

# HP Device Manager 4.7

## Privilege Management System



## Table of contents

Overview.....	2
Privilege management system .....	2
System-level privilege .....	2
Template-level privilege .....	3
HPDM behavior under privilege management system.....	5
Security filter.....	7
Privilege-related operations.....	7
Examples.....	10
Example 1 .....	10
Example 2 .....	10
Example 3 .....	10
For more information .....	11

## Overview

The purpose of this document is to explain the privilege management system in HP Device Manager (HPDM) 4.7. HPDM 4.7 has a more detailed system for privilege classification. HPDM provides not only traditional role-based privilege, but also provides template-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.

## Privilege management system

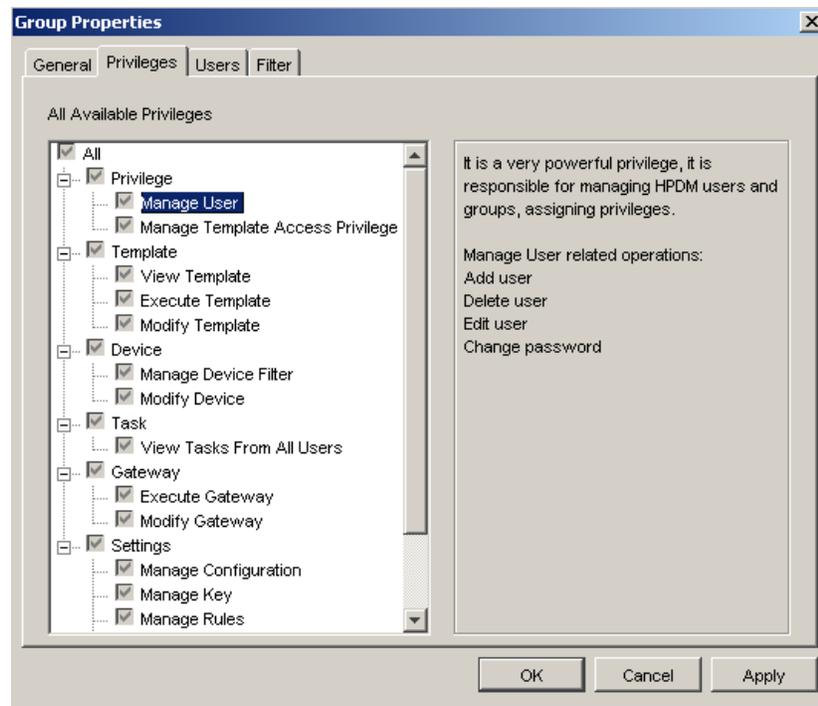
### System-level privilege

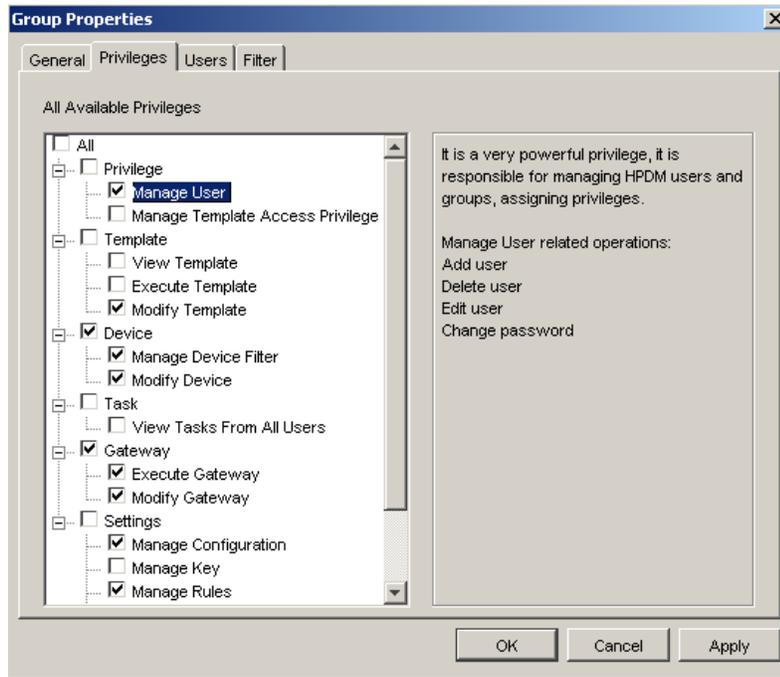
System-level privilege, or role-based privilege, has been available in previous HPDM versions. It assigns privileges to a group, and then users within the group inherit those privileges.

To see the privileges user interface:

1. In the HPDM Console, select **Tools > User Management**.
2. On the **Groups** tab, select a group.
3. In the group properties dialog, select the **Privileges** tab.

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**

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



This is different for the template View operation. If you do not have the **View** privilege, the template will not display on the HPDM Console.

**Template-level privilege**

Template-level privilege controls each user group's access to the View, Modify, and Execute operations for each template.

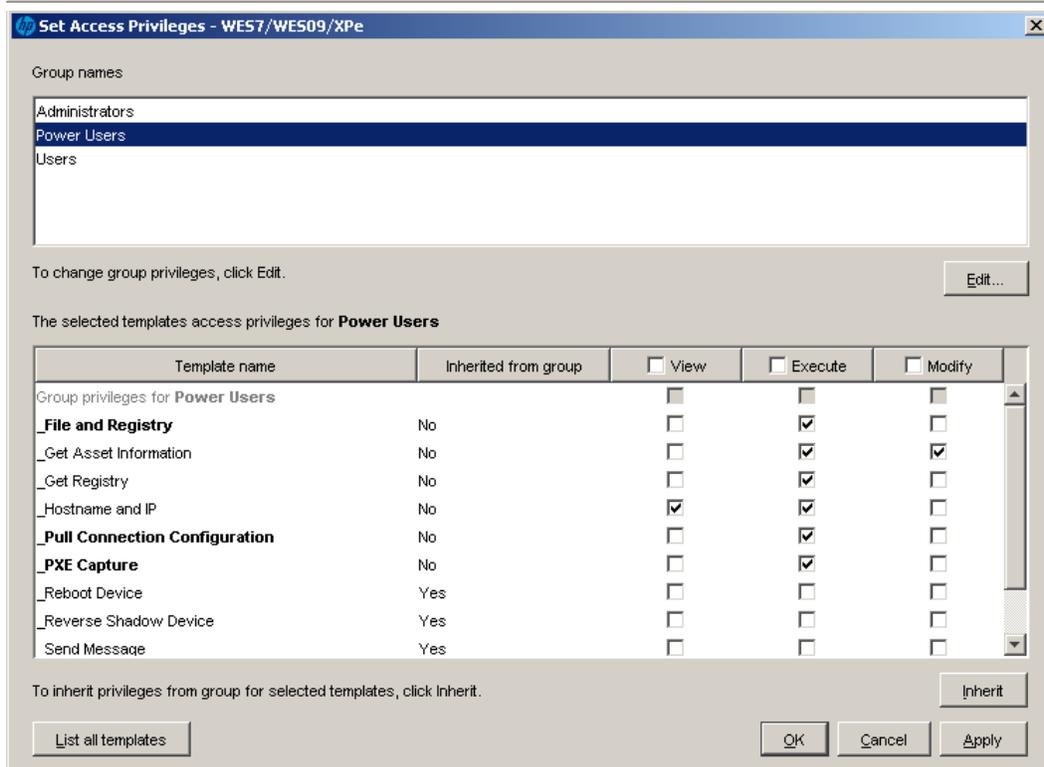
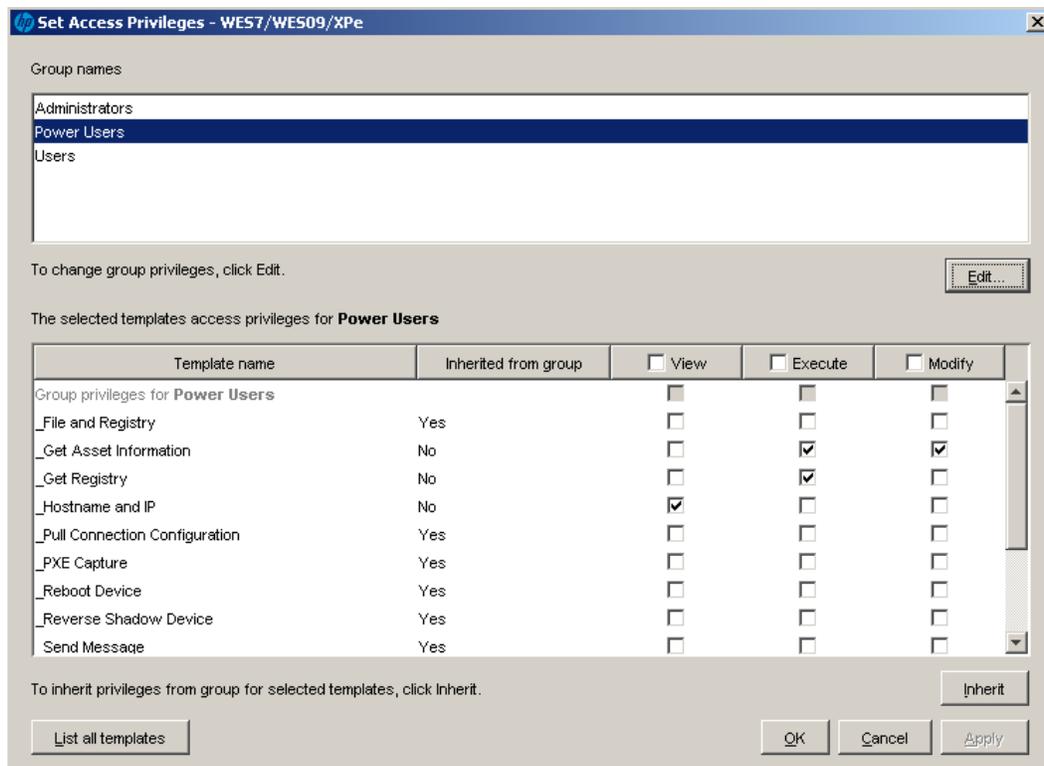
To configure template-level privileges:

1. In the HPDM Console, select **Template > Set Access Privileges**.  
– or –  
Right-click a template and select **Set Access Privileges**.
2. If necessary, to configure the default privileges, select a group, and then select **Edit** to change the group's system-level privileges.
3. To see all current templates, select **List all templates**.
4. If you can give a group privilege to access a template's operations, the value under **Inherited from group** is **Yes**. To enable a group to inherit privileges to templates, select **View**, **Execute**, and/or **Modify** next to the templates' names and then select **Inherit**.

**Note**

The group inherits privileges to the selected operations only.

- Verify that the template privilege has changed. If the template privilege has been changed, the template name appears bold.



## 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

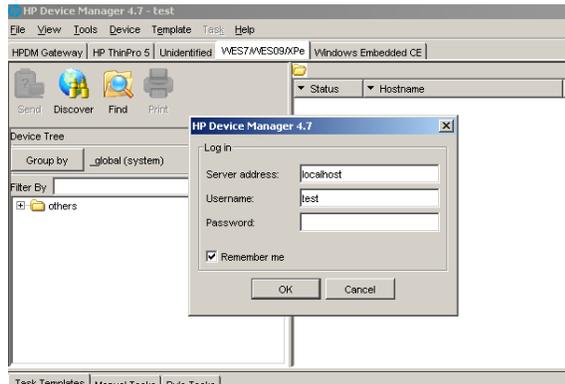
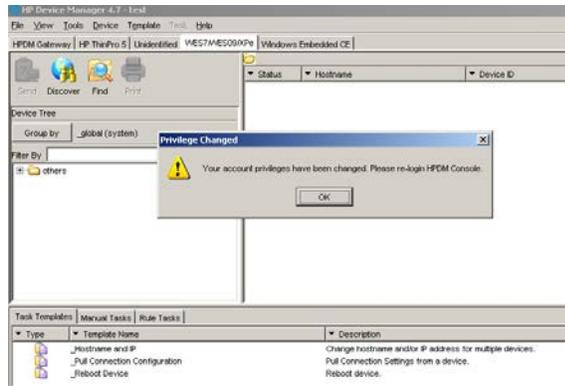
In HPDM, there is a default super user created during the HPDM installation process. By default, the user name is root. You can change the password, but cannot delete user. It belongs to the Administrators group and cannot be modified.

---

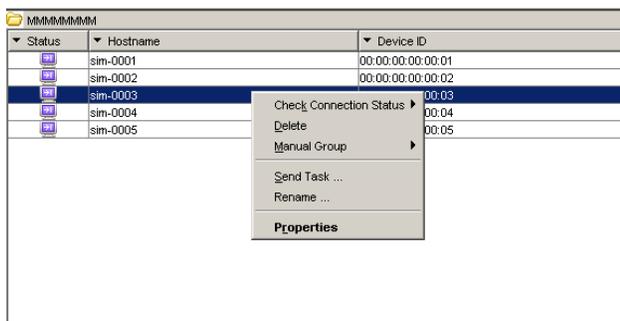
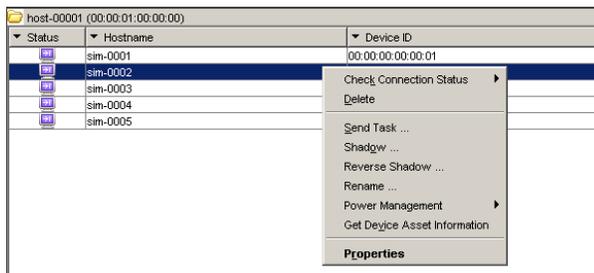
HPDM privileges use the following rules:

- 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 privilege. If a user does not have this privilege for a template, the template is not displayed in the user interface.
- 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 “save as” 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 template 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 do not appear in the HPDM Console.
  - For other privileges the user might not have, if the user tries to access or modify that privilege, the HPDM Server sends a message to the HPDM Console that the action is not allowed.

- If the privileges of a specified group change, the users in the group are logged out from any live sessions to the HPDM Server. The users must log in to HPDM again.



- In the HPDM Console device view, there are some context menu items for sending tasks. If the user does not have that template View privilege, the items do not appear in the HPDM Console.



## 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	Subcategory	Atom privilege	Comment	Power Users	Users
Privilege	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					
Template Access Privileges management		Set privileges for single or multiple templates		X	X	

Category	Subcategory	Atom privilege	Comment	Power Users	Users
<b>Template</b>	View	View	Make template visible or not	√	√
	Execute	Send task		√	√
		Resend task			
		Configure template in rule			
	Modify	Sava as template	If no modify privilege, the template will not be editable.	√	X
		Import template			
		Delete template			
		Update template			
Rename template					
Merge templates					

Category	Subcategory	Atom privilege	Comment	Power Users	Users
<b>Device</b>	Modify Device	Add device		√	X
		Delete device			
	Manage Device Filter	Manage Device Filter	Add device filter Delete device filter Edit device filter	√	X

Category	Subcategory	Atom privilege	Comment	Power Users	Users
<b>Tasks</b>	View task from all users	View task from all users		X	X

Category	Subcategory	Atom privilege	Comment	Power Users	Users
<b>Gateway</b>	Execute Gateway	Discover device		√	X
		Discover Gateway			
	Modify Gateway	Configure Gateway		√	X
		Update Gateway			
		Delete Gateway			

Category	Subcategory	Atom privilege	Comment	Power Users	Users
<b>Settings</b>	(The same as atom privilege)	Configuration management	Set configuration parameters	√	X
		Repository management	Add repository Import repository Remove repository Edit repository View repository Mapping Sync	√	X
		Key management	Update current key Import key Clear key log	×	X
		HPDM Gateway access control	Acknowledge Ban Manually control device management access	√	X
		Rules management	Add rule Edit rule Delete rule Order rule View rule	√	X
		Status walker	Add status walker Edit status walker Delete status walker	√	X
		Status snapshot	Add status snapshot Edit status snapshot Delete status snapshot	√	X
		Report management	Add report Edit report Delete report Preview report Export report	√	X

---

**Note**

Every privilege is independent and does not influence other privileges.

---

## Examples

### 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.

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`.

### Example 3

There are two user groups.

- Group1 has the `_Update Agent` privilege only.
- Group2 has the `_Get Asset Info` privilege only.

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.

## For more information

To read more about HP Device Manager, go to [hp.com/go/hpdm](http://hp.com/go/hpdm).

### Sign up for updates

[hp.com/go/getupdated](http://hp.com/go/getupdated)

---

© Copyright 2015 HP Development Company, L.P.

ARM is a registered trademark of ARM Limited. Java is a registered trademark of Oracle and/or its affiliates. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Pentium is a trademark of Intel Corporation in the U.S. and other countries.

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: October 2015

