port: 8443

Session timeout in seconds: 300

Minimum memory for each connection in MB: 256

Maximum memory for each connection in MB: 1024

Maximum simultaneous connections: 5

DISCARD APPLY

Downloading HPDM Console Web Bridge packages...

HP Device Manager - Configuration

Device Manager

- About
- Configuration Summary
- General Configuration
- HPDM Server
- HPDM Database
- HPDM Gateway
- HPDM Master Repository Controller
- HPDM HTTPS Repository
- HPDM Console Web Bridge**

HPDM Console Web Bridge

Security Update

Status: Update downloaded Update

General

Listening Port: 8443

Session timeout in seconds: 300

Minimum memory for each connection in MB: 256

Maximum memory for each connection in MB: 1024

Maximum simultaneous connections: 5

The update package has been successfully downloaded. DISCARD APPLY

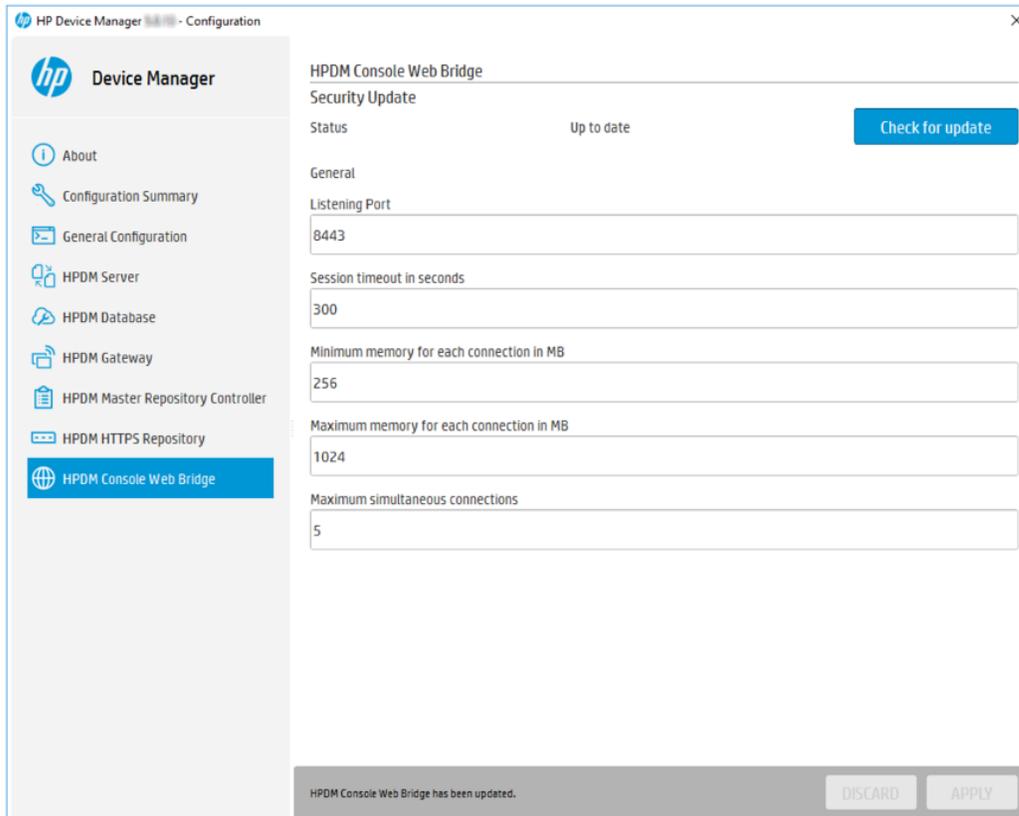
HPDM Console Web Bridge Update

Performing this update will restart the HPDM Console Web Bridge. Do you want to continue?

YES NO

Upgrading HPDM Console Web Bridge...

Progress bar: [Orange segment] [Grey segment]



Listening Port: Indicates the port used by the server and browsers to communicate. The default value is 8443.

Session timeout in seconds Indicates the longest time for inactive session to maintain a connection. The default value is 300.

Minimum memory for each connection in MB: Indicates the minimum heap memory each web console can consume. The default value is 256m

Maximum memory for each connection in MB: Indicates the maximum heap memory each web console can consume. The default value is 1024m.

Maximum simultaneous connections: Indicates how many clients can access web resources at the same time. The default value is 5.

Security Updates

HPDM releases the security updates related to HTTPS Repository and Console Web Bridge services. It includes the Apache, PHP, OpenSSL, and Tomcat 3rd party tools. HPDM will release the security patch to HP Update Center when a new version of them is released.

If the system which running the HPDM can access the internet directly or via a proxy server, you can use the following ways to perform the security updates.

- Using HPDM Configuration Center
Open the shortcut “**HPDM Configuration Center**”. If any security updates are available, they are noted on the page. For details, please refer to [Configuration Center](#).
- Using HTTPS upgrade tool
The HP Device Manger installation provides a command-line utility that can be used to identify and install updates to the HPDM HTTPS Repository and HPDM Web Console Bridge components. This tool HTTPSUpgrade.exe supports the following command-line parameters.

```

Administrator: C:\Windows\System32\cmd.exe
HTTPSUpgrade -a|c|d|h|t|u [component]

-l Use local package to upgrade the HPDM security components.
-d Download the new package.
-u Use downloaded package to upgrade the HPDM security components.
-a Automatically check, download, upgrade the HPDM security components.
-c Check current security version.
-t Test the connection.
-h Help.

component:
  https      Upgrade the security components related to the HPDM HTTPS Repository. This is the default component.
  webconsole Upgrade the security components related to the HPDM Console Web Bridge.

```

Using the HTTPS Upgrade tool can be automated using Windows Task Scheduler. Notice that the -u and -a options will terminate the related service and restart the service in order to complete the update.

If the system which running the HPDM cannot access the internet, please use the following ways to perform the security updates.

- Perform the security updates for HTTPS Repository
 - a. Download the following files on the system which can access the internet.
 - <https://ftp.hp.com/pub/hpdm/dmcatalog.xml>
 - https://ftp.hp.com/pub/hpdm/Patches/HTTPS_Updates/Apache.zip
 - https://ftp.hp.com/pub/hpdm/Patches/HTTPS_Updates/PHP.zip
 - https://ftp.hp.com/pub/hpdm/Patches/HTTPS_Updates/OpenSSL.zip
 - b. Copy them to the system which the HPDM Configuration Center and HTTPS Repository run. These files must be copied to the <HPDM Installed Path>\HP Device Manager\Configuration Center\ directory without any subfolder.
 - c. Open the **Command Prompt**, then go to <HPDM Installed Path>\HP Device Manager\Configuration Center\ directory.
 - d. Run the command '**HTTPSUpgrade.exe -l**' to perform the security updates.
- Perform the security updates for Console Web Bridge
 - a. Download the following files on the system which can access the internet.
 - <https://ftp.hp.com/pub/hpdm/dmcatalog.xml>
 - https://ftp.hp.com/pub/hpdm/Patches/ConsoleWebBridge_Updates/Tomcat.exe
 - b. Copy them to the system which the HPDM Configuration Center and Console Web Bridge run. These files must be copied to the <HPDM Installed Path>\HP Device Manager\Configuration Center\ directory without any subfolder.
 - c. Open the **Command Prompt**, then go to <HPDM Installed Path>\HP Device Manager\Configuration Center\ directory.
 - d. Run the command '**HTTPSUpgrade.exe -l webconsole**' to perform the security updates.

Disaster Recovery

This section provides guidance to help you recover your HPDM components in the event of a system crash or catastrophic failure. The following HPDM components can be recovered:

- HPDM Server
- Database
- Master Repository

Note

This document provides a typical HPDM disaster recovery process. As your HPDM environment may differ, adapt your strategy as required.

General recovery process

The recovery process includes the following steps:

- Recovering the HPDM Server

- Recovering the Master Repository

Figure 11. Typical HPDM distribution diagram

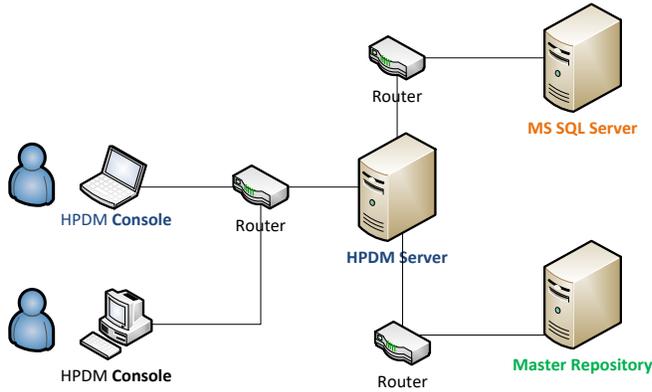
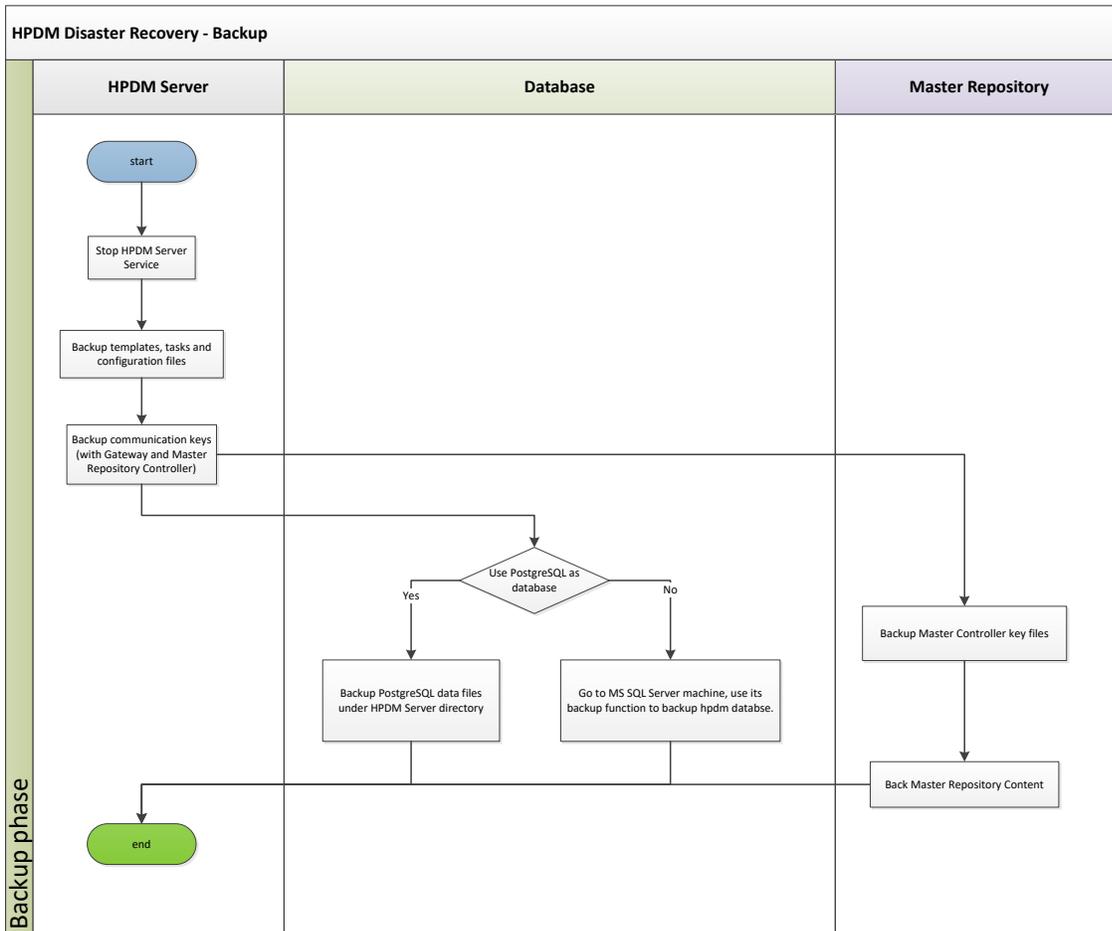


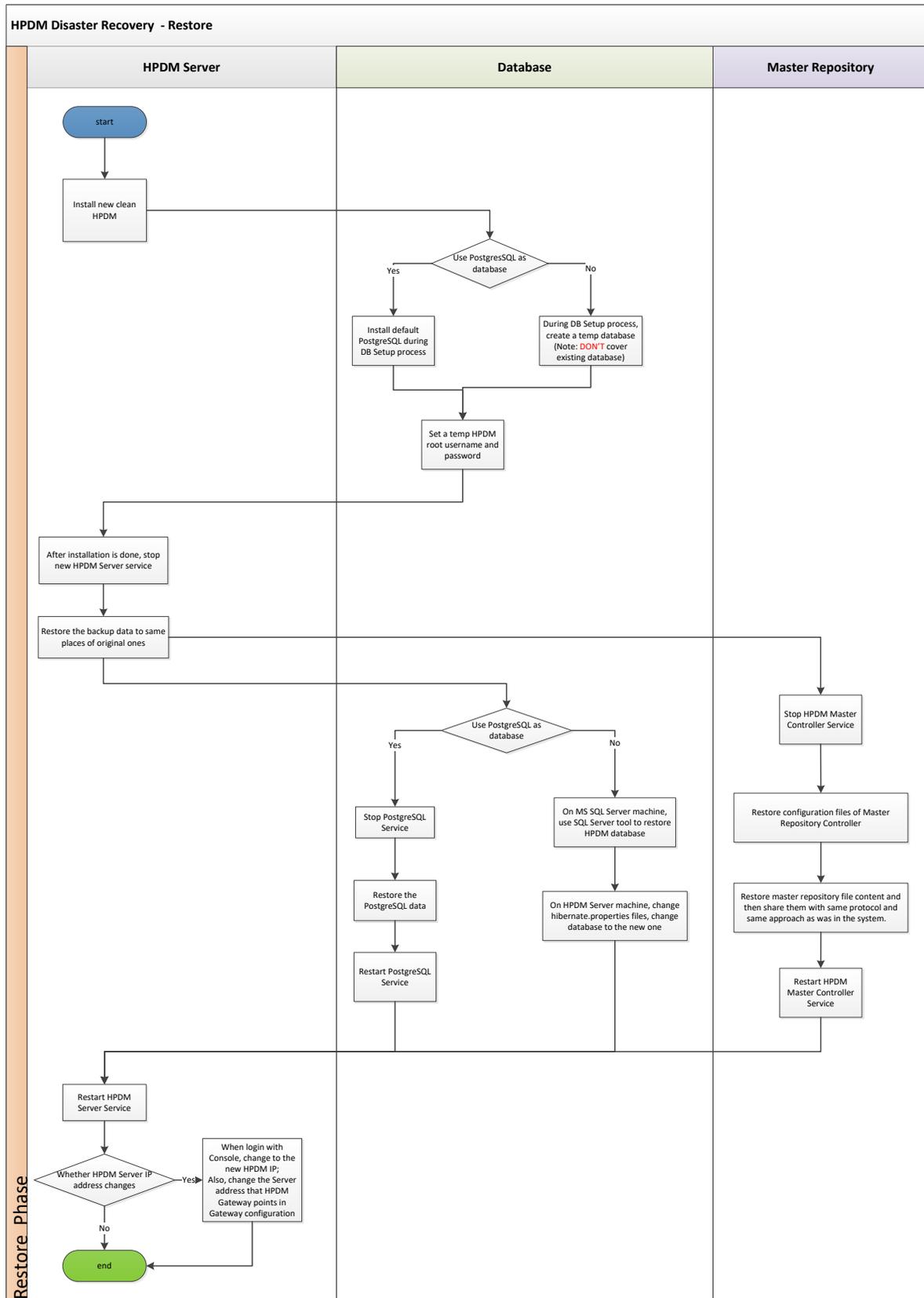
Figure 12. General HPDM disaster recovery workflow (backup phase)



Note

In case of an unpredictable disaster, backup your HPDM data periodically according to your strategy.

Figure 13. General HPDM disaster recovery workflow (restore phase)



Recovering the HPDM Server

The HPDM Server content that you can recover is as follows:

- Templates, tasks, and template plug-ins
- Configuration files and communication keys
- Databases

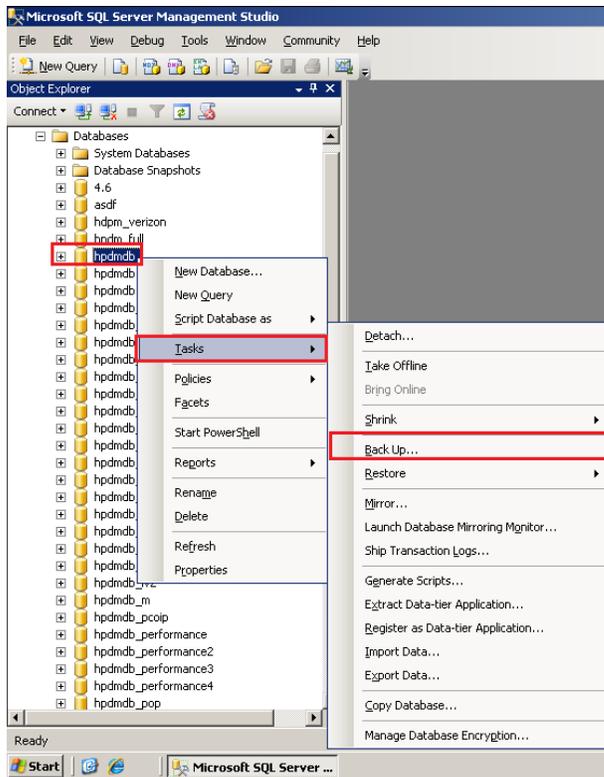
Backing up the data

After the HPDM Server crashes, first back up your data as follows:

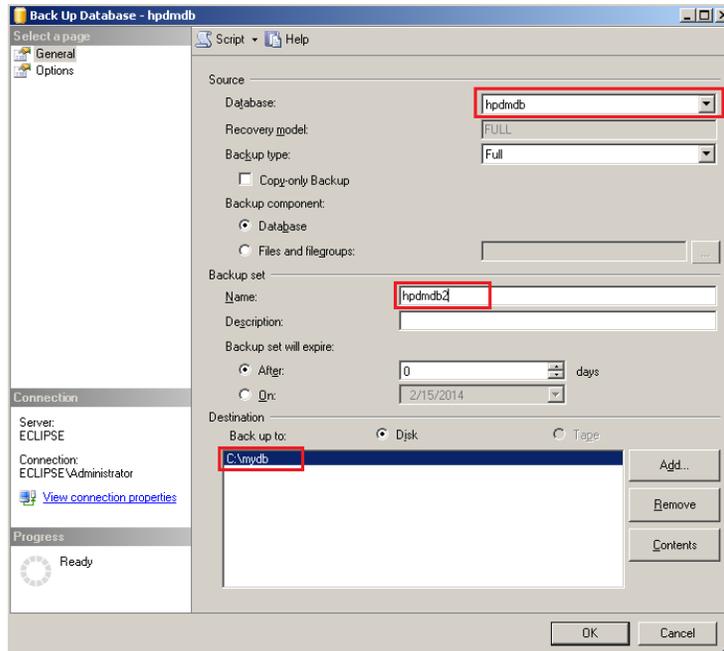
1. Stop the HPDM Server Service.
2. On the HPDM Server installation path, go to <HPDM installation path>\HP Device Manager\Server, and then back up the following directories:
 - a. conf
 - b. template
 - c. task
 - d. report
3. Go to the directory <HPDM installation path>\HP Device Manager\Server\bin, and then back up the following files:
 - a. hpdmcert.key
 - b. Server_Keystore
 - c. hpdmskey.keystore
4. To back up the database, perform the following tasks, depending on which type of database you use with HPDM:
 - a. If you use PostgreSQL as the HPDM database:
 - i. Back up its data to the HPDM Server installation path.
 - ii. Go to the directory <HPDM installation path>\HP Device Manager\Server\pgsql.
 - iii. Back up the data folder.
 - b. If you use MS SQL Server as the HPDM database:
 - i. Back up its data using the MS SQL Server tool.
 - ii. Open **MS SQL Server Management Studio** and use to connect to your source database. Be sure that you have installed this tool.



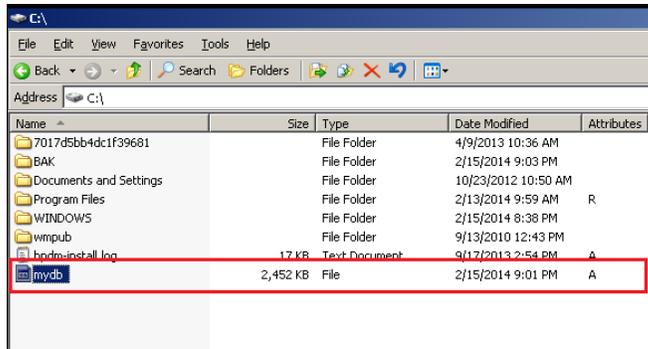
- iii. Select the HPDM database you want to back up, right-click, and then select **Tasks > Back Up**. This example uses the database name hpdmdb.



iv. Specify the source database **hpdmdb**, and create a backup database named **hpdmdb2**. Then, set the destination path **c:\mydb**. Select **OK**.



The backup file is now available in c:\ disk.



Note

PostgreSQL is a database integrated with HPDM, so its data is aligned with HPDM installation path. MS SQL Server provides tool to do backup and restore operations. It is best to use the same version of MS SQL Server; otherwise, the backup might be incompatible.

5. The HPDM Server is now backed up. If you plan to back up the Master Repository, see **Backing up the data**.

Installing the clean HPDM Server

After the HPDM Server is backed up, prepare an HPDM Server environment as follows:

1. Download the same version of the HPDM installer as the one that crashed.

Note

Be sure to use the same version of the HPDM installer; otherwise, it might have a compatibility issue.

2. Install HPDM. If you are reinstalling HPDM on the crashed device, the installer guides you through uninstalling the old version. Or, you can manually uninstall the old version before reinstalling HPDM.
3. During the database setup process, do the following (depending on which type of database you use in HPDM):
 - If you use PostgreSQL as the HPDM database, create a default PostgreSQL database, and then set a temporary HPDM root username and password.
 - If you use MS SQL Server as the HPDM database, create a temporary database directing to the MS SQL Server, and then set a temporary HPDM root username and password.

Note

This database is only for temporary use, so do not write over a useful existing database in the MS SQL Server.

For detailed installation process, please refer to Installation chapter of this guide.

Restoring the data

After you install the HPDM Server in a clean environment, recover your data.

1. Stop the HPDM Server Service.
2. Restore the files that you backed up. (See Backing up the data.) Copy and paste over the original files.
3. To restore the database, do the following (depending on which type of database you use in HPDM):

To restore the database if you use PostgreSQL as the HPDM database:

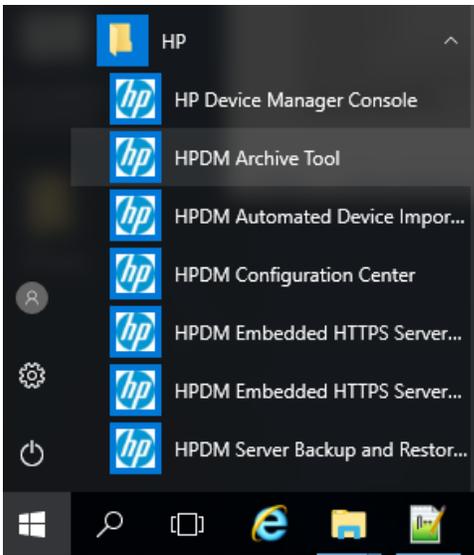
 - a. Stop the HPDM PostgreSQL service.
 - b. Restore the data directory under Server\[pgsql_dir].
 - c. Restart the HPDM PostgreSQL service.

HPDM Archive Tool

HPDM Archive Tool allows you to archive or purge outdated devices, 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.

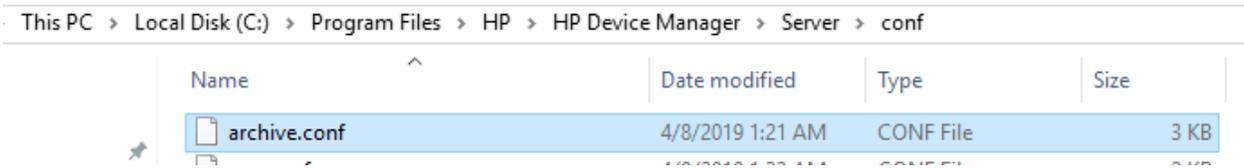
To use HPDM Archive Tool:

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:



- `object`—By default, the **Both** option handles both devices and tasks. Select **Device** to handle devices only. Select **Task** to handle tasks only.
- `device_action_type`—By default, the **Archive** option deletes devices and archives database tables. Select **Delete** to delete tasks without archiving any files.
- `task_action_type`—By default, the **Archive** option deletes tasks and archives database tables and task files. Select **Delete** to delete tasks without archiving any files.
- `device/task_outdate_month`—By default, devices/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.
- `Device/task_outdate_time`—Devices/tasks before this time are outdated. The value must be in the form of YYYY-MM-DD HH:mm:ss. It should be at least 1 day before the current day.
- `Archive folder`—By default, the folder where archived device/task data is stored is `C:\HPDM_Archived`.

```

1 #####
2 # This is the archive configuration file. #
3 #####
4
5
6 # Notice: It is highly recommend to STOP HPDM Server before doing archive job.
7 # Or it might cause some uncertain problems.
8
9
10 # This value defines which object will be handled. The value can be: Both, Device and Task
11 # Both: Both devices with related information and tasks with related information will be handled.
12 # Device: Only devices with related information will be handled.
13 # Task: Only tasks with related information will be handled.
14 # Notice: If value is Both, task with related information will be handled first.
15 object=Both
16
17 # This is the device action type. There are two type: Archive and Delete.
18 # Archive: Devices will be deleted and saved as files. Its related information will be deleted without saving as files.
19 # Delete: Devices and related information will be deleted without saving as files.
20 device_action_type=Archive
21
22 # This is the task action type. There are two type: Archive and Delete.
23 # Archive: Tasks and related information will be deleted and saved as files.
24 # Delete: Tasks and related information will be deleted without saving as files.
25 task_action_type=Archive
26
27 # This value is the default device outdated time, all devices (\ update time) before this time will be archived or deleted.
28 # Notice1: device_outdate_month and device_outdate_time can only use 1 item at one time, please comment one.
29 # Notice2: This value should be at least 1 day before the current date.
30 # Notice3: the format of outdate_time is: YYYY-MM-DD HH:mm:ss
31 #device_outdate_time=2014-09-01 18:00:00
32
33 # This value is the default task outdated time, all task (\ update time) before this time will be archived or deleted.
34 # Notice1: task_outdate_month and task_outdate_time can only use 1 item at one time, please comment one.
35 # Notice2: This value should be at least 1 day before the current date.
36 # Notice3: the format of outdate_time is: YYYY-MM-DD HH:mm:ss
37 #task_outdate_time=2014-09-01 18:00:00
38
39 # This value is default device out date months, all devices (\ update time) before this time will be archived.
40 # Notice: This value is a natural number (1-n).
41 device_outdate_month=3
42
43 # This value is default task out date months, all tasks (\ update time) before this time will be archived.
44 # Notice: This value is a natural number (1-n).
45 task_outdate_month=3
46
47
48 # This value is default path that archived files will be stored
49 # Notice: the format could either c:/folder1/folder2 OR c:\\folder\\folder2
50 archived_folder=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.

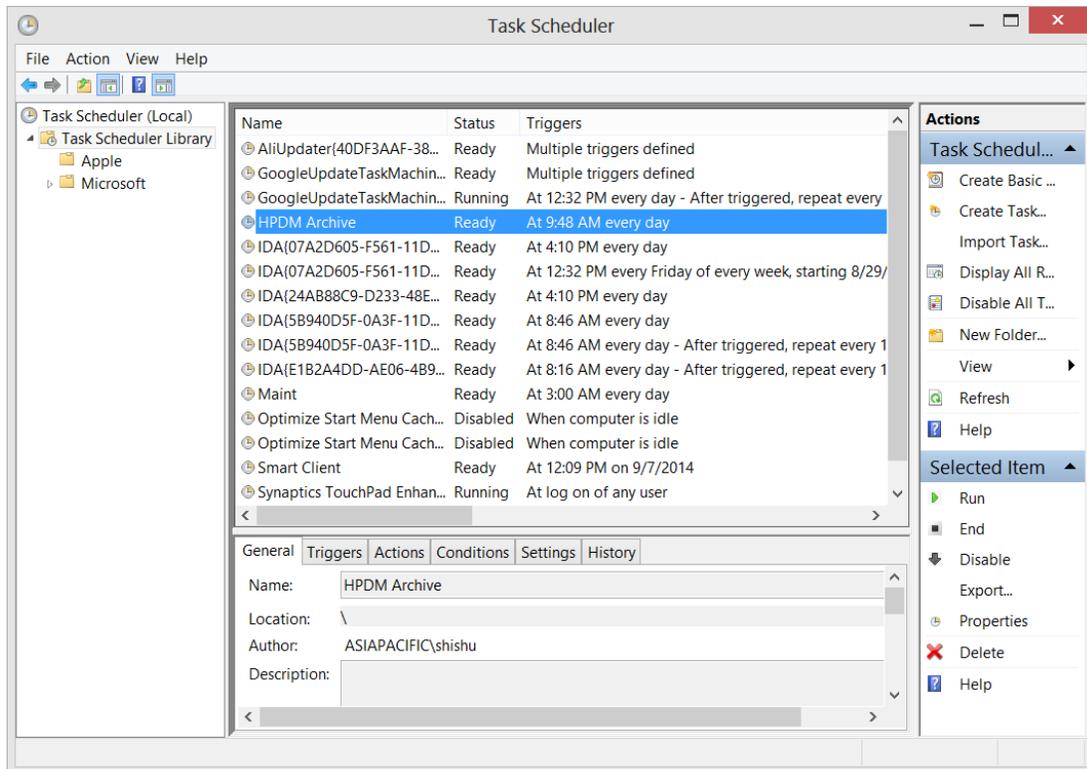
4. Under \Server\logs is the archive tool log: hpdm-archive.log. This shows the process information.

This PC > Local Disk (C:) > Program Files > HP > HP Device Manager > Server > logs

Name	Date modified	Type	Size
wrapperlog	4/8/2019 10:12 AM	File folder	
hpdm-archive.log	10/8/2019 10:09 AM	Text Document	69 KB

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, as in the following example:
 C:\Program Files\HP\HP Device Manager\Server\bin\archive.cmd
 For **Add arguments**, enter the following: -config:archive.conf
4. For **Start in**, enter the full path to \Server\bin, like in the following example:
 C:\Program Files\HP\HP Device Manager\Server\bin
5. Select **Create Basic Task**, and then schedule the task.

Troubleshooting

This section introduces some general information that can help troubleshoot and triage issues in HP Device Manager.

Log files

HPDM Agent log files

Path:

Windows—C:\Windows\xpeagent

HP ThinPro series—/etc/hpdmagent

Files:

- agent.log—The log file for the HPDM Agent main process.
- child.log—The log file for the HPDM Agent child process.
- discovery.log—The log file for detailed information about the HPDM Agent discovering the HPDM Gateway.

HPDM Gateway log files

Path:

The path of the HPDM Gateway log files depends on the HPDM install path, which is specified by users. The default install path is C:\Program Files\HP\HP Device Manager\Gateway.

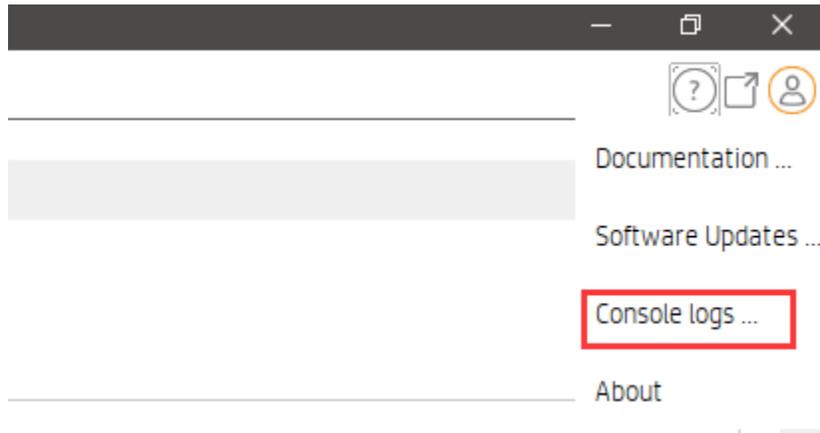
Files:

- Gateway.log and Gateway.log.x (1–30)—The log files for the HPDM Gateway.

HPDM Console log files

Path:

The log files for the HPDM Console are in the %programdata%\HP\HP Device Manager\Console\logs*username* folder, where *username* refers to the name of the user of the console. The %programdata% folder is an accessible folder under the Windows UAC policy. It refers to either C:\ProgramData or C:\Documents and Settings\All Users\Application Data, depending on the operating system. You can also browse that folder in the HPDM Console by selecting **Console logs**.



Files:

- hpdm-console.log and hpdm-console.log.x (1–10, configurable)—The log files for the HPDM Console.

HPDM Server log files

Path

The path of the HPDM Server log files depends on the HPDM install path, which is specified by users. The default install path is either C:\Program Files\HP\HP Device Manager\Server\logs.

Files:

- hpdm-dbsetup.log—The log file for the installation process of the database.
- hpdm-server.log and hpdm-server.log.x (1–10, configurable)—The log files for the HPDM Server.
- hpdmwrapper.date(yyyy-MM-dd, current date).log— The log file for the wrapper to start the HPDM Server, located in the wrapperlog folder.

Master Repository Controller log files

Path:

The path of the Master Repository Controller log files depends on the HPDM install path, which is specified by users. The default install path is either C:\Program Files\HP\HP Device Manager\MasterRepositoryController\log.

Files:

MasterRepositoryController.log and MasterRepositoryController.log.x (1–30)—The log files for the Master Repository Controller.

HPDM installation log files

Path:

The path of the HPDM installation log files is C:\. Each service pack generates another installation log file.

Files:

- HP Device Manager 5.0-install.log—The log file for the installation process of HPDM.
- HP Device Manager Configuration Center-install.log—The log file for the installation process of HPDM Configuration Center.
- HP Device Manager Console-install.log—The log file for the installation process of HPDM Console.
- HP Device Manager HTTPS Repository-install.log—The log file for the installation process of HTTPS Server.
- HP Device Manager Gateway-install.log—The log file for the installation process of HPDM Gateway.

- HP Device Manager Master Repository Controller-install.log—The log file for the installation process of HPDM Master Repository Controller.
- HP Device Manager Server-install.log—The log file for the installation process of HPDM Server.

Collecting useful log information

HPDM Agent

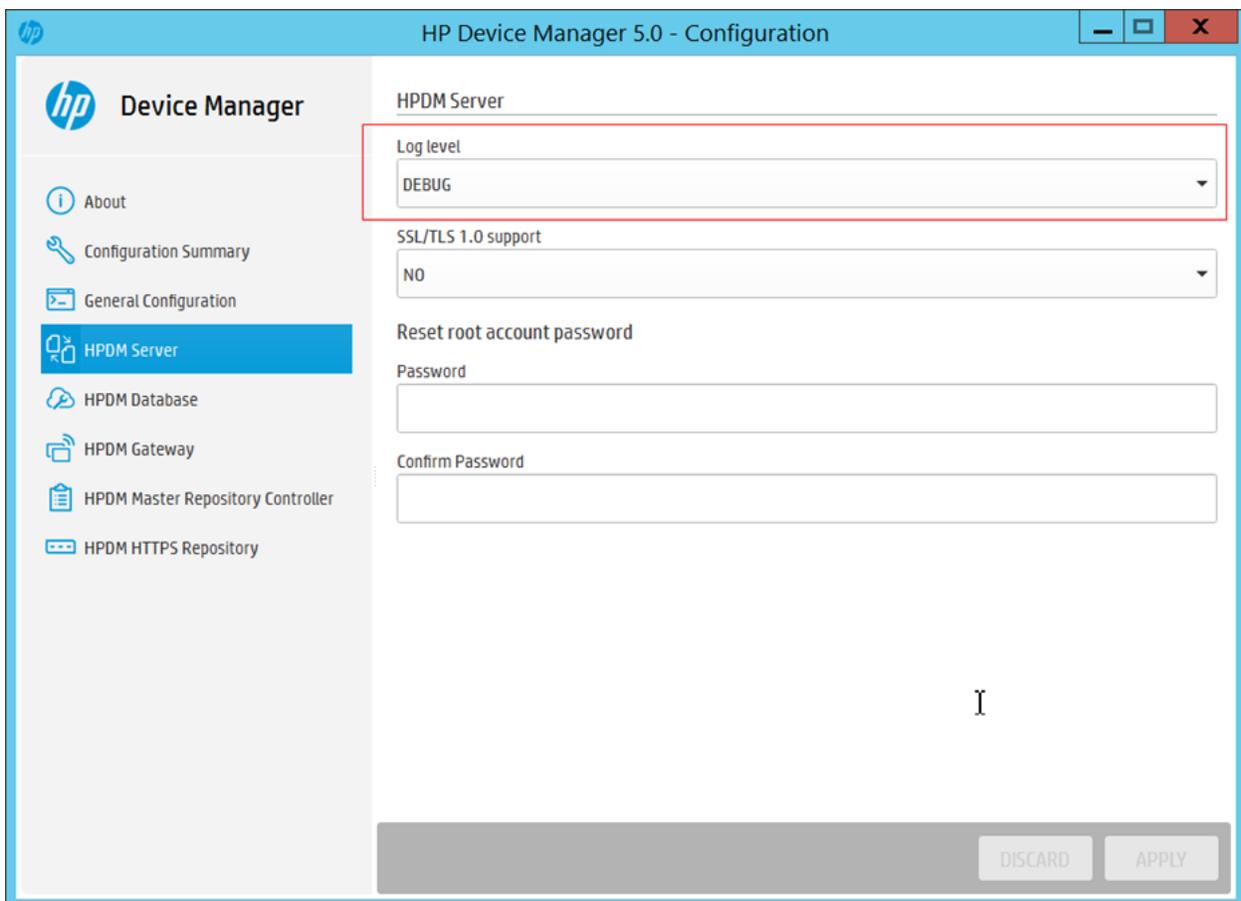
Upload the HPDM Agent logs files with a Capture File task or copy them locally.

The default log level of the HPDM Agent is Error. If your issue can be reproduced, set the **Log Level** to **Information** with a Configure Agent task. Then attempt to reproduce the issue. Upload the HPDM Agent logs files with a Capture File task or copy them locally.

HPDM Gateway

The default log level of the HPDM Gateway log files is **Trace**. You do not need to change the log level. If you want to change the log level of the gateway, open the Configuration Center, select the HPDM Gateway, and you can change the gateway log level. Copy the HPDM Gateway logs to another folder and compress them to a package.

Figure 22. Modify gateway log level through the Configuration Center



HPDM Console

The default log level of the HPDM Console log files is **Warn**. Only Warn and Error logs are printed. Copy the HPDM Console logs if you see the keyword **Exception**, and then compress them to a package.

If a task fails, you can select the target device to find useful information. Right click the target device to Export Task Log.

Figure 23. Failed task

Device Task View - 13_7E_1628_image

Information

Task Name: 13_7E_1628_image
Task ID: 00000178 OS Family: HP ThinPro 7
Sender: root Sequence: No

Parameters

Valid Time: 1440 minute(s) Write Filter Policy: Execute & Commit
Batch amount: 2 General Batch Interval: 10 minute(s)
Execution Timeout: 30 minute(s) WOL Before Task: No
Cached Updates: No Task Deferment: No
Exclude Working Hours: No HTTPS Repository Speed Limits: No
Upload Limit: No Download Limit: No

Task Status

Device Name	Status	Error Code	Action	End Time
HP-480FCF8B518B	Failed	311	Continue	19-05-

Select target device

Task Log

Device Name: HP-480FCF8B518B
Device ID: 480FCF8B518B
IP Address: 10.0.60.130

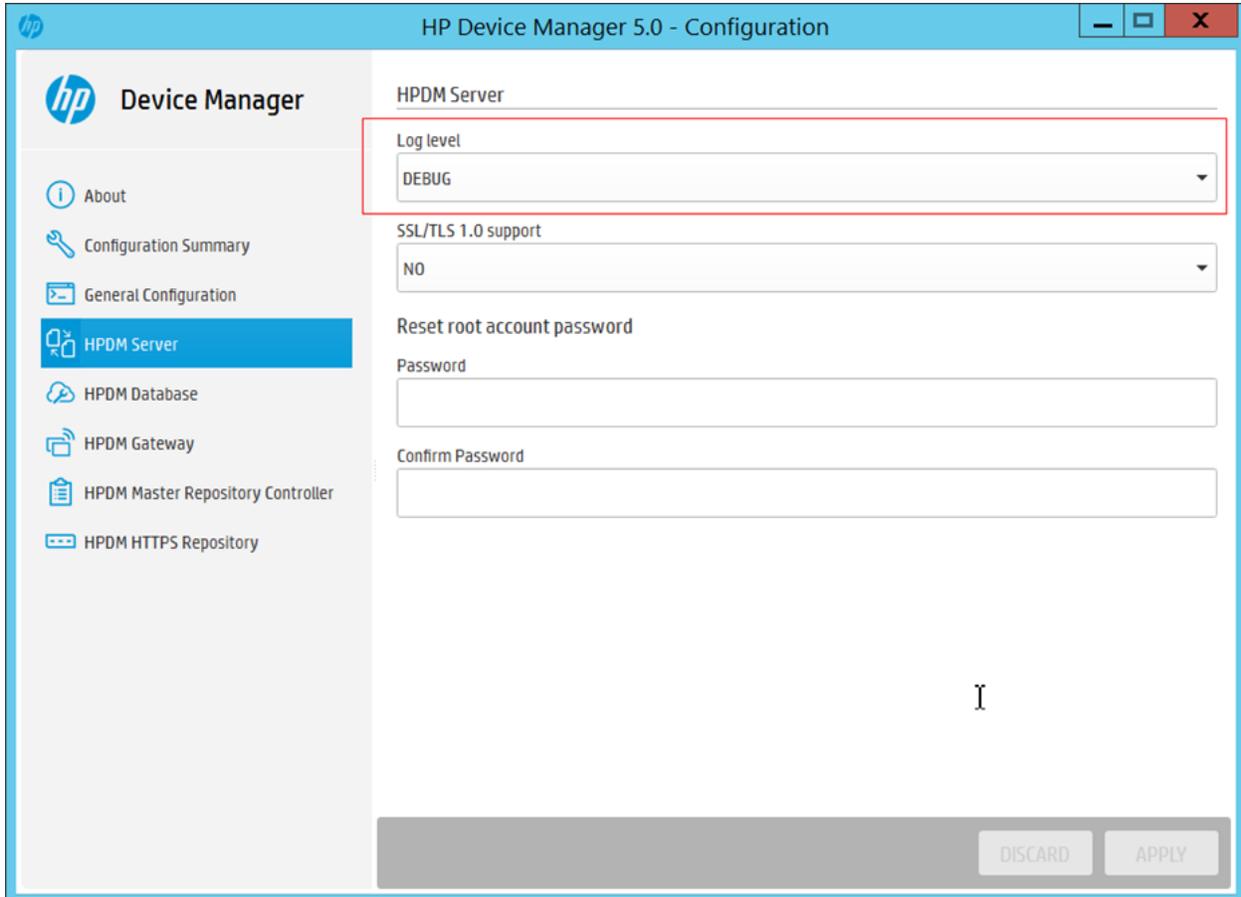
Log Time	Log
2019-05-16 09:25:33	Map repository to: Master Repository
2019-05-16 09:25:38	Successfully sent task to the HPDM Gateway
2019-05-16 09:26:45	Task has been retrieved by the Agent
2019-05-16 09:26:50	Failed to download 13_7E_1628_image.ibr from /Repository/Images/13_7E_1628_image.
2019-05-16 09:26:50	Failed to execute PXEDeploy task. ErrorCode: 311, Error Detail: Failure downloading image file from FTP server., Error Info: Not find SMB protocol, for WES need SMB
2019-05-16 09:26:50	Failed to execute PXETask task. ErrorCode: 311, Error Detail: Failure downloading image file from FTP server.

Display error details for further investigation

HPDM Server

The default log level of the HPDM Server is Warn. Only Warn and Error logs will be printed. If you have a server issue, open **server.conf**, change **hpdm.log.level** to **DEBUG**. Or modify the log level through the Configuration Center, select **HPDM Server**, change **Log level** to **DEBUG**, select **APPLY** to save the settings.

Figure 24. Modify server log level through the Configuration Center



Set the following flags to true:

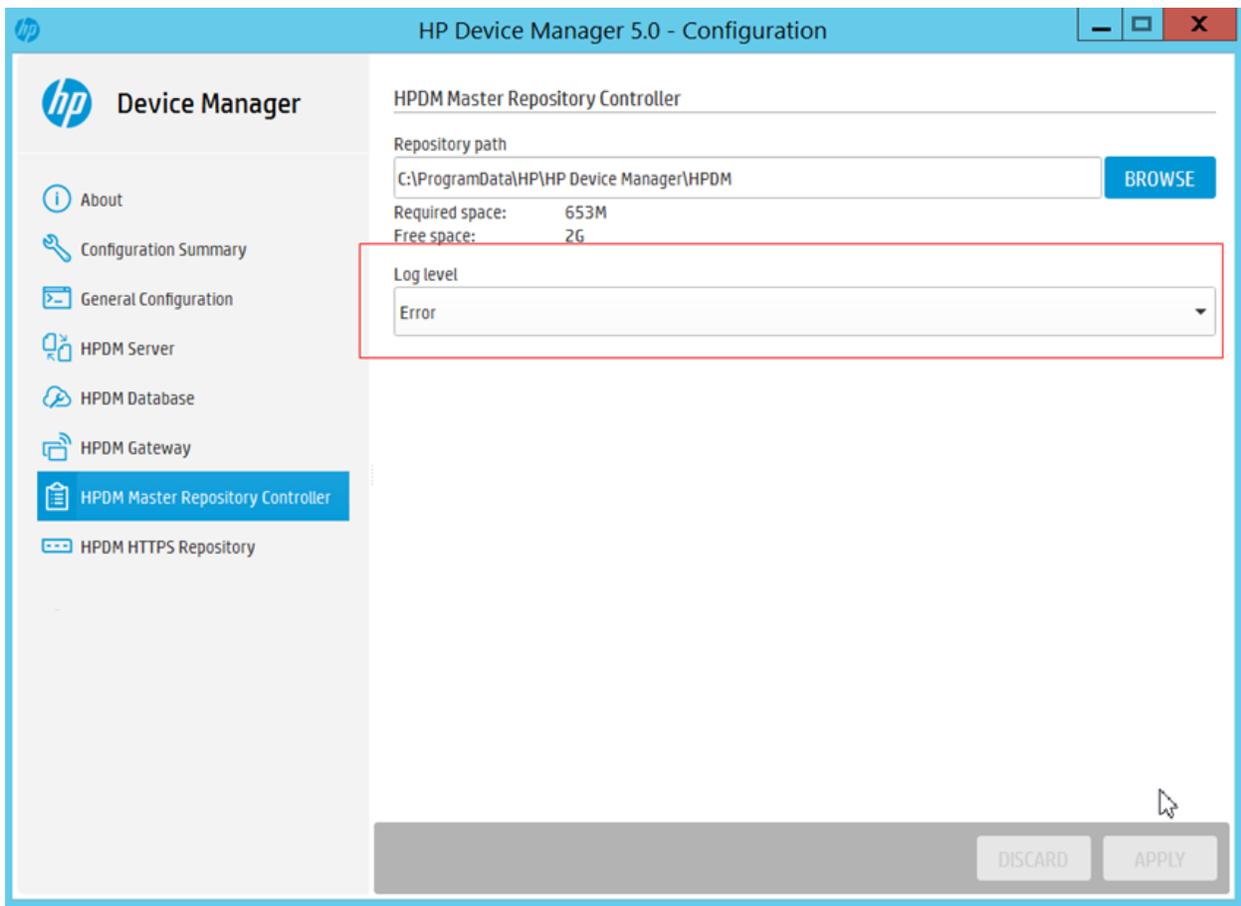
- hpdm.log.gateway
- hpdm.log.console
- hpdm.log.task
- hpdm.log.masterController

After reproducing the issue, copy the HPDM Server logs to another folder and compress them to a package.

Master Repository Controller

The default log level of HPDM Master Repository Controller is **Error**. Only the error log is printed. If your issue is related to the Master Repository Controller, open **Controller.conf**, and change **LogLevel** to **2**. Or open the Configuration Center, select **HPDM Master Repository**, change **Log level** to **Info**, and then select **APPLY** to save the settings. Restart the Master Repository Controller. After reproducing the issue, copy the HPDM Master Repository Controller logs to another folder and compress them to a package.

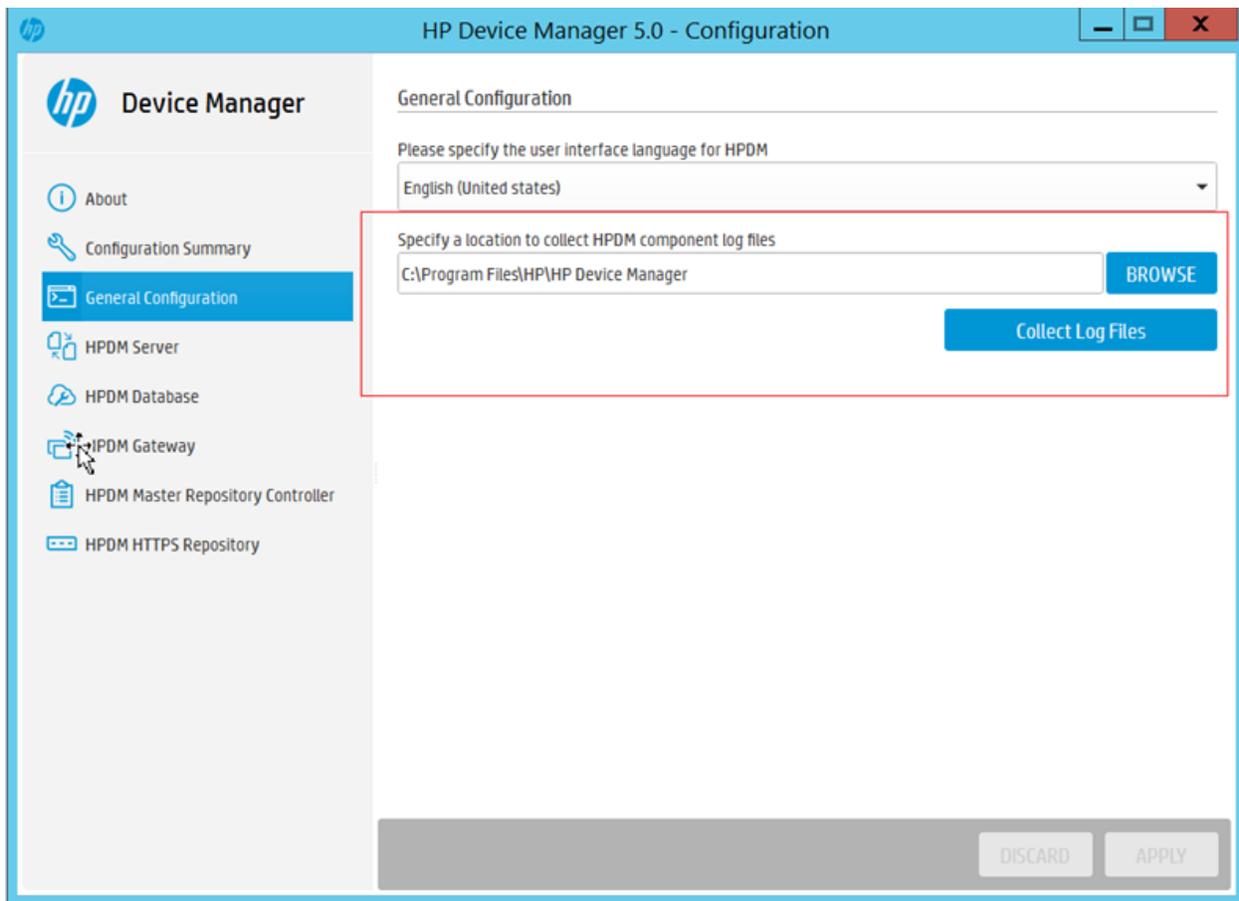
Figure 25. Modify Master Repository log level through the Configuration Center



Collect all HPDM component logs

Open the Configuration Center, select **General Configuration**, select **BROWSE** to select the directory where you want to output the log, and then select **Collect Log Files** button to retrieve the logs. The local installed component logs are saved to the directory you have selected.

Figure 26. Get all HPDM component logs



General Troubleshooting

1. The HPDM components (HPDM Console, HPDM Server, HPDM Gateway, HPDM Agent, and Master Repository Controller) are not communicating correctly.

This problem is usually caused by the firewall. Often, you can ping the devices but HPDM does not work. See the **Port Usage** section for instructions to add rules or exceptions to the firewall.

HPDM also includes a port check tool. The path is <HPDM root folder>\Configuration Center\HPDMPortCheck. To use the tool, in the command prompt, execute HPDMProtCheck.exe without parameters. You also can find this tool usage at the Network issues section.

2. The HPDM Agent failed to download files.

Verify that the repository settings are correct.

Use a third-party tool to check whether the devices can access and download files from repositories. For Windows, use Windows Explorer. For HP ThinPro, use wget.

If you are using a hostname or FQDN as a repository's address, try using the IP address. Some devices might not be able to get the IP address from the hostname or FQDN. You can ping the hostname or the FQDN from the device to verify whether it is a HPDM issue.

For more details, see the **Gateway & Repository** section.

3. A Windows HPDM Agent can perform an Update Agent task but cannot image.

Win10/11 IoT imaging solution needs a shared folder. Be sure the shared folder is set correctly in the Repository settings.

4. The HPDM Gateway cannot connect to the HPDM Server, or the HPDM Gateway does not accept the tasks from the HPDM Server.

Be sure that the server address of the HPDM Gateway points to the HPDM Server. Verify that the correct NIC for the HPDM Gateway is selected, and then restart the HPDM Gateway.

Be sure that if **Manage control HPDM Gateway access** is selected in the **HPDM Gateway access control** dialog, **HPDM Gateway is Acknowledged** is also selected.

5. A repository cannot be accessed by an HPDM Agent, but it can be accessed by a FileZilla client.

Be sure that the address you used in the repository is exactly same as the one in the FileZilla client. If your environment is in DMZ, see the **DMZ considerations** section.

6. A Windows software package cannot be installed correctly by HPDM.

The HPDM Agent runs as a service and its TEMP path is Z:\temp, by default. However, partition Z might not have enough space for some big software packages.

To change the partition used, HP recommends using a Script subtask in the File and Registry template. Enter these lines before using the task:

- set TEMP="C:\temp"
- set TMP="C:\temp"
- <install software command line>

Set a different folder than C:\temp as the TEMP path.

Error Codes

Prior to HPDM 4.5, error codes started with 1400 and were eight digits long. The current HPDM error codes provide a combination of the component and the category of the error.

Table 41. Error code matrix, part one

	HPDM Agent	DMMC (HPDM Agent Library)	UCT (HPDM Agent Library)	DMAC (HPDM Agent Library)	WES7DISP (HPDM Agent Library)	MINILINUX
Network connection	1064960	1130496	1196032	1261568	1327104	1392640
Disk I/O	1065984	1131520	1197056	1262592	1328128	1393664
Memory error	1067008	1132544	1198080	1263616	1329152	1394688
Remote file/dir operation	1068032	1133568	1199104	1264640	1330176	1395712
File integrity	1069056	1134592	1200128	1265664	1331200	1396736
Credential	1070080	1135616	1201152	1266688	1332224	1397760
Other FTP-related error	1071104	1136640	1202176	1267712	1333248	1398784
Write Filter error	1072128	1137664	1203200	1268736	1334272	1399808
Unmanageable device	1073152	1138688	1204224	1269760	1335296	1400832
Unsupported task	1074176	1139712	1205248	1270784	1336320	1401856
Incompatible platform	1075200	1140736	1206272	1271808	1337344	1402880
Message syntax error	1076224	1141760	1207296	1272832	1338368	1403904
Message semantic error	1077248	1142784	1208320	1273856	1339392	1404928
Registry error	1078272	1143808	1209344	1274880	1340416	1405952
Command return non-zero	1079296	1144832	1210368	1275904	1341440	1406976
Thread/process error	1080320	1145856	1211392	1276928	1342464	1408000
Task expire	1081344	1146880	1212416	1277952	1343488	1409024
HPDM task process crash	1082368	1147904	1213440	1278976	1344512	1410048

Other HPDM workflow error	1083392	1148928	1214464	1280000	1345536	1411072
Other API/sys call error	1084416	1149952	1215488	1281024	1346560	1412096

Table 42. Error code matrix, part two

	Windows PE	HPDM Gateway	HPDM Server	HPDM Console	Master Repository Controller
Network connection	1458176	2113536	3162112	4210688	5259264
Disk I/O	1459200	2114560	3163136	4211712	5260288
Memory error	1460224	2115584	3164160	4212736	5261312
Remote file/dir operation	1461248	2116608	3165184	4213760	5262336
File integrity	1462272	2117632	3166208	4214784	5263360
Credential	1463296	2118656	3167232	4215808	5264384
Other FTP-related error	1464320	2119680	3168256	4216832	5265408
Write Filter error	1465344	2120704	3169280	4217856	5266432
Unmanageable device	1466368	2121728	3170304	4218880	5267456
Unsupported task	1467392	2122752	3171328	4219904	5268480
Incompatible platform	1468416	2123776	3172352	4220928	5269504
Message syntax error	1469440	2124800	3173376	4221952	5270528
Message semantic error	1470464	2125824	3174400	4222976	5271552
Registry error	1471488	2126848	3175424	4224000	5272576
Command return non-zero	1472512	2127872	3176448	4225024	5273600
Thread/process error	1473536	2128896	3177472	4226048	5274624
Task expire	1474560	2129920	3178496	4227072	5275648
HPDM task process crash	1475584	2130944	3179520	4228096	5276672
Other HPDM workflow error	1476608	2131968	3180544	4229120	5277696
Other API/sys call error	1477632	2132992	3181568	4230144	5278720

Database Issues

This section provides background on the HPDM database and help customer to troubleshoot the database-related problems.

HPDM can be used with two types of database: Microsoft® (MS) SQL Server and PostgreSQL. To use MS SQL Server, you must install and configure it yourself. PostgreSQL is an open-source database that is bundled with the HPDM Server. You do not need to install or configure it yourself.

Using MS SQL Server

MS SQL Server can be used with one of two authentication types: SQL Server Authentication or Windows Authentication. Both authentication types are supported by HPDM. SQL Server Authentication has an inner security mechanism that is easy to use. Windows Authentication needs the Windows operating system security mechanism.

The minimum privilege required depends on the status of the database. They are listed as below:

Table 51:

Status of database	Minimum role required
Not exist	dbcreator
Legacy schema	db_owner

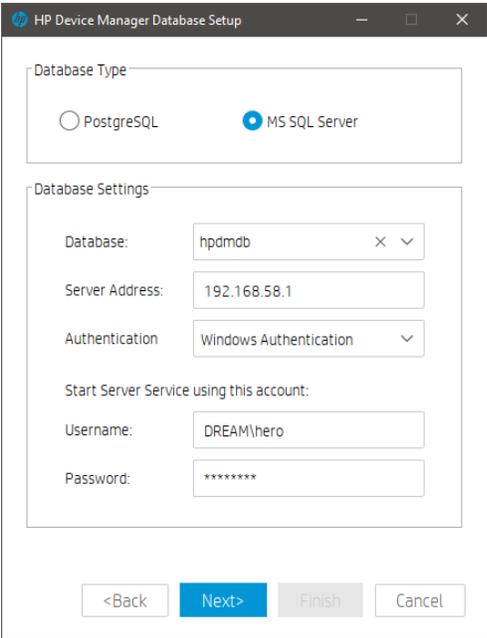
Up to date	db_datareader + db_datawriter + db_ddladmin
------------	---

To configure MS SQL Server using Windows Authentication:

1. Log on to a Windows domain account and assign it a server-level role according to table 51. Below screenshot is an example with **dbcreator** which has the only privileges to create any database in Microsoft SQL Server.

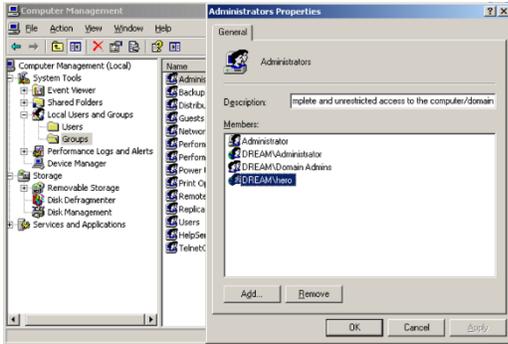


2. Open the **HP Device Manager Database Setup** dialog. Select **MS SQL Server** under **Database Type** and select **Windows Authentication** under **Authentication**.



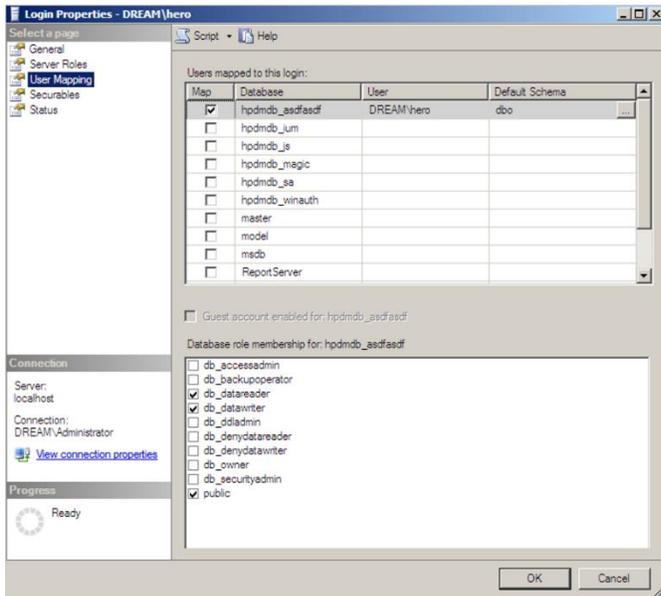
3. Under **Start Server Service using this account**, enter a Windows account username and password. In order to have privileges to access the created database, you can either enter the same windows account or enter a different account with required database-level roles as seen in table 51. If a different account is entered, it should satisfy the following requirements:

- In the Windows operating system, the account must be in the Administrators group.



– In MS SQL Server, the account is assigned sufficient roles as seen in table 51.

During the boot of the server service, the database is checked, and then the database schema is upgraded if it is not the latest version. Use either the account with higher privileges, which has the database-level roles of **db_datareader**, **db_datawriter** and **db_ddladmin**, for the first boot of the server service, or upgrade the database to the latest version by running **HP Device Manager Database Setup** with the account in step 2, which created the database and is assigned **db_owner**,



Using PostgreSQL

PostgreSQL is automatically installed and runs in the background on the same device as the HPDM Server. Because there is only one PostgreSQL database instance, you do not need to configure the database.

Troubleshooting steps

Migrate Database

Migrate Database is a function during the HPDM installation process that does two things.

- It updates the source database schema to the current schema if there are any changes.
- It lets you migrate the source database to another place. For example, you can migrate from PostgreSQL to MS SQL Server, from MS SQL Server to PostgreSQL, or from MS SQL Server to another MS SQL Server.

Backup and Restore Tool

The Backup and Restore Tool is a standalone tool that helps back up the current HPDM database, templates, tasks, and the configuration files. It can restore data to the same version of HPDM and the same database type only. For example, if you back up a MS SQL Server database, you can only restore it to a MS SQL Server database. HP does not recommend restoring the data to different versions of MS SQL Server.

Additional resources

HPDM Database Schema

For HPDM database schema, see **Appendix B**.

Microsoft SQL Server

For more information on Microsoft SQL Server, go to <http://msdn.microsoft.com/en-us/sqlserver/default>.

PostgreSQL

For more information on PostgreSQL, go to <http://www.postgresql.org/>.

Network Issues

HPDM Port Check Tool

Windows Configuration

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 Console side: <HPDM root folder>\Configuration Center\HPDMPortCheck\HPDMPortCheck.exe

HPDM Agent windows side: C:\windows\xpeagent\HPDMPortCheck\HPDMPortCheck.exe

To check a 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 device, copy the folder to that device.

The command line syntax is as follows: `HPDMPortCheck <target> [<flags>]`

The target can be 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.

Table 44. Valid flags

Flag	Description
-a	Check the port for HPDM Agent (40001)
-g	Check the port for HPDM Gateway (40003)
-s	Check the port 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)

Linux configuration

Only HPDM Agent is available within the Linux system.

The tool is located at the following path: /usr/sbin/hpdmportcheck

Use the Thin Pro command prompt entering into the path of the tool, run this tool and the same usage with the Windows package.

Domain name resolution

Note:

On Windows, if you set multiple gateways using multiple DNS service records, HPDM Agent does not properly follow the priority order that you set.

1. Verify the network information (including the IPv4 address and domains) of HPDM Agent.
2. Use the following command to make sure the device can get DNS service records (replace DomainName with your domain name):

- Windows: `nslookup -timeout=30 -type=SRV _hpdm-gateway._tcp.DomainName.com`
- HP ThinPro: `host -t SRV _hpdm-gateway._tcp.DomainName.com`

Setting a static domain name in Windows:

1. Open the Network Connections dialog via Control Panel or the network notification icon.
2. Right-click the network adapter, and then select **Properties**.
3. Select the **Internet Protocol Version 4 (TCP/IPv4)** item, and then select **Properties**.
4. Select **Advanced**.
5. Select **DNS**, select **Append these DNS suffixes (in order)**, and then add the DNS domain to the list.

Repositories

Common repository problems include the HPDM Server cannot connect to HPDM Master Repository Controller and the device fails to connect the repository. Before troubleshooting, please be sure that the settings of file server (HTTPS,FTP/FTPS, SFTP server, or Shared Folder) are correct.

Connectivity of the repository

Go to the device that fails to connect the repository, then follow below steps to troubleshoot on this device.

- Verify that the devices on the network can connect to the repository through the FTP/FTPS, SFTP, or Shared Folder and can read/write files and create/delete folders.

Note

HTTPS does not support access through third-party clients such as Internet Explorer; however, you can verify access using the following command: telnet host port.

If using FQDN of the repository as its address, please change it to IP address and try again.

- For the Shared Folder on a Linux device, use the following command to check access to the repository. If you do not have a domain, remove the relative parameter.

```
mount -t cifs -o username=XXX,password=XXX,domain=XXX //192.168.1.101/HPDM
/tmp/HPDMSamba
```

- Verify that the FTP access is enabled if you have any devices with an older version of HPDM, because they might not work with any new repositories until the HPDM Agent updates.
- Verify that the HPDM Console can connect to the Master Repository through the HTTPS, FTP/FTPS, SFTP, or Shared Folder and can read and write files. Use the **Test** button in the Repository Configuration Wizard.
- Check if the following firewall ports are opened:
 - 20 and 21: FTP server
 - 22: SFTP server
 - 443: HTTPS server
 - 990: FTPS server
 - 137: NetBIOS Name Service
 - 138: NetBIOS Datagram Service
 - 139: NetBIOS Session Service

Log level setting of the Master Repository Controller

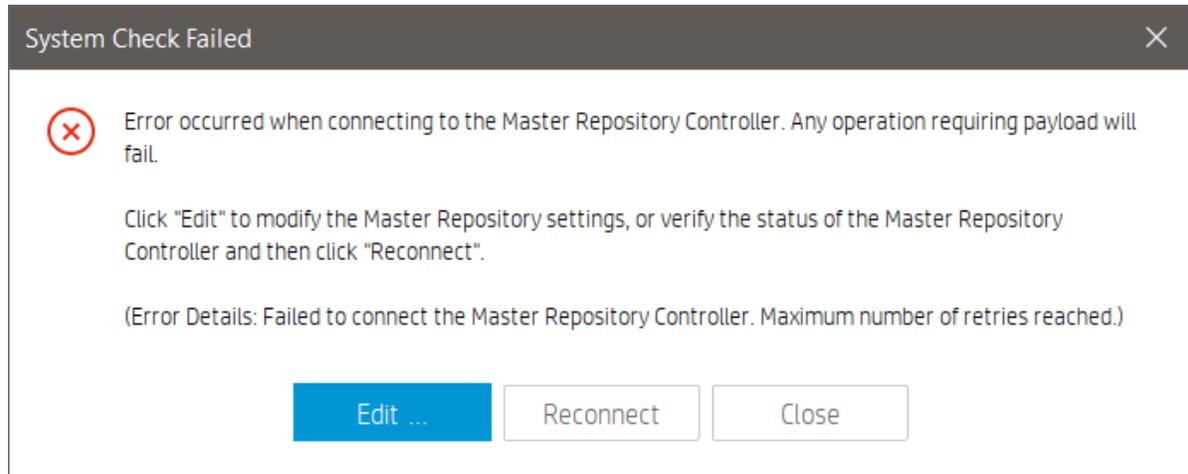
Use Configuration Center to modify the Master Repository Controller log level to get detailed log information for debugging. For more details, see the Configuration Center of this Guide.

After changing the log level, restart the Master Repository Controller service for the changes to take effect.

Connection between the HPDM Server and the Master Repository Controller

- Check that the HPDM Server can connect to the Master Repository Controller.
If the HPDM Server cannot connect to the Master Repository Controller after you have configured the Master Repository information using the Master Repository Editor, the following error dialog appears. Verify that the server address for the Master Repository is correct and that the 40012 port is allowed through the firewall. If the server address is not correct, select the **Edit** button in the error dialog, enter the correct server address, and then try to connect. If the port is not allowed through the firewall, change your firewall's permissions, and then select the **Reconnect** button in the error dialog.

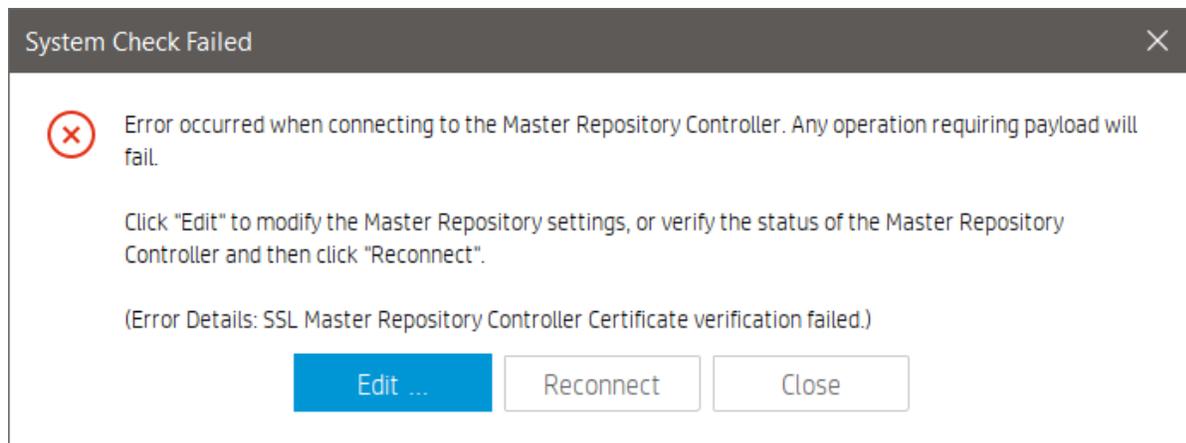
Figure 10. System Check Failed dialog



- Make sure that the connection passes the authentication.
SSL authenticates the connection between the HPDM Server and the Master Repository Controller. After the configuration finishes successfully for the first time, an authentication certificate and private key are generated between the HPDM Server and the Master Repository Controller.
 - a. Go to the installation folder of the HPDM Server and find the keystore file `hpdmskey.keystore` in the folder `InstallerFolder/Server/bin`. This file stores the HPDM Server's private key, the HPDM Server's certificate, and the Master Repository's certificate.
 - b. Go to the installation folder of the Master Repository Controller and find the following three files:
 - `Controller.key`—Master Repository Controller's private key
 - `Controller.crt`—Master Repository Controller's certificate
 - `Client.crt`—HPDM Server's certificate

The Master Repository Controller refuses any connection requests that do not include the authentication certificate. Also, the HPDM Server refuses the Master Repository Controller if it does not pass the authentication. If the authentication fails, the following message appears.

Figure 11. System Check Failed dialog



HPDM supports only one server and only one Master Repository Controller in the system. If you use another server or Master Repository Controller, the authentication fails.

Use the following steps to delete the authentication file and reset the authentication between the HPDM Server and Master Repository Controller. The new authentication file is created when the HPDM Server and the Master Repository Controller connect for the first time. Before you reset the authentication, make sure that there is only one HPDM Server and only one Master

Repository Controller in your system. Also, make sure that the system clocks are same if the HPDM Server and the Master Repository Controller are installed on different machines. Otherwise, the authentication might fail.

1. Stop the HPDM Server and Master Repository Controller. You can stop Master Repository Controller in the Services Control Panel.
2. Delete all authentication files.
3. Start the Master Repository Controller. You can start the Master Repository Controller in the Services Control Panel.
4. Start the HPDM Server.
5. Open the HPDM Console again. The system now authenticates successfully.

Note

If you want to use the customized certificate, please refer to Appendix E: Configuring HPDM Master Repository Controller Certificate.

Wake on LAN

This section is intended to demonstrate how to troubleshoot issues that might occur while attempting a Wake-on-LAN (WOL) task on thin clients.

WOL types

HPDM supports two types of WOL:

- **Subnet-directed WOL**—The HPDM Gateway broadcasts the WOL packet to the subnet address of devices on port 7.
- **Buddy WOL**—This sub-feature has a condition that the target subnet must have an online device other than the target device. The HPDM Gateway sends the WOL task to the online device, and the device broadcasts the WOL packet in the subnet on port 40000.

Users do not need to assign the online devices for Buddy WOL; the HPDM Gateway detects them automatically.

Behavior

For devices that are in the same subnet as the HPDM Gateway, the HPDM Gateway reports success to the HPDM Server immediately after it sends subnet-directed WOL.

For devices that are not in the same subnet as the HPDM Gateway, the HPDM Gateway sends both subnet-directed WOL and Buddy WOL. The HPDM Gateway only reports success when it receives the success report from the online device (Buddy WOL is successful) because the subnet-directed broadcasts are often disabled in routers.

Device configuration

- Make sure that the WOL option is enabled in the BIOS.
- Make sure that the device can be woken up via WOL. Some devices do not support WOL because of limitations of the hardware or BIOS. See **Third-party tools for WOL** to verify if the device can be woken up.

Note

A BIOS update might affect WOL capability because of either a BIOS defect or the WOL option being reset to disabled.

- If the thin client is powered off forcibly, it might not be able to wake up via WOL.
- WOL tasks fail on Windows devices that are in an S3 power state (sleep).

To enable WOL from an S3 power state, open the Windows Device Manager on the thin client and navigate to the **Power Management** tab of the network adapter properties. Change the settings to enable **Allow this device to wake the computer**, accept the changes.

If UWF/HPWF is enabled, select **Disable UWF/HPWF** and reboot. Then, do the above changes, select **Enable UWF/HPWF**, and then reboot again. The display on the device will remain off until local input (keyboard/mouse) is received, but it can be pinged and otherwise managed. Also note that HPDM does not show any indication of suspended devices.

Network connections

Make sure that the network connections are okay; for example, check that the network cable is plugged in and the NIC lights are on.

Network topology

- If the thin client is in the same subnet as the HPDM Gateway, use a third-party WOL tool to verify if the thin client is in a state that can be woken (see Section: Third-party tools for WOL).

- If the thin client is in a different subnet than the HPDM Gateway, do the following:
 - Check if subnet-directed broadcasts are disabled on intervening routers. If yes, it must rely on Buddy WOL.
 - Check if there is an online thin client in the same subnet as the target thin clients.
- If there is no online thin client, then the HPDM Gateway cannot wake up the thin client. This is by design.
- If there is at least one online thin client other than the target, check to see if the online thin client is behind NAT. If it is, check to see if it receives a WOL task by checking agent.log/child.log. If it is not, wait, because there is a delay based on the HPDM Agent pull interval on the thin client. Also, confirm that the expiration time is longer than the interval value.

If the online thin client is not behind NAT, check to see if the HPDM Gateway sends a WOL task by checking Gateway.log.

- In any situation, use a WOL tool to verify if the thin client is in a state that can be woken (see **Appendix A: Third-party tools for WOL**). If not, HPDM cannot wake it up.

Third-party tools for WOL

wolcmd.exe is a command-line WOL tool available at <http://www.depicus.com/wake-on-lan/wake-on-lan-cmd.aspx>.

The syntax is as follows:

```
wolcmd.exe [mac address] [ip address] [subnet mask] [port number]
```

1. Open a command window.
2. Execute the following command: `Wolcmd.exe AABBCCDDEEFF 192.168.1.100 255.255.255.0`

The default port number is 7.

3. Check whether the thin client with the MAC address AA-BB-CC-DD-EE-FF is woken up.

WakeOnLanGui.exe is a GUI WOL tool available at <http://www.depicus.com/wake-on-lan/wake-on-lan-gui.aspx>.

PXE-Based Imaging

- Verify that the device supports imaging using PXE (see the HPDM release notes).
- Verify that all HPDM components are ~~4.7 SP6~~ 5.0 or newer.
- Verify that the device is set to boot from PXE (see **Configuring a device 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 the **Wake On LAN** setting in the BIOS is set to Boot to Network (the name depends on the device's BIOS version).

LDAP Integration

Most LDAP related issues stem from misconfiguration, use the items below to verify connectivity and configuration of the LDAP service within your environment.

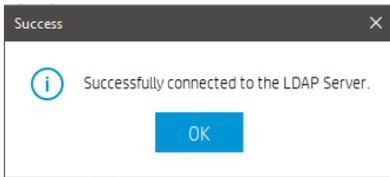
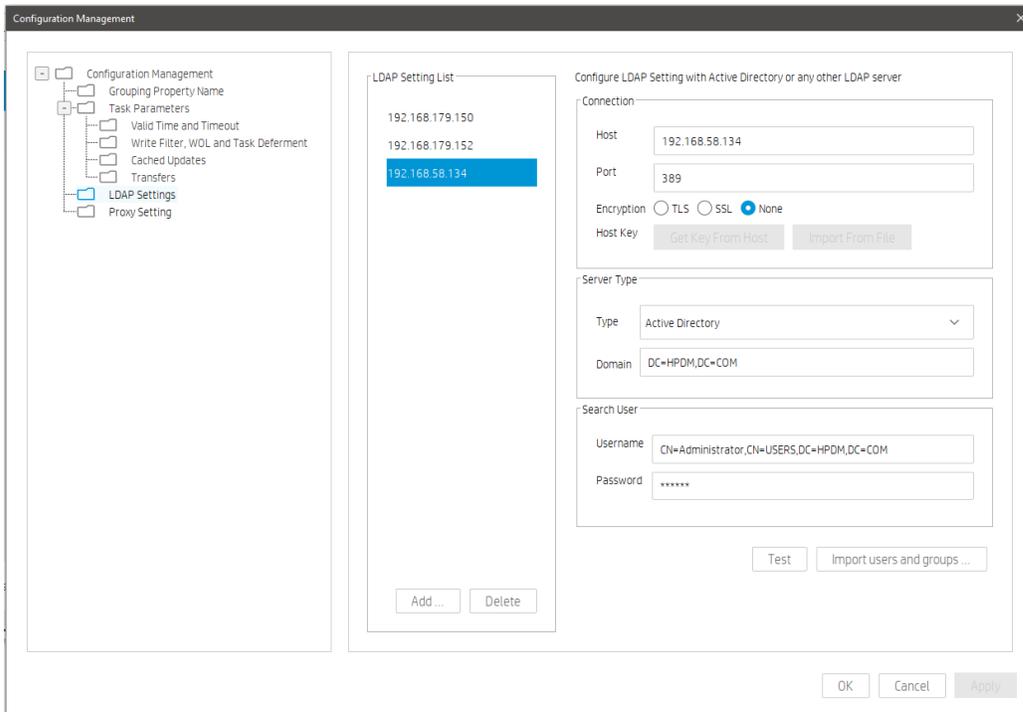
- Make sure that the network between the HPDM Server and the LDAP server is working and that the HPDM Server can access the LDAP server.
 - Verify using the ping command. The following example uses 192.168.58.134 as the LDAP server address.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 192.168.58.134
Pinging 192.168.58.134 with 32 bytes of data:
Reply from 192.168.58.134: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.58.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator>_
```

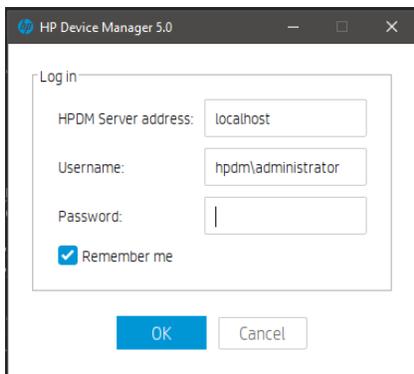
- Make sure that the LDAP server firewall does not block the port.
 - Verify using the telnet command. The following example uses the default port 389.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>telnet 192.168.58.134 389
```

- Make sure that the LDAP User Authentication is configured correctly from the HPDM Console before importing users and groups. See Configuring User Authentication.
 - To configure the User Authentication using the FQDN, you must enter the full name in both the **Domain** and the **Username** fields, such as dc=hpdm,dc=com for the domain and cn=Administrator,cn=Users,dc=hpdm,dc=com for the user named Administrator in the Users folder.
 - Verify that the LDAP server works by selecting the **Test** button during the User Authentication configuration.



- To log in to HPDM as an LDAP user, enter the short username, not the FQDN.
 - For example, if the FQDN is cn=Administrator,cn=Users,dc=hpdm,dc=com, enter hpdm\Administrator as the user name.
 - In the **Server Address** field, enter the HPDM Server address, not the LDAP server address.



If an HPDM internal user and an imported LDAP user share credentials, HPDM defaults to the inner user.

If a user or group is modified on the LDAP server, their information will not be updated in the HPDM Console until their next login.

For example, if the imported LDAP user Administrator changes their password on the LDAP Server side, the Administrator must log in to the HPDM Console again for the new password to take effect.

Duplicated Devices

Please refer to [Appendix F: Agent Device ID Filter Policy](#).

Appendix A: Database Schema

This Appendix provides documentation for the database schema of HP Device Manager 5.0. Also, this document will provide some examples of how to use tables to produce a desired report.

Overall, there are 72 tables in the HPDM database that can be divided into the following categories:

- Repository-related tables
- Device-related tables
- Task-related tables
- Template-related tables
- Gateway-related tables
- Privilege-related tables
- Rule- and Filter-related tables
- Grouping-related tables
- Configuration-related tables
- Deprecated tables

Device Tables

dm_devices

The devices table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
device_id	nvarchar	50	NO	√	<u>dm_group_values.device_id</u> ; <u>dm_inv_display.device_id</u> ; <u>dm_inv_ewf.device_id</u> ; <u>dm_inv_ex_property.device_id</u> ; <u>dm_inv_hardware.device_id</u> ; <u>dm_inv_max_hotfix.device_id</u> ; <u>dm_inv_ms_hotfix.device_id</u> ; <u>dm_inv_nic.device_id</u> ; <u>dm_inv_partition.device_id</u> ; <u>dm_inv_software.device_id</u> ; <u>dm_inv_time.device_id</u> ;	Device ID
os_configuration	nvarchar	16	YES			For ThinPro, Smart Zero
active	nvarchar	6	NO			Device active status: 0: off 1: on 2: broken
agent_version	nvarchar	20	NO			Agent version
asset_tag	nvarchar	200	YES			Asset tag
base_snapshot	nvarchar	255	YES			Base snapshot
bios_version	nvarchar	20	YES			BIOS version
device_name	nvarchar	255	YES			Device name
device_sn	nvarchar	50	NO			Device serial number
Ewf	nvarchar	8	NO			Write filter status:

						0: disabled 1: enabled 2: N/A
first_contact	smallint		NO			First contact flag, will be reset to 1 by Factory Reset task to enable First Contact rule again.
found_date	datetime	23	NO			The date that the device is found
inv_md5	nvarchar	50	YES			MD5
ip	nvarchar	15	NO			IP address
Mac	nvarchar	17	NO			MAC address
Mask	nvarchar	15	NO			Mask
master_id	nvarchar	50	NO			Gateway ID
Mode	nvarchar	4	NO			"pull" or "push"
net_addr	nvarchar	15	NO			Net address
os_type	nvarchar	20	NO			Operating system type
p1	nvarchar	50	NO			The dynamic grouping values of the device. These values are reported by HPDM Agent retrieving the values from DHCP tag, configured on the device, or set from HPDM Console.
p2	nvarchar	50	NO			
p3	nvarchar	50	NO			
p4	nvarchar	50	NO			
p5	nvarchar	50	NO			
p6	nvarchar	50	NO			
product_type	nvarchar	100	NO			Product type
product_version	nvarchar	100	NO			Product version
pull_interval	smallint	5	YES			Pull interval
update_date	datetime	23	NO			Update date
vnc_pwd	nvarchar	255	YES			VNC password
grouping	int	10	YES			Manual grouping path ID, reported by device or set from HPDM Console.
tpm_owned	nvarchar	3	YES			Device owns TPM module
has_tpm	nvarchar	3	YES			Device has TPM module
os	nvarchar	255	YES			Operating system
ipv4_value	bigint		YES			
license_description	nvarchar	255	YES			
license_enddate	nvarchar	20	YES			
license_state	nvarchar	20	YES			
wf_type	nvarchar	8	YES			
disk_encryption	nvarchar	50	YES			

dm_hash_extprop

The device properties table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
Device_id	nvarchar	50	NO	√	

Hash	nvarchar	50	NO	√	
group_order	nvarchar	1	NO		

dm_inv_display

The inventory display table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
color_depth	tinyint	3	YES		
refresh_rate	tinyint	3	YES		
resolution	nvarchar	10	YES		
update_date	datetime	23	NO		

dm_inv_ewf

The inventory write filter table is as follows:

Column name	Type name	Column size	Primary key	Description
device_id	nvarchar	50	√	
ewf_id	tinyint	3	√	
boot_command	tinyint	3		
drive_label	nchar	1		
state	tinyint	3		
update_date	datetime	23		

dm_inv_hardware

The inventory hardware table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
filesystem	nvarchar	50	YES		
free_disk	nvarchar	255	YES		
free_mem	nvarchar	100	YES		
frequency	nvarchar	100	YES		
ispxe	tinyint	3	YES		
iswol	tinyint	3	YES		
model	nvarchar	100	YES		
processor_type	nvarchar	100	YES		
processor_vendor	nvarchar	100	YES		
serial_no	nvarchar	100	YES		
total_disk	nvarchar	255	YES		
total_mem	nvarchar	100	YES		
update_date	datetime	23	NO		

dm_inv_max_hotfix

The inventory Maxspeed hotfix table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
-------------	-----------	-------------	----------	-------------	-------------

device_id	nvarchar	50	NO	√	
hotfix_id	nvarchar	50	NO	√	
hotfix_value	nvarchar	100	YES		
update_date	datetime	23	NO		

dm_inv_ms_hotfix

The inventory MS hotfix table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
hotfix_id	nvarchar	50	NO	√	
comment	nvarchar	100	YES		
installed_by	nvarchar	100	YES		
installed_date	nvarchar	20	YES		
service_pack	tinyint	3	YES		
update_date	datetime	23	NO		

dm_inv_nic

The inventory network interface card table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
nic_id	nvarchar	10	NO	√	
description	nvarchar	100	YES		
gateway	nvarchar	15	YES		
hostname	nvarchar	100	YES		
ip	nvarchar	15	YES		
is_dhcp	nchar	1	YES		
is_dnshcp	nchar	1	YES		
mac	nvarchar	17	NO		
mask	nvarchar	15	YES		
primarydns	nvarchar	255	YES		
secondarydns	nvarchar	15	YES		
update_date	datetime	23	NO		

dm_inv_partition

The inventory partition table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
partition_id	nvarchar	50	NO	√	
available	nvarchar	255	YES		
capacity	nvarchar	255	YES		
filesystem	nvarchar	50	YES		
update_date	datetime	23	NO		

Disk_capacity	nvarchar	255	YES		
Disk_id	nvarchar	255	YES		
Disk_type	nvarchar	255	YES		

dm_inv_software

The inventory software table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
sw_name	nvarchar	128	NO	√	
installed_date	nvarchar	20	YES		
size	nvarchar	100	YES		
update_date	datetime	23	NO		
vendor	nvarchar	100	YES		
version	nvarchar	100	YES		
compareversion	nvarchar	255	YES		

dm_inv_time

The inventory time table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
device_time	nvarchar	50	YES		
server_time	nvarchar	50	YES		
time_zone	nvarchar	50	YES		
update_date	datetime	23	NO		

dm_group_values

The grouping values table stores the flags that indicate whether the grouping value of a device is set from HPDM Console. For rows p1 through p6, if the value is set by HPDM Console, the grouping value is y. Otherwise, the value is NULL.

For grouping, if the global manual grouping value is set from HPDM Console, the grouping value is -1; otherwise, it is NULL.

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
p1	nvarchar	50	YES		
p2	nvarchar	50	YES		
p3	nvarchar	50	YES		
p4	nvarchar	50	YES		
p5	nvarchar	50	YES		
p6	nvarchar	50	YES		
grouping	int	10	YES		

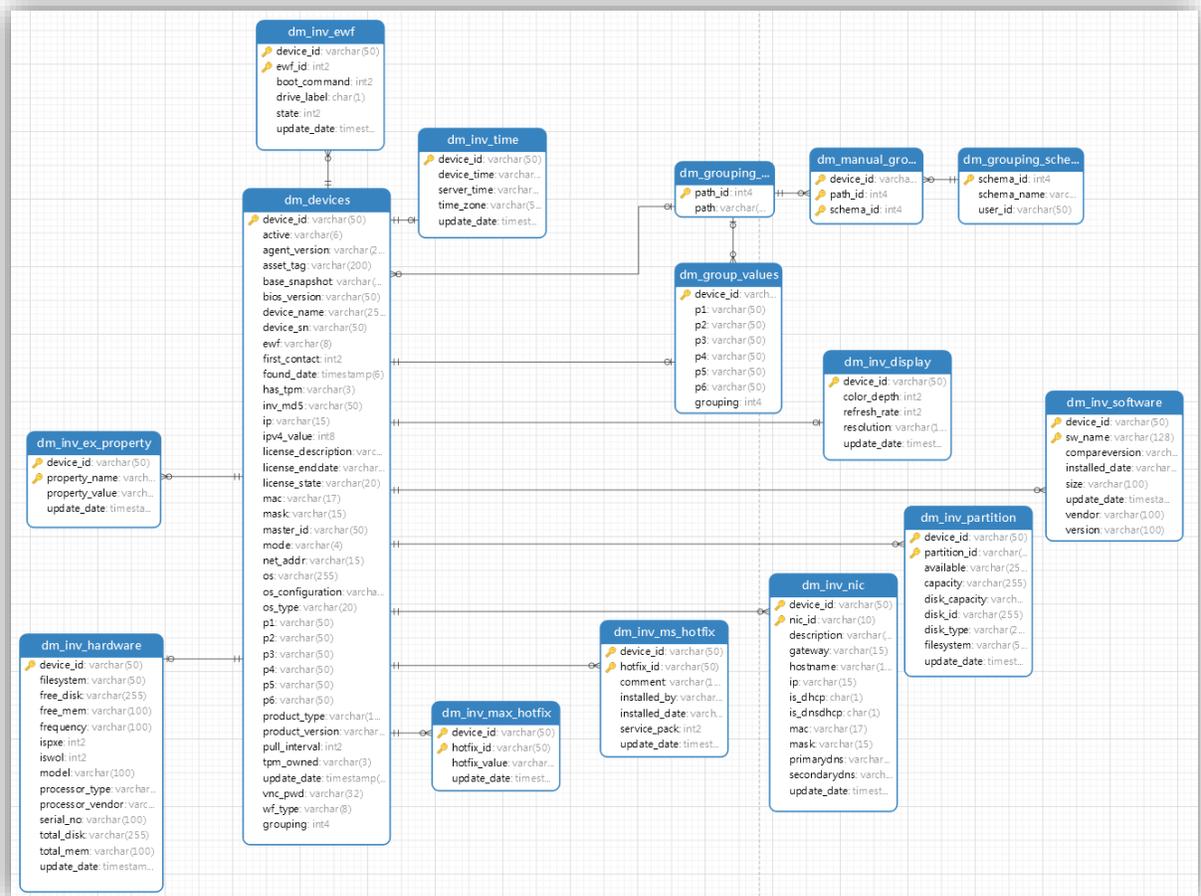
dm_inv_ex_property

The extended property table of a device is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	

property_name	nvarchar	50	NO	√	
property_value	nvarchar	100	NO		
update_date	date	23	NO		

Device tables diagram



Grouping Tables

dm_group_attribute

Grouping attributes is an inner table used by the dynamic group that should not be changed.

Column name	Type name	Column size	Nullable	Primary key	Description
attr_id	nvarchar	50	NO	√	
attr_name	nvarchar	50	NO		Attribute name

dm_group_policy

The dynamic grouping policy table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
policy_id	nvarchar	50	NO	√	Dynamic grouping ID
alias	nvarchar	50	NO		Dynamic grouping name
attrs	nvarchar	50	NO		
user_id	nvarchar	50	NO		The creator's user ID

dm_group_policy_extprop

The dynamic grouping policy table for extended properties is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
Policy_id	nvarchar	50	NO	√	
Property_name	Nvarchar	50	NO	√	

dm_grouping_path

The grouping path information table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
path_id	int	10	NO	√	dm_devices.grouping dm_group_values.grouping dm_manual_grouping.path_id	Path ID
path	nvarchar	255	NO			Value

dm_grouping_schema

The manual grouping schema table is as follows:

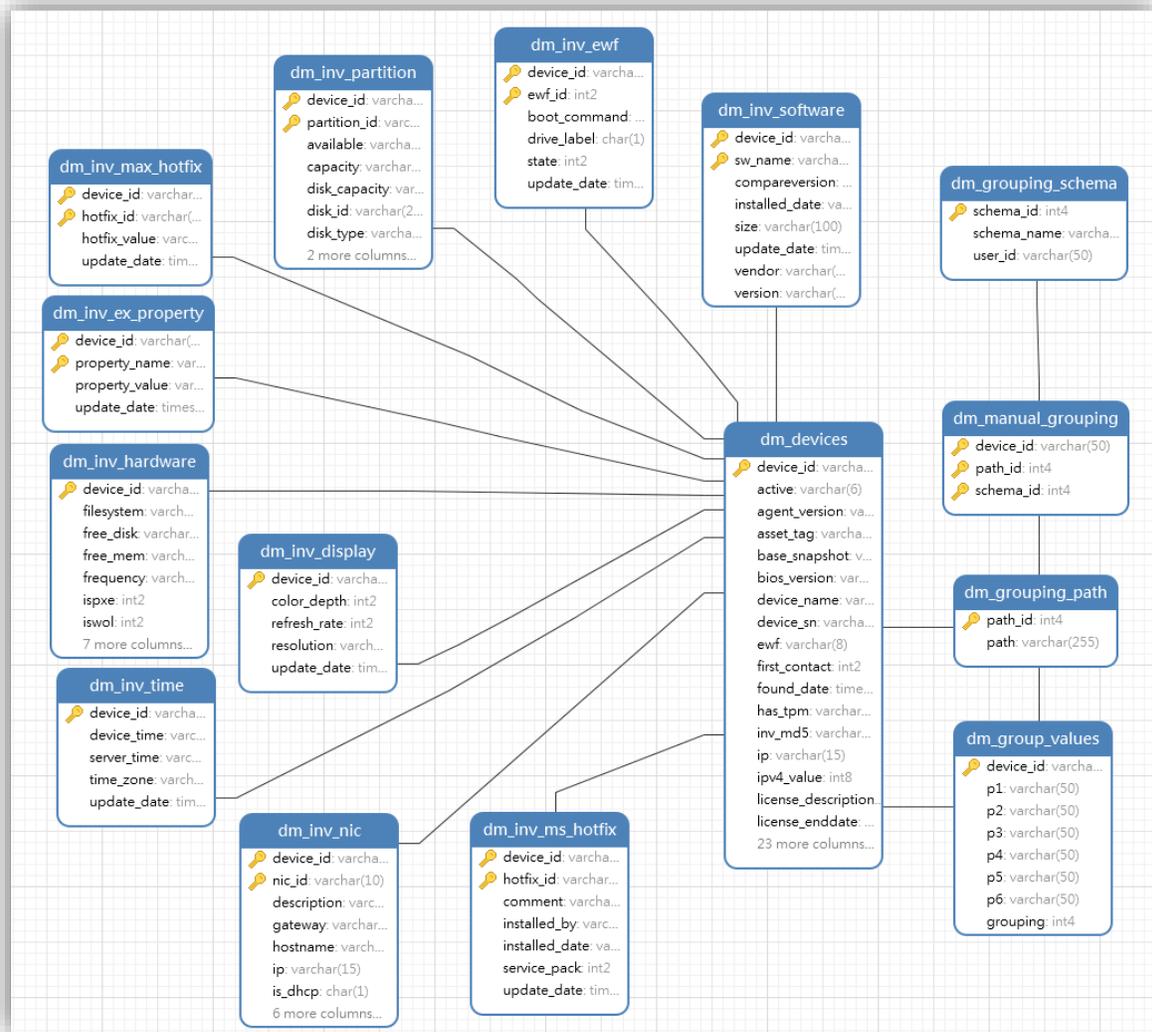
Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
schema_id	int	10	NO	√	dm_manual_grouping.schema_id	Manual schema ID
schema_name	nvarchar	50	NO			Manual schema name
user_id	nvarchar	50	NO			The creator's user ID

dm_manual_grouping

The manual grouping table stores the device relationship with a manual schema and path.

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
path_id	int	10	NO	√	
schema_id	int	10	NO	√	

Grouping tables diagram



Rule and filter Tables

dm_rule

The rule table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
rule_name	nvarchar	50	NO	√	Rule name
create_time	datetime	23	NO		Create time
creator	nvarchar	50	NO		The user ID that creates this rule
enable	int	10	NO		Rule is enabled or not: 0: disabled 1: enabled
rule_order	int	10	NO		Rule order to determine the execution sequence: 1 ~n (priority high to low)
task_id	nvarchar	50	NO		The task ID that is generated when a rule is created and then triggered by that rule

template_name	nvarchar	50	NO		Template name
trigger_type	int	10	NO		Trigger type: 1: first contact 2: startup 3: schedule
update_time	datetime	23	NO		Update time
version	int	10	NO		HPDM inner attribute, don't modify it
filter_id	nvarchar	32	YES		Filter ID
schedule_id	nvarchar	50	YES		Schedule ID (if no schedule type, it will be null)
os_type	nvarchar	50	NO		Operating system type
Rule_desc	ntext		YES		
Dynamic_folder	Nvarchar	255	YES		
Manual_folder	Nvarchar	255	YES		
Need_compliance	int		NO		
Task_parameter	test				

dm_schedule

The schedule table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
schedule_id	nvarchar	50	NO	√	dm_rule.schedule.id dm_walkingschedule.schedule_id	Schedule ID
category	nvarchar	50	NO			Schedule category (belong to): 1: snapshot 2: walking tool 3: rule
creator	nvarchar	50	NO			The user ID of creator
lastruntime	datetime	23	YES			Last run time
nextruntime	datetime	23	YES			Next run time
period	nvarchar	50	NO			The weeks number (how many weeks)
schedule_time	datetime	23	YES			Schedule time
schedule_type	nvarchar	50	NO			Schedule type: 1: daily 2: weekly 3: once
status	nvarchar	50	NO			0: disabled 1: enabled
weekday	nvarchar	50	NO			The selected weekdays (combined to one value)

dm_filter

The filter table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
filter_id	nvarchar	40	NO	√	dm_filter_fields.field_id	Filed ID

					dm_group_sec_filter.field_id dm_rule.field_id dm_user.security_filter dm_user_filter.field_id dm_user_sec_filter.field_id	
logical_operator	nvarchar	3	YES			It includes two types: and, or
update_date	datetime	23	NO			
Content	ntext		YES			Filter logic expression

dm_filter_fields

The filter fields table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
field_name	nvarchar	32	NO	√	
filter_id	nvarchar	32	NO	√	
operand	nvarchar	255	NO	√	
operator	nvarchar	32	NO	√	It contains: "=", ">", "<", ">=", "<=", "like", "has software", "has NIC", "has harddisk driver", "has hotfix", "has Microsoft hotfix", "starts with", "regardless"

Template Tables

dm_unit_template

The unit template table stores unit template information, including the templates in a sequence template.

Column name	Type name	Column size	Nullable	Primary key	Description
os_type	nvarchar	50	NO	√	Operating system type
template_name	nvarchar	200	NO	√	The template name
unit_id	nvarchar	50	NO	√	The unit ID
action_type	smallint	5	YES		Inner column to identify template action type
base_name	nvarchar	50	NO		Base template name
category	nvarchar	50	NO		Template category
file_path	nvarchar	255	NO		The file path that stores the unit template, by default "../template"
size	int	10	YES		Default is null

dm_basic_template

The basic template table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
os_type	nvarchar	50	NO	√	Operating system type
template_name	nvarchar	200	NO	√	Template name
action_type	smallint		YES		Action type (inner attribute)
category	nvarchar	50	NO	√	Category

dm_favorite_temp

The favorite template table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
os_type	nvarchar	50	NO	√	Operating system type
template_name	nvarchar	200	NO	√	Template name
user_id	nvarchar	50	NO	√	Username of the last user who modified this template

dm_report_template

The report template table stores report template information.

Column name	Type name	Column size	Nullable	Primary key	Description
report_name	nvarchar	32	NO	√	Report name
report_type	nvarchar	32	NO	√	Report type: Device: device type, Task: task type
report_content	ntext		YES		Report content
update_date	datetime		NO		Update date
Report_root	ntext		YES		

dm_template_folder

The template folder is as follows:.

Column name	Type name	Column size	Nullable	Primary key	Description
Folder_name	Nvarchar	200	NO	• √	Template name

Folder_type	Int		NO	• √	0 – private folder 1 – shared folder
Os_type	Nvarchar	50	NO	• √	Os type
User_id	Nvarchar	50	NO	• √	User name
Create_date	Datetime		YES		Create time
Templates_name	ntext		YES		Template name list
Update_date	datetime		YES		Update time

Task Tables

dm_tasks

The task table stores basic task-related information.

Column name	Type name	Column size	Nullable	Primary key	Description
action_type	smallint	5	YES		Inner column to identify the template action type
defer	smallint	5	YES		Allow defer: 0: false 1: true
batch_amount	smallint	5	YES		Units per batch (0-99, 0 for disable batch)
batch_interval	smallint	5	YES		Minutes between batches (1-180)
cache_mode	smallint	5	YES		Cache mode: 0: false 1: true
downLimit	numeric	19	YES		Bandwidth downlimit
ewf_policy	smallint	5	YES		Writer Filter Policy (default is 2): 0: If the Write Filter is on, send back failure information. 1: Execute regardless of Write Filter status. 2: If the Write Filter is on, restart to a clean overlay, execute, and commit, and then restart for commitment to take effect.
ewh	smallint	5	YES		
hidden	nchar	1	YES		Deprecated column. Default value is 1(do not change this value) History: 1 means visible and 0 means invisible.
is_sequential	nchar	1	YES		Whether a task is sequential: Y: sequential N: not sequential
os_type	nvarchar	50	NO		Operating system type
task_id	nvarchar	50	NO	√	Task ID
task_name	nvarchar	200	YES		Task name
throttling	smallint	5	YES		Bandwidth throttling
timeout	numeric	19	YES		Timeout of task
update_date	datetime	23	NO		Time will be updated when task status changes

upLimit	numeric	19	YES		Bandwidth uplimit
user_id	nvarchar	50	NO		The user who creates the task
valid_time	float	53	YES		Valid time of task
wake	smallint	5	YES		Wake on lan before task: 0: false 1: true
work_begin	smallint	5	YES		Start working time: minutes
work_end	smallint	5	YES		End working time: minutes

dm_subtasks

The subtasks table stores subtask information.

Column name	Type name	Column size	Nullable	Primary key	Description
subtask_id	nvarchar	50	NO	√	If it is a sequence task: it will be 0, 1, or 2. If it is not: the field value will be blank.
task_id	nvarchar	50	NO	√	See task_id in Error! Reference source not found..
base_name	nvarchar	200	NO		Base template name.
file_name	nvarchar	255	YES		The generated task file name. The file is stored in HPDM_DIR/Server/tasks.
task_comment	nvarchar	255	YES		Comment.
task_type	nvarchar	50	YES		It contains PXETask, Clone, GatewayTask, and Task.

dm_task_temp

The task template table stores task template information, including user-defined templates.

Column name	Type name	Column size	Nullable	Primary key	Description
os_type	nvarchar	50	NO	√	Operating system type
template_name	nvarchar	200	NO	√	Template name
category	nvarchar	50	NO		Template category
create_time	datetime	23	NO		Create time of template
description	nvarchar	255	YES		Description
is_sequential	nchar	1	NO		Whether it is a sequence template: Y: sequence template N: not a sequence template (A sequence template executes a series of tasks in sequence. See the _Template Sequence template in HPDM Console.)
update_date	datetime	23	NO		Update date of template
hint	nvarchar	2046	YES		Template hint information (when template status is not success)
status	int	10	YES		Template status: 0: success 1: transferring 2: fail
Update_user	nvarchar	255	YES		Update user

dm_tasklog

The task log table stores the task log information.

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	See device_id in Error! Reference source not found.
sequence_num	numeric	19	NO	√	The sequence number of every log (from 1 to n)
subtask_id	nvarchar	50	NO	√	Subtask ID
task_id	nvarchar	50	NO	√	Task ID
comment	ntext		YES		The log comment
error_code	nvarchar	16	YES		Error code of log
error_detail	nvarchar	255	YES		Error detail information
update_date	datetime	23	NO		Update time
error_md5	nvarchar	255	YES		HASH value of error

dm_task_error_msg

The task error message table stores the task error message and its MD5 value.

Column name	Type name	Column size	Nullable	Primary key	Description
md5	nvarchar	64	NO	√	Md5
content	ntext		YES		Error message content

dm_device_subtasks

The device subtasks table stores a device's related tasks.

Column name	Type name	Column size	Nullable	Primary key	Description
task_id	varchar	50	NO	√	
subtask_id	varchar	50	NO	√	
device_id	varchar	50	NO	√	
start_time	datetime		NO		
end_time	datetime		NO		
status	varchar	16	YES		It contains one of the following values: ready, waiting, sending, processing, success, failure, waitForAgent, processPercent, pause, waiting, chaos, unretrieved, Operational, Deleting, Deleted, Canceling, and Canceled.
visible	char	1	YES		
error_code	varchar	20	YES		
update_date	datetime		NO		

dm_snapshottask

The snapshot task table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
task_id	nvarchar	50	NO	√	dm_snapshottaskresult.task_id	Snapshot task id
comment	smallint	5	YES			Snapshot task comment
task_time	datetime	23	NO			Snapshot task start time

dm_snapshottaskresult

The snapshot task report table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	Device ID
task_id	nvarchar	50	NO	√	Snapshot task ID
active	nvarchar	50	NO		Device status, either on or off

Gateway Tables

dm_gateway

The gateway table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
gateway_id	nvarchar	50	NO	√	Gateway ID (use MAC address as default)
Active	smallint	5	NO		Whether the gateway is active or not: 0: inactive 1: active 2: broken
authentic	smallint	5	NO		Authentic type: 0: unknown 1: acknowledged 2: banned
found_date	datetime	23	NO		Gateway found date
gateway_name	nvarchar	50	NO		Gateway name
ip	nvarchar	50	NO		Gateway IP
Mac	nvarchar	50	NO		Gateway MAC address
Mask	nvarchar	50	NO		Mask
netaddress	nvarchar	50	NO		Net address
os_type	nvarchar	20	NO		Operating system type
poll_interval	nvarchar	50	NO		Poll interval, by default null
update_date	datetime	23	NO		Update date
Version	nvarchar	50	NO		Version

dm_gateway_walkingscope

The gateway walking scope table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
scope_name	nvarchar	50	NO	√	Scope name
creator	nvarchar	32	NO		Creator (user ID)
file_location	nvarchar	50	YES		File location, by default blank
update_date	datetime	23	YES		Update time

dm_gateway_walkingtask

The gateway table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
task_id	nvarchar	16	NO	√	dm_gateway_walkingtaskresult.task_id	Discover gateway task ID
end_time	datetime	23	YES			Task end time
progress	int	10	YES			Process status: 0~100

scope_name	nvarchar	50	NO			Related scope name
start_time	datetime	23	YES			Task start time

dm_gateway_walkingtaskresult

The gateway walking task result table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
ip	nvarchar	16	NO	√	Gateway IP
task_id	nvarchar	16	NO	√	Gateway task ID
status	int	10	YES		Task result status: 0: success 1: unconnected 2: deny 3: error
walking_time	datetime	23	YES		Result walking time

Repository Tables

dm_repositories

The repository table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
repo_id	int		NO	√	dm_repo_mapping.repo_id; dm_repo_protocols.repo_id	Repository ID
repo_address	nvarchar	255	NO			Repository address
repo_name	nvarchar	50	NO			Repository name
status	smallint		NO			Repository sync status
sync_date	datetime	23	YES			Last synchronization time

dm_repo_protocols

The repository protocols table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
repo_id	int	10	NO	√	Repository ID
protocol_type	int	10	NO	√	Repository protocol type: FTP: 10 FTPS: 11 SFTP: 12 SMB: 20 HTTPS: 31
password	nvarchar	100	YES		The encrypted password
repo_path	nvarchar	50	NO		Repository root path
port	int	10	NO		Port: -1: default port for this type of protocol Other value: customized port value
username	nvarchar	70	YES		Username

dm_repo_mapping

The repository mapping table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
repo_id	int		NO		Repository ID
category	int		NO		Mapping type: 1: Map by gateway 2: Map by subnet 3: Map by device
map_key	nvarchar	50	NO	√	Map key: Gateway id; Subnet address; Device_id

Privilege System Tables

dm_group

The group table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
group_name	nvarchar	50	NO	√	dm_group_sec_filter.group_name	Group name
dn	nvarchar	250	YES			Distinguished name, which only has a value when the group type is LDAP
description	nvarchar	200	YES			Description information
group_type	int	10	NO			Group type: 0: unknown 1: DB (HPDM local group) 2: LDAP (LDAP server group)
Device_limit_amount	Int		No			Limit maximum number of device when sending a task
Ldap_setting_id	Int		YES			

dm_group_sec_filter

The security filter table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
filter_id	nvarchar	32	NO	√	Filter ID
group_name	nvarchar	50	NO	√	Group name

dm_user

The user table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
user_id	nvarchar	50	NO	√	dm_user_filter.user_id dm_user_sec_filter.user_id	User name
dn	nvarchar	255	YES			Distinguished name, which only has a value when the group type is LDAP

description	nvarchar	50	NO			Description information
password	nvarchar	64	NO			Encrypted password
privilege	int	10	YES			Privilege
user_type	int	10	NO			User type: 0: unknown 1: local 2: LDAP
security_filter	nvarchar	32	YES			Security filter name
Ldap_setting_id	int		YES			
Sign	Int		YES			
salt	nvarchar	64	YES			

dm_user_sec_filter

The user security filter table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
filter_id	nvarchar	32	NO	√	
user_id	nvarchar	50	NO	√	

dm_group_user

The group and user table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
group_name	nvarchar	50	NO	√	
user_id	nvarchar	50	NO	√	

dm_auth_group

The authority in group table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
group_name	nvarchar	255	NO	√	
auth_id	int		NO		

dm_template_privilege

The template privilege table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
group_name	nvarchar	50	NO	√	Group name
os_type	nvarchar	255	NO	√	OS type
template_name	nvarchar	200	NO	√	Template name
privileges	int		NO		Template privileges

dm_key

The key table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
authkey	nvarchar	250	NO	√	
create_date	datetime	23	YES		
expire_interval	smallint	5	NO		
import_date	datetime	23	YES		
md5Key	nvarchar	250	YES		

dm_keylog

The key log table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
logdescription	nvarchar	200	NO	√	
logevent	smallint	5	NO	√	
logtime	datetime	23	NO	√	

dm_keyzero

The keyzero table is an HPDM internal table that is created when the database is installed. The record values are fixed.

Column name	Type name	Column size	Nullable	Primary key	Description
authkey	nvarchar	250	NO	√	
create_date	datetime	23	YES		
expire_interval	smallint	5	NO		
import_date	datetime	23	YES		
md5Key	nvarchar	250	YES		

Configuration Tables

dm_certificate

This certificate table stores private key, password of private key, certificate:

Column name	Type name	Column size	Nullable	Primary key	Description
conf_option	nvarchar	50	NO	√	The configuration name
conf_value	ntext		NO		The configuration value

dm_conf

The configuration table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
conf_option	nvarchar	50	NO	√	The configuration name
conf_value	nvarchar	255	NO		The configuration value

dm_dbversion

The database version table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
version	nvarchar	50	NO	√	Version value

dm_ipscope

The IP scope table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
alias	nvarchar	50	NO	√	Alias name
start_ip	nvarchar	50	NO		Starting IP address
stop_ip	nvarchar	50	NO		Ending IP address

dm_network_alias

This is the network alias table.

Column name	Type name	Column size	Nullable	Primary key	Description
network	nvarchar	50	NO	√	
alias	nvarchar	50	NO		

dm_os_types

The operating system type table stores all activated operating system type information. Each record refers to an operating system tab on HPDM Console.

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
os_type	nvarchar	50	NO	√	dm_rule.os_type	Operating system type

dm_ldap_setting

The LDAP setting table stores all LDAP settings for HPDM, which is used to connect to each LDAP Server.

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
id	int		NO	√		LDAP setting ID
Base_dn	nvarchar	255	YES			LDAP-based dn
domain	nvarchar	255	YES			LDAP domain
encrypt	nvarchar	255	YES			LDAP encryption type

host	nvarchar	255	YES			LDAP Server host
name	nvarchar	255	YES			LDAP setting name
page_size	nvarchar	255	YES			LDAP page size
port	nvarchar	255	YES			LDAP Server port
rnd_attr	nvarchar	255	YES			LDAP RDN attribute
search_pwd	nvarchar	255	YES			Searches for LDAP password
search_user	nvarchar	255	YES			Searches for LDAP username
server_type	nvarchar	255	YES			LDAP Server type

Auditlog Tables

dm_event

The audit log table is as follows:

Column name	Type name	Column size	Nullable	Primary key	Description
Id	nvarchar	255	NO	√	
Category	nvarvhar	50	No		
Detail	ntext		YES		
Logged_time	Datetime		NO		
Operation	nvarchar	200	No		
Result	Int		YES		
username	nvarchar	50	NO		

Deprecated tables

- dm_tasks_attachment
- dm_template_attachment
- dm_walkingschedule
- dm_walkingscope
- dm_walkingtask
- dm_walkingtaskresult
- dm_buildid_alias
- dm_user_filter
- dm_updatelog
- dm_upgrade_agent
- dm_ftp_servers
- dm_device_ftp
- dm_subnet_ftp
- dm_authority

Accessing the database

Generate device information

To find the device name and status for all operating system types, use the following procedure. The Device Report function will also generate these results but will include more information than necessary.

1. Connect to the database server.

2. Locate the table dm_devices.
3. Write the following SQL statements, which include only the device name and if the status is on:

```
select device_name, active
from DB_NAME.dbo.dm_devices
where dm_devices.active = 'on';
```

4. View the results.

Use the following procedure to determine which devices do not use auto-map FTP based on the results of the previous procedure.

1. Locate the table dm_repo_mapping.
2. Join the tables dm_devices and dm_repo_mapping using the following SQL statements:

```
Select dm_devices.device_NAME, dm_devices.active
from DB_NAME.dbo.dm_devices, DB_NAME.dbo.dm_repo_mapping
where dm_devices.active = 'on' and dm_devices.device_id = dm_repo_mapping.map_key
and dm_repo_mapping.category = 3;
```

3. View the results.

Generate all device inventory information

1. Locate the Device-related tables, which include the dm_devices table and the inventory-related tables.
2. Write the following SQL statements. You can use **left join** to connect all the tables you need. Left join generates the related results.

```
-- You can replace the "*" with specified columns you care about
select * from DB_NAME.dbo.dm_devices
-- append hardware information
left join DB_NAME.dbo.dm_inv_hardware
on dm_devices.device_id = dm_inv_hardware.device_id
-- append software information
left join DB_NAME.dbo.dm_inv_software
on dm_devices.device_id = dm_inv_software.device_id
-- append ewf information
left join DB_NAME.dbo.dm_inv_ewf
on dm_devices.device_id = dm_inv_ewf.device_id
-- append display information
left join DB_NAME.dbo.dm_inv_display
on dm_devices.device_id = dm_inv_display.device_id
-- ... (you can keep appending the table)
-- If you want devices with specified device ID information, you can add a "where" clause:
where dm_devices.device_id = "xxxxx";
```

3. View the results.

Generate unsuccessful task information

The HPDM Task Report function cannot be used to generate task information where the status is not success, because a criterion can only be set once. To find this task information, use the following procedure.

1. Locate the dm_device_subtasks table.
2. Write the following SQL statement:

```
select * from DB_NAME.dbo.dm_device_subtasks
where dm_device_subtasks.status != 'success';
```

3. View the results.

Display the task count grouped by task status

1. Locate the table dm_device_subtasks.
2. Write the following SQL statement:

```
select status, count(status) from DB_NAME.dbo.dm_device_subtasks group by status;
```

3. View the results.

Appendix B: Additional Configuration Options

Configuring HPDM Console

This section explains each parameter in HPDM Console configuration file.

Accessing the Console configuration file

1. Open File Explorer and find C:\ProgramData\HP\HP Device Manager\Console\conf\console.conf.
2. Right-click the file console.conf, select **Open With**, and then select **Notepad**. A Notepad file displays the content of console.conf, and you can modify some of its parameters.

Notification settings

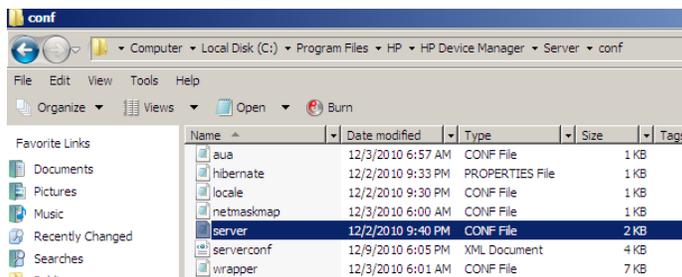
Parameter	Description
hpdm.startup.notification.optimization.enabled	This parameter should be enabled only when Console becomes sluggish while handling a substantial volume of startup notifications.

Configuring HPDM Server

This section explains each parameter in HPDM Server configuration file.

Accessing the Server configuration file

3. Open File Explorer and find the installation folder for HPDM.



4. Right-click the file server.conf, select **Open With**, and then select **Notepad**. A Notepad file displays the content of server.conf, and you can modify some of its parameters.

Thread settings

HPDM Server creates a thread pool to contain all services.

Parameter	Description
hpdm.thread.poolSize=400	This parameter indicates the maximum amount of thread used by HPDM Server. The default value is 400.
hpdm.thread.maxNum.task=100	This parameter indicates the maximum amount of thread for tasks.
hpdm.thread.maxNum.report=200	This parameter indicates the maximum amount of thread for processing reports.
hpdm.thread.maxNum.gatewayWalker=20	This parameter indicates the maximum amount of thread for walking HPDM Gateways.

Port settings

The following ports are used to communicate with HPDM Gateway.

Parameter	Description
<code>hpdm.poll.port=40000</code>	This parameter indicates the port that HPDM Server uses to poll an HPDM Gateway.
<code>hpdm.task.port=40003</code>	This parameter indicates the port that HPDM Server uses to send tasks to an HPDM Gateway.
<code>hpdm.report.port=40005</code>	This parameter indicates the port that HPDM Server uses to receive reports from an HPDM Gateway.

Poll settings

HPDM Server can be set to poll HPDM Gateways periodically and to refresh their status with the polling results.

Parameter	Description
<code>hpdm.poll.enabled=false</code>	This parameter indicates whether HPDM Server needs to poll HPDM Gateways periodically.
<code>hpdm.poll.batchNumber=10</code>	This parameter indicates how many HPDM Gateways to poll at a time. This takes effect only if <code>poll.enabled</code> is set to <code>true</code> .
<code>hpdm.poll.batchInterval=60</code>	This parameter indicates how long in seconds HPDM Server waits before polling another batch of HPDM Gateways. This takes effect only if <code>poll.enabled</code> is set to <code>true</code> and the total HPDM Gateway amount is larger than <code>poll.batchNumber</code> .
<code>hpdm.poll.roundInterval=600</code>	This parameter indicates how long in seconds HPDM Server waits before starting a new round of HPDM Gateway polling. This takes effect only if <code>poll.enabled</code> is set to <code>true</code> .
<code>hpdm.poll.retryTimes=5</code>	This parameter indicates how many times HPDM Server retries after it fails to connect to HPDM Gateway when polling it. This takes effect only if <code>poll.enabled</code> is set to <code>true</code> .
<code>hpdm.poll.retryInterval=180</code>	This parameter indicates how long in seconds HPDM Server waits before retrying polling HPDM Gateway when the last connection failed. This takes effect only if <code>poll.enabled</code> is set to <code>true</code> .

Task settings

Parameter	Description
<code>hpdm.task.SSL.enabled=true</code>	This parameter indicates whether HPDM Server sends a task to HPDM Gateway with SSL-encrypted communication. Available values are <code>true</code> and <code>false</code> .
<code>hpdm.task.retry=true</code>	This parameter indicates whether HPDM Server retries when failing to send a task to HPDM Gateway. If set to <code>false</code> , HPDM Server drops the task and marks it as a failure.
<code>hpdm.task.retryInterval=60</code>	This parameter indicates how long in seconds HPDM Server retries sending tasks. It only takes effect when <code>hpdm.task.retry</code> is set to <code>true</code> .
<code>hpdm.task.report.maxNum=200</code>	This parameter indicates the capacity of a queue which holds the task reports taken from gateway by server
<code>hpdm.task.report.maxNum=200</code>	This parameter indicates the capacity of a queue which holds the startup reports taken from gateway by server

SSL settings

Parameter	Description
<code>hpdm.ssl.downwardcompatible=false</code>	This parameter indicates whether the SSL protocol HPDM Server employs is backward compatible or not. Available values are <code>true</code> and <code>false</code> .

Log settings

HPDM Server outputs logs to a rolling file named `hpdm-server.log`.

Parameter	Description
<code>hpdm.log.level=WARN</code>	This parameter indicates the log levels to write into the log file. The log levels in HPDM Server are: DEBUG = 1: Logs for developer debugging. INFO = 2: Logs of running information, not errors. WARN = 3: Logs with warning if something unexpected happened. FATAL = 4: Logs of fatal errors or what must be logged, such as server start. Setting the log level makes HPDM Server write specified logs of no lower than the specified level to the log file. For example, when setting the log level to <code>INFO</code> , HPDM Server writes <code>INFO</code> , <code>WARN</code> , and <code>FATAL</code> logs after the next start.
<code>hpdm.log.dailyRolling=false</code>	This parameter specifies whether the log is appended with a daily rolling. If set to <code>true</code> , the following two configurations (<code>hpdm.log.maxBackupIndex</code> and <code>hpdm.log.maxFileSize</code>) are ignored.

<code>hpdm.log.maxBackupIndex=10</code>	This parameter indicates the maximum number of log files HPDM Server keeps.
<code>hpdm.log.maxFileSize=5MB</code>	This parameter indicates the maximum size of each log file.
<code>hpdm.log.gateway=false</code>	This parameter indicates whether HPDM Server writes logs about communicating with HPDM Gateway.
<code>hpdm.log.console=false</code>	This parameter indicates whether HPDM Server writes logs about communicating with HPDM Console.
<code>hpdm.log.task=false</code>	This parameter indicates whether HPDM Server writes logs about tasks.
<code>hpdm.log.taskQueueInterval</code>	This parameter indicates how often (in seconds) HPDM Server writes a log about the tasks in the queue. Set to 0 to disable HPDM Servers from writing logs about tasks.
<code>hpdm.log.db=false</code>	This parameter indicates whether HPDM Server writes logs about database operations.
<code>hpdm.log.masterController</code>	This parameter indicates whether HPDM Server writes logs about communication with the Master Controller.
<code>hpdm.log.maxListSize</code>	This parameter indicates the maximum number of devices shown in a task log. An ellipsis is appended if the device list size is greater than this parameter.
<code>hpdm.log.audit</code>	This parameter indicates whether HPDM Server writes logs about auditing HPDM Console. Set to <code>true</code> to write HPDM Console logon information to log, set to <code>false</code> to not write auditing information, and set to <code>all</code> to write every HPDM Console request to log.
<code>hpdm.log.auditFile</code>	This parameter indicates the location of the auditing file log.
<code>hpdm.hibernate.debug</code>	This parameter indicates whether HPDM Server writes logs about advanced database query details.
<code>hpdm.log.reportInterval</code>	This parameter indicates the interval in seconds to log report queue size, 0 for not logging

Cache settings

Parameter	Description
<code>hpdm.cache.enabled=true</code>	This parameter indicates whether HPDM Server keeps a cache in memory to speed up its reaction to HPDM Consoles.

LDAP settings

Parameter	Description
<code>hpdm.ldap.loopInterval</code>	This parameter indicates how often HPDM checks the imported LDAP group and its related users

Authentication settings

Parameter	Description
<code>hpdm.rmi.needClientAuth</code>	This parameter indicates whether mutual authentication is enabled

Notification settings

Parameter	Description
<code>hpdm.asynchronous.startup.notification.enabled</code>	This parameter indicates whether asynchronous startup notification is enabled. It improves the performance on processing startup reports when a great number of consoles are connected and a great number of startup reports come from gateways.

Resetting Device State

In some cases, a managed device may not be able to report its status to the management server before going offline. This behavior will cause the device to show as online indefinitely within the management console. Beginning with HP Device Manager 5.0.3, you can enable a status check to scan for inactive devices and set the device status to offline.

To enable this function:

1. Open the HPDM Server configuration file `serverconf.xml` under the `server/conf/` directory.
2. Locate the following lines:

```
<Attribute Name="hpdn.setInactiveDevicesOffline.hoursInactive" Value="24"
Enabled="no" SN="0"></Attribute>
<Attribute Name="hpdn.setInactiveDevicesOffline.checkEveryXHours" Value="24"
Enabled="no" SN="0"></Attribute>
```

Note: If you do not see these two options, please restart server

3. Change the values.

```
<Attribute Name="hpdn.setInactiveDevicesOffline.hoursInactive" Value="24"
Enabled="yes" SN="0"></Attribute>
```

When **Enabled** is **yes**, the server will do the check immediately. **Value** expects a positive integer and is used for filtering devices with last time online earlier than now minus **%Value%** (ex: 24) hours and device status is online.

```
<Attribute Name="hpdn.setInactiveDevicesOffline.checkEveryXHours" Value="12"
Enabled="yes" SN="0"></Attribute>
```

When **Enabled** is **yes** for both this item and the above item, the server will check every **%Value%** (ex: 12) hours and notify consoles if device status has been updated.

4. Save the file. The server will load the change immediately without restarting.

Configuring HPDM Gateway

HPDM Configuration Center provides some options for configuring HPDM Gateway, but more settings are in the Gateway configuration file.

HPDM Gateway configuration file is the `%ProgramData%\HP\HP Device Manager\Gateway\Gateway.cfg`.

Users can set most of the parameters from **HPDM Configuration Center – HPDM Gateway** page.

Here is the content of `Gateway.cfg`:

```
<ConfigFile>
<Server address="localhost" encrypt_connection="yes" report_delay="30"
report_interval="0" retry_interval="60" report_session_timeout="5"/>
<GatewayScale>large</GatewayScale>
<AgentPoll batch="50" poll_interval="0"/>
<GatewayID>00:1C:29:7A:22:ED</GatewayID>
<NIC></NIC>
<Timeout network_timeout="30"/>
<LogLevel>TRACE</LogLevel>
<LogInterval log_interval=""/>
<PXEShutdown>no</PXEShutdown>
<ServiceForceStart>yes</ServiceForceStart>
<UseExcpStorage>0</UseExcpStorage>
<JudgeAgentMode>yes</JudgeAgentMode>
<BroadcastPort>40000</BroadcastPort>
<Discover batch="1024" timeout="15"/>
<SslLegacySupport>no</SslLegacySupport>
<UseBuddyWOL>yes</UseBuddyWOL>
<WOLType>0</WOLType>
</ConfigFile>
```

It is an XML file.

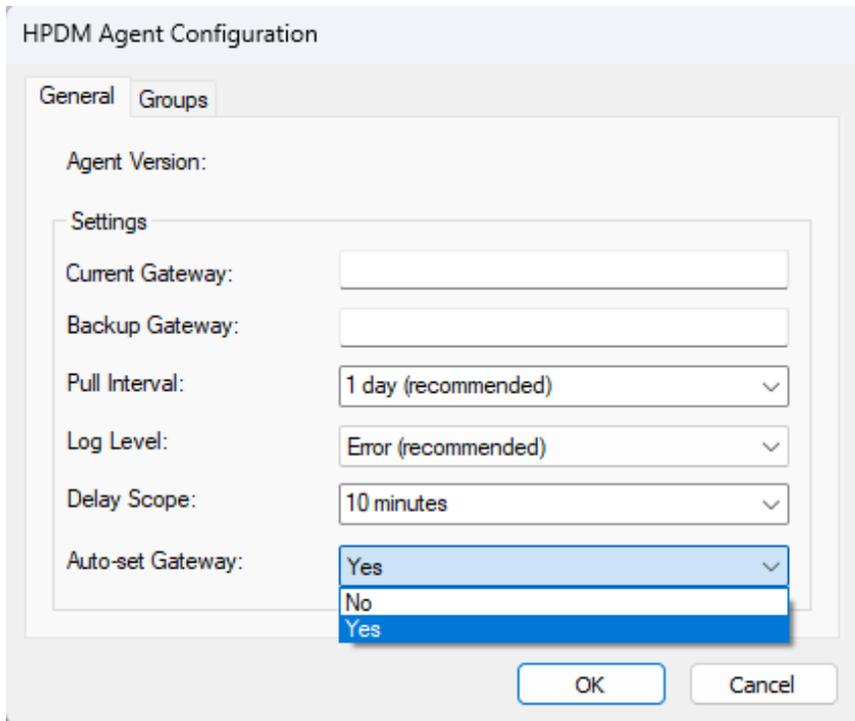
1. `<Server>` is the parameters for HPDM Gateway communicates with HPDM Server.
 - **address** is the HPDM Server address. You can set it from HPDM Configuration Center.
 - **encrypt_connection** is if the communication is encrypted by TLS. Usually do not change it.
 - **report_delay** is deprecated. Keep it for compatibility.

- **report_interval** is the interval (in seconds) of HPDM Gateway sending its report to HPDM Server. By default, it is 0. It means HPDM Gateway only reports to HPDM Server when it starts. Usually do not change it.
 - **retry_interval** is the retry interval (in seconds) when HPDM Gateways fails to connect to HPDM Server. Do not change it.
 - **report_session_timeout** is the timeout (in seconds) of the communication session of HPDM Gateway sending reports to HPDM Server. After HPDM Gateway builds up the communication for send reports, it will continuously send reports. When there is no report to send, Gateway does not close the communication until it meets the timeout. Do not change it.
2. **<GatewayScale>** is deprecated. Now HPDM Gateway can support any scale intelligently.
 3. **<AgentPoll> the Poll mechsium:** HPDM Gateway can be set to communicate with HPDM Agent periodically and update device status (on/off) to HPDM Server. It can be set from HPDM Conformation Center. For more details, please refer to the **Gateway poll** of **Optimizing HP Device Manager**.
 4. **< GatewayID>** is the Gateway ID. Please do not change it manually. You can set it from **HPDM Configuration Center – HPDM Gateway** page.
 5. **<NIC>** is the selected NIC which HPDM Gateway will bind at. Do not manually change it. You can set it from **HPDM Configuration Center – HPDM Gateway** page.
 6. **<Timeout>** is the timeout of Gateway connections. Do not change it.
 7. **<LogLevel>** is the log level of HPDM Gateway log files. You can set it from **HPDM Configuration Center – HPDM Gateway** page.
 8. **<LogInterval>** is deprecated. Keep it for compatibility.
 9. **<PXESetup>** is whether HPDM Gateway launches HPDM PXE Service automatically when HPDM Gateway starts. You can set it from **HPDM Configuration Center – HPDM Gateway** page. Currently this option is not important, because HPDM Gateway starts HPDM PXE Service when it receives a PXE task.
 10. **<ServiceForceStart>** is to allow multiple running HPDM Gateways in a subnet. You should set it to yes, if you want to running multiple HPDM Gateway in your subnet. You can set it from **HPDM Configuration Center – HPDM Gateway** page.
 11. **<UseExcpStorage>** is deprecated. Keep it for compatibility.
 12. **<SupportTeradici>** is deprecated. Keep it for compatibility.
 13. **<JudgeAgentMode>** can be set from **HPDM Configuration Center – HPDM Gateway** page – **Advanced Options**. In the HPDM Configuration Center, its display string is “**Ignore network address translation**”.
 14. **<BroadcastPort>** is the port to receive broadcast package from Agents. Do not change it.
 15. **<Discover>** is the parameters for discovering HPDM Agents. Do not change it.
 - Batch is the set size of discovery.
 - Timeout is the timeout of connections.
 16. **<SslLegacySupport>** can be set from **HPDM Configuration Center – HPDM Gateway** page – **Advanced Options**. In the HPDM Configuration Center, its display string is “**TLS 1.0 compatibility**”. Enable it to support ThinPro5 Agents or some old Agents.
 17. **<UseBuddyWOL>** is whether HPDM Gateway sends Buddy WOL tasks to Agents when it receives Wake On Lan tasks.
 18. **<WOLType>** is the types of Wake On Lan packages that HPDM Gateway sends.
 - **0:** Subnet-directed broadcast only (**by default**)
 - **1:** Unicast only
 - **2:** Both of subnet-directed broadcast and unicast

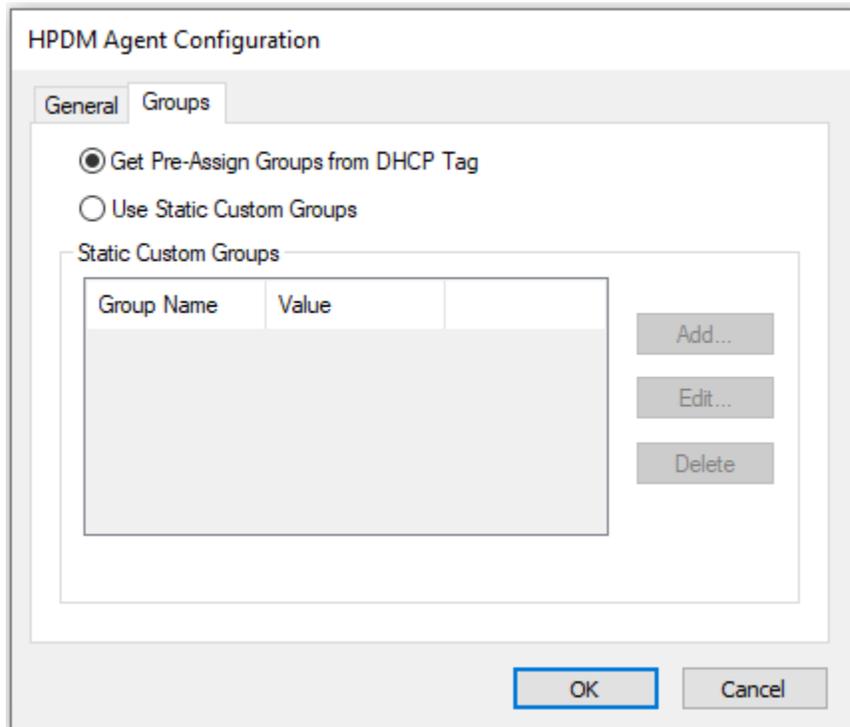
Configuring HPDM Agent

Configuring Windows clients

1. Log on to the device as Administrator.
2. Open the Control Panel and select **HPDM Agent**.



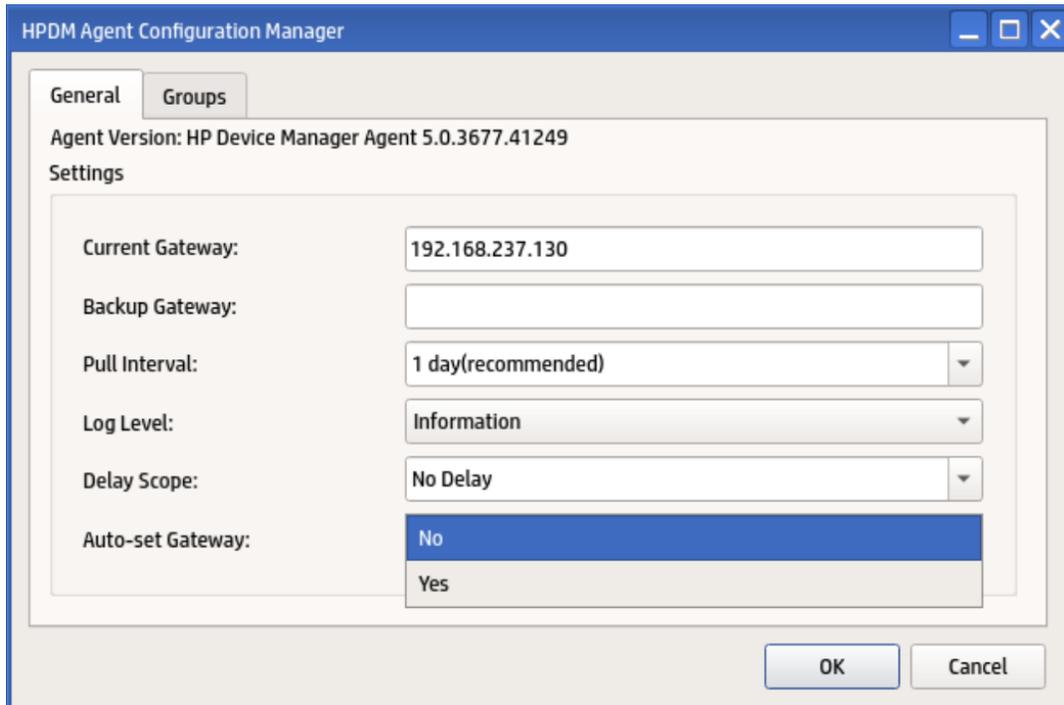
There are two tabs in this dialog. The **General** tab contains all parameters for HPDM Agent settings. The **Groups** tab is used to set special grouping information for HPDM Console and HPDM Server use.



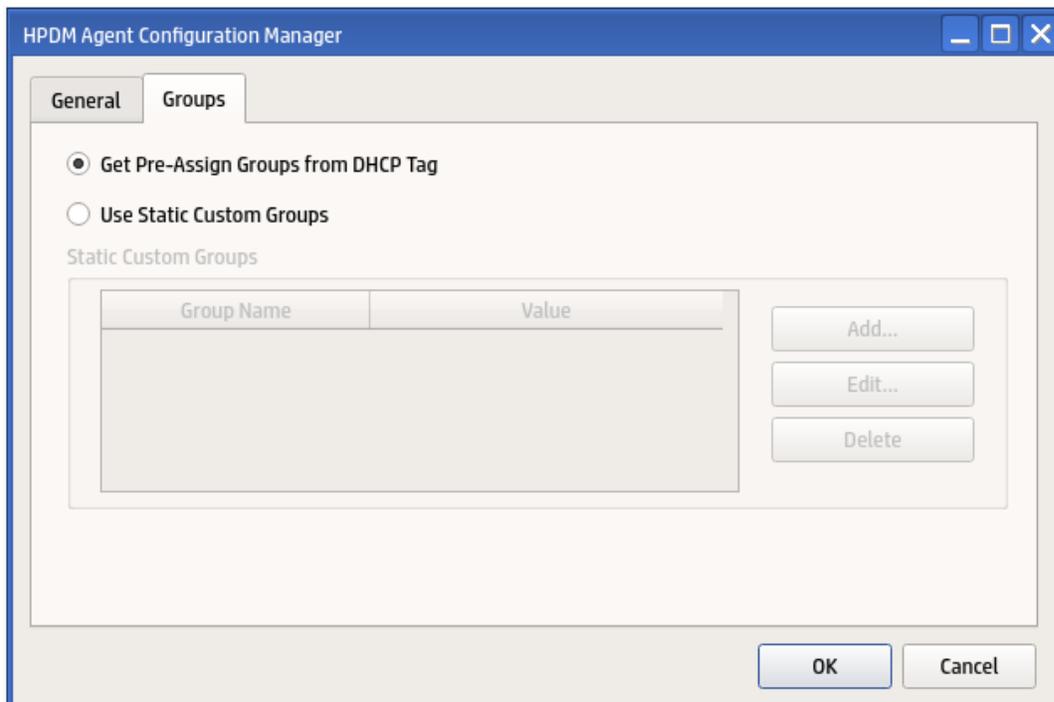
There are two options in the Groups tab. Select **Get Pre-Assign Groups from DHCP Tag** to make HPDM Agent report with grouping values to get from the DHCP server. Select **Use Static Custom Groups** to set custom grouping values manually. To set the grouping values manually, select **Use Static Custom Groups**, and then select **Add**. Enter the grouping value in the dialog that opens. You can choose the **Group Name** from a drop-down list and enter a value for it.

Configuring HP ThinPro clients

1. Log on to the device as Administrator.
2. Open the **Control Panel**, select the **Management** tab, and select **HPDM Agent**. The Agent Configure Manager dialog opens.



There are two tabs in this dialog. The **General** tab contains all parameters for HPDM Agent settings. The **Groups** tab is used to set special grouping information for HPDM Console and HPDM Server use.



There are two options in the Groups tab. Select **Get Pre-Assign Groups from DHCP Tag** to make HPDM Agent report with grouping values to get from the DHCP server. Select **Use Static Custom Groups** to set custom grouping values manually.

To set the grouping values manually, select **Use Static Custom Groups** and then select **Add**. Enter the grouping value in the dialog box that opens. You can choose the **Group Name** from a drop-down list and enter a value for it.

HPDM Agent parameters

Although the GUIs differ a little between Windows and Linux, their parameters are the same. The following are the explanations for each parameter.

- **Agent Version**—Indicates the current version of HPDM Agent.
- **Current Gateway**—Indicates the IP address of HPDM Gateway that is currently managing this HPDM Agent. You can change this value to make HPDM Agent report to another HPDM Gateway with either an IP address or a hostname. HPDM Agent refreshes this value into a valid IP address every time it receives a task from an active HPDM Gateway.
- **Backup Gateway**—Indicates the IP address of a backup HPDM Gateway. HPDM Agent tries to find an HPDM Gateway to work with on startup. If the current HPDM Gateway is not available, HPDM Agent attempts to connect to the backup HPDM Gateway.
- **Pull Interval**—Indicates the time interval that HPDM Agent connects to HPDM Gateway and asks for a task. Normally, tasks are pushed from HPDM Gateway to HPDM Agent when HPDM Gateway gets a task. Sometimes HPDM Agent is running on a device behind NAT, which means that HPDM Gateway has no approach to connect to HPDM Agent. Tasks for devices behind NAT can only be executed after HPDM Agent establishes a connection to HPDM Gateway and pulls tasks from HPDM Gateway.
- **Log Level**—Indicates which log levels should be written into the log file. When set at a particular level, errors of that level and higher are logged. There are three levels for HPDM Agent: INFORMATION, WARNING, and ERROR (from low to high). See the *HP Device Manager 4.75.0 Administrator Guide* for more details about logging.
- **Delay Scope**—Indicates a time range during which HPDM Agent sends a startup report to HPDM Gateway after startup. HPDM Agent randomly selects a time in that range and sends a startup report. This avoids creating a net traffic peak. For example, suppose there are 100 devices. All of them have Delay Scope set to 10 minutes, and you send a reboot task to them all. The 100 devices all reboot, and then their HPDM Agents start. They do not report in at the 10th minute after that startup time. Each of them uses a random time between 0 and 10 minutes. So, all 100 devices report within 10 minutes, avoiding a net traffic peak.
- **Auto-set Gateway**—: Indicates if Agent will change the Current Gateway address automatically when it receives a task from a Gateway successfully. If you create this registry key and set its value to 0, HPDM Agent will not change the Current Gateway address. If the key does not exist, the default value is 1.
- **Get Pre-Assign Groups from DHCP Tag**—Makes HPDM Agent report with grouping values to get from the DHCP server. For information on how to set grouping values on a DHCP server for HPDM, see **Configuring DHCP tags**.
- **Use Static Custom Groups**—Allows you to set custom grouping values for this device manually. HPDM Agent ignores values from the DHCP server and reports the custom settings.
- **Group Name**—Indicates the group. There are seven fields to choose from. You can set some or all of them.
- **Value**—Indicates the grouping value for the specified file.

HPDM Agent configurations

Location:

Windows Agents record their configurations in Windows registry: HKEY_LOCAL_MACHINE\SOFTWARE\HP\DM Agent\Config

ThinPro Agents record their configurations in ThinPro registry: root/hpdm/agent

Most can be found in the Agent configuration user interface:

CurrentGateway: Current Gateway in HPDM Agent parameters

BackupGateway: Backup Gateway in HPDM Agent parameters

LogLevel: Log Level in HPDM Agent parameters

DelayScope_min: Delay Scope in HPDM Agent parameters

Interval_min: Pull Interval in HPDM Agent parameters
GetGroupsFromDHCP: Get Pre-Assign Groups from DHCP Tag in HPDM Agent parameters

PreAssignGroups: Use Static Custom Groups in HPDM Agent parameters

Several advanced options are not listed on Agent configuration user interface:

AutoSetGateway: If you create this registry key and set its value to 0, HPDM Agent will not change the Current Gateway address when it receives a task from a Gateway successfully. If the key does not exist, the default value is 1.

MaxLogBackupIndex: Defines how many Agent log files will be created. If the key does not exist, the default value is 1. If you need more Agent log files, you can set it to a proper number.

SQL Server Always-on Support

HPDM supports the always-on function within Microsoft SQL Server. In order to use this feature, you must perform the following configuration in DM:

1. Make sure that the Always-on feature for Microsoft SQL Server is available and that the database is connected to the SQL Server cluster.
2. Shutdown the HPDM server and locate the `hibernate.properties` file within the `server/conf` directory.
3. Open the file and place the parameter "`MultiSubnetFailover = True;`" before the `DatabaseName` property within the `hibernate.properties` file.
4. After saving the changes, restart the HPDM server. If the server starts successfully, the SQL Server always-on support has been successfully enabled.

Note

If you need to add parameters in the database connection string, the parameters must be added before `DatabaseName`.

Appendix C: Configuring DHCP tags

Configuring a DHCP server for use with PXE

Do not install HPDM PXE Service (under HPDM Gateway) into the computer which has DHCP server.

If problems occur when using PXE, verify that the DHCP server settings do not conflict with PXE. These issues rarely occur. The PXE boot ROM uses the DHCP server to get an IP address, as well as other basic networking information such as a subnet mask or a default gateway.

Note

The network must be configured using DHCP to use the PXE service.

To configure the DHCP server:

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

Note

The HPDM PXE service detects the DHCP packets sent by any PXE boot ROMs and offers PXE network parameters without disturbing the standard DHCP negotiation process. This is called DHCP Proxy.

The DHCP server is now ready to use with PXE.

Configuring options 202 and 203

Option 202 is used to set the IP address for the HPDM Server and HPDM Gateway.

To set option 202:

1. Select **Start > Run**.
2. Type `cmd` in the box. A command shell appears.
3. Type `netsh`, and then press **Enter**.
4. Type `dhcp`, and then press **Enter**.
5. Type `server \\<server_name>` (using the UNC name for the DHCP server).
—or—
Type `server <IP_address>` (using the IP address of the DHCP server).
A `<dhcp server>` prompt appears in the command window.
6. Type `add optiondef 202 <custom_option_name> STRING 0`, and then press **Enter**.

7. Type set optionvalue 202 STRING "<HPDM_Server_IP> <HPDM_Gateway_IP>", and then press **Enter**.
For example: set optionvalue 202 STRING "192.168.1.100 192.168.1.200"
8. To confirm that the settings are correct, type show optionvalue all, and then press **Enter**.

Note

Replace the items in brackets with the appropriate value.

When setting optionvalue 202, the syntax must be written exactly as shown above, separated by a single space, otherwise errors occur. See the following example:

```
192.168.1.100 192.168.1.200
```

Option 203 is used to set up to six grouping parameters (P1–P6), which can be used as part of a dynamic grouping scheme, and a special parameter labeled MG, which is used for manual grouping. The instructions are the same as option 202, and the option value format is as follows:

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

See the following example:

```
add optiondef 203 CustomName STRING 0
set optionvalue 203 STRING
"P1='Asia';P2='China';P3='Shanghai';MG='Company/Department/Group' "
```

Note

All grouping parameters (P1–P6 and MG) are optional, but those specified must be assigned a value.

To allow users to input multiple groups using option 203 on the command line, HPDM supports using single quotes. Double-quotes are still supported.

Configuring options for scopes (scope options)

All of above options are server options. If you want to set different options for scopes:

1. Follow the 1 – 5 steps of "Configuration option 202 and 203".
2. Type add optiondef <option_code> <custom_option_name> STRING 0, and then press **Enter**.
3. Type scope <scope-ip-address>, and then press **Enter**.
4. Type set optionvalue <option_code> STRING <option_value>, and then press **Enter**.
For example: set option 202 under the scope192.168.1.0.
5. netsh dhcp server> add optiondef 202 HPDM_SERVER_GATEWAY
6. netsh dhcp server> scope 192.168.1.0
7. netsh dhcp server scope> set optionvalue 202 STRING "192.168.1.10 192.168.1.10"

Appendix D: 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 UEFI: IPv4 (TFTP) network controller as the first UEFI boot source or 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. This is an example of setting the PXE network controller as the first legacy boot source. If there is no PXE network controller in Legacy Boot Sources list, set UEFI: IPv4 (TFTP) network controller as the first UEFI boot source. Steps are almost same with this example.

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

Install BCU on the same computer as HPDM Console.

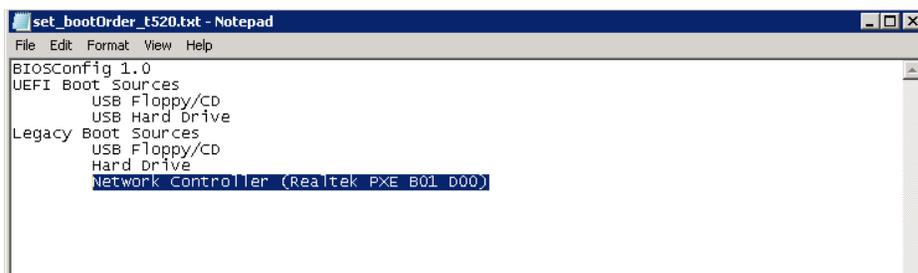
In HPDM Console, create a File and Registry template with the following subtasks in order:

1. Deploy Files (to deploy **BiosConfigUtility64.exe** to the device)
2. Script (to execute a BCU command that gets the BIOS settings of the device and writes them to a file)

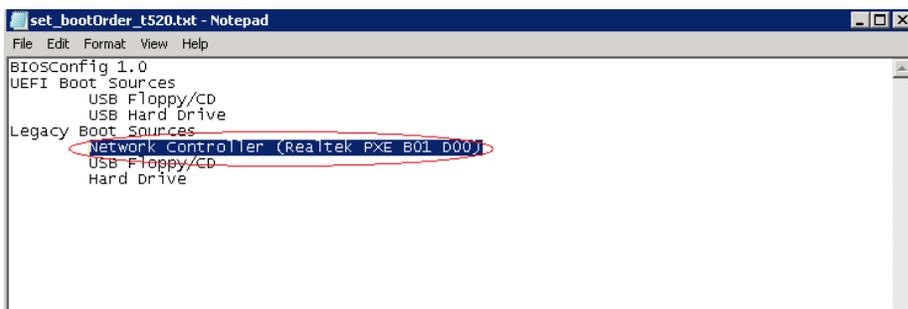
See the following table for an example script.

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

3. Capture Files (to capture the file from c:\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 is 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_t520.txt in Notepad.
7. Delete all file contents except for the file heading and the two boot source sections, like in the following image.



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



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

1. Deploy Files (to deploy **BiosConfigUtility64.exe** and **set_bootOrder_t520.txt** to the device)
2. Script (to execute a BCU command that applies the new settings, in this case, the boot order)

See the following example scripts:

Field	User input
Start in	c:\temp
Content	cd c:\temp BiosConfigUtility64.exe /set "c:\temp\set_bootOrder_t520.txt"

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

Note

The hardware platform of the target devices must be 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. This is an example of setting the PXE network controller as the first legacy boot source. If there is no PXE network controller in Legacy Boot Sources list, please set UEFI: IPv4 (TFTP) network controller as the first UEFI boot source. Steps are almost same with this example.

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.

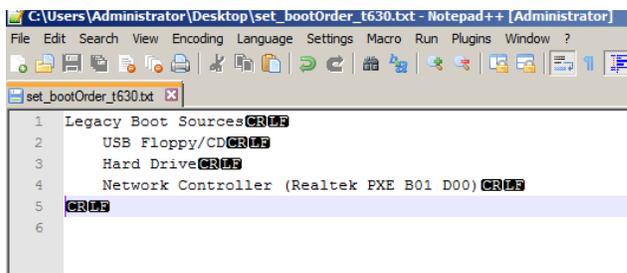
In HPDM Console, create a File and Registry template with the following subtasks in order:

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

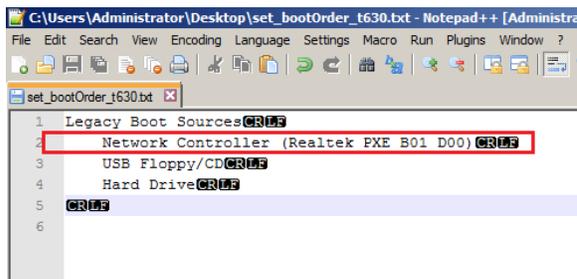
For example:

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

2. Capture Files (to capture the file from `/tmp/t630_BiosConfig.txt` to the master repository)
3. Send the File and Registry task to the target device. After the task is complete, the captured file is located in the master repository at `\Repository\Files\Captured\`.
4. Create a copy of `t630_BiosConfig.txt`, and then rename the new file to `set_bootOrder_t630.txt`.
5. Open `set_bootOrder_t630.txt` in Notepad++
6. Select **Edit > EOL Conversion**, and then select the item for **Windows** (the name depends on your version of Notepad++).
7. If not already enabled, enable the **Show End of Line** option under **View > Show Symbol**.
8. Delete all of the file contents except for the Legacy Boot Source section, like in the following image.



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



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

1. Deploy Files (to deploy `set_bootOrder_t630.txt` to the device)
2. 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`

3. Send the File and Registry task to the target devices.
-

Note

The hardware platform of the target devices must be 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.

4. Send a Reboot Device task to reboot the target device. For example: `hptc-bios-cfg -S /tmp/set_bootOrder_t630.txt`
 5. Send the File and Registry task to the target devices.
-

Note

The hardware platform of the target devices must be 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.

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

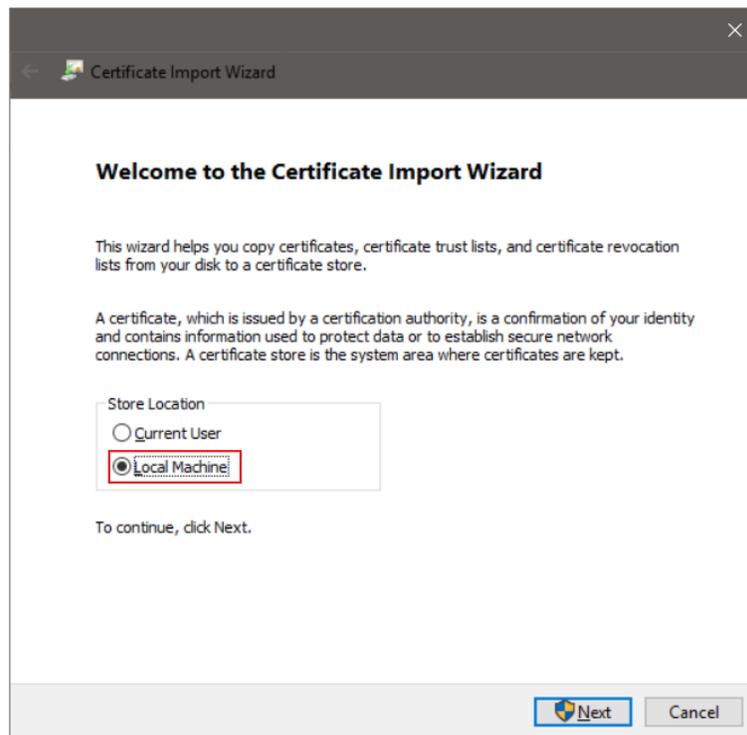
Appendix E: Configuring HPDM Master Repository Controller Certificate

By default, the HPDM Master Repository Controller uses the self-signed certificate to communicate with the HPDM Server. Follow the steps below to replace the default one with the customized certificate. For example, the certificate issued by CA infrastructure.

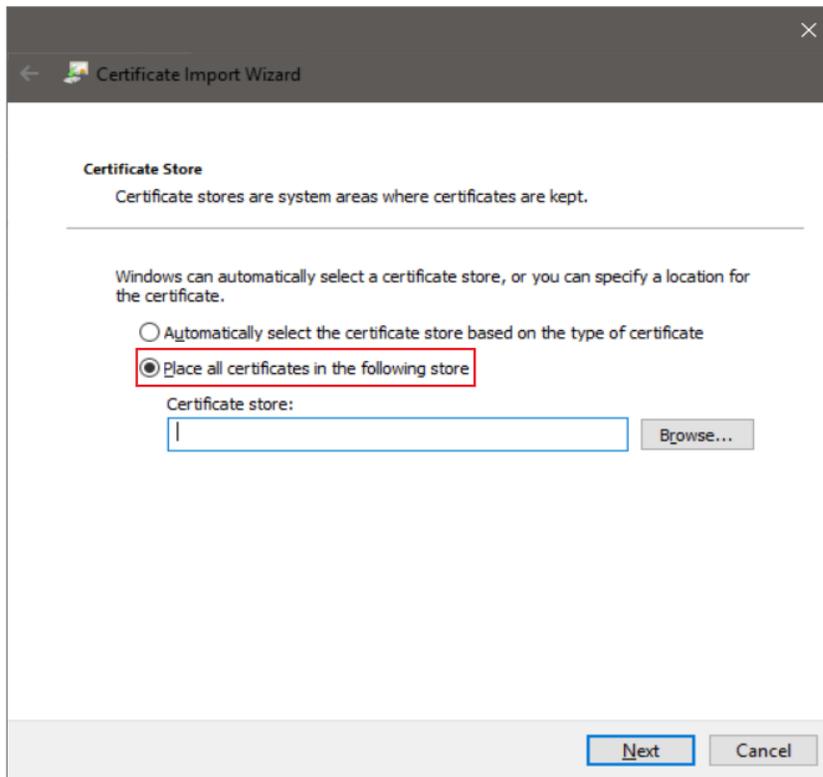
1. Stop HPDM Master Repository Controller and HPDM Server services
2. Replace certificate on HPDM Master Repository Controller side
 - a. Prepare the public certificate and private key that used by MRC
 - i. HPDM MRC only supports PEM format certificate. If the certificate isn't the PEM format, please convert it to PEM format at first.
 - ii. The private key cannot with a password.
 - b. Go to the directory `%HPDMInstalledPath%\MasterRepositoryController\
 - i. Delete Controller.crt, Controller.key and Client.crt.
 - ii. Rename your public certificate file to Controller.crt and rename your private key file to Controller.key, then copy them to this folder.`
3. Install root CA and intermediate CA certificates on HPDM Server side
If the certificate is issued by an intermediate CA, you need to install all intermediate CA certificates and root CA certificate on HPDM Server side.
 - a. Go to the directory `%HPDMInstalledPath%\Server\bin\`.
 - b. Delete `hpdmkey.keystore`.
 - c. Install CA and intermediate CA certificates by following steps.
 - i. Double clicks the CA or intermediate certificate file, select "Local Machine" and click "Next".

Select “Local Machine”

Note: This means that the certificate is associated with this machine.



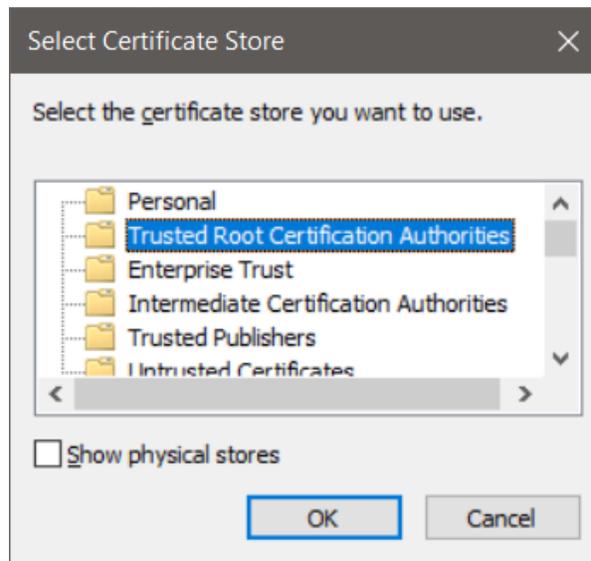
- ii. Select “Place all certificates in the following store” and click “Browse...”.



- iii. Select "Trusted Root Certification Authorities" and click "OK".

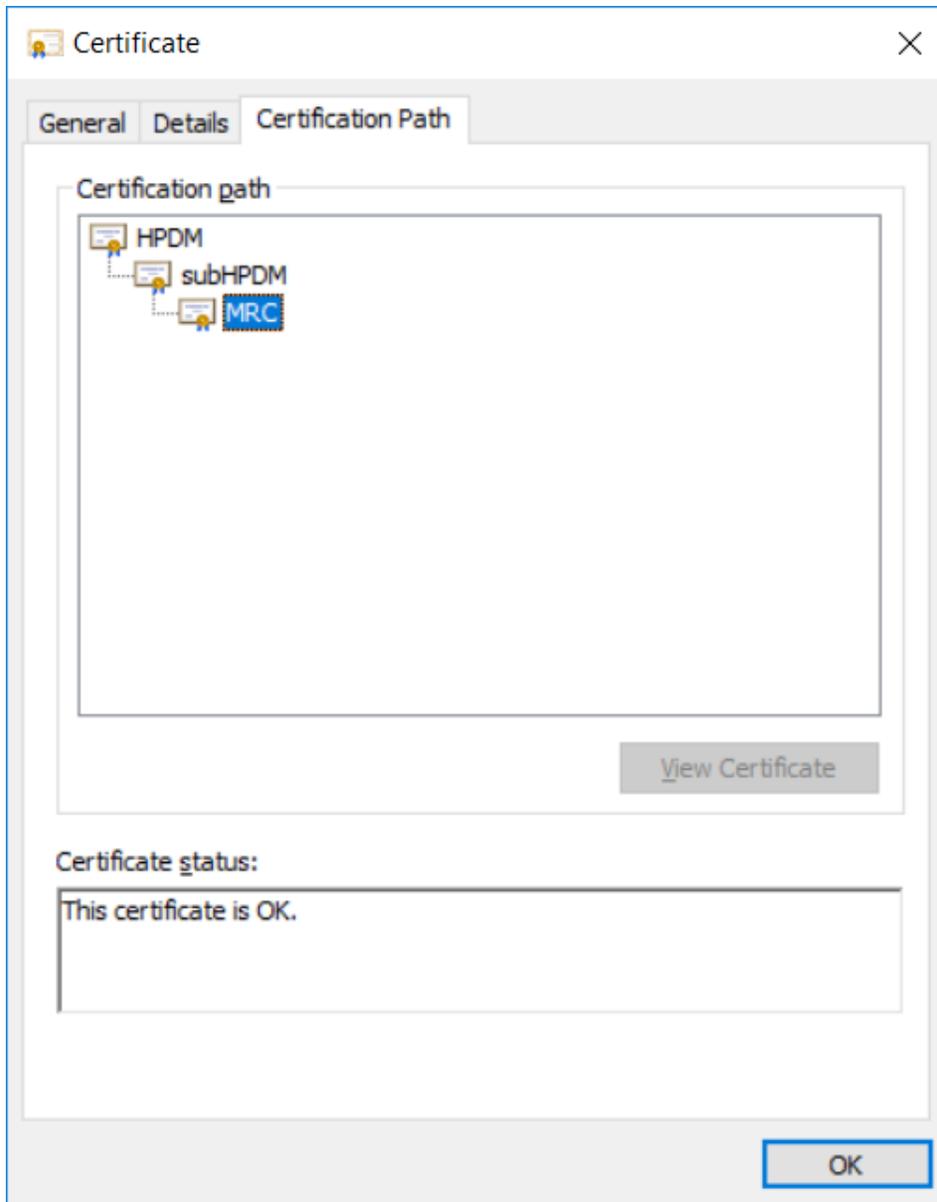
Select "Trusted Root Certification Authorities"

Note: Add the certificate to the System's Root certificate List.



- iv. Click "Next".
- v. Repeat i to iv to install other CA or intermediate certificates.

For example, below is sample certificate and its certificate chain. You need to deploy the certificate named MRC on HPDM MRC side and install root CA HPDM and intermediate CA subHPDM on HPDM Server machine.



4. At last, start HPDM Server and HPDM MRC services

Appendix F: Agent Device ID Filter Policy

Background

The HPDM Agent uses the MAC address of a device's network adapter as the Device ID. If a device is connected to a docking station, it is possible that the HPDM Agent will choose the MAC address of the docking station's network adapter as Device ID instead. When this happens, a duplicated device is added into HPDM Console/Server and the Device ID of the docking station. This document introduces an approach to resolve this issue.

Mechanism

To choose a proper network adapter's MAC address, HPDM Agent has 2 built-in policies to filter out some network adapters.

- **MAC Filter Policy:** Filter out network adapters by the prefix of MAC address.
Example: "00:0C:29" filters out vmware device network adapters. The HPDM Agent ignores all "00:0C:29:?:?:??" MAC addresses when it is configured.
- **NIC Filter Policy (Windows only):** Filter out network adapters by keywords in description.
Example: If "Wireless" is a filter keyword, the HPDM Agent will ignore all network adapters that have "Wireless" in their description.

The filter policy can be modified by filter configuration files.

Filter Configuration Files

The HPDM Agent supports 4 filter configuration files: macfilter_base.cfg, nicfilter_base.cfg, macfilter.cfg and nicfilter.cfg.

macfilter_base.cfg can overwrite the MAC Filter Policy.

nicfilter_base.cfg can overwrite the NIC Filter Policy.

macfilter.cfg only can append rules into the MAC Filter Policy.

nicfilter.cfg only can append rules into the NIC Filter Policy.

The files must be placed in the Agent folder: C:\Windows\hpdagent (on Windows) or /etc/hpdmagent (on ThinPro).

Overwrite

Only macfilter_base.cfg and nicfilter_base.cfg can overwrite the built-in Filter Policies. It means if they exist, the HPDM Agent does not use the built-in Filter Policy and instead uses these 2 files. You can append or reduce filter rules in these 2 files. If they exist but they are empty, HPDM Agent will not filter out any network adapter.

Append

The HPDM Agent will still use the built-in Filter Policies. When macfilter.cfg and nicfilter.cfg exist, the Agent will append the filter rules of them into Filter Policies.

Default macfilter_base.cfg and nicfilter_base.cfg

These are 2 default filter configuration files. They are the same with the built-in Filter Policies.



macfilter_base.cf
g

Default macfilter.cfg and nicfilter.cfg

There is no default macfilter.cfg and nicfilter.cfg. The macfilter.cfg is in the same format as macfilter_base.cfg, and the nicfilter.cfg is in the same format as nicfilter_base.cfg.

Usage

Basic Usage

Example: How to filter a network adapter of a docking station.

1. Execute cmd.exe to open Command Prompt on the thin client.
2. Execute "ipconfig /all".
3. Find the prefix of the MAC address of the network adapter.

Example: Below is the network adapter I found that I want to filter it out.

```
Ethernet adapter Ethernet 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek USB GbE Family Controller
Physical Address. . . . . : 9C-7B-EF-9E-28-6A
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

4. Create a macfilter.cfg and add a line
9C:7B:EF
5. Put this file into Agent folder (C:\Windows\xpeagent) of devices
6. Restart the devices for the change to take effect.

Advanced Usage

Example: How to allow the HPDM Agent to use the MAC address of a vmware network adapter as Device ID.

Because vmware network adapters are filtered out by the HPDM Agent built-in Filter Policy, you must modify macfilter_base.cfg and nicfilter_base.cfg and deploy them into the Agent folder (C:\Windows\xpeagent)

1. Execute cmd.exe to open Command Prompt on the vmware device.
2. Execute "ipconfig /all".
3. Find the MAC address and the Description of the vmware network adapters.
 - a. Usually MAC address is 00:0C:29:?:?:??
4. Open macfilter_base.cfg and remove the prefix of the MAC address (usually is 00:0C:29).
5. Open nicfilter_base.cfg and remove the keywords you find in the description.
6. Put the files into the Agent folder (C:\Windows\xpeagent).
7. Restart the vmware device for the change to take effect.

Sign up for updates
hp.com/go/getupdated

© Copyright 2024 Hewlett Packard Development Company, L.P.

Microsoft and Windows are trademarks of the Microsoft group of companies.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Fourth Edition: November 2024

First Edition: May 2019

Document Part Number: L70795-002

