

# HP Device Manager 5.0

## Administrator's Guide



## Table of contents

Overview .....	11
Terminology .....	11
Installation.....	12
Installation requirements .....	12
HPDM Server requirements .....	12
HPDM Gateway requirements .....	12
HPDM Master Repository Controller requirements .....	12
HPDM HTTPS Repository requirements .....	13
HPDM Console requirements.....	13
HPDM Console Web Bridge requirements .....	13
HPDM Configuration Center requirements.....	14
Network requirements .....	14
Port requirements .....	14
Product Support Matrix.....	14
Server preparation.....	15
Selecting a database management system.....	15
Choosing repository protocols .....	15
Windows firewall settings .....	15
Installation options.....	17
Server-side Components.....	17
Complete Setup .....	17
Custom Setup .....	17
Updating an Existing Installation .....	22
Upgrading a Previous Installation.....	23
Migrating HP Device Manager 4.7 data to a new machine and upgrading.....	23
Uninstalling HP Device Manager .....	25
HPDM Component Installers.....	25
Preparation.....	25
HPDM Server Component Installer.....	26
HPDM Gateway for Windows® Component Installer .....	26
HPDM Master Repository Controller Component Installer .....	26
HPDM HTTPS Repository Component Installer .....	26
HPDM Console Component Installer .....	27

HPDM Console Web Bridge Component Installer .....	27
HPDM Configuration Center .....	27
Deployment .....	27
Overview .....	27
Typical Device Manager topology .....	28
Port usage .....	30
Console ports (inbound) .....	30
Console ports (outbound) .....	31
Server ports (inbound) .....	32
Server ports (outbound) .....	32
Gateway ports (inbound) .....	32
Gateway ports (outbound) .....	33
Agent ports (inbound) .....	34
Agent ports (outbound) .....	34
Repository ports (inbound) .....	36
Repository ports (outbound) .....	37
Deployment factors .....	38
Hardware environment .....	38
Database storage .....	39
Repository capacity .....	39
Network infrastructure .....	39
Limitations .....	43
Ports between networks .....	43
Failover redundancy .....	44
Number of devices .....	45
Deployment options .....	46
Deployment scenarios .....	47
Deploying to Amazon EC2 .....	48
Deploying to Microsoft Azure .....	55
HPDM HTTPS Repository .....	59
Installation .....	59
Certificate configuration .....	60
Performance .....	63
Bandwidth throttling .....	66
Manually update Apache and PHP .....	67
FTP Repositories .....	68
Overview .....	68
IIS FTP server configuration .....	68
Configuring HPDM to use FTPS .....	74
TLS 1.0 Compatibility .....	77
FileZilla FTP server configuration .....	79
For more information .....	83

Operation .....	84
Management Console .....	84
Logging into the Console .....	84
The homepage .....	84
Console layout .....	85
Manage Devices .....	87
Templates & Rules.....	90
Tasks & Reports.....	91
Users & Groups .....	94
Gateways & Repositories.....	95
Administration .....	96
Console management.....	96
Console Web Bridge .....	100
Device Discovery .....	101
Automatic registration .....	101
DNS service records .....	101
Searching for devices .....	102
Using the Scan using IP Range method .....	102
Using the Scan using IP List method .....	103
Using the Scan using subnet of specified Gateway method .....	103
Manually registering a device.....	103
Manually registering multiple devices .....	104
Device Management.....	106
Viewing devices .....	107
Deleting devices .....	107
Grouping devices .....	107
Dynamic Grouping .....	108
Filtering devices.....	109
Device Properties.....	112
Grouping Tool .....	113
Dynamic Properties .....	116
Checking device connection status .....	125
Template Navigator.....	125
Templates & Rules.....	126
Task Templates.....	126
Working with Task Templates .....	126
Creating a task template .....	127
Exporting task templates .....	127
Importing task templates.....	128
Importing Templates Across OS Versions .....	128
Generating a template from payload.....	130
Copying a Deploy Image template for use with a different OS type.....	131

Template sequences .....	131
Templates folder.....	132
Adding a folder .....	132
Deleting a folder .....	132
Renaming a folder .....	132
Adding template to a folder .....	132
Removing template from the folder .....	133
Task Rules .....	133
Trigger Type.....	133
Target Folder .....	133
Rule Compliance .....	133
Adding a New Rule .....	133
Export and Import Rules.....	134
Tasks & Reports.....	135
Tasks .....	135
Tasks Interface .....	136
Working with Tasks .....	138
Performing a task.....	138
Task status .....	138
Task parameters.....	139
Task deferment .....	139
Viewing task properties.....	139
Pausing a task.....	139
Resuming a task .....	140
Resending a task .....	140
Canceling a task.....	140
Deleting a task.....	140
Viewing task logs.....	140
Viewing a Task's Success Ratio .....	141
Device shadowing.....	141
Result Template .....	141
Displaying tasks from all users .....	141
Task Notifications.....	141
Cached Tasks.....	142
Cached updates .....	142
Usage scenarios.....	143
Using cached updates .....	143
Configuring cached updates.....	146
Cached Update Limitations.....	147
Task template Reference.....	147
File and Registry .....	147
Agent.....	151

Connections .....	152
Imaging .....	152
Operations .....	152
Settings.....	153
Template Sequence .....	154
Imaging Devices .....	154
Imaging support matrix.....	154
Capturing an image.....	154
Deploying an image .....	165
Deploying an image using the cached updates mode.....	170
Deploying an image with PXE.....	172
Preserved settings during imaging .....	173
Imaging task performance .....	174
Known issues .....	175
Reporting Tools.....	176
Adding a report .....	176
Editing a report .....	176
Deleting a report.....	176
Generating a report preview .....	177
Gateways & Repositories.....	177
Page Layout .....	177
Managing Repositories .....	178
Mechanics .....	179
Protocols.....	179
Modifying Repository settings withinin HPDM Console .....	179
Configuring the Master Repository .....	180
Child Repository configuration.....	181
Deleting an HPDM Child Repository .....	181
Exporting repositories .....	181
Importing repositories.....	181
Repository mapping .....	181
Synchronizing repositories.....	182
Content management.....	182
Customized Packages.....	183
Users and Groups.....	184
Page Layout .....	185
Users .....	186
Add users .....	186
Deleting users.....	186
Assigning users to groups .....	186
Changing a user's password.....	186
Viewing privileges and template access .....	186

Groups .....	186
Adding a group.....	187
Assigning privileges to groups .....	187
Assigning users to groups .....	187
Assigning security filters to groups .....	187
Policy .....	187
Viewing privileges and template access .....	187
Deleting groups .....	188
Directory Services .....	188
LDAP settings.....	188
Importing users and groups .....	189
Multiple trusted domains login .....	190
Universal group login .....	193
LDAP subgroup login .....	194
Privilege System .....	194
Action based privilege .....	195
Object based privilege .....	195
HPDM behavior under privilege management system .....	195
Security filter .....	196
Privilege-related operations .....	197
Sample Scenarios .....	199
Administrative Functions.....	200
Page Layout .....	200
Security Controls.....	200
Database confidentiality .....	201
File repository confidentiality .....	201
HPDM logon integrity .....	201
Confidential data in log files.....	201
User management .....	201
Authentication management .....	202
Master Repository Controller access control.....	202
Gateway access control.....	202
Network communication .....	202
Secure file server .....	203
Task verification .....	203
Compatibility with Older Components .....	203
HP Update Center .....	203
Generating task templates.....	204
Configuring HP Update Center proxy settings .....	204
Documentation and software updates .....	204
Configuration Center .....	205
Configuration Summary .....	206

General Configuration .....	206
HPDM Server .....	207
HPDM Database .....	208
HPDM Gateway .....	211
HPDM Master Repository Controller .....	212
HPDM HTTPS Repository .....	212
HPDM Console Web Bridge .....	213
Disaster Recovery .....	214
General recovery process .....	214
Recovering the HPDM Server .....	217
HPDM Archive Tool .....	220
Optimizing Device manager .....	222
Troubleshooting .....	222
Log files .....	222
HPDM Agent log files .....	222
HPDM Gateway log files .....	223
HPDM Console log files .....	223
HPDM Server log files .....	223
Master Repository Controller log files .....	223
HPDM installation log files .....	224
Collecting useful log information .....	224
HPDM Agent .....	224
HPDM Gateway .....	224
HPDM Console .....	225
HPDM Server .....	226
Master Repository Controller .....	227
Collect all HPDM component logs .....	228
General Troubleshooting .....	229
Error Codes .....	230
Database Issues .....	231
Using MS SQL Server .....	231
Using PostgreSQL .....	233
Troubleshooting steps .....	233
Additional resources .....	233
Network Issues .....	233
HPDM Port Check Tool .....	233
Domain Name Resolution .....	234
Repositories .....	235
Wake on LAN .....	237
PXE-Based Imaging .....	238
LDAP Integration .....	239
Appendix A: Database Schema .....	241

Device Tables .....	241
dm_devices.....	241
dm_hash_extprop .....	242
dm_inv_display .....	242
dm_inv_ewf.....	243
dm_inv_hardware .....	243
dm_inv_max_hotfix .....	243
dm_inv_ms_hotfix .....	244
dm_inv_nic .....	244
dm_inv_partition.....	244
dm_inv_software .....	244
dm_inv_time.....	245
dm_group_values.....	245
dm_inv_ex_property.....	245
Device tables diagram .....	246
Grouping Tables .....	246
dm_group_attribute.....	246
dm_group_policy.....	246
dm_group_policy_extprop.....	247
dm_grouping_path.....	247
dm_grouping_schema.....	247
dm_manual_grouping.....	247
Grouping tables diagram .....	248
Rule and filter Tables.....	248
dm_rule .....	248
dm_schedule .....	249
dm_filter .....	249
dm_filter_fields.....	250
Rule and filter diagram.....	251
Template Tables .....	251
dm_unit_template.....	251
dm_basic_template.....	252
dm_favorite_temp .....	252
dm_report_template.....	252
dm_template_folder .....	252
Task Tables .....	253
dm_tasks .....	253
dm_subtasks .....	254
dm_task_temp .....	254
dm_tasklog.....	254
dm_task_error_msg.....	255
dm_device_subtasks.....	255



dm_snapshottask.....	255
dm_snapshottaskresult.....	255
Gateway Tables.....	255
dm_gateway.....	255
dm_gateway_walkingscope.....	256
dm_gateway_walkingtask.....	256
dm_gateway_walkingtaskresult.....	256
Repository Tables.....	257
dm_repositories.....	257
dm_repo_protocols.....	257
dm_repo_mapping.....	257
Privilege System Tables.....	258
dm_group.....	258
dm_group_sec_filter.....	258
dm_user.....	258
dm_user_sec_filter.....	259
dm_group_user.....	259
dm_auth_group.....	259
dm_template_privilege.....	259
dm_key.....	259
dm_keylog.....	259
dm_keyzero.....	260
Configuration Tables.....	260
dm_conf.....	260
dm_dbversion.....	260
dm_ipscope.....	260
dm_network_alias.....	260
dm_os_types.....	260
dm_ldap_setting.....	260
Auditlog Tables.....	261
dm_event.....	261
Deprecated tables.....	261
Accessing the database.....	262
Generate device information.....	262
Generate all device inventory information.....	262
Generate unsuccessful task information.....	263
Display the task count grouped by task status.....	263
Appendix B: Additional Configuration Options.....	264
Configuring HPDM Server.....	264
Accessing the Server configuration file.....	264
Thread settings.....	264
Port settings.....	264

Poll settings .....	264
Task settings .....	265
SSL settings .....	265
Cache settings .....	265
Configuring HPDM Gateway .....	266
Configuring HPDM Agent.....	267
Configuring HP WES clients .....	267
HPDM Agent parameters .....	270
HPDM Agent configurations .....	270
Appendix C: Configuring DHCP tags.....	271
Configuring a DHCP server for use with PXE.....	271
Configuring a DHCP server with the HPDM Server installed on a different machine.....	271
Configuring a DHCP server with the HPDM Server installed on the same machine.....	271
Configuring a DHCP server on Linux.....	272
Configuring options 202 and 203 .....	272
Configuring options for scopes (scope options).....	273
Appendix D: Configuring a device to boot from PXE .....	274
Changing the boot order locally .....	274
Changing the boot order remotely .....	274
Windows .....	274
HP ThinPro .....	275

## 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 state 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 GUI for administrators, allowing the inventory and management of devices and other administrative activities.
- **HPDM Console Web Bridge**—This component 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 table below defines common terminology used when working with HP Device Manager.

Term	Definition
HPDM Server	The central management service, which monitors all state 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	This component provides access to a subset of 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 the configuration files, master repository contents and database 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

#### HPDM Server requirements

Component	Requirements
Operating system	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
Third-party software	OpenJDK 11.0.3 (bundled with installer) One of the following database management systems (DBMS): Microsoft® SQL Server 2016 or later PostgreSQL 10.4.1 (bundled with installer)
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 1 GB RAM 2 GB free disk space

#### HPDM Gateway requirements

Component	Requirements
Operating system	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 1 GB RAM 2 GB free disk space

#### HPDM Master Repository Controller requirements

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

Operating system	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 1 GB RAM 4 GB free disk space <b>NOTE:</b> The above hardware is the minimum required for the Master Repository. If there will be a large number of imaging or file-copying operations, then HP recommends using a more powerful system with 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

### HPDM HTTPS Repository requirements

Component	Requirements
Operating system	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 2 GB RAM 2 GB free disk space 7200 RPM disk <b>NOTE:</b> The above hardware is the minimum required for the Master Repository. If there will be a large number of imaging or file-copying operations, then HP recommends using a more powerful system with additional free disk space.
Protocol	HTTPS

### HPDM Console requirements

Component	Requirements
Operating system	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows 10
Third-party software	OpenJDK 11.0.3 (bundled with installer)
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 1 GB RAM 1 GB free disk space

### HPDM Console Web Bridge requirements

Component	Requirements
Operating system	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 1 GB RAM

2 GB free disk space

### HPDM Configuration Center requirements

Component	Requirements
Operating system	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows 10
Hardware	Intel® compatible 64-bit processor supporting 2 or more CPU cores 2 GB RAM (For 1 Console instance and Console Web Bridge server. Add 1 GB for each additional Console) 1 GB free disk space

### 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 of this Guide 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.

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

Model	Windows 10 IoT Enterprise (64-bit)	Windows Embedded Standard 7P (64-bit)	Windows Embedded Standard 7E (32-bit)	HP ThinPro 7	HP ThinPro 6	HP ThinPro 5
HP t730 Thin Client	●	●		●	●	●
HP t630 Thin Client	●		●	●	●	
HP t628 Thin Client	●		●	●	●	
HP t620 PLUS Flexible Thin Client	●	●	●	●	●	●
HP t620 Flexible Thin Client	●	●	●	●	●	●
HP t530 Thin Client	●		●	●	●	
HP t520 Flexible Thin Client	●	●	●	●	●	●
HP t430 Thin Client	●			●	●	

HP t420 Thin Client		●	●	●	●
HP t240 Thin Client		●			
HP mt45 Mobile Thin Client	●		●		
HP mt44 Mobile Thin Client	●				
HP mt43 Mobile Thin Client	●				
HP mt42 Mobile Thin Client	●	●			
HP mt31 Mobile Thin Client	●		●		
HP mt21 Mobile Thin Client	●		●	●	
HP mt20 Mobile Thin Client	●		●	●	
HP ThinPro PC Converter				○	
HP PC Converter for Windows	○				

## Server preparation

For this setup, you will need Windows Server 2012 R2 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 of this Guide.

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

This chapter focuses on the post-installation steps of installing HPDM onto Windows Server 2012 R2. 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

#### 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:

- FTP family protocols must be chosen for ThinPro5 non-cached imaging.
- SMBv2 must be chosen for WES 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 2012 R2, 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 2012 R2 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 located 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, enter 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, enter 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, enter 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, enter 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`

After following these steps, HPDM Server, HPDM Gateway and HPDM Agents can 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, please 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:

2. 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, enter 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, enter 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. 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:

3. Right-click **Start Menu button**, and then select **Command Prompt**. If not logged on as Administrator, be sure to select **Command Prompt (Admin)**.
4. 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`
5. Activate firewall application filter for FTP (aka Stateful FTP) that will dynamically open ports for data connections, enter the following command and then press **Enter**:  
`netsh advfirewall set global StatefulFtp enable`
6. 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, maybe you shall configure the port changes in the routers' firewall manually.



---

**Note:**

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

---

## Installation options

Beginning with Device Manager 5.0, the HP Device Manager installer is composed 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 you already have an older version (prior to 5.0) of HPDM 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 will install all the HPDM server-side components. The user doesn't need to configure anything during the installation and the user can use most of HPDM functions after the installation is finished, such as update agent, capture/deploy files, etc.

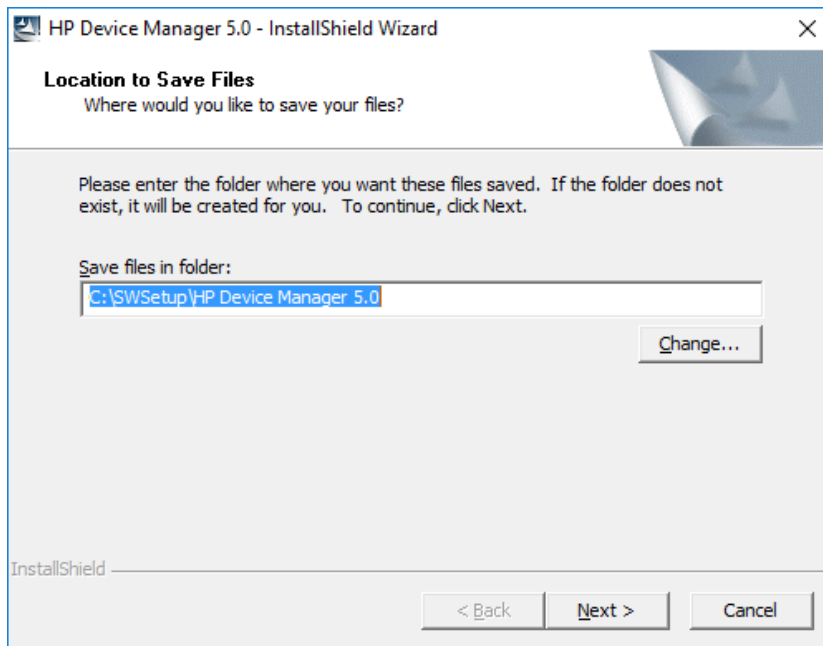
The following are the default settings for complete setup:

- 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 during initializing database, and the root user must change this random password at first logon.
- HPDM Server uses the local HTTPS Repository as its master repository and imports its randomly created user and password to database automatically.
- The check box of "Launch HPDM Configuration Center" is unchecked after installation.

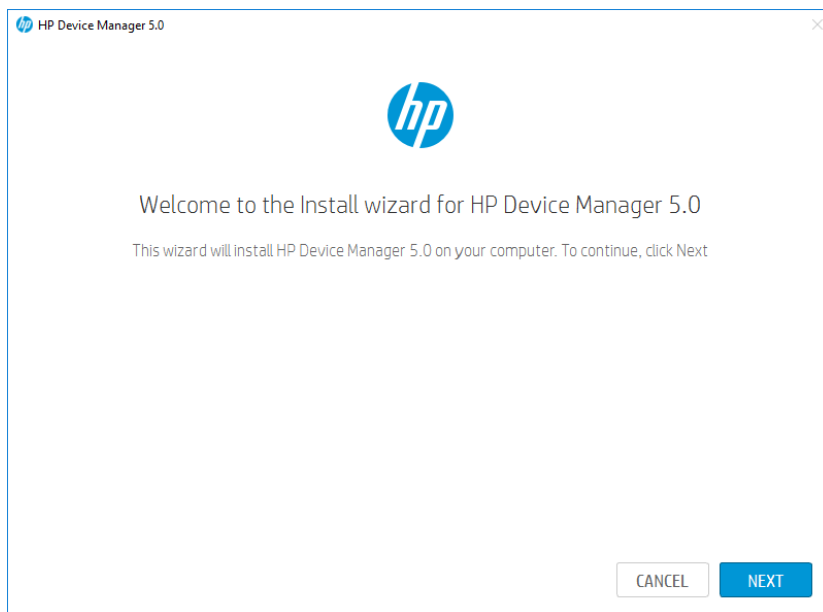
#### Custom Setup

This process will allow you to choose which Device Manager components are installed. When performing a custom installation over a previous Device Manager install, the HPDM Install process will attempt to preserve configuration settings from the previous HPDM installation instance. Otherwise, it is recommended to use the HPDM Configuration Center utility to manage the Device Manager installation configuration. The following steps will guide a custom installation:

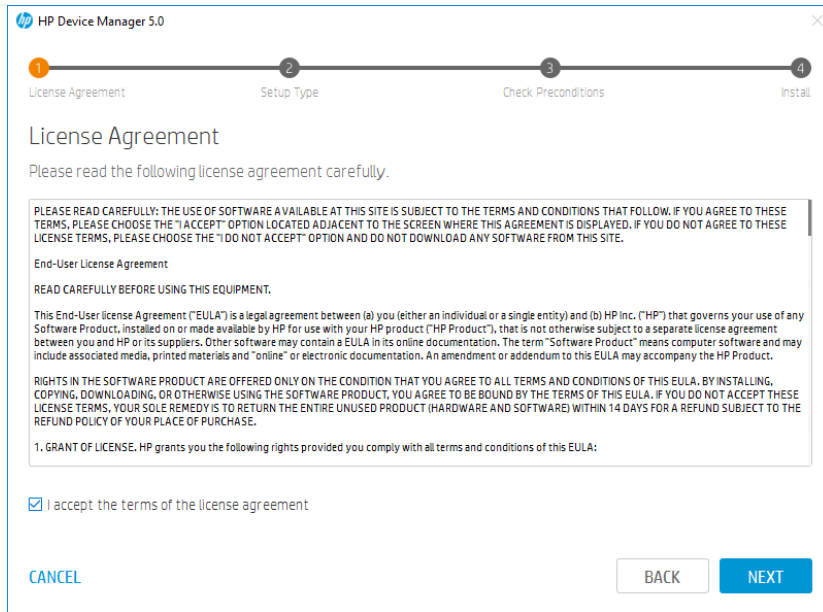
1. Double-click the HPDM setup file. If it pops up "User Account Control" dialog, select **Yes**.
2. Select the "Location to Save Files", and then click **Next**.
  - This is the location to save the extracted files from the installation package, instead of the installation path of HP Device Manager. Such as the component installers.



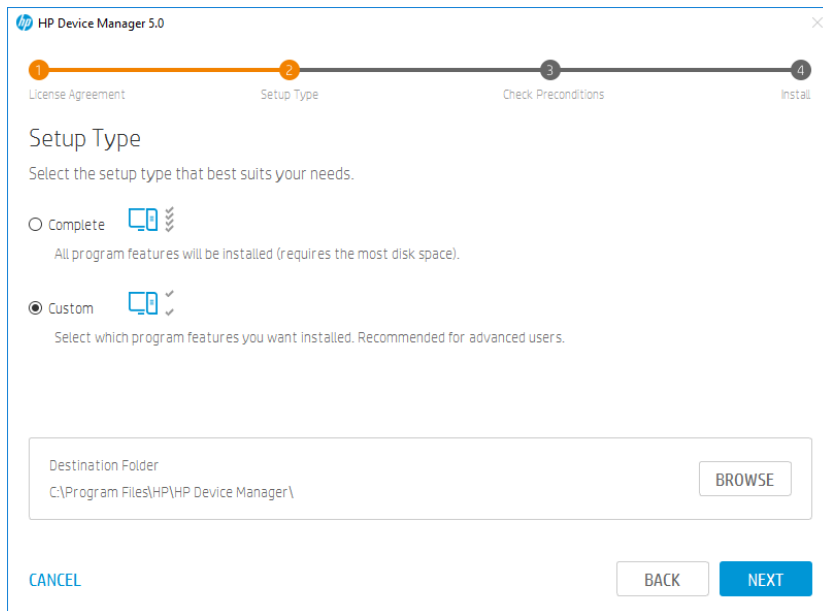
- 
- 3. If the “Overwrite Protection” dialog is popped up during extracting files, select **Yes to All**.
- 4. Click **Next**.



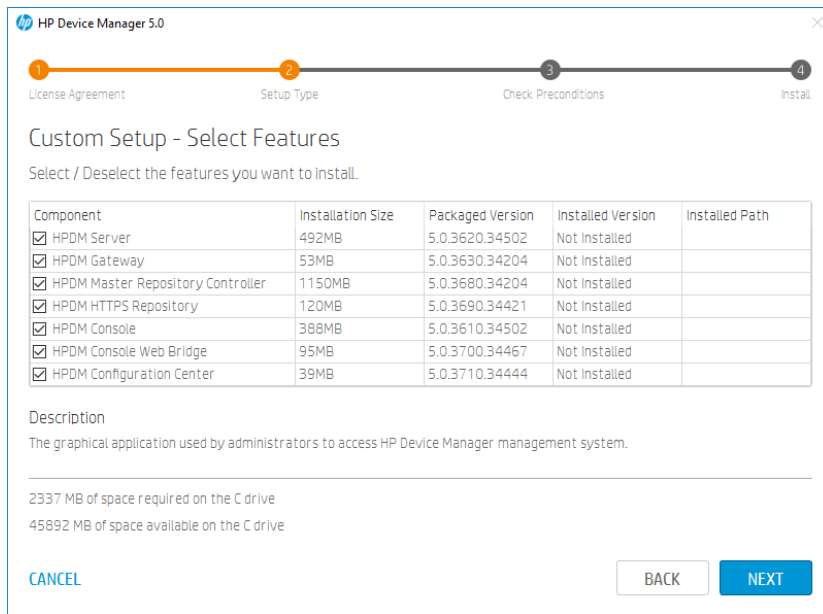
- 
- 5. Check “I accept the terms of the license agreement”, and then click **Next**.



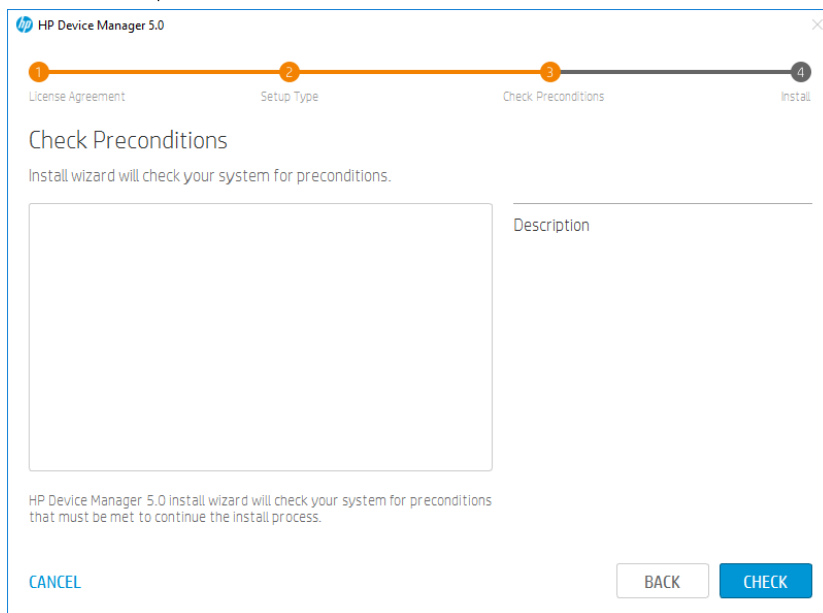
6. Select **Custom** setup type and choose the destination folder, this is the installation path of HP Device Manager.



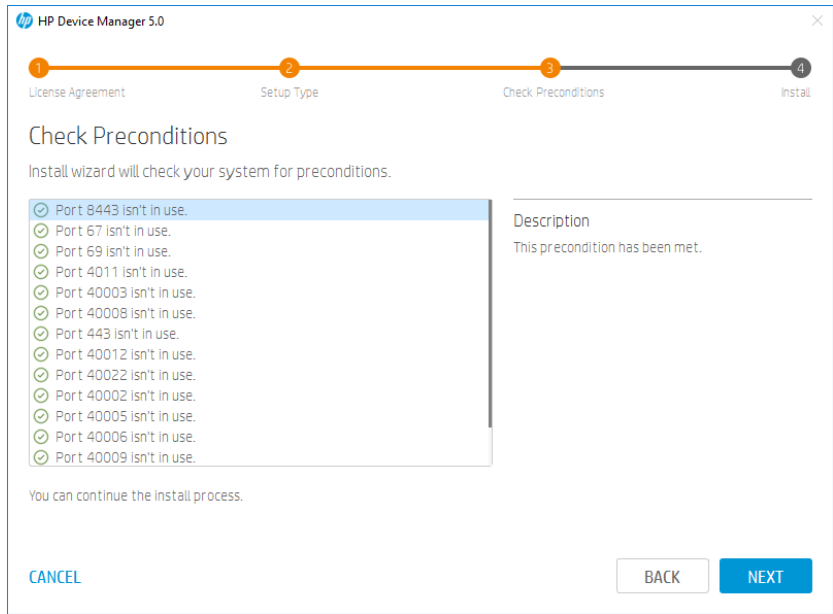
7. Select the components you want to install, and then click **Next**. Please note that the dependent components will be selected automatically when you select a component, and you cannot deselect a component **A** when there is another component **B** is selected and component **B** depends on component **A**.



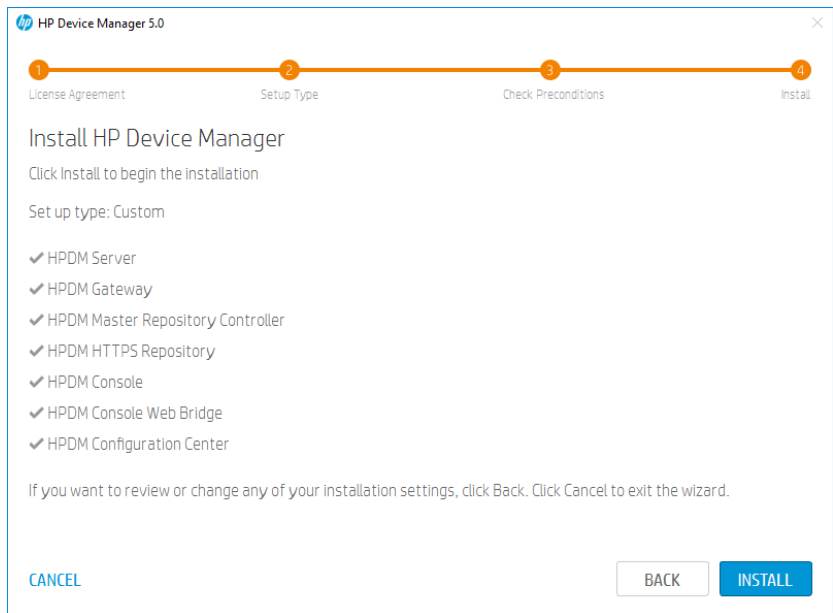
- Click **Check** to check preconditions.



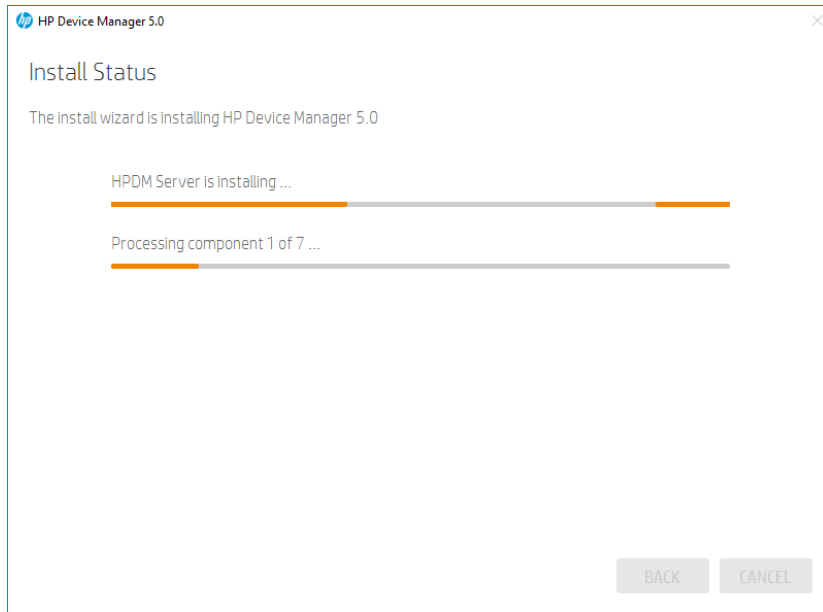
- If all preconditions are met, click **Next**. If there are any unmet preconditions, please view the detailed description to resolve them manually, then click **Check** to check again.



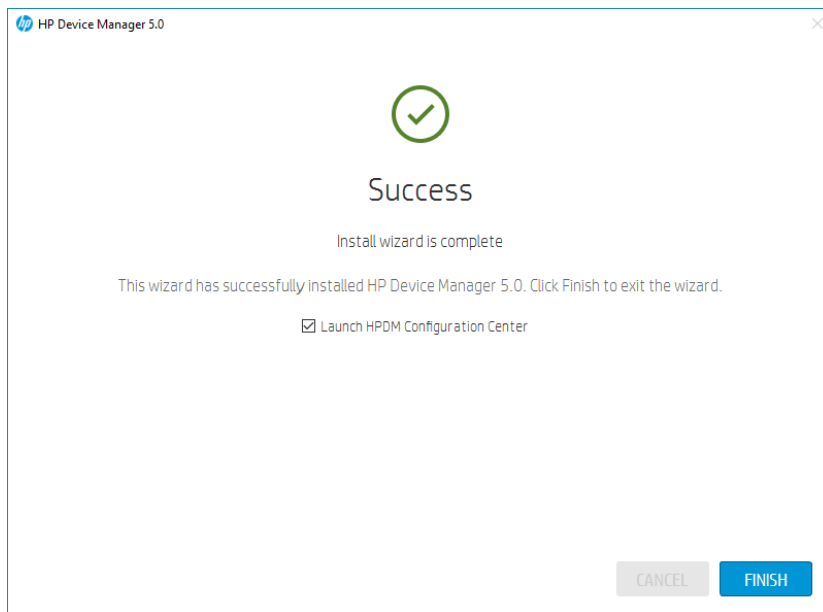
10. View the installation settings summary, and then click **INSTALL**.



11. Installing.



- 
- 12. Click **Finish** to finish this installation. If “**Launch HPDM Configuration Center**” is checked, the HPDM Configuration Center will be opened. See HPDM Configuration Center section to view how to configure HPDM components.



---

**Note:**

- If the HPDM Server, HPDM Master Repository Controller and HPDM HTTPS Repository aren't installed on the same machine, you need to reset the user account of HPDM HTTPS Repository and its password via HPDM Configuration Center. If the HPDM Server and HPDM Console aren't installed on the same machine, you need to reset the password of HPDM root user via HPDM Configuration Center before you log in HPDM Console.
- 

**Updating an Existing Installation**

HP Device Manager 5.0 enables a new streamlined installation process that differs from previous versions of HPDM. As the first product to enable this improved installation experience, updates do not yet exist. We will provide updated instructions for this process as HPDM 5.0 service packs become available.

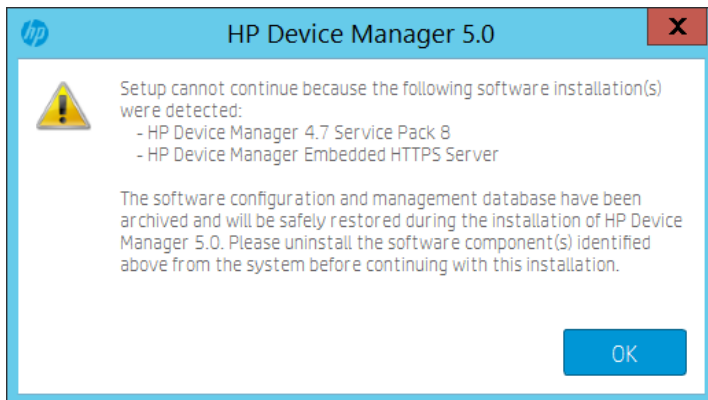
### Upgrading a Previous Installation

HPDM 5.0 provides instructional steps for upgrading from HPDM 4.7 or 4.7 Service Packs. For HPDM versions prior to 4.7, you will need to upgrade your installation to HPDM 4.7 before attempting an upgrade to HPDM 5.0.

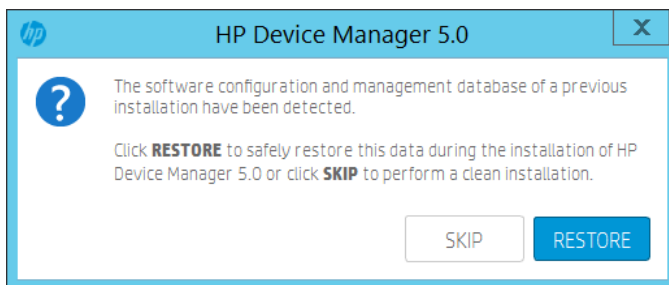
#### Device Manager 4.7 or Service Packs

To upgrade Device Manager 4.7 or Service Packs to HPDM 5.0:

1. Double-click the HPDM setup file. If it pops up “User Account Control” dialog, select **Yes**.
2. Select the “Location to Save Files”, and then click **Next**.
3. Click **OK** when the following warning dialog is popped up.



4. Manually uninstall the software component(s) listed on above warning dialog.
  5. Run HPDM 5.0 installer again or go to the location you selected at step 2 and run **HPDMSetup.exe**.
- Click **Restore**.



- The following steps are same with the new installation.

---

#### Note:

- If the HPDM Server uses SQL Server Database with Windows Authentication, you need to re-configure the logon account and password of HPDM Server service after installation.
- If there is only the old HPDM Embedded HTTPS Server is installed, for example it is just a child repository, we recommend that you upgrade it with the new HPDM HTTPS Repository component installer. About the component installer, see **HPDM Component Installers**.

For HPDM 4.7 or Service Packs, you only can upgrade it using the HP Device Manager installer.

---

#### Device Manager versions Prior to 4.7

HPDM 5.0 does not support upgrading from HPDM versions prior to 4.7 directly. To upgrade HPDM versions prior to 4.7, please upgrade the current HPDM to 4.7 before attempting to upgrade to HPDM 5.0.

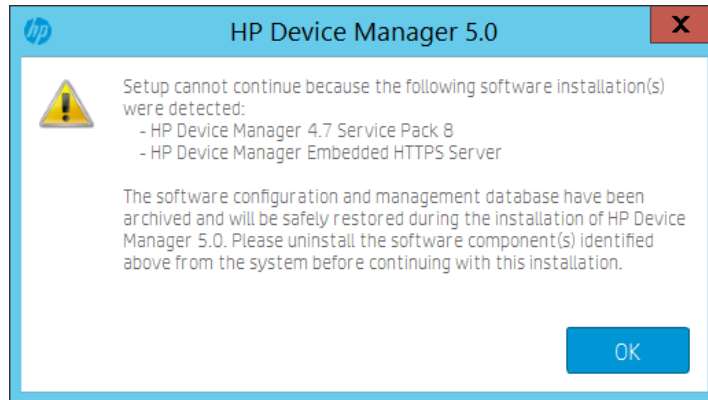
### Migrating HP Device Manager 4.7 data to a new machine and upgrading

The supported operating systems matrix for HPDM 5.0 may differ from the operating system of the previous HPDM installation, if the currently installed HPDM is running on an operation system that is not included in the HPDM 5.0 system requirements, you need to install HPDM 5.0 on another system or update the operating system prior to installing HPDM. This section will guide you through the steps required to migrate the current HPDM data to a new machine and upgrade it to HPDM 5.0.

#### Backup current HPDM 4.7 data

To back up current HPDM 4.7 data:

1. Go to the machine that HPDM 4.7 installed and copy HP Device Manager 5.0 installer to this machine.
2. Run HP Device Manager 5.0 installer. If it pops up “User Account Control” dialog, select **Yes**.
3. Select the “Location to Save Files”, and then click **Next**.
4. Click **OK** when the following warning dialog is popped up.



5. The backup data is saved at “C:\SWSetup\HPDMMBackup”. This is a fixed location and cannot be configured.

#### Move the backup data to new machine

To move the backup data to new machine:

1. Copy the folder “C:\SWSetup\HPDMMBackup” from current machine to new machine, the path and the folder structure cannot be changed.
2. If HPDM Master Repository Controller is installed on original machine, you also need to copy the whole repository to the new machine, the path and the folder structure cannot be changed.
3. Copy the following text to a txt file and change the file extension to .reg, then double click this reg file to import the registry key.

*Windows Registry Editor Version 5.00*

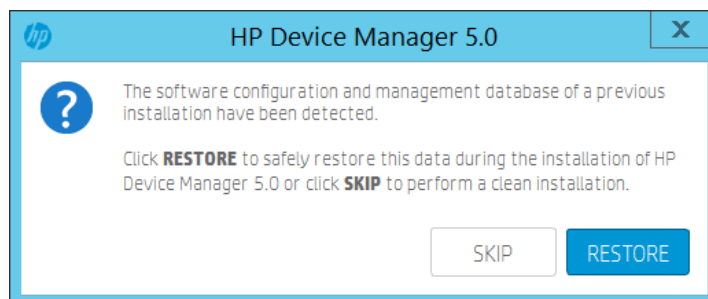
*[HKEY\_LOCAL\_MACHINE\SOFTWARE\HP\HP Device Manager]*

*"Backup"="yes"*

#### Install HPDM 5.0 on new machine

To install HPDM 5.0 on new machine:

1. Copy HP Device Manager 5.0 installer to the new machine and run it. If it pops up “**User Account Control**” dialog, select **Yes**.
2. Select the “Location to Save Files”, and then click **Next**.
3. Click **Restore**.



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



---

**Note:**

If you move the master repository to new machine, you need to re-configure the repository settings after new installation.

---

**Uninstalling HP Device Manager**

To uninstall all installed HP Device Manager components:

6. Go to the “Location to Save Files” that selected during installation. By default, the location is “C:\SWSetup\HP Device Manager 5.0\”.
7. Run the script **uninstall.cmd**. If not logged on as Administrator, be sure to right click and select **Run as administrator**.
  - To uninstall an individual component:
    1. Go to the **Control Panel > Programs and Features**.
    2. Select the component that you want to uninstall from the programs list, uninstall it.

**HPDM Component Installers**

Beginning with Device Manager 5.0, the HP Device Manager 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 one by one.

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*

Though each component has an individual component installer, only the HP Device Manager installer is released on HP Website. You can get the component installers after installing or extracting the HP Device Manager installer. All component installers locate at the “Location to save Files” that you selected during installing HP Device Manager. By default, the location is “C:\SWSetup\HP Device Manager 5.0\”.

---

**Note:**

1. This location isn't the installation path of HP Device Manager. If you just want to get the component installers, you can just extract the HP Device Manager installer, instead of installing the HP Device Manager.
- 

To extract the HP Device Manager installer:

1. Run the HP Device Manager installer.
2. Select the “Location to Save Files” and click **Next**.
3. After the “Welcome to the install wizard for HP Device Manager 5.0” dialog appears, click **CANCEL**.

*Installing HPDM Component with component installer*

Each component installer only supports silent installation, there is no user interface for the component installer. You can install a component with default installation path and configuration by double clicking the component installer or install a component with command line. For the detailed command line parameters, see following sections.

---

**Note:**

1. Please check whether the **Microsoft Visual C++ 2015 Redistributable (x64)** is installed or not on the target machine before installing a component with component installer. If it isn't installed, please install it at first. The installer file of this redistributable is included in HP Device Manager installer, it locates at the same location with the component installer and the name is **VC\_redist.x64.exe**.

If you want to configure the component that you installed, please install HPDM Configuration Center after you install the desired 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 installation path is "C:\Program Files\HP\HP Device Manager".

START: Starts HPDM Server service or not after installation. 1 means start, 0 means not start. The default value is 1.

---

#### **Note:**

An initial database is created when the HPDM Server service starts and no database is configured. In this scenario, a random password is created for the root user. You need to reset the password or re-create 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 or not after installation. 1 means start, 0 means not start. The default value 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 repository is "%ProgramData%\HP\HP Device Manager\HPDM", this path cannot be changed during installing. You can change it via 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:**

1. If the HPDM Master Repository Controller is installed on the machine, the installation process will set the location of the repository as the root path of HTTPS Repository. Otherwise, the default root path of repository is “%ProgramData%\HP\HP Device Manager\HPDM”.
  2. A random user and password are created during installation, you need to reset them after installation via HPDM Configuration Center.
  3. This component installer can be used to upgrade the old HPDM Embedded HTTPS Server when no other HPDM component is installed. Just double click HPDMHTTPSRepository.exe or run the following command. All configuration will be restored after upgrading.  
HPDMHTTPSRepository.exe /hide\_progress
- 

### **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:**

This component can only be installed on a system where the HPDM Console is installed and must be installed in the same installation path as the installed HPDM Console component. The installation process will stop when it doesn't detect that HPDM Console is installed. So please install HPDM Console at first when you want to install this component.

---

### **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:**

If you want to configure other components after installation, you must install this component.

---

## **Deployment**

### **Overview**

This part is to assist customers who are planning the architecture of HP Device Manager (HPDM) components and configuring those components for the number of devices that will be managed. It focuses on managing larger device deployments using HPDM. It also includes tips to fine-tune the performance of HPDM.

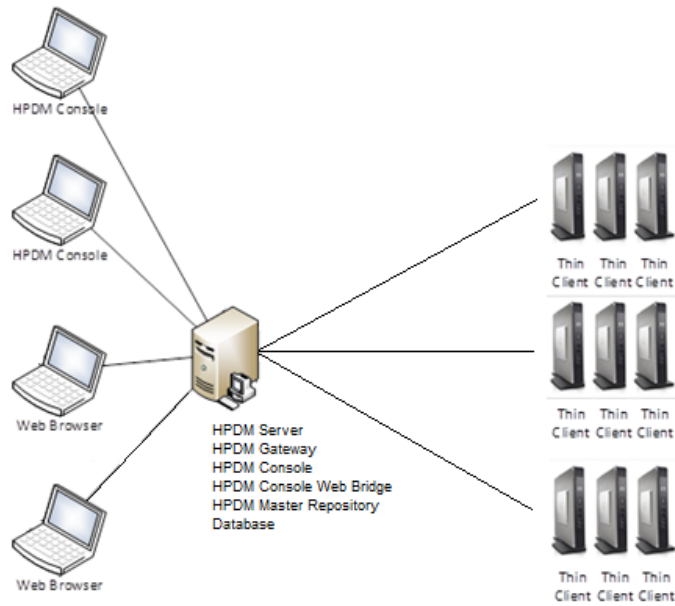
After the installation of HPDM, it can be divided into the following components:

- 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

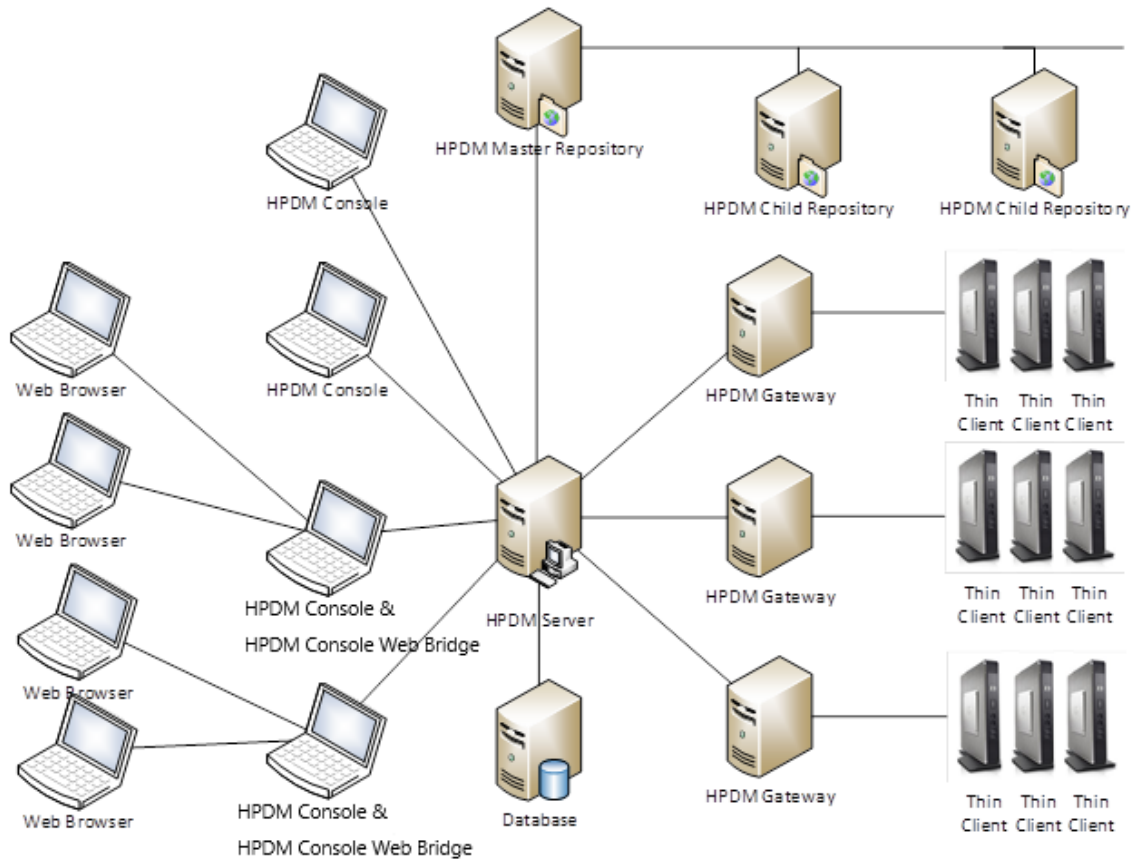
### **Typical Device Manager topology**

The following diagrams show the topology of 22 HPDM deployments.

**Figure 1.** Topology of a common HPDM deployment



**Figure 2.** Topology of a typical HPDM deployment

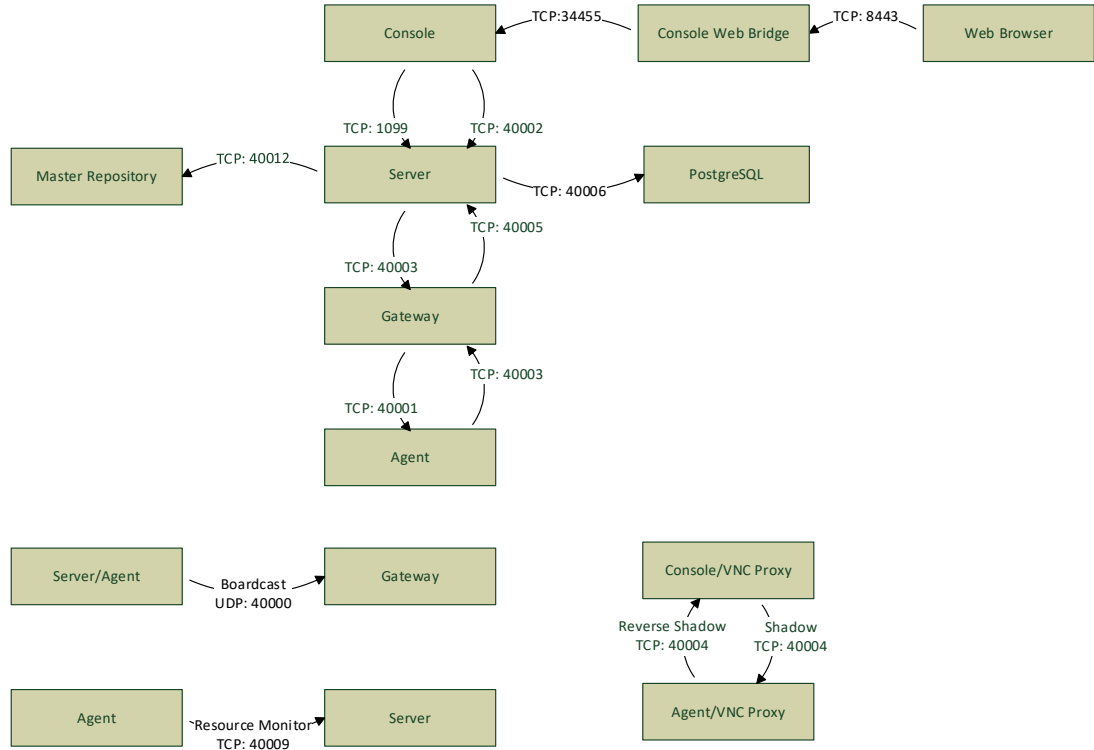


**Note**

If you want to generate templates through 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

**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 hijacked by other processes.

### 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, this port can be modified in the configuration center.
34455	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)

In addition, each time the web browser opens a web console, a session is created, and two ports are dynamically created. And the value of the port is not fixed.

### Console ports (outbound)

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

### 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.

### 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

### Gateway ports (inbound)

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



40008	HPDM Gateway	HPDM Gateway Controller	TCP	Allows HPDM Gateway to notify HPDM Gateway Controller there are other gateways running in the same subnet
-------	--------------	-------------------------	-----	---

### Gateway ports (outbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Gateway	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	HPDM Gateway	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
68	HPDM PXE Server (bundled with HPDM Gateway)	HPDM Imaging Mini Linux Tool (client-side)	UDP	PXE bootstrap
137	HPDM Gateway	NetBIOS Name Service	UDP	Allows NetBIOS Name Resolution
138	HPDM Gateway	NetBIOS Datagram Service	UDP	Allows NetBIOS Datagram transmission and reception
139	HPDM Gateway	NetBIOS Session Service	TCP	Allows NetBIOS Session Services connections
443	HPDM Gateway	HPDM Embedded HTTPS Server	TCP	This is the default port for HTTPS (used for repositories). HTTPS ports can be configured via HPDM Console. If you do not use the default port, configure the firewall appropriately.
445	HPDM Gateway	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
989 & 990	HPDM Gateway	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.
40001	HPDM Gateway	HPDM Agent	TCP	Allows HPDM Gateway to send tasks to HPDM Agent
40001	HPDM Gateway	HPDM Agent	UDP	Allows HPDM Agent to receive replies of broadcasting from HPDM Gateway
40005	HPDM Gateway	HPDM Server	TCP	Allows HPDM Gateway to send reports to HPDM Server

40008	HPDM Gateway	HPDM Gateway Controller	TCP (loopback)	Allows HPDM Gateway to notify HPDM Gateway Controller there are other gateways running in the same subnet
-------	--------------	-------------------------	----------------	---

### 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)

### Agent ports (outbound)

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

67	PXE client (client-side)	HPDM PXE server (bundled with HPDM Gateway)	UDP	PXE bootstrap
67	HPDM Agent	DHCP server	UDP	Allows HPDM Agent to send DHCP option requests
69	PXE client (client-side)	HPDM PXE server (bundled with HPDM Gateway)	UDP	TFTP (Trivial File Transfer Protocol)
137	HPDM Agent	NetBIOS Name Service	UDP	Allows NetBIOS Name Resolution
138	HPDM Agent	NetBIOS Datagram Service	UDP	Allows NetBIOS Datagram transmission and reception
139	HPDM Agent	NetBIOS Session Service	TCP	Allows NetBIOS Session Services connections
443	HPDM Agent	HPDM Embedded HTTPS Server	TCP	This is the default port for HTTPS (used for repositories). HTTPS ports can be configured via HPDM Console. If you do not use the default port, configure the firewall appropriately.
445	HPDM Agent	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes
5500	VNC Server on the thin client  Windows: TightVNC (bundled with HPDM Agent)  HP ThinPro: X11VNC (bundled with platform)	SSL VNC Proxy (bundled with HPDM Agent)	TCP (loopback)	SSL VNC Proxy in Listen Mode (reverse VNC)
5900	SSL VNC Proxy (bundled with HPDM Agent)	VNC Server on the thin client 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.
-------	------------	-------------	-----	---

### Repository ports (inbound)

Receiver port	Sender	Receiver	Protocol	Purpose
20 & 21	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	FTP server (third-party software)	TCP	These are the default ports for FTP (used for repositories). Port 20 is for data transfer and port 21 is for listening to commands. FTP ports can be configured via HPDM Console. If you do not use the default ports for your FTP server, please configure the firewall appropriately.
22	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	SFTP server (third-party software)	TCP	This is the default port for SFTP (used for repositories). SFTP ports can be configured via HPDM Console. If you do not use the default port for your SFTP, please configure the firewall appropriately.
137	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	NetBIOS Name Service	UDP	For File and Printer Sharing to allow NetBIOS Name Resolution  This is required for Shared Folder.
138	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	NetBIOS Datagram Service	UDP	For File and Printer Sharing to allow NetBIOS Datagram transmission and reception This is required for Shared Folder.
139	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	NetBIOS Session Service	TCP	For File and Printer Sharing to allow NetBIOS Session Service connections  This is required for Shared Folder.
443	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	HPDM Embedded HTTPS Server	TCP	This is the default port for HTTPS (used for repositories). HTTPS ports can be configured via HPDM Console. If you do not use the default port, configure the firewall appropriately.

445	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	Microsoft Directory Services	TCP	For File and Printer Sharing to allow Server Message Block transmission and reception through Named Pipes  This is required for Shared Folder.
989 & 990	HPDM Console HPDM Gateway HPDM Agent HPDM Master Repository Controller	FTPS server (third-party software)	TCP	These are the default ports for FTPS (used for repositories). Port 989 is for data transfer and port 990 is for listening to commands. FTPS ports can be configured via HPDM Console. If you do not use the default ports for your FTPS server, please configure the firewall appropriately.
40012	HPDM Server	HPDM Master Repository Controller	TCP	Allows HPDM Server to communicate with HPDM Master Repository Controller to manage the HPDM Master Repository (this port is for the HPDM Master Repository only)

### Repository ports (outbound)

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

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

## 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 1.** System requirements

HPDM component	Operating system	Suggested minimum hardware
<b>HPDM Console</b>	– Windows Server 2012 R2	– Intel® compatible 64-bit processor supporting 2 or more CPU cores
	– Windows Server 2016	– 1 GB RAM
	– Windows Server 2019	– 1 GB free disk space
	– Windows 10	
<b>HPDM Server</b>	– Windows Server 2012 R2	– Intel® compatible 64-bit processor supporting 2 or more CPU cores
	– Windows Server 2016	– 1 GB RAM
	– Windows Server 2019	– 2 GB free disk space
<b>HPDM Configuration Center</b>	– Windows Server 2012 R2	– Intel® compatible 64-bit processor supporting 2 or more CPU cores
	– Windows Server 2016	– 1 GB RAM
	– Windows Server 2019	– 1 GB free disk space
	– Windows 10	
<b>HPDM Gateway</b>	– Windows Server 2012 R2	– Intel® compatible 64-bit processor supporting 2 or more CPU cores
	– Windows Server 2016	– 1 GB RAM
	– Windows Server 2019	– 2 GB free disk space
<b>HPDM Master Repository Controller</b>	– Windows Server 2012 R2	– Intel® compatible 64-bit processor supporting 2 or more CPU cores
	– Windows Server 2016	– 1GB RAM
	– Windows Server 2019	– 2 GB free disk space
NOTE: The above hardware is the minimum required for the Master Repository. If there will be a large number of imaging or file-copying operations, then HP recommends using a more powerful system that has free available disk space.		
<b>HPDM HTTPS Repository</b>	– Windows Server 2012 R2	– Intel® compatible 64-bit processor supporting 2 or more CPU cores
	– Windows Server 2016	– 2 GB RAM
	– Windows Server 2019	– 2 GB free disk space – 7200 RPM disk
NOTE: The above hardware is the minimum required for HPDM Embedded HTTPS Server. If there will be a large number of imaging or file transfer-operations, then HP recommends using a more powerful system that has free available disk space.		

<b>HPDM Console Web Bridge</b>	-	Windows Server 2012 R2	-	Intel® compatible 64-bit processor supporting 2 or more CPU cores
	-	Windows Server 2016	-	1.5 GB RAM (For 1 Console instance and Console Web Bridge server. Add 1 GB for each additional Console)
	-	Windows Server 2019	-	
	-	Windows 10	-	1 GB free 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.** Recommended size reserved for repository

Device Operating System	Minimum Recommended Size
Windows 10 IoT Enterprise	8GB
Windows Embedded Standard 7 Professional	5GB
Windows Embedded Standard 7 Enterprise	5GB
HP ThinPro 7	1GB
HP ThinPro 6	1GB
HP ThinPro 5	1GB

### Network infrastructure

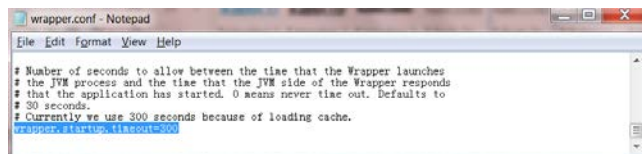
There are many network factors that might influence the deployment of HPDM, such as the network bandwidth or whether HPDM components are deployed on one or more subnets. Some companies might have different network strategies, such as devices are required to be in a NAT environment, or devices are required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

To manage large-scale deployments, HP recommends having the HPDM Server and the HPDM Gateway services installed on 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. It causes obvious delays for HPDM Console users if the network latency between the HPDM Server and database is higher than 30 milliseconds. In addition, HP recommends deploying a Child Repository as close to its related devices as possible.

### Note

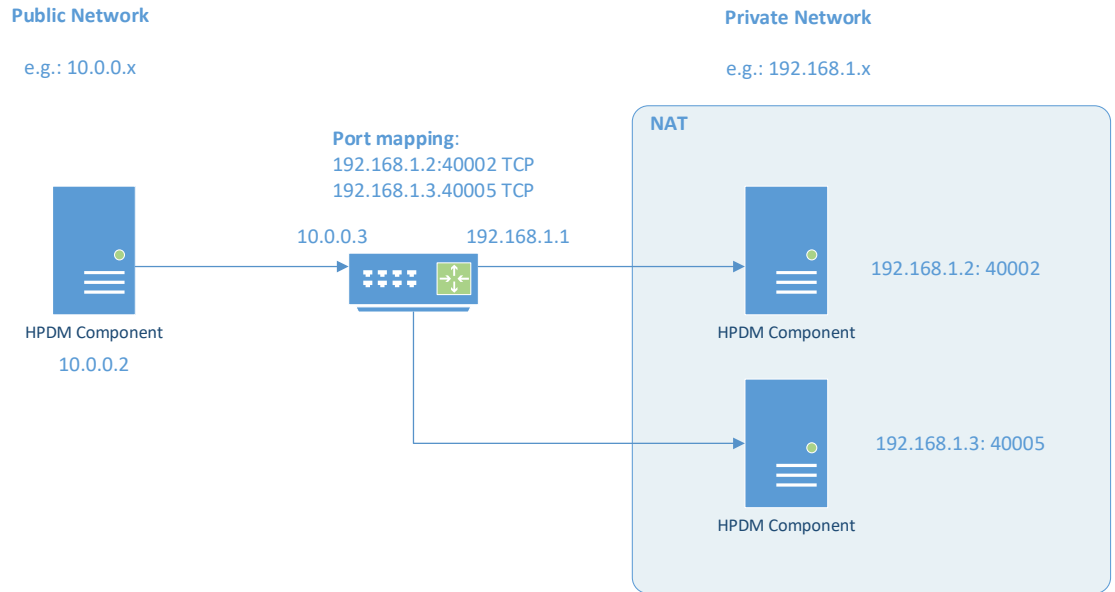
If latency is unavoidable, go to ...\\Server\\conf\\wrapper.conf, and increase the value of **wrapper.startup.timeout** in wrapper.conf on the HPDM Server side. The default value is 300 seconds. This makes the HPDM Server more tolerant to database latency.



*Network address translation (NAT)*

The physical network in which HPDM is deployed might be complex. When allocating components between two networks, such as a public network and private network, different NAT cases can be separated as 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, or inner, network can connect to the public, or outer, network and that applications on the public, or outer, network cannot connect to the private, or inner, network.

**Figure 4.** Topographical model of NAT environment





**Table 3.** Evaluated NAT scenarios

				With outer router ports mapped to inner ports <sup>5</sup>	Without outer router ports mapped to inner ports	
<b>HPDM Server</b>	HPDM Gateway	40000	UDP	Passed	N/A <sup>4</sup>	
	HPDM Gateway	40003	TCP	Passed		
	Master Repository Controller	40012	TCP	Passed	N/A	
<b>HPDM Console</b>	HPDM Server	1099	TCP	Failed <sup>2</sup>	N/A	
	HPDM Agent	40004	TCP	Failed <sup>2</sup>		
<b>HPDM Gateway</b>	HPDM Agent	40001	TCP	Passed	N/A <sup>3</sup>	
	HPDM Server	40005	TCP	Passed	N/A <sup>3</sup>	
	PCoIP Zero Client	50000	TCP	Failed	N/A	Only PCoIP-related tasks fail.
<b>HPDM Agent</b>	HPDM Gateway	40000	UDP	Passed	N/A <sup>4</sup>	
	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.

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

<sup>2</sup> To connect the HPDM Console to the HPDM Server successfully, do the following 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>`
- Restart the HPDM Server.

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

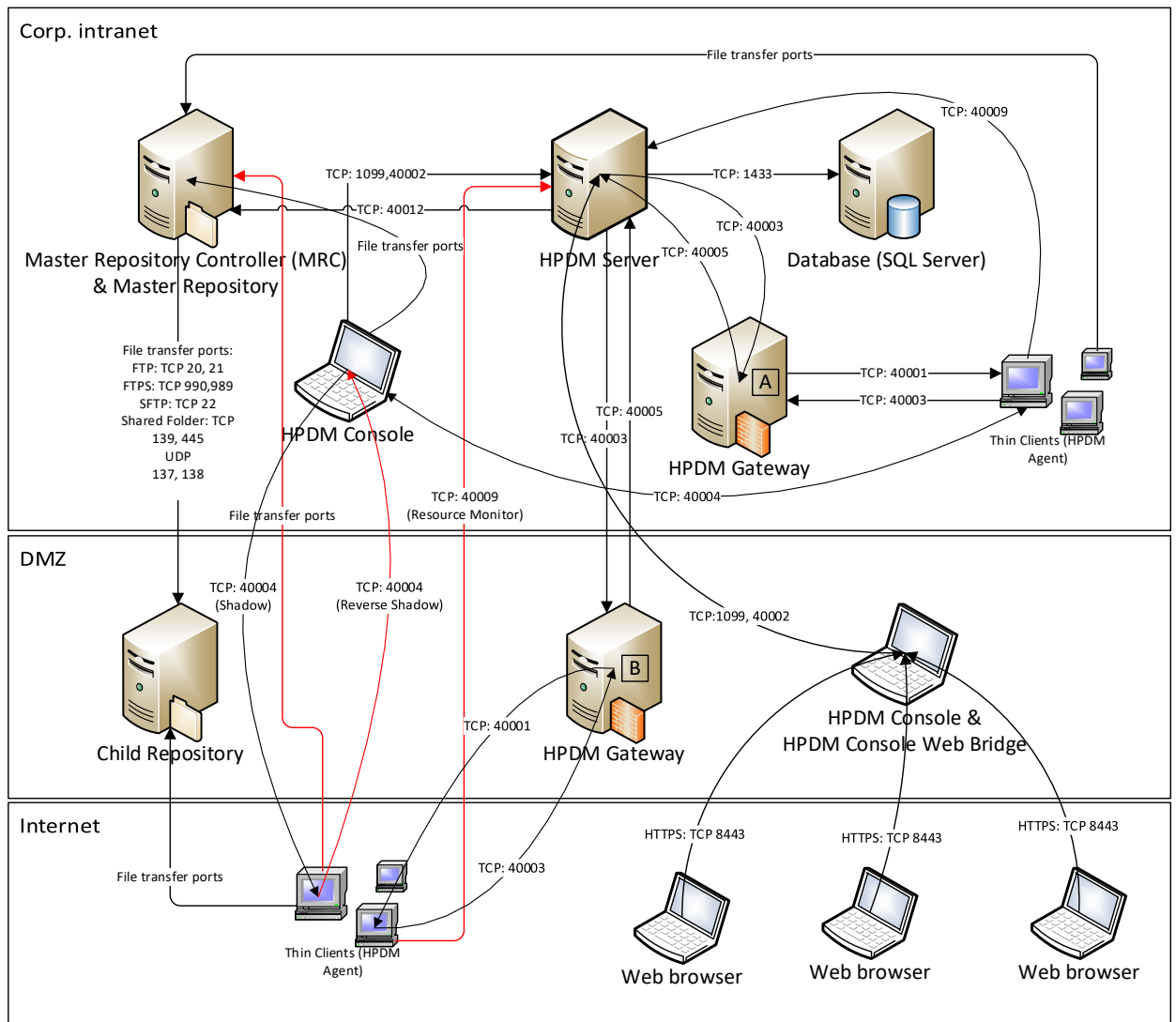
<sup>4</sup> Port 40000 is for HPDM poll mode only, and can be replaced by ports 40001 and 40005.

<sup>5</sup> 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*

You might want to use HPDM to manage devices located in both the corporate (intranet) network and the Internet. To enable this configuration, you must place an HPDM Gateway, an HPDM repository and an HPDM Console Web Bridge 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:**

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

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

If you install all HPDM Server-side components in the DMZ environment it usually makes the topology simpler; however, most companies have 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 ensure 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 ensure 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

In Figure 5, there are three red lines. These lines represent connections that cannot be resolved easily.

- 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.

If you can move all HPDM Server-side components to the DMZ environment, these issues can be resolved. However, you might not be able to use this configuration based on your security policy.

### Ports between networks

**Table 4.** 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

			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**

You do not need 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 Manager within F5 Network’s BIG-IP infrastructure.

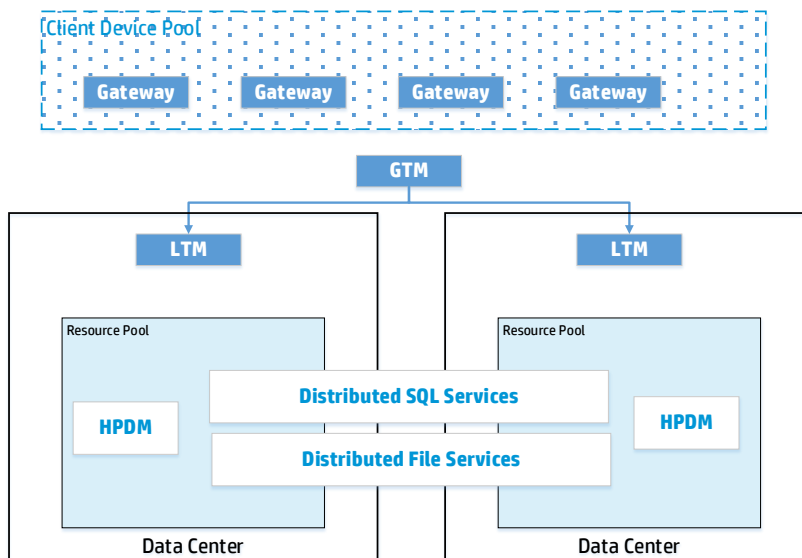
HPDM is a management solution that provides an easy-to-use interface and workflows that are streamlined for the management of HP thin clients. HPDM is a highly scalable management solution for thin clients. HPDM can scale from managing thousands of devices to over a hundred thousand devices, all on a single management server.

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.



In this model, F5’s 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 are used to monitor the availability of and provide access to resources within each data center. The local traffic manager does this by managing the resources available, in our case, 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. This VM can also be used to create local redundancy within each data center by being able to support 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 can be configured for high availability.
- Be sure that both data centers have access to the same user level; typically, this access can be configured 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*

We have presented a scenario demonstrating where additional fault tolerance and disaster recovery support for HPDM can be achieved through data center redundancy using F5 Network's BIG-IP infrastructure. While this example does not take into account all environments or customer implementations of BIG-IP or similar software-defined networking infrastructure, it does demonstrate the basic requirements for implementing redundancy with HPDM.

### **Number of devices**

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

Current customers 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 of where Device Manager's implementation logic might influence the deployment. See 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 HPDM Consoles connected to an HPDM Server. From 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 re-imaged 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 certificate for HPDM Console Web Bridge*

An example is as follows:

1. Generate keystore.jks and truststore.jks
  - Perform the following command to generate a pfx format file:

```
openssl pkcs12 -export -clcerts -in client.crt -inkey client.key -out client.pfx
```

Once prompted, enter the passwords required.

- Perform the following command to generate keystore.jks  
keytool -importkeystore -destkeystore "keystore.jks" -srckeystore client.pfx -srcstoretype PKCS12  
Once prompted, enter the passwords required.
- Perform the following commands to generate truststore.jks:  
keytool -import -file firstCA.cert -alias firstCA -keystore trustStore.jks  
keytool -import -file secondCA.cert -alias secondCA -keystore trustStore.jks  
keytool -import -file thirdCA.cert -alias thirdCA -keystore trustStore.jks  
Once prompted, enter the passwords required.

2. Edit jetty.properties under webswing folder. Four settings need to be modified if necessary:  
org.webswing.server.https.truststore  
org.webswing.server.https.truststore.password  
org.webswing.server.https.keystore  
org.webswing.server.https.keystore.password

Figure 6. jetty configuration file

```

1 org.webswing.server.host=0.0.0.0
2
3 org.webswing.server.http=false
4 org.webswing.server.http.port=8080
5
6 org.webswing.server.https=true
7 org.webswing.server.https.port=8443
8 org.webswing.server.https.truststore=ssl/truststore.jks
9 org.webswing.server.https.truststore.password=hpdmwebconsole
10 org.webswing.server.https.keystore=ssl/keystore.jks
11 org.webswing.server.https.keystore.password=hpdmwebconsole

```

3. Replace keystore.jks, truststore.jks with your own files under webswing\ssl folder.

Figure 7. certificate files

Name	Date modified	Type	Size
keystore.jks	4/8/2019 1:21 AM	JKS File	3 KB
truststore.jks	4/8/2019 1:21 AM	JKS File	2 KB

### Simultaneously connected users

There is no significant increase of memory or CPU usage on HPDM Server for any additional, connected HPDM Consoles. However, it requires more resources for database access and communication. Do not have too many connected HPDM Consoles.

## Deployment scenarios

The following are some typical scenarios.

Table 1. 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+

M15 SQL

---

---

**Note**

This 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.

---

*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 machine.

*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 machine. 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 it as multiple Normal scale deployments to deploy.

## Cloud deployments

**Deploying to Amazon EC2**

HP Device Manager (HPDM) is a device management tool capable of working 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.

---

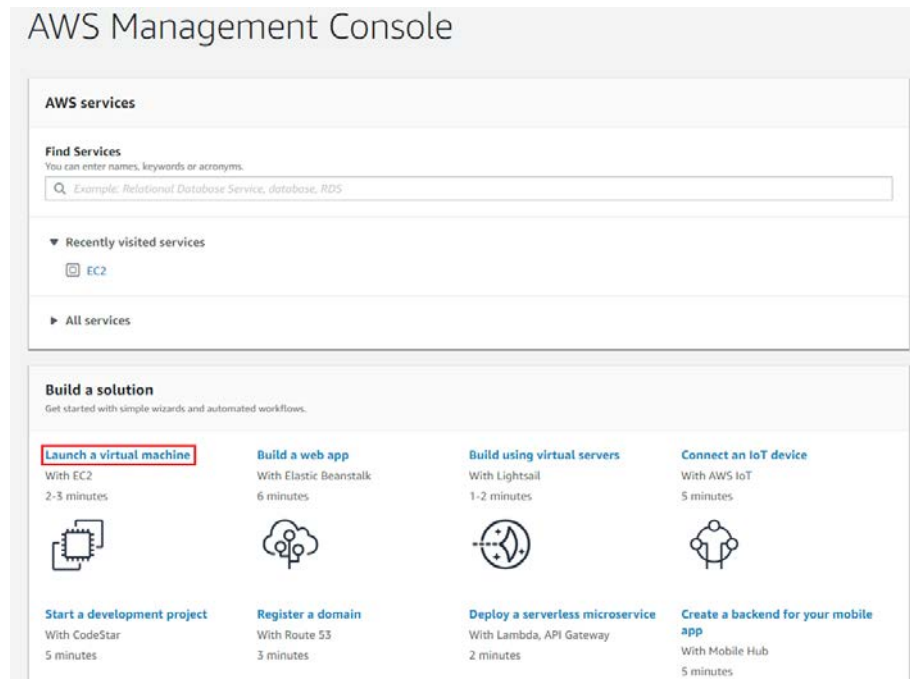
To deploy HPDM in Amazon EC2 and manage HP devices:

- Create an Amazon EC2 instance. See Amazon documentation. See [Creating an Amazon EC2 instance](#).
- Install HPDM. See [Install HP Device Manager 5.0](#).
- Configure the security groups. See [Configuring the security groups](#).
- Launch the Amazon EC2 instance.

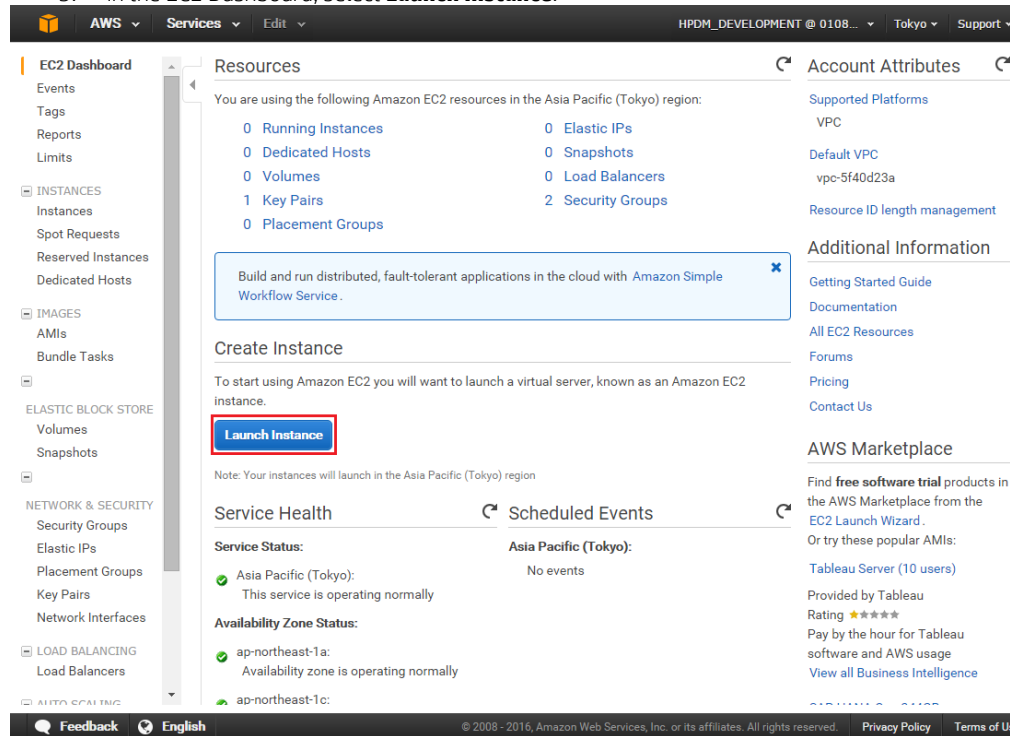


### Creating an Amazon EC2 instance

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



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



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

	<b>Microsoft Windows Server 2012 Base</b> - ami-7f799e1e	Select
Windows Free tier eligible	Microsoft Windows 2012 Standard edition with 64-bit architecture. [English] Root device type: ebs Virtualization type: hvm	64-bit
	<b>Microsoft Windows Server 2012 with SQL Server Express</b> - ami-7d799e1c	Select
Windows	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Express. [English] Root device type: ebs Virtualization type: hvm	64-bit
	<b>Microsoft Windows Server 2012 with SQL Server Web</b> - ami-6c47a00d	Select
Windows	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Web edition. [English] Root device type: ebs Virtualization type: hvm	64-bit
	<b>Microsoft Windows Server 2012 with SQL Server Standard</b> - ami-eb7a9d8a	Select
Windows	Microsoft Windows Server 2012 Standard edition, 64-bit architecture, Microsoft SQL Server 2012 Standard edition. [English] Root device type: ebs Virtualization type: hvm	64-bit
	<b>Microsoft Windows Server 2008 R2 Base</b> - 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 [Configuring the security groups](#).

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**.

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

### 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.

**⚠ 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](#)

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

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**.

HPDM\_DEVELOPMENT @ 0108... Tokyo Support

**EC2 Dashboard**

**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

[Build and run distributed, fault-tolerant applications in the cloud with Amazon Simple Workflow Service.](#)

**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

**Account Attributes**

- Supported Platforms: VPC
- Default VPC: vpc-5f40d23a
- Resource ID length management

**Additional Information**

- Getting Started Guide
- Documentation
- All EC2 Resources
- Forums
- Pricing
- Contact Us

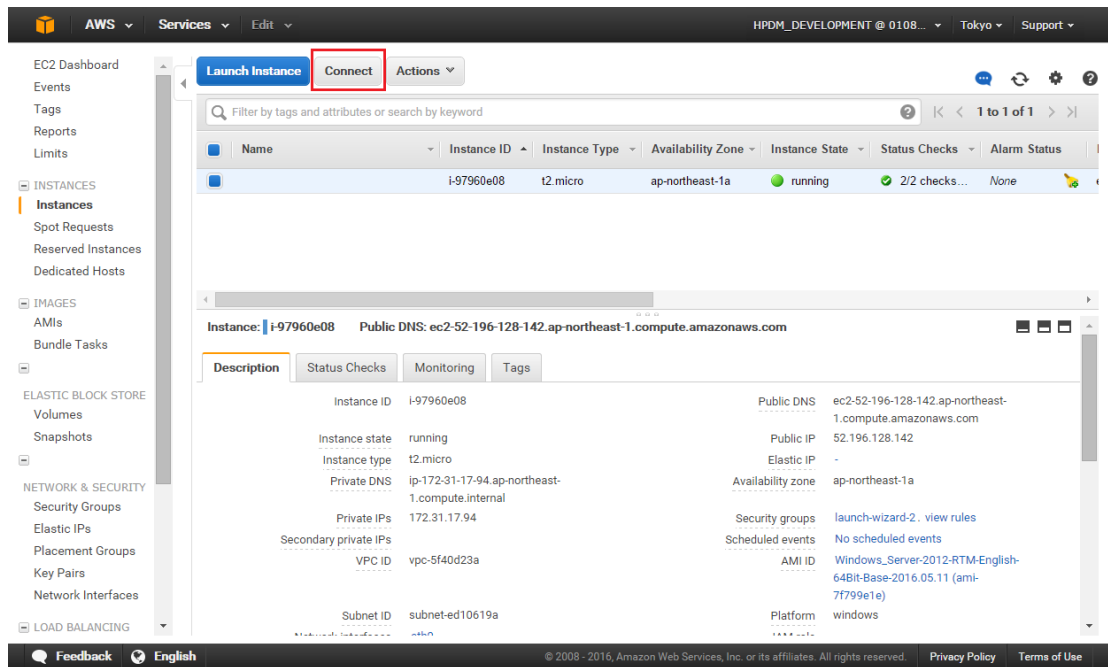
**AWS Marketplace**

Find **free software trial** products in the AWS Marketplace from the EC2 Launch Wizard. Or try these popular AMIs:

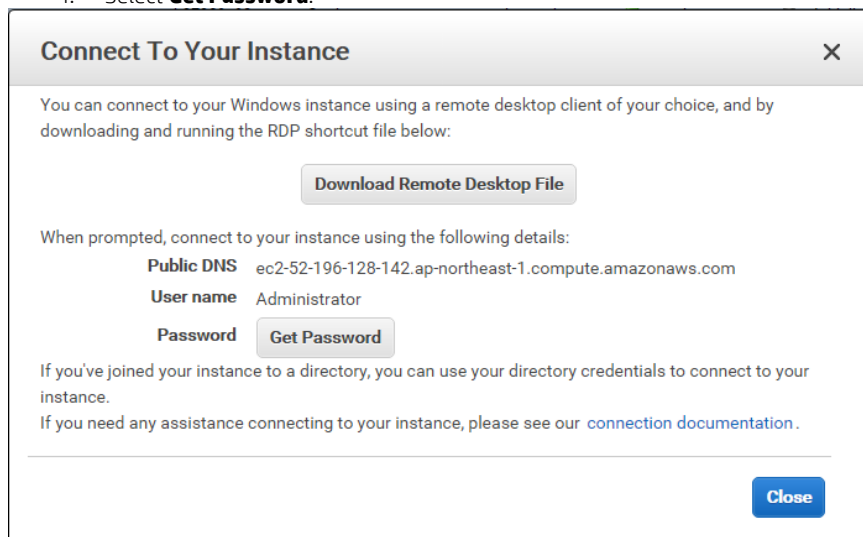
- Tableau Server (10 users)
- Provided by Tableau
- Rating ★★★★★
- Pay by the hour for Tableau software and AWS usage

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

2. Select **Connect**.



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



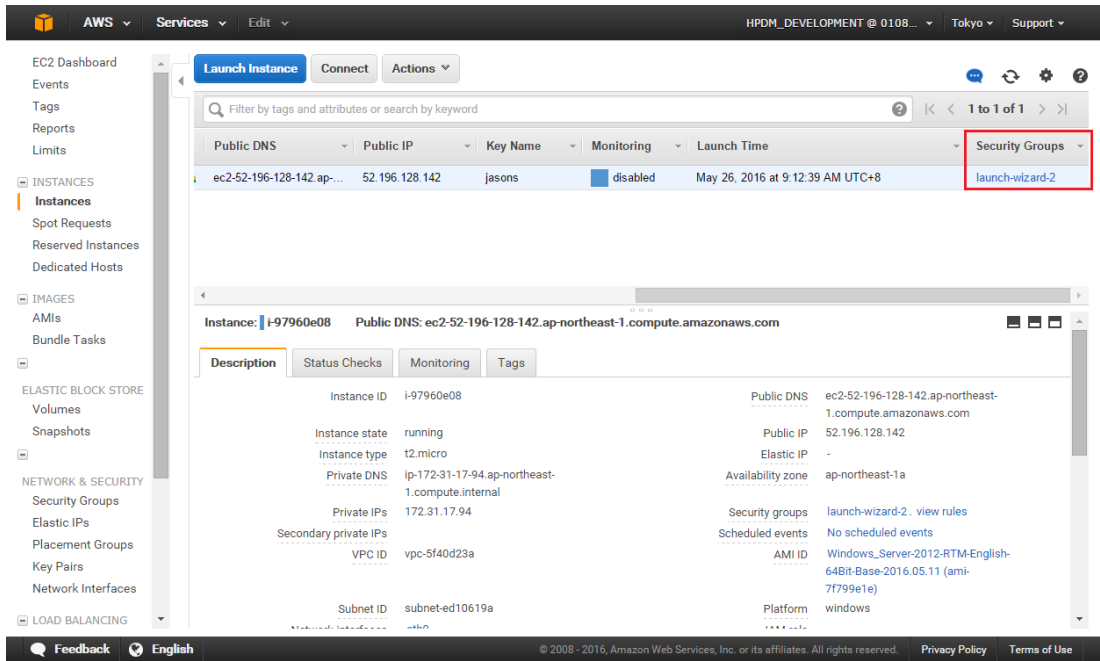
5. Use this password and file to connect to your instance.
6. Upload the HPDM package to the instance, and then install it. For instructions on installing HPDM, refer to the Installation section of the guide.

### Configuring the security groups

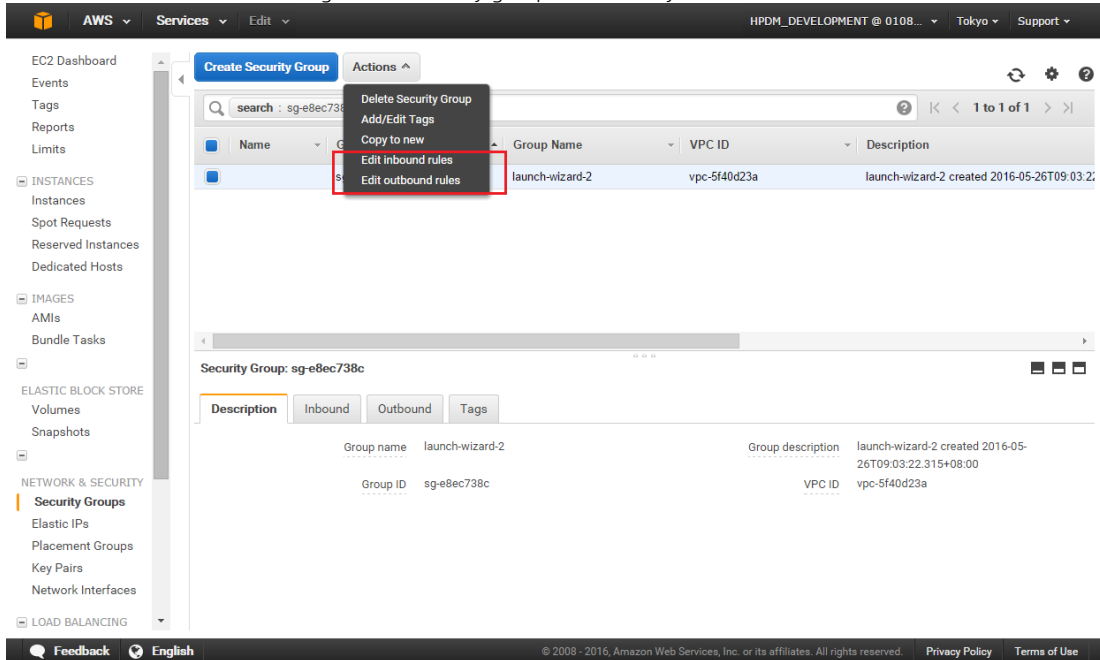
By default, an Amazon EC2 instance opens only the RDP connection through port 3389. You must map the ports corresponding to HPDM to manage your device over the Internet.

To add a port to your firewall:

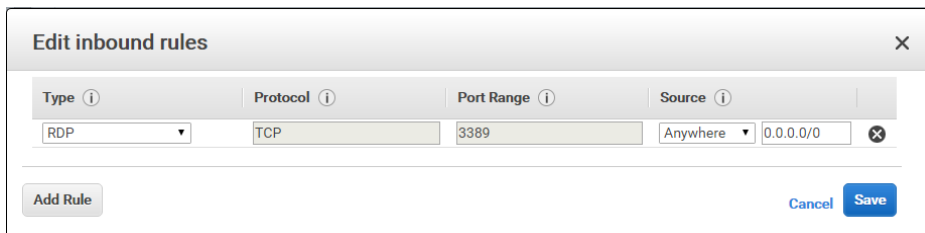
1. Select the instance where HPDM was installed, and then select the **Security Groups** column value.



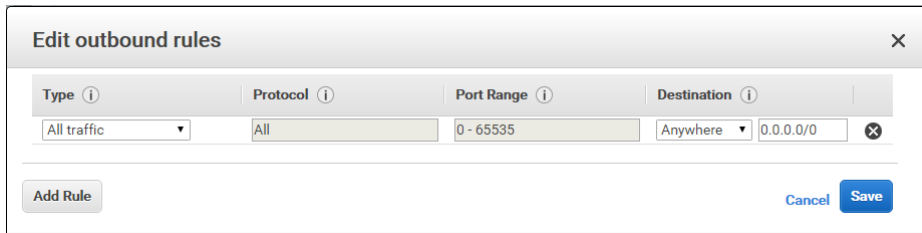
2. Select **Actions** to configure this security group as necessary.



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



- **Edit outbound rule**—Specifies which ports on the selected machines 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.

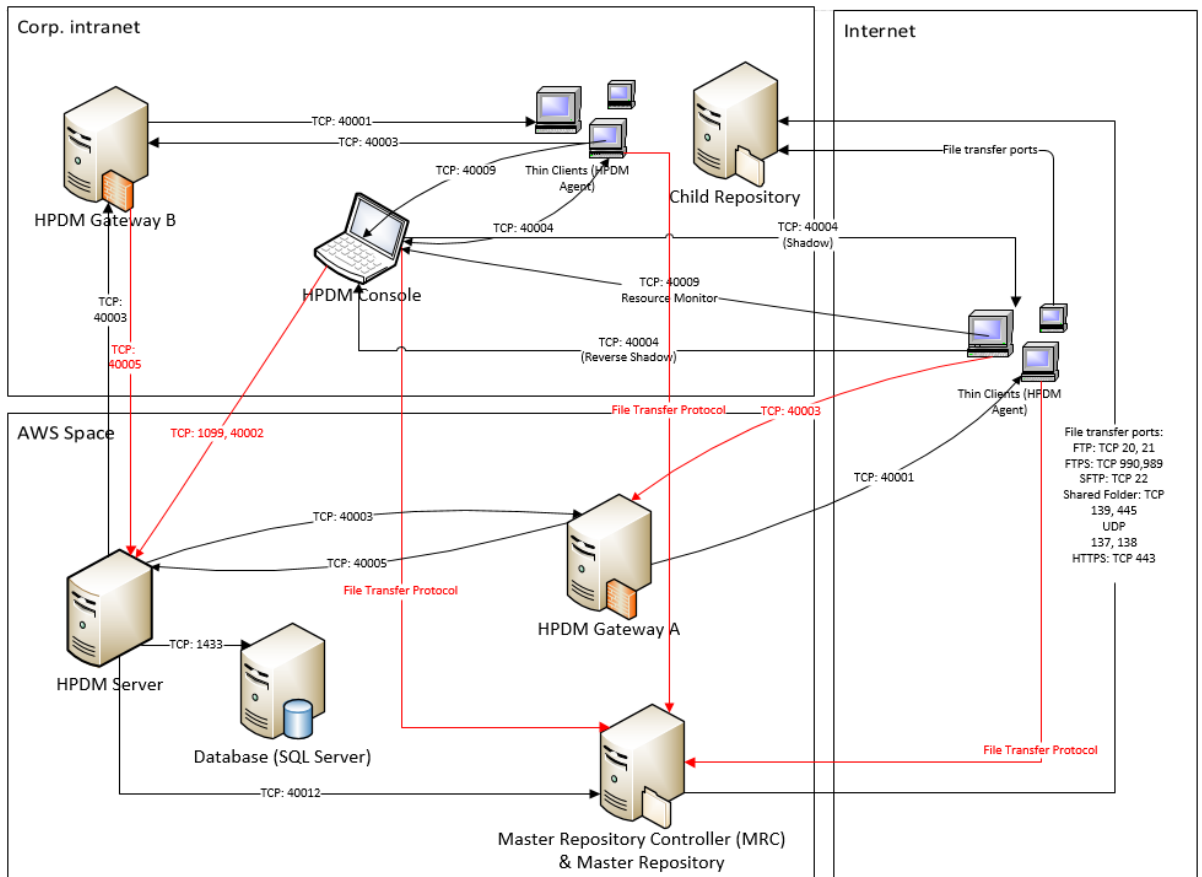
*Sample scenario*

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 8.** Typical topography



All ports in red in above figure must be added to the endpoint firewall.

**Table 1.** 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:

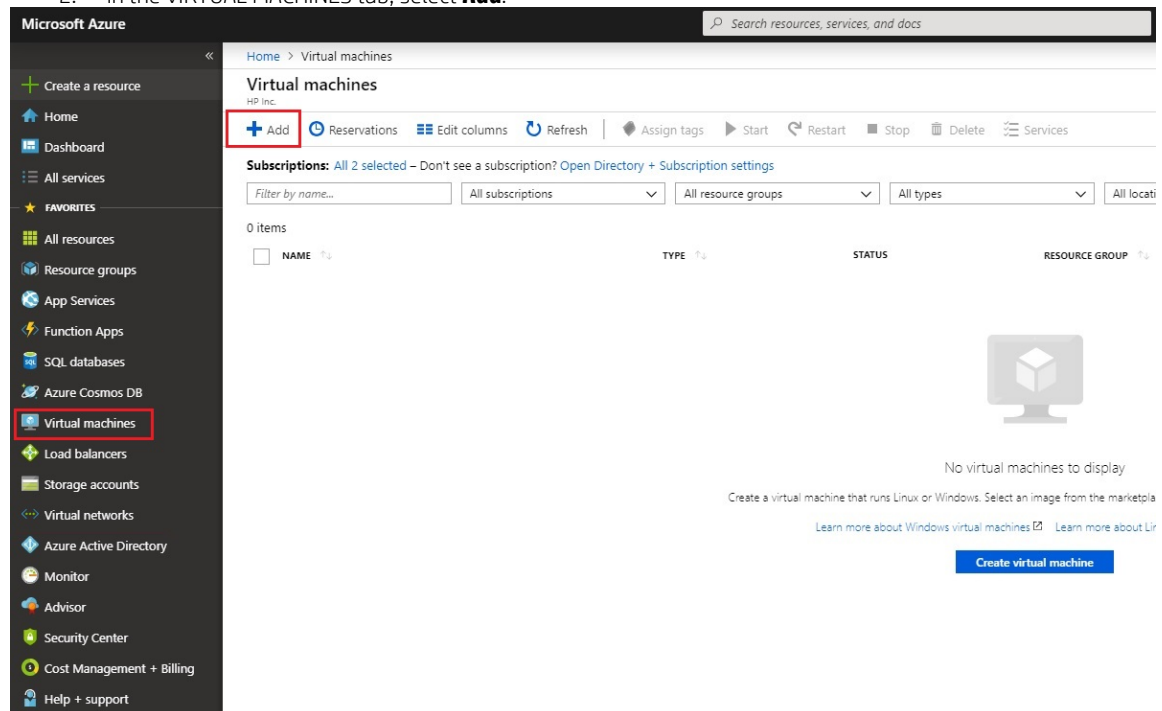
Make sure your Azure account has the necessary privileges, and that you have created your Azure workspace before deploying HPDM. For more information of creating an Azure account, contact Microsoft.

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 click **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 ⓘ

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](#)

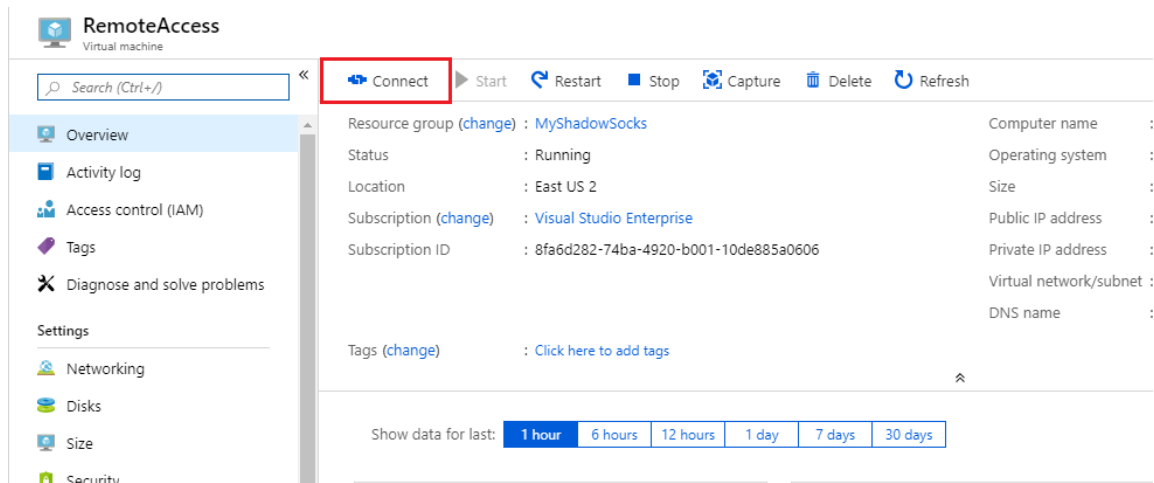
1 items

<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 virtual machines in your Azure workspace](#), and then select **CONNECT**.





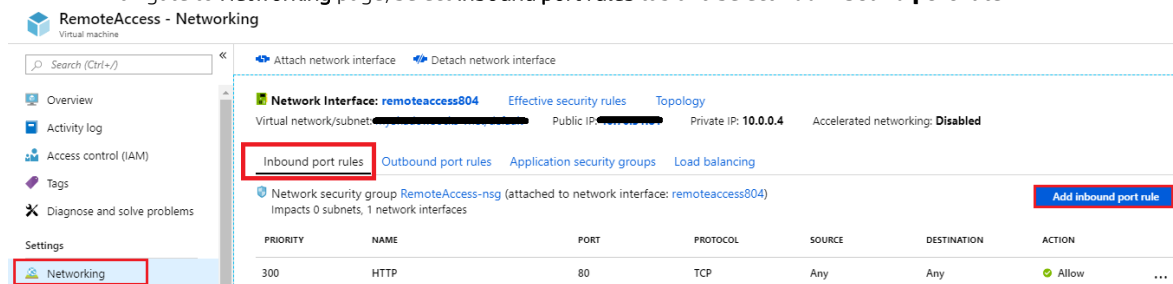
2. Save the RDP file your local system, and then use it to connect.
3. Upload the HPDM package to the virtual machine, and then install it. For instructions on installing HPDM, see the [Installation](#) section of this guide.

### 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 appears, input the **NAME** of your HPDM component, enter the **Destination port ranges** it uses, and select **TCP** as **Protocol**, then click **Add** to add the firewall rule

**Add inbound security rule**
✕

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 the step of 2.A to add outbound port rule.

RemoteAccess - Networking
⋮

🔍 Search (Ctrl+V)
🔗 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

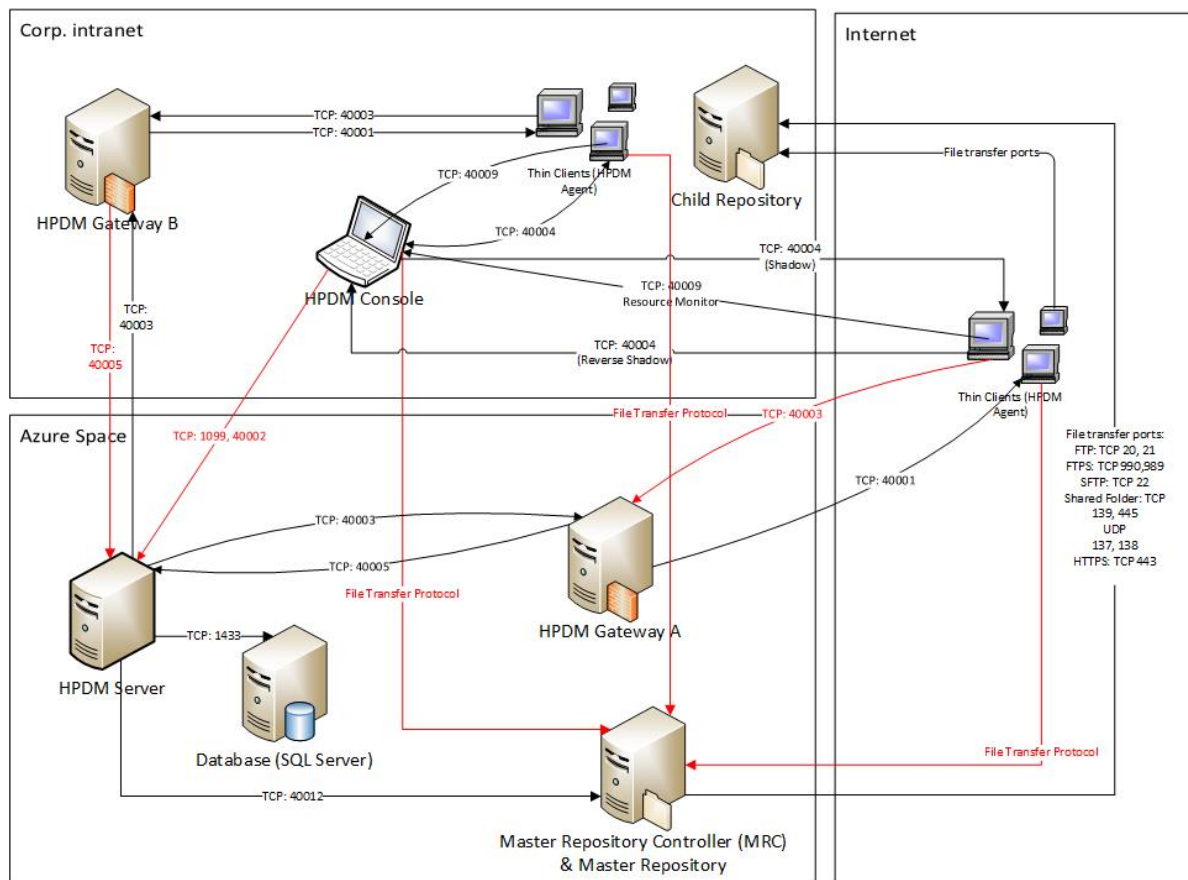
### Sample scenario

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 9. Typical topography



All ports in red in above figure 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.

Operating system	Minimum hardware	Recommended hardware
<ul style="list-style-type: none"> <li>- Windows Server 2012 R2</li> <li>- Windows Server 2016</li> <li>- Windows Server 2019</li> </ul>	<ul style="list-style-type: none"> <li>- Intel® Core™ 2 or AMD Athlon 64 processor 2 GHz</li> <li>- 2 GB RAM</li> <li>- 2 GB free disk space</li> <li>- 100 Mbps NIC</li> </ul>	<ul style="list-style-type: none"> <li>- Intel Core i5 quad-core processor 2.5 GHz or higher</li> <li>- 4 GB RAM</li> <li>- 20 GB free disk space</li> <li>- 1000 Mbps NIC</li> </ul>

### Network environment

There are many network factors that might influence the deployment of HPDM HTTPS Repository, such as the 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, refer to **Installation** section. For the configuration about user, port and root path, refer to the section Configuration Center > HPDM HTTPS Repository.

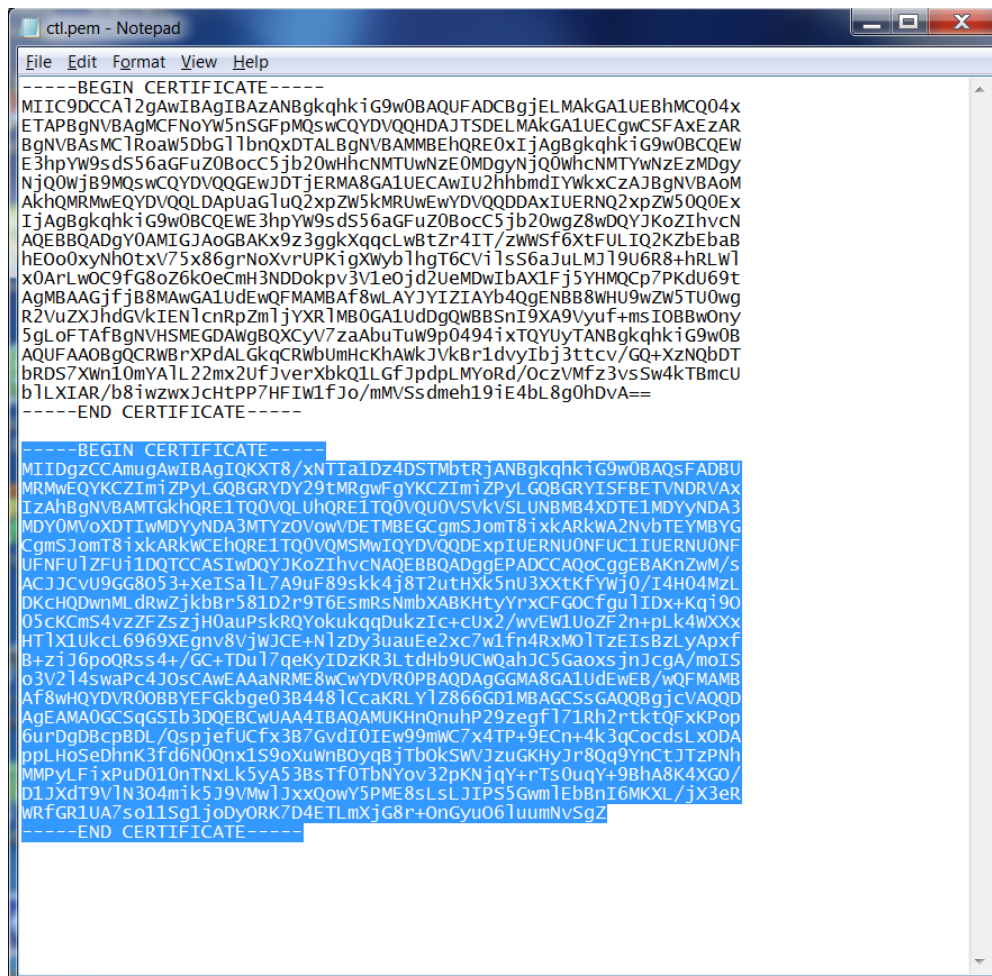
### Certificate configuration

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.

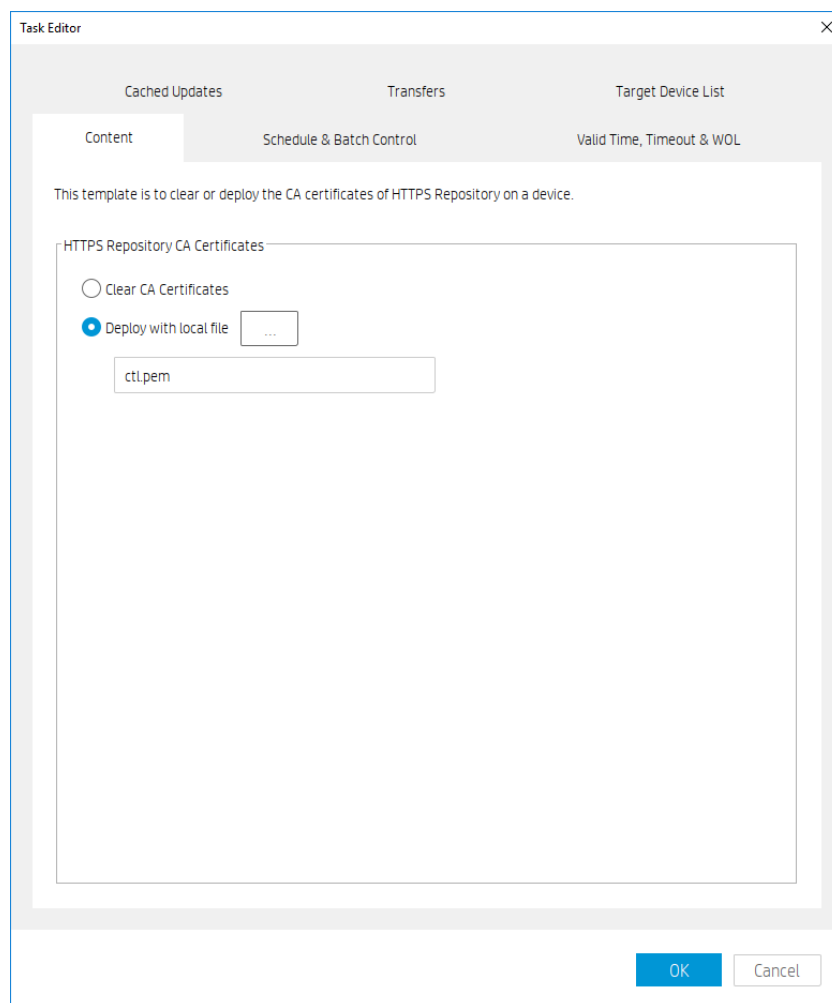
To create a CTL file:

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 the **Deploy with local file** option, and then select the file **ctl.pem**.



#### *Server certificate management*

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

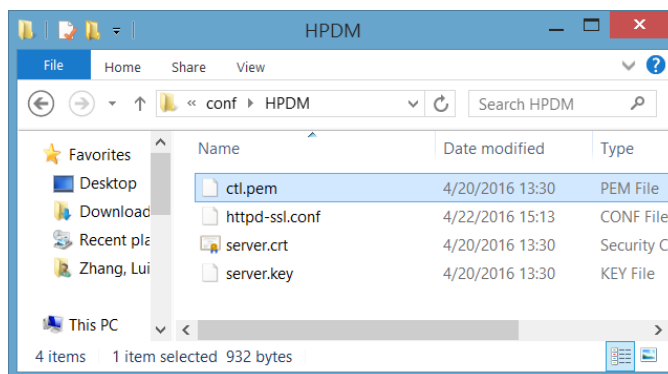
#### *Client certificate management*

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

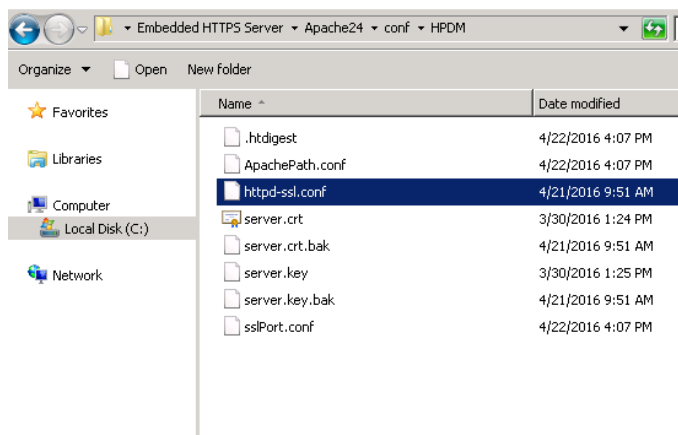
If your deployment requires to the server to verify the client certificate, use the following procedure:

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**.



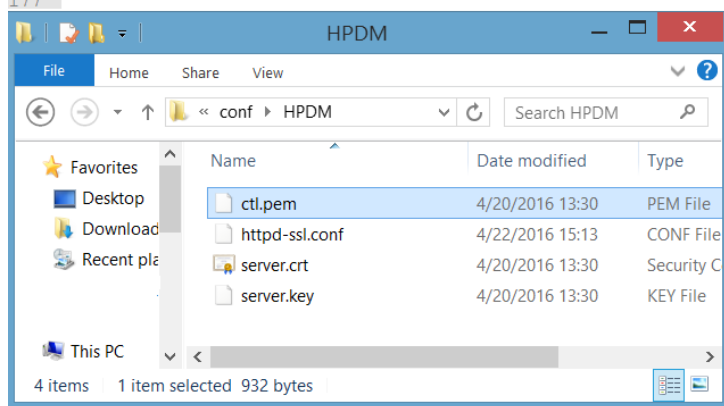
2. To configure the certificate authentication of HTTPS client, modify the SSL configuration on HPDM HTTPS Repository.

- 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 SSLCertificateFile is a comment. Make it not a comment, and then save the file.

```
168 # Certificate Authority (CA):
169 # Set the CA certificate verification path where to find CA
170 # certificates for client authentication or alternatively one
171 # huge file containing all of them (file must be PEM encoded)
172 # Note: Inside SSLCertificatePath you need hash symlinks
173 # to point to the certificate files. Use the provided
174 # Makefile to update the hash symlinks after changes.
175 #SSLCertificatePath "${SRVROOT}/conf/ssl.crt"
176 SSLCertificateFile "${SRVROOT}/conf/HPDM/ctl.pem"
177
```



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 Embedded or 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

There are many factors which impact performance, such as disk, CPU, RAM size, and so on. The suggested minimum hardware only ensures HPDM HTTPS Repository can run on the machine, but the performance is very poor. HP recommends that you deploy HPDM HTTPS Repository on a machine 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 Embedded 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 regarding how to configure the bandwidth, see [Bandwidth throttling](#).

Deploying large files and images

The following are 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:

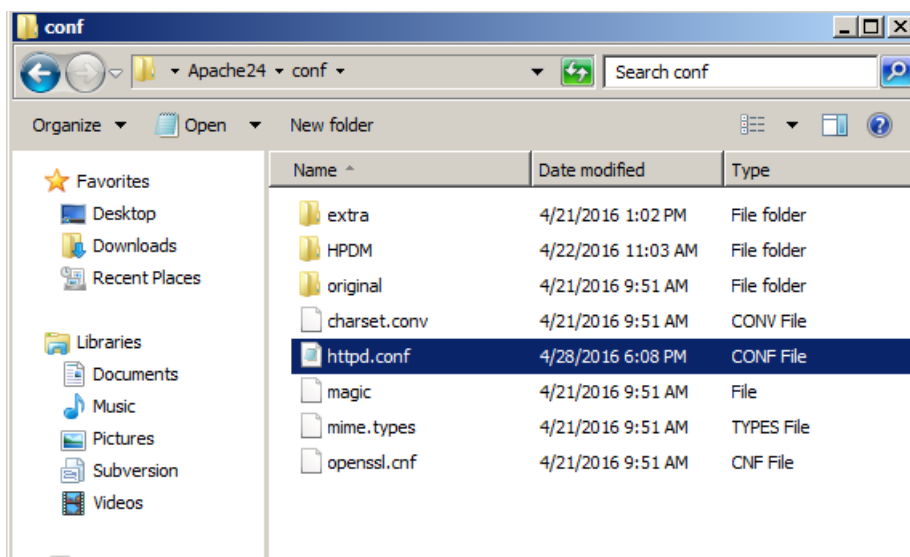
- Divide the target devices into different scenarios that would be used for targeting a single device. Execute each scenario one by one following the previous steps.

*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 this file.



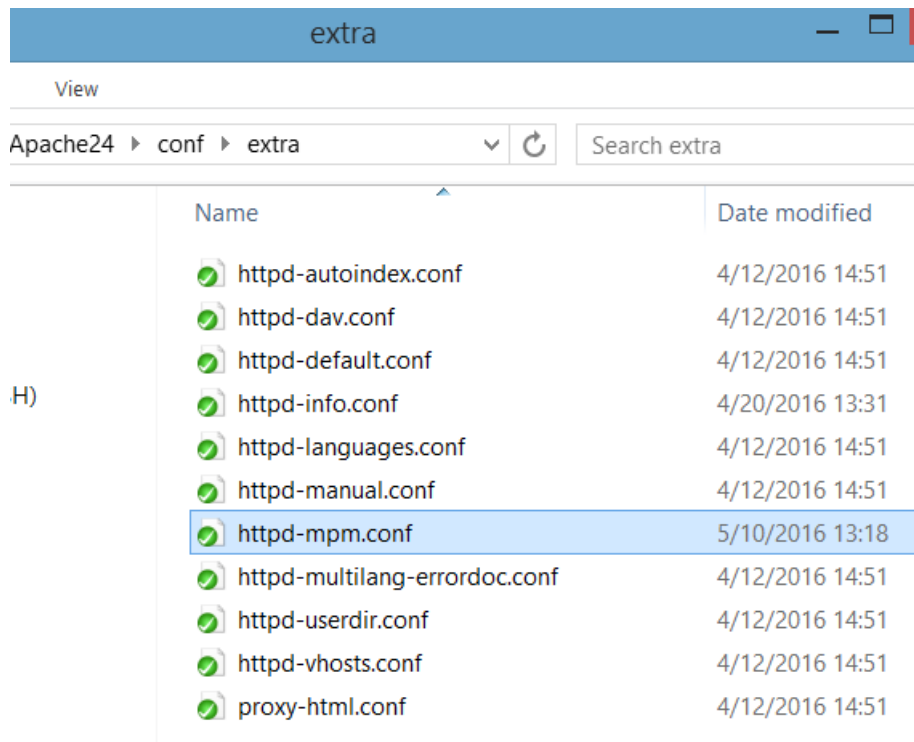
```

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 the
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, it 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.

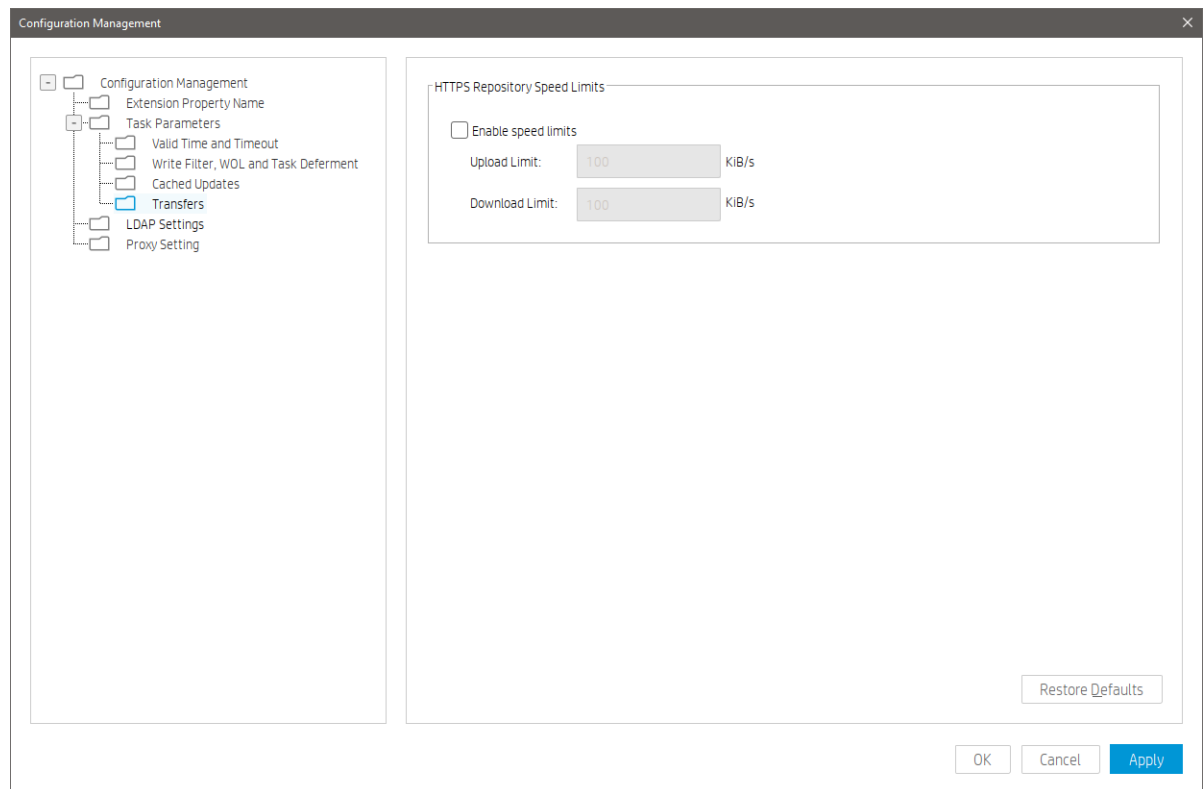
### Hardware performance

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.

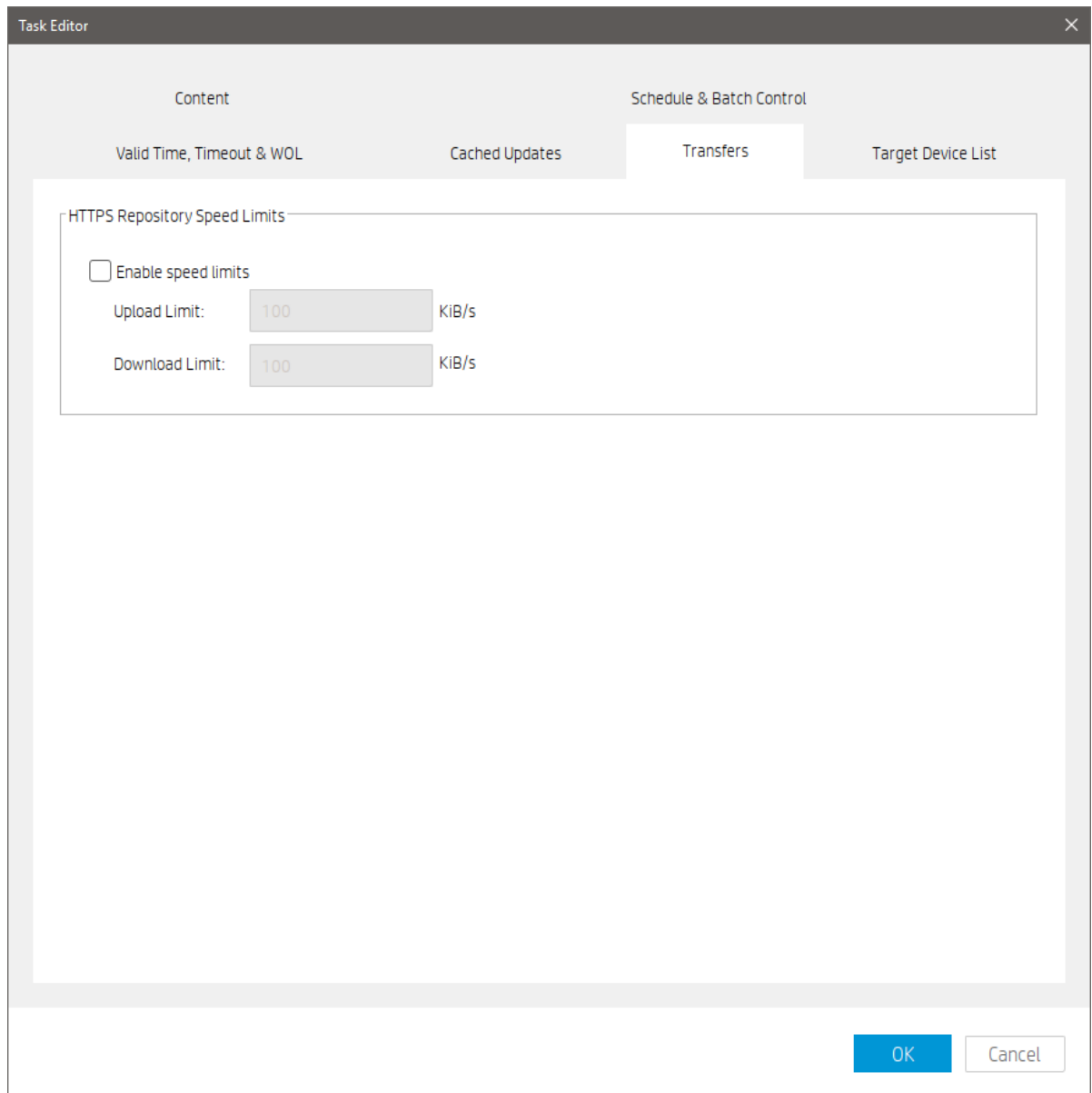
### Bandwidth throttling

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.



Also, 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 click **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.

#### **Manually update Apache and PHP**

Before proceeding, using the Service control panel in Windows, stop HPDM HTTPS Repository service.

#### *Updating PHP:*

1. Download latest PHP 7.3.x, VC15 x64 Thread Safe version from: <https://windows.php.net/download#php-7.3>.

2. Extract php-7.3.x-Win32-VC15-x64.zip to the folder "php-7.3.x-Win32-VC15-x64".
3. If php.ini exists in the folder "php-7.3.x-Win32-VC15-x64", remove it at first.
4. Backup the folder <HPDM Installed Path>\HP Device Manager\HTTPSRepository\PHP\.
5. Open the folder "php-7.3.x-Win32-VC15-x64", copy all files and subfolders to <HPDM Installed Path>\HP Device Manager\HTTPSRepository\PHP\, and replace all old files and subfolders.

#### *Updating Apache:*

1. Download latest Apache 2.4.x, OpenSSL 1.1.1, VC15 x64 from: <https://www.apachehaus.com/cgi-bin/download.plx>.
2. Extract httpd-2.4.x-o111x-x64-vc15.zip to the folder httpd-2.4.x-o111x-x64-vc15".
3. Remove the folder conf\ssl and the file conf\httpd.conf from httpd-2.4.x-o111x-x64-vc15\Apache24.
4. Remove all files from httpd-2.4.x-o111x-x64-vc15\Apache24\bin\iconv.
5. Backup <HPDM Installed Path>\HP Device Manager\HTTPSRepository\Apache24\.
6. Open the folder httpd-2.4.x-o111x-x64-vc15 and copy the folder Apache24. Then go to <HPDM Installed Path>\HP Device Manager\HTTPSRepository\, overwrite the old Apache24 folder.

When finished, restart the HPDM HTTPS Repository service.

## **FTP Repositories**

### **Overview**

This document contains the following parts:

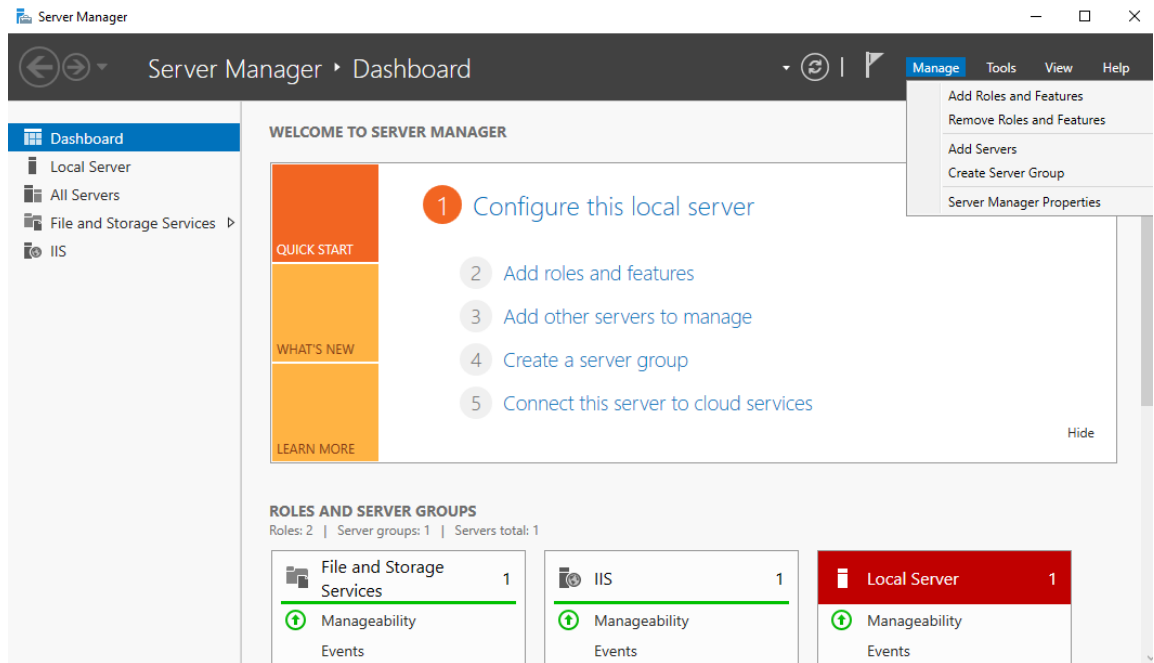
- Configuration of an IIS FTP server
- Configuration of FTP over SSL
- Configuration of a FileZilla FTP server

### **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, skip to Creating an FTP site with basic authentication.

- A. Click **Start > Windows Administrative Tools > Server Manager**.
- B. In the Server Manager, click **Manage**, and then click **Add Roles and Features** to open the Add Roles Wizard.



3. Select **Server Roles**, select **Web Server (IIS)**, and then click **Next**.
4. Click **Next**.
5. On the Select Role Services page, expand the **FTP Server** option. Then, select **FTP Service**.
6. Click **Next**.
7. On the Confirm Installation Selections page, click **Install**.
8. On the Results page, click **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. Click **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, click **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. Click **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 [Configuring HPDM to use FTPS](#).

---

- Click **Next**.
- 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. Click **Finish**.

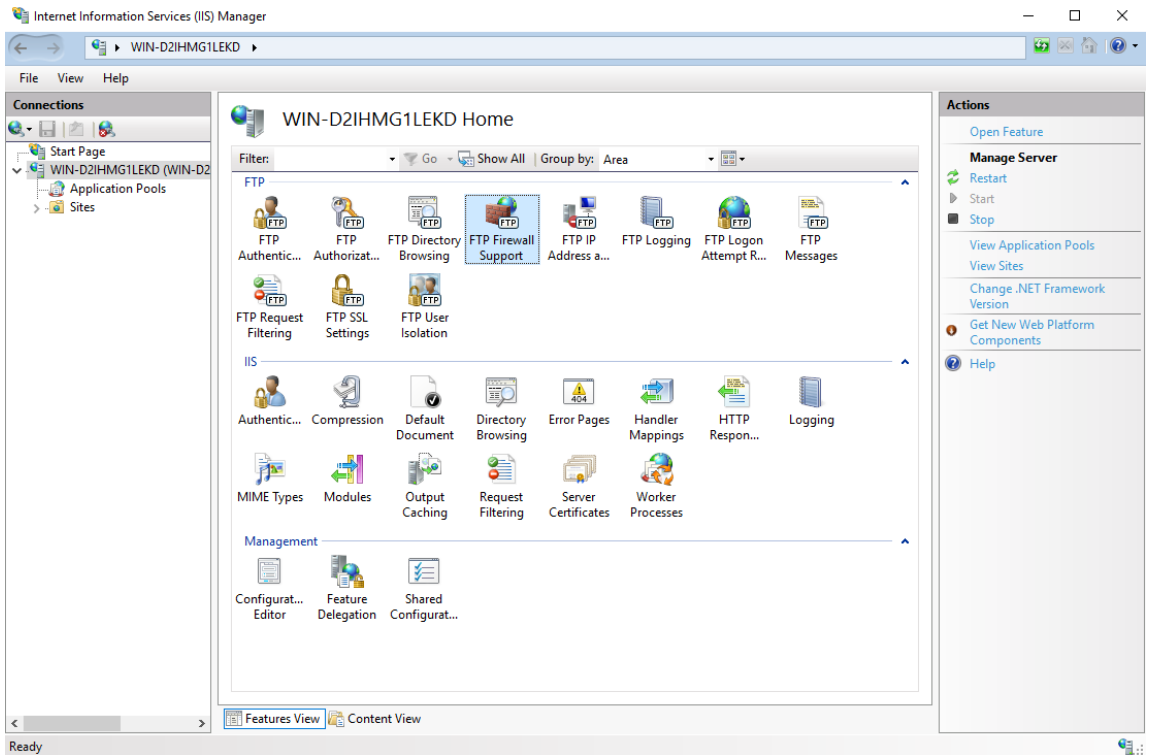
*Configuring the passive port range for the FTP service*

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.

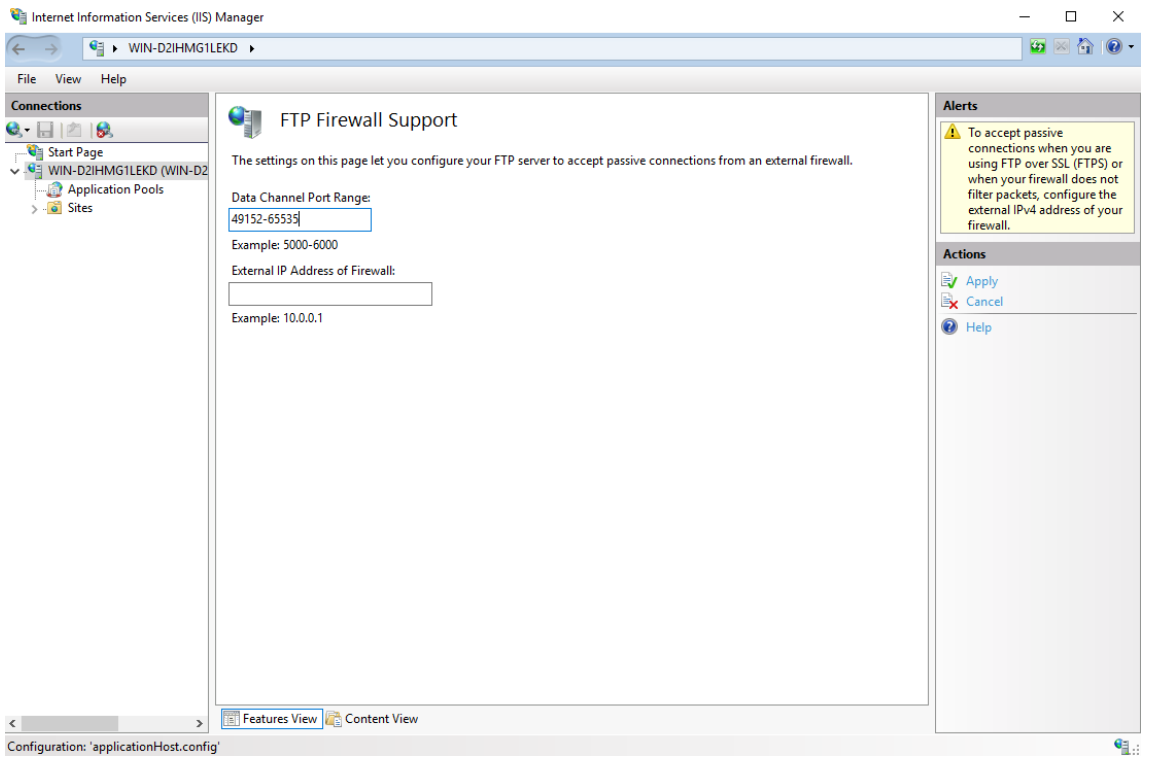
To configure the passive port range:

1. Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the Connections pane, select the server-level node, and then double-click 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.



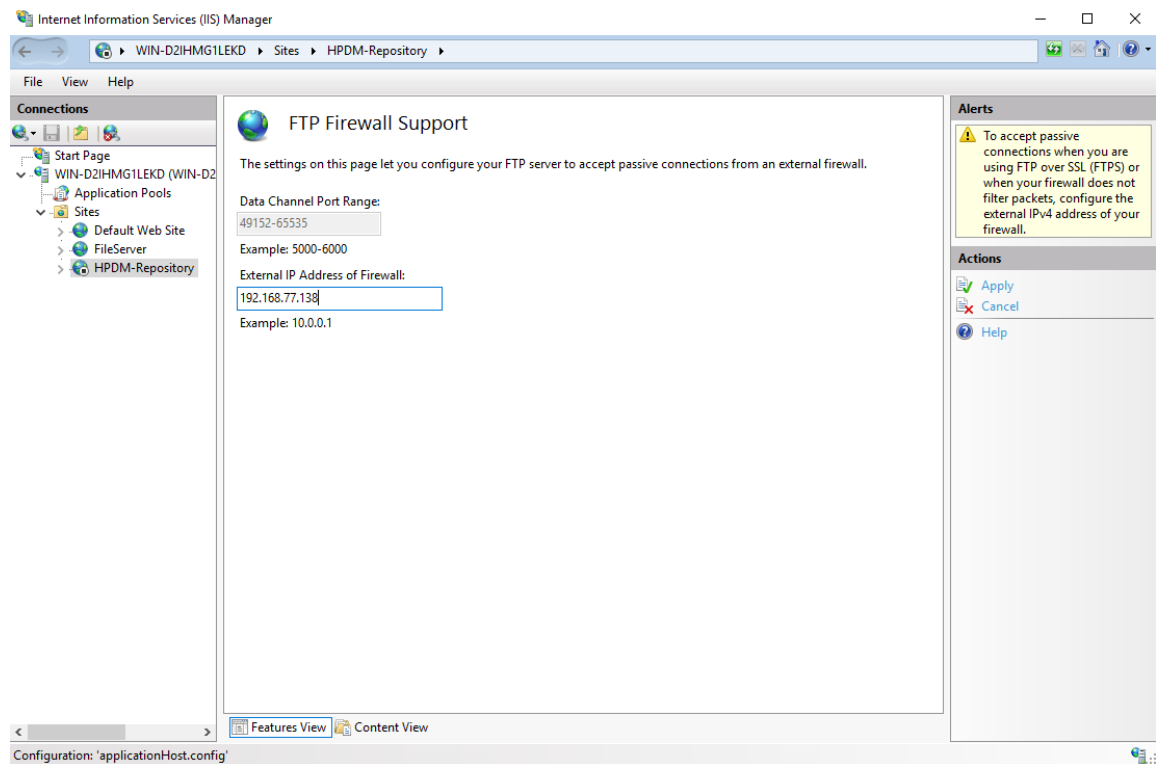
4. In the Actions pane, click **Apply**.
5. A warning message indicating that the ports need to be added to the server firewall might appear. For information on how to add the ports, see Windows Firewall settings. Click **OK**.

#### *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. Click **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 double-click 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, click **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. Click **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**:  

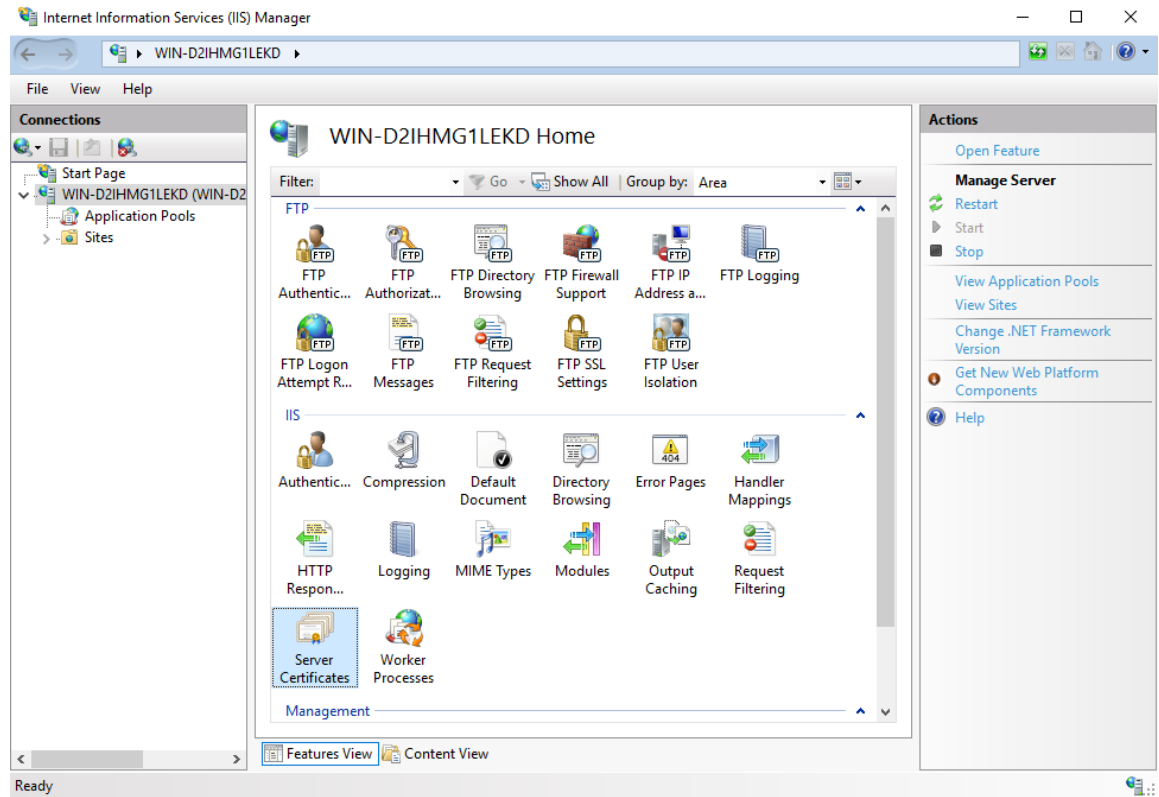
```
netsh advfirewall firewall add rule name="FTP (non-SSL)" action=allow  
protocol=TCP dir=in localport=21
```
3. To disable stateful FTP filtering so that Windows Firewall does not block FTP traffic to the passive port range, enter the following command and then press **Enter**:  

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

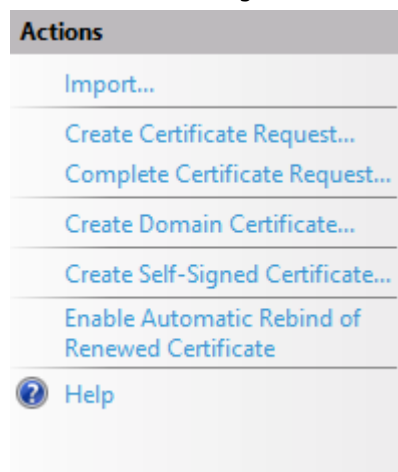
#### **Configuring HPDM to use FTPS**

Configuring Microsoft IIS & FTP

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



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



4. Enter the common name for the certificate and click **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:

Personal

OK

Cancel

5. Enter the **FTP site name** and select the **Physical path**. Click **Next**.
6. Select **Require SSL** and then select the **SSL Certificate** you created. Enter 990 in the **Port** box. Click **Next**.

**Binding and SSL Settings****Binding**

IP Address:

All Unassigned

Port:

990

Enable Virtual Host Names:

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

Start FTP site automatically

**SSL**

No SSL

Allow SSL

Require SSL

SSL Certificate:

hpdmftps.milestone.com

Select...

View...

Previous

Next

Finish

Cancel

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**. Click **Finish**.

Add FTP Site

? X



### Authentication and Authorization Information

**Authentication**

Anonymous

Basic

**Authorization**

Allow access to:

Specified users

hpdmadmin

**Permissions**

Read

Write

Previous Next Finish Cancel

### TLS 1.0 Compatibility

TLS 1.0 is disabled on some operation systems by default. But the HP ThinPro 5.2 only supports SSL3.0 and TLS 1.0; if you want to capture/deploy file from/to HP ThinPro 5.2 device via FTPS protocol, you must enable TLS 1.0 on FTP service side.

For IIS FTP Server, please refer to <https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings#tls-10>.

#### 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 double click 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.

&lt; Back

Next &gt;

Finish

Cancel

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

&lt; Back

Next &gt;

Finish

Cancel

6. Click **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
FTP		<a href="http://192.168.77.1">http://192.168.77.1</a>	admin
FTPS	990	<a href="ftps://192.168.77.1">ftps://192.168.77.1</a>	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

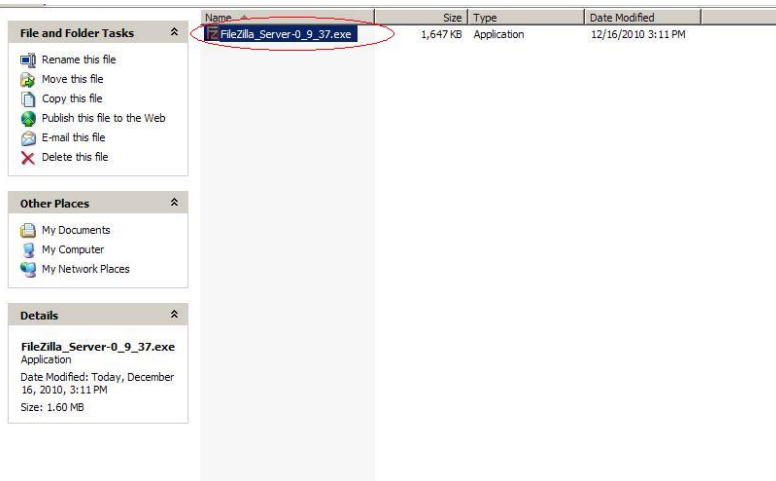
FileZilla is free, open-source, cross-platform FTP software, consisting of FileZilla Client and FileZilla Server. You only need to download, install, and configure FileZilla Server.

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

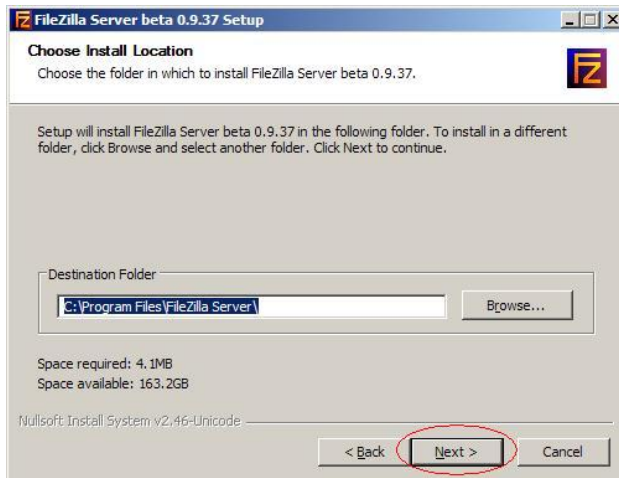
2. Select your Windows platform.



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

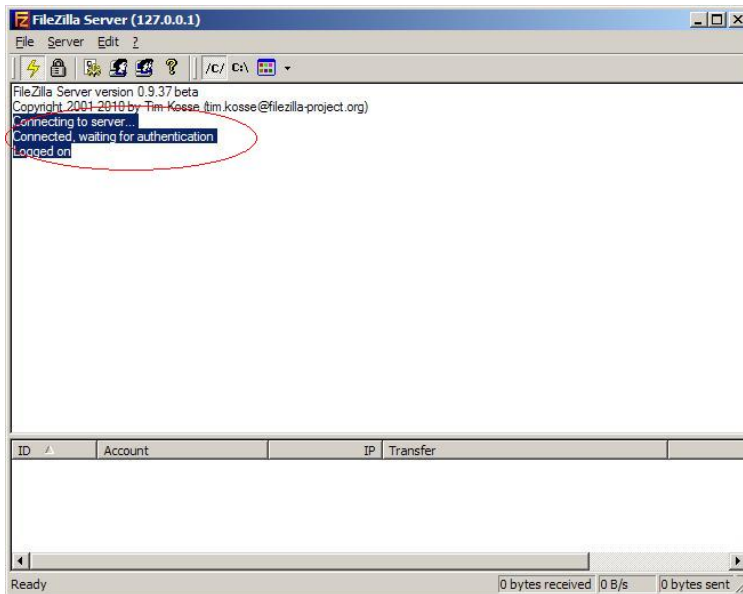


4. Click **I Agree**.
5. Click **Next**.
6. Select the **Destination Folder**, and then click **Next**.

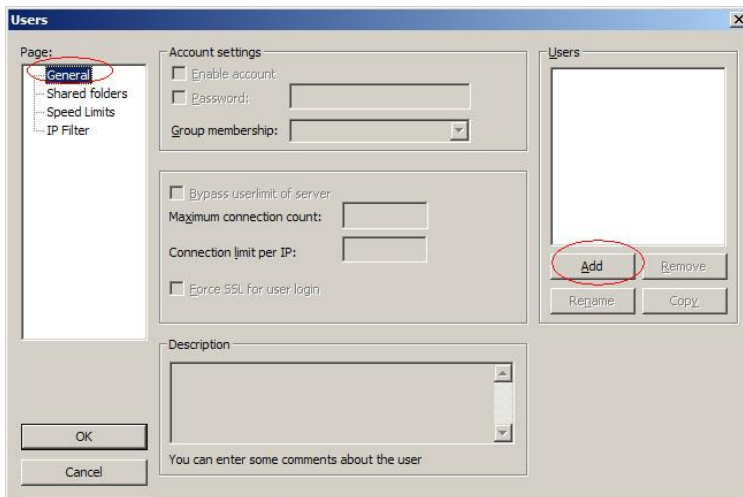


7. Click **Next**.
8. Click **Install**.
9. After the installation is complete, click **Close**.
10. Open the FileZilla Server dialog.

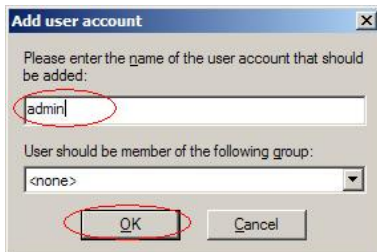




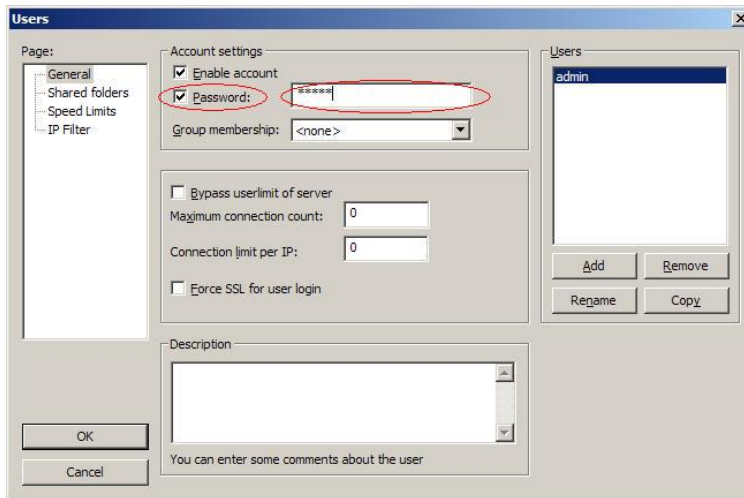
11. Select **Edit > Users** to open the Users dialog. Select the **General** page, and then click the **Add** button to add a user.



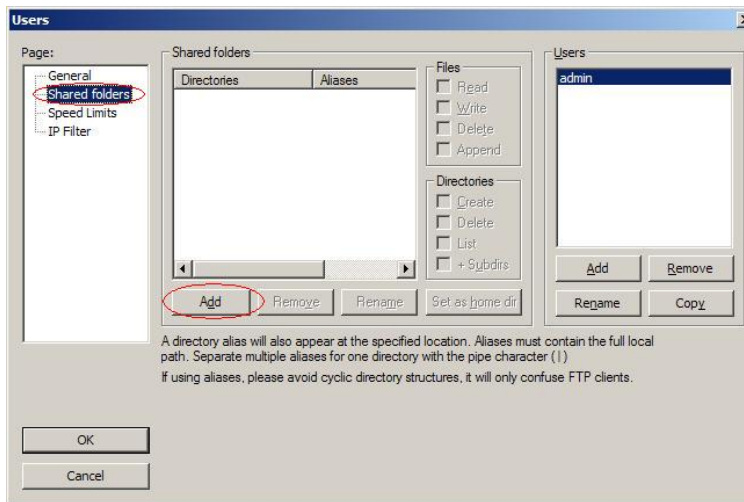
12. Enter a username, and then click **OK**.



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



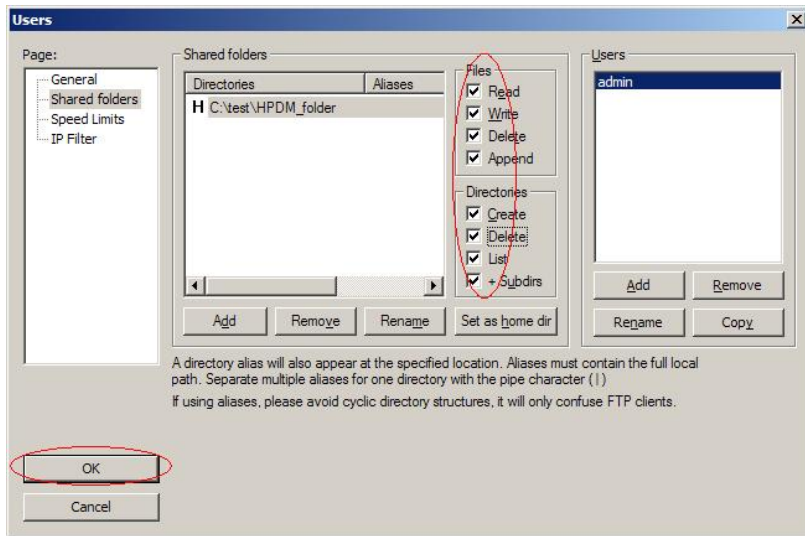
14. Select the **Shared folders** page, and then click the **Add** button to add a shared folder.



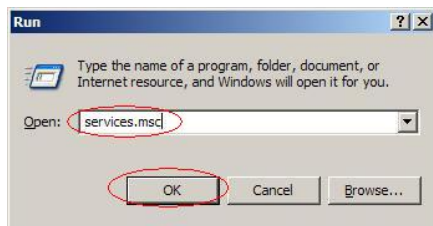
15. Select the Shared Folder, and then click **OK**.



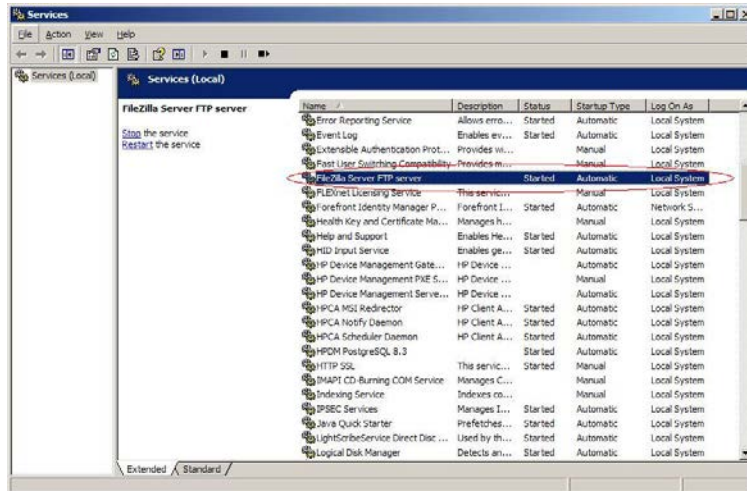
- 16. In the User dialog, select the **Read**, **Write**, **Delete**, and **Append** options in Files panel, select the **Create**, **Delete**, **List**, and **+ Subdirs** options in Directories panel, and then click **OK**.



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 now 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>.

# 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:

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

– or –

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

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

- For Complete Installation

Your first log in to the Console does require a password, after the Console is initialized, you will be prompted to change the password.

---

### Note

Initializing the Console the first time, may take additional time.

---

- For Custom Installation:

Pop up a dialog box, enter the hostname or IP address, user name and password for HPDM Server, and then select OK.

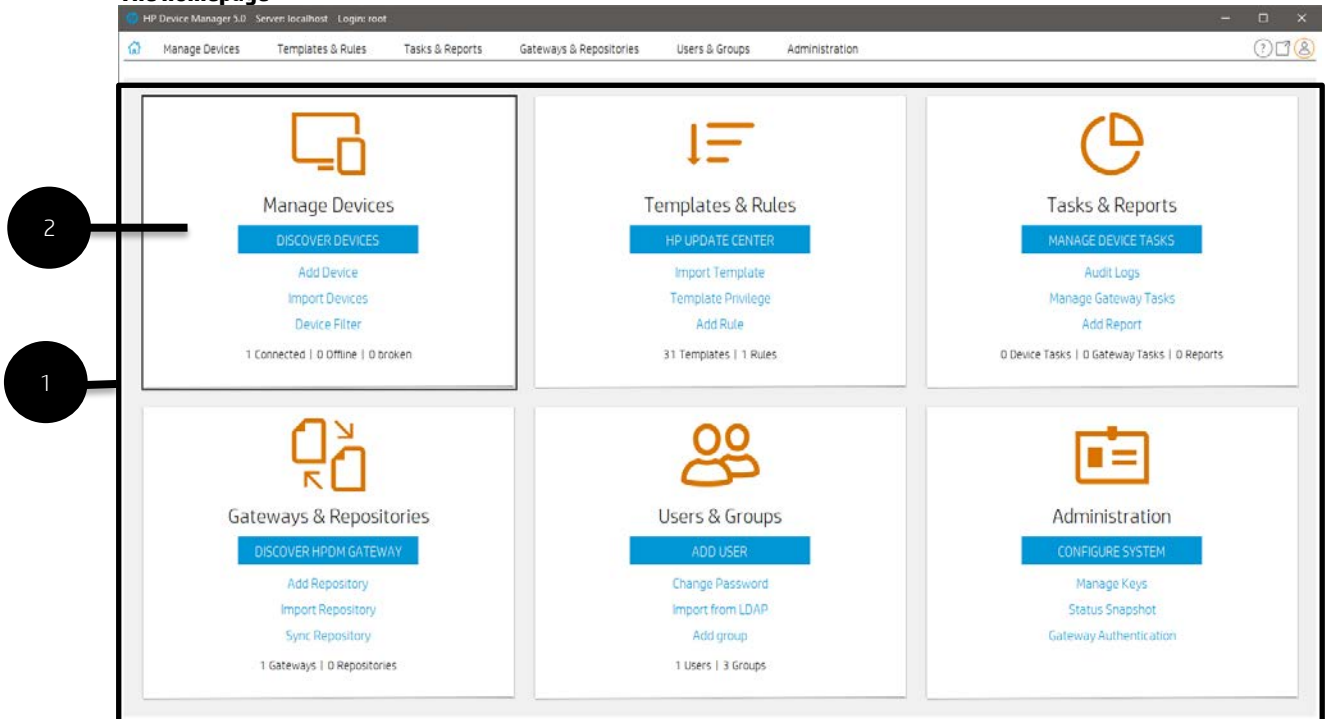
---

### Note

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

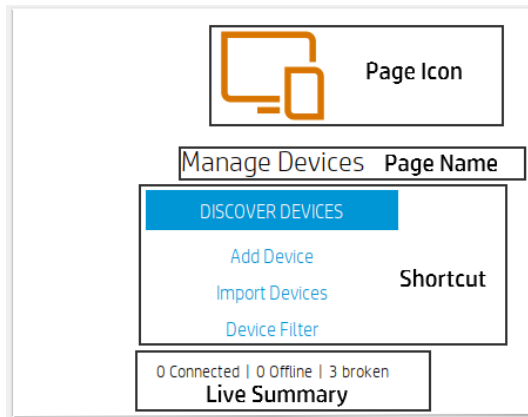
---

### 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 clicking a tile’s icon or name, the console will locate and maximize the specified page.

Shortcut(s)—The most commonly features within the Page tile. The tile contains one main shortcut and several secondary shortcuts. For each shortcut, the behavior is as follows:

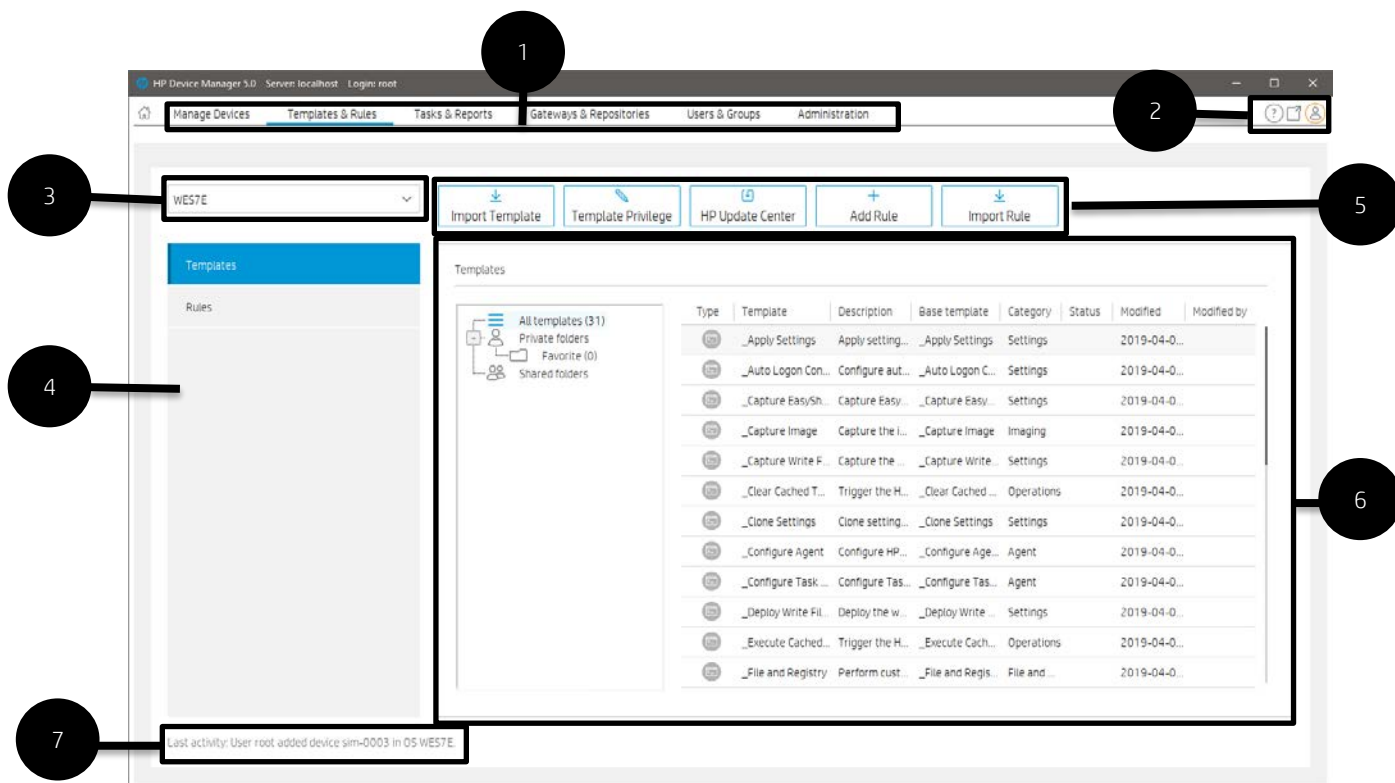
- After the shortcut is clicked, the console will transition to the related management page
- Then navigate to the management page’s Detail View
- Finally, perform the action defined by the shortcut

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

### Console layout

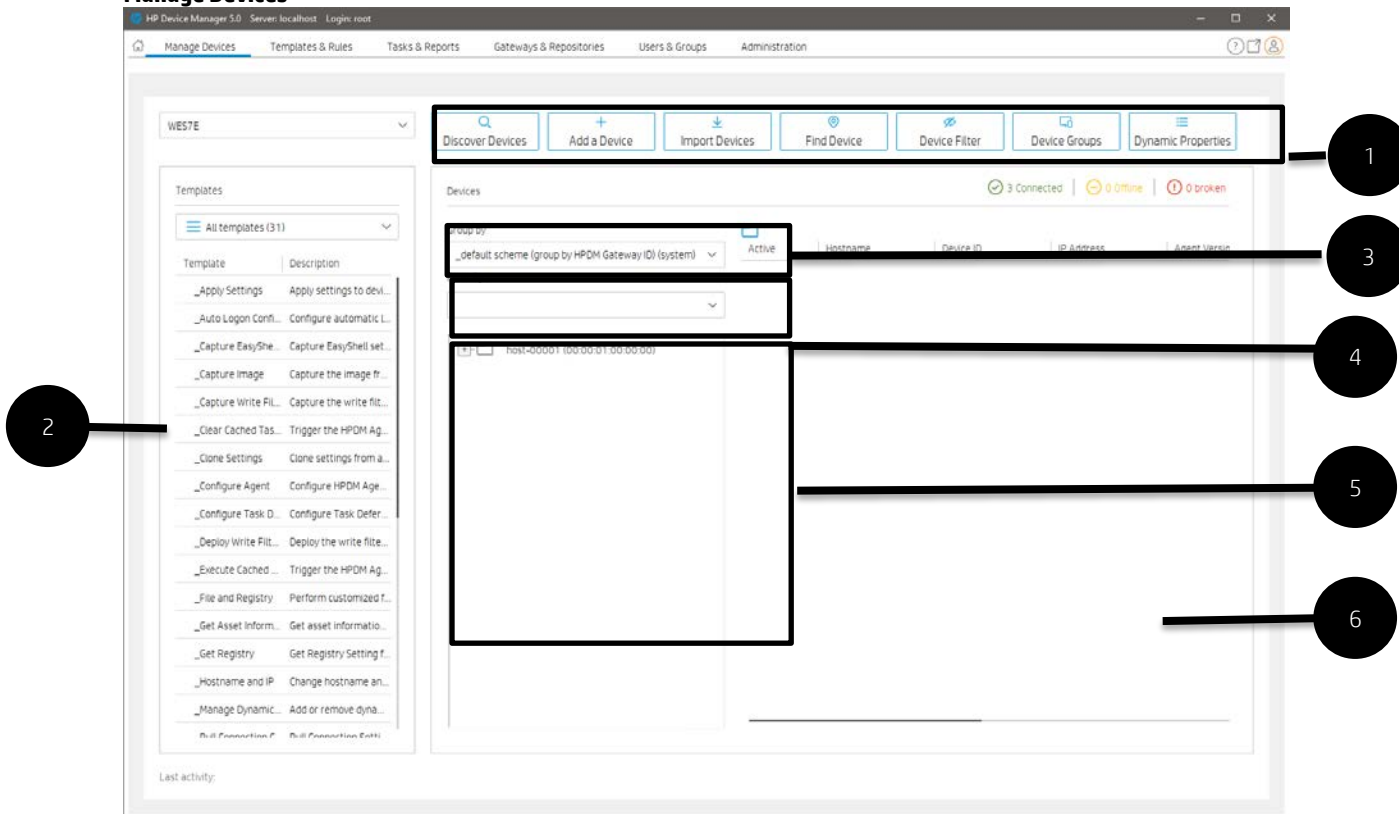
General diagrams of main activity window layout:

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

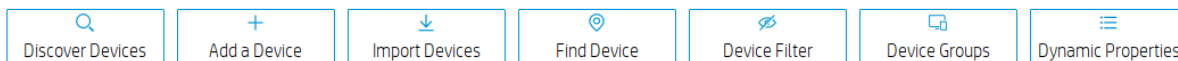


1. Page—Summary of features and navigators.
2. Global Shortcuts—It contains: Help, Docking and Profile. Please refer to the introduction of the corresponding feature.
3. OS family selector—Used to switch different OS, and the contents of the Manage Devices page will change.
4. Navigation view—Assort for features.
5. Toolbar—An enumeration of common operations.
6. Detail view—Corresponding to the content under the navigator.
7. Last Activity— Displays the last operation associated with the current user.

## Manage Devices

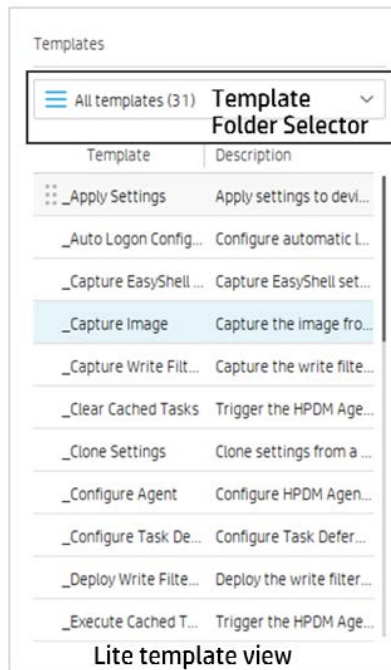


1. Toolbar—An enumeration of common operations.



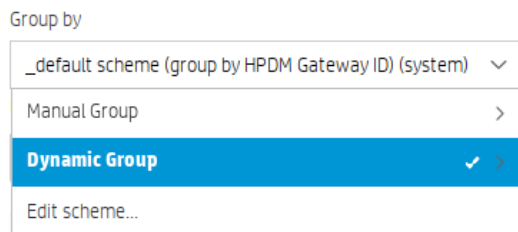
- Discover Devices—HPDM Gateway automatically discovers most devices and adds them to the HPDM database by listening for a network broadcast message made by a device when it starts up, but this method requires that the Gateway is running before the device starts up.
- Add Device—Manually register a device.
- Import Devices—Manually register multiple devices.
- Find Device— Find registered devices by condition.
- 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.

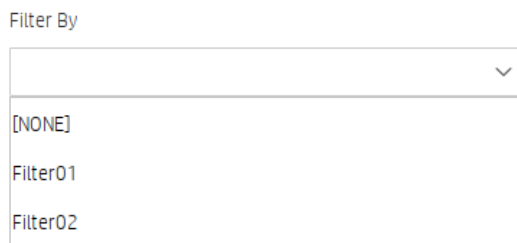


- 2.1 Template folder Selector—Switch between different template folders.
- 2.2 Lite Template View—Display the template under the current template folder.

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.



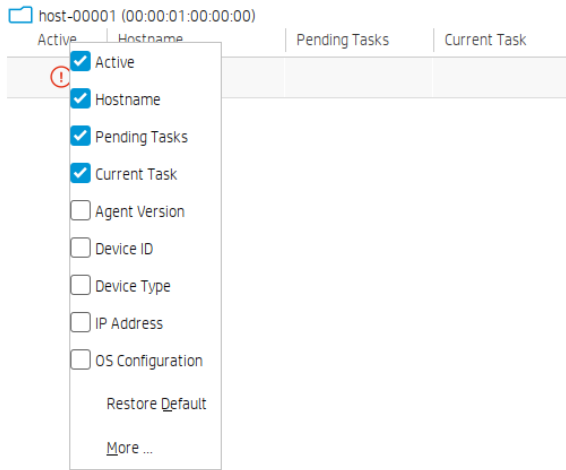
4. Device Filter Selector—Filtering enables you to work with a subset of your devices. It can be combined with User Privileges to divide the management of your devices between different administrators.



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.





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

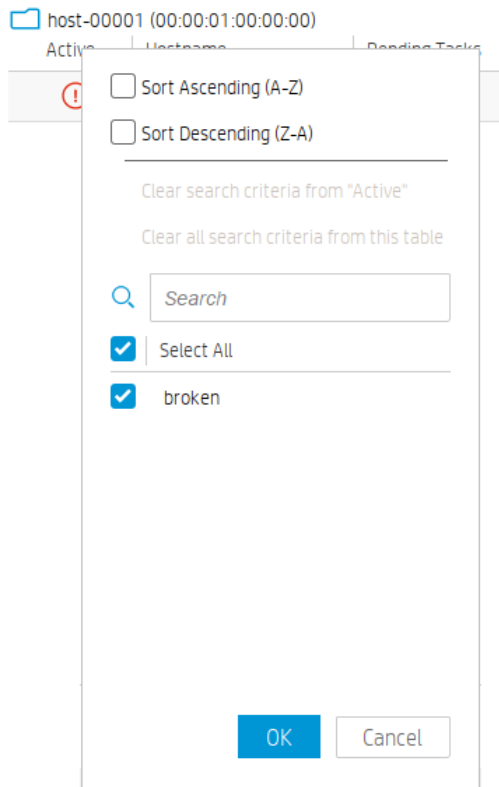


Table quick search—HPDM enables you to search quickly among currently listed devices. You can select any column header in the device table to add a search criteria or sort. All criteria are automatically cleared after switching to another folder.

## Templates & Rules

HP Device Manager 3.0 Server: localhost Login: root

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

WES7E

Import Template Template Privilege HP Update Center Add Rule Import Rule

Templates

Rules

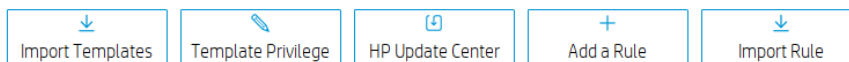
Templates

All templates (31)  
Private folders  
Favorite (0)  
Shared folders

Type	Template	Description	Base template	Category	Status	Modified	Modified by
Settings	._Apply Settings	Apply setting...	._Apply Settings	Settings		2019-04-0...	
Settings	._Auto Logon Con...	Configure aut...	._Auto Logon C...	Settings		2019-04-0...	
Settings	._Capture Easy/Sh...	Capture Easy...	._Capture Easy...	Settings		2019-04-0...	
Imaging	._Capture Image	Capture the I...	._Capture Image	Imaging		2019-04-0...	
Settings	._Capture Write F...	Capture the ...	._Capture Write...	Settings		2019-04-0...	
Operations	._Clear Cached T...	Trigger the H...	._Clear Cached ...	Operations		2019-04-0...	
Settings	._Clone Settings	Clone setting...	._Clone Settings	Settings		2019-04-0...	
Agent	._Configure Agent	Configure HP...	._Configure Age...	Agent		2019-04-0...	
Agent	._Configure Task ...	Configure Tas...	._Configure Tas...	Agent		2019-04-0...	
Settings	._Deploy Write Fil...	Deploy the w...	._Deploy Write ...	Settings		2019-04-0...	
Operations	._Execute Cached...	Trigger the H...	._Execute Cach...	Operations		2019-04-0...	
File and ...	._File and Registry	Perform cust...	._File and Regis...	File and ...		2019-04-0...	

Last activity: User root added device sim-0003 in OS WES7E

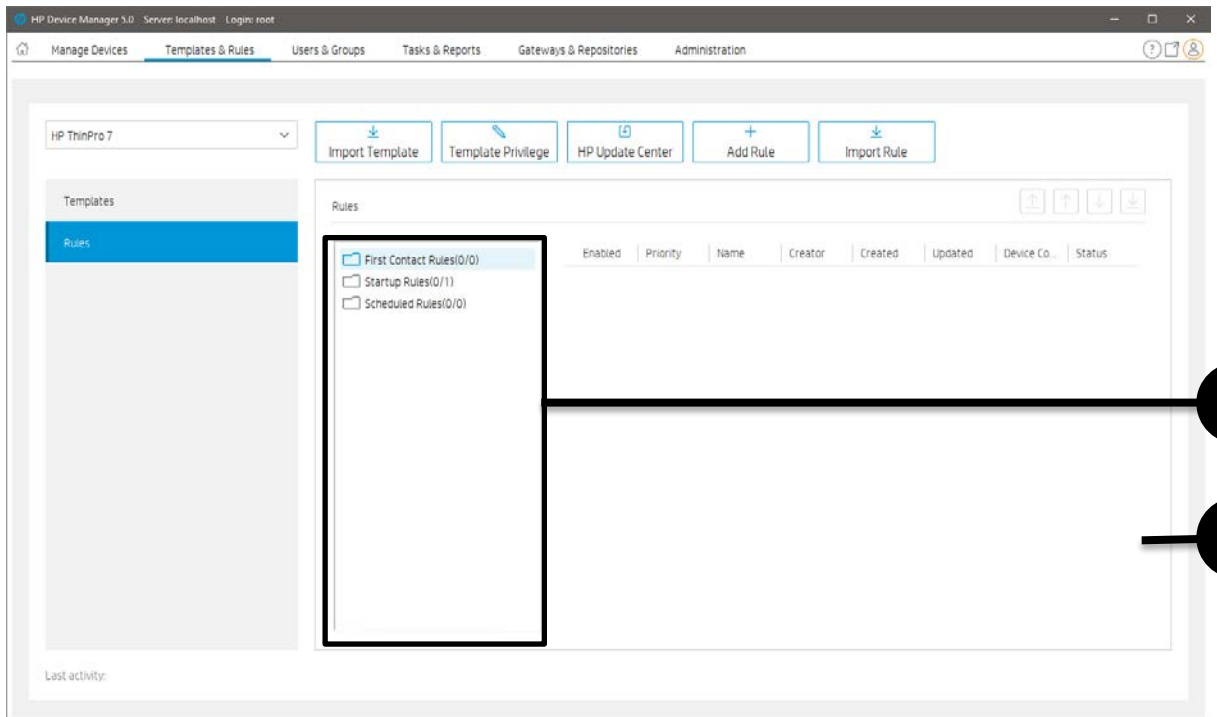
1. Toolbar— An enumeration of common operations.



- Import Template—Import templates from a file (xml, zip).
- Template Privilege— there is an additional template privilege to control each template, including viewing, modifying, and executing operations.
- HP Update Center—Allows you to leverage software components from the HP FTP server for use as payload.
- Add Rule—Create a new Rule.
- Import Rule—Import rule from a rule file.

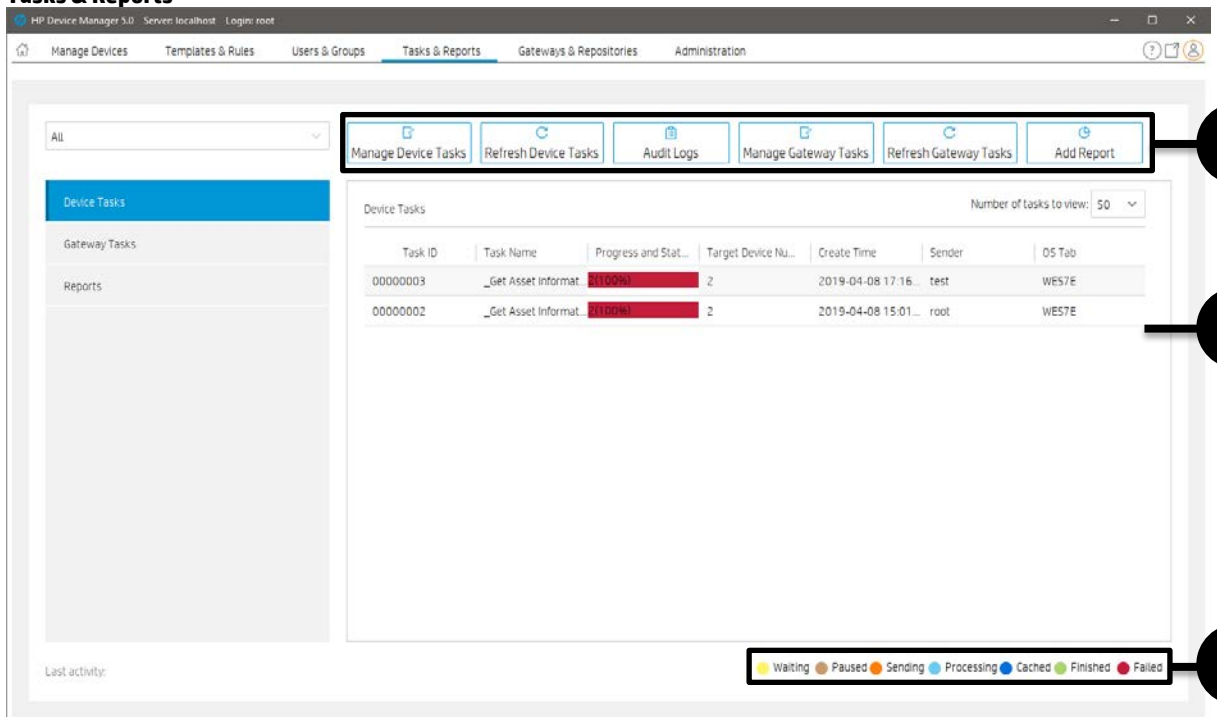
2. Template Folder View—A collection of template folders.

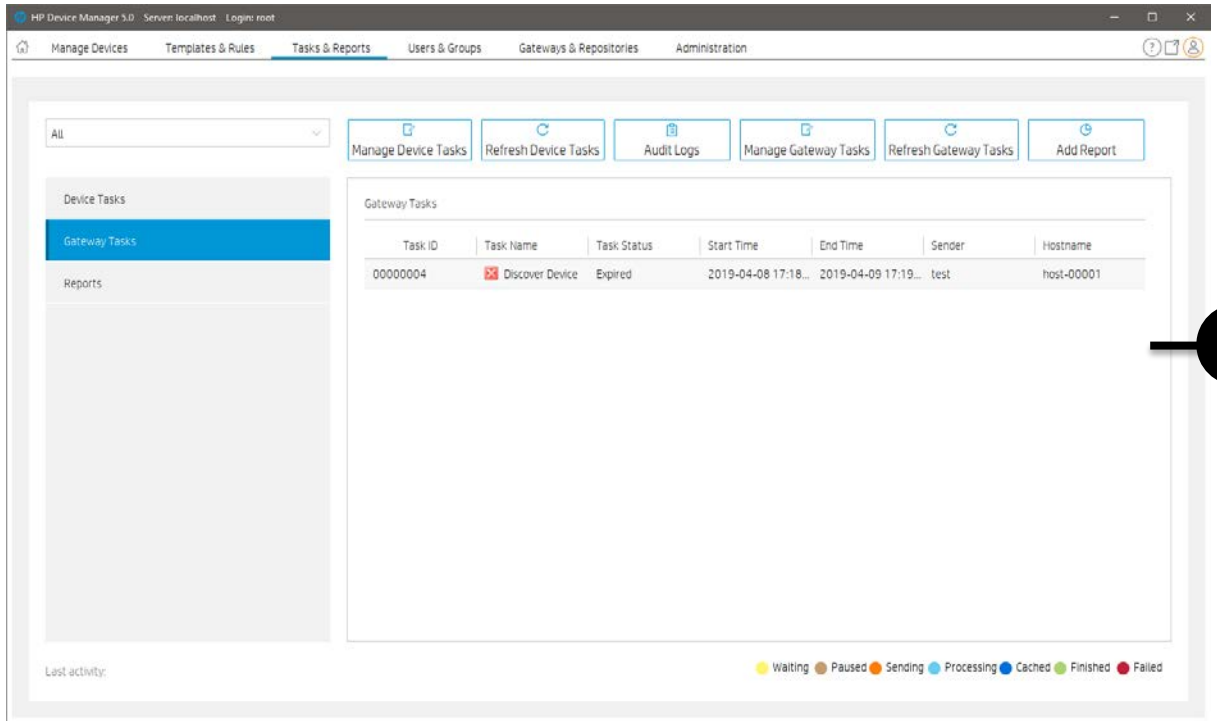
3. Template View—List all the templates under the corresponding template folder.



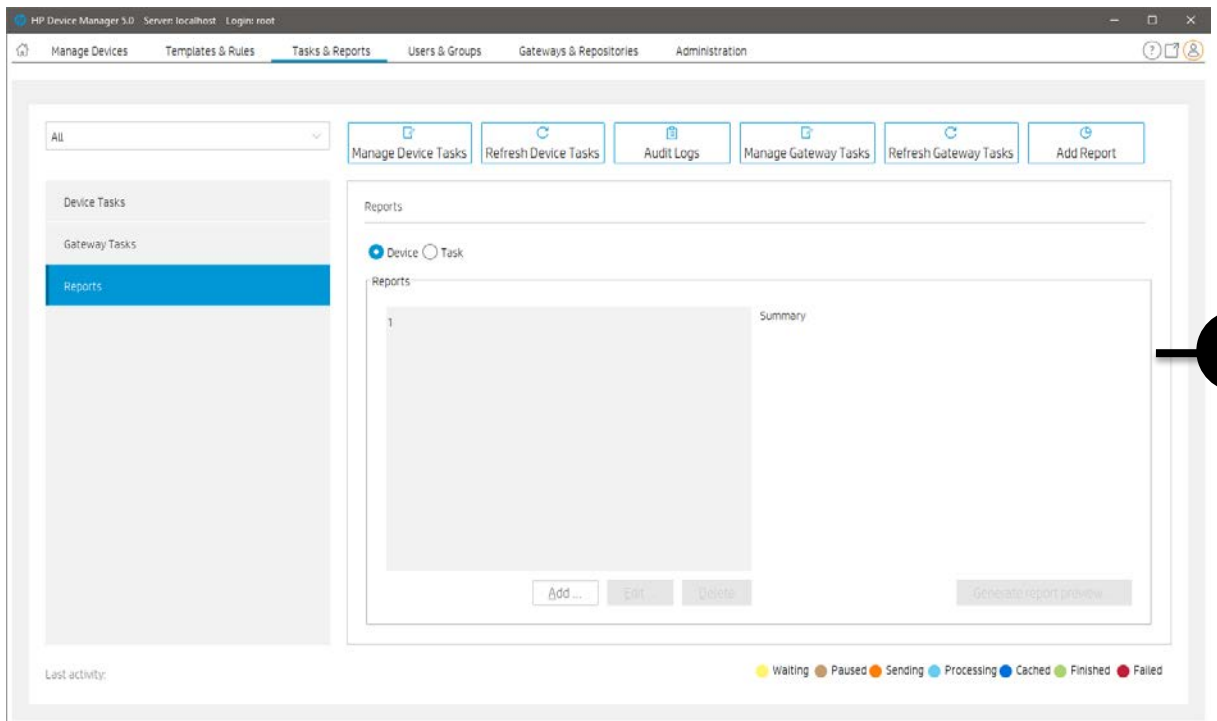
1. Rule Type List—Assort for rules.
2. Rule View—List all the rules for the corresponding rule type.

### Tasks & Reports





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—All device tasks visible to the current user.

Note: The Device filter will filter the devices in the task here. “Number of tasks to view” sets the maximum number of tasks visible to the user.

3. Task status legend

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



Waiting

The task has been scheduled or queued for sending at a later time, and has not been sent yet.



Paused

The task has been paused.



Sending

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



Processing

The task has been accepted by the device and is being processed.



Cached

The task and its payload have been 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.

4. Gateway Tasks View—List all Gateway tasks.

5. Report View—Report management

## Users & Groups

The top screenshot shows the 'Users & Groups' interface with the 'Users' view selected. A toolbar at the top contains four buttons: 'Add User', 'Change Password', 'Import from LDAP', and 'Add group'. A black box highlights this toolbar, with a callout '1' pointing to it. Below the toolbar is a table of users:

Username	Description	Type	DN
root		Local	
test		Local	

The bottom screenshot shows the same interface with the 'Groups' view selected. A callout '3' points to the toolbar area. Below the toolbar is a table of groups:

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

1. Toolbar—An enumeration of 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.

## Gateways & Repositories

HP Device Manager 3.0 Server: localhost Login: root

Management > Gateways & Repositories

Discover HPDM Gateway Find HPDM Gateway Add Repository Import Repositories Sync Repository Mapping Policy Repository Content

Active Status	Hostname	HPDM Gateway ID	IP Address	HPDM Gateway Version	Last Update	Subnet Mask	Subnet Address
on	host-00001	00.00.01.00.00.00	127.0.0.1	3.0	May 15, 2019	NA	NA

Last activity:

HP Device Manager 3.0 Server: localhost Login: root

Management > Gateways & Repositories

Discover HPDM Gateway Find HPDM Gateway Add Repository Import Repository Sync Repository Mapping Policy

Name	Server Address	HTTPS	FTP/FTPS	SFTP	Shared Folder	Last Time Synchron...
Master Repository	15.15.181.138	Enabled				Master
Child Repository	15.15.181.138	Enabled				Never

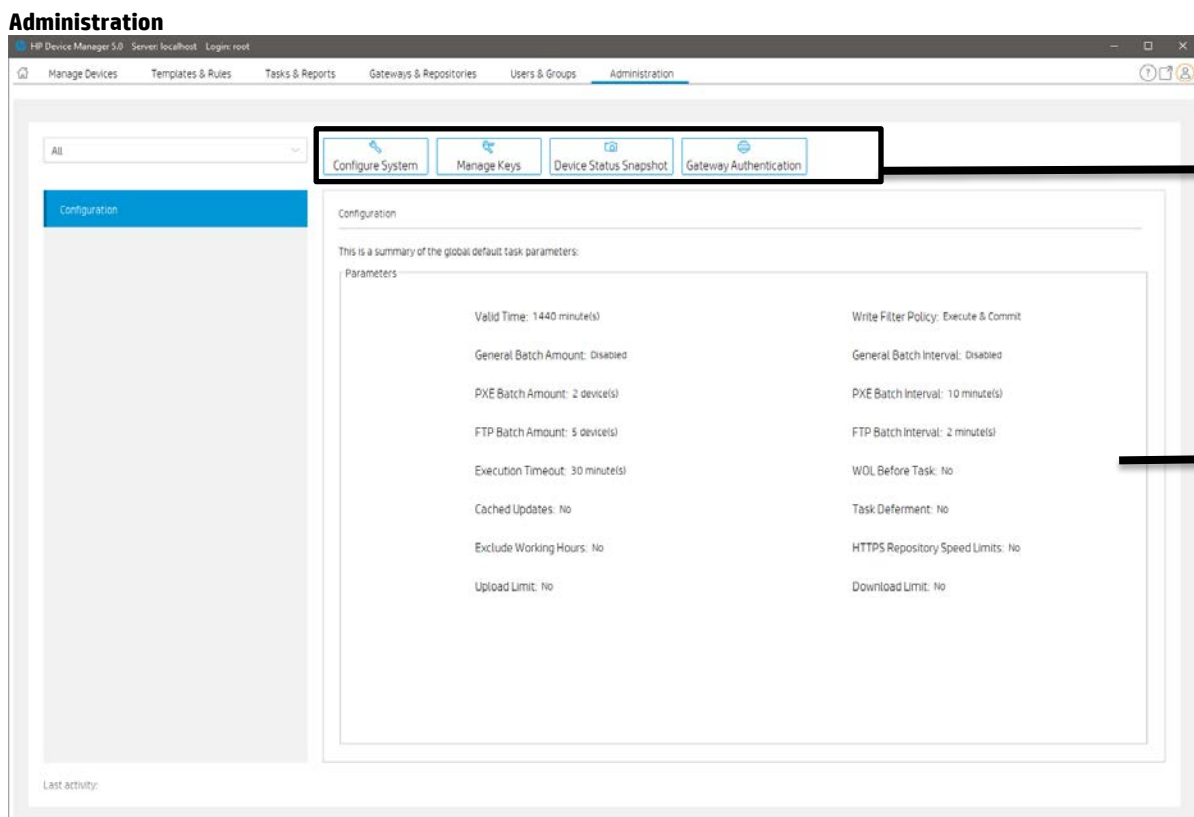
Last activity:

1. Toolbar— An enumeration of common operations.

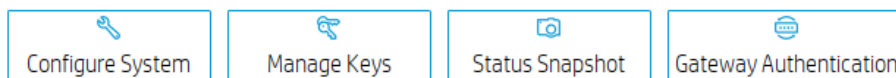
Discover HPDM Gateway Find HPDM Gateway Add Repository Import Repository Sync Repository Mapping Policy

- Discover HPDM Gateway—Discover 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 done 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—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.



1. Toolbar— An enumeration of common operations.



- Configure System—Configuration management
- 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 will check the key passed by HPDM Server before executing tasks.
- Status Snapshot—Status snapshot schedule.
- Gateway Authentication—HPDM Gateway access control.

2. Configuration View—Summary of the global default task parameters.

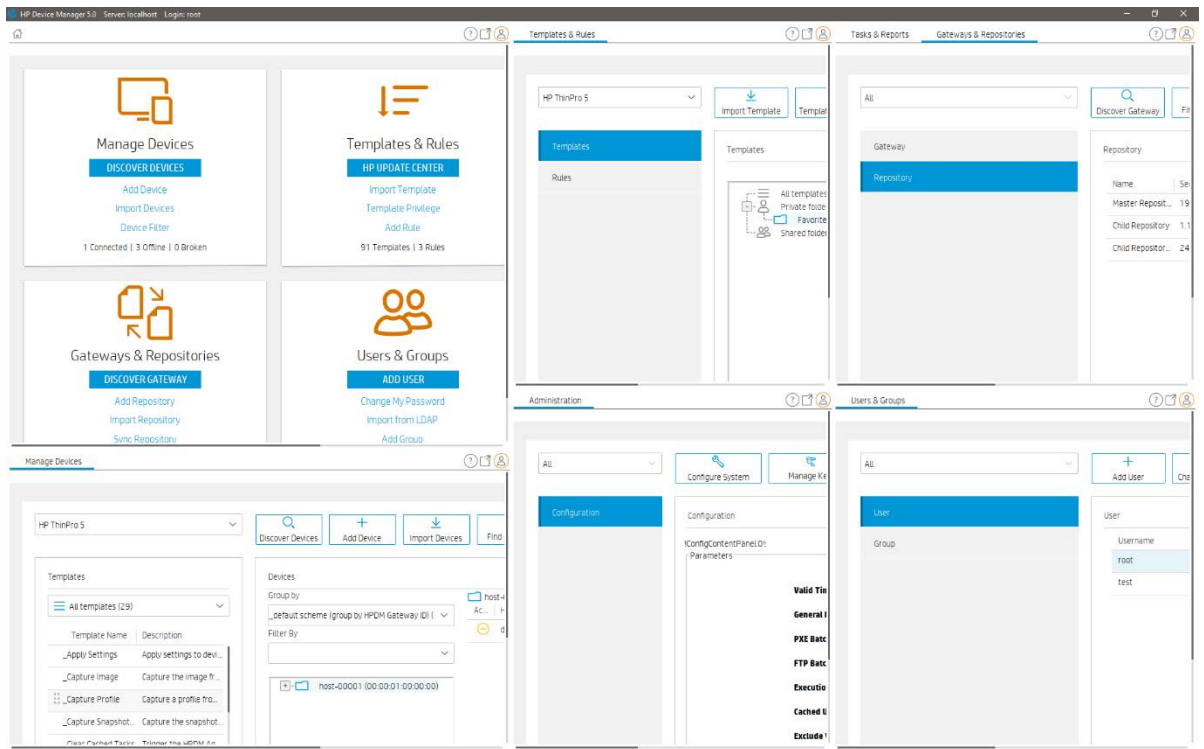
## Console management

### Docking Controls

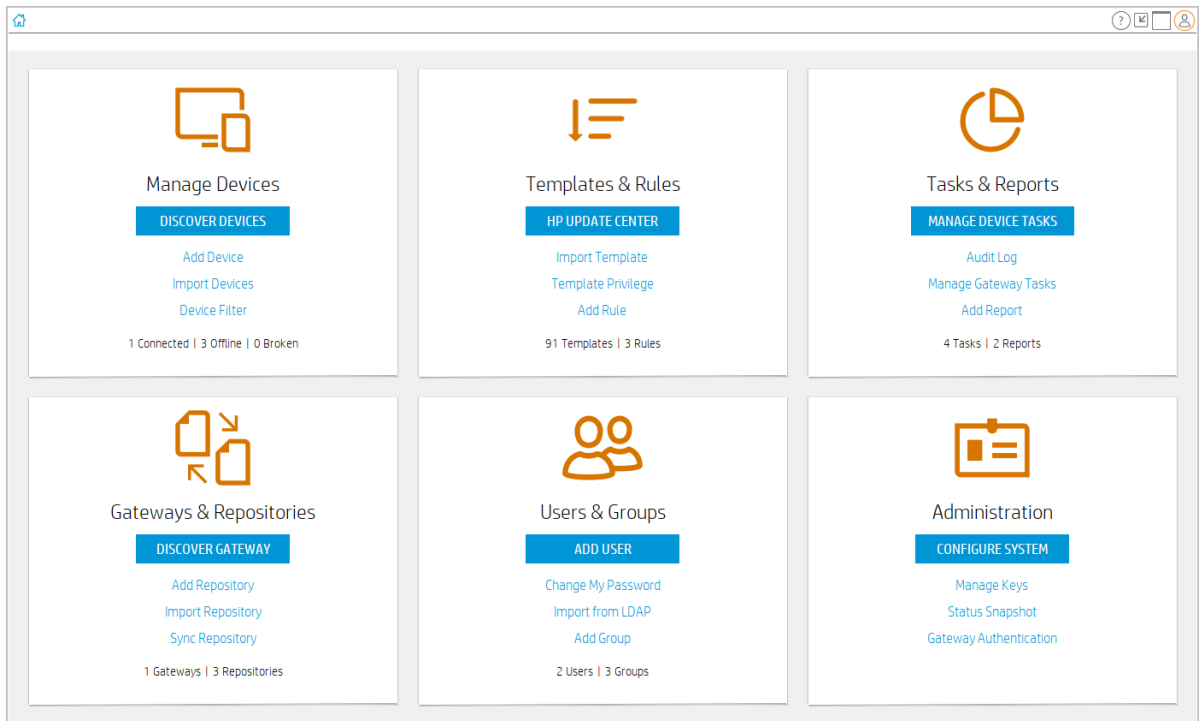
You can personalize the layout of console and unlock tabbed pages to utilize multiple displays.

1. All page support personalized layout.



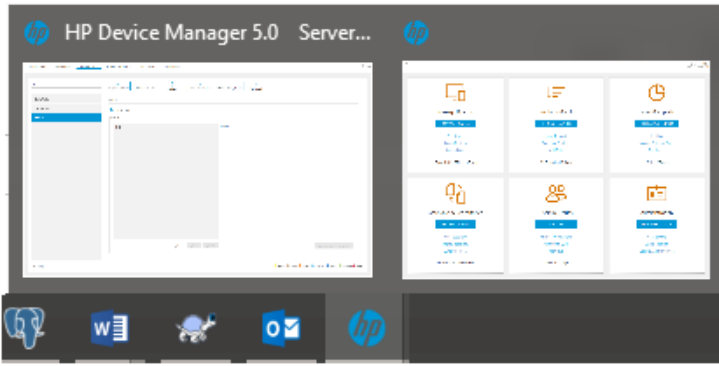


2. All Page can be dragged out of the main window, and can be maximized.

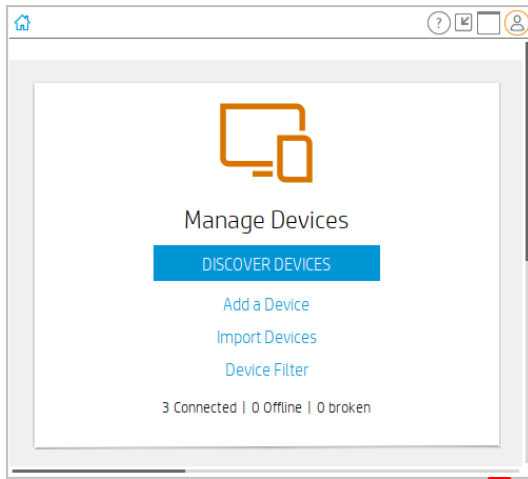


- Each window can be resized and positioned separately.
- An independent window can be merged with other independent windows.

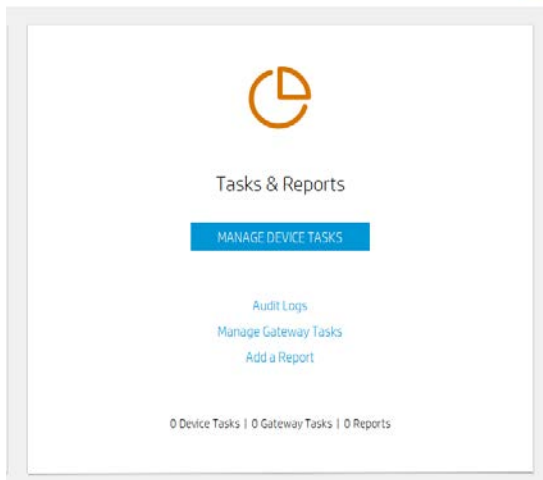
A detached window will be displayed in the taskbar of Windows. When the main window is closed from the taskbar, the console will be closed. When a detached window is closed from the task-bar, the paged will be displayed in the main window again.



Detach/Back to controller window  
Maximize the current window



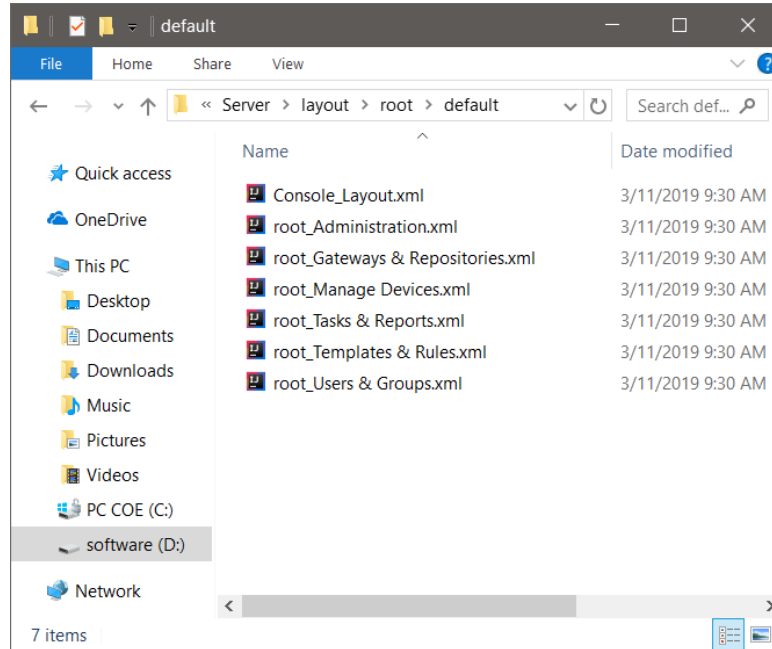
The current window back to the size and position before the maximized operation.



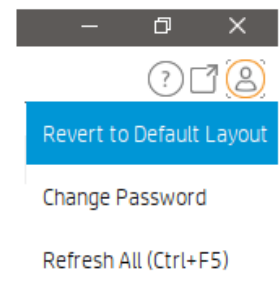
### Layout Management

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 (Ends the console through task manager, the computer suddenly loses power, and so on...) does not save the console layout and content to the server.

All documents are as followed :



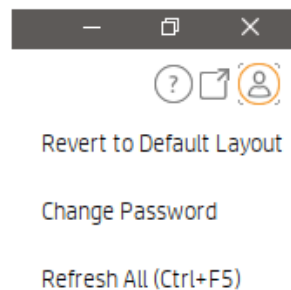
In the profile menu there is a menu item "Revert to default layout" which is used to restore to the default layout. As followed:



This menu item ("Revert to default layout") is used to restore to the default layout/content of the console. Also clear all the changeable items in the console. The same as the user's first login to the console.

### User Profile

The actions associated with the current user.



Revert to default layout—Let the console return to the default layout.

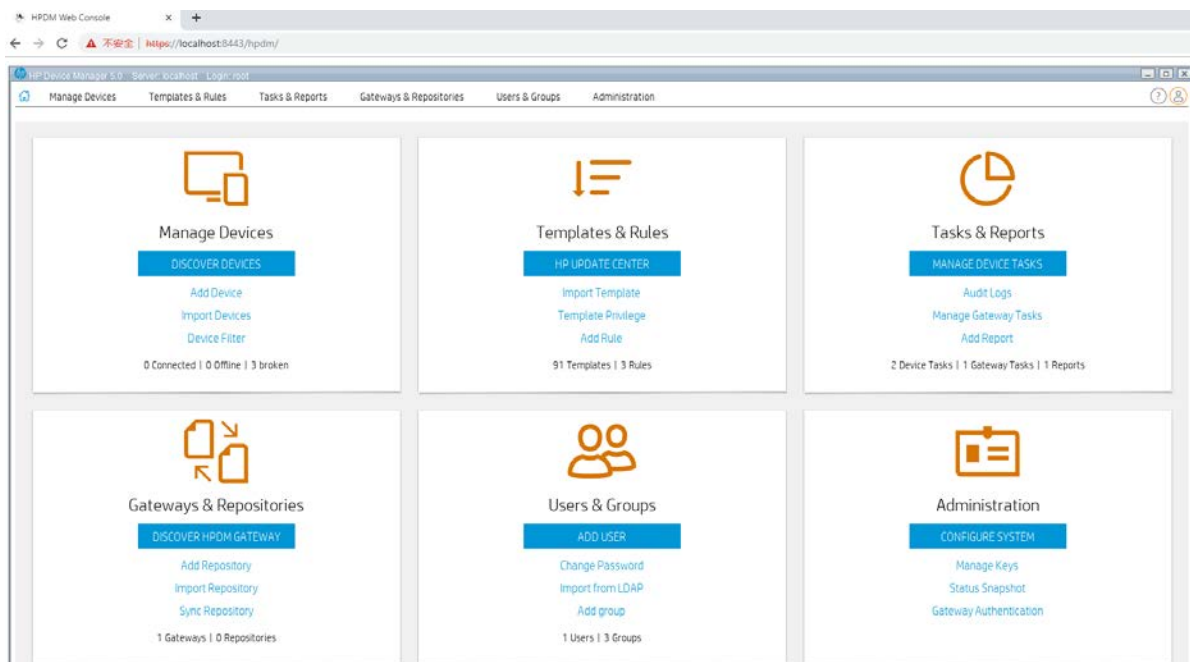
Change password—Change current user’s password.

Refresh All (Ctrl+F5)— Refresh the contents of the entire console.

### Console Web Bridge

To start a web console, visit the link <https://server-address:8443/hpdm> in a browser. The GUI of a web console is almost the same as a HPDM console. Therefore, usage of a web console is similar with usage of a HPDM console.

Figure 10. Web Console in Firefox



#### Functionality comparison with HPDM Console

The main purpose of HPDM Console Web Bridge is to provide a convenient access to HPDM Console users. It is not designed to replace HPDM Console. For daily usage, it is still highly recommended to use HPDM Console.

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

Table 1. 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	✓	

#### Note

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

## Device Discovery

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

### Automatic registration

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

1. Current gateway
2. Backup gateway
3. The gateway listed by DHCP tag 202
4. The gateway listed by the DNS server
5. The gateway or gateways listed in DNS service records
6. The gateway that responds to the broadcast from the device

---

### Note

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

---

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

### DNS service records

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

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

---

### Note

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

---

#### *Creating a DNS service record*

1. Open the DNS console.
2. Right-click the domain, and then select **Other New Records**.
3. Select **Service Location (SRV)**.
4. Select the **Create Record** button.
5. Set the service as **\_hpdm-gateway**.
6. Set the protocol as **\_tcp**.
7. Optional: Set the priority to a numerical value (lower values indicate a higher priority).
8. Set the host as the fully qualified domain name (FQDN) of the gateway.
9. Select **OK**.
10. Optional: Repeat steps 4–9 to add additional records.
11. Select **Done**.

### Troubleshooting

1. Verify the network information (including the IPv4 address and domains) of the device.
2. Use the following command to make sure the device can get DNS service records:
  1. Microsoft Windows:

```
nslookup -timeout=30 -type=SRV _hpdm-gateway._tcp.<domain name>.com
```
  2. HP ThinPro:

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

### Setting a static domain name (Windows only)

1. Open the Network Connections dialog via Control Panel or the network notification icon.
2. Right-click the network adapter and select **Properties**.
3. Left-click the **Internet Protocol Version 4 (TCP/IPv4)** item in the list, and then select the **Properties** button.
4. Select the **Advanced** button.
5. Select **DNS** tab.
6. Select **Append these DNS suffixes (in order)**, and then add the DNS domain to the list.
7. Select **OK**.

### 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 specified Gateway**. Each of these methods begin in the same manner:

1. In HPDM Console, select the **Gateways & Repositories** page.
2. Click **Gateways** on the navigator view, all Gateways are listed on the details view.
3. Right-click the desired HPDM Gateway and select **Discover Device** in the menu.
4. Proceed to Using the Scan using IP Range method on page x, Using the Scan using IP List method on page x or Using the Scan using subnet of specified Gateway on page x, depending on the method you wish to use.

Or

1. In HPDM Console, select the **Homepage** or the **Manage Devices** page.
2. Click **Discover Devices**.
3. Select the desired HPDM Gateway.
4. Proceed to Using the Scan using IP Range method on page x, Using the Scan using IP List method on page x or Using the Scan using subnet of specified Gateway on page x, depending on the method you wish 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**.
2. You can specify the range of IP addresses to search by using either an IP scope or by manually specifying an IP range. An IP scope is a range of IP addresses that you have built and saved for future scans.

To search using an IP scope:

- 3a Select the **Use Preset IP Scope** checkbox, select an **IP Search Scope**, and then select **OK**.

To search using a manually-specified IP range:

- 3b Deselect the **Use Preset IP Scope** checkbox, enter a **Starting IP Address** and an **Ending IP Address**, and then select **OK**.

---

### Tip

### *Configuring an IP scope*

To configure an IP scope:

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

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

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

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

### **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 select **Next**.

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

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

### **Manually registering a device**

To manually register a device:

1. In HPDM Console, select the **Gateways & Repositories** page.
2. Click **Gateways** on the navigator view, all Gateways are listed on the details view.
3. Right-click the desired 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 dropdown list, and then select **OK**.

Or

1. In HPDM Console, select the **Homepage** or the **Manage Devices** page.
2. Click **Add Device**.
3. Enter the device ID, MAC address, and IP address of the device.
4. Select an operating system from the dropdown list.

5. Select a HPDM Gateway from the dropdown 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

This section demonstrates how to use the Automated Device Importer feature within HPDM. 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.

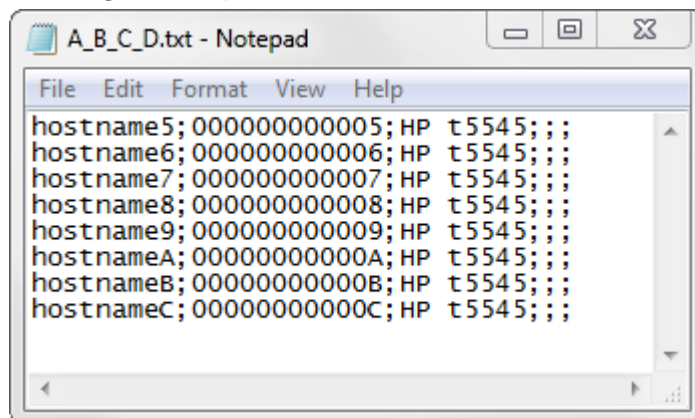
#### Input file preparation

1. Create a folder containing some 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 a “;” or a “,” character.
4. The columns must be in the following order:

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

5. The hostname and MAC columns are required.
  - a. MAC is used as unique device ID. Entries in the formats AABBCDDDEEFF or AA:BB:CC:DD:EE:FF are both accepted.
  - B. HPDM can send a task to rename a device if the hostname of the registered device in the database differs from the hostname 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 will be updated as soon as a device reports to the HPDM Server.
  - i. **Type**—Indicates the device type, such as HP t610.
  - ii. **OS**—Indicates the device OS family, such as WES 8 64 bit or HP ThinPro 4. If the OS family is not specified, the device is added to the Unidentified. The device moves to the correct tab when it reports to the HPDM Server.
  - iii. **gw**—Indicates 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.

7. The following is an example of valid content in txt:





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

	A	B	C	D	E	F
1	hostname	mac	type	sn	os	gw
2	myHostname	00000000000D	HP t610	A23456789	HPXPe	gw
3	MXL2090FBV	9C8E99D4988A		MXL2090FBV		
4	9C8E99D49931	9C:8E:99:D4:99:31		MXL2090FC2		
5						
6						
7						
8						

9. The expected behavior is as follows:

- i. All new devices are imported.
- ii. The First Contact Rules for new devices are not triggered until they report to the HPDM Server.
- iii. All known devices are ignored unless there is hostname change.

#### *Importing devices*

To manually register multiple devices:

1. In HPDM Console, select the **Homepage** or the **Manage Devices** page.
2. Click **Import Devices**.
3. Select the **Select** button, 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 will only allow 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 GUI.

#### *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 is an example of the content of importer.conf:

```

1 #Device Management Console Profile Properties
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

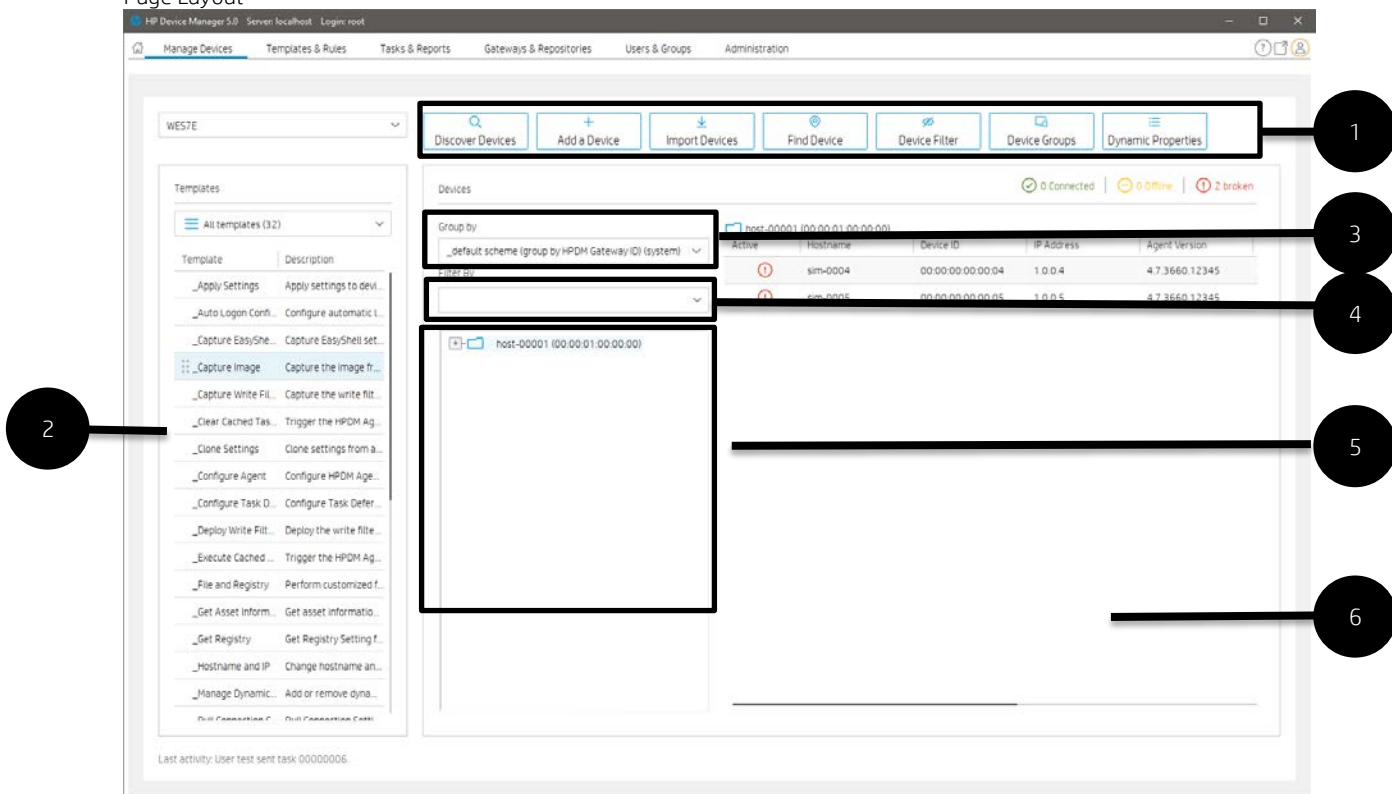
Remove this line to select import path on next run

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

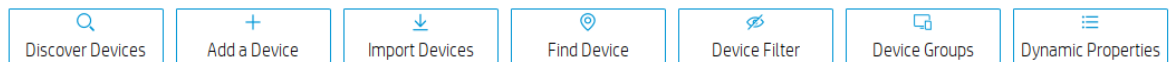
You can create a Scheduled Task to run this importer periodically. Go to [http://technet.microsoft.com/en-us/library/cc786711\(ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc786711(ws.10).aspx) for more information.

## 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.
- 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, 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 3 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** from the menu.

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** from the menu.

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)

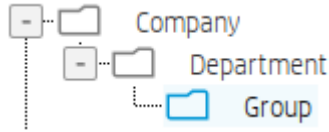
In addition, you can use the device asset information to filter the devices. This enables you to divide your devices into sets and then assign those sets to specific administrators.

#### *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 to this, you can include a special parameter labeled MG and set it to a path to use for manual grouping. This path is used to create a subtree in the device tree of HPDM Console when manual grouping is selected.

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



The format that is used by HPDM for tag 203 is as follows:

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

---

**NOTE:**

All the parameters are optional, but any that are specified must be assigned a value.

---

For example:

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

*Switch to Manual Grouping*

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

*Adding a new Manual Group*

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

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

**Dynamic Grouping**

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

*Creating a new Dynamic Grouping scheme*

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

*Switching to a Dynamic Group*

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

*Quick search*

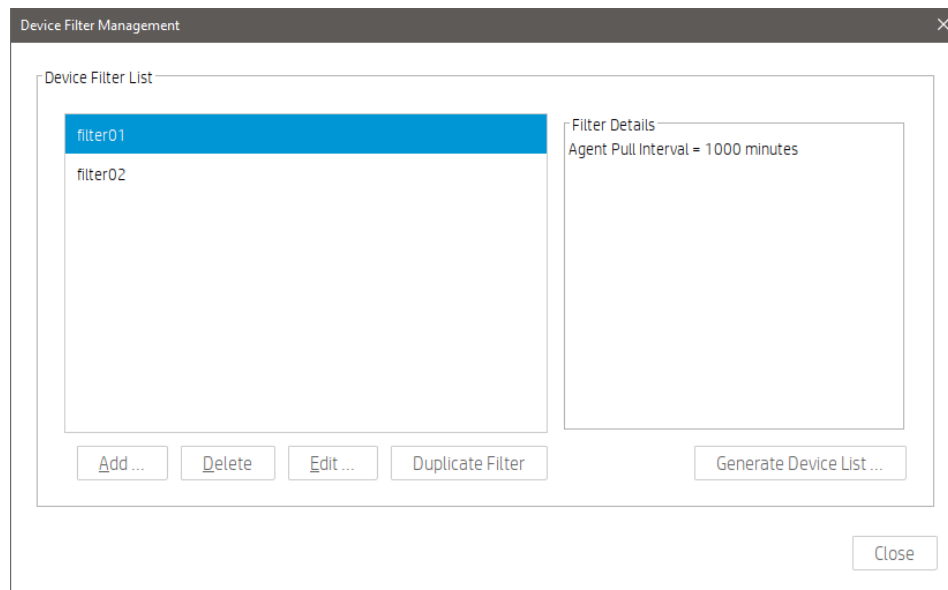
HPDM enables you to search quickly among currently listed devices. You can select any column header in the device table to add a search criteria or sort. All criteria are automatically cleared after switching to another folder.

## Filtering devices

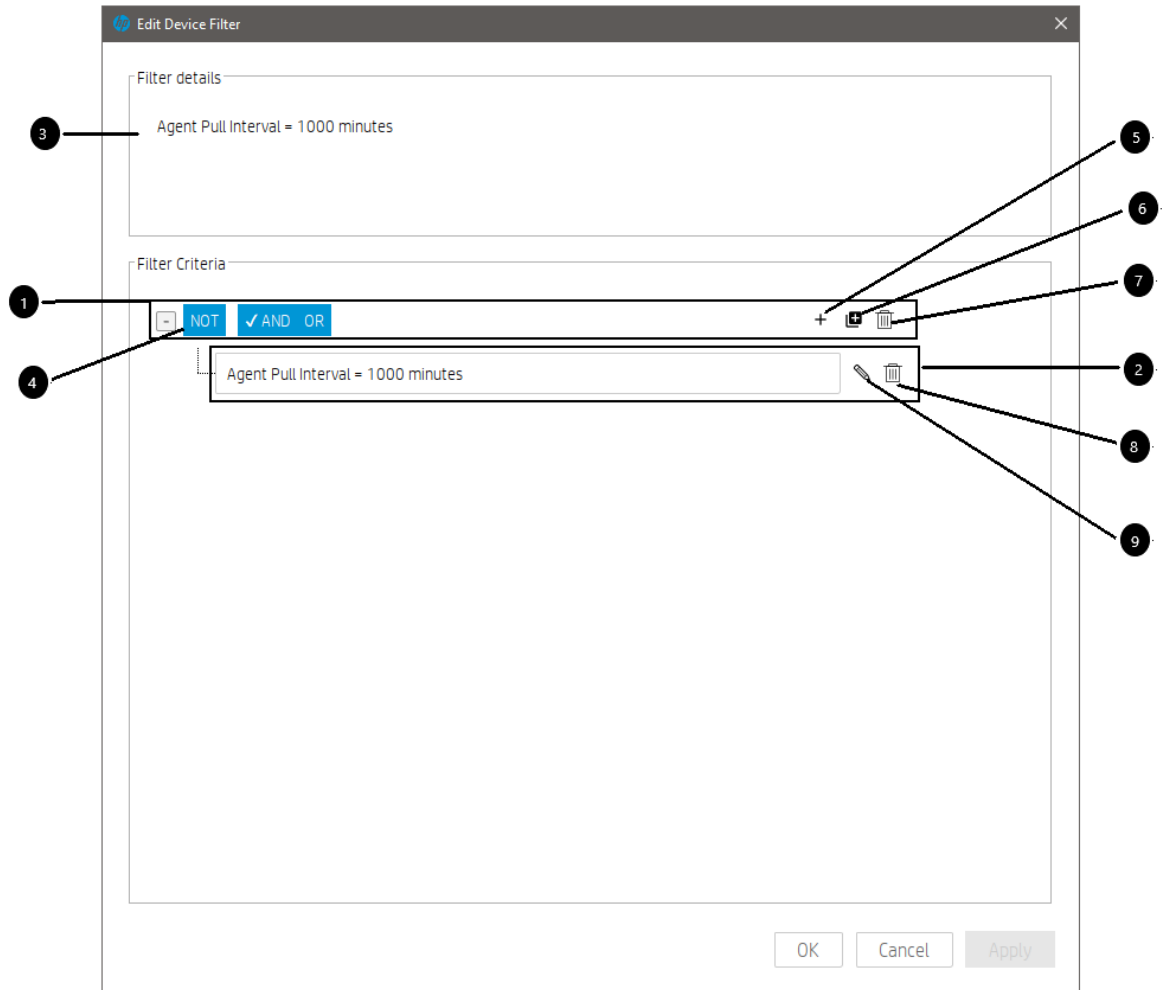
Filtering enables you to work with a subset of your devices. It can be combined with User Privileges to divide the management of your devices between different administrators.

### Create a new Device Filter

1. Select the Manage Devices page, click Device Filter toolbar button.
2. Pop up Device Filter Management window.

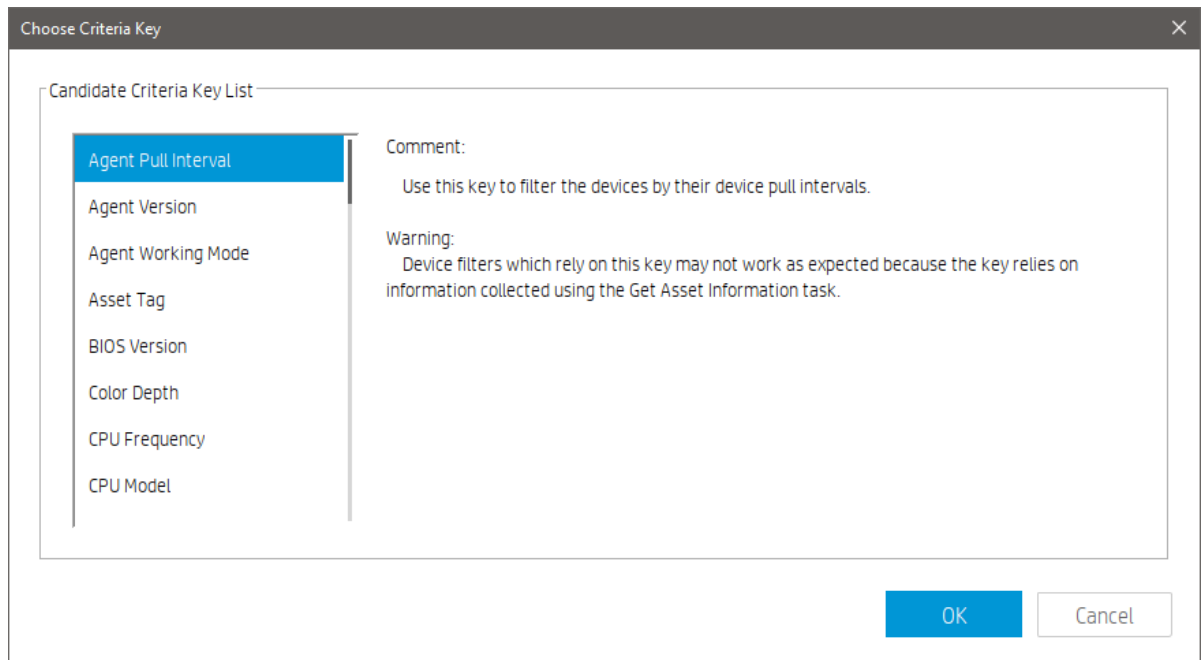


- 1) Generate Device List: Show all matched devices.
  - 2) Duplicate Filter: Copy a selected filter as basic to create a new filter.
3. Click **Add...** button.
  4. Give your new filter a name. Click **OK** to accept the name.
  5. Pop Edit Device Filter window.



- 1) Filter Group
- 2) Filter Criteria
- 3) Filter details, the expression of this filter will be shown here.
- 4) Relationship button used to control the relation of child group or child criterion.
- 5) Add Criteria button used to add a child criterion under the selected group.

Pop up Choose Criteria Key window.



- Select a criteria key from the list, click OK.
- Pop up Criteria Editor window.



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

- 6) Add Group button used to add a new child group under the selected group.
  - 7) Delete the selected group.
  - 8) Edit selected criteria.
  - 9) Delete selected criteria.
6. Click **OK**.

#### *Edit a Device Filter*

1. Go to **Device Filter Management** window.
2. Select an existing filter, click the **Edit** button.
3. Pop up Edit Device Filter window.
4. Edit **Filter Group** and **Filter Criteria**.

5. Click the **OK** button.

#### *Filter Security*

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

1. Select **User & Groups** page - Groups navigation view.
2. Select a group and open group properties.
3. Select **Security Filter** panel.
4. Click **Add...** button.
5. Select the filter to use from the **Security Filter** list.

When the users under this group log on, they see that 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 it can be uniquely identified and HPDM can communicate with it. You can both view and export this information.

#### *Standard Properties*

1. Basic asset information

To display a device's basic asset information:

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

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

Basic asset information can be used to filter and group your devices.

The following table 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 t610, have a TPM chip built in.

TPM Owned—Indicates whether a TPM is owned. A TPM must be owned before it can be used to secure a computer. The ownership of a TPM is set by assigning a password to it so that only the authorized TPM owner can access and manage the TPM. Only one password exists per TPM, so anyone who knows that password is effectively the TPM owner. Once an owner is set, no other user or software can claim ownership of the TPM.

Base Snapshot— Indicates the base snapshot of the device.

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.



2. the basic asset information available on the Agent page

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.

3. the other asset information available on the other page

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

Command	Description
<code>set &lt;key&gt; &lt;value&gt;</code>	Sets a grouping property, overriding the original one
<code>unset &lt;key&gt;</code>	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:

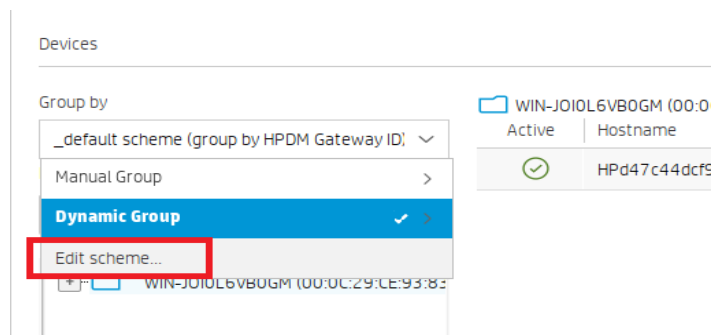
```
schtasks /create /tn DailyUpdateNIC /tr UpdateNIC.bat /sc hourly /ru SYSTEM /rp MyPassword
```

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

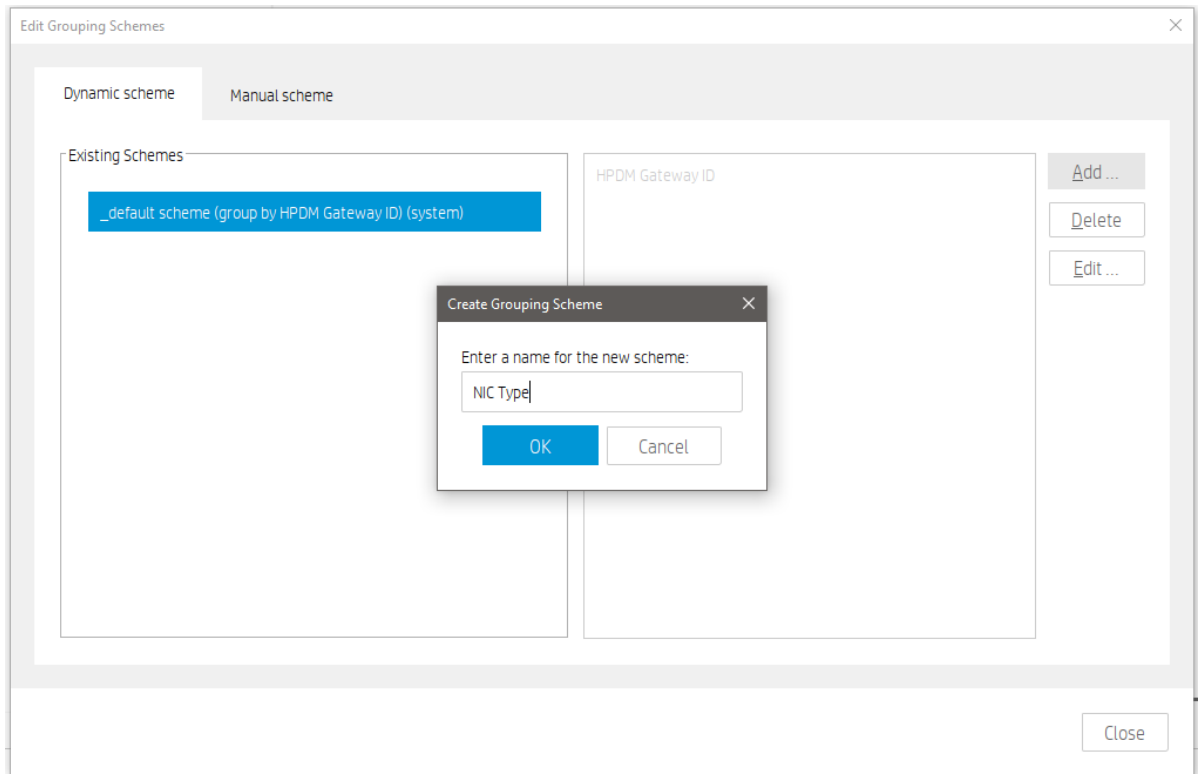
*Example procedure*

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

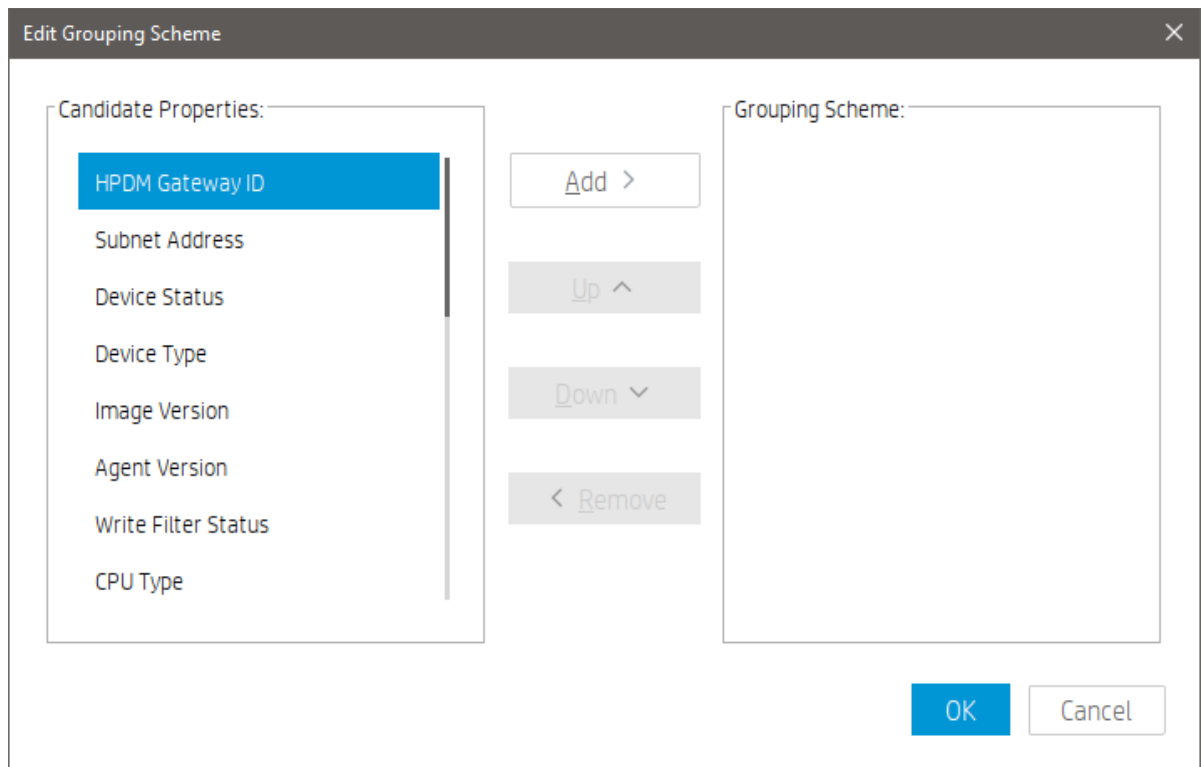
1. Remotely execute a script on the thin client that retrieves the NIC card type and assigns it to grouping key (P3 for this example).
2. In HPDM Console, select **Group by**, and then select **Edit scheme**.



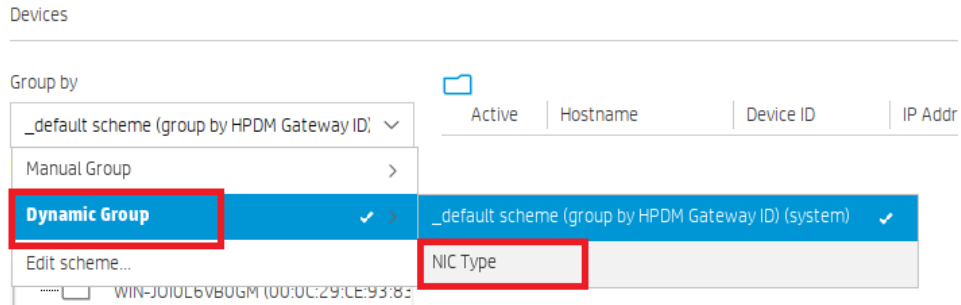
3. In the Edit Grouping Schemes dialog box, select **Add**, enter NIC Type (or any custom name) for the grouping scheme name, and then select **OK**.



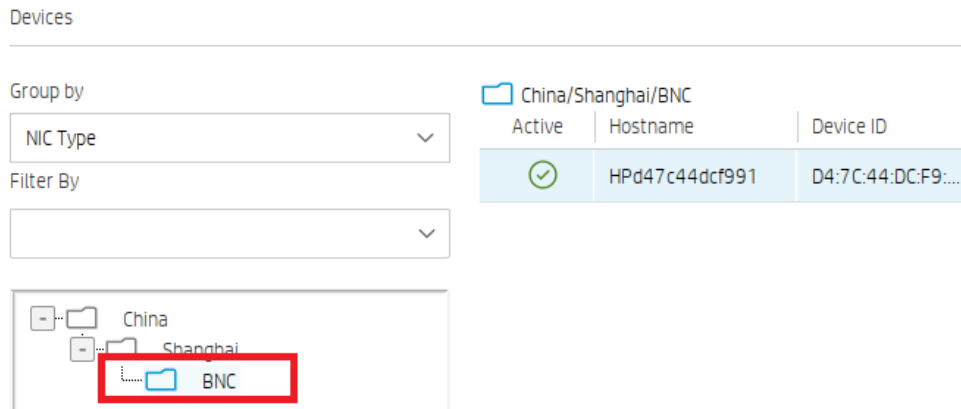
4. Select extension properties 1–3, select **Add**, and then select **OK**.



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

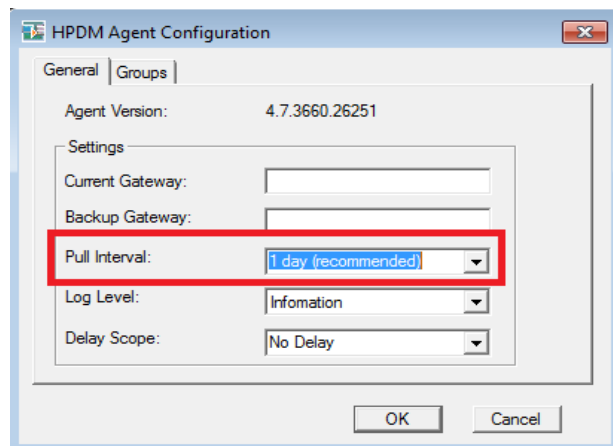


Devices are now grouped by NIC type, such as BNC.



### Note

It might take some time for the new grouping properties to display in HPDM Console after being sent by HPDM Agent to HPDM Server. If you can't see the change in HPDM Console after some time, try reducing the Pull Interval setting in HPDM Agent on the device side, or try restarting the thin client.



### Dynamic Properties

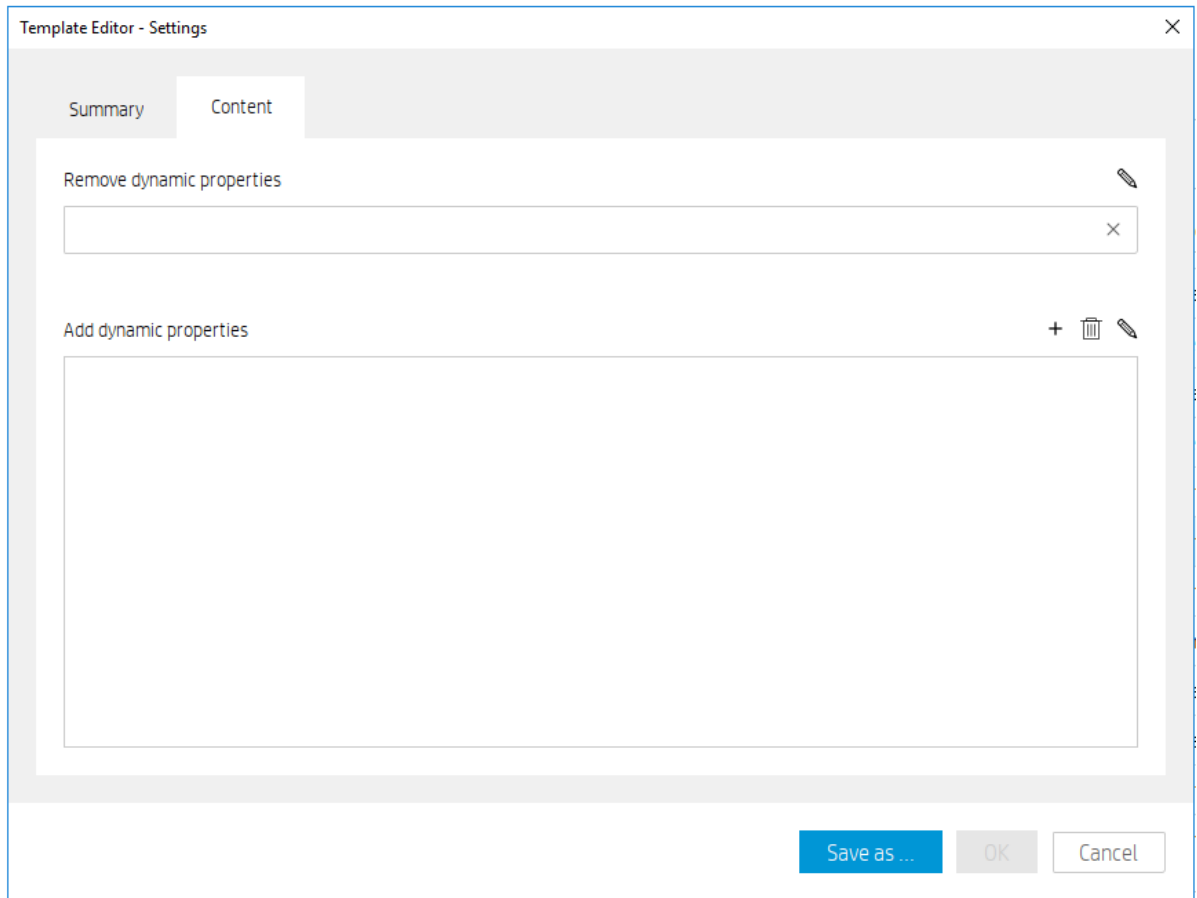
Dynamic properties are designed for HPDM administrator to use as many properties as they are interested in. Currently there are three types of dynamic properties:

- **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.

Figure 11. Template Editor of **\_Manage Dynamic Properties**

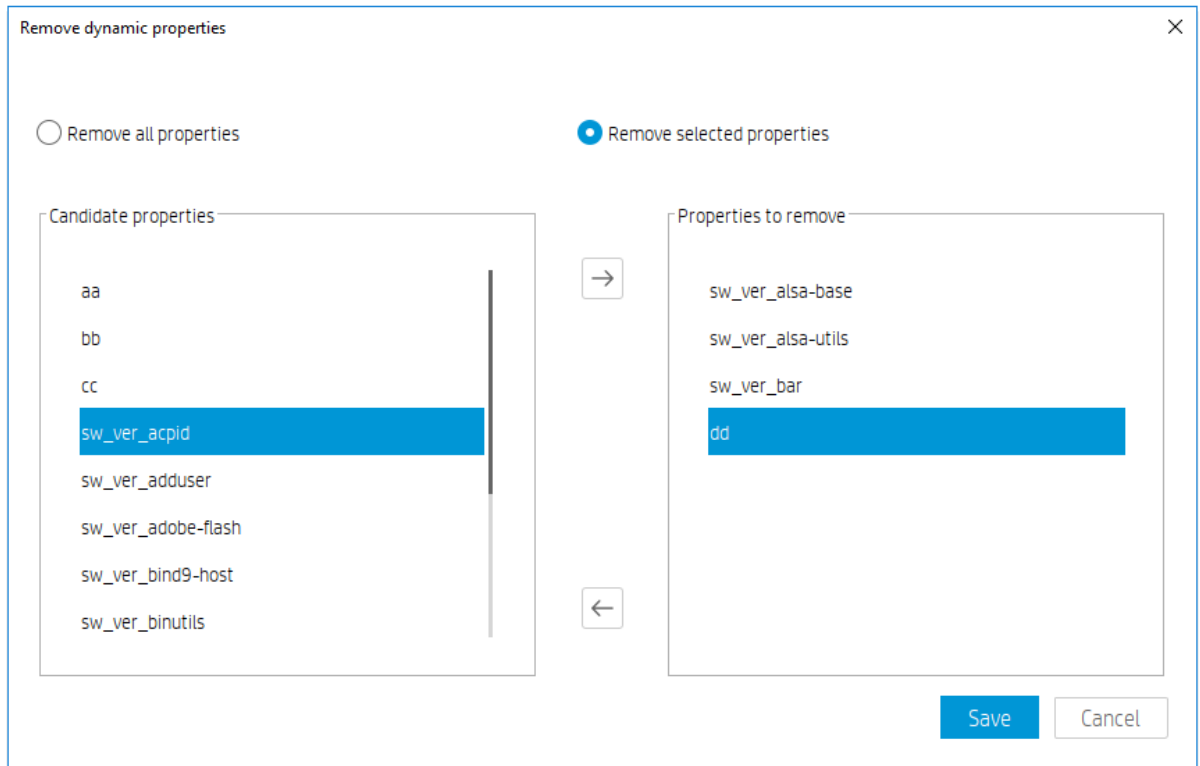


If both sections are defined in the task template, **Remove dynamic properties** action is always performed before **Add dynamic properties** action since HPDM administrator may clean up old properties before adding new properties.



### 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.

Figure 12. Dialog Editor of Remove dynamic properties



To remove dynamic properties from the target device

1. Open the template editor of **\_Manage Dynamic Properties**. Click  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  to reset text box if you want to abandon your previous selections.

**Figure 13.** Remove dynamic properties section



**Note**

As shown in above figure, dynamic properties in Candidates properties are the set of all properties of specific OS 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 will be reported, otherwise no value will be reported.

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

Figure 14. Dialog Editor of Add dynamic properties

**Add dynamic properties** [X]

**Schedule**

Check interval

30 minutes

**Properties**



Software version  
 Microsoft Hotfix  
 Customized script

Property Name

Software Name [X] v

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** and **Customized Script**.
4. If **Software version** or **Microsoft Hotfix** is selected, select a software name of Microsoft hotfix from the drop-down list. Property name will be created automatically.
5. If **Customized script** is selected, input property name and script content in the corresponding text boxes.
6. **Sample Scripts** are provided and can be accessed by hovering mouse on it. A pop-up text editor lists all sample scripts you can refer to. Click **←** or **→** to navigate and **+** to use the sample script.
7. Select **SAVE** to save one custom property and property name will show in the list.
8. Select the saved property name. Click  to edit it and  to delete it.

---

**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.

---

**Figure 15.** Sample Scripts

Add dynamic properties ×

**Schedule**

Check interval

30

**Properties**

Software version

Microsoft Hotfix

Customized script

Property Name

loginName

Script

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

echo value=%loginName%

[Sample Scripts](#)

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

echo value=%loginName%

---

**Note**

As shown in figure 14, drop-down list content of property name or Microsoft Hotfix is empty. The content can be retrieved after performing Get Asset Information on devices.

---

**Figure 16.** Add dynamic properties section lists new dynamic properties

Add dynamic properties + 🗑️ ✎

loginName

ms\_hf\_KB1234567

sw\_ver\_citrix



### Collect dynamic properties

There are two ways of collecting dynamic properties:

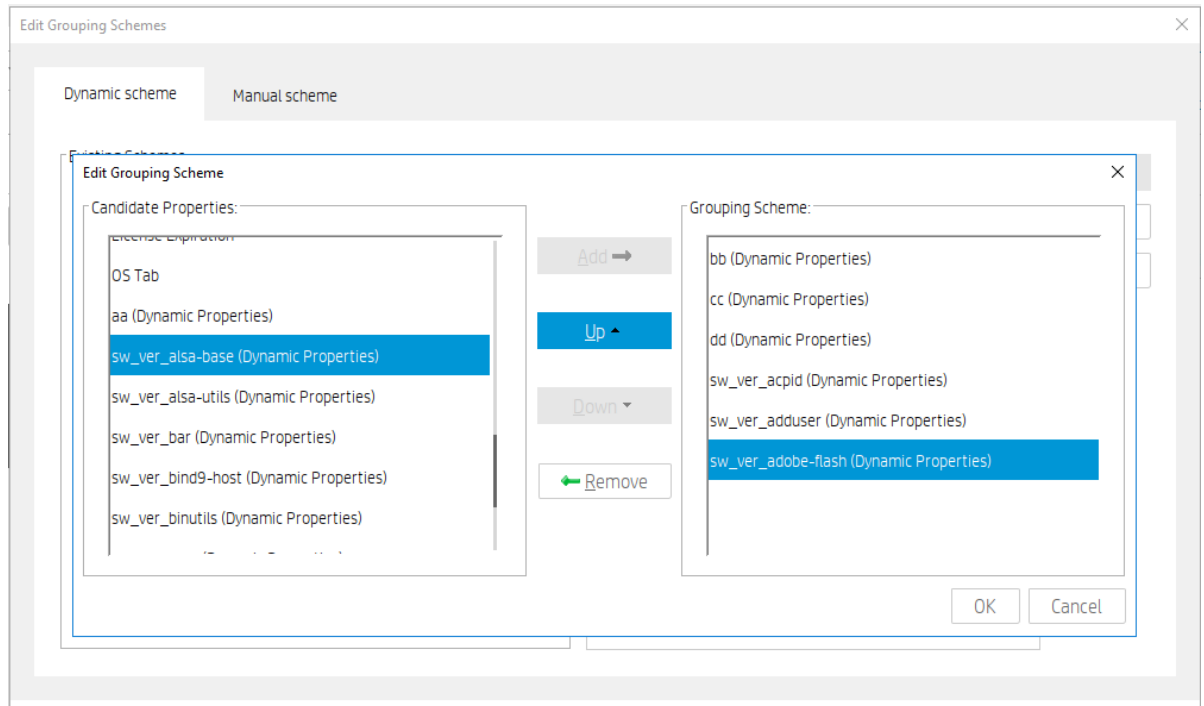
- Perform a Get Asset Information task to retrieve all dynamic properties from devices. View dynamic properties in Dynamic Properties page of the Device Properties window.
- Perform a Manage Dynamic Properties task to add multiple dynamic properties. Agent will immediately report the values and afterwards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

### Manage Devices with Dynamic Properties

#### Device Groups

HPDM administrator now can group device by dynamic properties. When creating or editing grouping scheme, dynamic properties can be easily identified by an indicator (Dynamic Properties).

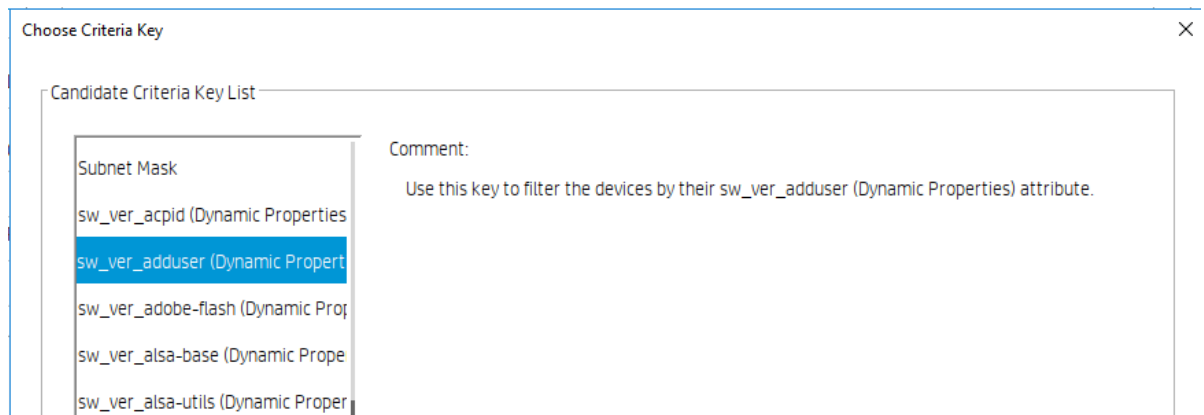
**Figure 17.** Dialog of **Edit Grouping Scheme** with Dynamic Properties



#### Device Filter

HPDM administrator now can filter device by dynamic properties. When creating or editing criteria key, dynamic properties can be easily identified by an indicator (Dynamic Properties).

**Figure 18.** Dialog of Choose Criteria Key

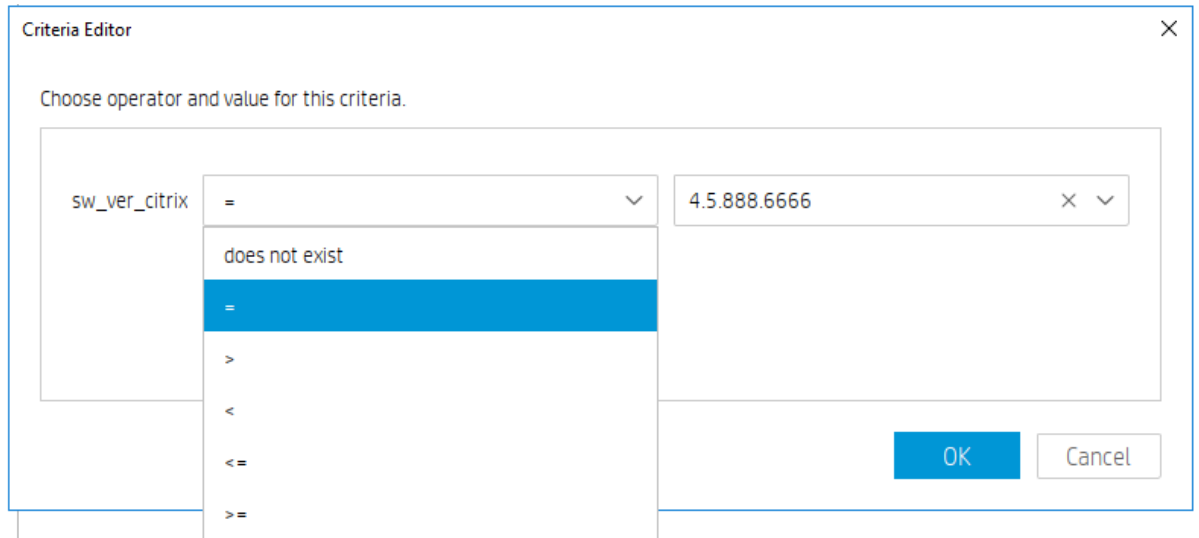


Currently there are two sets of operators applied to dynamic properties:

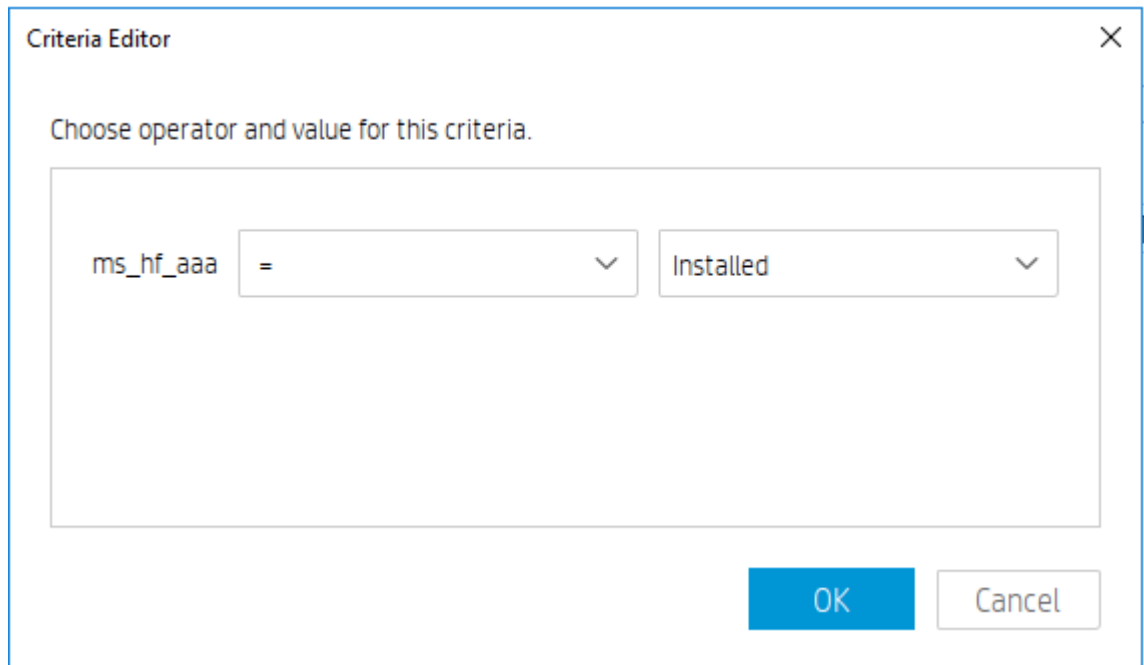
As for **Software versions** and **Customized script**, the set of operators is: does not exist, =, >, <, <=, >=.

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

**Figure 19.** Dialog of Criteria Editor - Software version



**Figure 20.** Dialog of Criteria Editor – Microsoft hotfix



#### Device Table

HPDM administrator now can view devices with dynamic properties. When choosing columns, dynamic properties can be easily identified by an indicator (Dynamic Properties). Choose and order columns as following figures will allow you to view dynamic properties of devices under the current selected OS.

**Figure 21.** Dialog of Choose Columns for device table

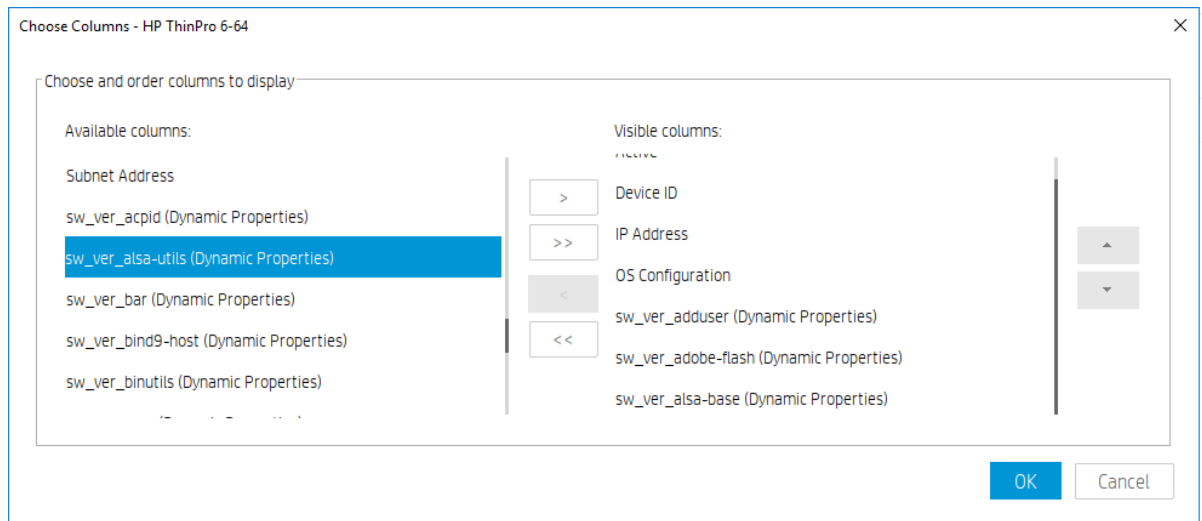


Figure 22. Device table with dynamic properties

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

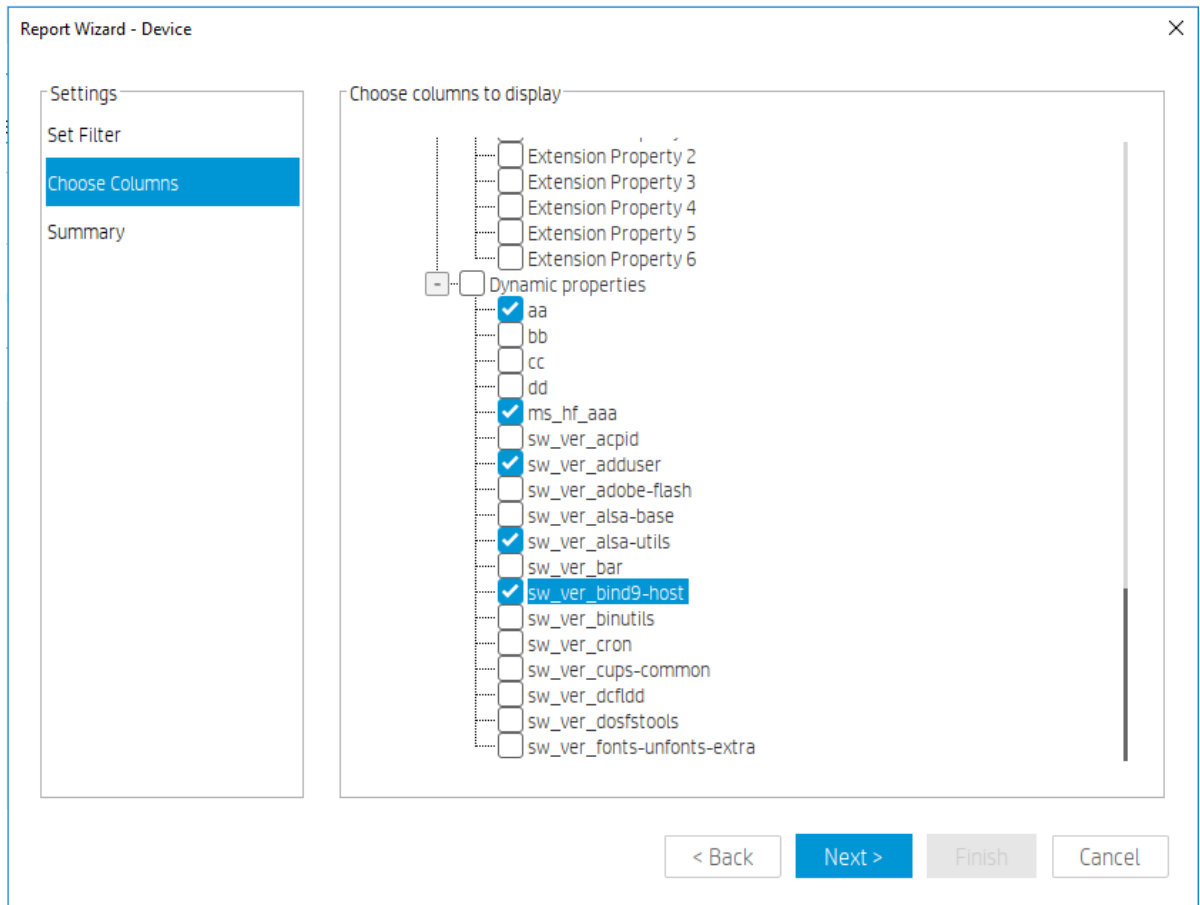
#### Device Report

HPDM administrator now can generate device reports with dynamic properties.

#### To generate a device report with dynamic propertis

1. Go to **Tasks & Reports** tab.
2. Choose Reports in the left panel and select Device for report type.
3. Click Add to open Report Wizard – Device.
4. Select several properties in dynamic properties section. Refer to below figure.
5. Follow the rest steps of wizard and generate a report.

Figure 23. Choose Columns step in Report Wizard

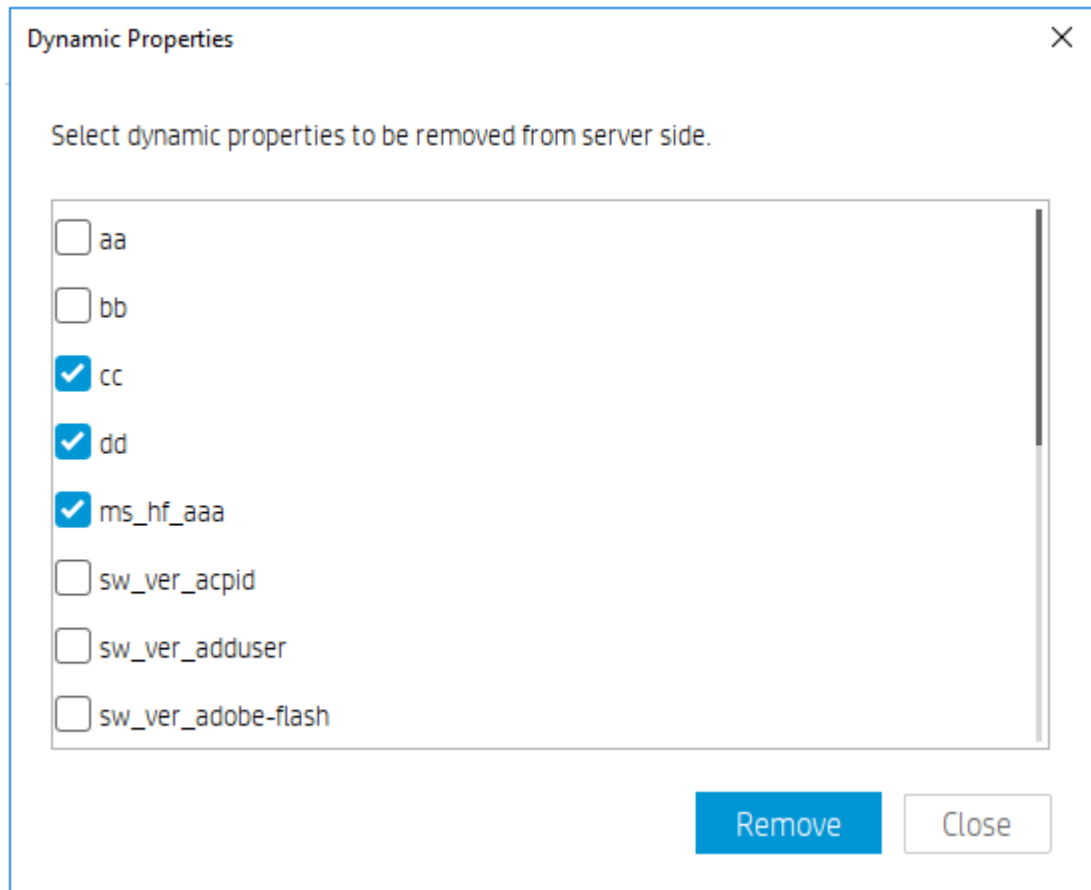


*Delete dynamic properties from server side*

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. Click **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 in the list.
3. Click Remove to remove the custom properties from server side.
4. Click Close to close the editor.

**Figure 24.** Dialog of Dynamic Properties



### Checking device connection status

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

1. In the device table, select one or more devices, right-click and select **Check Connection Status** from the context menu.
2. Select the utility you want to use to check the connection status of the device. You can choose from:

- **Ping**—A basic Internet program that lets you verify that a particular Internet address exists and can accept requests. Pinging is diagnostically used to make sure that a host computer, which you are trying to reach, actually operates.
- **Trace Route**—This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer.

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

3. Select **Close**.

### Template Navigator

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

---

#### NOTE:

Templates in Template Navigator are not editable.

---

## Templates & Rules

HP Device Manager is designed to centrally control and monitor devices. The primary mechanism used to drive configuration changes and updates to devices is through Templates, Tasks, and Rules.

- **Templates** represent a plan or set of instructions that can be executed which can be edited, organized and shared between administrators.
- **Tasks** represent the manifestation of a given Template on a managed device; and can be tracked 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

Type	Template	Description	Base template	Category	Status	Modified	Modified by
⊖	_Apply Settings	Apply setting...	_Apply Settings	Settings		2019-04-0...	
⊖	_Auto Logon Con...	Configure aut...	_Auto Logon C...	Settings		2019-04-0...	
⊖	_Capture EasySh...	Capture Easy...	_Capture Easy...	Settings		2019-04-0...	
⊖	_Capture Image	Capture the i...	_Capture Image...	Imaging		2019-04-0...	
⊖	_Capture Write F...	Capture the ...	_Capture Write...	Settings		2019-04-0...	
⊖	_Clear Cached T...	Trigger the H...	_Clear Cached...	Operations		2019-04-0...	
⊖	_Clone Settings	Clone setting...	_Clone Settings	Settings		2019-04-0...	
⊖	_Configure Agent	Configure HP...	_Configure Age...	Agent		2019-04-0...	
⊖	_Configure Task ...	Configure Tas...	_Configure Tas...	Agent		2019-04-0...	
⊖	_Deploy Write Fil...	Deploy the w...	_Deploy Write ...	Settings		2019-04-0...	
⊖	_Execute Cached...	Trigger the H...	_Execute Cach...	Operations		2019-04-0...	
⊖	_File and Registry	Perform cust...	_File and Regis...	File and ...		2019-04-0...	

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



- Import Template—Import templates from a file (xml, zip).
- Template Privilege— there is an additional template privilege to control each template, including viewing, modifying, and executing operations.
- HP Update Center—Allows you to leverage software components from the HP FTP server for use as payload.
- Add Rule—Create a new Rule.
- Import Rule—Import 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**—Indicates 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**—A generic template consisting of a customizable combination of tasks for managing device operating systems
  - **Connections**—Used to get or set the connection settings of a device
  - **Agent**—Used to configure HPDM Agent settings and update HPDM Agent
  - **Imaging**—Used to capture or deploy flash-memory images of devices
  - **Operations**—Used to perform various operations on a device, such as restart, shadow, shut down, and wake up
  - **Settings**—Used to change various settings on the device, such as display, network, time, and write filter
  - **Template Sequence**—Used to define sequences in which tasks are performed
- **Status**—Indicates the status of each template

The status could be one of the following:

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

- **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, like in the following example: **\_File and Registry**.

To create or edit a task template:

1. Double-click a task template.
- or –
- Right-click a task template and select **Properties** from the context menu.
2. Specify your requirements for the template using the options available. To clear a value of the target device, leave the corresponding field for that value blank on the template.
3. When you have finished defining a new template, select the Save as button and enter a name for the new template.
4. Select **OK**. The new template is created and added to the Task Templates list.

### Exporting task templates

1. Right-click the template to export and select **Export**.
2. If one or more of the selected templates utilizes payload files, you are asked if the payload files should also be exported. If you choose to export payload files, they are downloaded from the HPDM Master Repository.
3. Enter the name of the template.
4. Select the destination of the exported file.

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

### Importing task templates

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

-or-

Click **Import Template** toolbar button.

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

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

---

### NOTE:

If you want to import and export the template sequence, the Deploy image subtask of this template sequence can only be allowed to be at most one.

---

### Importing Templates Across OS Versions

#### Overview

Each template is associated with a specific operating system tab in the HPDM system. Because more operating systems are being supported and there are now more operating system tabs, some templates can be useful for devices under similar but different operating system tabs. The purpose of this document is to demonstrate how to copy a template to another supported operating system tab.

Templates might or might not 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, the templates still need to be verified case by case.

By similar operating systems, we mean either both operating systems are Windows or both operating systems are Linux.

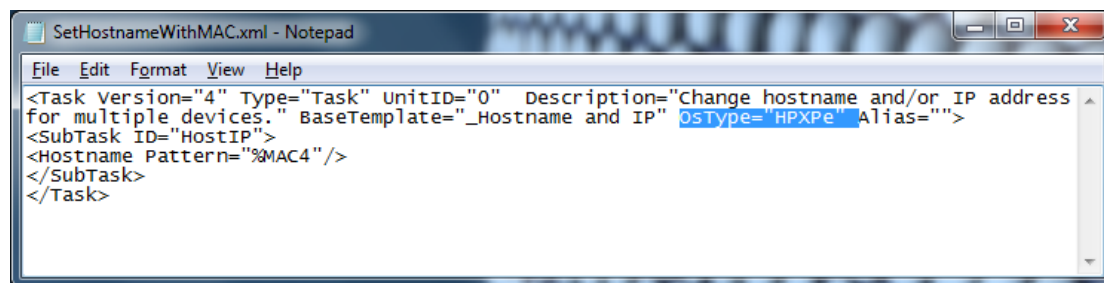
#### Preparation

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. See the following figure:



3. Change the value of this attribute to the operating system type you want to import the template into.



For example, if you want to copy the template to Windows 10 IoT Enterprise (64-bit), enter OsType="HPWE8\_64".

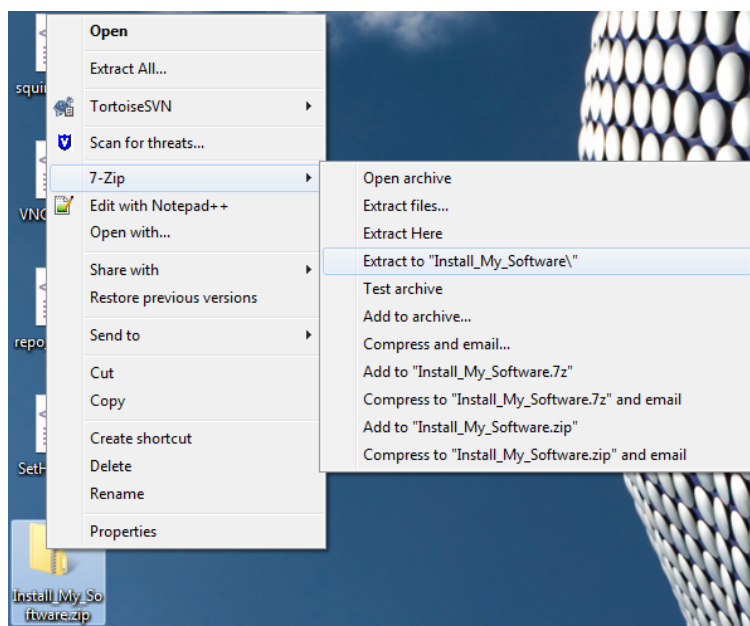
Table 1. Operating system name and database value

Operating system name in HPDM Console	OsType value in database
Windows 10 IoT Enterprise (64-bit)	HPWE8_64
Windows Embedded Standard 7P (64-bit)	HPWES7_64
Windows Embedded Standard 7E (32-bit)	HPXPe
Windows (32-bit)	Win32
Windows (64-bit)	Win64
HP ThinPro 5	HPTThinPro5
HP ThinPro 6 (64-bit)	HPTThinPro6_64
HP ThinPro 7	HPTThinPro7_64

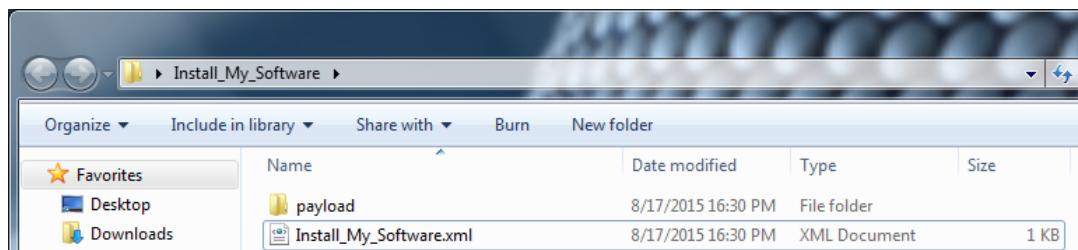
4. Save the exported XML file.

#### 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. There is a folder names payload and an XML file.



3. Open the XML file with any text editor.

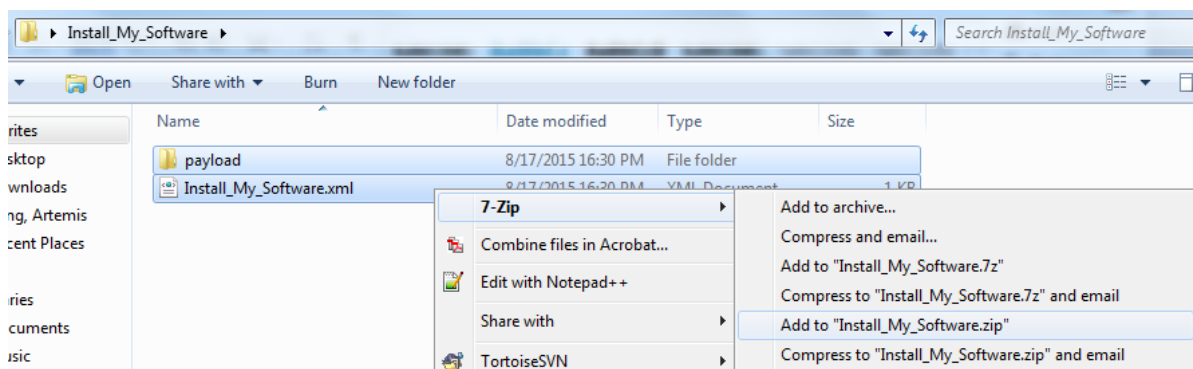
4. Find the OsType attribute. See the following screenshot:

```

<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
        <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
+f8jIkby2vGhPGw7ZlM=</Content><StartIn encrypt="aes_128_cbc" convert="base64">TlIRv4SLK0c1K
+FWqW4DlQ=</StartIn><RunAs><User encrypt="aes_128_cbc" convert="base64">FL
+02upp4VjtI196tmnlqW=</User><Password encrypt="aes_128_cbc"
convert="base64">D0djByuqdi2jToR79306W=</Password></RunAs>
      </SubTask>
    <SubTask ID="Reboot"></SubTask>
  </Task>

```

5. Change the value of this attribute to the operating system type you want to import the template into. For example, if you want to copy the template to Windows Embedded 8 Standard, 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. In the template page, right click on any template, select **Import > Exported Templates (\*.xml, \*.zip)**. Or click the **Import Template** toolbar button on the template page.
2. Select the modified XML files and then click **Import**.

#### Importing a ZIP Template

1. In the template page, right click on any template, select **Import > Exported Templates (\*.xml, \*.zip)**. Or click 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 click **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 (.ibr, .img, .hping, .dd, .dd.gz)**
2. Select the file that you want to import.
3. Select **Import**. Then add payload information in the **Package Description Editor** dialog box.
4. Select **Generate**.

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




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

1. Right-click on a **Deploy Image** or **PXE Deploy Image** task template.
2. Select **Copy to 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.

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

To create a template sequence:

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

#### Basic template sequences

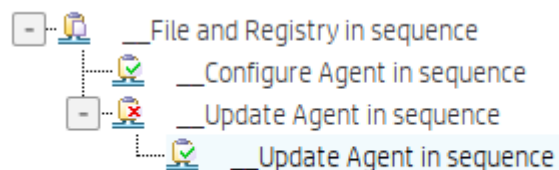
A basic template sequence uses the same condition between every task and can be defined by selecting the **Content** tab and then selecting **Basic**.

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

#### Advanced template sequences

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

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



This example shows four tasks to be executed as follows:

- Unconditionally execute the File and Registry task.
- If the previous task completed successfully, execute the first Configure Agent task and exit the sequence.
- If the initial task fails, execute the Update Agent task.
- If the Update Agent task completes successfully, execute the final Configure Agent task and exit the sequence.

Each level of templates in an advanced template sequence is called a dependency level. An advanced template sequence can have a maximum depth of 50 dependency levels. Each dependency level can have one of the following:

- One **anyway** condition
- or–
- One **success** condition and one **failure** condition

## 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 all task templates.
- **Private folders**—Private folder that can only be seen and operated by the current user. 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 select **Add Folder** from the pop-up menu

– or –

Right-click a folder and select **Add Private/Shared Folder** from the pop-up menu.

2. A template folder with a default name of “New Folder” is added. You can also enter the name you want.
3. You can save the folder by pressing the enter key 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:

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

---

### Renaming a folder

1. Right-click the folder and select **Rename** from the pop-up menu.
2. Enter the name, press enter or click on the blank to save.

---

#### NOTE:

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

---

### Adding template to a folder

- Right-click the task template and select **Copy to** or **Move to**, then click on the folder name you want to add to.
- Drag the task template to the target folder.
- Save the template in the folder, and the template will be added to the folder.

### Removing template from the folder

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

---

### NOTE:

A template can be removed in the folder except "All templates". 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 is 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 rule will be shown at the **Templates & Rules** page – **Rule** navigation view– **Rule detail** view, you can execute operations in this view contains **edit, delete, import, export, run a rule immediately** and **sort** (only **Startup** rules and **First Contact** rules can be sorted).
- All rule on a selected folder will be shown at the specified folder – **Properties – Rule panel**.
- All rule on a selected device will be shown at the specified device – **Properties – Rule panel**.

### Trigger Type

- **First Contact** - The rule executes for each device that matches its filter criteria once when the device first registers itself with HPDM Server, or after completing a Factory Reset task.
- **Startup** - The rule executes for each device that matches its filter criteria every time the device restarts.
- **Schedule** - Specify time and date for when the rule is executed and the frequency at which it is repeated.
  - Only once
  - Daily
  - Weekly

### Target Folder

Select a folder (Manual group folder or Dynamic group folder), all device under the selected folder will be target devices of this rule.

### Rule Compliance

Compliance means image version and software and other settings/configurations on device matching the expected value/state or not.

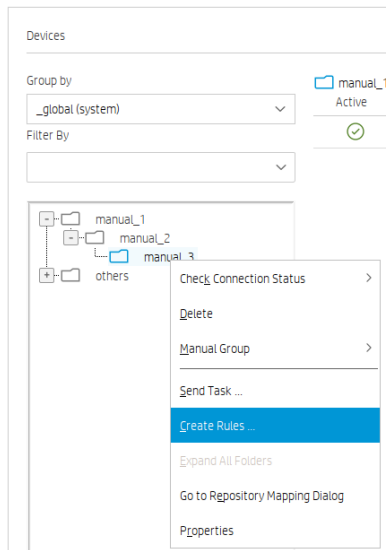
You can view the Compliance of rule at:

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

### Adding a New Rule

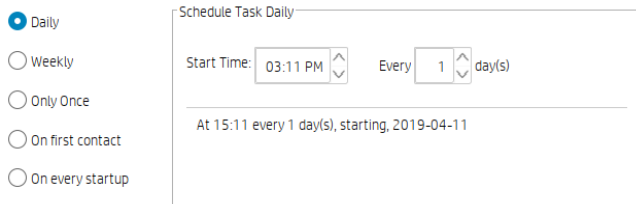
1. Entrance to create a rule:

- Right click on a folder (Manual group folder or Dynamic group folder) and click **Create Rule** menu item.



- Click **Add Rule** toolbar button.

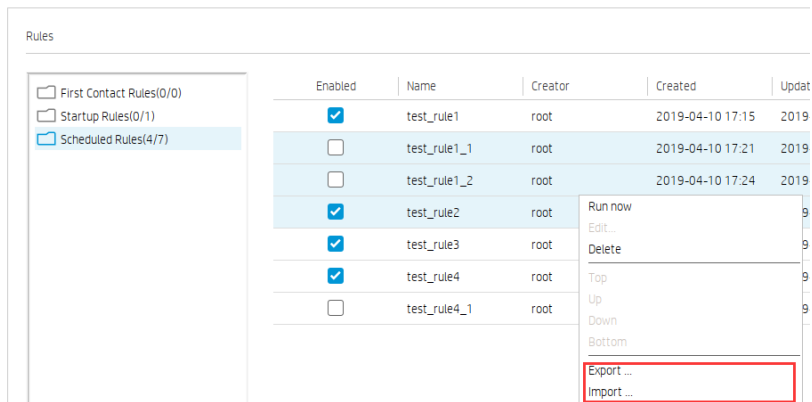
2. Pop up the **Rule Wizard Dialog**, enter a rule name and description at General page.
3. Specify **OS Type** and **Target devices** (All devices or devices in the specified folder).
4. Specify any device properties you would like to use to constrain this rule. For Startup rules, devices matching below criteria will show as “Noncompliant”. Please ensure the action will change device properties so that this rule will not fall into an endless loop.
5. Select a rule trigger. There are five options:



6. Specify the template to use.
7. Edit task parameter as you needed.
8. **Show devices** button can view all target devices
9. Click **Finish** to end the process and the rule will be run immediately if you checked **Run now** check box.
10. All rule will be shown at the **Templates & Rules** page – **Rule** navigation view– **Rule detail** view.

### Export and Import Rules

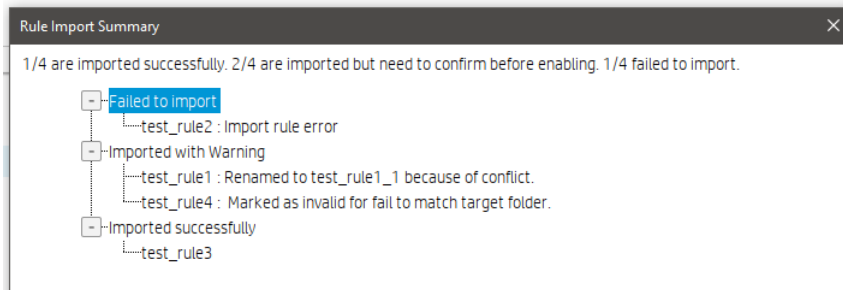
1. Entrance to export or import rule, at Templates & Rules page – Rule navigation view:
  - Right-click rule table and select **Export** or **Import**:



- **Import Rule** toolbar button:



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



4. Imported rules will be set disabled by default, you can enable it manually.
5. The rules who have not a matched folder will be marked as invalid, invalid rules cannot be triggered and enable, you can edit them and set a new target folder.

## Tasks & Reports

### Tasks

## Tasks Interface

HP Device Manager 3.0 Server: localhost Login: root

Management > **Tasks & Reports** > Gateways & Repositories > Administration

All

Device Tasks

Gateway Tasks

Reports

Number of tasks to view: 50

Task ID	Task Name	Progress and Stat...	Target Device Nu...	Create Time	Sender	OS Tab
00000003	._get Asset Informat	100%	2	2019-04-08 17:16...	test	WE57E
00000002	._get Asset Informat	100%	2	2019-04-08 15:01...	root	WE57E

Last activity:

● Waiting 
 ● Paused 
 ● Sending 
 ● Processing 
 ● Cached 
 ● Finished 
 ● Failed

HP Device Manager 3.0 Server: localhost Login: root

Management > **Tasks & Reports** > Users & Groups > Gateways & Repositories > Administration

All

Device Tasks

**Gateway Tasks**

Reports

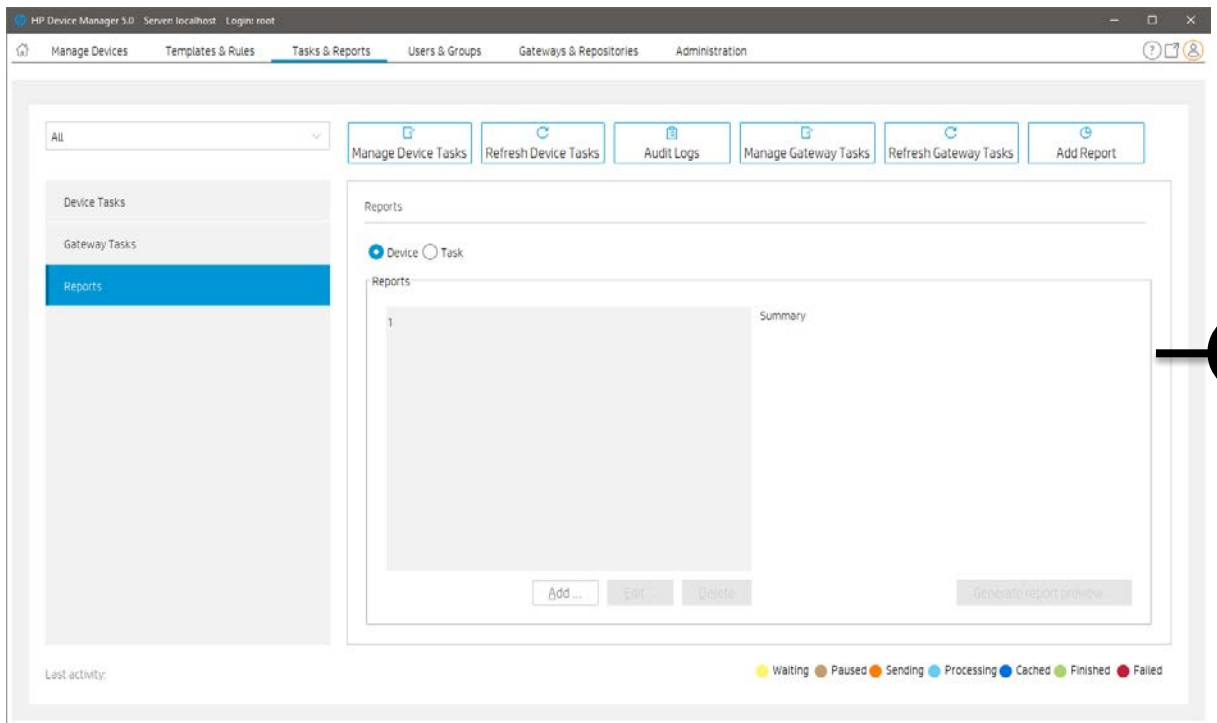
Number of tasks to view: 50

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

Last activity:

● Waiting 
 ● Paused 
 ● Sending 
 ● Processing 
 ● Cached 
 ● Finished 
 ● Failed





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 will filter the devices in the task here. “Number of tasks to view” sets the maximum number of tasks visible to the user.

3. Task status legend

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

-  Finished  
 The task was executed successfully by the device.
-  Sending  
 The task is being sending from HPDM Server through HPDM Gateway to the device and is waiting for a reply.
-  Failed  
 The task has failed or timed out.
-  Paused  
 The task has been paused.
-  Waiting  
 The task has been scheduled for sending at a later time, and has not been sent yet.
-  Cached

The task and its payload have been cached on the device and can be processed later.



Processing

The task has been accepted by the device and is being processed.

4. Gateway Tasks View—List all gateway tasks.
5. Report View—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 the tasks that have been sent are monitored and the results are displayed in the task pane. The task pane lists all the tasks that have been sent to devices.

The task list consists of the following columns:

- Task ID—Indicates the ID of the task.
- Task Name—Indicates the name of task template used to send this task.
- Progress and Status—Indicates the progress and status of the task.
- Target Device Number—Indicates the number of devices to which the task was assigned.
- Create Time—Indicates when the task was created.
- Sender—Indicates the sender of the task.
- OS Family—Indicates the OS 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** from the context menu to open the Template Chooser. Select a category, select a task template, and then select **Next**.

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

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

### Task status

There are following task status as following diagrams show.

Waiting Paused Sending Processing Cached Finished Failed

- Waiting: The task has been scheduled for sending at a later time, and has not been sent yet.
- Paused: The task has been paused.
- Sending: The task is being sending from HPDM Server through HPDM Gateway to the device and is waiting for a reply.
- Processing: The task has been accepted by the device and is being processed.
- Cached: The task and its payload has been 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 via the Configuration Management dialog. In HPDM Console, go to Administration, Configure System, and then expand the **Task Parameters** tree in the left-hand pane.

The Task Parameters tree consists of the following items:

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

Also, 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. Prior to the restart/shutdown, a dialog box is displayed to the user allowing them to postpone the restart/ shutdown or initiate it immediately. The user can postpone the restart/shutdown a maximum of three times.

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

---

### NOTE:

If the device needs to forcibly restart, the dialog box is not displayed.

---

### Viewing task properties

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

### Pausing a task

To pause a task:

1. Select a task in the task pane.

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

The status of the task is changed to Paused.

---

**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 and select **Continue** from the pop-up menu.

The status of the paused task changes to Waiting.

---

**NOTE:**

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

---

**Resending a task**

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

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

**Canceling a task**

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

---

**NOTE:**

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

---

**Deleting a task**

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

---

**WARNING!**

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

---

**NOTE:**

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

---

**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** from the context menu or double-click a task in the task pane. A Device Task View window appears.

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

---

**NOTE:**

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

---

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

**Viewing a Task's Success Ratio**

To display a task's success rate:

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

**Device shadowing**

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

**Result Template**

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

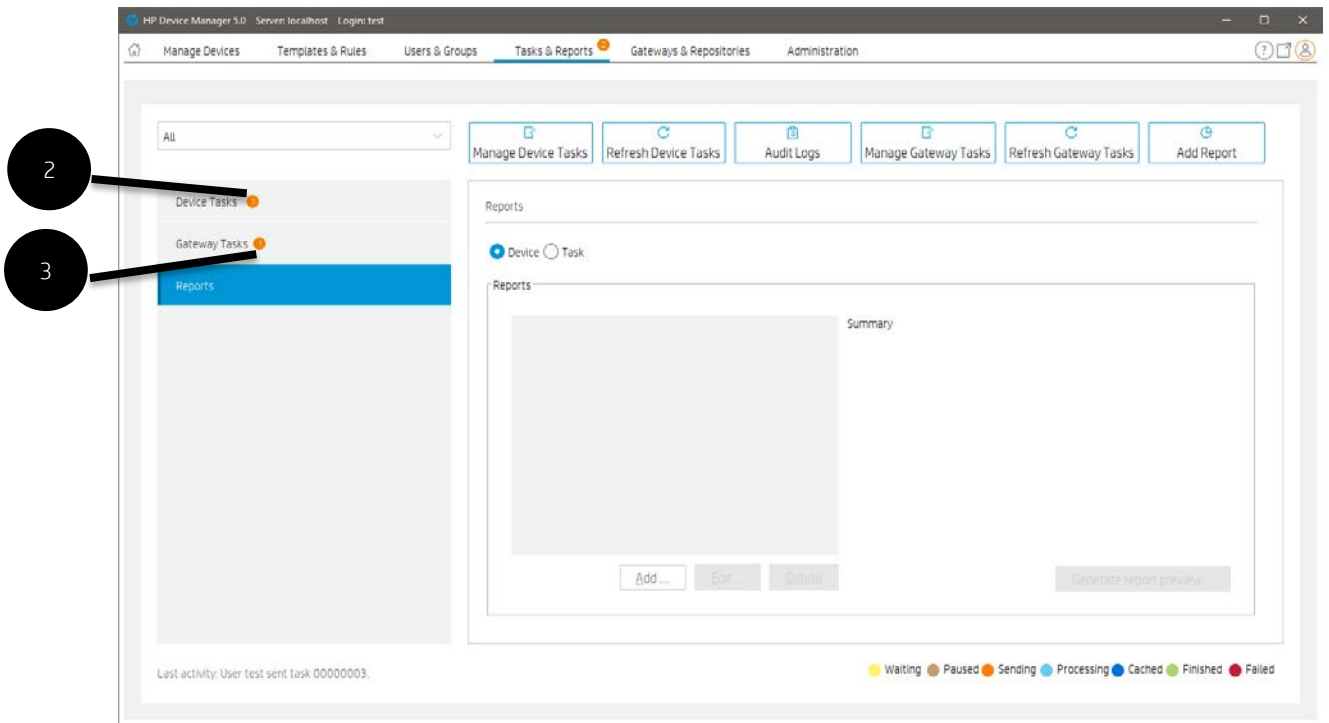
**Displaying tasks from all users**

If you have the **View Tasks From All Users** privilege, you could 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 will be displayed.





The notification of the "Tasks & Reports" page informs only the sum of the device task and the gateway task.

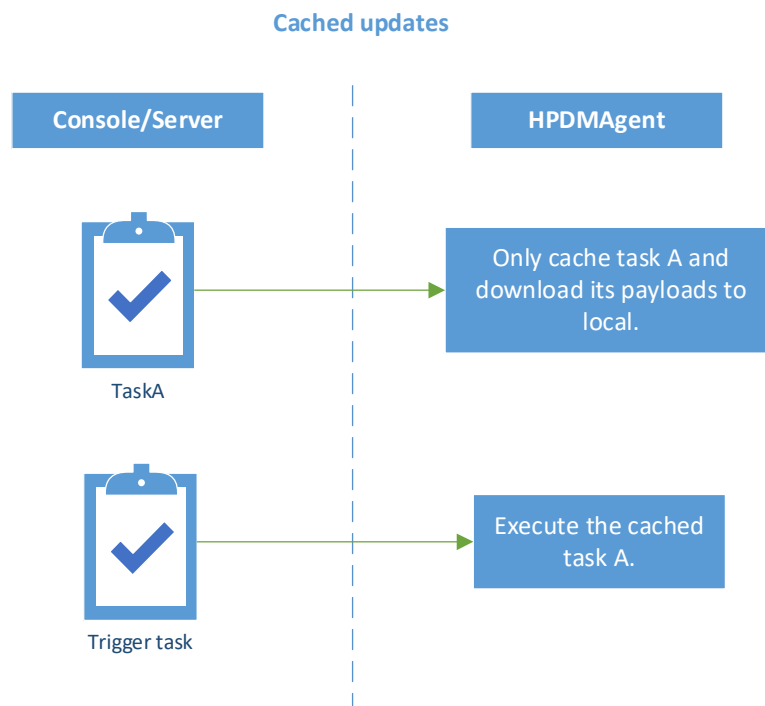
The notification is cleared when the item on navigation view is selected.

## Cached Tasks

Cached updates is a new solution introduced in HP Device Manager (HPDM) 4.7. In this solution, 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 how the cached updates feature works.



In cached updates, when the HPDM Agent receives a task, it caches the task content and downloads its payloads (if necessary) to a local cache. Then, the HPDM Agent notifies HPDM Server to update the task status to Cached. If you want the

HPDM Agent to execute this cached task, you need to send a trigger task to the target device. Then, the HPDM Agent executes the cached task and sends reports to the HPDM Server.

---

**Note**

Because of the limitations of the Enhanced Write Filter (EWF), the cached updates feature is unavailable on a device when the EWF is enabled. If you want to use cached updates on the device, disable the EWF. You can use a File-Based Write Filter.

---

**Usage scenarios**

Cached updates is a solution that enhances the flexibility of HPDM. It solves some problems that exist in many complex network environments. It is useful in the following scenarios:

- You are using a complex networks, such as VPN or 802.1x.
  - For most of the tasks, because of the limitations of write filters on Windows® Embedded operating systems, the HPDM Agent needs to reboot to disable the write filter to execute the tasks.
  - Before HPDM 4.7, the HPDM Agent needed network access to retrieve the task after a reboot. However, some networks, such as VPN or 802.1x, stop working after a reboot until you restart them.
  - 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 evening.
- You do not want to interrupt the current local user's operation when doing 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 click **OK**.

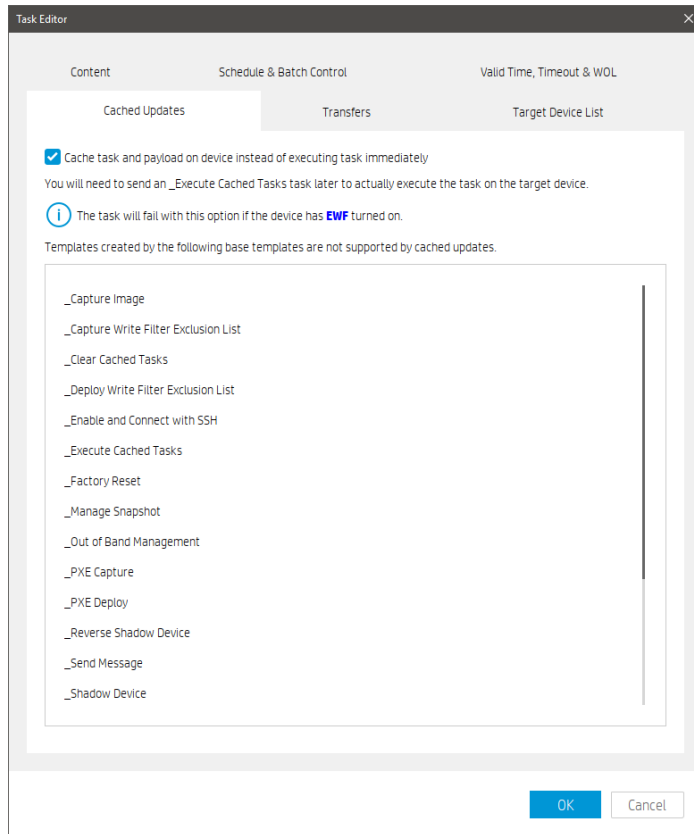
---

**Note:**

The default value of the Cache task and payload on device instead of executing task immediately option is false. To change this, see Configuring the task parameter of a cached update on the HPDM Console.

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

---



3. When the status of the task becomes 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 send to the device after this task is cached locally. This means that 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 has been cached on the device, send an **\_Execute Cached Tasks** task to the device to execute this cached task.

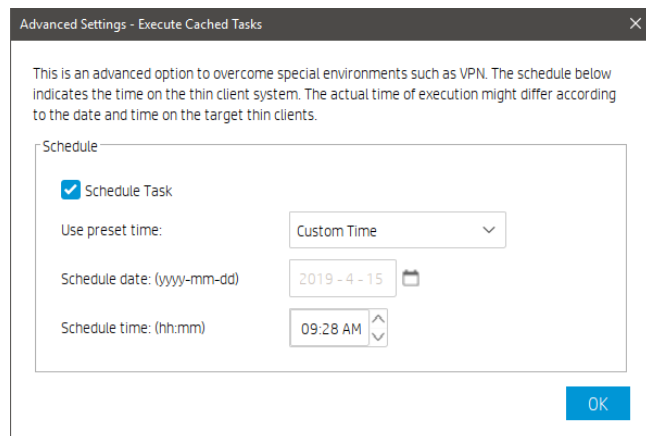
*Executing tasks cached on a device*

To execute the cached tasks, you must 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. Click **Advanced**.
  - B. In the **Advanced Settings** dialog that appears, select **Schedule Task**, select a preset time or a schedule date and time, and then click **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
<b>Schedule control</b>	HPDM Agent	HPDM Server
<b>Time basis</b>	Device local time	HPDM Server local time
<b>Blocking follow-up tasks</b>	Yes	No
<b>Requires network connection when schedule hits</b>	No	Yes

4. 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.
5. 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. Click **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:**

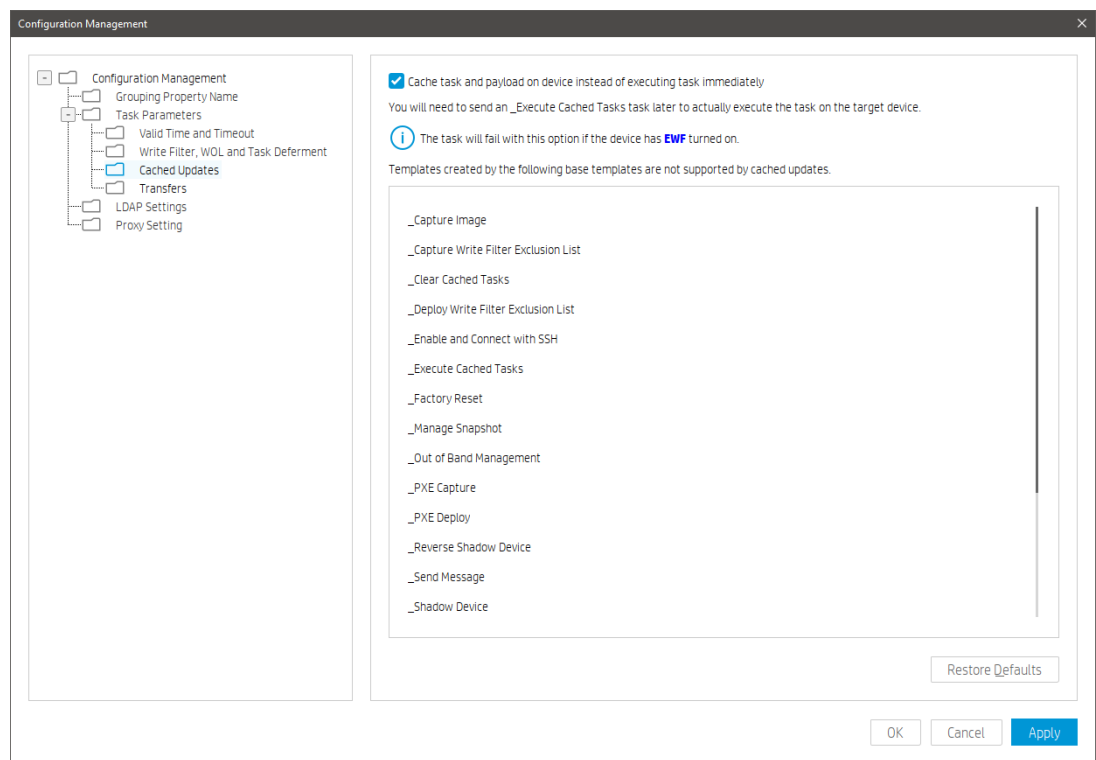
HPDM does not support removing a single cached task when multiple tasks are cached on a device.

**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. Click **OK** or **Apply** to save the value.

*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 or not, these templates are never sent cached updates mode.

To view which base template included in the blacklist:

1. In the HPDM Console, select **Tools > Configuration > Configuration Management**
2. Select **Task Parameters > Cached Updates**.

### Disabling the lock screen option

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

To disable this option:

1. Open the HPDM Server configuration file serverconf.xml.
2. Locate the following line:

```
<Attribute Name="hpdn.lockscreen.showtime" Value="10" Enabled="yes" SN="0"></Attribute>
```

3. Change the value of **Enabled** to **no**.

```
<Attribute Name="hpdn.lockscreen.showtime" Value="10" Enabled="no" SN="0"></Attribute>
```

4. Restart the HPDM Server.

### Cached Update Limitations

- Because of the limitations of the EWF, cached update is not supported when the EWF is enabled.
- 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.

## Task template Reference

### 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 sub-tasks:

#### Capture Files

This sub-template allows you to capture files from devices.

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

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

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

Example Description

a\* Specifies all files that start with the letter "a" and are followed by any number of characters.

a? Specifies all files that start with the letter "a" and are followed by only one other character.

\*a Specifies all files that end with the letter "a" and are preceded by any number of characters.

?a Specifies all files that end with the letter "a" and are preceded by only one other character.

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

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

It supports 5 parameters (macros) to allow you put captured files from different devices to different folders. You can click the button after "Files\Captured\" to set them into the Target Path. You also can input them manually. They are:

- a) %ID% - Device ID
- b) %SN% - Device Serial Number
- c) %HOSTNAME% - Device Hostname
- d) %DATE% - Device Local Date
- e) %TIME% - Device Local Time

You can set multiple macros at a time. The Sample string can tell you the format of the folders.

For example: If you want to capture a file daily, you can set %ID%\_%DATE%.

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

### Deploy Files

The sub-template allows you to deploy files to devices.

To deploy files to devices:

1. Double-click the **\_File and Registry** template to open the Template Editor.
2. Select **Add**, select the **Deploy Files** subtask, and then select **OK**.
3. Select the **Add from local** button to choose files from the local machine.
  - a) 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 are finished 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. Click **Generate** to generate HPDM Package and the template.
9. Drag and drop the template onto the desired devices.
10. Select **OK** to apply the task to the devices.

### Delete Files

The sub-template allows you to delete files in devices.

To delete files from devices:

1. Double-click the **\_File and Registry** template to open the Template Editor.
2. Select **Add**, select the **Delete Files** subtask, and then select **OK**.
3. Add files or folders to delete. Each line has the following options:
  - **File or Folder Name**—Enter the file or folder name to delete. The wildcards \* and ? are also supported.
  - **Path On Device**—Enter the path on the device where the file or folder is located.
  - **Delete Recursively**—Set this option to Yes if you want to delete all files or folders that match the pattern entered in File or Folder Name in all subdirectories under the Path On Device. If set to No, subdirectories will not be affected.

4. Select **OK** when you are finished specifying files.
5. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.
6. Drag and drop the template onto the desired devices.
7. Select **OK** to apply the task to the devices.

## Script

The sub-template allows you to run a script in devices.

To run a script on a device:

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

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

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

In HPDM 5.0, we added an extra option for Script: **Wait for the script to finish executing**. It is enabled by default. When it is enabled, Agent waits for the exit of process, captures outputs and the exit code, and then reports execution result to HPDM Server. When it is disabled, Agent only executes the script and reports successful to HPDM Server immediately.

This option is for the cases that the script will reboot devices. If the script reboots devices, Agents have no chance to report the executing result, so Agents will retrieve the task again and again. If you assume the script will reboot device, please uncheck 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 sub-template 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, double-click that template, and then double-click the **Registry** subtask.

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

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

- Use the **Registry Tree** to navigate the registry node and add, rename, or delete registry keys and values.
- Use the **Registry Settings** pane to add or delete values from the selected registry key.
- Use the **Action to Perform** pane to add or delete a registry key. If you have modified the key's values individually in the Registry Settings pane, the options in this pane are greyed out.
- Select **Import Registry File** to import registry settings.

3. Select **OK** when you are finished editing registry settings.
4. Select **Save as**, enter a name for the new template, and then select **OK**. The template is added to the Task Templates list.
5. Drag and drop the template onto the desired devices.

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

#### **Program record:**

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

#### **Command (deprecated)**

The sub-template allows you to execute commands. It is deprecated. HPDM 5.0 still has it for backward compatibility. We recommend you to use the **Script** subtask.

#### **Pause**

You can pause a **\_File and Registry** task to wait for certain events such as the previous Script sub-task 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 devices' registry.

To get registry settings from a device:

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

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

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

## 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

1. Set Current Gateway: Agent will get the current Gateway value and try to connect it when Agent starts.

#### Backup Gateway

1. Set Backup Gateway: when the current Gateway value is empty, Agent will get backup Gateway value and try to connect.

#### Pull Interval

1. Set Pull Interval: defines the frequency at which HPDM Agent sends a startup reports to HPDM Gateway to get tasks.

#### Delay Scope

1. Set Delay Scope: After it is started, HPDM Agent sends a startup report at a randomly chosen time between 0 and the chosen Delay Scope.

#### Log Level

1. Set Log Level: you can select the log level in the comboBox.

After configuring the Agent options, click **OK**.

### *\_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/shutdown, a dialog box is displayed to the user allowing them to postpone the restart/ shutdown or initiate it immediately. The user can postpone the restart/shutdown a maximum of three times.

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

1. Move **\_Configure Task Deferment** template to the device to open the Task Editor.
2. In the Content panel, configuring some options in the Task deferment parameters dialog. And you can customize the Title and Message in the Prompt Information Dialog.
3. In the Task deferment parameters dialog.

Maximum chances to postpone: defines the maximum chances to postpone. You can define value in 0-65535 in this line edit.

Maximum postponement time: defines the maximum times to postpone. You can define value in 0-65535 in this line edit.

Default postponement time: defines the default postponement time in minutes. You can define value in 0-65535 in this line edit.

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, click **OK**.

Note: If the device needs to forcibly restart, the dialog box is not displayed.

#### *\_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 Edit.
2. Click **OK**.

## **Connections**

### **Imaging**

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

### **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 <b>Current Profile</b> option is unique to the HP ThinPro operating system.
_Get Asset Information	This template extracts a full asset report from the targeted devices.
_Reboot Device	This template restarts the targeted devices. A warning message displays on the devices' screen for 15 seconds before the restart actually takes place.
_Reverse Shadow Device	This template causes HPDM Agent on a target device to connect to the VNC viewer bundled with HPDM Console by SSL tunnel. This template is not available for the HPCE thin clients.
_Send Message	This template sends a customized message to targeted devices. This template is not available for HP ThinPro thin clients.
_Execute Cached Tasks	This template executes all cached tasks on the target devices.
_Clear Cached Tasks	This template removes all cached tasks on the target devices. The status of each cached task changes to "failed."
_Shadow Device	This template causes the VNC viewer bundled with HPDM Console to connect to the VNC service on a targeted device via an SSL tunnel.
_Shutdown Device	This template shuts down the targeted devices. A warning message displays on the devices' screen for 15 seconds before the restart actually takes place.



_Start Resource Monitor	This template starts the Resource Monitor for the target device. This template can only be sent to a single device at a time and is not available for HP ThinPro thin clients.  When this template is sent to a device successfully, a Resource Monitor dialog pops up. You can monitor Process, Performance, and Network Disk information.
_Wake Up Device	This template causes the HPDM Gateway associated with the targeted devices to send them a Wake On LAN message. The Wake device works not only for devices in the same subnet with HPDM Gateway, but also for devices that are not in the same subnet of HPDM Gateway, if the subnet has at least one online HPDM Agent. We can wake up devices behind NAT, if the subnet has at least one online HPDM Agent. During timeout, HPDM Gateway reports the unfinished part as failure.

## Settings

Template	Description
_Apply Settings	This template enables you to create a set of custom settings and deploy them to one or more devices.
_Auto Logon Configuration	This template allows to configure automatic logon settings on devices.
_Capture EasyShell Settings	This template allows to capture EasyShell settings from a device.
_Capture Profile	This template captures a profile from a device running HP ThinPro 5.
_Capture Snapshot List	This template captures a snapshot list from a device running HP ThinPro 5.
_Capture Write Filter Exclusion List	This template captures the FBWF/UWF exclusion list from a device running a Windows operating system with FBWF or UWF.
_Clone Settings	This template enables you to copy a selection of custom settings from one device and deploy them to other devices.
_Deploy License	This template allows to deploy licenses to devices.
_Deploy Profile	This template is used to configure a profile and deploy it to devices running HP Smart Zero Core or HP ThinPro 5.
_Deploy Write Filter Exclusion List	This template deploys the write filter exclusion list to devices running a Windows operating system with FBWF or UWF.
_Enroll Certificate With SCEP	This template enables you to enroll certificates with SCEP on normal thin clients.
_Hostname and IP	This template enables you to change the hostname and IP address of one or more devices. There are two options: <ul style="list-style-type: none"> <li>• <b>Modify specified devices</b>—Only functions when you drag it to one or more target devices.</li> <li>• <b>Set with pattern</b>—Changes hostname and IP with the same pattern.</li> </ul>
_Manage Dynamic Properties	This template allows to add or remove dynamic properties to collect from devices.
_Manage Snapshot	This template manages snapshots on devices running HP ThinPro 5.
_Set CA Certificates	This template allows to clear or deploy CA certificates to devices.

_Set Domain	This template allows devices to join a domain or a workgroup.
_Set OS Configuration	This template switches the target device's operating system configuration on devices running HP ThinPro 5. <b>NOTE:</b> This template does not set the default connection if switching to Smart Zero. You can use a connection template to implement that change.
_Set Password	This template enables you to set a password for one or more users on one or more devices. You can select the <b>Hide password</b> check box to hide the password, or clear the check box it to show the password. <b>NOTE:</b> This template is not available for thin clients running HP Smart Zero Core.
_Take TPM Ownership	This template enables/activates TPM and sets the TPM owner password and BIOS setup password to take the TPM ownership of the selected devices.
_Write Filter Settings	This template enables you to change the Write Filter settings for a device.

### Template Sequence

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

## 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 flavors 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, you need to make sure that the repository has been configured. See the "Repository management" chapter of the *Administrator Guide* for HP Device Manager for more information.

### Imaging support matrix

For information on 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	File-based	.ibr
Windows Embedded 8 Standard	File-based	.ibr
Windows Embedded Standard 7	File-based	.ibr
HP ThinPro 7	Disk-based	.dd.gz
HP ThinPro 6	Disk-based	.dd.gz

HP ThinPro 5	Disk-based	.dd.gz

*Capturing an image using the non-cached mode*

---

**Note**

If you want to capture images from Windows-based thin clients using the non-cached mode, a Shared Folder is required.

Capturing images using the non-cached mode cannot be done when using a wireless connection.

When capturing an image from a Windows 10 IoT Enterprise-based, Windows Embedded Standard 7-, or Windows Embedded 8 Standard-based device, there must be at least 300 MB of free disk space on the thin client.

---

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 wish to capture. The Task Editor dialog appears.

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, enter 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:

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. Click **OK** to apply the task to the device immediately.

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 click Device Tasks in the navigator, you can find 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.

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 Windows XP Embedded or Windows Embedded CE 6.0 operating system.

When capturing an image from a Windows-based device, the free disk space must be at least 70% of the total file system size. When capturing an image from an HP ThinPro device, the free disk space must be at least 50% of the total disk size and the available RAM needs to be at least 1 GB. When capturing an image from an HP Smart Zero Core device, the free disk space must be at least 50% of the total disk size and the available RAM needs to be at least 512 MB.

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 wish to capture. The Task Editor dialog appears.

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, enter a name in the **Image Name** field, and then enter a description for the captured image in the **Description** field.



Cached Updates

Transfers

Target Device List

Content

Schedule &amp; Batch Control

Valid Time, Timeout &amp; 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: 

OK

Cancel

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**. If the thin client uses an advanced network, such as wireless or 802.1x, this option is necessary.

**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:

OK Cancel

4. In the **Save result as template** field, enter a name for the resulting template.

Task Editor
X

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

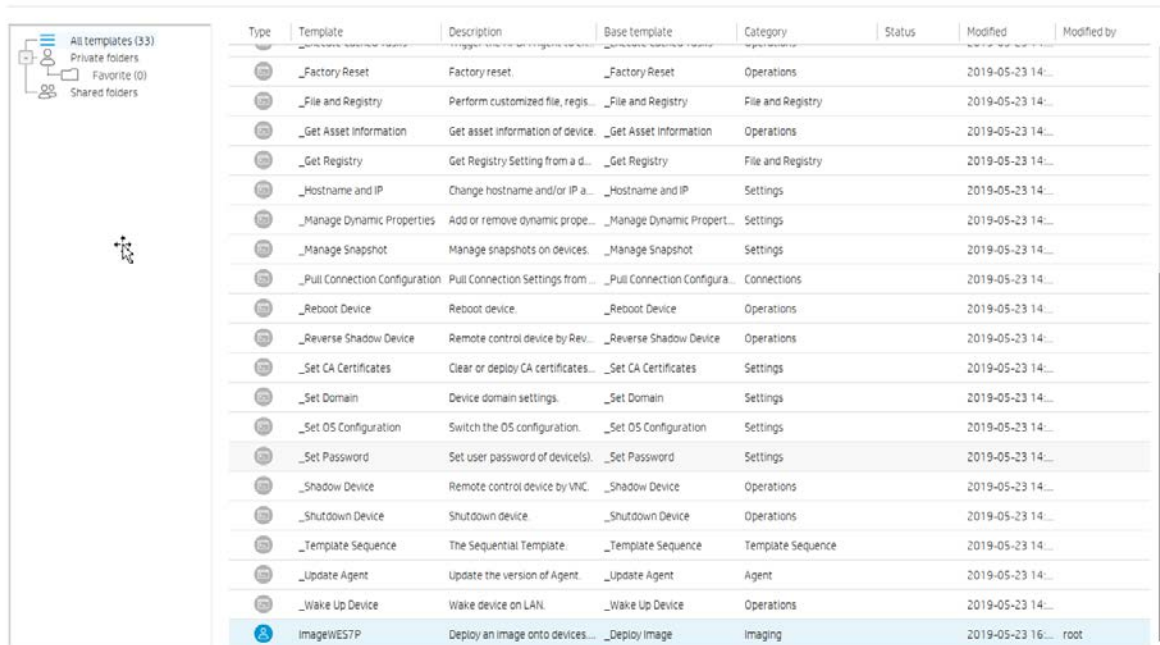
Note: It is necessary for environments where advanced networks are used, such as wireless, 802.1x, etc. It requires enough free space on the thin client to cache the captured image.

Save result as template:

OK
Cancel

5. Click **OK** to apply the task to the device immediately.

After you send the task, you can find there is a notification on the **Tasks & Reports** page of HPDM Console. Go to the **Tasks & Reports** page and click **Device Tasks** in the navigator, you can find 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.



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 prope...	_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:...	
	ImageWES7P	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.

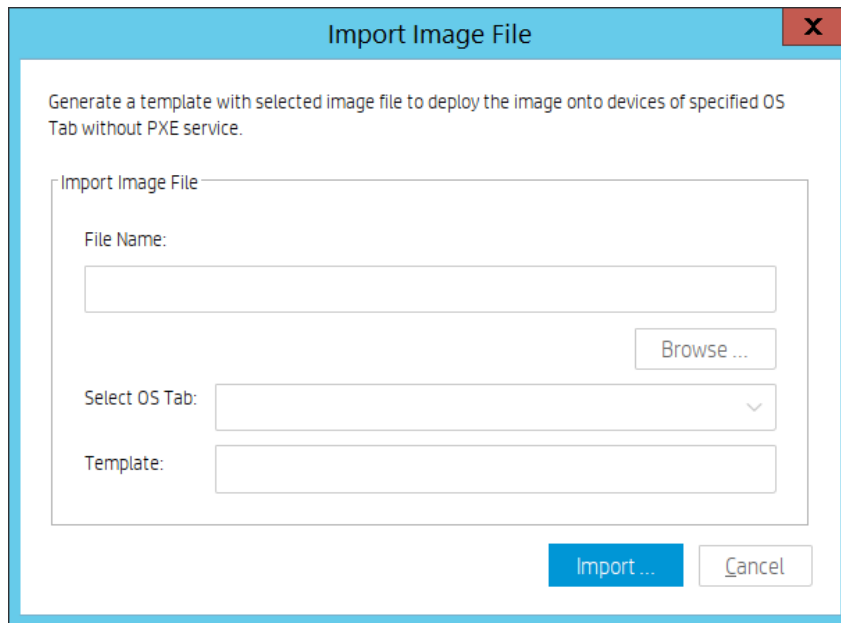
#### *Importing an image file for deployment without PXE*

1. Go to the **Templates and Rules** page of HPDM Console, right click in the **Templates** pane. Select **Import** -> **Imaging Files** -> **to deploy without PXE** from the popup menu.

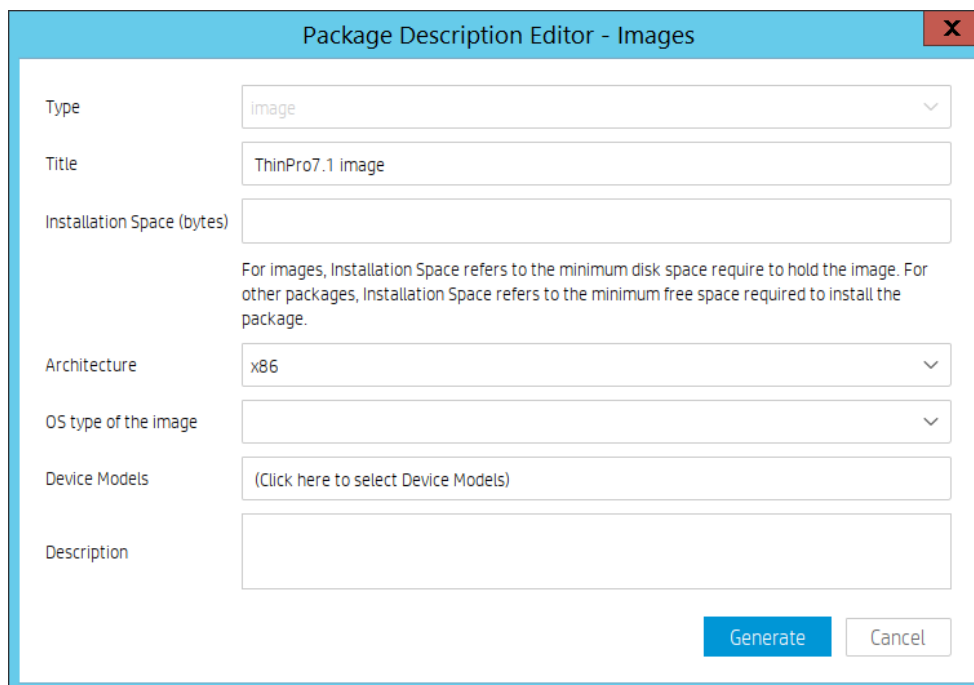
#### **Note**

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** > **to deploy using PXE**. The other steps are the same.

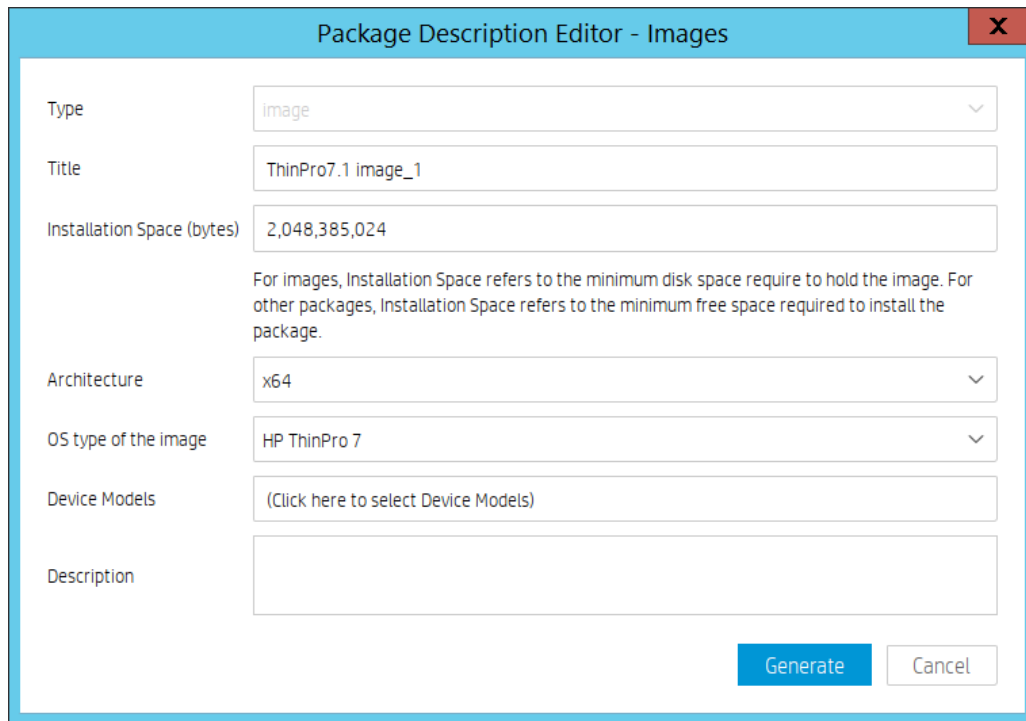
2. In the **Import Image File** dialog box, click **Browse** to select the image file that you want to import.



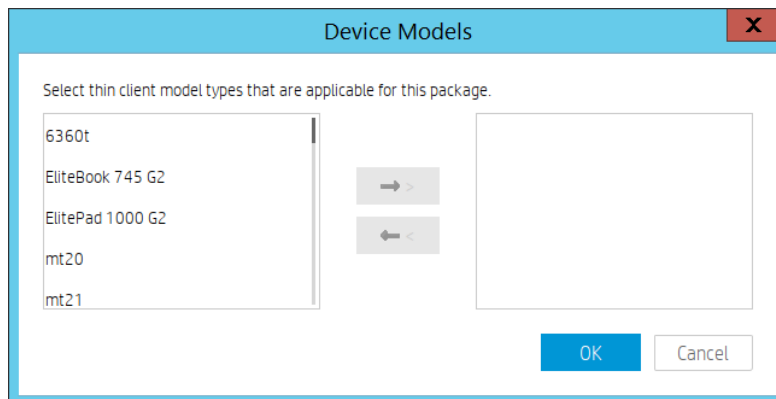
3. After selecting the desired image file, click **Import**.
4. In the Package Description Editor, enter the necessary information about this image file.
  - A. Enter a title for this package in the **Title** field.



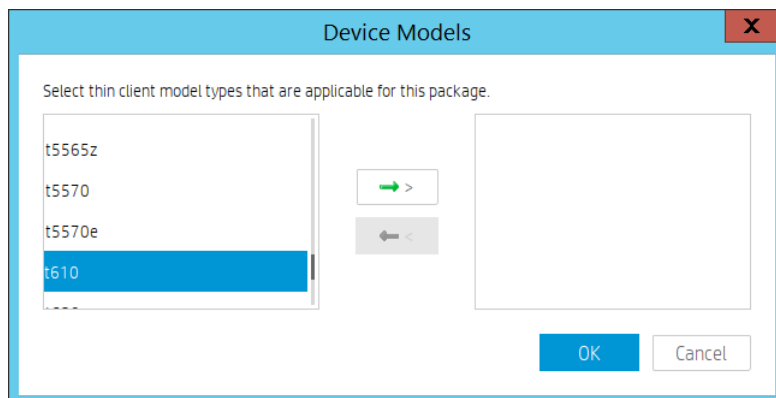
- B. Enter the **Installation Space** in bytes. This is the minimum disk size required to install this image. Usually HPDM can retrieve the space requirement for image files and input it correctly.
- C. Select the **Architecture**.  
For example: ThinPro 7.1 should be x64.
- D. Select the **OS type of the image**. This is the image file's operating system. You can select the operating system from the supported OS list.



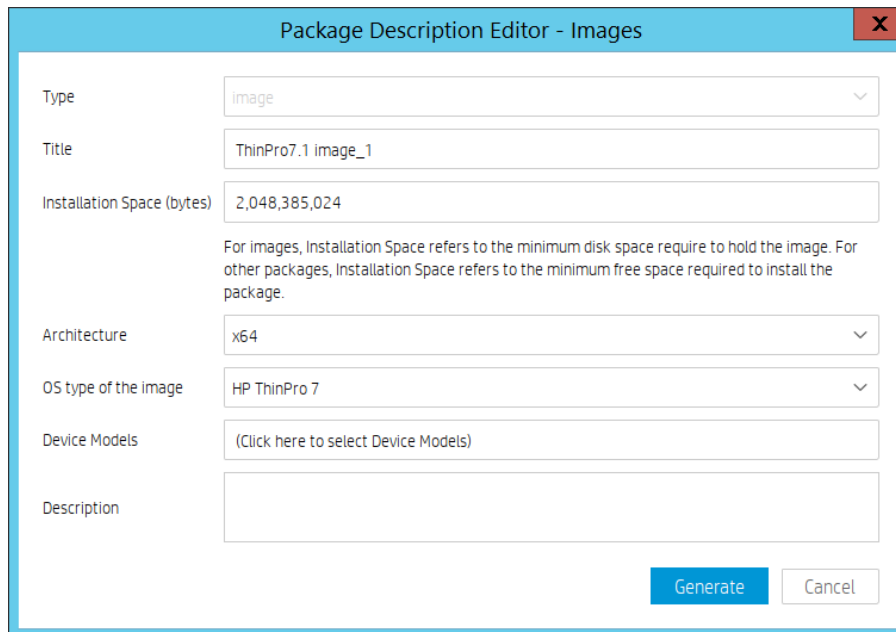
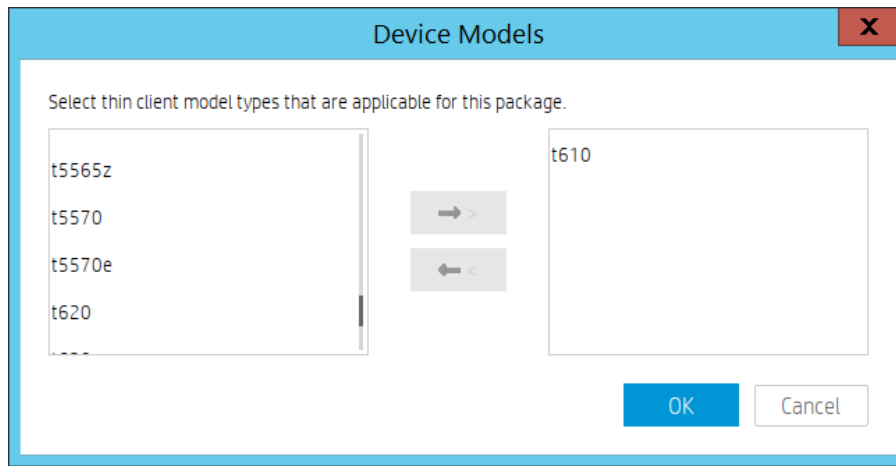
- E. Select the **Thin Client Models** that the image supports. You can select the thin client models using the following steps.
  - i. Click the **Thin Client Models** field, and the Thin Client Models dialog appears.



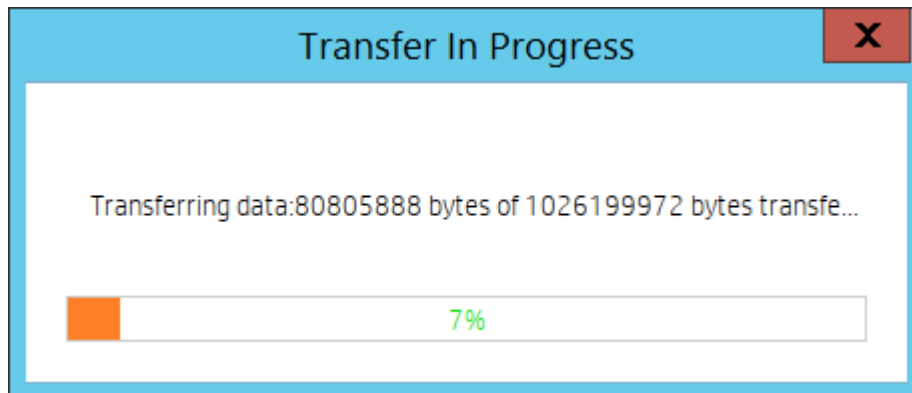
- ii. Select the desired thin client model from the left pane, such as t610 and click -> button.



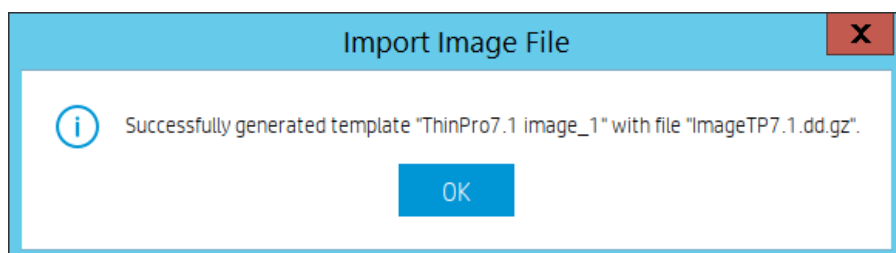
- iii. Click **OK** to return to the Package Description Editor.



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








6. After the upload is complete, a confirmation message appears. Click **OK** to finish this operation.





If the image file imported successfully, a new Deploy Image template appears 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: non-cached 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 of this Guide.

The following table shows which formats are supported when deploying images to thin clients.

<b>Operating system</b>	<b>Image format (non-cached mode)</b>	<b>Image format (cached updates mode)</b>
Windows 10 IoT Enterprise	.ibr	.ibr
Windows Embedded 8 Standard	.ibr	.ibr
Windows Embedded Standard 7	.ibr	.ibr
HP ThinPro 7	.dd.gz	.dd.gz
HP ThinPro 6	.dd.gz	.dd.gz
HP ThinPro 5	.dd.gz	.dd.gz

#### **Deploying an image using the non-cached mode**

Note the following requirements for deploying an image using the non-cached mode:

- A shared folder is required to deploy an .ibr image to a Windows-based thin client
- Deployment cannot be done via a wireless connection.
- When deploying an .ibr image to a Windows 10 IoT Enterprise, Windows Embedded Standard 7-, or Windows Embedded 8 Standard-based 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 to which you want to deploy the image. The Task Editor dialog box appears and 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, if you captured an image from an HP t510 and want to deploy it to an HP t610, 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.

---

5. **Retain HP ThinPro Configuration** is a special option for ThinPro imaging only. When you select it, Agent will restore the ThinPro profile after image deployment. **Note:** Maybe some options are not restored perfectly due to profile compatibility.

6. Click **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 the cached updates mode:

- When deploying an image to a Windows-based device, the free disk space must be greater than the image file size.

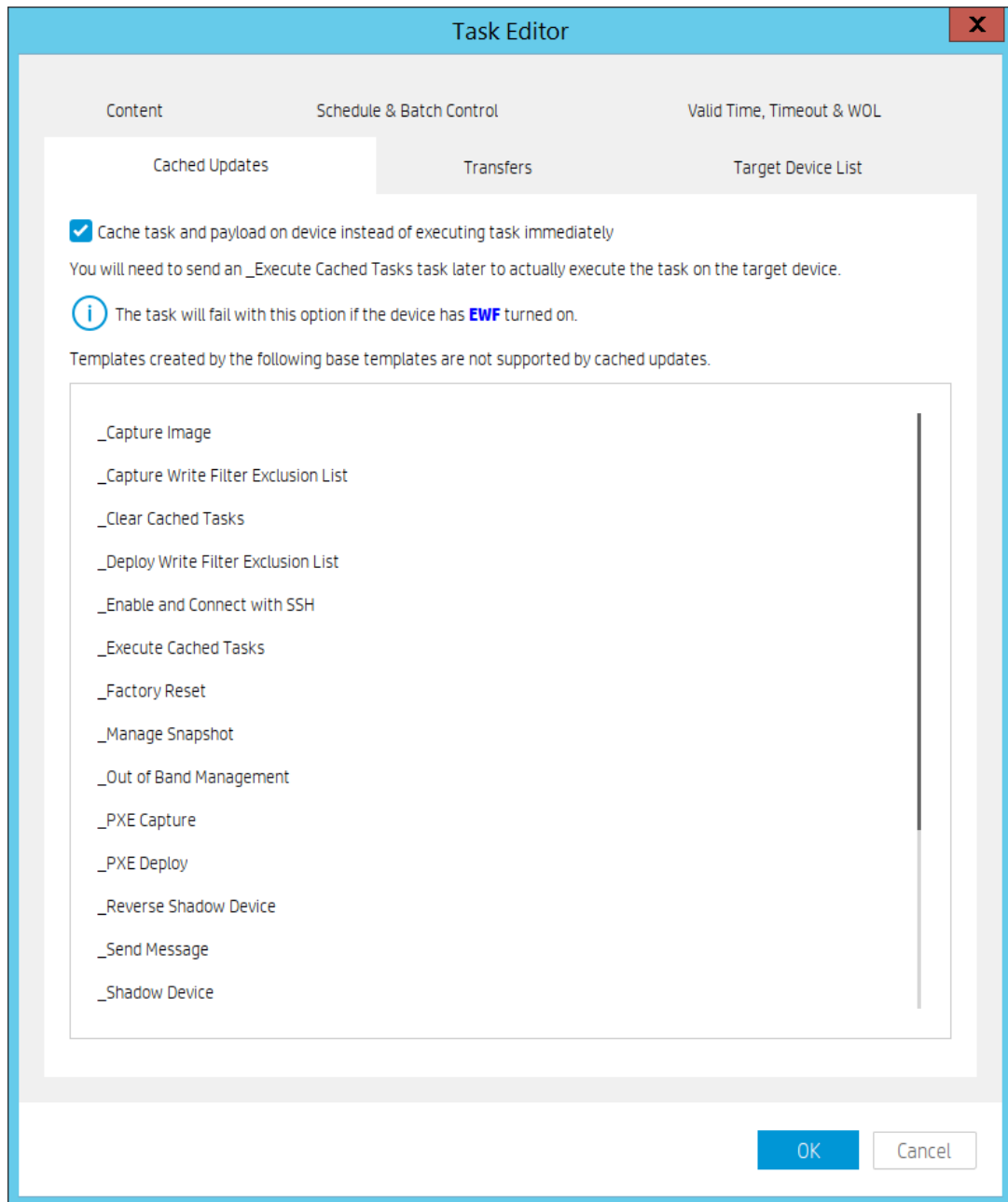
- When deploying an image to an HP ThinPro device, the free disk space must be greater than the image file size and the total RAM must be greater than the image file size + the imaging OS.

**Note:** The ThinPro5 imaging OS needs about 100MB, but the ThinPro6 and ThinPro7 image OS needs at least 1.1GB. So 2GB probably is not enough for ThinPro6 or ThinPro7 cached image deployment. 4GB is the recommended memory size for ThinPro6 or ThinPro7 cached image deployment.

- To deploy an image to a device that uses a wireless network, ensure 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 to which you want to deploy the image. The **Task Editor** dialog box appears and displays detailed information about the image.
4. On the Cached Updates tab, select **Cache task and payload on device instead of executing task immediately**. 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, this option is necessary.



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 t510 and want to deploy it to an HP t610, 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. Click **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**

A PXE Deploy template can be generated by importing an image from the Template and Rule page and then right click in the Templates pane to select Import > Image Files > to deploy using PXE from the popup menu.

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. Click **OK** to apply the PXE Image task to the devices.

---

**Note**

Currently HPDM PXE Imaging only support legacy PXE boot. If UEFI boot is enabled, the PXE imaging cannot be successful.

HPDM Agent will try to change the boot order before PXE imaging, but the result is not guaranteed. Please 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 will be captured.
- Target device—The device to which the captured image will be deployed.

*Settings preserved when capturing an image*

Windows 10 IoT Enterprise / Windows Embedded 8 Standard:

All settings from the source device are preserved on both the source device and the captured image, except the hostname, network settings, domain settings, and Write Filter status.

Windows Embedded Standard 7:

For devices running the Windows Embedded Standard 7, Windows Embedded Standard 7E, or Windows Embedded Standard 7P operating system, all settings from the source device are preserved on both the source device and the captured image, except the hostname, network settings, domain settings, and Write Filter status.

HP ThinPro:

All settings from the source device are preserved on both the source device and the captured image, except the hostname and network settings.

*Settings preserved when deploying an image*

When deploying an image, the following settings on the target device will be preserved and restored after the image deployment.

Windows 10 IoT Enterprise / Windows Embedded 8 Standard / Windows Embedded Standard 7:

- Writer 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 for ThinPro imaging only. When you select it, Agent will restore the ThinPro profile after image deployment.

**Note:** Maybe some options are not restored 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 1. Windows Embedded Standard 7 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)
Windows Embedded Standard 7E	Wireless	Cached	t510	16	59	73	N/A
			t610	16	45	58	N/A
	Wired	Cached	t510	4+16	42	53	58
			t610	16	38	48	48
			t620	16+32	26	25	
			t820	16	16	20	
			t5740e	16	31	42	
			t510	16	30	46	52
		Non-cached	t610	16	30	35	
			t620	64	24	17	
			t820	16	15	22	
			t5570e	4	35	40	45
t5740e	4	43	37	47			
Windows Embedded Standard 7P	Wireless	Cached	t610	16	56	77	
	Wired	Cached	t610	16	45	65	
		Non-cached	t610	16	41	50	
Mobile	Wireless	Cached	mt40	16	49	50	N/A
	Wired	Cached	mt40	16	22	23	
			mt41	16	18	29	
		Non-cached	6360t	4	28	24	27
	Non-cached	mt41	16	17	20		
		mt40	16	27	20		

Table 2: 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 3. 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

- HPDM does not support deploying a Windows 10 IoT Enterprise or Windows Embedded 8 Standard image file to a Windows Embedded Standard 7-based thin client.
- 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.

- For Windows Embedded Standard 7E and Windows Embedded Standard 7P, 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 a Windows Embedded Standard 7P image downloaded from HP.com.

Workaround:

1. Deploy this image to a device using a local image tool, such as HP ThinState or Ghost by Symantec.
2. Capture the image from this device via HPDM.
3. Deploy the newly captured image to other devices.

- 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 ThinState or Ghost by Symantec.

– or –

Configure the device to use a wired network, and then deploy the image to this device via HPDM.

- A. Configure the wireless network settings after deploying the image.
  - B. Capture the image from this device via HPDM.
  - C. Deploy the newly captured image to other devices that use a wireless network.
- The t240 device does not support legacy PXE boot, so it does not support PXE imaging.

## 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. Either option can be used to generate a report, or you can define a report without any criteria to include all devices and tasks.

---

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

---

#### NOTE:

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

---

5. Optionally, select **Summary** to see a summary of the report. Then, select **Next**.
6. Select **Finish**. A prompt asks if you would like to preview the report.

### Editing a report

To edit an existing report:

1. Navigate to **Reports**.
2. From the **Report List**, select a report and then select **Edit**.
3. To edit the report's filter, use the options under **Set Filter**. To edit the report's columns, use the options under **Choose Columns**. To see a summary, select **Summary**.
4. After editing, select **Finish**. A prompt asks if you would like to preview the report.

### Deleting a report

To delete a report:

1. 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**.

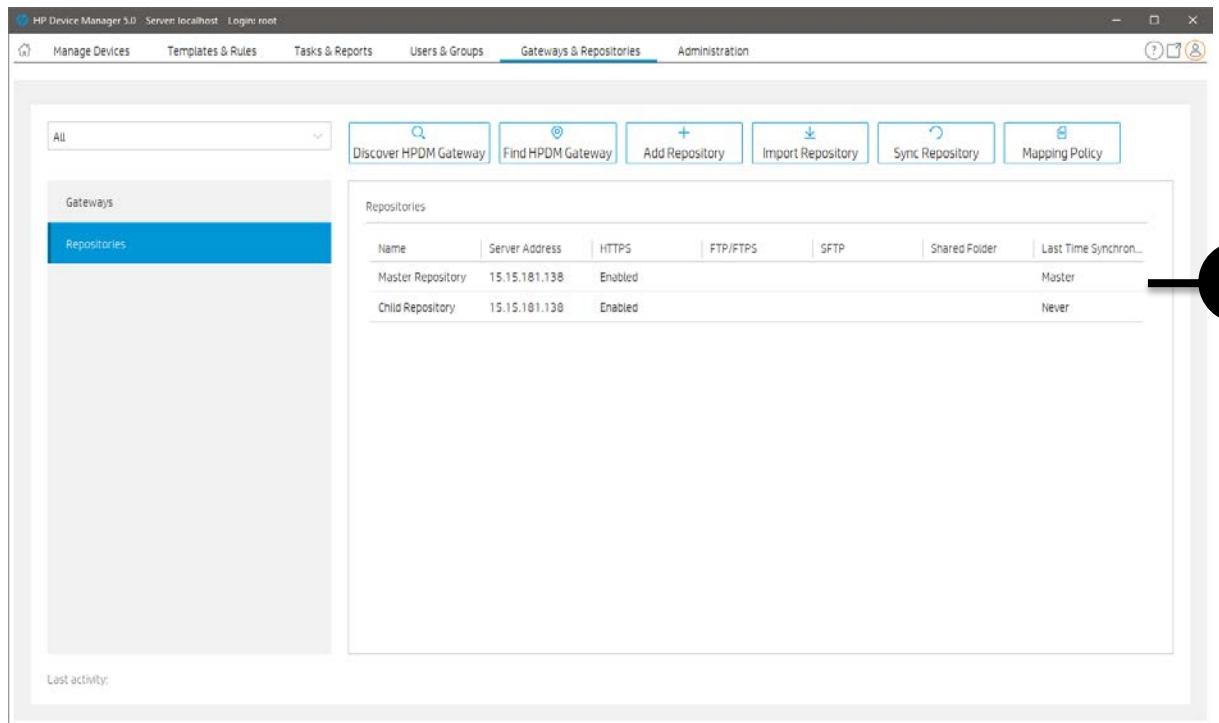
## Gateways & Repositories

### Page Layout

The screenshot shows the HP Device Manager 5.0 interface. The top navigation bar includes 'Manage Devices', 'Templates & Rules', 'Tasks & Reports', 'Gateways & Repositories', 'Users & Groups', and 'Administration'. The left sidebar has 'Gateways' selected. The main content area features a toolbar with the following buttons: 'Discover HPDM Gateway', 'Find HPDM Gateway', 'Add a Repository', 'Import Repositories', 'Sync Repository', 'Mapping Policy', and 'Repository Content'. Below the toolbar is a table titled 'Gateways' with the following data:

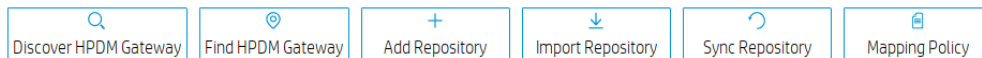
Active Status	Hostname	HPDM Gateway ID	IP Address	HPDM Gateway Version	Last Update	Subnet Mask	Subnet Address
off	host-00001	00:00:01:00:00:00	127.0.0.1	3.0	May 15, 2019	NA	NA

At the bottom left, there is a status message: 'Last activity: User test sent task 00000006'.



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

A new mechanism called “Automated Repository Management” has been implemented to improve the efficiency of HPDM and ensure 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

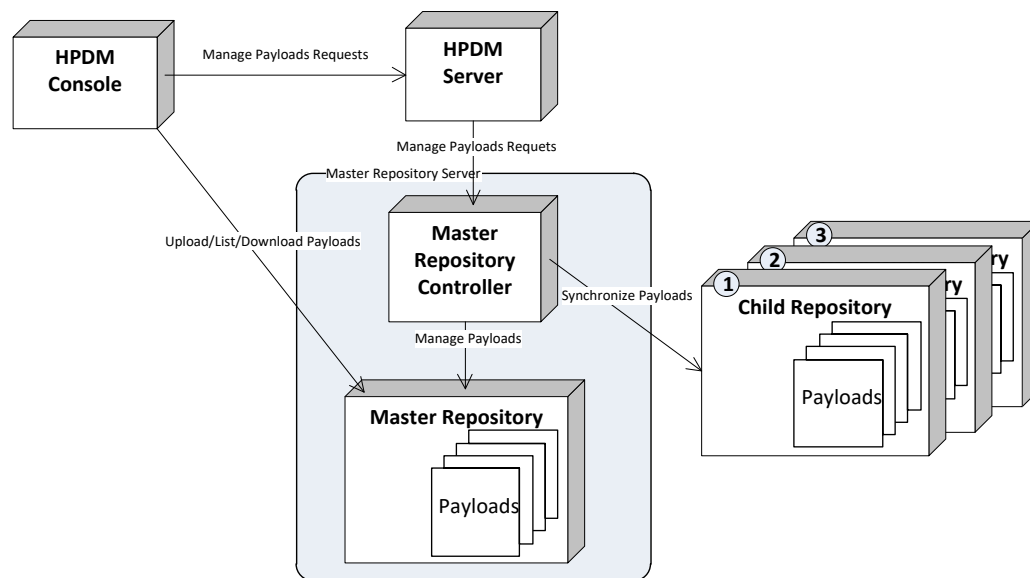
- \_Apply Easy Tools Configurations
- \_Apply Easy Tools Settings
- Imaging
- \_Capture Image
- \_Deploy Image
- \_PXE Capture
- \_PXE Deploy

### 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 1. 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. There are two limitations as follows:

- FTP family protocols must be chosen for Linux non-cached imaging.
- SMB must be chosen for WES 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. Click the Repositories in the Navigator pane.
  - C. Double click 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. Each selected protocol have their own page, you can change settings in them.
  - iv. In the last Summary page, please click the “Test Repository” button. The test report will be outputted in the Test Result pane.
  - v. If test is successful, you can click Finish to save the changes and close the dialog. Otherwise, please modify the settings and test again.
- E. Finished.

### **Configuring the Master Repository**

When you install HPDM Master Repository with the HPDM 5.0 intaller, HPDM Master Repository Controller and HPDM Embedded HTTPS Server are necessarily required.

#### *HPDM Master Repository Controller*

The HPDM Master Repository Controller installer installs the Master Repository to %ProgramData%\HP\HP Device Manager\HPDM.

If you want to move the Master Repository path, please install HPDM Configuration Center to move it. After you move the Master Repository path, please do not forget to modify the root path of the file servers to point the new Master Repository Path.

For more details, please refer to the HPDM Configuration Center section.

#### *HPDM Embedded HTTPS Server*

Currently HPDM 5.0 only support HPDM Embedded HTTPS Server as the https server. When installing it, it will generate a random user and a random password.

Its 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 machine with the HPDM 5.0 installer, the full installer will send the HTTPS Server to HPDM Server intelligently. It means the Repository setting is configured automatically.

If you want to change the random user and the random password, please intall HPDM Configuration Center to change them. After you change the user or the password, please do not forget to modify the Repository setting from HPDM Console.

For more details, please refer to the HPDM Embedded HTTPS Server Deployment section.

#### *Add other protocols*

### **Configuring FTP**

1. If you have not installed an FTP server, please install one.
2. Point the root path to the Master Repository folder.
3. Follow “How to modify Repository settings in HPDM Console” to add the FTP setting. Please notice the URL setting of FTP/FTPS.

For example: 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 URL after ftp://<ip address> with empty.

If you set %ProgramData%\HP\HP Device Manager as the FTP root path, you should 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 “**Modifying Repository settings withinin HPDM Console**” to add the Shared Folder setting.

## Configuring SFTP

1. Install a proper SFTP server and configure it well.
2. Follow “**Modifying Repository settings within HPDM Console**” to add the SFTP setting.

## Child Repository configuration

There is almost no difference between configuring a Child Repository and the Master Repository, except that 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, click **Add Repository** button.
3. In the **Repository Configuration Wizard**, enter a repository name and the server address.
4. Select the protocols to use.
5. Configure the **user name**, **password**, and **path** for each protocol.
6. Select **Test** to test the connections you've configured and display results on-screen.
7. Select **Finish**.

## Deleting an HPDM Child Repository

1. In HPDM Console, 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, select a repository and right-click it and select **Export**.
3. Browse to the location where you want to save the repositories.
4. Select the **Export** button. All repositories are exported to an XML file.

## Importing repositories

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the **Repositories** view, click Import **Repository** button.
3. Browse to the location where the repositories you want to import are located.
4. Select the **Import** button.

## 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. Click **Mapping Policy**.

### *Batch mapping*

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

- Auto Map—HPDM Server assigns a repository to each HPDM Gateway or subnet address.
- Use Master—Uses the HPDM Master Repository.
- Use Specified—Allows you to choose a repository from a list for the specified HPDM Gateway or subnet address.

---

### **NOTE:**

You can view all mapping results by clearing the Show exceptions only option. HPDM automatically maps any new devices in the network.

---

### *Per device mapping*

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

## **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 the **Enable schedule synchronization** option.
4. Configure the schedule settings.
5. Select **Save**.

## **Content management**

To view the contents of the HPDM Master Repository:

1. In HPDM Console, go to **Gateways & Repositories**, then navigate to **Repositories**.
2. In the Repositories, right-click a repository and select **Content**.

#### *Viewing detailed payload information*

To view detailed payload information:

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

#### *Deleting contents from the HPDM Master Repository*

To delete contents from the HPDM Master Repository:

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

NOTE: Bultin-in content provide by HP cannot be deleted.

#### *Downloading contents from the Files Captured category*

To download contents from the HPDM Master Repository:

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

## **Customized Packages**

#### *HPDM package*

An HPDM package contains two required parts: payload files and a description file. For example, there could be a package called Test, in which there are the following folder and file, and the folder contains the payload files.

- Folder: Test
- File: Test-D653B4C263C399E924FF5F70AE5BD9EF.desc

The description file is named by combining the payload name and the MD5 hash value for the payload, separated by a “-” character. 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 UI input or other sources such as imported HP FTP components.

#### Capture Image task

1. Send a Capture Image task to a device. For details about the Capture Image task, see the Imaging Devices/Capturing an image section of this Admin Guide.
2. *After the Capture Image task finishes, 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. Find the **\_File and Registry** template in the Templates pane, and then double click it.
3. Click **Add ...** in the Template Editor dilaog.
4. Choose **Deploy Files** in the Sub-Task Chooser and click **OK**.
5. Click **Add from local** button to add a file or a folder. Modify **Path On Device** to set the path will be deployed on devices. Click **OK** to close the Deploy Files dialog.
6. Click **Save as ...**, and then enter a name for the new template. Click **OK**.
7. Enter the payload information in the **Package Description Editor** dialog.
8. Click **Generate**. The file is added as a new template. Payload files are uploaded to the Master Repository automatically

### 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 -> to deploy without PXE** or **to deploy using PXE**.
3. Select the image file that you want to import.
4. Click **Import**. Then, enter the payload information in the **Package Description Editor** dialog.
5. Click **Generate**. The imaging file is added as a new template. Payload files are uploaded to the Master Repository automatically.

For more details about Imaging, please refer to the Imaging section of this guide.

### 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 the [HP Update Center](#) section of this guide.

## Users and Groups

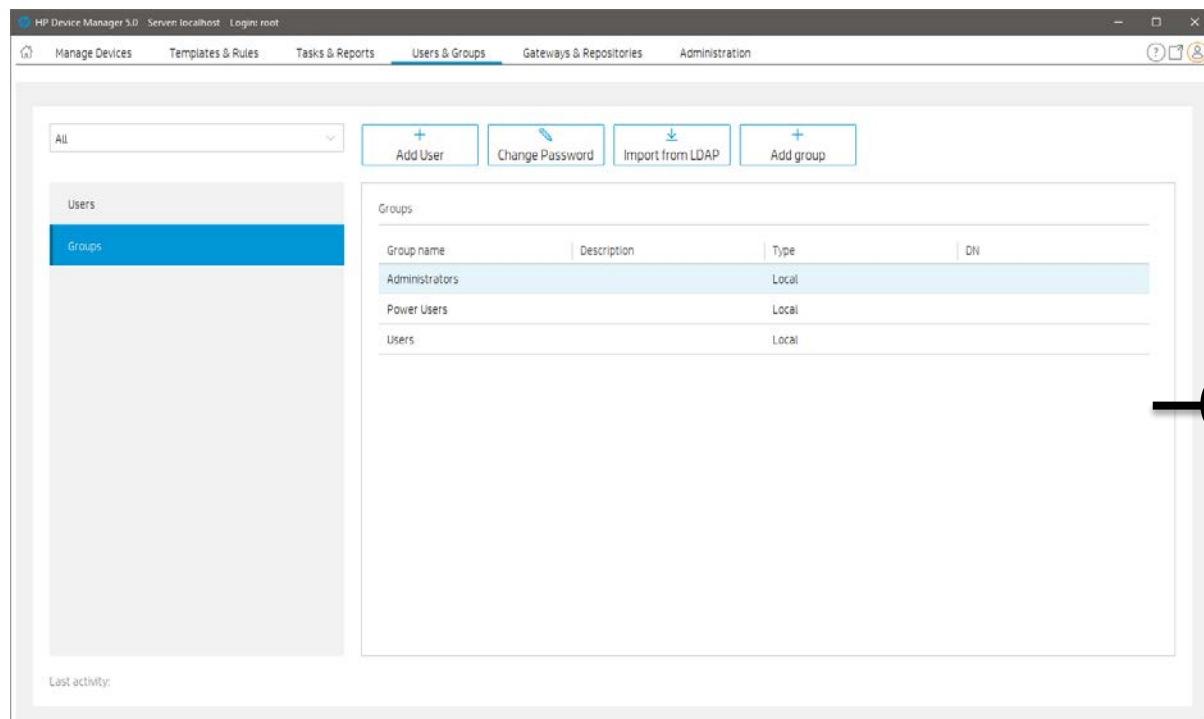
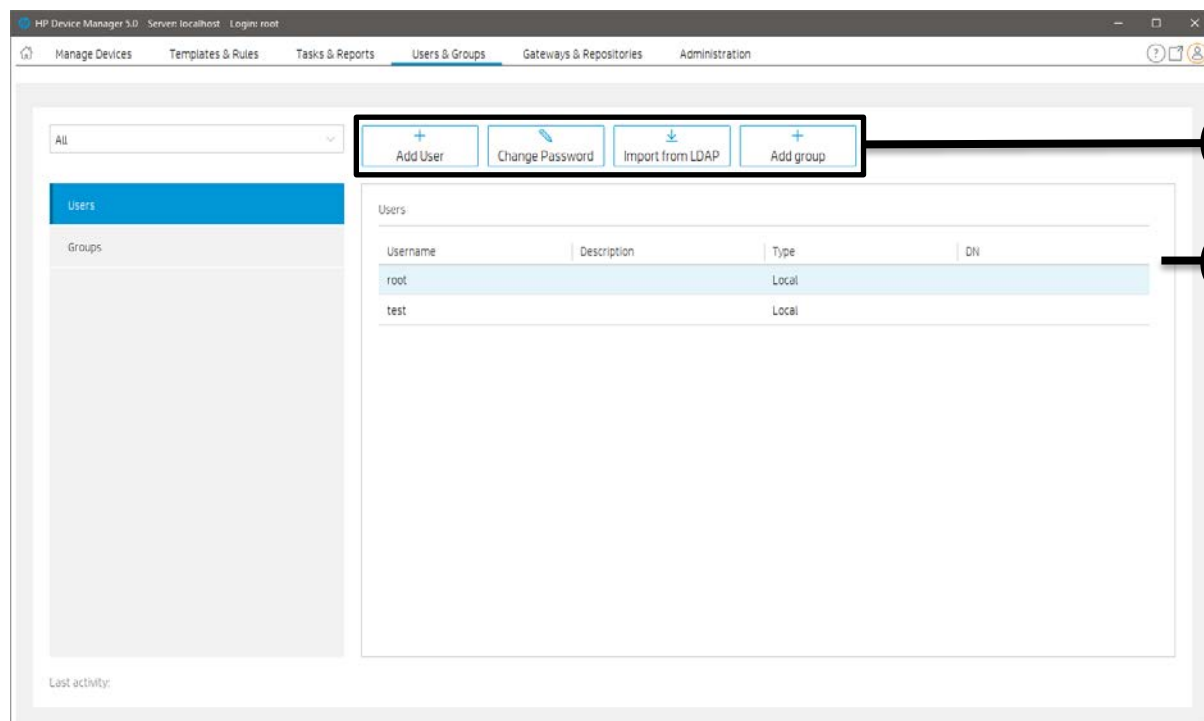
In the section we will explore Users and Groups within HP Device Manager. The controls herein allow you to dictate fine-grained responsibilities within your organization.

In HPDM Console, select **Users & Groups** page, can see all users and groups.

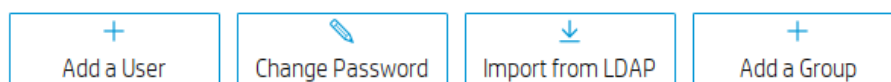
Each user account can have customized privileges, according to their level of need. Privileges are assigned based on the groups a user is added to.



## Page Layout



1. Toolbar— An enumeration of the Users and Groups most commonly 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 Toolbar to add a new user. The Create New User dialog box appears.
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. This username can be used to log in to HPDM Console the next time it starts.

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

NOTE: This user will be added to the **Power Users** group by default.

NOTE: Multiple instances of HPDM Console cannot log on to HPDM Server with the same username 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. Double-click 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** from the pop-up menu.
3. Enter the **New Password** for the user, and then re-enter it in the **Confirm Password** field.
5. Select **OK** to finish.

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

NOTE: **Change Password** in Toolbar can only change your user password.

### Viewing privileges and template access

1. Double-click a user from the list in the **Users** table.
2. Select **View general privileges** tab, you can see **Action based privilege**.
3. Select **View template privileges** tab, you can see **Object based privilege**.

NOTE: **Action based privilege**, or role-based privilege, has been available in previous HPDM versions. It assigns privileges to a group, and then users within the group inherit those privileges.

NOTE: **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** to add a new group. This group can now be assigned a set of privileges, and then users can be assigned 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** in the pop-up menu.
3. Select the **Privileges** tab.
4. Select the privileges you wish to assign to the group.
5. Select **OK** to finish.

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

### **Assigning users to groups**

1. Right-click on a group from the list in the **Groups** table.
2. Select **Properties** in the pop-up menu.
3. Select the **Users** tab.
4. Use the **Add** and **Delete** buttons to modify the members of this group.
5. Select **OK** to finish.

### **Assigning security filters to groups**

1. Double-click 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. The **User & Group** page - **Groups** navigation view.
2. Select a group and open group properties.
3. Click the **Policy** category.
4. Enable the checkbox and enter a number in the text area.
5. Click the **OK** button

### **Viewing privileges and template access**

1. In the HPDM Console, click **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, you can see **System-level privileges**.
4. In privileges tree, check **Template Access Management**.
5. Click **Templates & Rules** page, click **Template Privilege** in Toolbar, you can view template access privileges.

### Deleting groups

1. select a group from the list in the **Groups** table.
2. Select the **Delete Group** button, and then select **Yes** to confirm.

## 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. Click **Add** to create a new LDAP setting.
3. Enter the name of the LDAP setting, and click **OK**.
4. In the **Host** field, type the LDAP server hostname or IP address. If an encrypted connection is used, the LDAP server must be specified by the hostname.
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 double-click the search user. The Display Name is shown on the General panel of the Properties window and is the LDAP CN.

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

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

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

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

To open the Import Tool:

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 many results. If so, a blue **Show 20 more** entry will be present. Select **Show 20 more** to show more results.

To search for a user or group:

1. Select the **Search** tab in the upper left of the **Import Users and Groups** dialog box.
2. The **Base DN** is the starting point from which the search runs. All searches are done recursively from this origin.
3. The **Query** allows the specification of what to search for. It contains 3 parts: the Attribute, the Search Value, and the Comparison between the two.
  - a. The **Attribute**, on the left side of the query, offers several common attributes to search on. If the desired search attribute is not present, type the attribute into this field.
  - b. The **Search Value**, on the right side of the query, is what is being searched for. An asterisk, \*, can be used as part of the Search Value. This permits searching when the full **Search Value** is unknown. Example: Searching Attribute UID with an Equals comparison for Value \*.smith@testnet.com will match all users with a UID that end with .smith@testnet.com.
  - c. The **Comparison**, in the middle of the query, offers several ways to compare the value of the attribute to what you are searching for.
    - The **Equals** comparison, =, finds LDAP objects that are equivalent to the search value.
    - The **Greater than or Equals** comparison, >=, finds LDAP objects with an attribute value that is numerically larger than the search value.

- The **Less than or Equals** comparison, <=, similarly finds LDAP objects with an attribute value that is numerically smaller than the search value.
  - The **Similar to** comparison, ~=, permits searching for attribute values that are similar to the search value.
  - Finally, the **Not Equals** comparison, !=, permits searching for attribute values that are not equivalent to the search value.
4. Finally, press the **Search** button. Results appear in the **Search** tree to the left.

To add a user or group to the import list:

1. Locate the user or group, either by **Browse** or **Search**.
2. Add the user or group using one of the following methods:

Double-click the user or group.

– or –

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

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

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

To remove a user or group from the import list:

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

To examine a user or group:

1. Select a user or group.
2. Select the **Show Attributes** button.
3. If desired, this object can be added to the import list by selecting the **Add** button.

### **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

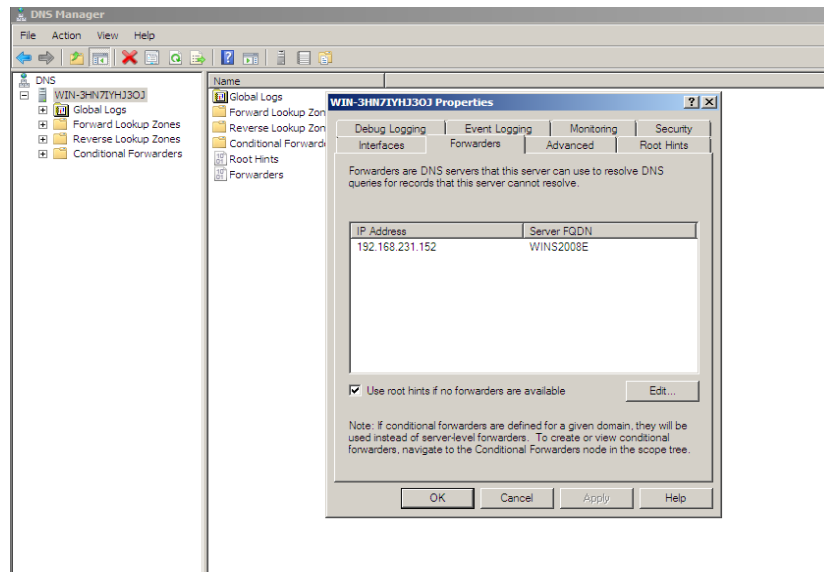
## DNS Server

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.

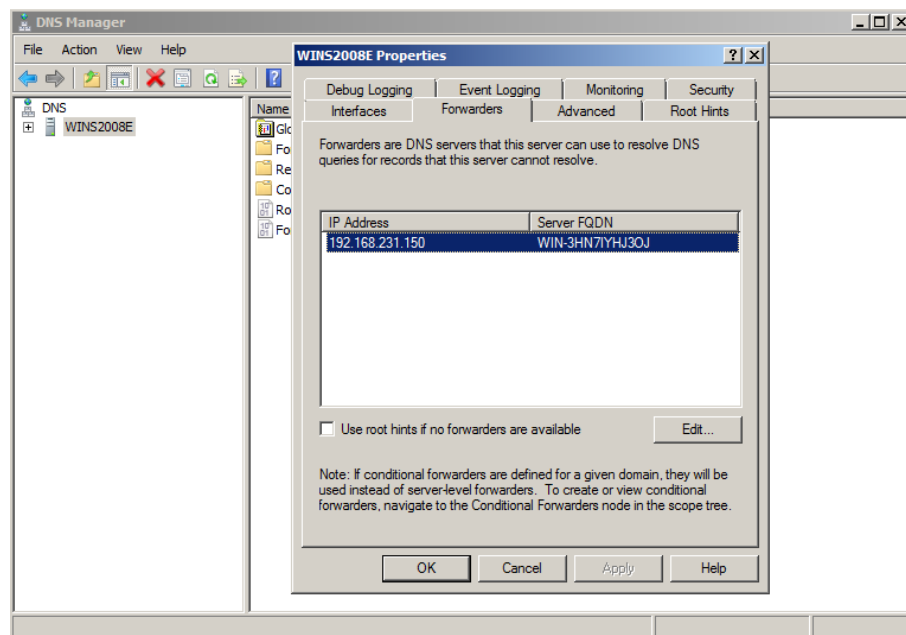
1. If the parent domain and child domain use the same DNS Server, the DNS of the HPDM Server needs to point to this DNS Server.
2. If the parent domain and child domain use different DNS Servers, be sure the **Forwarders** of both the parent domain and child domain DNS Server point to each other. Then, 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.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping hpdn.com
Pinging hpdn.com [192.168.231.150] with 32 bytes of data:
Reply from 192.168.231.150: bytes=32 time<1ms TTL=128
Reply from 192.168.231.150: bytes=32 time<1ms TTL=128
Reply from 192.168.231.150: bytes=32 time<1ms TTL=128
Reply from 192.168.231.150: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.231.150:
    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>_

```

```

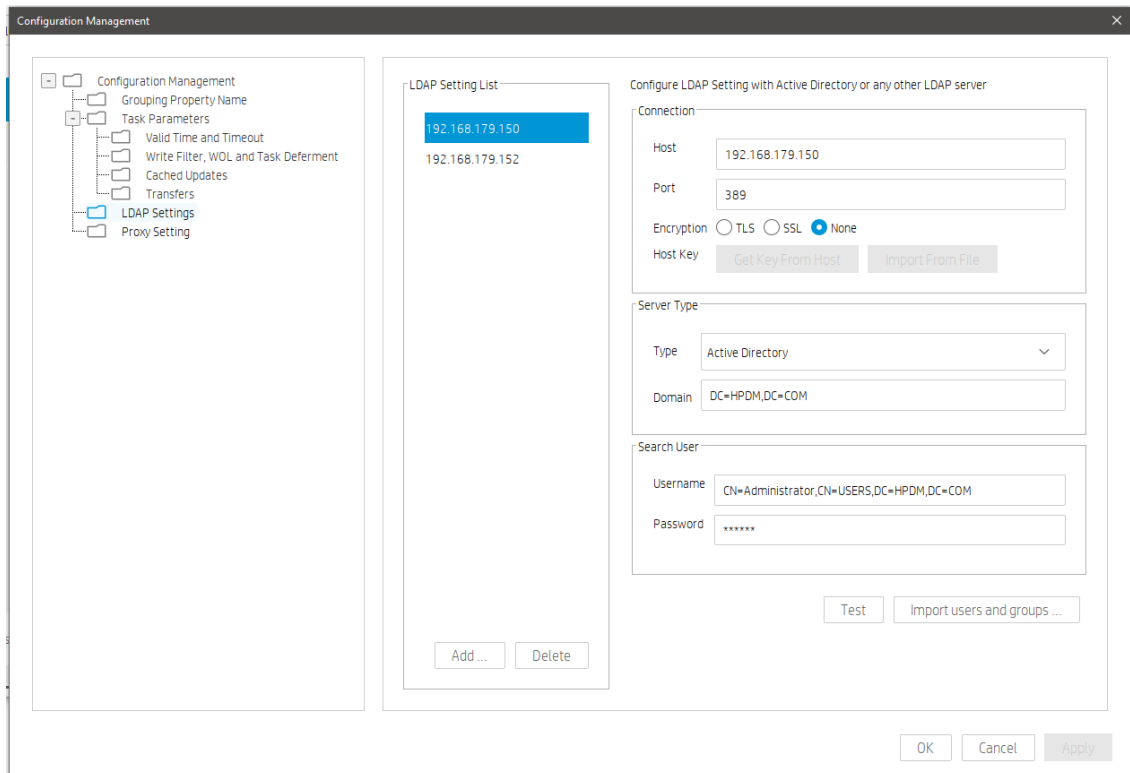
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ping test.hpdn.com
Pinging test.hpdn.com [192.168.231.152] with 32 bytes of data:
Reply from 192.168.231.152: bytes=32 time<1ms TTL=128
Reply from 192.168.231.152: bytes=32 time<1ms TTL=128
Reply from 192.168.231.152: bytes=32 time<1ms TTL=128
Reply from 192.168.231.152: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.231.152:
    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>_

```

*Multiple trusted domains support*  
 User authentication with hpdn.com

To log in to HPDM with a child domain account using parent user authentication:

1. Go to HPDM Console > **Administration** > **Configure Systems** > **LDAP Settings**
2. Use the user account for hpdn.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. It can log in to HPDM successfully.

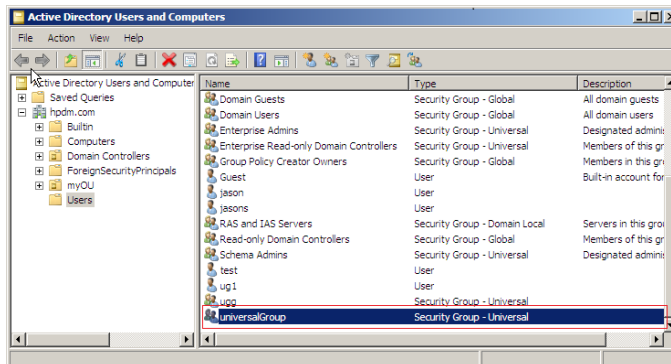
### Universal group login

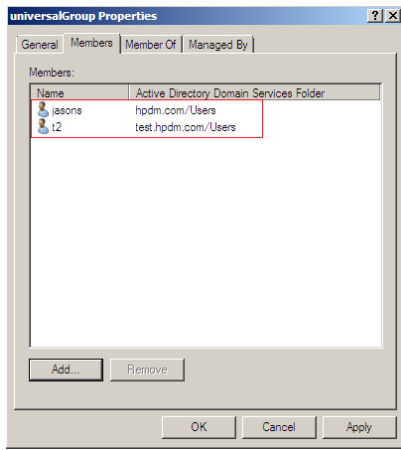
A universal group is a group that can contain accounts from the current domain and other trusted domains. The advantage of using a universal group is that you can import the group into HPDM. You only need to add accounts from different domains into it.

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 hpdn.com) and t2 (from test.hpdn.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 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, click **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 rule requires **Template Viewing** privilege, when selecting **Rule Management**, **Template Viewing** is selected default. And when **Template Viewing** is unchecked, the **Rule Management** will be unchecked automatically.

---

### Note

If you do not have the privilege to perform an operation, an HPDM Console error message appears.

This is different for the **template View** and **User Management** operation. If you do not have the **template View** privilege, the **Templates & Rules** will not display on the HPDM Console. If you do not have **User Management privilege**, the **Users & Groups** will 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 –
2. Right-click a template and select **Set Access Privileges**.
3. If necessary, to configure the default privileges, select a group, and then select **Edit** to change the group's system-level privileges.
4. To see all current templates, select **List all templates**.
5. 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 the template privilege has been changed, the template name become bigger.

---

### HPDM behavior under privilege management system

In HPDM, there are three default groups:

- **Administrators**—This group has all privileges and cannot be edited.

- **Power Users**—This group has basic privileges. New users are assigned to this group by default.
- **Users**—This group has only the template Execute privilege and other read-only privileges.

You can create and customize new groups. By default, these groups will 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 cannot delete user. 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 the all privileges assigned to those groups.
- For system-level privilege operations, if a user has no right to operate, there a message appears to notify the user. The only exception is the Template View and User Management.
- If a template's privileges are inherited from a group, the template privileges change when the group privileges change. If a template has its own privileges, the template privileges do not change with the group privileges.
- A newly generated template has the following privileges:
  - It inherits its privileges from its parent template; that is, the template it “name become bigger” from.
  - 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 happens:
  - If the user does not have the **Template View** privilege, the **Templates & Rules** does not appear in the HPDM Console.
  - If the user does not have the **User Management** privilege, the **Users & Groups** does not appear 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.

**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 are diagrams of privilege related operations.

Category	Subcategory	Atom privilege	Comment	Power Users	Users
Administartion	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				
		Import template				
		Delete template		If no modify privilege, the template will not be editable.	√	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**

Every privilege is independent and does 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.

You 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.

You 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.

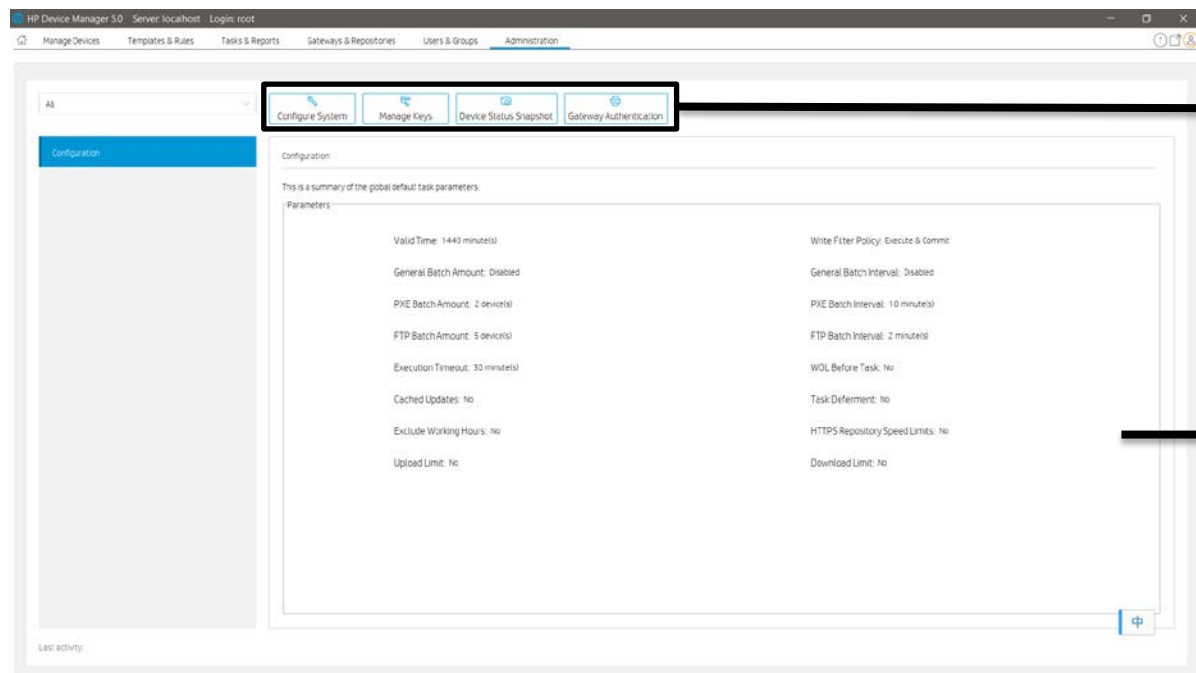
- Group1 has the \_Update Agent privilege only (View, Modify).
- Group2 has the \_Get Asset Info privilege only (View, Execute).

You 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 of their subtemplates.

The new template will only have 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 will check the key passed by HPDM Server when executing tasks.
- Status Snapshot—Status snapshot schedule.
- Gateway Authentication—HPDM Gateway access control

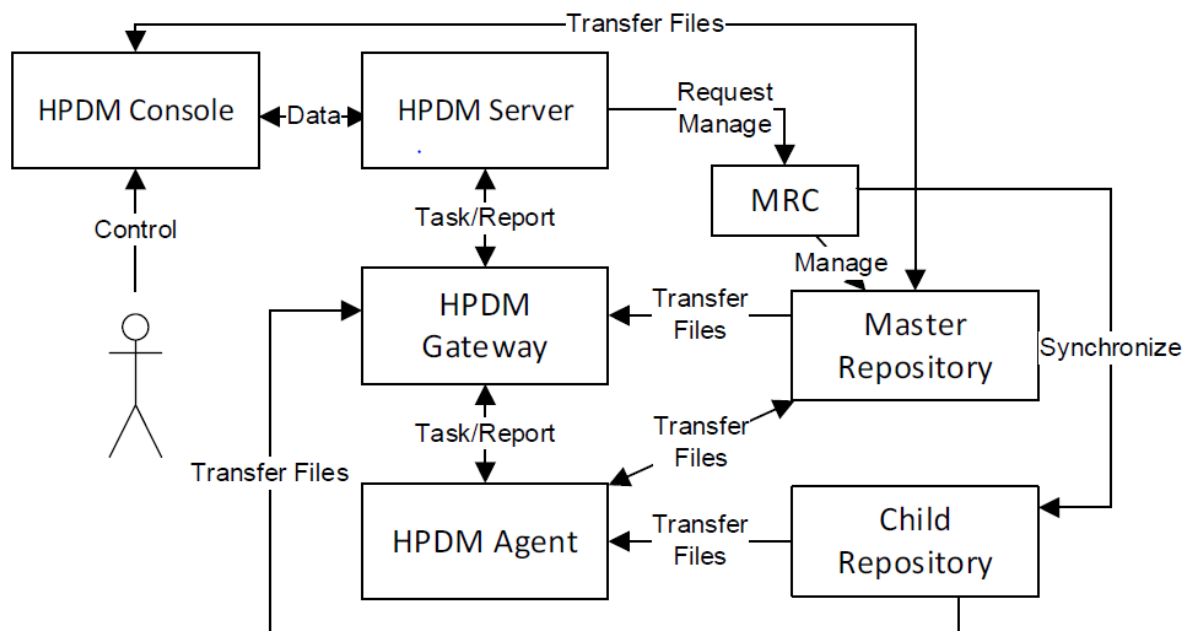
2. Configuration View—Summary of the global default task parameters.

## 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 18. 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 integrity

When HPDM is installed, it will prompt you to set a password for the super administrator account. The HPDM Administrators' usernames and the MD5 hash values of their passwords will be saved in the database you select. When an HPDM Administrator tries to log on to the HPDM Console, the HPDM Server compares the input (username and MD5 hash value of the password) to the data in the database to determine whether to allow or deny access. HPDM saves only the MD5 hash value of the password, which is unlikely to reveal the original password to a hacker, because MD5 is an asymmetric 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 MD5 hash value.
  - A. If the agent key's MD5 cannot be recognized, the gateway will refuse the connection.
  - B. If the agent key's MD5 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 DES algorithm before being sent to the agent.
  - C. If the agent key's MD5 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](http://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: AES256-GCM-SHA384:ECDSA-AES128-GCM-SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-AES128-SHA:ECDSA-AES256-SHA:ECDSA-AES128-SHA256:ECDSA-AES256-SHA384:ECDSA-RSA-AES128-GCM-SHA256:ECDSA-RSA-AES256-GCM-SHA384:ECDSA-RSA-AES128-SHA:ECDSA-RSA-AES256-SHA:ECDSA-RSA-AES128-SHA256:ECDSA-RSA-AES256-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256

### **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/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. A challenge message includes two parts:
    - i. MD5 checksum of the HPDM Agent's current key.
    - ii. 128-byte randomly generated string.
7. When the HPDM Gateway receives the challenge message, it searches the MD5 hash values of the keys from the key list. If it finds the key, it calculates the MD5 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 MD5 hash value. If the MD5 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 guarantee you can upgrade Agents and Gateways from 4.7 to 5.0. If your Agents or Gateways are not 4.7, please install HPDM 4.7 to upgrade them to 4.7 at first.

### **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—Generate **\_File and Registry** templates

### 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-

Click **HP Update Center** toolbar button in **Template & Rules** page.

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

**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.

---

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

---

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

---

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

---

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

---

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

### Configuring HP Update Center proxy settings

1. In HPDM Console, click **Configure System** in **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 lists all versions of HPDM.

---


**IMPORTANT:** This feature requires Internet access. If the system running HPDM Console or HPDM MasterRepository 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. Click  button in the upper right corner of the console, select Documentation.
2. The documentation table dialog will pop up, then click on the document's name hyperlink.
3. The default browser will open a link to this document.

### Access software updates

1. Click  button in the upper right corner of the console, select Software Updates.
2. The software table dialog will pop up, then click on the software's name hyperlink.
3. The default browser will open a link to this software.

---

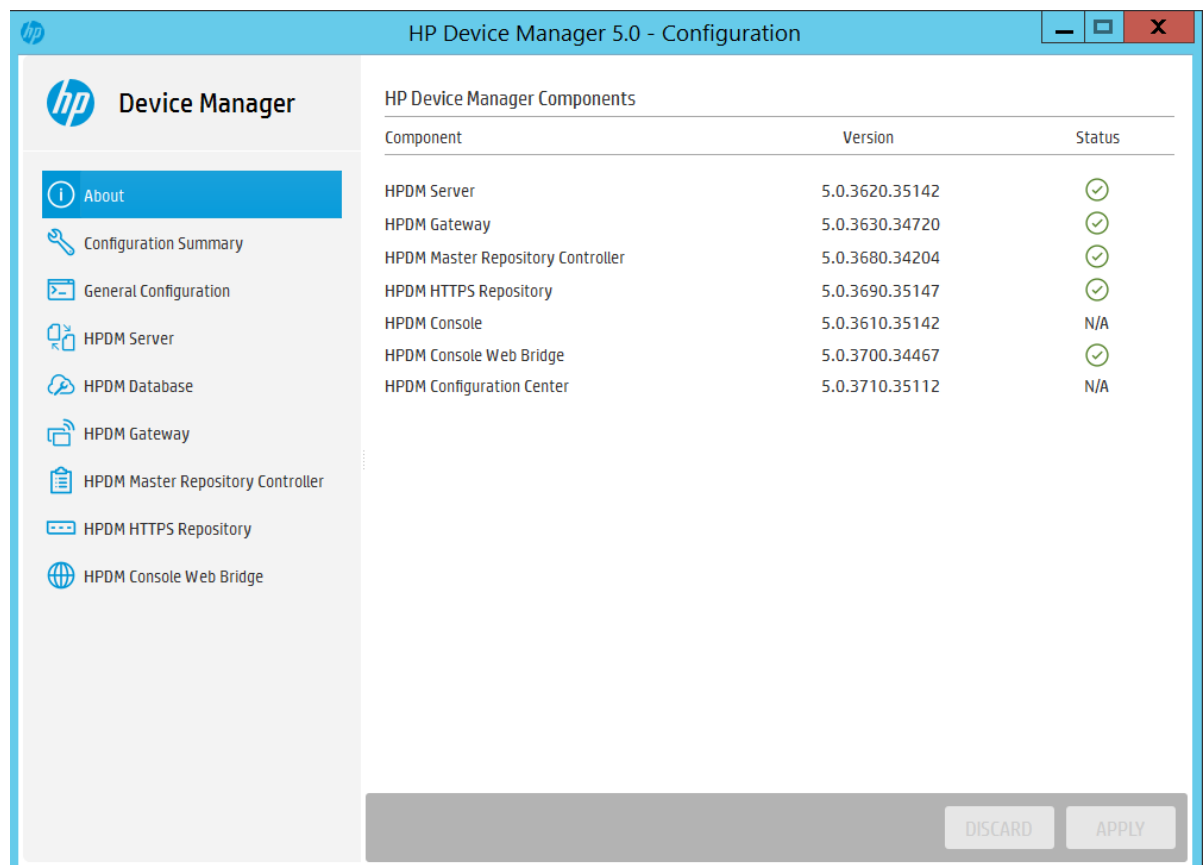
### Note:

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.



The screenshot shows the HP Device Manager 5.0 - Configuration window. On the left is a navigation pane with the HP logo and 'Device Manager' title. Below it are menu items: About (selected), 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 is titled 'HP Device Manager Components' and contains a table with three columns: Component, Version, and Status. The table lists several components with their respective versions and status indicators (green checkmarks for installed, N/A for not installed). At the bottom right of the main area are 'DISCARD' and 'APPLY' buttons.

Component	Version	Status
HPDM Server	5.0.3620.35142	✓
HPDM Gateway	5.0.3630.34720	✓
HPDM Master Repository Controller	5.0.3680.34204	✓
HPDM HTTPS Repository	5.0.3690.35147	✓
HPDM Console	5.0.3610.35142	N/A
HPDM Console Web Bridge	5.0.3700.34467	✓
HPDM Configuration Center	5.0.3710.35112	N/A

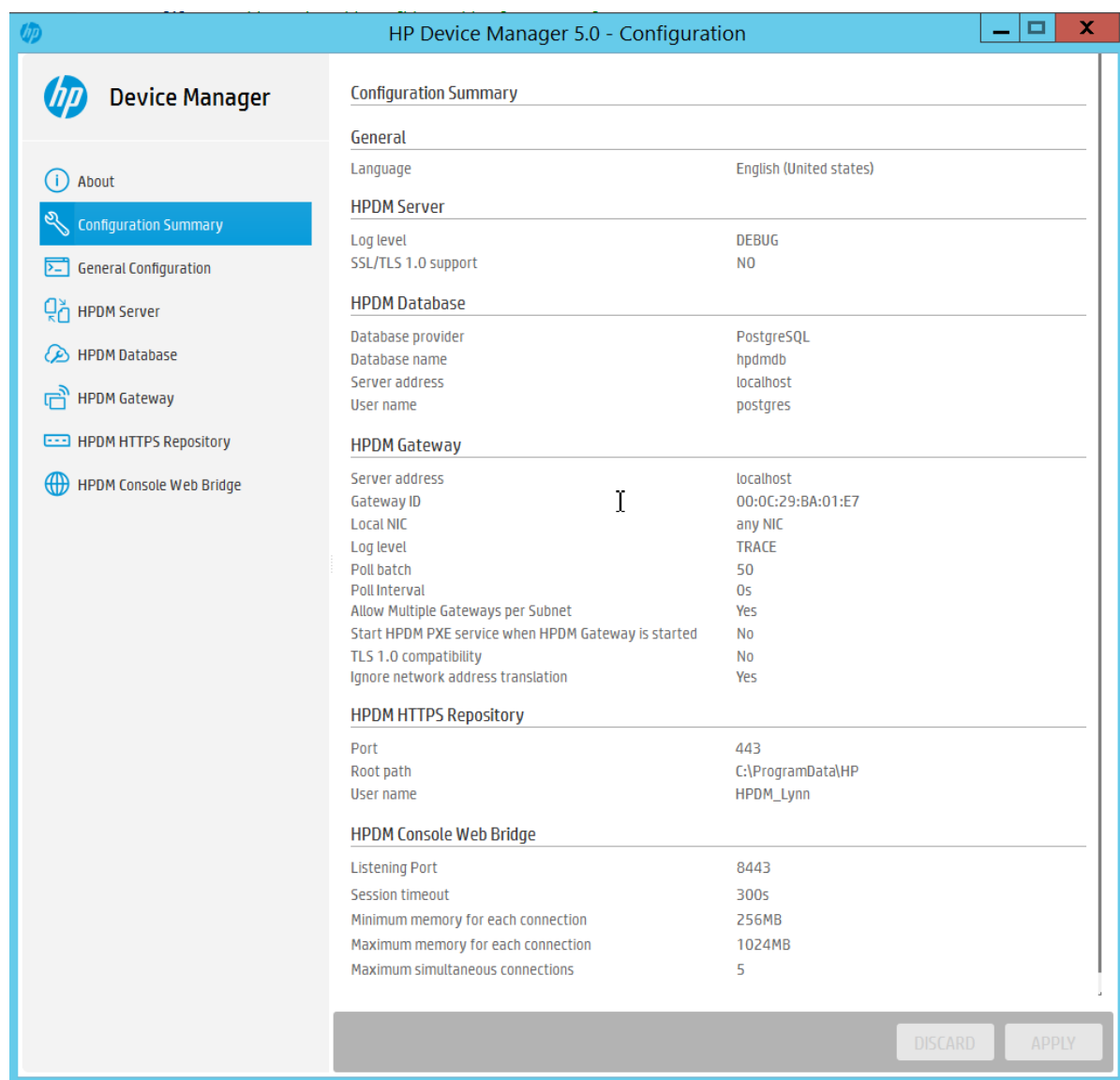
Note: 1. **Component:** list all the installed HPDM Component.

2. **Version:** the version of HPDM Component.

3. **Status:** the status of HPDM Component service, if there is not a service of HPDM Component, display "N/A".

## Configuration Summary

In Configuration Summary page, you can see the detailed configuration about the HPDM Components you have installed.



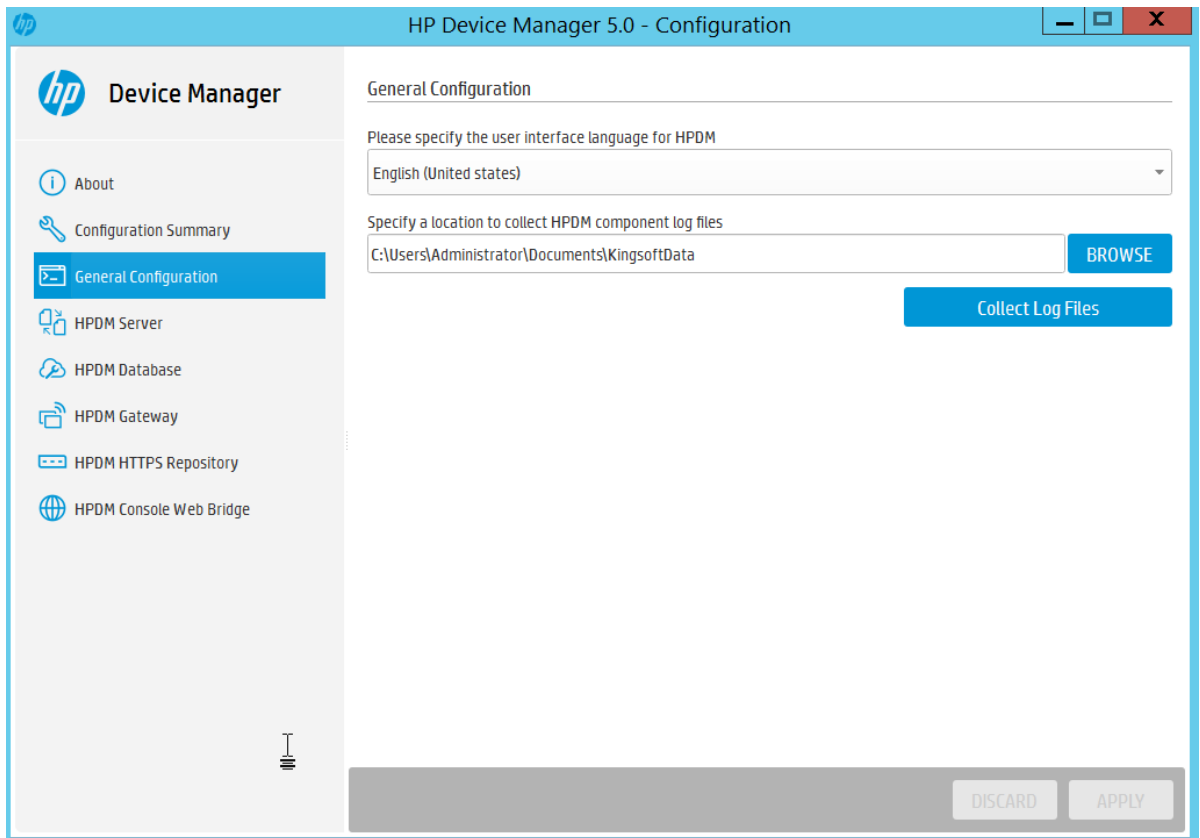
The screenshot shows the HP Device Manager 5.0 - Configuration window. The left sidebar contains the following navigation items: About, Configuration Summary (highlighted), General Configuration, HPDM Server, HPDM Database, HPDM Gateway, HPDM HTTPS Repository, and HPDM Console Web Bridge. The main content area displays the Configuration Summary for various components:

Configuration Summary	
<b>General</b>	
Language	English (United states)
<b>HPDM Server</b>	
Log level	DEBUG
SSL/TLS 1.0 support	NO
<b>HPDM Database</b>	
Database provider	PostgreSQL
Database name	hpdmdb
Server address	localhost
User name	postgres
<b>HPDM Gateway</b>	
Server address	localhost
Gateway ID	00:0C:29:BA:01:E7
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	Yes
<b>HPDM HTTPS Repository</b>	
Port	443
Root path	C:\ProgramData\HP
User name	HPDM_Lynn
<b>HPDM Console Web Bridge</b>	
Listening Port	8443
Session timeout	300s
Minimum memory for each connection	256MB
Maximum memory for each connection	1024MB
Maximum simultaneous connections	5

At the bottom right of the configuration area, there are two buttons: DISCARD and APPLY.

## General Configuration

In General Configuration page, you can specify the operating language for HPDM, or collect all HPDM component log files.

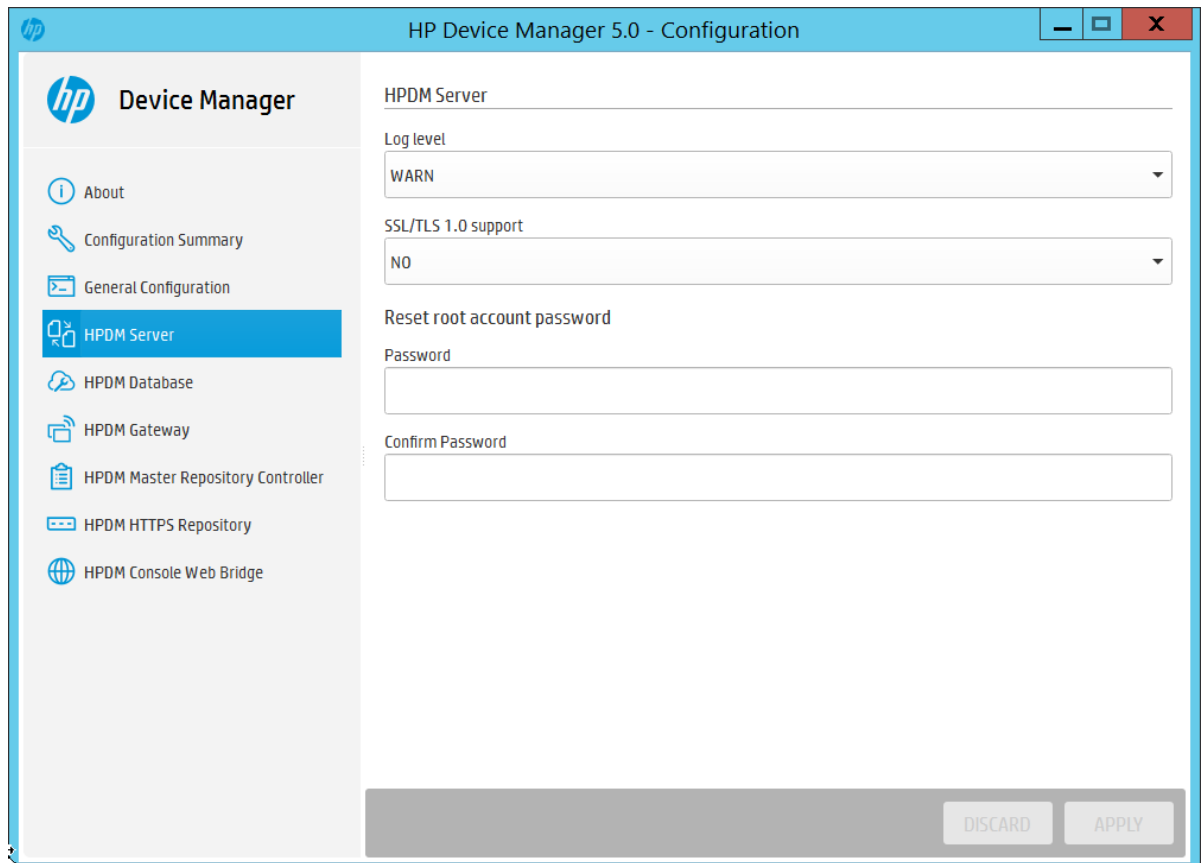


Note: 1. the language you want to use with HPDM, it will take effect on HPDM Console, HPDM Server and this Configuration Tool. If you change the language, the language will be changed immediately after applying, but you need to restart other components.

2. Collect log: use BROWSE to select a to save HPDM components log. Click “Collect Log Files” button to collect logs.

### **HPDM Server**

In HPDM Server page, you can see the detailed configuration of HPDM server.



Note: 1. **Log level:** you can configure the log level of HPDM Server component by choosing the value in combo Box.

2. **SSL/TLS 1.0 support:** if you want to use the SSL/TLS 1.0 support, choose **YESYES** in the combo Box.

3. **Reset root account password:** you can change root account password by using HPDM Configuration Center in the HPDM Server page.

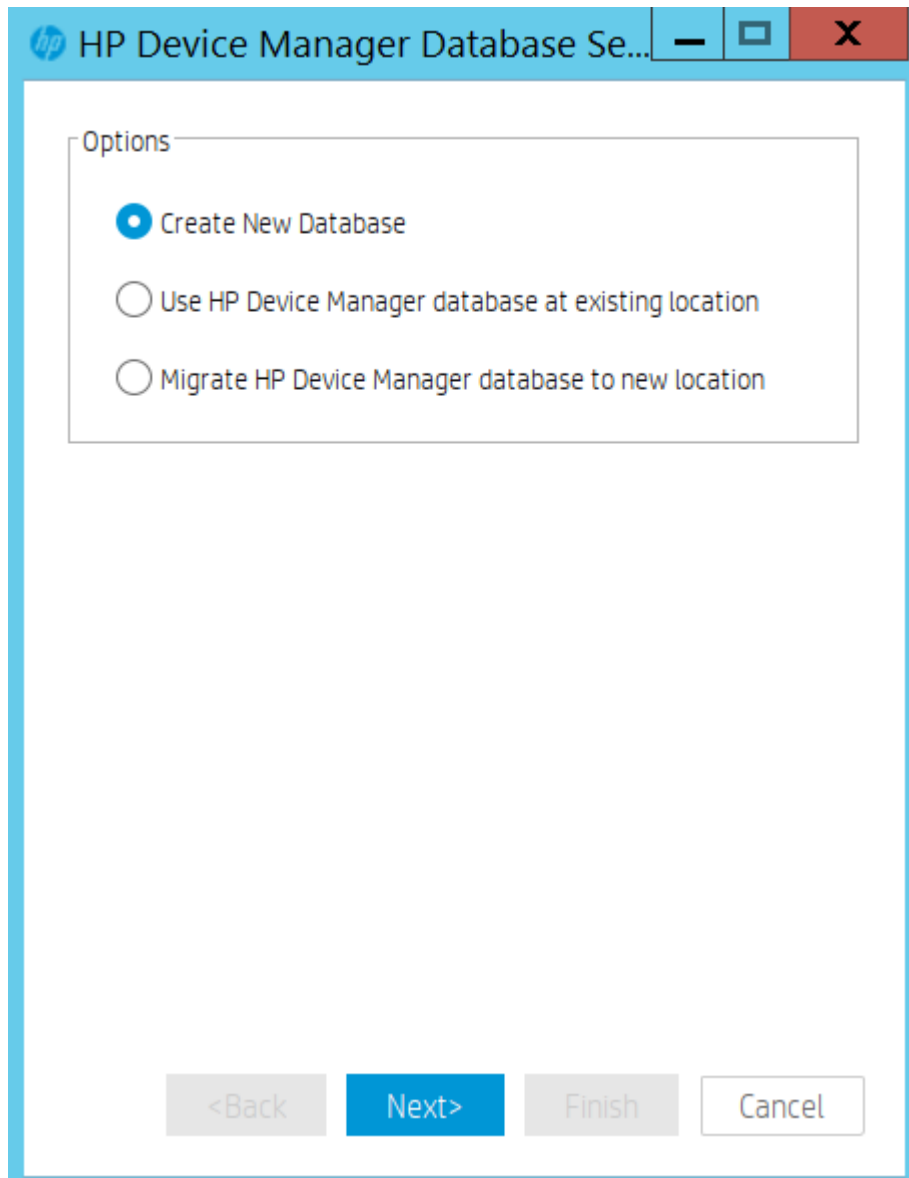
### **HPDM Database**

In HPDM Database, you can see the detailed configuration of HPDM Database Component.

Note: If you are not initializing the HPDM Database, it will show NA about the four properties.

You can click the Manage Database button to operate the HPDM Database.





#### *Create New Database*

1. Select **Create New Database**, and then click **Next**.

HP Device Manager supports two database types:

- **PostgreSQL**—If you choose PostgreSQL, there is no need to do any other database configuration because it is embedded in HPDM
- **MS SQL Server**—If you choose MS SQL, you must first create an independent MS SQL Server instance for you 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 desired database type, and then click **Next**.

- A. If you choose PostgreSQL, you must set a password.

- B. If you choose MS SQL Server, you need to manually input the database information
3. A process bar appears. When the database creation is finished, enter and confirm the password for the root Administrator account, and then click **Finish**.
4. Click **OK**. The database is created successfully.

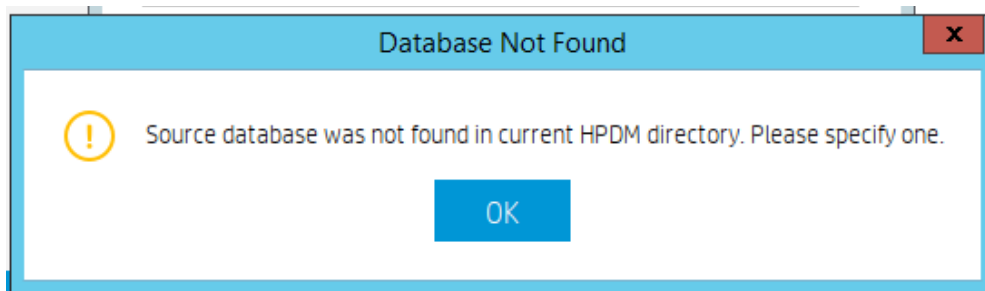
#### *Using an existing database*

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 4.7 database.

1. Select **Use HP Device Manager database at existing location**, then click **Next**.

A processing dialog box is displayed while a connection is made to the existing database. Then, a dialog appears 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, click **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 click **Browse**.
5. Go to the HPDM directory `.../Server/conf`, select the **hibernate.properties** file, and then click **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. Click **Browse**, select the installation path of the last installed HPDM, and then click **Next**.
7. Enter and confirm the password for the root Administrator account, and then click **Finish**.
8. Click **OK**. The existing database is now being used.

#### *Migrate an existing database to a new location*

If you select **Migrate HP Device Manager database to new location**, do the following:

1. Select **Migrate HP Device Manager database to new location**, then click **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 will be loaded automatically.
4. Click **Next**.
5. Specify the destination database, choose the database type, and then click **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 click **Finish**.
7. Click **OK**. The database is now migrated.

## HPDM Gateway

In HPDM Gateway page, you can see the detailed configuration of HPDM Gateway component.

The screenshot shows the HP Device Manager 5.0 Configuration window for the HPDM Gateway component. The window title is "HP Device Manager 5.0 - Configuration". On the left, there is a navigation pane with the following items: About, Configuration Summary, General Configuration, HPDM Server, HPDM Database, HPDM Gateway (highlighted), HPDM Master Repository Controller, HPDM HTTPS Repository, and HPDM Console Web Bridge. The main configuration area is titled "HPDM Gateway" and contains the following fields:

- HPDM Server address: localhost
- Gateway ID: 00:0C:29:BA:01:E7
- 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, there are two more dropdown menus:

- TLS 1.0 compatibility: No
- Ignore network address translation: No

At the bottom right of the configuration area, there are two buttons: "DISCARD" and "APPLY".

Note:1. **HPDM Server address:** you can configure the address of HPDM Server so that the HPDM components are able to interact with this address.

2. **Gateway ID:** the mac address of HPDM Gateway.if there are mutilple NICs, select one mac address as the Gateway ID.

3. **Local NIC:** the IP address of HPDM Gateway.if there are multiple NICs, select ne IP address as Local NIC.

4.**Log level:** you can configure the log level of HPDM Gateway Component by choosing the value in the combo Box.

5. **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.

6. **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 may be 0 or not less than 60. The default value is 0 seconds, which denotes polling is disabled.

7. **Allow Multiple Gateways per Subnet:** forcibly start gateway even if other gateways are detected in the same subnet.

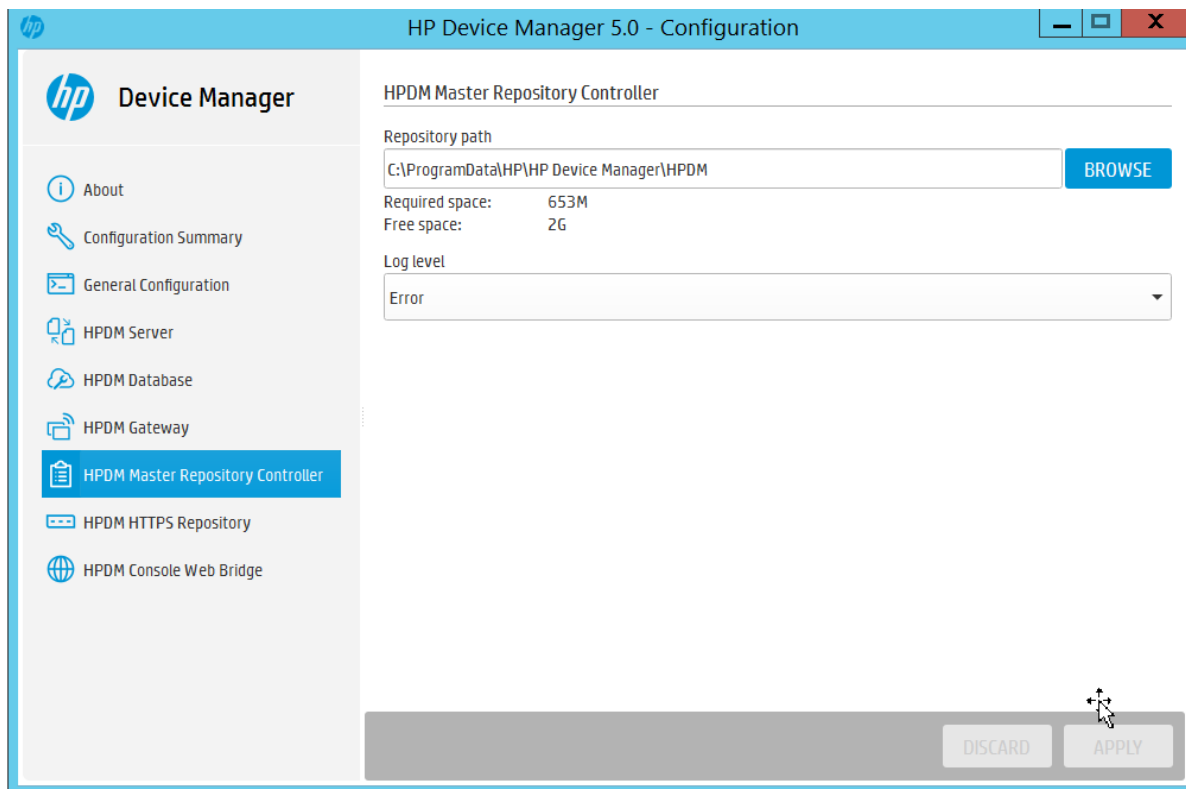
8. **Start HPDM PXE service when HPDM Gateway is started:** PXE service will always be started when Gateway is started.

9. **TLS 1.0 compatibility:** especially This option is for the ThinPro 5 operating system, due to ThinPro 5 supports and for systems that support SSL3.0 and TLS 1.0. This option is especially for ThinPro 5.

10. **Ignore network address translation:** By default HPDM Gateway treats devices with network address translation as not reachable and mark them as working in PULL mode. Choose YES option in the drop-down box to disable this function if your devices behind NAT are reachable.

### HPDM Master Repository Controller

In HPDM Master Repository Controller page, you can see the detailed configuration of HPDM Master Repository Controller component.



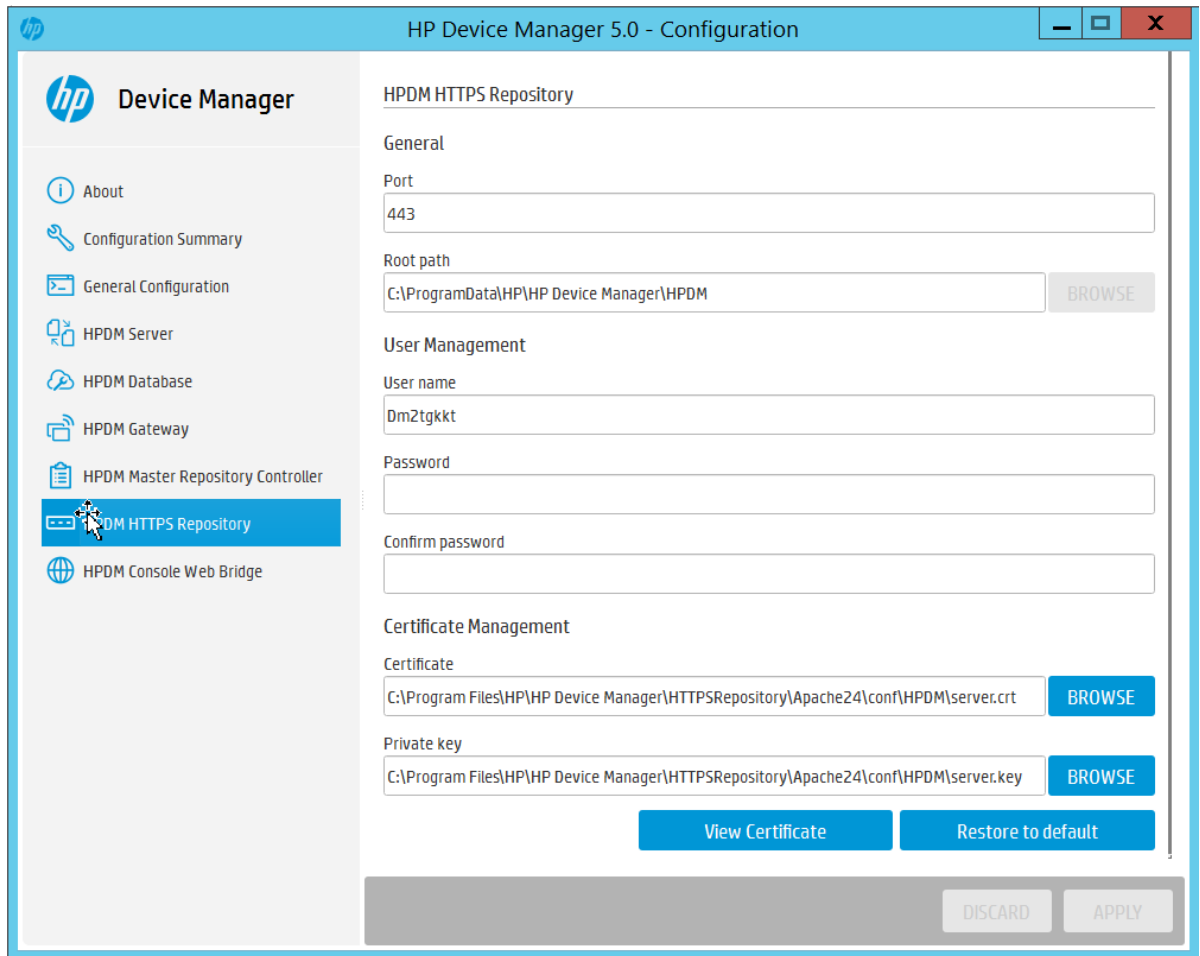
Note:

1. **Repository path:** you can remove the repository root path to where you want to put. Changes will take effect after the HPDM Master Repository has been restarted.

2. **Log level:** you can configure the log level of HPDM Master Repository by choosing the value in the combo Box.

### HPDM HTTPS Repository

In HPDM HTTPS Repository page, you can see the detailed configuration of HPDM HTTPS Repository component.



Note: 1. **Port:** you can configure the occupied port of HPDM HTTPS Repository Component.

2. **Root path:** display the root path of the HPDM HTTPS Repository. The BROWSE button is enabled when the install path of HPDM Master Repository Controller and HPDM HTTPS Repository are not the same.

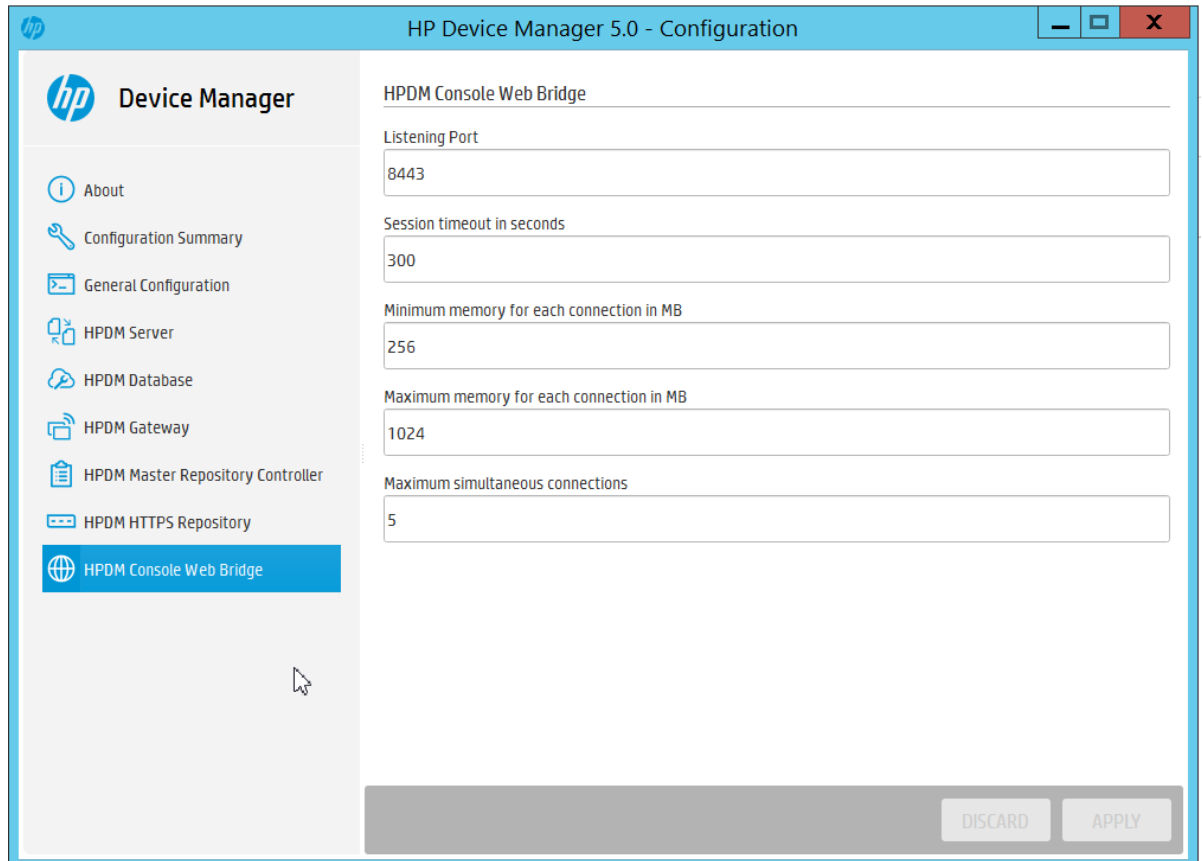
3. **User name:** you can configure the HTTPS user name based on detailed rule when you configure HPDM Master Repository use HTTPS protocol

4. **Password:** you can reset HTTPS account password in the HPDM HTTPS Repository page when you configure HPDM Master Repository use HTTPS protocol.

5. **Certificate Management:** you can 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.



- Note: 1. **Listening Port:** It indicate the port which the server and browsers use to communicate. The default value is 8443.
2. **Session timeout in seconds:** It indicates the longest time for inactive session to maintain a connection. The default value is 300.
3. **Minimum memory for each connection in MB:** It indicate the minimum heap memory each web console can consume. The default value is 256m.
4. **Maximum memory for each connection in MB:** It indicates the maximum heap memory each web console can consume. The default value is 1024m.
5. **Maximum simultaneous connections:** It indicates how many clients can access web resource at the same time. The default value is 5.

## Disaster Recovery

The purpose of this section is to provide 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 normal HPDM disaster recovery process, but your HPDM environment might be different. You need to adapt your strategy accordingly.

---

### General recovery process

This is an overview of the recovery process. For detailed steps, see the following:

- Recovering the HPDM Server
- Recovering the Master Repository

Figure 19. Typical HPDM distribution diagram

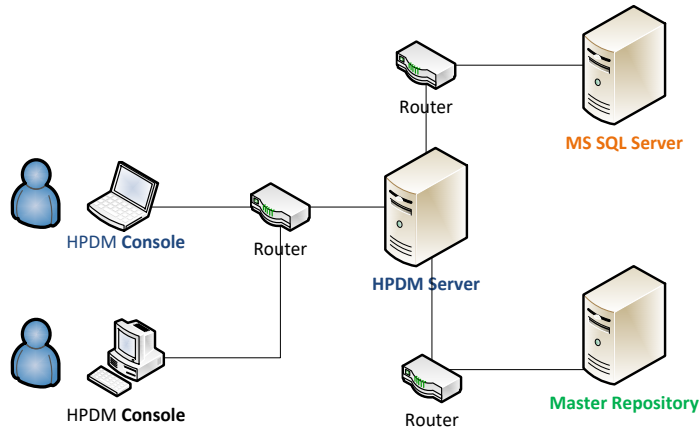
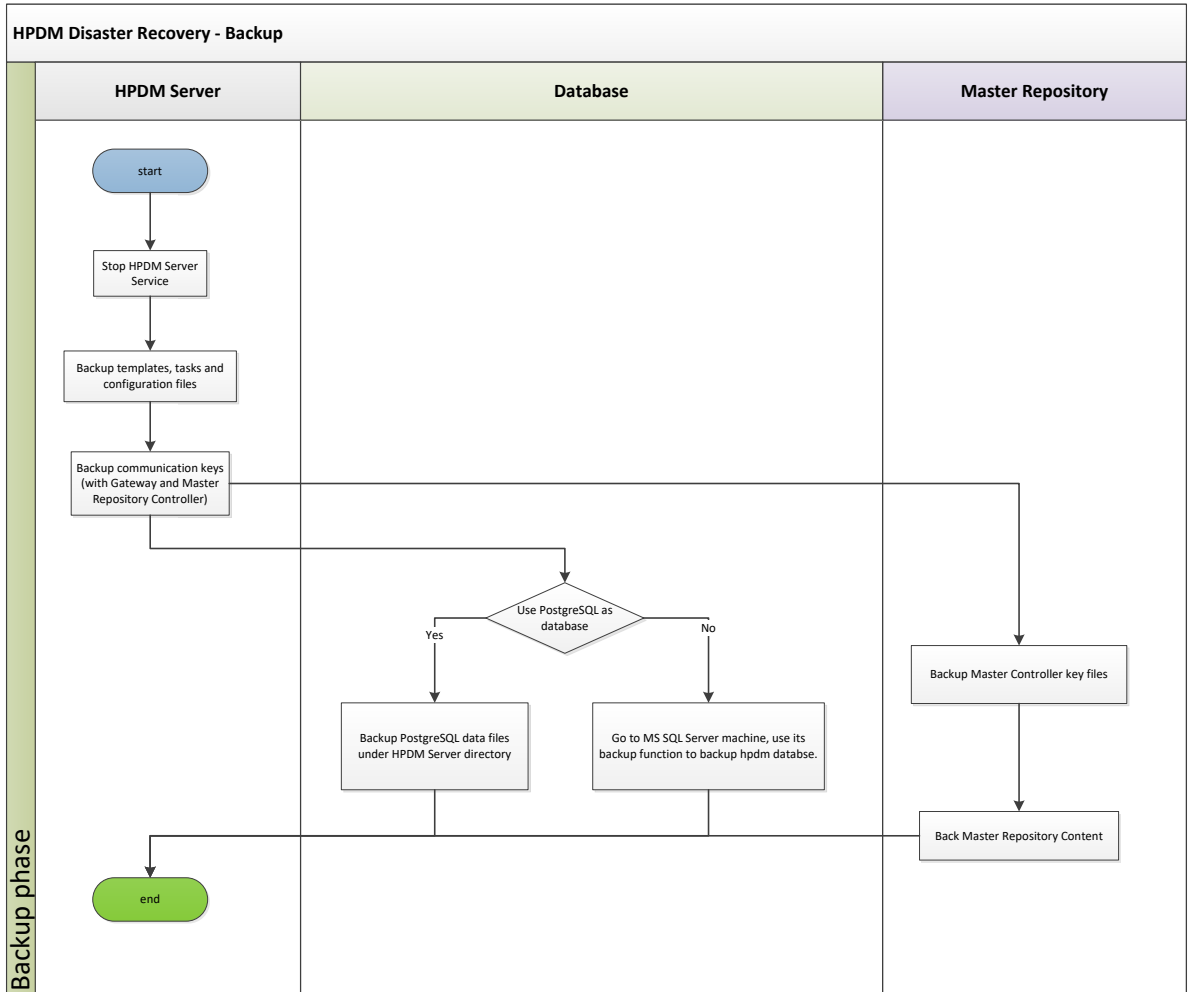


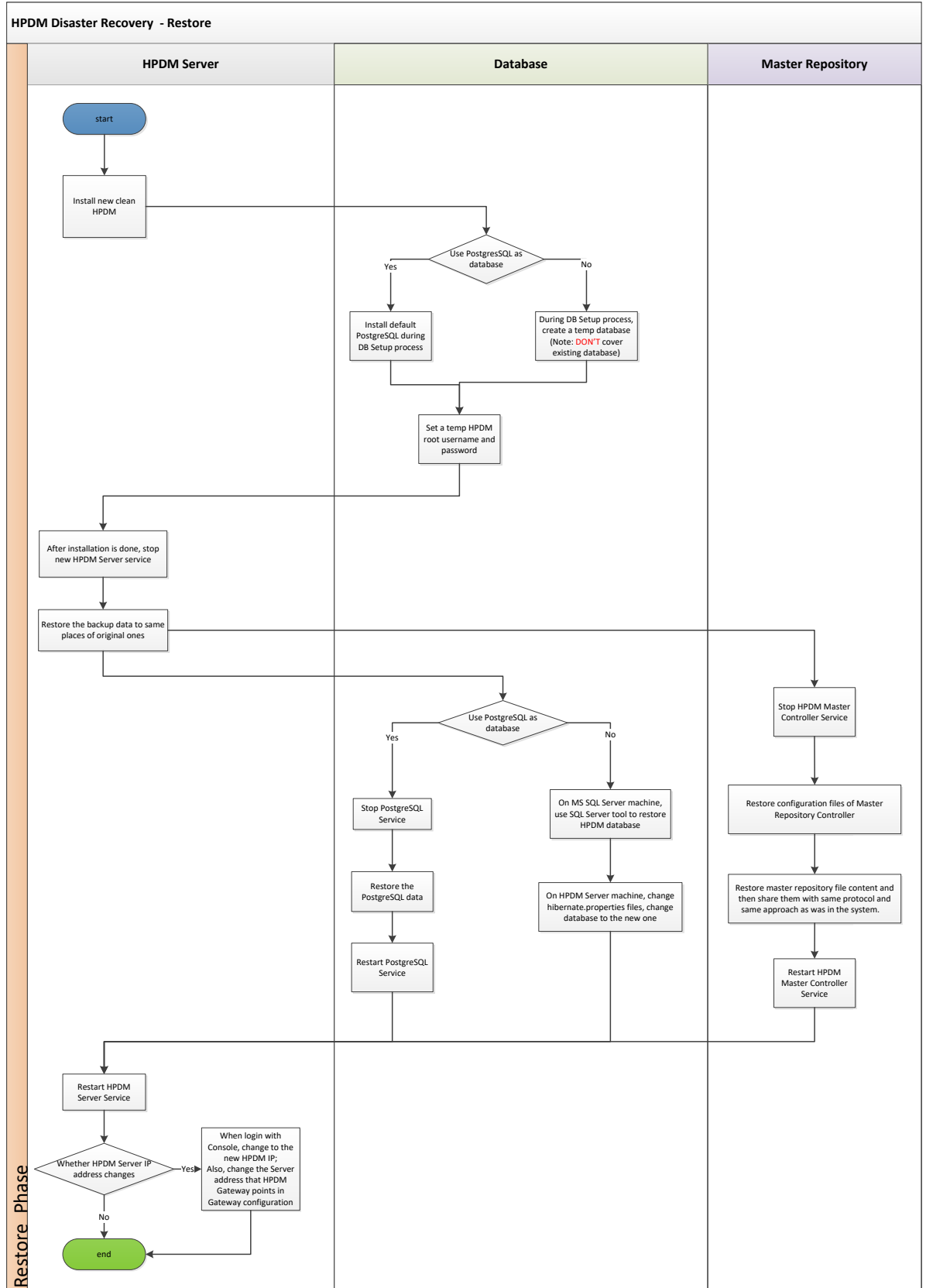
Figure 20. General HPDM disaster recovery workflow (backup phase)



**Note**

In case of an unpredictable disaster, backup your HPDM data periodically according to your strategy.

Figure 21. General HPDM disaster recovery workflow (restore phase)





## Recovering the HPDM Server

The HPDM Server content that can be recovered is as follows:

- Templates, tasks, and template plugin-ins
- Configuration files and communication keys
- Database

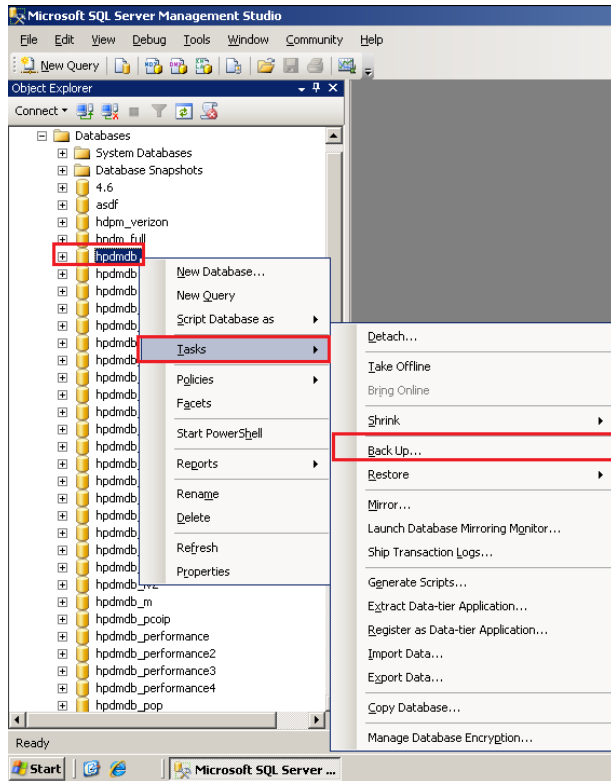
### Backing up the data

After the HPDM Server crashes, back up your data first.

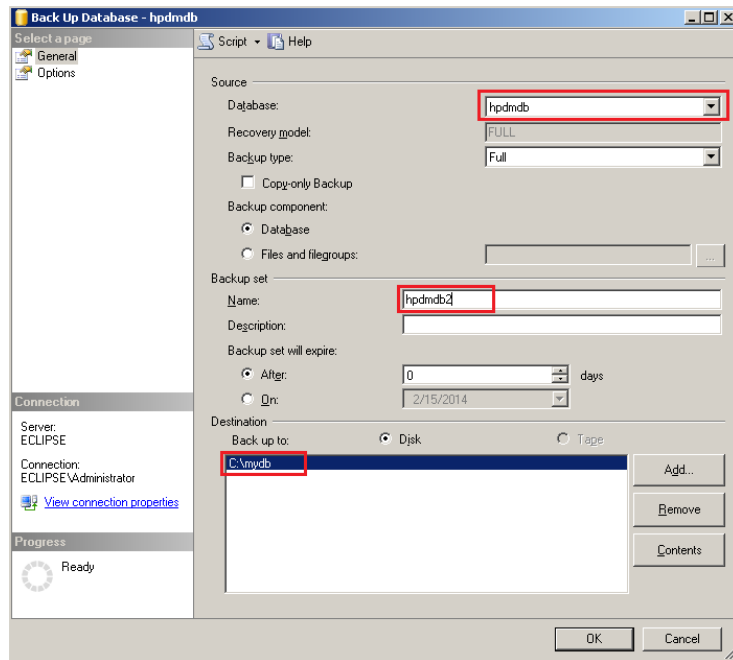
1. Stop the HPDM Server Service.
2. On the HPDM Server installation path, go to <HPDM installation path>\HP Device Manager\Server. Then, back up the following directories:
  - A. conf
  - B. template
  - C. task
  - D. template\_plugins (if it exists)
3. Go to the directory <HPDM installation path>\HP 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, do the following, depending on which type of database you use with HPDM:
  - A. If you use PostgreSQL as the HPDM database, you need to back up its data to the HPDM Server installation path.
  - B. Go to the directory <HPDM installation path>\HP Device Manager\Server\pgsql.
  - C. Back up the data folder.
  - A. If you use MS SQL Server as the HPDM database, back up its data using the MS SQL Server tool.
  - B. Open **MS SQL Server Management Studio**, and use it to connect to your source database. Be sure that you have installed this tool.



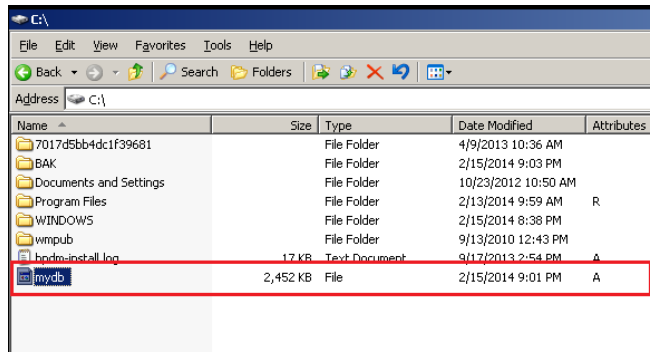
- C. Select the HPDM database you want to back up, right-click to open a pop-up menu, and then select **Tasks > Back Up**. This example uses the database name hpdmdb.



D. Specify the source **databasehpdmdb**, and create a backup database named **hpdmdb2**. Then, set the destination path **c:\mydb**. Click **OK**.



E. 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.

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]`.

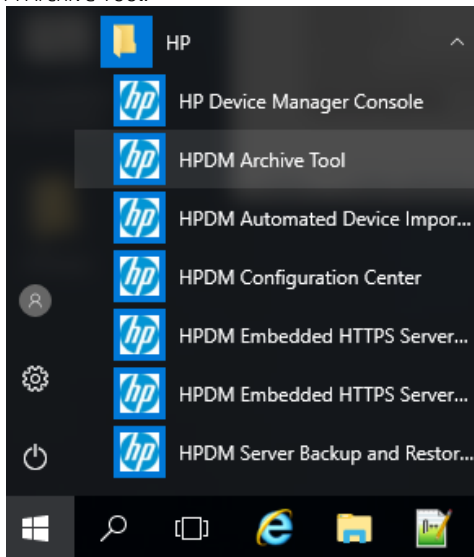
- C. Restart the HPDM PostgreSQL service.

### 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:

This PC > Local Disk (C:) > Program Files > HP > HP Device Manager > Server > conf

Name	Date modified	Type	Size
archive.conf	4/8/2019 1:21 AM	CONF File	3

- object—By default, the Both option handle 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.

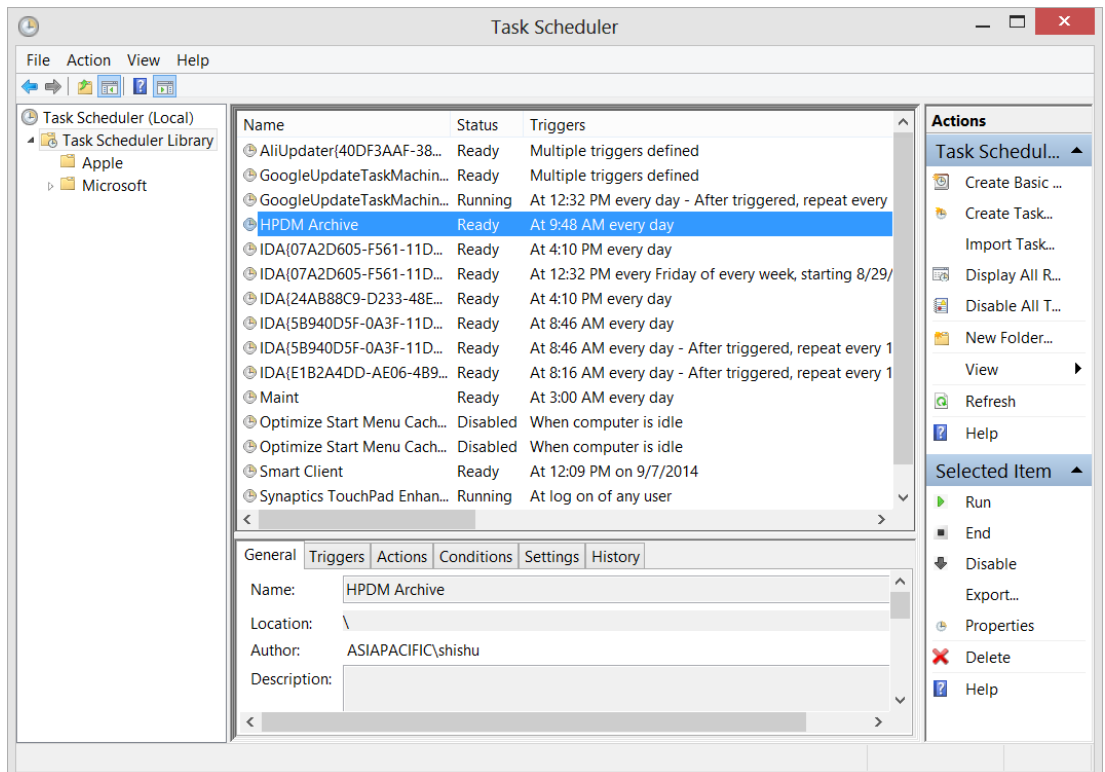
4. Under \Server\logs, there is the archive tool log: hpdm-archive.log. This shows the process information.

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, like in the following example:  
C:\Program Files\HP\HP Device Manager\Server\bin\archive.cmd
4. For Add arguments, enter the following:  
-config:archive.conf
5. For Start in, enter the full path to \Server\bin, like in the following example:  
C:\Program Files\HP\HP Device Manager\Server\bin
6. Select Create Basic Task, and then schedule the task.

## Optimizing Device manager

TODO WP\_Deployment-Guide\_HPDM-4.7-SP3

## Troubleshooting

This section introduces some general information that can help troubleshoot and triage issues in HP Device Manager (HPDM).

### Log files

#### HPDM Agent log files

Path

WES/XPe—C:\Windows\xpeagent

HP ThinPro series/Smart Zero Core—/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 either C:\Program Files\HP\HP Device Manager\Gateway.

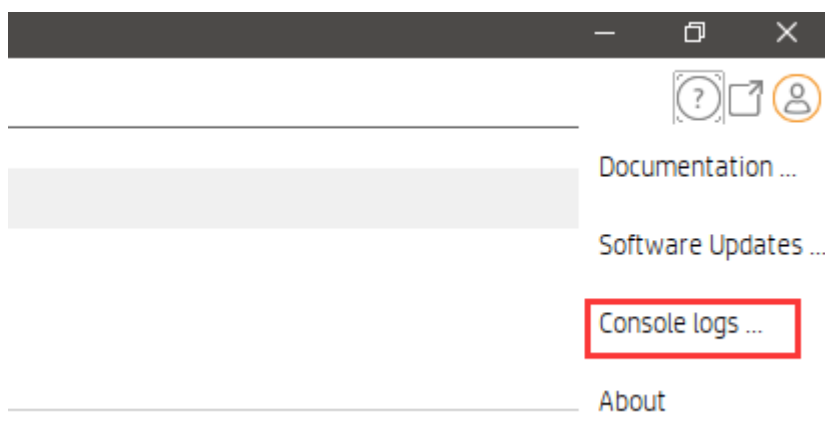
#### Files

- 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 located in the %programdata%\HP\HP Device Manager\Console\logs\username folder, 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, and it is 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 Embedded HTTPS Server-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**

First, upload the HPDM Agent logs files with a Capture File task or copy them locally.

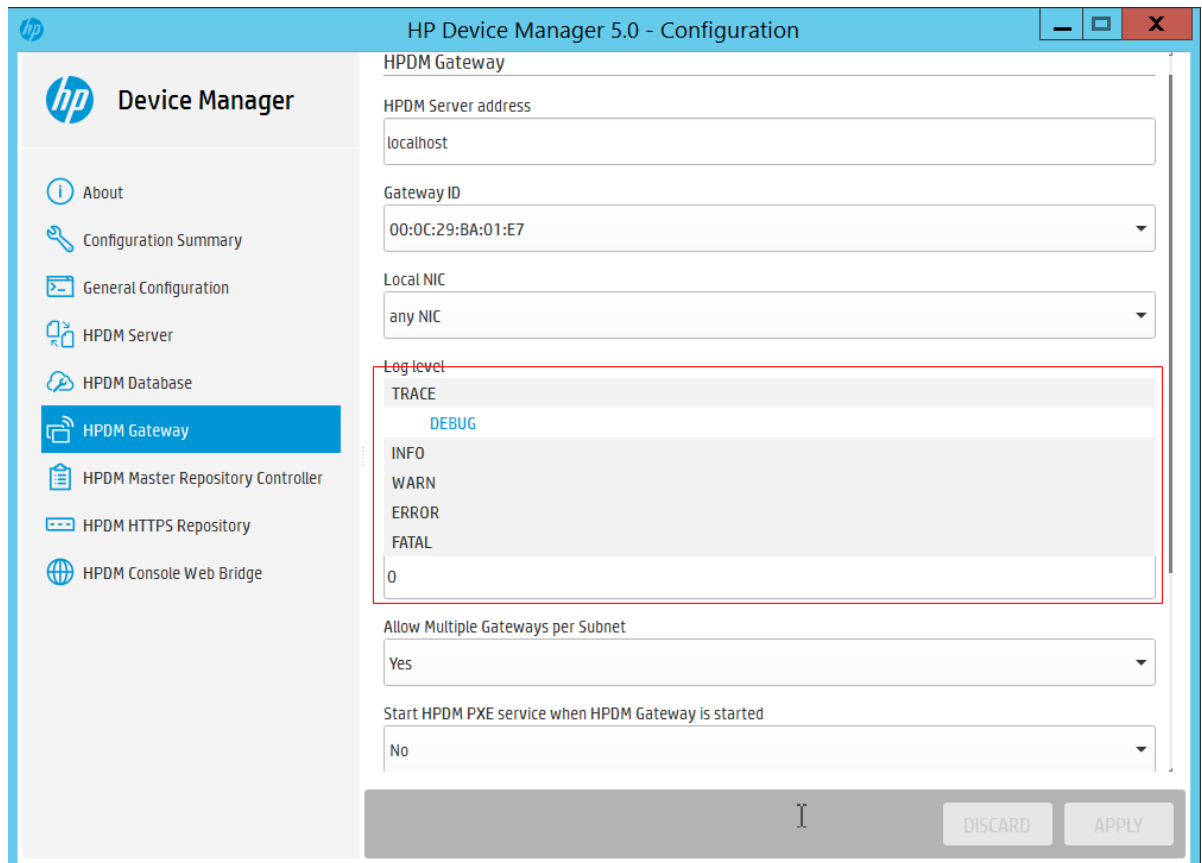
The default log level of the HPDM Agent is Error. If your issue can be reproduced, set the Log Level to Information with a Configure Agent task. Then, reproduce the issue. Finally, upload the HPDM Agent logs files with a Capture File task or copy them locally.

### **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 will be printed. Copy the HPDM Console logs if you see the keyword Exception in them, and then compress them to a package.

If a task fails, you can select the target device to find useful information.

Figure 23. Failed task

The screenshot displays the 'Device Task View' for task '13\_7E\_t628\_image' on device 'HP-480FCFBB51BB'. The interface is divided into several sections:

- Information:** Task Name: 13\_7E\_t628\_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:** A table with columns: Device Name, Status, Error Code, Start Time, End Time. One entry is highlighted with a red box: HP-480FCFBB51BB, Failed, 311, 2019-05-..., 2019-05-...
- Task Log:** A list of log entries. A red box highlights the error details for the failed task:
 

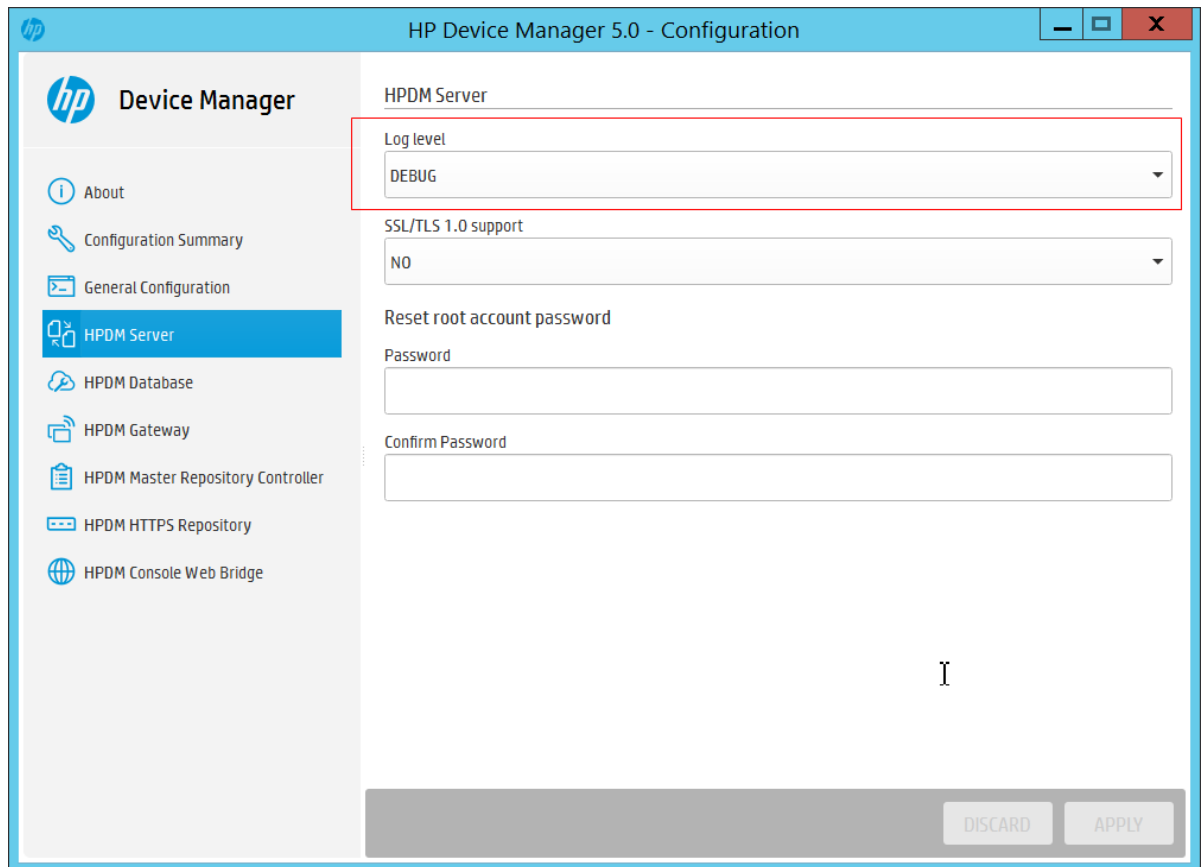
Log Time	Log
2019-05-16 09:25:33	Map repository to: Master Repository
2019-05-16 09:25:38	Successfully sent task to the HPDM Gateway
2019-05-16 09:26:45	Task has been retrieved by the Agent.
2019-05-16 09:26:50	Failed to download 13_7E_t628_image.ibr from /Repository/Images/13_7E_t628_image.
2019-05-16 09:26:50	Failed to execute PXEDeploy task. Error Code: 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. Error Code: 311, Error Detail: Failure downloading image file from FTP server.

Red annotations include a box around the task status table entry with the text 'Select target device' and a box around the error log entries with the text '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**, click **APPLY** to save the settings. And then restart the HPDM Server.

Figure 24. Modify server log level through the Configuration Center



Set the following flags to true:

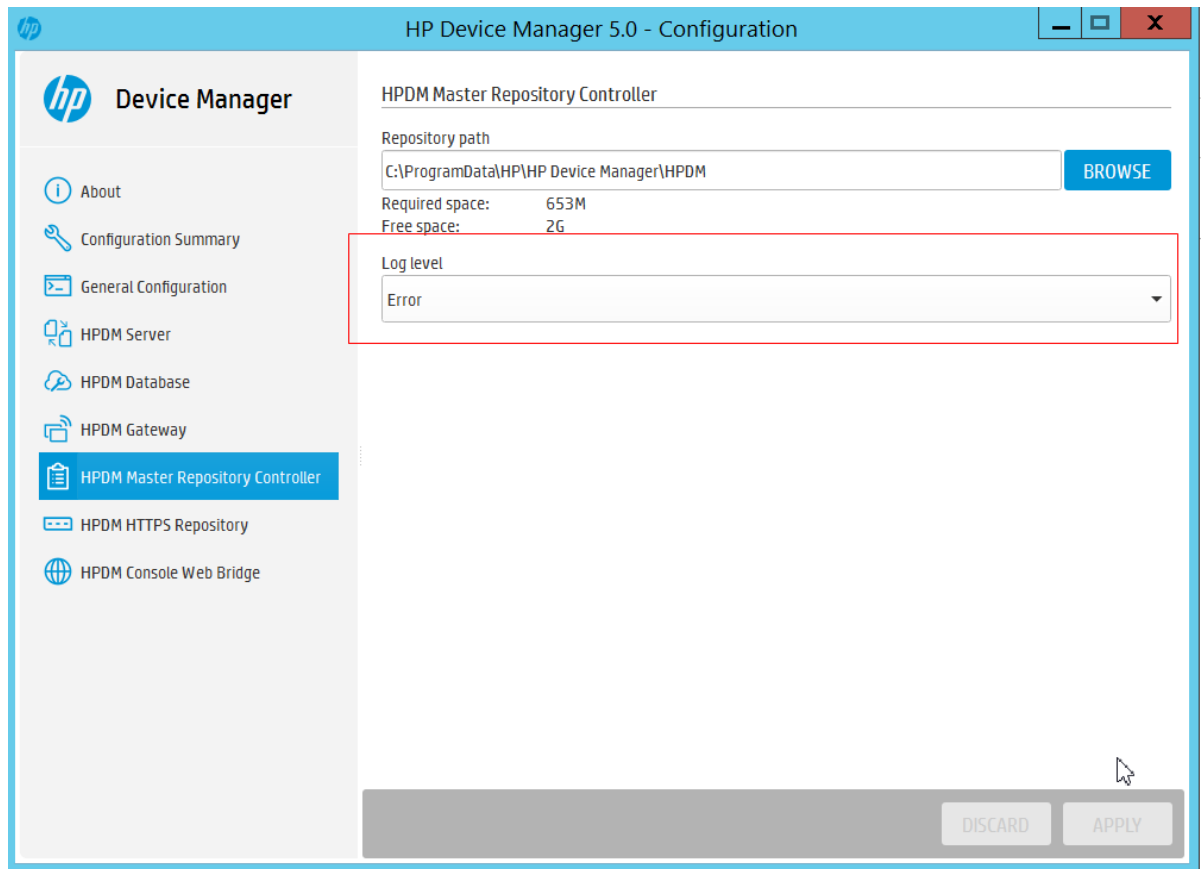
- `hpdm.log.gateway=false`
- `hpdm.log.console=false`
- `hpdm.log.task=false`
- `hpdm.log.masterController=false`

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 will be printed. If your issue is related to the Master Repository Controller, open **Controller.conf**, change **LogLevel** to **2**. Or open the Configuration Center, select **HPDM Master Repository**, change **Log level** to **Info**, click **APPLY** to save the settings. Then 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.

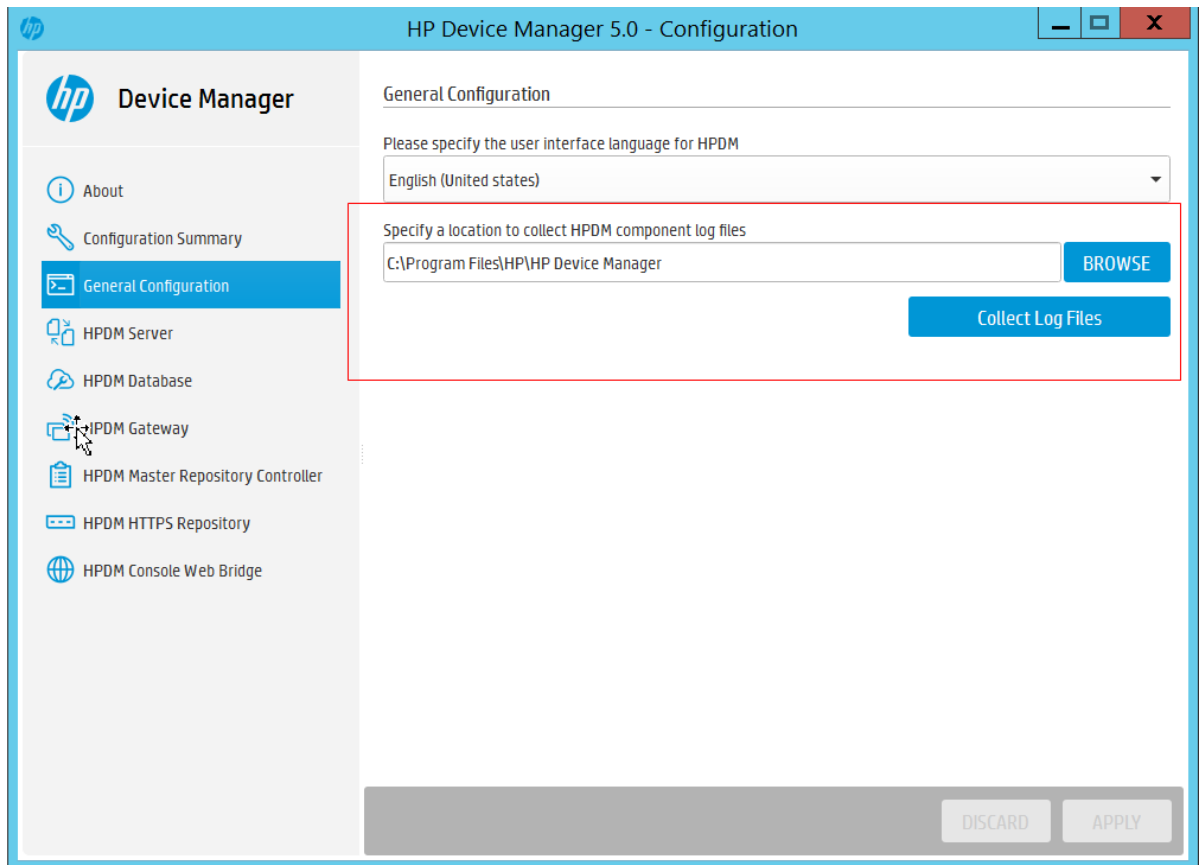
Figure 25. Modify Master Repository log level through the Configuration Center



## Collect all HPDM component logs

Open the Configuration Center, select **General Configuration**, click **BROWSE** to select the directory where you want to output the log, then click **Collect Log Files** button to get all the logs. The local installed component logs will be saved to the directory which 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 of this Guide 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 HPDMPortCheck.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 WES and XPe, 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 WES HPDM Agent can do an Update Agent task, but it cannot image.

WES7E, WES7P or Win10 IOT imaging solution must need shared folder, please make sure 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.

Make 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 selected too.

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 of this Guide.

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 that customers use 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>

You can set another folder, instead of 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 1. Error code matrix, part one

	<b>HPDM Agent</b>	<b>DMMC (HPDM Agent Library)</b>	<b>UCT (HPDM Agent Library)</b>	<b>DMAC (HPDM Agent Library)</b>	<b>WES7DISP (HPDM Agent Library)</b>	<b>MINILINUX</b>
<b>Network connection</b>	1064960	1130496	1196032	1261568	1327104	1392640
<b>Disk I/O</b>	1065984	1131520	1197056	1262592	1328128	1393664
<b>Memory error</b>	1067008	1132544	1198080	1263616	1329152	1394688
<b>Remote file/dir operation</b>	1068032	1133568	1199104	1264640	1330176	1395712
<b>File integrity</b>	1069056	1134592	1200128	1265664	1331200	1396736
<b>Credential</b>	1070080	1135616	1201152	1266688	1332224	1397760
<b>Other FTP-related error</b>	1071104	1136640	1202176	1267712	1333248	1398784
<b>Write Filter error</b>	1072128	1137664	1203200	1268736	1334272	1399808
<b>Unmanageable device</b>	1073152	1138688	1204224	1269760	1335296	1400832
<b>Unsupported task</b>	1074176	1139712	1205248	1270784	1336320	1401856
<b>Incompatible platform</b>	1075200	1140736	1206272	1271808	1337344	1402880
<b>Message syntax error</b>	1076224	1141760	1207296	1272832	1338368	1403904
<b>Message semantic error</b>	1077248	1142784	1208320	1273856	1339392	1404928
<b>Registry error</b>	1078272	1143808	1209344	1274880	1340416	1405952
<b>Command return non-zero</b>	1079296	1144832	1210368	1275904	1341440	1406976
<b>Thread/process error</b>	1080320	1145856	1211392	1276928	1342464	1408000
<b>Task expire</b>	1081344	1146880	1212416	1277952	1343488	1409024
<b>HPDM task process crash</b>	1082368	1147904	1213440	1278976	1344512	1410048
<b>Other HPDM workflow error</b>	1083392	1148928	1214464	1280000	1345536	1411072
<b>Other API/sys call</b>	1084416	1149952	1215488	1281024	1346560	1412096

<b>error</b>						
--------------	--	--	--	--	--	--

Table 2. Error code matrix, part two

	<b>Windows PE</b>	<b>HPDM Gateway</b>	<b>HPDM Server</b>	<b>HPDM Console</b>	<b>Master Repository Controller</b>
<b>Network connection</b>	1458176	2113536	3162112	4210688	5259264
<b>Disk I/O</b>	1459200	2114560	3163136	4211712	5260288
<b>Memory error</b>	1460224	2115584	3164160	4212736	5261312
<b>Remote file/dir operation</b>	1461248	2116608	3165184	4213760	5262336
<b>File integrity</b>	1462272	2117632	3166208	4214784	5263360
<b>Credential</b>	1463296	2118656	3167232	4215808	5264384
<b>Other FTP-related error</b>	1464320	2119680	3168256	4216832	5265408
<b>Write Filter error</b>	1465344	2120704	3169280	4217856	5266432
<b>Unmanageable device</b>	1466368	2121728	3170304	4218880	5267456
<b>Unsupported task</b>	1467392	2122752	3171328	4219904	5268480
<b>Incompatible platform</b>	1468416	2123776	3172352	4220928	5269504
<b>Message syntax error</b>	1469440	2124800	3173376	4221952	5270528
<b>Message semantic error</b>	1470464	2125824	3174400	4222976	5271552
<b>Registry error</b>	1471488	2126848	3175424	4224000	5272576
<b>Command return non-zero</b>	1472512	2127872	3176448	4225024	5273600
<b>Thread/process error</b>	1473536	2128896	3177472	4226048	5274624
<b>Task expire</b>	1474560	2129920	3178496	4227072	5275648
<b>HPDM task process crash</b>	1475584	2130944	3179520	4228096	5276672
<b>Other HPDM workflow error</b>	1476608	2131968	3180544	4229120	5277696
<b>Other API/sys call error</b>	1477632	2132992	3181568	4230144	5278720

## Database Issues

The intent of this section is to give some background on the HPDM database and help customer to troubleshoot the database-related problems.

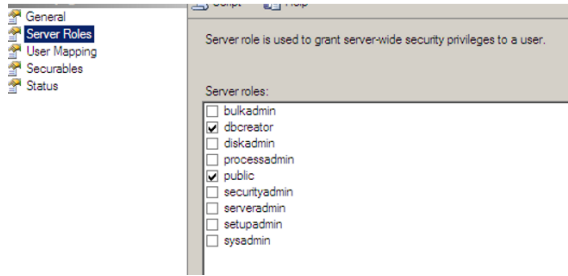
HPDM can be used with two types of database: Microsoft® (MS) SQL Server and PostgreSQL. To use MS SQL Server, you must install and configure it yourself. PostgreSQL is an open-source database that is bundled with the HPDM Server. You do not need to install or configure it yourself.

### Using MS SQL Server

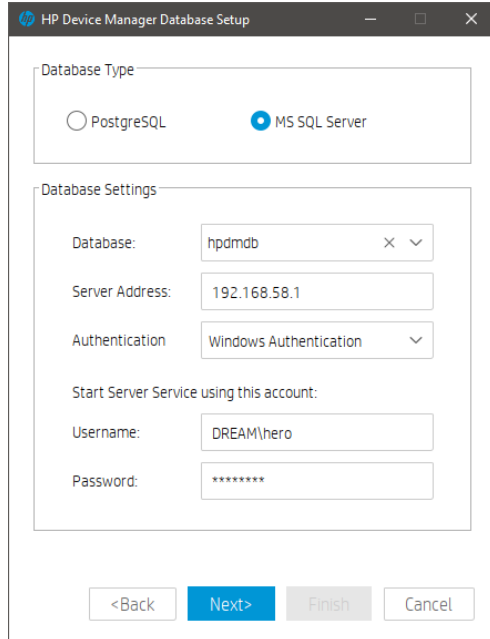
MS SQL Server can be used with one of two authentication types: SQL Server Authentication or Windows Authentication. Both authentication types are supported by HPDM. SQL Server Authentication has an inner security mechanism that is easy to use. Windows® Authentication needs the Windows operating system security mechanism.

To configure MS SQL Server using Windows Authentication:

1. Log on to a Windows domain account and assign it the minimum privilege **dbcreator** 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**.

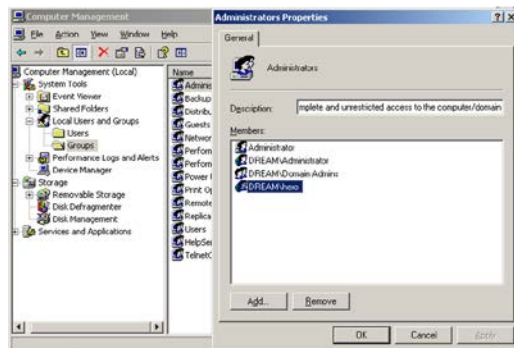


3. Under **Start Server Service using this account**, enter a Windows account username and password.

Note

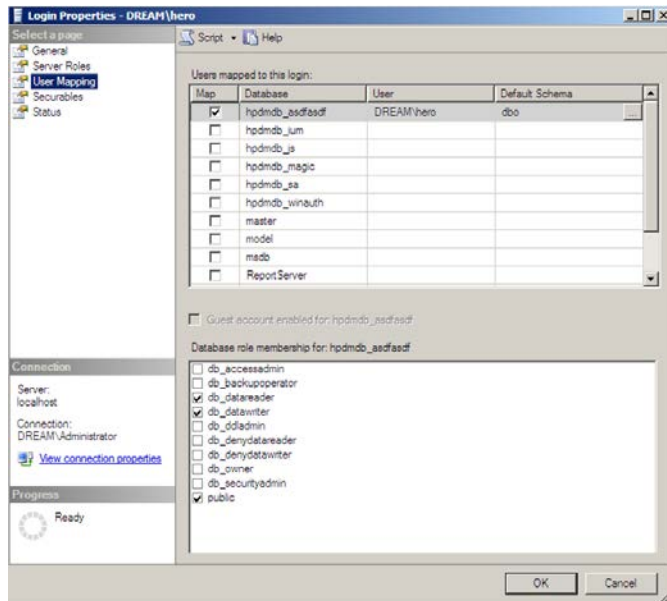
This account needs the following privileges:

- In the Windows operating system, it needs to be in the Administrators group.



- In MS SQL Server, it needs the minimum privileges **db\_datareader** and **db\_datawriter**.





## 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 template plugin 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 of this guide

### 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.

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

## Repositories

For repositories, the common problems are the HPDM Server cannot connect to HPDM Master Repository Controller and the device fails to connect the repository. Before troubleshooting, please make 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/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.

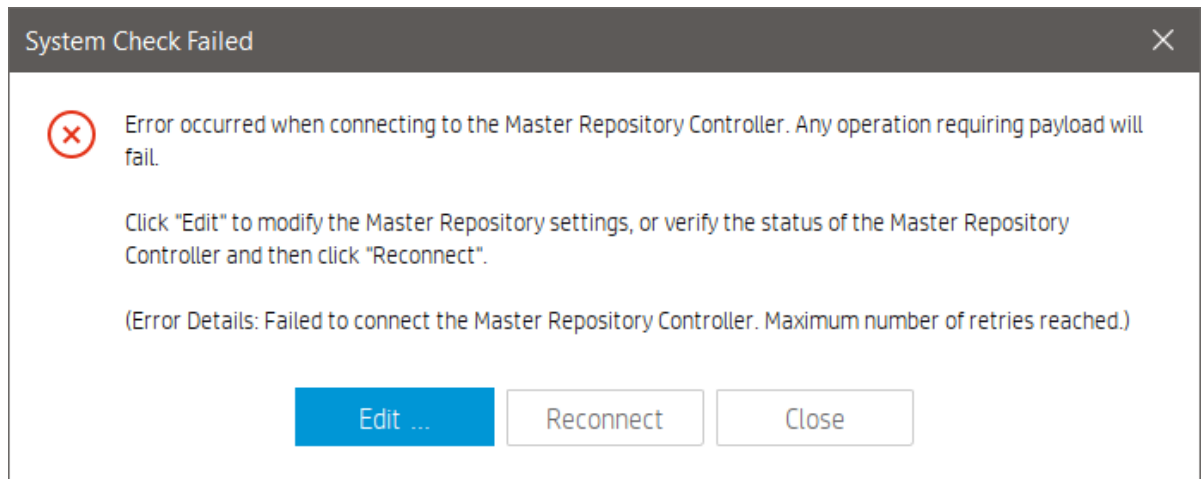
After changing the log level, restart the Master Repository Controller service for the changes to take effect.

### *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, click 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 click the **Reconnect** button in the error dialog.

Figure 10. System Check Failed dialog



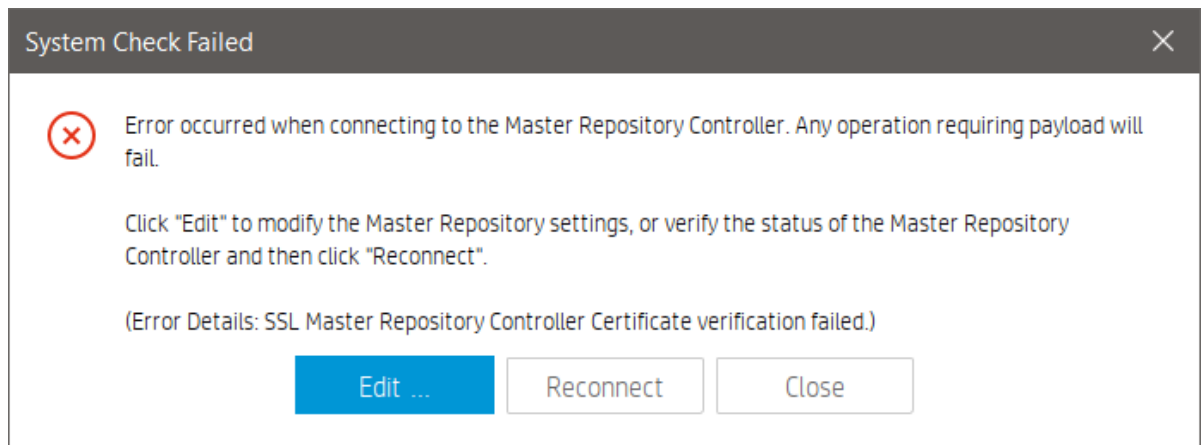
- Make sure that the connection passes the authentication.

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.

- 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.
- 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 will be 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.

### **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:

1. **Subnet-directed WOL**—The HPDM Gateway broadcasts the WOL packet to the subnet address of devices on port 7.
2. **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*

1. 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.
2. 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 Section: 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 XPe and WES 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. Then, change the settings to enable **Allow this device to wake the computer**, accept the changes. If EWF is enabled, right-click the EWF tray icon, select **Commit EWF (C)**, and then reboot. If UWF is enabled, select **Disable UWF** and reboot. Then, do the above changes, select **Enable UWF**, 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 has to 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 will not be able to wake it up either.

### *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 AABBCDDDEEFF 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>.

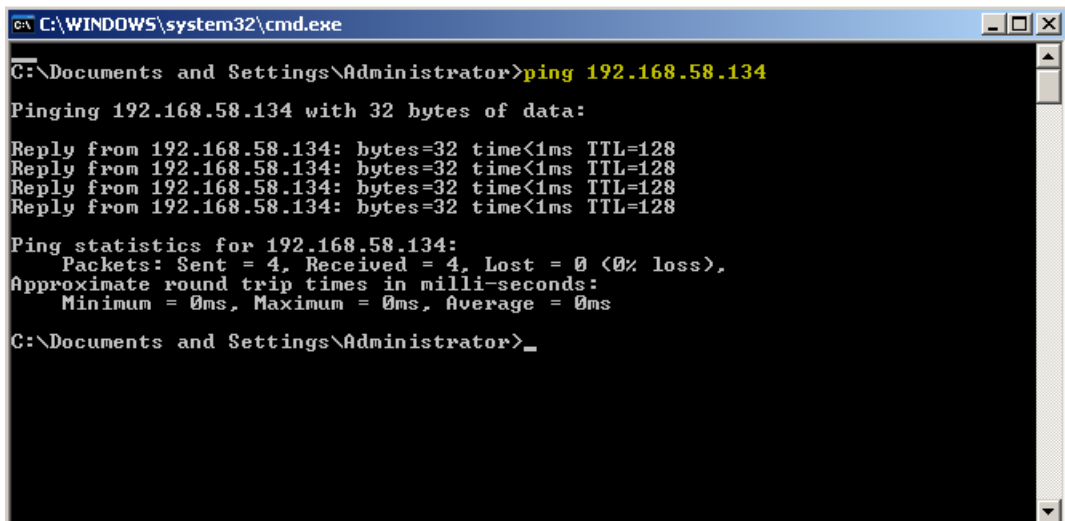
### **PXE-Based Imaging**

- Verify that the device supports imaging using PXE (see the HPDM release notes).
- Verify that all HPDM components are 4.7 SP6 or newer.
- Verify that the device is set to boot from PXE (see Section: 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

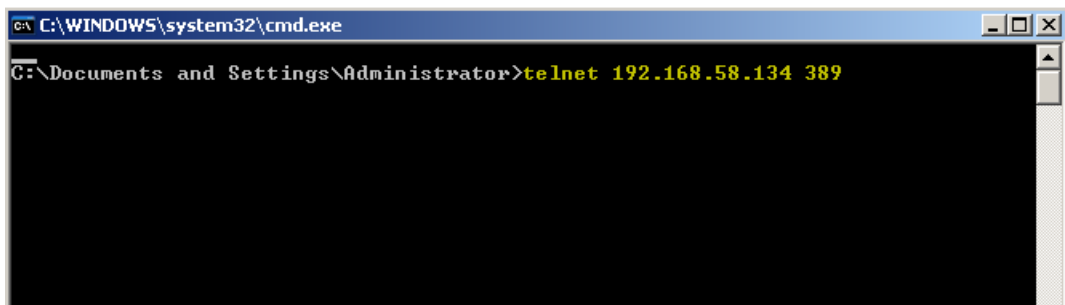
Most LDAP related issues stem from misconfiguration, use the items below to verify connectivity and configuration of the LDAP service within your environment.

- 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.



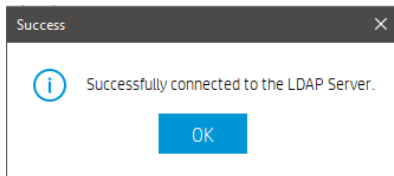
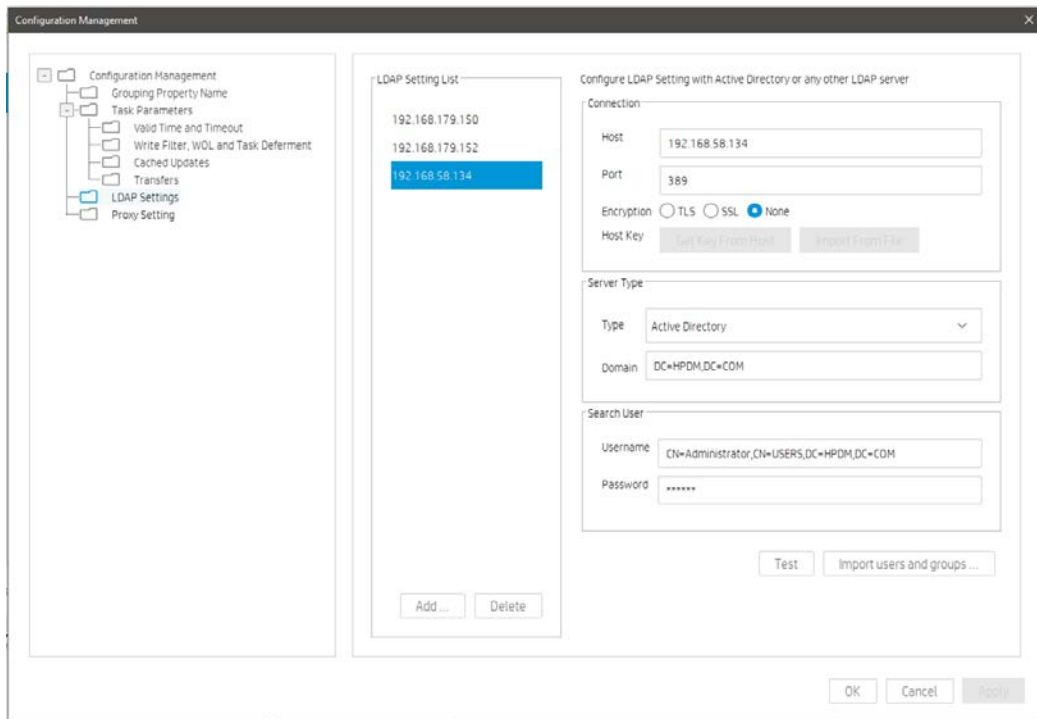
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 192.168.58.134
Pinging 192.168.58.134 with 32 bytes of data:
Reply from 192.168.58.134: bytes=32 time<1ms TTL=128
Reply from 192.168.58.134: bytes=32 time<1ms TTL=128
Reply from 192.168.58.134: bytes=32 time<1ms TTL=128
Reply 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.

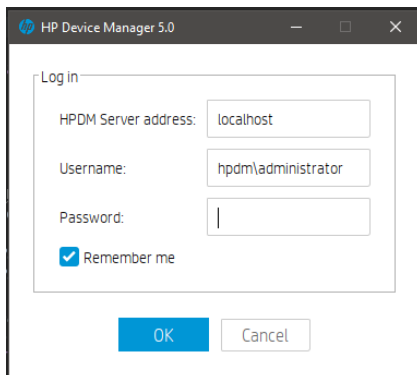


```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>telnet 192.168.58.134 389
```

- 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 clicking 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 username.
  - 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 will default 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, they must log in to the HPDM Console again for the new password to take effect.



## 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, and they 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

This is the devices table.

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
device_id	nvarchar	50	NO	√	<a href="#">dm_group_values.device_id</a> ; <a href="#">dm_inv_display.device_id</a> ; <a href="#">dm_inv_ewf.device_id</a> ; <a href="#">dm_inv_ex_property.device_id</a> ; <a href="#">dm_inv_hardware.device_id</a> ; <a href="#">dm_inv_max_hotfix.device_id</a> ; <a href="#">dm_inv_ms_hotfix.device_id</a> ; <a href="#">dm_inv_nic.device_id</a> ; <a href="#">dm_inv_partition.device_id</a> ; <a href="#">dm_inv_software.device_id</a> ; <a href="#">dm_inv_time.device_id</a> ;	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	32	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			

### dm\_hash\_extprop

This is device properties table.

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

This is the inventory display table.

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

This is the inventory write filter table.

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

This is the inventory hardware table.

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

This is the inventory Maxspeed hotfix table.

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**

This is the inventory MS hotfix table.

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**

This is the inventory network interface card table.

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**

This is the inventory partition table.

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**

This is the inventory software table.

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

This is the inventory time table.

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

This is the grouping values table, which 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.

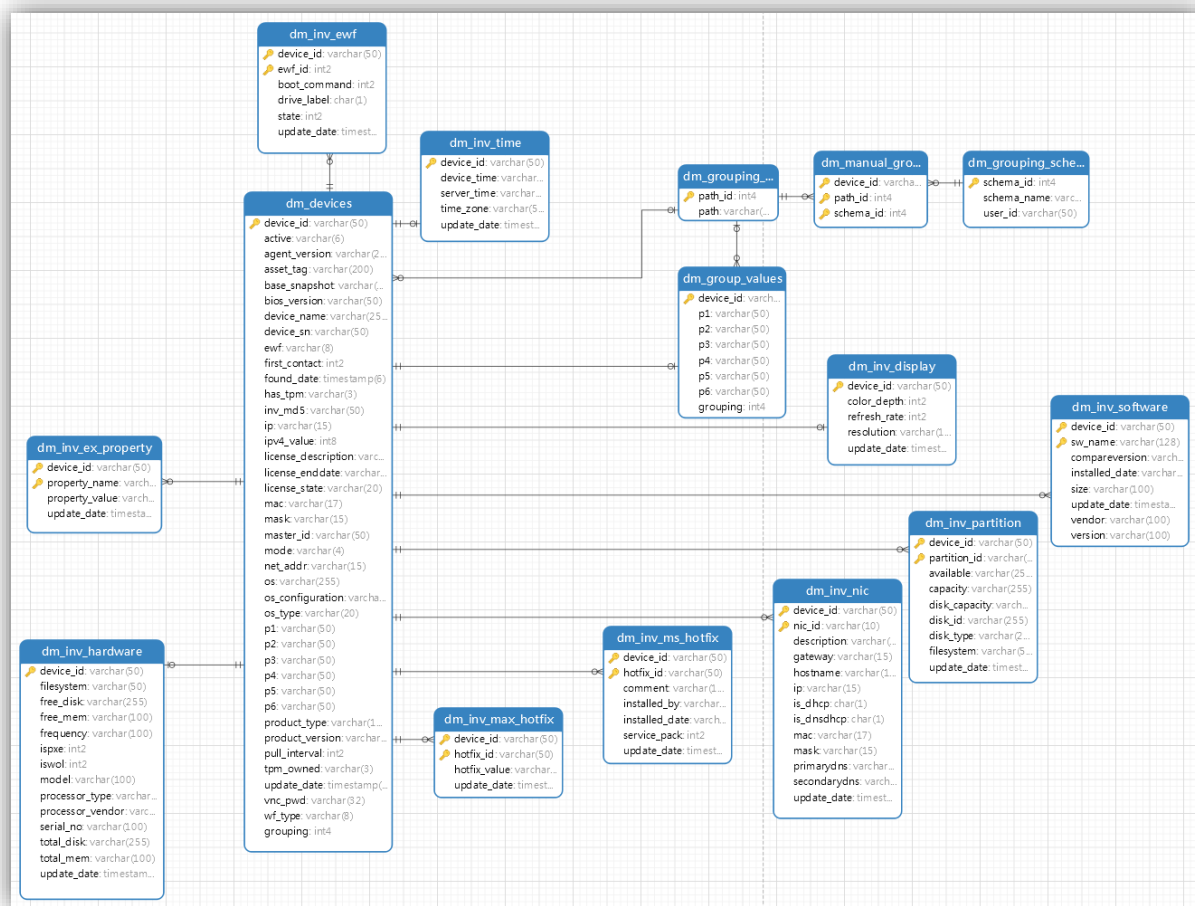
Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	
p1	nvarchar	50	YES		
p2	nvarchar	50	YES		
p3	nvarchar	50	YES		
p4	nvarchar	50	YES		
p5	nvarchar	50	YES		
p6	nvarchar	50	YES		
grouping	int	10	YES		

### dm\_inv\_ex\_property

This is the extended property table of a device.

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

This is the grouping attribute table. It is an inner table, used by the dynamic group, and 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

This is the dynamic grouping policy table.

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**

This is the dynamic grouping policy table for extended properties.

Column name	Type name	Column size	Nullable	Primary key	Description
Policy_id	nvarchar	50	NO	√	
Property_name	Nvarchar	50	NO	√	

**dm\_grouping\_path**

This is the grouping path information table.

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**

This is the manual grouping schema table.

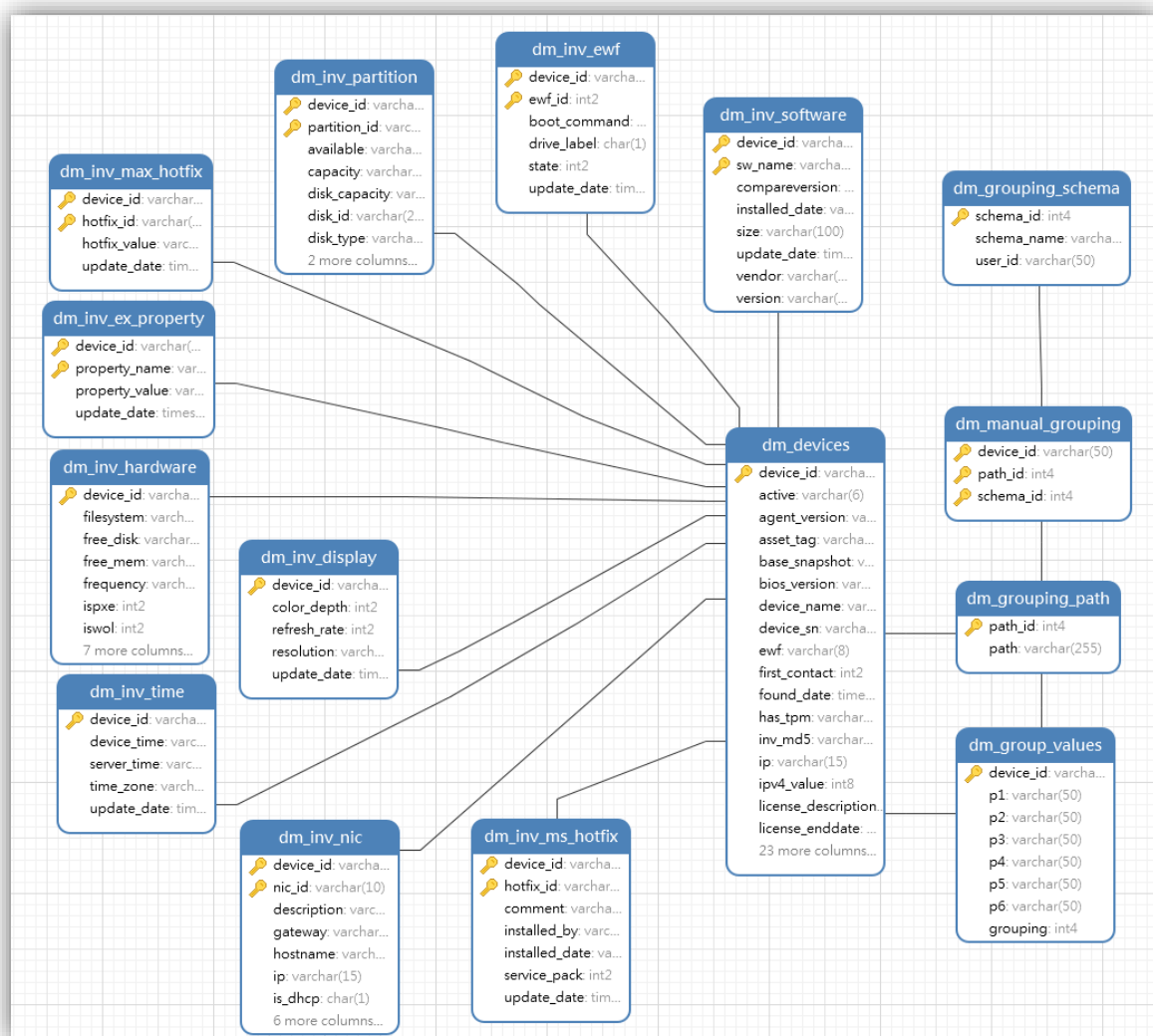
Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
schema_id	int	10	NO	√	dm_manual_grouping.schema_id	Manual schema ID
schema_name	nvarchar	50	NO			Manual schema name
user_id	nvarchar	50	NO			The creator's user ID

**dm\_manual\_grouping**

This is the manual grouping table, which 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

This is the rule table.

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

This is the schedule table.

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

This is the filter table.

Column name	Type name	Column size	Nullable	Primary key	Foreign key	Description
filter_id	nvarchar	40	NO	√	dm_filter_fields.field_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	Filed ID

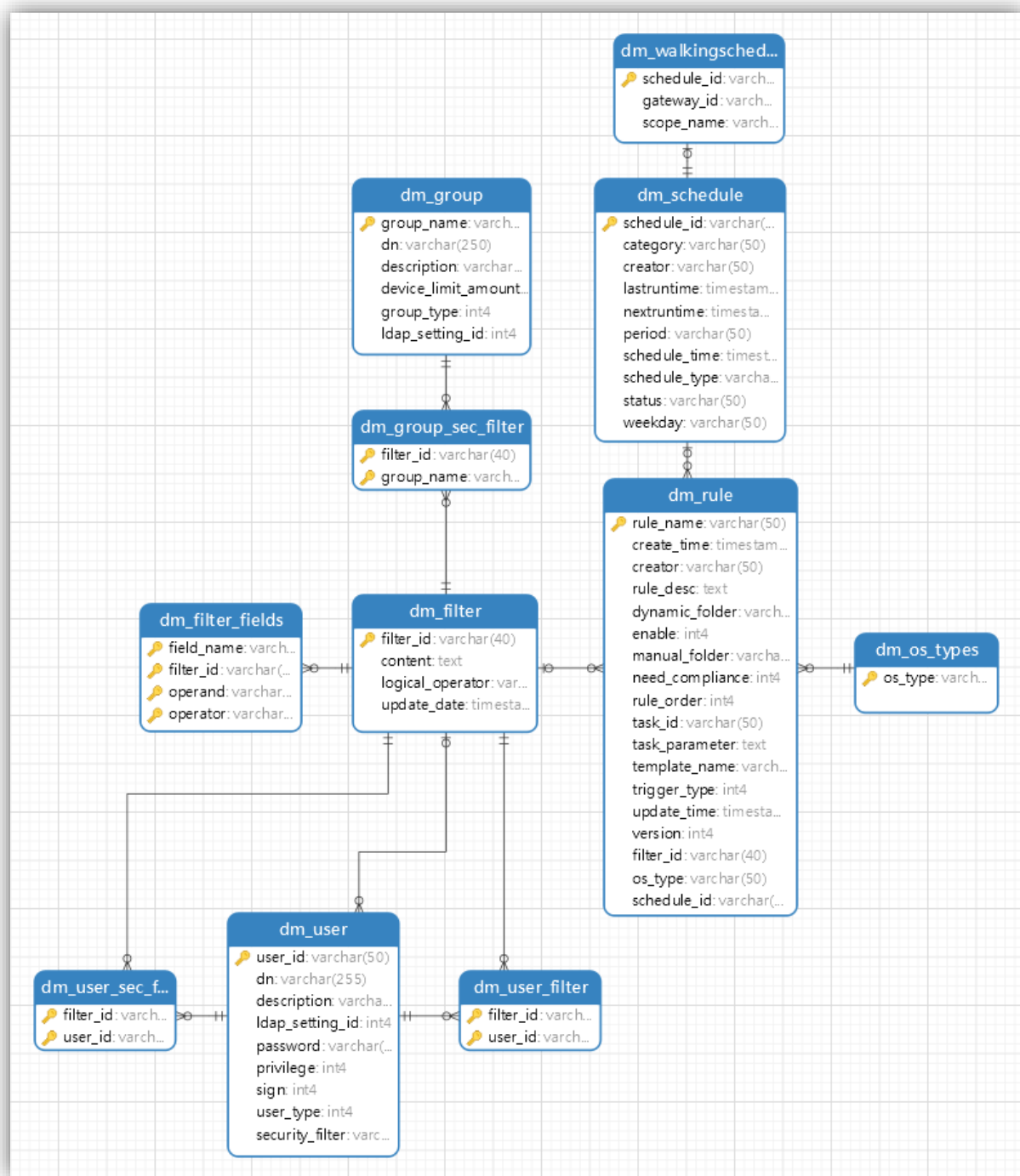
logical_operator	nvarchar	3	YES			It includes two types: and, or
update_date	datetime	23	NO			
Content	ntext		YES			Filter logic expression

### **dm\_filter\_fields**

This is the filter fields table.

<b>Column name</b>	<b>Type name</b>	<b>Column size</b>	<b>Nullable</b>	<b>Primary key</b>	<b>Description</b>
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"

## Rule and filter diagram



## Template Tables

### dm\_unit\_template

This is the unit template table, which 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

This is the basic template table.

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

This is the favorite template table.

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

This is the report template table, which 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

This is the template folder.

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

This is the task table, which 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 (1-60)
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

This is the subtasks table, which 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 dm_tasks.
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

This is the task template table, which 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

This is the task log table, which stores the task log information.

Column name	Type name	Column size	Nullable	Primary key	Description
device_id	nvarchar	50	NO	√	See device_id in dm_devices
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		MD5 value of error
-----------	----------	-----	-----	--	--------------------

### dm\_task\_error\_msg

This is the task error message table, which stores the task error message and its MD5 value.

Column name	Type name	Column size	Nullable	Primary key	Description
md5	nvarchar	32	NO	√	Md5
content	ntext		YES		Error message content

### dm\_device\_subtasks

This is the device subtasks table, which 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

This is the snapshot task table.

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

This is the snapshot task report table.

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

This is the gateway table.

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

This is the gateway walking scope table.

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

This is the gateway table.

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

This is the gateway walking task result table.

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

This is the repository table.

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

This is the repository protocols table.

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

This is the repository mapping table.

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

This is the group table.

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

This is the security filter table.

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

This is the user table.

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	50	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			

### dm\_user\_sec\_filter

This is the user security filter table.

Column name	Type name	Column size	Nullable	Primary key	Description
filter_id	nvarchar	32	NO	√	
user_id	nvarchar	50	NO	√	

### dm\_group\_user

This is the group and user table.

Column name	Type name	Column size	Nullable	Primary key	Description
group_name	nvarchar	50	NO	√	
user_id	nvarchar	50	NO	√	

### dm\_auth\_group

This is the authority in group table.

Column name	Type name	Column size	Nullable	Primary key	Description
group_name	nvarchar	255	NO	√	
auth_id	int		NO		

### dm\_template\_privilege

This is the template privilege table.

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

This is the key table.

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		

### dm\_keylog

This is the key log table.

Column name	Type name	Column size	Nullable	Primary key	Description
logdescription	nvarchar	200	NO	√	
logevent	smallint	5	NO	√	
logtime	datetime	23	NO	√	

### dm\_keyzero

This is the keyzero table. This table is an HPDM internal table. It is created when the database is installed, and 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		

## Configuration Tables

### dm\_conf

This is the configuration table.

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

This is the database version table.

Column name	Type name	Column size	Nullable	Primary key	Description
version	nvarchar	50	NO	√	Version value

### dm\_ipscope

This is the IP scope table.

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

This is the operating system type table. This 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

This is the LDAP setting table. This 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

This is the audit log table.

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 will generate 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.

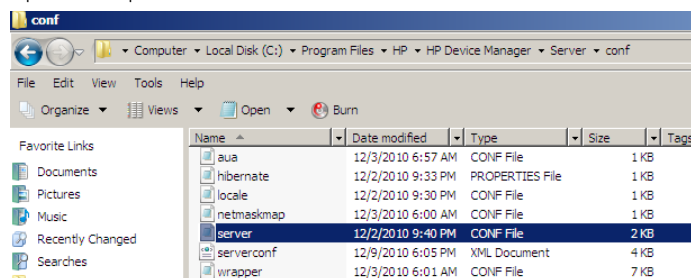
## Appendix B: Additional Configuration Options

### Configuring HPDM Server

This section explains each parameter in HPDM Server configuration file.

#### Accessing the Server configuration file

- Open File Explorer and find the installation folder for HPDM.



- Right-click the file `server.conf`, select **Open With**, and then select **Notepad**.

Now, you have a Notepad file displaying the content of `server.conf`, and you can modify some of the parameters in it.

#### Thread settings

HPDM Server creates a thread pool to contain all services.

Parameter	Description
<code>hpdm.thread.poolSize=400</code>	This parameter indicates the maximum amount of thread used by HPDM Server. The default value is 400.
<code>hpdm.thread.maxNum.task=100</code>	This parameter indicates the maximum amount of thread for tasks.
<code>hpdm.thread.maxNum.report=200</code>	This parameter indicates the maximum amount of thread for processing reports.
<code>hpdm.thread.maxNum.gatewayWalker=20</code>	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> .

### 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: <code>DEBUG</code> = 1: Logs for developer debugging. <code>INFO</code> = 2: Logs of running information, not errors. <code>WARN</code> = 3: Logs with warning if something unexpected happened. <code>FATAL</code> = 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.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.

### 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

## 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="300" report_session_timeout="5"/>
<GatewayScale>large</GatewayScale>
<AgentPoll batch="50" poll_interval="0"/>
<GatewayID>3C:A8:2A:DF:28:D9</GatewayID>
<NIC></NIC>
<Timeout network_timeout="30"/>
<LogLevel>TRACE</LogLevel>
<LogInterval log_interval=""/>
<PXEShutdown>no</PXEShutdown>
<ServiceForceStart>yes</ServiceForceStart>
<UseExcptStorage>0</UseExcptStorage>
<SupportTeradici>no</SupportTeradici>
<JudgeAgentMode>yes</JudgeAgentMode>
<BroadcastPort>40000</BroadcastPort>
<Discover batch="1024" timeout="15"/>
<SslLegacySupport>no</SslLegacySupport>
</ConfigFile>
```

It is an XML file.

1. <Server> is the parameters for HPDM Gateway communicates with HPDM Server.
  - a. address is the HPDM Server address. You can set it from HPDM Configuration Center.
  - b. encrypt\_connection is if the communication is encrypted by TLS. Usually do not change it.
  - c. report\_delay is deprecated. Keep it for compatibility.
  - d. 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.
  - e. retry\_interval is the retry interval (in seconds) when HPDM Gateways fails to connect to HPDM Server. Usually do not change it.
  - f. 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 the communication for send reports, it will continuously send reports. When there is no report to send, Gateway will not close the communication until it meets the timeout. Usually do not change it.
2. <GatewayScale> is deprecated. Now HPDM Gateway can support any scale intelligently.
3. <AgentPoll> the Poll mechisum: 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 **Optimziing 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. Please do not change it manually. You can set it from **HPDM Configuration Center – HPDM Gateway** page.

6. <Timeout> is the timeout of Gateway connections. Usually 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. <PXEShutdown> 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 will start HPDM PXE Service when it receive 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. Please do not change it.
15. <Discover> is the parameters for discovering HPDM Agents. Usually do not change it.
  - a. batch is the set size of discovery.
  - b. 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**”. You should enable it to support ThinPro5 Agents or some old Agents.

## Configuring HPDM Agent

### Configuring HP WES clients

8. Log on to the device as Administrator.
9. Open the Control Panel and double-click **HPDM Agent**. The Configure HP Device Management Agent dialog box appears.



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.

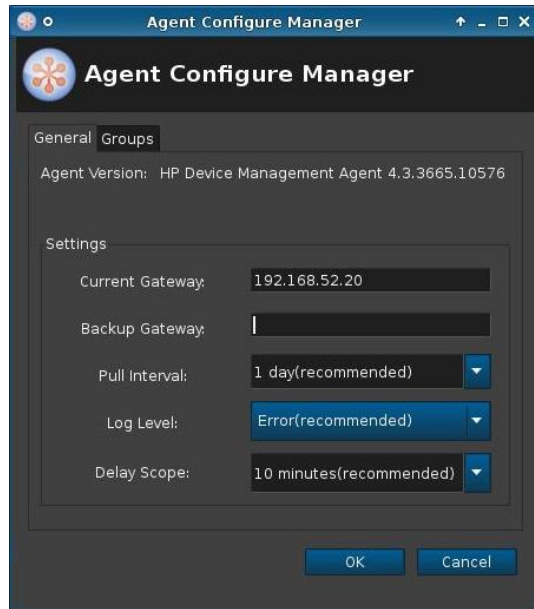


There are two options in the Groups tab. Select **Get Pre-Assign Groups from DHCP Tag** to make HPDM Agent report with grouping values to get from the DHCP server. Select **Use Static Custom Groups** to set custom grouping values manually.

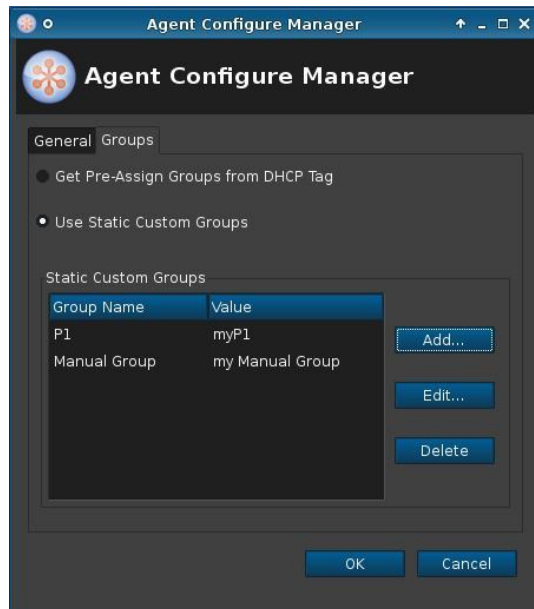
To set the grouping values manually, select **Use Static Custom Groups**, and then click **Add**. Enter the grouping value in the dialog that opens. You can choose the **Group Name** from a drop-down list and enter a value for it.

## Configuring HP ThinPro clients

10. Log on to the device as Administrator.
11. Open the **Control Panel**, select the **Management** tab, and double-click **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 click **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 4.7 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.
- **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`

Items:

- A. Most of them can be found in the Agent configuration GUI:
  - 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
- B. There are several advanced options are not listed on Agent configuration GUI:
  - 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: It 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.

## Appendix C: Configuring DHCP tags

### Configuring a DHCP server for use with PXE

#### Configuring a DHCP server with the HPDM Server installed on a different machine

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:

12. Make sure that the DHCP server has not been previously configured for a PXE bootstrap.
13. 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 be used with PXE.

#### Configuring a DHCP server with the HPDM Server installed on the same machine

If the HPDM Server is installed with a DHCP server on the same machine, it requires some manual configuration. The HPDM Server installation process installs the HP PXE service, which provides the PXE remote-imaging function. The service automatically starts and stops with the operating system. The DHCP server is used by the PXE boot ROM to get an IP address, as well as other basic networking information such as a subnet mask or a default gateway.

These instructions assume the following:

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

By default, options 60 and 201 are not set in Windows 2000. Add these options to tell PXE clients where to find the HPDM Server.

To configure the DHCP server:

14. If DHCP option 43 is set, remove it because the HPDM Server is installed on the same machine as the DHCP server.
15. Add option 60, and set the value to **PXEClient**. If option 60 does not exist, use the following procedure.
  - A. Select **Start > Run**.
  - B. Type `cmd` in the box. A Command shell appears.
  - C. Type `netsh`, and then press the **Enter** key.
  - D. Type `dhcp`, and then press **Enter**.
  - E. 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.
  - F. Type `add optiondef 60 <custom_option_name> STRING 0`, and then press **Enter**.
  - G. Type `set optionvalue 60 STRING "PXEClient"`, and then press **Enter**.
  - H. To confirm that the settings are correct, type `show optionvalue all`, and then press **Enter**.
16. Add option 201 using the following procedure.
  - A. Type `add optiondef 201 <custom_option_name> STRING 0`, and then press **Enter**.
  - B. Type `set optionvalue 201 STRING '<HPDM_Gateway_IP >' '40003'`, and then press **Enter**.

---

**Note**

Replace the items in brackets with the appropriate value.

When setting optionvalue 201, the syntax must be written exactly as shown, including the single quotes and single space, otherwise errors will occur. See the following example:

```
'192.168.1.1' '40003'
```

---

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

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

**Configuring a DHCP server on Linux**

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

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

18. Restart **dhcpd** to use the new configuration.

**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:

19. Select **Start > Run**.
20. Type `cmd` in the box. A command shell appears.
21. Type `netsh`, and then press **Enter**.
22. Type `dhcp`, and then press **Enter**.
23. 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.
24. Type `add optiondef 202 <custom_option_name> STRING 0`, and then press **Enter**.
25. Type `set optionvalue 202 STRING <HPDM_Server_IP> <HPDM_Gateway_IP>`, and then press **Enter**.
26. 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 of the 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:

27. Follow the 1 – 5 steps of “Configuration option 202 and 203”.
28. Type `add optiondef <option_code> <custom_option_name> STRING 0`, and then press **Enter**.
29. Type `scope <scope-ip-address>`, and then press **Enter**.
30. Type `set optionvalue <option_code> STRING <option_value>`, and then press **Enter**.
- 

For example: set option 202 under the scope 192.168.1.0.

31. `netsh dhcp server> add optiondef 202 HPDM_SERVER_GATEWAY`
32. `netsh dhcp server> scope 192.168.1.0`
33. `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

34. Turn on or restart the device.
35. Press **F10** during startup to access the BIOS settings.
36. Locate the boot order settings, and set the PXE network controller as the first legacy boot source.

### Changing the boot order remotely

#### Windows

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

37. Download the HP BIOS Configuration Utility (BCU) from [https://ftp.hp.com/pub/caps-softpag/cmit/HP\\_BCU.html](https://ftp.hp.com/pub/caps-softpag/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:

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

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"

Capture Files (to capture the file from **c:\temp\t520\_BiosConfig.txt** to the master repository)

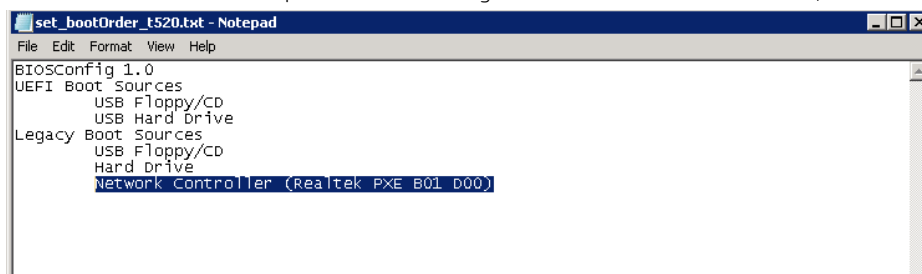
Send the File and Registry task to the target device.

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

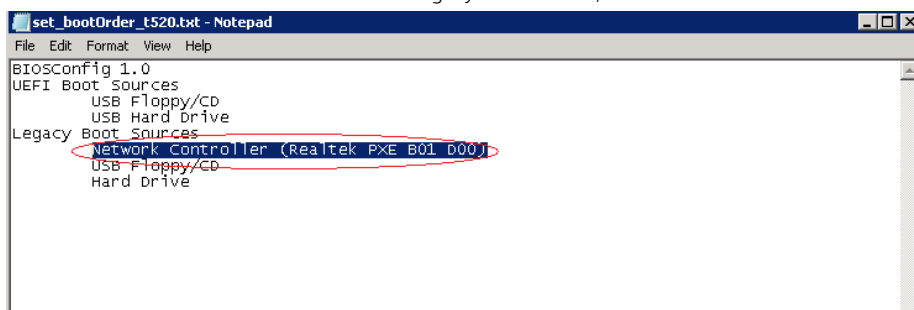
Create a copy of t520\_BiosConfig.txt, and then rename the new file to **set\_bootOrder\_t520.txt**.

Open set\_bootOrder\_t520.txt in Notepad.

Delete all of the file contents except for the file heading and the two boot source sections, like in the following image.



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:

Deploy Files (to deploy **BiosConfigUtility64.exe** and **set\_bootOrder\_t520.txt** to the device)

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

See the following table for an example script.

Field	User input
Start in	c:\temp
Content	cd c:\temp BiosConfigUtility64.exe /set "c:\temp\set_bootOrder_t520.txt"

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 6 (64-bit).

#### 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.

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

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
```

Capture Files (to capture the file from **/tmp/t630\_BiosConfig.txt** to the master repository)

Send the File and Registry task to the target device.

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

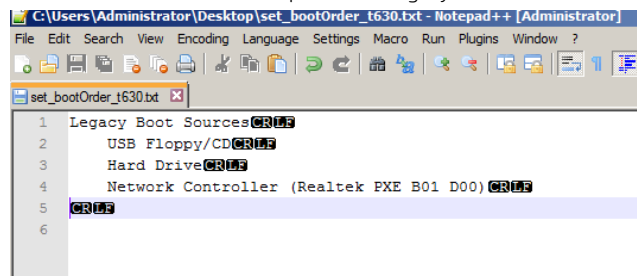
Create a copy of t630\_BiosConfig.txt, and then rename the new file to **set\_bootOrder\_t630.txt**.

Open set\_bootOrder\_t630.txt in Notepad++

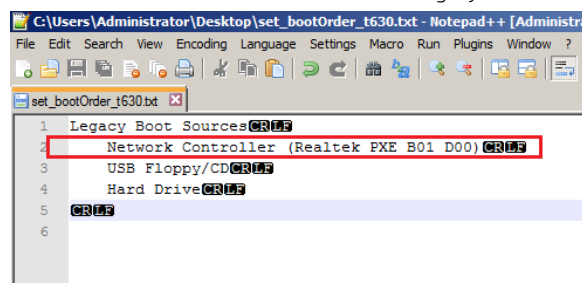
Select **Edit > EOL Conversion**, and then select the item for **Windows** (the name depends on your version of Notepad++).

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

Delete all of the file contents except for the Legacy Boot Source section, like in the following image.



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:

Deploy Files (to deploy **set\_bootOrder\_t630.txt** to the device)

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
```

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.

---

Send a Reboot Device task to reboot the target device

For example:

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

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.

---

Send a Reboot Device task to reboot the target devices

**Sign up for updates**  
[hp.com/go/getupdated](https://hp.com/go/getupdated)

---

© Copyright 2019 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.

First Edition: May 2019

Document Part Number: L70795-001

