

# **Dell EMC OpenManage Power Center 4.1**

## User's Guide

## Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

<b>Chapter 1: Overview.....</b>	<b>8</b>
Key features.....	8
New in this release.....	9
Topology.....	9
System requirements.....	10
Hardware and software requirements for the server system.....	10
Hardware and software requirements for devices.....	11
<b>Chapter 2: Getting started.....</b>	<b>12</b>
Management console introduction.....	12
Home page.....	14
Common use cases.....	16
Supported and unsupported devices.....	16
<b>Chapter 3: Using OpenManage Power Center.....</b>	<b>20</b>
Preinstallation requirement for OpenManage Power Center.....	20
Using Power Center on Microsoft Windows operating systems.....	20
Installing OpenManage Power Center on Microsoft Windows Server.....	20
Installed directories in Windows.....	21
OpenManage Power Center services on Microsoft Windows operating systems.....	22
Upgrading Power Center on Microsoft Windows operating systems.....	22
Uninstalling OpenManage Power Center on Microsoft Windows operating system.....	23
Launching OpenManage Power Center on Microsoft Windows operating systems.....	23
Configuring Enhanced Security Configuration for Internet Explorer.....	23
Using OpenManage Power Center on Linux operating systems.....	24
Installing Power Center on a Linux server.....	24
Installed directories in Linux.....	25
Power Center services in Linux.....	25
Uninstalling Power Center in Linux.....	26
Launching Power Center in Linux.....	26
<b>Chapter 4: Using OpenManage Power Center through Command Line Interface .....</b>	<b>27</b>
Command Line Interface error handling.....	27
Command Line Interface commands.....	28
Command line interface error codes.....	37
<b>Chapter 5: Access control.....</b>	<b>38</b>
About authentication.....	38
Logging in.....	38
Logging in with a user name and password.....	38
Logging in with Single Sign-on (SSO).....	39
Multiple domain environment.....	40
Windows NT LAN Manager (NTLM) authentication limitation.....	41
Logging out.....	41

Managing user roles and privileges.....	42
Adding a custom role.....	42
Editing a role.....	42
Deleting a role.....	42
Privileges.....	43
Managing user accounts.....	45
Adding a user account.....	45
Adding a group account.....	46
Editing a user or group account.....	47
Deleting a user or group account.....	47
Changing a user account password.....	47
Viewing current user information.....	47
<b>Chapter 6: Task management.....</b>	<b>48</b>
Discovery tasks.....	48
Creating discovery tasks.....	49
Re-running recent discovery tasks.....	49
Power control tasks.....	50
Creating power tasks.....	50
Protocol profile.....	50
Redfish protocol support.....	51
Adding a protocol.....	52
Editing a protocol.....	53
Deleting a protocol.....	53
<b>Chapter 7: Device Management.....</b>	<b>54</b>
Adding a new device.....	54
Adding an existing group.....	55
Adding a device from the network.....	55
Viewing resource utilization history.....	55
Filtering devices.....	55
Editing a device.....	57
Deleting devices using a filter.....	57
Sorting devices.....	57
Updating Device location.....	58
Chained PDU Support.....	58
Viewing chained PDUs.....	58
Managing groups.....	59
Mapping Group Structure Information.....	59
Creating a new group.....	59
Moving device groups or devices.....	60
Viewing devices in a chassis.....	60
Managing Racks.....	60
Deleting a group.....	62
Emergency Power Reduction.....	63
<b>Chapter 8: Virtual machines.....</b>	<b>64</b>
Filtering virtual machines.....	64
Creating a new virtual machine group.....	65

Adding a virtual machine to an existing group.....	65
Moving a virtual machine group.....	65
Viewing a virtual machine power history graph.....	66
Viewing a virtual machine power distribution graph.....	66
Deleting a VM group.....	66
<b>Chapter 9: Power Monitoring.....</b>	<b>67</b>
Power monitoring levels.....	67
Power thresholds.....	67
Viewing power details.....	68
Viewing Energy Consumption.....	69
Viewing a power history graph.....	69
Viewing system airflow graph.....	70
Monitoring PDU.....	70
Monitoring UPS Power.....	70
<b>Chapter 10: Temperature Monitoring.....</b>	<b>71</b>
Temperature Monitoring Level.....	71
Viewing Temperature Details.....	71
Viewing a temperature history graph.....	72
Monitoring the Temperature of the Chassis/Blade Server.....	73
Applying circuit breaker limits to chassis.....	73
Monitoring the Temperature of Devices/Groups.....	73
<b>Chapter 11: Policies.....</b>	<b>74</b>
Dynamic power caps.....	74
Power Policy Capabilities.....	75
Upgrading Device Power Policy Capability.....	76
Creating a policy.....	76
Policy Priority Levels.....	77
Policy Modes.....	77
Enabling or disabling a policy.....	78
Viewing policies in the power details graph.....	78
Editing a policy.....	78
Deleting a policy.....	78
Filtering policies.....	78
<b>Chapter 12: Analysis.....</b>	<b>80</b>
Server characteristics.....	80
Viewing server power characteristics graph.....	80
Viewing peak power distribution graph.....	80
Viewing active idle power distribution graph.....	81
Exporting server power report .....	81
Underutilized servers.....	81
Configuring underutilized servers settings.....	81
Power Analysis.....	82
Analyzing capacity expansion.....	82
Viewing placement suggestions.....	82
Viewing resource suggestions.....	83

Cooling Analysis.....	83
Configuring cooling analysis settings.....	83
Viewing a hot spot room.....	83
Viewing an over cooled room.....	84
Viewing devices under large temperature span room.....	84
Viewing devices under hot outlier room.....	84
<b>Chapter 13: Managing reports.....</b>	<b>85</b>
Viewing Report Details.....	86
Creating reports.....	86
Editing reports.....	88
Deleting reports.....	88
Adding report groups.....	88
Editing report groups.....	88
Deleting report groups.....	88
<b>Chapter 14: Event Management.....</b>	<b>89</b>
Pre-defined events.....	89
Custom events.....	92
Application log events.....	93
Supported PDU and UPS events.....	93
Event severity levels.....	94
Viewing events.....	94
Sorting events.....	95
Adding comments to events.....	95
Deleting events.....	95
Filtering events.....	96
Sending test events from an IPMI device.....	96
<b>Chapter 15: Security.....</b>	<b>98</b>
Starting Services with a Windows operating system standard user account.....	98
Operating system hardening.....	99
Audit log.....	99
Managing certificates.....	100
<b>Chapter 16: Configuring settings.....</b>	<b>101</b>
General settings.....	101
Configuring console session timeout.....	101
Setting protocol timeout periods.....	101
Monitoring settings.....	102
Configuring the power and temperature sampling intervals.....	102
Configuring the power and temperature monitoring units.....	103
Configuring energy consumption cost settings.....	103
Database policy settings.....	103
Setting or editing the database policy.....	104
Configuring database backup.....	104
Directory.....	105
Editing directory settings.....	106
Viewing directory settings.....	107

Alerts.....	107
Setting SNMP traps.....	107
Sending SNMP traps to a Third-Party Application.....	108
Editing email alert settings.....	108
Viewing alert forward settings.....	108
Editing SMTP settings.....	108
Licensing.....	108
Importing a License.....	109
Inventory.....	109
Configuring inventory settings.....	109
<b>Chapter 17: Logs.....</b>	<b>110</b>
Sorting the logs display.....	110
Setting the application log size.....	110
<b>Chapter 18: Troubleshooting.....</b>	<b>111</b>
<b>Appendix A: Upgrade failure recovery on Microsoft Windows operating system.....</b>	<b>116</b>
<b>Appendix B: Upgrade failure recovery on Linux operating system.....</b>	<b>118</b>

# Overview

OpenManage Power Center is a power management solution for the data center. It enables you to monitor and manage power consumption and temperature in your data center through the management console.

## Topics:

- [Key features](#)
- [New in this release](#)
- [Topology](#)
- [System requirements](#)

## Key features

**Table 1. OpenManage Power Center features**

Feature	Description
Easy Installation	The OpenManage Power Center installation wizard has easy-to-use steps that allow you to install the application easily and in a few minutes.
Power Monitoring	Monitors power-related metrics on the following levels: <ul style="list-style-type: none"><li>• Individual device</li><li>• Data center/Room/Aisle/Rack/Chassis</li><li>• User-defined group</li></ul>
Temperature Monitoring	Monitors temperature data of devices or device groups.
Power Control	Creates policies that control power consumption at the device and group levels.
Tasks	You can create power control and discovery tasks. Power control tasks help you avoid power cuts and power spikes. Discovery tasks help you to add devices to the Power Center management console. This in turn helps you to manage them.
Device Discovery	Supports enterprise systems including PowerEdge blade and tower/rack servers, chassis, and Power Distribution Units (PDUs) and Uninterruptible Power Supply (UPS) devices.
Role-based Access Control	Supports user authentication and multiple role-based rights.
Event Management	Enables you to monitor and manage device and group events.
Report Management	Enables you to generate reports for inventory and monitoring.
Stranded Power Information	Stranded power, also known as headroom, is the excess power available for a device group. OpenManage Power Center helps you to calculate the stranded power for devices



**Table 1. OpenManage Power Center features (continued)**

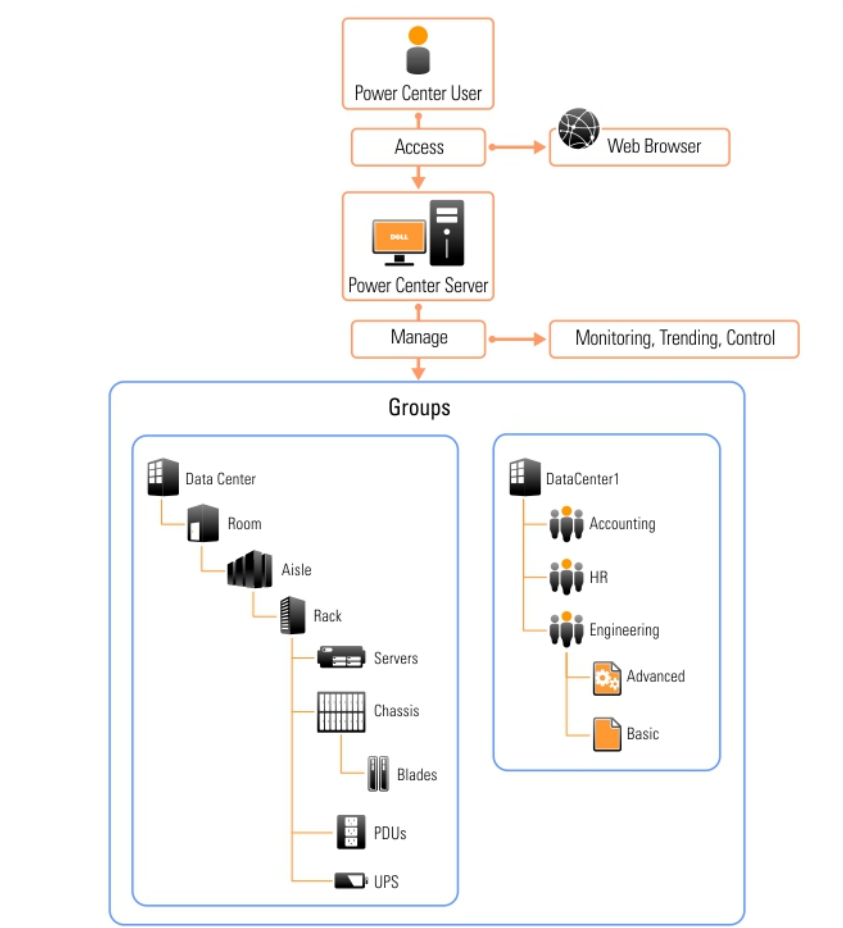
Feature	Description
	<p>and device groups. The formula for calculating stranded power is:</p> $\text{Stranded Power}(\tau) = \text{Allocated Power}(\tau) - \text{Peak Power Consumption}(\tau)$ <p>where <math>(\tau)</math> is calculated as a function of time. You can specify a time range in the report. By default, <math>(\tau)</math> is the time range of monitored data.</p>
Power and Thermal Analysis	Enables you to analyze power and the thermal characteristics. You can also analyze the underutilized servers and identify the potential cooling issues in a data center.
Integration with the iDRAC Location	Enables you to replicate the data center hierarchy on the iDRAC location based on OMPC physical location modeling.
Database Backup	Enables you to schedule a backup of all the policies, recovery logs, or the OMPC database. The backup data can be used on a different OMPC server or can be used as a restore point if there is a disk failure.
Measuring virtual machine power consumption	Enables you to measure the power utilized by virtual machines. The measured values help you to balance the workload between VMs based on power consumption and identify any issues with assignment of VMs to the servers.

## New in this release

- Support for new platforms and browsers. For more information, see [Supported and unsupported devices](#).
- Support for new operating systems and browsers. For more information, see [Software requirements](#).

## Topology

The following figure shows how to use a web browser to access the Power Center server and manage the data center.



**Figure 1. OMPC Topology**

## System requirements

This section describes the general requirements of OMPC and provides information on supported operating systems and the basic system requirements for server system and devices that use OMPC.

### Hardware and software requirements for the server system

#### Hardware requirements

You must install Power Center on a system with at least:

- A dual-core processor of 2.6Ghz or higher
- 4GB RAM
- 60GB free space of hard drive
- Gigabit bandwidth of network infrastructure

**NOTE:** For the latest list of hardware and software requirements, refer to the `readmefirst.txt` file included with the OpenManage Power Center software download, and the Release Notes available at [dell.com/support/home](https://dell.com/support/home).

#### Software requirements

OpenManage Power Center supports the following operating systems:

- Microsoft Windows Server 2012 R2 Essentials Edition
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition
- Microsoft Windows Server 2016 Standard Edition
- Microsoft Windows Server 2016 Data Center Edition
- Microsoft Windows Server 2019 Standard Edition
- Microsoft Windows Server 2019 Data Center Edition
- Microsoft Windows 8.1 Professional
- Microsoft Windows 8.1 Enterprise
- Microsoft Windows 10 Professional
- Red Hat Enterprise Linux 6.9 x86\_64
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5
- SUSE Linux Enterprise Server 11 SP4 x86\_64
- SUSE Linux Enterprise Server 12 SP3

OpenManage Power Center supports the following web browsers:


- Google Chrome 63, 64, and 65
- Mozilla Firefox 57, 58, and 59
- Microsoft Internet Explorer 11
- Microsoft Edge


 **NOTE:** OMPC performs best with Google Chrome, Mozilla Firefox, or Microsoft Edge as these browsers prevent Cross-site script (XSS) using Content Security Policy (CSP) 1.0. The CSP 1.0 is not supported on Internet Explorer 11.

The OpenManage Power Center installation includes the following major software tools:

- Oracle Java Runtime Environment (JRE) 8 Update 162
- Apache Tomcat application server 7.0.85
- PostgreSQL 9.3.14

## Hardware and software requirements for devices

- Managed servers must have Integrated Dell Remote Access Controller (iDRAC) 6, 7, 8, or 9.
-  **NOTE:** You can use OMPC on iDRAC6 for monitoring the devices; however power capping feature is not supported.
- Power Distribution Unit (PDU) and Uninterruptible Power Supply (UPS) devices must comply with the Management Information Base (MIB) the vendor provides through SNMP interface.
- Devices must provide exclusive access for Power Center because the policies set on the devices from other management software affect the Power Center power control function.
- The Baseboard Management Controller (BMC) user, through which Power Center communicates with devices, must be a local user account whose roles include Administrator. The device must be configured to allow the Administrator to use at least one of the cipher suite levels 0–3, and enable the **IPMI over LAN** setting.
- The WSman user, through which Power Center communicates with the chassis, must be a local user with the Administrator role. The chassis must be configured to enable the **Web Server** service.

 **NOTE:** For a list of Dell OpenManage Power Center-supported devices, see [Supported and unsupported device](#).

# Getting started

This chapter introduces the OpenManage Power Center management console, and presents several use cases that describe standard uses of OpenManage Power Center.

## Topics:

- [Management console introduction](#)
- [Home page](#)
- [Common use cases](#)
- [Supported and unsupported devices](#)

## Management console introduction

To use OpenManage Power Center, you must open a Web browser and [log in](#). The management console opens with a list of the available screens in the left navigation pane, and the currently open screen in the right pane.

**Table 2. Main OMPC Pages**

Main Screen	Available actions on the screen
<b>Home</b>	<p>The <b>Home</b> screen introduces OpenManage Power Center features, and lists initial setup steps that you can complete after setup. You can click the <b>Help</b> to get additional information. On this screen you can view:</p> <ul style="list-style-type: none"> <li>• Overall events generated by the managed devices</li> <li>• Events from the top five groups generated by the managed devices</li> <li>• The total number and type of discovered devices</li> <li>• The top five energy consuming device groups at the root level</li> <li>• Information about power and space headroom</li> <li>• Analyze top power cap and temperature threshold offenders</li> <li>• Most underutilized racks</li> <li>• Top 10 most recent critical and warning events</li> <li>• Information about power and temperature history</li> </ul>
<b>Tasks</b>	<p>The Tasks feature enables you to perform device discovery and power control tasks such as power-on and power-off, on a specific device or group of devices. On the <b>Tasks</b> screen you can:</p> <ul style="list-style-type: none"> <li>• Create new discovery and power control tasks</li> <li>• Edit or delete discovery and power control tasks</li> <li>• Start or re-run discovery and power control tasks</li> <li>• Refresh the list of discovery or power control tasks</li> <li>• View the summary of the discovery or power control tasks</li> </ul>
<b>Devices</b>	<p>On the <b>Devices</b> screen, you can view both network-discovered and manually added devices. On this screen you can:</p> <ul style="list-style-type: none"> <li>• Add groups</li> <li>• Add unsupported devices</li> <li>• Create logical groups</li> <li>• Set the estimated maximum power for devices</li> <li>• Edit devices or managed groups</li> <li>• Delete devices or managed groups</li> </ul>

**Table 2. Main OMPC Pages (continued)**

Main Screen	Available actions on the screen
	<ul style="list-style-type: none"> <li>● Refresh the list of devices or managed groups</li> <li>● Filter and search the list of devices</li> <li>● Sort the list of devices</li> <li>● Move devices from one group to another</li> <li>● Enable or disable Emergency Power Reduction (EPR)</li> <li>● View details of the devices or managed groups</li> </ul> <p>All devices, whether grouped or unassigned are listed in the <b>All Devices</b> tab. Device groups are displayed in the <b>Managed Groups</b> tab.</p>
<b>Virtual Machines</b>	<p>On the <b>Virtual Machines</b> screen, you can view both network-discovered and manually added devices. On this screen you can:</p> <ul style="list-style-type: none"> <li>● Create a new virtual machine group</li> <li>● Add a virtual machine to an existing group</li> <li>● Filter virtual machines based on various attributes</li> <li>● Move a virtual machine group</li> <li>● View a virtual machine power history and power distribution graph</li> <li>● Delete a virtual machine group</li> </ul>
<b>Policies</b>	<p>On the <b>Policies</b> screen, you can manage the power policies applied to your devices. On this screen you can:</p> <ul style="list-style-type: none"> <li>● Create power and thermal policies</li> <li>● Edit power or thermal policies</li> <li>● Enable or disable power or thermal policies</li> <li>● Delete power or thermal policies</li> <li>● Filter power or thermal policies so that only certain policies are displayed</li> <li>● Sort the list of policies</li> </ul>
<b>Reports</b>	<p>The <b>Reports</b> screen helps you to periodically generate reports for inventory and monitoring. On this screen you can:</p> <ul style="list-style-type: none"> <li>● Create reports</li> <li>● Edit reports</li> <li>● Delete reports</li> <li>● Refresh the Reports list</li> <li>● Add or edit report groups</li> <li>● Set estimated max power</li> </ul>
<b>Analysis</b>	<p>The <b>Analysis</b> screen helps you to analyze power and thermal characteristics. On this screen you can:</p> <ul style="list-style-type: none"> <li>● Analyze server characteristics</li> <li>● View, filter, and export peak power or active idle power reports</li> <li>● View, analyze, filter, and export underutilized servers reports</li> <li>● Identify the number of servers that can be accommodated in a specific group</li> <li>● View placement recommendation for servers</li> <li>● Estimate the power and space you can save by consolidating the underutilized servers</li> <li>● Identify and analyze the potential cooling issues in a data center</li> </ul>
<b>Events</b>	<p>The <b>Events</b> screen lists the system and log events at the following severity levels:</p> <ul style="list-style-type: none"> <li>● Critical</li> <li>● Warning</li> <li>● Info</li> </ul> <p>On this screen you can:</p> <ul style="list-style-type: none"> <li>● Acknowledge Events</li> </ul>

**Table 2. Main OMPC Pages (continued)**

Main Screen	Available actions on the screen
	<ul style="list-style-type: none"> <li>• Add a note to an event</li> <li>• Delete Events</li> <li>• Sort events</li> <li>• Filter events</li> <li>• Export Events</li> </ul>
<b>Logs</b>	The <b>Logs</b> screen displays information about unexpected or informational events or internal errors that occur in OpenManage Power Center.
<b>Settings</b>	<p>From the <b>Settings</b> submenus you can configure all OpenManage Power Center settings, including:</p> <ul style="list-style-type: none"> <li>• General — Configure the timeout for console and device communication.</li> <li>• Monitoring — Configure the power/thermal units and energy consumption parameters.</li> <li>• Alerts — Configure alerts for SNMP traps, enable or disable sending alerts through emails, configure email recipients, and event severity-level.</li> <li>• SMTP — Configure SMTP parameters for sending alert emails.</li> <li>• Database — Configure database compression and purging policy.</li> <li>• Directory — Configure Lightweight Directory Access Protocol (LDAP) settings to support authentication through LDAP. This tab is displayed only on systems running the Linux operating systems where OpenManage Power Center is installed.</li> <li>• User and Group Accounts — Manage user or group accounts for accessing OpenManage Power Center.</li> <li>• Roles — Managing roles and rights.</li> <li>• Licensing — Manage the issued licenses.</li> <li>• Inventory — Track chassis inventory.</li> </ul>

## Home page

On the **Home** page, you can view the following information.

- **Events (Overall)**
- **Events (Top 5 Groups)**
- **Devices Discovered [Total: <number>]**
- **Energy Consumers (Top 5 Groups) [kwh]**
- **Power Headroom**
- **Space Headroom**
- **Top Offenders (Power)**
- **Top Offenders (Temperature)**
- **Underutilized Racks (Power)**
- **Underutilized Racks (Space)**
- **Top 10 Events (Critical and Warning)**
- **Power History**
- **Temperature History**

## Events

On the **Home** page, you can view a pie graph representation of events occurring in OpenManage Power Center. Move the pointer over the graph to view the number of each event type.

## Events (Top 5 Groups)


On the **Home** page, you can view a bar graph representation of the top five device groups, that have the highest number of events with severity as **Critical**, followed by the events that has the events with severity as **Warning** and **Information**. Move the pointer over the graph to view the number of each event type for the top-five device groups.

## Devices Discovered [Total: <number>]

On the **Home** page, you can view a pie graph representation of the total number and type of discovered devices.

## Energy Consumers (Top 5 Groups) [kwh]

On the **Home** page, you can view a bar graph representation of the top five energy consuming device groups at the root level.

Click  to specify the number of months for calculating the peak power consumption. By default, the number of months is 6.

## Power Headroom

OMPC enables you to monitor and manage the available excess power in a top-level group. The observed monitoring data is helpful in planning capacity expansion.

## Space Headroom

OMPC enables you to monitor and manage the available excess space in a data center. The observed monitoring data is helpful in providing placement suggestion.

## Top Offenders (Power)

This option enables you to view the names of the racks that exceeded the power threshold.

## Top Offenders (Temperature)

This option enables you to view the names of the racks that exceeded the Temperature threshold. Click **Actual** or **Percentage** to arrange the devices or groups by the actual amount or percentage by which the racks have exceeded the temperature thresholds or caps.


## Underutilized Racks

This option enables you to view the names of the racks in which the power capacity and rack space remain unused. Click **Actual** or **Percentage** to arrange the racks by the actual or utilization percentage of power and rack space.

## Top 10 (Most Recent) Critical and Warning Events

This option enables you to view the recent top 10 critical and warning events.

## Customizable Dashboard Settings

This option enables you to customize the dashboard available on the home page. You can select individual information referred as dashlets, from a list of predefined set of dashlets. Click  to select the required dashlets.

## Power History

A visual representation of the power history of the system groups.

## Temperature History

A visual representation of the temperature history of the system groups.

## Common use cases

This section provides a standard scenario to help Administrators to get started with OpenManage Power Center.

If you are a first-time user, you can follow the sequence of steps 1-5 to install OpenManage Power Center and set up the group structure for monitoring your data center. Then, see steps 6, 7, and/or 8 to use OpenManage Power Center for monitoring, comparing power and temperature data between devices and/or time slots, and creating policies:

1. Install OpenManage Power Center in a [Windows](#) or [Linux](#) environment
2. [Launch](#) OpenManage Power Center.
3. [Discover](#) devices and add one or more devices from the network.
4. [Manage](#) your devices. You can delete, edit, and filter devices.
5. [Create](#) one or more data center group structures.
6. [Create](#) one or more power policies, and apply to devices.
7. [Create](#) power control tasks.
8. Monitor [Power](#) and [Temperature](#) events on devices.
9. Generate reports and compare power or temperature status and the energy cost for two or three devices or groups.

## Supported and unsupported devices

You can discover supported devices, and create a group structure to build out the data center. Power Center cannot discover or manage all device types, and unsupported devices must be manually added to make the data center group structure complete.

For supported devices:

- Device types include chassis, server, UPS, and PDU.
- Set the connection protocol and credential information so that the device can communicate with Power Center.
- Perform management functions including discovery, adding to the group structure, monitoring power and temperature, applying power management policies, and sending events.

Power Center supports up to 6000 managed devices in one data center.

**Table 3. Supported devices**

Category	Supported Platform	Validated Model
Server	Dell	<ul style="list-style-type: none"><li>• PowerEdge R310 Server</li><li>• PowerEdge R410 Server</li><li>• PowerEdge R515 Server</li><li>• PowerEdge R610 Server</li><li>• PowerEdge R710 Server</li><li>• PowerEdge R715 Server</li><li>• PowerEdge R810 Server</li><li>• PowerEdge R815 Server</li><li>• PowerEdge R910 Server</li><li>• PowerEdge M610 Server</li></ul>



**Table 3. Supported devices**

Category	Supported Platform	Validated Model
		<ul style="list-style-type: none"> <li>• PowerEdge M610x Server</li> <li>• PowerEdge M710 Server</li> <li>• PowerEdge M710HD Server</li> <li>• PowerEdge M910 Server</li> <li>• PowerEdge T610 Server</li> <li>• PowerEdge T710 Server</li> <li>• PowerEdge FM120 Server</li> <li>• PowerEdge R320 Server</li> <li>• PowerEdge R420 Server</li> <li>• PowerEdge R520 Server</li> <li>• PowerEdge R620 Server</li> <li>• PowerEdge R720 Server</li> <li>• PowerEdge R720xd Server</li> <li>• PowerEdge R820 Server</li> <li>• PowerEdge R920 Server</li> <li>• PowerEdge M420 Server</li> <li>• PowerEdge M620 Server</li> <li>• PowerEdge M520 Server</li> <li>• PowerEdge T320 Server</li> <li>• PowerEdge T420 Server</li> <li>• PowerEdge T620 Server</li> <li>• PowerEdge R330 Server</li> <li>• PowerEdge R430 Server</li> <li>• PowerEdge R440 Server</li> <li>• PowerEdge R530 Server</li> <li>• PowerEdge R530XD Server</li> <li>• PowerEdge R540 Server</li> <li>• PowerEdge R540XD Server</li> <li>• PowerEdge R630 Server</li> <li>• PowerEdge R730 Server</li> <li>• PowerEdge R730Xd Server</li> <li>• PowerEdge R930 Server</li> <li>• PowerEdge R640 Server</li> <li>• PowerEdge R740 Server</li> <li>• PowerEdge R740XD Server</li> <li>• PowerEdge R840 Server</li> <li>• PowerEdge R940 Server</li> <li>• PowerEdge R940xa Server</li> <li>• PowerEdge M630 Server</li> <li>• PowerEdge M640 Server</li> <li>• PowerEdge M640 Server-VRTX</li> <li>• PowerEdge M830 Server</li> <li>• PowerEdge T330 Server</li> <li>• PowerEdge T430 Server</li> <li>• PowerEdge T440 Server</li> <li>• PowerEdge T630 Server</li> <li>• PowerEdge FC430 Server</li> <li>• PowerEdge FC630 Server</li> <li>• PowerEdge FC640 Server</li> <li>• PowerEdge FC830 Server</li> <li>• PowerEdge FD332 Server</li> <li>• PowerEdge C4130 Server</li> <li>• PowerEdge C4140 Server</li> </ul>

**Table 3. Supported devices (continued)**

Category	Supported Platform	Validated Model
		<ul style="list-style-type: none"> <li>PowerEdge C6320 Server</li> <li>PowerEdge C6420 Server</li> <li>PowerEdge MX740C Server</li> <li>PowerEdge MX840C Server</li> </ul>
	HP	<ul style="list-style-type: none"> <li>HP ProLiant DL360 G5</li> <li>HP ProLiant DL380 G7</li> <li>HP ProLiant DL360p G8</li> <li>HP ProLiant DL360p G9</li> <li>HP ProLiant BL460c G6</li> <li>HP ProLiant BL460c G7</li> <li>HP ProLiant BL460c G9</li> </ul>
	IBM	<ul style="list-style-type: none"> <li>IBM System x3550 M4</li> <li>IBM System x3550 M5</li> <li>IBM Blade HS12 (Type 8028)/8028IC2</li> <li>IBM Blade HS23 (Type 7875)/7875OI5</li> </ul>
	Cisco	Cisco UCSB-B200-M3
	Intel	<ul style="list-style-type: none"> <li>Intel S2600CP</li> <li>Intel S2600WT</li> <li>Intel S5500WB</li> </ul>
Chassis	Dell	<ul style="list-style-type: none"> <li>PowerEdge M1000e</li> <li>VRTX Blade Enclosure</li> <li>PowerEdge FX2/FX2s</li> <li>PowerEdge MX7000</li> </ul>
	HP	HP BladeSystem c7000 Enclosure G2
	IBM	IBM AMM BladeCenter-E/86774TC
	Cisco	Cisco N20-C6508
PDU	Dell	<ul style="list-style-type: none"> <li>6804 Metered PDU</li> <li>6607 Metered PDU</li> <li>XX5T6 Metered PDU</li> <li>6803 Metered PDU</li> <li>6605 PDU</li> <li>Tripplite PDU</li> </ul>
	APC	<ul style="list-style-type: none"> <li>APC Metered Rack PDU AP7801</li> <li>APC Switched Rack PDU AP7900</li> <li>APC Switched Rack PDU AP7920</li> <li>APC AP8853 PDU</li> <li>APC AP8953 PDU</li> <li>APC AP8653 PDU</li> </ul>
	Eaton	<ul style="list-style-type: none"> <li>Eaton Monitored PDU PW312MI0UC07</li> <li>Eaton Switched PDU PW105SW0U154</li> </ul>
	Emerson	<ul style="list-style-type: none"> <li>Emerson Liebert MPH MPH-NCR09NXXE30</li> </ul>
	ServerTech	<ul style="list-style-type: none"> <li>ServerTech Switched PDU CW-24V4J411</li> </ul>


**Table 3. Supported devices (continued)**

Category	Supported Platform	Validated Model
		<ul style="list-style-type: none"> <li>ServerTech Smart CDU, 0U CS-24V1-C20M</li> </ul>
	Raritan	<ul style="list-style-type: none"> <li>Raritan DPXS20A-16 PDU</li> <li>Raritan PX3-4731I2V PDU</li> <li>Raritan PX3-4732V-F5 PDU</li> <li>Raritan PX2-1497 PDU</li> </ul>
	BayTech	<ul style="list-style-type: none"> <li>MMP17</li> <li>MMP20</li> </ul>
UPS	Dell	<ul style="list-style-type: none"> <li>N313P Line interactive UPS w/ web card H910P</li> <li>Online Rack UPS 3750R OL K804N</li> <li>UPS, 2700/2300VA, 120V, 3U K802N</li> </ul>
	APC	<ul style="list-style-type: none"> <li>APC Online UPS w/ Web card SURTD3000XLI</li> <li>APC Smart-UPS 3000VA RM SUA3000RM2U</li> <li>Smart-UPS 5000VA RM DL5000RMT5U</li> <li>APC Smart-UPS 2200 RM</li> <li>APC Smart-UPS 3000</li> </ul>
	Eaton	<ul style="list-style-type: none"> <li>Eaton Line interactive UPS w/ Web card PW5130I1750-XL2U</li> </ul>
	Emerson	<ul style="list-style-type: none"> <li>Emerson Online UPS w/ Web card GXT2-2700RT208</li> </ul>

For unsupported devices:

- Power Center does not communicate with unsupported devices; therefore, connection protocol and credential information is not necessary.
- Unsupported devices cannot be discovered, they can only be added to the device list on the **All Devices** tab.
- Power Center adds the unsupported device to the group structure, but cannot manage it using the available management functions.

You may need to enter **Estimated Max Power** value when adding supported or unsupported devices.

 **NOTE:** OMPC support platforms with redundant PSUs only.

# Using OpenManage Power Center

This chapter explains how to install, uninstall, and launch OpenManage Power Center on Microsoft Windows and Linux platforms.

## Topics:

- [Preinstallation requirement for OpenManage Power Center](#)
- [Using Power Center on Microsoft Windows operating systems](#)
- [Using OpenManage Power Center on Linux operating systems](#)

## Preinstallation requirement for OpenManage Power Center

Ensure that you assess the following before installing OMPC.

- Administrator privileges.
- Read/write access to the destination folder.
- Ensure that the system meets or exceeds the minimum requirement. For more information, see [System Requirements](#).

**NOTE:** On Microsoft Windows operating systems, OpenManage Power Center uses the Windows Network Service account to start the OpenManage Power Center service during the installation. For better security, you can turn off the OpenManage Power Center services and change to an account other than the Windows Network Service account to start the OpenManage Power Center services.

**NOTE:** On Linux operating systems, use `-prefix=<dir>` to save the installation binary file to a location other than the default path.

**NOTE:** The Diffie–Hellman (DH) cipher is not supported on OMPC server.

## Using Power Center on Microsoft Windows operating systems

This section explains how to install, uninstall, launch, and upgrade OpenManage Power Center on Microsoft Windows platforms.

### Installing OpenManage Power Center on Microsoft Windows Server

1. Download the OpenManage Power Center software at [dell.com/powercenter](http://dell.com/powercenter).
2. Double-click `OpenManagePowerCenter.exe`.
3. In the **Installation Wizard** home window, click **Next**.
4. In the **License Agreement** window, read the license agreement, select **I accept the terms in the license agreement**, and then click **Next**.
5. In the **Administrator Account** window, enter a name for the super user account or installation account in the **User Name** text box. By default, the user name is 'admin'.  
The user name must be:
  - Unique for each OpenManage Power Center user
  - Up to 20 uppercase or lowercase printable characters, except “`/\[:;|=,+'*?<>.@`”

- Not case-sensitive

6. Enter the password in the **Password** text box and then, in the **Verify Password** text box to confirm it.

**NOTE:** The password must be a minimum of eight characters, with characters from at least three of the following categories: uppercase, lowercase, numeric, and non-alphanumeric.

If you want to customize the installation, select the **Custom Install** check box and proceed to step 7 else, proceed to step 10.

7. In the **Destination Folder** window, either leave the default installation path or click **Change...** to navigate to the desired location on your system and click **Next**.

**NOTE:** Ensure that you have **Full Control** permission on the destination folder. The installation may fail if you try to install OMPC on a system folder such as C:\Users\Administrator or at a root level.

**NOTE:** The installation path only supports ANSI characters (English characters, numbers, and simple symbols). Do not use an installation path with non-ANSI characters.

8. In the **HTTPS** window, configure the following HTTPS settings, and then click **Next**.

- **HTTPS Port** — By default, the OpenManage Power Center uses port 8643 for HTTPS communication. To select a different port, enter a new port number between 1000 and 9999.
- **Redfish Event Port** — By default, the OpenManage Power Center uses port 8644 for Redfish events. To select a different port, enter a new port number between 1000 and 9999.
- **Keystore Password** — Enter a password that is used to access the keystore file. In the **Verify Password** field, enter the password again to confirm. The password must be more than five characters, and cannot contain non-ANSI characters and double quotes (").

Alternatively, select the **Generate Random Password** to get a system-generated password to access the keystore file. If you select this option, change the password method option in the C:\Program Files\DELL\OpenManagePowerCenter\pgdata to trust. This modification helps you to log into the PostgreSQL database using the database administrator tool for any debugging.

9. In the **Database** window, enter the following information for the PostgreSQL database server account.

- **User Name** — Enter your PostgreSQL database server user name.
- **Database Port** — Default value is 6443. If another database is already using the default port, enter a new port number between 6000 to 9999.
- **User Password** — Enter your PostgreSQL database server user password.
- **Verify Password** — Enter the password again to confirm.
- **Database Data Directory** — The location of PostgreSQL data.

**NOTE:** The password must be a minimum of eight characters in length with characters from at least three of the following categories: uppercase, lowercase, numeric, non-alphanumeric. It cannot include spaces.

10. Click **Next**. The **Ready to Install the Program** window is displayed.

In this window, you can view the installation summary information such as the destination folder on the system where the OpenManage Power Center folders and files are stored and database information.

11. Click **Install** to begin the installation.

After the installation is complete, the **InstallShield Wizard Completed** window is displayed.

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

## Installed directories in Windows

By default, the OpenManage Power Center package installs to C:\Program Files\Dell\OpenManagePowerCenter.

**NOTE:** You cannot install OpenManage Power Center in the root folders of the Windows volume. You must select a non-root folder or another volume.

The OpenManage Power Center package includes the following folders:

- **bin** — OpenManage Power Center binaries
- **conf** — OpenManage Power Center configuration files

- **external** — Other applications installed by OpenManage Power Center
- **Logs** — OpenManage Power Center event logs
- **Pgdata** (default) — Database files

To protect data, the following files are accessible only to Network Service or Administrator users:

- OpenManagePowerCenter\conf\app.config.xml
- OpenManagePowerCenter\external\apache-tomcat\conf\server.xml

## OpenManage Power Center services on Microsoft Windows operating systems

The OpenManage Power Center includes the following services:

- Dell EMC OpenManage Power Center – The Apache Tomcat server that hosts the Power Center web application which passes action requests to the OpenManage Power Center server.
- Dell EMC OpenManage Power Center Database Server – The PostgreSQL internal database for OpenManage Power Center.
- Dell EMC OpenManage Power Center SNMP Dispatcher – If the Windows SNMP trap service is installed, then it reroutes SNMP traps to the OpenManage Power Center Server service. If the Windows SNMP trap service is not installed, this service stops automatically.
  - NOTE:** If the Windows SNMP trap service is installed, make sure it is not disabled. Otherwise, Power Center cannot function properly.
- Dell EMC OpenManage Power Center Server – The Power Center server core service. It carries out all actions including communication with devices.

To stop or start a service, select the appropriate service from the Windows Services list, and select the action to perform.

Power Center uses the Network Service account to start all services. You can change to a normal Windows operating system user account for security purposes.

## Upgrading Power Center on Microsoft Windows operating systems

To upgrade Power Center from a previous version on a system running supported Microsoft Windows operating systems, the system must have at least 366 MB of free space on the C: drive.

1. Install OpenManage Power Center. For more information, see [Installing Power Center](#).  
A dialog box is displayed, informing you that an older version of OpenManage Power Center is installed.
2. If you want to migrate the previous Power Center database, ensure that **Migrate data** check box is selected. This migrates most of the Power Center data, such as hierarchy information, monitoring history, policy settings, events, and credential data. Uncheck **Keep Power/Thermal Data** checkbox if you do not need to migrate the existing power or thermal data.
  - NOTE:** The special characters, such as \ or a space cannot be used in the password after you upgrade to the latest version. It is recommended to use the OMPC reconfiguration tool to set a new password.
3. To upgrade, click **Upgrade now**. If you do not want to upgrade, click **Cancel**.
  - NOTE:** On upgrading OpenManage Power Center to the latest version on remote systems, the data in the OpenManage Power Center database is not migrated to the latest version.
  - NOTE:** Do not cancel the upgrade process, if cancelled, rollback to the previous version may fail. This may also result in data loss. For more information on upgrading and steps to handle failure during upgrade, see [Upgrade failure recovery on Microsoft Windows operating system](#).
  - NOTE:** It is recommended to have a database backup from the settings page before the upgrade. For more information, see [Configuring database backup](#).
  - NOTE:** After upgrading to the latest version of OpenManage Power Center, the rights assigned to the roles may change. Edit the roles to re-assign the rights.

## Uninstalling OpenManage Power Center on Microsoft Windows operating system

Before you uninstall OpenManage Power Center ensure to remove all devices from the Power Center management console. Otherwise, the existing power cap value set in the policies (including EPR) remains effective on the devices.

**NOTE:** Ensure to check your data center power capacity before removing the devices to avoid tripping the breaker, because the policies will be removed at the same time.

1. Click **Start > Control Panel > Programs/Programs and Features**.
2. Select **Dell OpenManage Power Center**, right-click and select **Uninstall**.

The following message is displayed.

Are you sure you want to uninstall Dell OpenManage Power Center?

3. Click **Yes** to confirm. Follow the on-screen instructions.

**NOTE:** On uninstalling OpenManage Power Center, the installation folder where OpenManage Power Center is installed, is removed.

**NOTE:** At times, after the uninstallation is complete, a message is displayed informing you that some files are not deleted and a service is not released automatically. You may have to delete the files manually and reboot server to release the service before installing OMPC again.

## Launching OpenManage Power Center on Microsoft Windows operating systems

After the OpenManage Power Center installation on the system is complete, a desktop icon of OpenManage Power Center is created on the desktop. You can use this icon to launch the OpenManage Power Center console. The console is launched in the default browser configured on the system.

Alternately, you can also launch OpenManage Power Center by opening a web browser. You may need to configure your web browser to launch OpenManage Power Center.

To launch OpenManage Power Center, enter the following address in lower case in your Web browser: `https://<Server_Name>:<HTTPS_Port>/`

For example: `https://localhost:8643/`

**NOTE:** It is recommended to use screen resolutions of 1280\*800 pixels or higher for using the OpenManage Power Center management console.

Select a user account and enter your name and password. The OpenManage Power Center console is displayed. You can use the OpenManage Power Center functions.

**NOTE:** To avoid the difference in timezone between your system and the server, ensure that the time zone of your system is same as that of the OMPC server.

## Configuring Enhanced Security Configuration for Internet Explorer

If the OpenManage Power Center server uses Windows Server 2012 or Windows Server 2016 and the Web browser is Internet Explorer 10 or later, then the Internet Explorer Enhanced Security Configuration (ESC) feature is enabled by default. To make sure OpenManage Power Center functions properly in Internet Explorer, you must either disable this feature or configure Internet Explorer to trust the OpenManage Power Center site and links.

### Disabling ESC in Windows Server 2012

1. Close any open Internet Explorer windows.
2. Open Server Manager.
3. On the left navigation bar, click **Local Server**.

4. Under **Properties**, locate **IE Enhanced Security Configuration**; click the **On** or **Off** radio buttons for both Administrators and Users as desired to enable or disable the feature for those groups.
5. Click **OK** to save your selections.

## Configuring ESC to Trust the Power Center Site and Links

1. Go to **Internet Explorer > Tools > Internet Options > Security**.
2. Click **Trusted Sites**, and add *about: Blank* as a trusted site.


 **NOTE:** You may need to restart Internet Explorer for the configuration to take effect.


# Using OpenManage Power Center on Linux operating systems

This section explains how to install, uninstall, launch, and upgrade Power Center on Linux platforms.


## Installing Power Center on a Linux server

1. Download the Power Center compressed (\*.zip or \*.tar.gz) installation file at **dell.com/powercenter**.

 **NOTE:** You must use the root user account to execute the following steps.

 **NOTE:** Use `-prefix=<dir>` to save the installation binary file to a location other than the default path.

2. Decompress the installation file to produce rpm and install.sh files

 **NOTE:** While the default installation directory is `/opt/dell/ompc`, it is recommended that you direct the installation to `INSTALLDIR` as described in the following step.


3. Run the following command to install the binary and automatically launch the initialization tool:

```
#./install.sh <INSTALLDIR>
```

4. Press <Enter> to continue.  
The **End User License Agreement** appears.
5. Read the End User's License Agreement (EULA), then type `accept` to continue.  
The **Power Center License** screen appears.
6. Review the license message, then press <Enter> to continue.  
The **HTTPS Setting** screen appears.
7. Configure the HTTPS settings by entering a number from the list, then providing the information requested.
  - **HTTPS Port**—Enter a port number between 1000 and 9999. OMPC uses a default port number 8643
  - **Redfish Event Port** — By default, the OpenManage Power Center uses port 8644 for Redfish events. To select a different port, enter a new port number between 1000 and 9999.
  - **Keystore Password**—Enter a password to access the keystore file. The password must be more than 5 characters, and cannot contain non-ANSI characters and double quotes (").

Press <Enter> when you have made all your changes. The **Database Server** screen appears.

8. Configure the PostgreSQL service by providing the following information:
  - **User Name**—Enter your PostgreSQL database server user name.
  - **User Password**—Enter your PostgreSQL database server user password.

 **NOTE:** The password must be a minimum of 8 characters in length with characters from at least three of the following categories: uppercase, lowercase, numeric, non-alphanumeric. The password can include spaces.
  - **PostgreSQL Port**—The default value is 6443. If another database is already using the default port, enter a different port.



- **PostgreSQL Data Directory**—The location of PostgreSQL data.

Press <Enter> to continue.


 **NOTE:** You must create a super user account to log into OpenManage Power Center following installation.

9. Create a super user account.

a. Type 1, then enter a super user account name. The account name must be:


- Unique for each Power Center user
- Up to 20 uppercase or lowercase printable characters, except “/\[;|=,+'\*?<>.@
- Not case sensitive

b. Type 2, then enter a password for the super user account.

 **NOTE:** The password must be a minimum of 8 characters in length, with characters from at least three of the following categories: uppercase, lowercase, numeric, and non-alphanumeric. The password can include spaces

10. Press <Enter> to initiate the installation.

11. Once the installation has completed, type q to quit the installation wizard.

 **NOTE:** You must install Linux Windows Management Instrumentation Command-line (WMIC), if you want to manage Hyper-V when OMPC is installed on Linux operating system. It is a Linux wmi tool and can be downloaded from <http://www.openvas.org/download/wmi/> link.

## Installed directories in Linux

By default, the OpenManage Power Center package is installed in /opt/dell/ompc.

The OpenManage Power Center package includes the following folders:

- **bin** — OpenManage Power Center binaries
- **conf** — OpenManage Power Center configuration files
- **external** — Other applications installed by OpenManage Power Center
- **logs** — OpenManage Power Center event logs
- **pgdata** (default) — Database files

## Power Center services in Linux

OpenManage Power Center includes the following services on Linux platform installations:

- Dell EMC OpenManage Power Center Database Services — The PostgreSQL internal database for OpenManage Power Center.
- Dell EMC OpenManage Power Center DataCenter Manager Service — The OpenManage Power Center server core service. It carries out all actions including communication with devices.
- Dell EMC OpenManage Power Center Authentication Service — Authenticates the local Linux user and group through a standard PAM interface.
- Dell EMC OpenManage Power Center WebServer Service — The Apache Tomcat server that hosts the OpenManage Power Center web application which passes action requests to the OpenManage Power Center server.

Use the following command at the command line interface to check OpenManage Power Center service status:

```
#opt/dell/ompc/ompcdaemons status
```

To start, stop, or restart OpenManage Power Center service, use the following command:

```
#/opt/dell/ompc/ompcdaemons start|stop|restart
```

## Uninstalling Power Center in Linux

**NOTE:** Ensure to remove all devices from the OpenManage Power Center console before uninstalling Power Center. Otherwise, the existing power cap value set in the policies (including EPR) will remain effective on the devices. Ensure to check your data center power capacity before removing the devices to avoid tripping the breaker, because the policies are also removed at the same time.

To uninstall Power Center on a Linux server, type the following at the command line interface:

```
rpm -e OpenManage_PowerCenter
```

**NOTE:** On uninstalling OpenManage Power Center, the installation folder where OpenManage Power Center is installed, is removed.

## Launching Power Center in Linux

Open a Web browser. You may need to configure your Web browser to launch OpenManage Power Center.

To launch OpenManage Power Center, enter the following address in lower case in your Web browser:

For example: `https://localhost:8643/`

**NOTE:** It is recommended to use screen resolutions of 1280\*800 pixels or higher for using the OpenManage Power Center management console.

Select a user account and enter your name and password. The OpenManage Power Center console is displayed. You can use the OpenManage Power Center functions.

# Using OpenManage Power Center through Command Line Interface

All commands supported by the command line interface (CLI) have the following format:

```
ompc_cli [COMMAND] [GENERIC_OPTIONS] [COMMAND_OPTIONS] [COMMAND_TARGET]
```

The operation must start with a valid [COMMAND]. Options can be entered anywhere after [COMMAND]. For each option that has a value, the value must be supplied immediately after the option.

**NOTE:** If a duplicate or incorrect option value is supplied with a command, the CLI window is closed with an error. For example, when both the `-profile` and `-protocol` options are supplied at the same time in a command, the CLI window is closed with an error.

GENERIC\_OPTIONS is used to run a generic job for this command line.

On Microsoft Windows operating system, user authentication credentials are specified as follows:

- `user_auth` <POWER\_CENTER|WINDOWS\_LOCAL|WINDOWS\_DOMAIN>
- `user_name` <user\_name>: If `user_type` is WINDOWS\_DOMAIN, then the `user_name` must be in domain\user format.
- `user_password` <password>

On Linux operating systems, user authentication credentials are specified as follows:

- `user_auth` <power\_center|linux\_local|ldap>
- `user_name` <user\_name>
- `user_password` <password>

The COMMAND\_TARGET specifies the targets on which the command operates. For example, the COMMAND\_TARGET for `add_profile` is a profile name to be added. For a specific command, the COMMAND\_TARGET cannot have the same value with the name of a generic option or an option supported by this command. For example, the COMMAND\_TARGET cannot be `-protocol` or `-user_name` for the command `add_profile`.

For COMMAND\_TARGET, the order of its content must be kept as defined in the specific command definition section. Any valid option can be mixed with the content of COMMAND\_TARGET. For example, the order of COMMAND\_TARGET of the `move_device` command must be supplied `FROM_GROUP_PATH` first, then `TO_GROUP_PATH`.

## Topics:

- [Command Line Interface error handling](#)
- [Command Line Interface commands](#)
- [Command line interface error codes](#)

## Command Line Interface error handling

On Microsoft Windows and Linux operating systems, an exit code is displayed indicating the successful execution of a command. An error code is displayed, if a command is not executed successfully.

On Microsoft Windows operating system, when the command is successful, the CLI exit code is 0. Refer [Command Line Interface Error Codes](#) to know about specific error codes.

On Linux operating system, when a command is successful, the CLI exit code is 0. If a command is not successful, a generic error code, 1, is displayed. Use `stderr` to get a more specific error code, and to find more information on that code, see [Command Line Interface Error Codes](#).

# Command Line Interface commands

This section lists the commands used to work with OMPC. In the following commands, [ ] represents optional attributes and < > represents variables. All command line text is case insensitive.

## help

Usage:

```
ompc_cli help [<COMMAND>] [<COMMAND_OPTION >]
```

The help command prints the help content for a command or a command option (including the generic option). Authentication is not required for the help command.

If no help command is specified (the ompc\_cli command was issued with no parameters), generic help information about the ompc\_cli tool displays. ompc\_cli help also displays the generic help.

ompc\_cli help help displays the help for the help command.

When only <COMMAND> is provided, the CLI prints the help for the specified command, including the command options that are available for the command. If you enter an invalid command, the CLI displays an error message.

When both <COMMAND> and <COMMAND\_OPTION> are provided, the CLI prints the help for the command option specified for the given command. If the command option is not a valid option for given command, the CLI displays an error message.

If more than one command or command option is provided, the CLI displays an error message.

## add\_profile

Usage:

```
ompc_cli add_profile -protocol <protocol_name> [-description <description>] [<pair of  
protocol property and value options>] <profile_name>
```

The add\_profile command adds a new discovery profile to OMPC. The profile\_name argument is used to identify the profile, and must be a unique name. The protocol property and value depend on the protocol used to perform discovery.

The protocol\_name should be <IPMI | SNMPv1v2c | SNMPv3 | WS-Man | SSH | HTTPS>

For IPMI, the properties are:

- ipmi\_user
- ipmi\_password
- ipmi\_key

For Redfish, the properties are:

- redfish\_user
- redfish\_password
- redfish\_port
- redfish\_validate\_cert

For WS-Man, the properties are:

- wsman\_port
- wsman\_user
- wsman\_password
- wsman\_validate\_cert (its value must be true or false)

For HTTPS, the properties are:

- https\_port
- https\_user
- https\_password
- https\_validate\_cert (its value must be true or false)

For SSH, the properties are:

- ssh\_port
- ssh\_user
- ssh\_password
- ssh\_validate\_cert

For SNMPv1v2c, the property is snmp\_community\_string. (Required).

For SNMPv3, the properties are:

- snmp\_user (Required)
- snmp\_authentication\_password
- snmp\_encryption\_password

For WMI, the properties are:

- wmi\_domain
- wmi\_user
- wmi\_password

## update\_profile

Usage:

```
ompc_cli update_profile [-description <description>] [<pair of protocol property and value options>] <profile_name> [<new_profile_name>]
```

The update\_profile command updates an existing discovery profile identified by profile\_name in OMPC. The semantics of the command options are the same as those in add\_profile. The protocol property set that can be updated depends on the protocol supported by this profile. If new\_profile\_name is provided, the profile\_name is updated to the new\_profile\_name.

## add\_device

Usage:

```
ompc_cli add_device [-device_name <device_name>] [-description <description>] [-size <size>] [-estimated_max_power <estimated_max_power>] -device_type <SERVER | PDU | UPS | UNSUPPORTED | CHASSIS | HYPERVISOR> [-model <model>] [-profile <profile-name>] [-protocol <protocol_name>] [<pair of protocol property and value options>] [host_name or ip]
```

The add\_device command adds a device to OMPC by using the profile name-identified profile or by using related protocol information directly supplied through the command option. You cannot enter -profile and -protocol at the same time.

The device\_name is optional, and if not provided, OMPC generates a device\_name (following the same rule as in network discovery). For unsupported devices, the default auto-generated device\_name is *Unsupported*. To ensure unique identifiers, OMPC appends numbers to the device name.

The [host\_name or ip] option is required, except when the device\_type is *Unsupported*.

The -model option is valid only when the type is *Unsupported*.

## update\_device

Usage:

```
ompc_cli update_device [-description <description>] [-size <size>] [-estimated_max_power <estimated_max_power>] [-host_name <host_name>] [-ip <ip>] [<pair of protocol property and value options>] <device_name > [<new_device_name>]
```

The `update_device` command updates device information identified by its `device_name`. If `new_device_name` is provided, the `device_name` is also updated to the `new_device_name`. [<pair of protocol property and value options>] depends on the protocol supported by this device.

## rediscover\_device

Usage:

```
ompc_cli rediscover_device [-service_tag <stag>] [<device_name>]
```

The `rediscover_device` command lets OMPC connect with the device and refresh properties that might be changed on the device side (for example, power capability and device model).

After rediscovery, the **Time of Discovery** is updated to the time of rediscovery.

For the Chassis Management Controller (CMC), if you try to rediscover the CMC before adding it to the rack, the blades inside it are not enumerated. If you are rediscovering a CMC after it is added to rack, the blades are enumerated.

You cannot use `-service_tag` and `device_name` at the same time.

If the device is an unsupported device (`device_type` is *Unsupported*), the CLI displays the error, "CLI does not allow rediscover for unsupported devices."

## find\_device

Usage:

```
ompc_cli find_device [-service_tag <stag>] [<device_name>]
```

The `find_device` command is used to list all groups' name (fully qualified) the device identified by service tag or `device_name` belongs to.

`service_tag` command option is supported.

## remove\_profile

Usage:

```
ompc_cli remove_profile <profile-name>
```

The `remove_profile` command removes a discovery profile.

## delete\_device

Usage:

```
ompc_cli delete_device [-service_tag <stag>] [<device_name>]
```

The `delete_device` command deletes a device. You cannot use `-service_tag` and `device_name` at the same time.

If the device is a chassis, it is deleted like a group (if the blades in it are already enumerated). The chassis itself is also deleted from OMPC, and is no longer visible on the **Devices** page.

## add\_group

Usage:

```
ompc_cli add_group [-description <description>] -group_type <DC|ROOM|AISLE|RACK|CUSTOM> [-capacity <capacity>] [-total_power_capacity <power_capacity>] GROUP_PATH
```

The `add_group` command adds a new group identified by `GROUP_PATH`. If the type is `RACK`, you must supply the `<capacity>` option.

Forward slash (/) cannot be used as `GROUP_PATH` in the `add_group` command.

The chassis can be added to any group at any time. You can only add Chassis Management Console (CMC) to one rack; not multiple racks.

When you add CMC to any group, the blades inside it can be enumerated.

## delete\_group

Usage:

```
ompc_cli delete_group [-preview] GROUP_PATH
```

The `delete_group` command deletes a group identified by `GROUP_PATH`. All devices in this group are removed. The devices still exists on the **Devices** page and in other groups that contain them.

All subgroups are removed from this group. If a subgroup belongs to multiple parent groups, this subgroup still exists in the other parent groups. If the subgroup no longer belongs to any parent group (after being removed from the current parent), this subgroup is deleted from OMPC. This also applies to the group itself.

If the `[-preview]` option is given, a summary of the groups, devices, and policies impacted is display. No deletion occurs.

- The summary includes the number of impacted devices, number of impacted groups, and number of impacted policies.
- All subgroups under the specified group path are counted in the summary irrespective of whether they are deleted from OMPC or not deleted. It is possible that a subgroup could be removed from the specified group path, but can not be deleted from OMPC due to a reference from another parent group.
- All devices and subgroups are counted in the summary and not only the direct children of a specified group.
- Any policies that you added to the impacted devices are not counted in the summary, because the devices are not deleted from OMPC, and these policies remain on these devices.

Example Summary:

- Number of impacted devices: 5
- Number of impacted subgroups: 10
- Number of impacted policies: 3

You can delete a chassis as a group with the `delete_group` command. In this case, after successful removal, the chassis is kept on the **Devices** page as a device, but it no longer appears as a group if there is no other group containing this chassis (if there is no connection between the chassis and the blades inside it).

## update\_group

Usage:

```
ompc_cli update_group [-description <description>] [-group_type <DC|ROOM|AISLE|CUSTOM|RACK>] [-capacity <capacity>] [-total_power_capacity <power_capacity>] GROUP_PATH [new_group_name]
```

The `update_group` command updates the properties of an existing group identified by `GROUP_PATH`. The `-capacity` and `-total_power_capacity` options are valid only when the group to be updated is a rack. The `-group_type` of a rack cannot be updated, and no other type of group can be updated to be a rack.

If `new_group_name` is provided, the CLI updates the name of the group to the new name. The group can belong to another group. If this is the case, the rename operation may fail because of the name confliction.

The chassis can be regarded as group, so the CLI allows updates to the properties of the chassis through the `update_group` command. You can only update the chassis' description and name through the `update_group` command. You cannot update other types of groups to be a chassis.

The name must be unique across devices and groups under the same parent group.

You cannot use "/" as `GROUP_PATH` in the `update_group` command.

## add\_device\_to\_group

Usage:

```
ompc_cli add_device_to_group [-slot <slot_num>] [-service_tag <stag>] [<device_name >]
GROUP_PATH
```

The `add_device_to_group` command adds a device to a group. If a device is added to a rack, the `slot_num` option is used to specify into which slot the device is added. If the value of the slot is -1, the system chooses a slot automatically. When adding UPS/PDU, if you do not provide a slot option, the UPS/PDU is attached to the rack. For adding a server or chassis to rack, `-slot` is allowed (when not provided, the system chooses a slot automatically). If adding a server or chassis to other groups, `-slot` is not allowed (an error is displayed).

Slots start from 1 (0 is an invalid slot number).

PDU and UPS can only be added to a rack. For PDU and UPS in other types of groups in a previous OMPC release, if the you upgrade the data, you must remove PDU and UPS from those groups after upgrading.

The `add_device_to_group` command does not move a device from one group to another group. This is done by `move_device`.

If a device already belongs to a group, you can use the `add_device_to_group` command to add the device to another group. After successfully adding the device, this device belongs to both the old group and the new parent group. The exception is that devices can only belong to one rack (not multiple racks), and blades can only belong to one chassis (not multiple chassis). You cannot add blades to a chassis with the `add_device_to_group` command.

When a chassis is added to any group, the blades inside the chassis is enumerated and the chassis becomes a group that contains all of the blades inside it.

## remove\_device\_from\_group

Usage:

```
ompc_cli remove_device_from_group [-service_tag <stag>] [<device_name >] GROUP_PATH
```

The `remove_device_from_group` command removes a device from a group identified by `GROUP_PATH`.

You can remove a chassis (as a device) from a group.

If a device belongs to multiple groups, after you remove it from one group, it still belongs to other groups.

A chassis can be removed through this command. In this case, the behavior is the same as removing a chassis by using the `delete_group` command.

## move\_device

Usage:

```
ompc_cli move_device [-service_tag <stag>] [<device_name >] [-slot <slot_num>]
FROM_GROUP_PATH TO_GROUP_PATH
```

The `move_device` command moves a device from `FROM_GROUP_PATH` to `TO_GROUP_PATH`. After successfully moving the device, the device no longer belongs to `FROM_GROUP_PATH`; it belongs to `TO_GROUP_PATH`.

The slot option is applicable only when moving a device (including a chassis) to a rack. It specifies which slot the device should be moved into. If it is not provided when moving a device to a rack, the CLI identifies a slot.



When moving a UPS/PDU from one rack to another rack and the slot is not provided:

- If the UPS/PDU is in a slot of a previous rack, the CLI selects one slot in the new rack.
- If the UPS/PDU is attached in a previous rack, the CLI attaches it in the new rack.

When moving a UPS/PDU from one rack to another rack and you have specified the slot:

- If the UPS/PDU is in a slot of a previous rack, the CLI uses the specified slot in the new rack.
- If the UPS/PDU is attached in a previous rack, the CLI reports an error.

You cannot change the UPS/PDUS properties between “slotted” and “attached” in Power Center. You can change between “slotted” and “attached” by removing the UPS/PDU from the rack, and re-adding it to the rack.

If the device to be moved is a chassis, the behavior is the same as moving it through the `move_group` command.

You cannot use the attributes `-service_tag` and `device_name` at the same time.

If the move operation fails, the device stays in the original group. There are exceptions for critical situations such as power failures, crashes, network failures for the remote database, and local network failures.

## move\_group

Usage:

```
ompc_cli move_group FROM_GROUP_PATH TO_GROUP_PATH
```

The `move_group` command moves a group from `FROM_GROUP_PATH` to `TO_GROUP_PATH`.

You cannot use the same group path as `FROM_GROUP_PATH` to `TO_GROUP_PATH`. Also, you cannot use “/” as `FROM_GROUP_PATH`.

After successfully moving a group, the group identified by `FROM_GROUP_PATH` no longer belongs to the original parent in `FROM_GROUP_PATH`. It belongs to `TO_GROUP_PATH`.

When moving a chassis to a rack, the CLI chooses one available slot (if a slot is available). If you want to specify a slot for the chassis in the new rack, you must use the `move_device` command.

If the move operation fails, the device stays in the original group. There are exceptions for critical situations such as power failures, crashes, network failures for the remote database, and local network failures.

## add\_group\_to\_group

Usage:

```
ompc_cli add_group_to_group GROUP_PATH TO__GROUP_PATH
```

The `add_group_to_group` command adds a group identified by `GROUP_PATH` to `TO_GROUP_PATH`. If the source group path also belongs to another parent group, after successfully adding the group, the source group belongs to both the old group and the new parent group. The exception is that a chassis can only belong to one rack (not multiple racks).

You cannot add groups to a rack (except for the chassis, which is a device before it is added to a rack, then a group after it is added to a rack).

When adding a chassis to a rack, the CLI chooses an available slot (if there is one available). If you want to specify a slot for the chassis in the rack, you must use the `add_device_to_group` command.

## List commands

The following are generic rules for list commands:

- The output of list commands is a simple table-like structure, where a comma-delimited list of column names will be output first, followed by the data, in comma-delimited format. There is one line per record. If a piece of data is not applicable or available, that data is represented by two commas next to each other (NULL field).
- Line breaks (CRLF) in the output fields must be replaced with spaces.

- Fields containing double quotes and commas must be enclosed in double quotes.
- If a double quote appears inside a field, it must be escaped by preceding it with another double quote. For example: “aaa”, “b””bb”, “ccc”.

## list\_device\_props

Usage:

```
ompc_cli list_device_props [-service_tag <servtag>]    [<device_name>]
```

The `list_device_props` command lists all properties for the device identified by `servtag` or `device_name`. Properties include `service_tag`, `protocol`, `protocol properties`, `device name`, `address (IP or host name)`, `model`, and `device type` (device name is the first column).

Secret data (password/key) is not listed as a protocol property.

## list\_devices

Usage:

```
ompc_cli list_devices [GROUP_PATH]
```

The `list_devices` command lists all devices immediately under the `GROUP_PATH`. If no `GROUP_PATH` is supplied, then the CLI lists all devices, connected or not, that are managed by OMPC. Properties include all properties of the `list_device_props` command, except for protocol information (the first column has the device name).

If “/” is provided as `GROUP_PATH`, the CLI lists the devices at the root level.

## list\_group\_props

Usage:

```
ompc_cli list_group_props GROUP_PATH
```

The `list_group_props` command lists all properties for a group identified by `GROUP_PATH`. Properties include `group_type` (DC, room, rack, aisle, etc.), `description`, and additional properties unique to that group type. For example, for rack, the additional properties include `capacity` and `total power capacity`.

This command does not apply to “/”.

## list\_groups

Usage:

```
ompc_cli list_groups [-unique] [GROUP_PATH]
```

The `list_groups` command lists all child groups for the `GROUP_PATH` (immediate only). If no `GROUP_PATH` is supplied, the CLI lists all group paths or all unique groups in OMPC. Properties include the fully-qualified group name, group type, and `member_count`. The `member_count` property is the number of devices and groups immediately under the child group.

`[-unique]` has no impact if `GROUP_PATH` is provided.

If “/” is provided as `GROUP_PATH`, then the CLI lists the groups at root level.

A group might have multiple fully-qualified group names. When `[-unique]` is provided, the CLI lists all unique groups; otherwise, the CLI lists all group paths.

Example output for `list_groups`:

```
group_name, group_type, member_count
myservers/mygroup, Room, 20
```

## list\_report\_groups

Usage:

```
ompc_cli list_report_groups
```

The `list_report_groups` command is used to list all report groups. Each report group is output in one row containing these fields: `report_group_name`, `description` and `created_by`.

## list\_reports

Usage:

```
ompc_cli list_reports [REPORT_GROUP]
```

The `list_reports` command is used to list user defined reports. `REPORT_GROUP` is the name of a report group. If no `REPORT_GROUP` is supplied, all reports are listed. Else, only those belonging to the specified `REPORT_GROUP` are listed.

Each report is output in one row containing these fields: `report_name`, `description`, `format`, `report_group_name`, `created_by` and `status` (running or not).

## run\_report

Usage:

```
ompc_cli run_report [-start_date <start_date>] [-end_date <end_date>] [-format <CSV|XML>] [-file_name <file_name>] [-detail] REPORT_NAME
```

The `run_report` command is used to run a saved report and export the result to the console or to a file.

The `REPORT_NAME` is mandatory and specifies which saved report are run.

The options `-start_date` and `-end_date` are optional: When supplied, they are used to run the report in precedence to the time range saved with the original report setting. If only `-start_date` is supplied, the current time is used as the end of the time range. If only `-end_date` is supplied, the earliest time of monitoring data is used as the beginning of the time range.

If `-file_name` is not supplied, the result is displayed in the console in CSV format, ignoring whatever format setting saved with the report or specified by the `-format` option.

If `-file_name` is supplied, the result is saved to the file in the format specified by the option `-format`. If `-format` is not supplied, the format saved with the report is used.

The `-detail` option is only applied to a "Power HeadRoom" report for exporting the calculation details of the stranded power.

After a report is run successfully, the report result is displayed in the console or saved to a file specified by `<file_name>`. Else, an error message is displayed.

## discover\_device

Usage:

```
ompc_cli discover_device -profile <profile-name> [-ip <ip>] [-host_name <host_name>] [-network_mask <network_mask>] [-end_ip <end_ip>]
```

The `discover_device` command is used to discover devices and automatically add the discovered devices to OMPC. This command supports only HTTPS profile.

The `-ip` and `-host_name` options must be supplied.

When `-ip` is supplied, the `-network_mask` must be supplied. The `-end_ip` is only acceptable when `-ip` is supplied.

If `-end_ip` is supplied, the discovery is performed for the IP range of `<ip>-<end_ip>`. Else, the discovery is performed for the single address `<ip>`.

After a discovery is complete, the discovered devices are added to OpenManage Power Center automatically and the count is displayed in the console. If the device discovery fails, an error message is displayed.

## backup\_database

Usage:

```
ompc_cli backup_database -path <path> -encrypt_password <encrypt_password> [-quiet]
```

The `backup_database` command is used to initiate the OMPC database backup.

The `-path` and `-encrypt_password` options must be supplied.

The database backup is complete and is saved in the common network share location.

## restore\_database

Usage:

```
ompc_cli restore_database -path <path> -encrypt_password <encrypt_password> [-quiet]
```

The `restore_database` command is used to initiate the OMPC database restoration.

The `-path` and `-encrypt_password` options must be supplied.

The database restore process is complete.

## add\_ssh\_server\_key

Usage:

```
ompc_cli add_ssh_server_key [-host_names <host_names>] [-key_type <key_type>] [-ssh_key <ssh_key>] <key_name>
```

The `add_ssh_server_key` command is used to add SSH keys to OMPC for device authentication.

The `-key_type`, `-host_names`, and `-ssh_key` are the supported command options.

The ssh server key is successfully added to OMPC.

## remove\_ssh\_server\_key

Usage:

```
ompc_cli remove_ssh_server_key <key_name>
```

The `remove_ssh_server_key` command is used to remove a SSH key specified by the from OMPC.

The ssh server key is successfully removed.

## list\_ssh\_server\_key

Usage:

```
ompc_cli list_ssh_server_key [-long] [<key_name>]
```

The `list_ssh_server_key` command is used to list SSH keys which are used by OMPC for server authentication.

The ssh keys used by OMPC for server authentication is successfully listed.

For example, `list_ssh_server_key -long 77s0d8f8sd89sd90099988s0d`, where `-long <ssh_key >` is used or `list_ssh_server_key XXXXX1`, where `<key_name>` is used.

# Command line interface error codes

An error code appears when one of the following two conditions occurs:

- The CLI identified an error, such as a command or command option validation error. The error code is generated by the CLI. The module number for the CLI is 0xEE. An error number for each command and option is displayed.
- An OpenManage Power Center back-end error occurs. In this situation, the error code from the server is returned by the CLI.

The error codes use the following format:

```
8E|Module|Related Module (Optional)|Detail (Optional)
```

OMPC modules and error codes:

- OMPC Database — 0x01
- DCM SDK — 0x02
- OMPC UI asset — 0x03
- DC Modeling — 0x04
- Overview — 0x05
- Monitoring — 0x06
- User Accounts — 0x07
- Setting — 0x08
- Event — 0x09
- Discovery — 0x0A
- License — 0x0B
- Policy — 0x0C
- Connection Pool — 0x0D
- Role/ Privilege — 0x0E
- Login/ Logout — 0x0F
- Profile — 0x10
- Available List — 0x11
- Security — 0x12
- Paging/Sorting/Filtering — 0x13
- Configuration — 0x14
- Unit Handler — 0x15
- Infrastructure — 0x16
- Unknown — 0xFF

# Access control

This chapter provides information about access control in OpenManage Power Center, including:

- Log in/Log out — Log into OpenManage Power Center by entering user account credentials.
- User/Role/Privilege Management — After logging in, you can manage user accounts from the **Settings > Users** screen of the management console. OpenManage Power Center provides role-based access control; to use these controls, set up roles first, and then define the privileges for each role. Then, you can set up OpenManage Power Center accounts and assign them to different roles.
- Licensing — OpenManage Power Center requires a valid license. Once the trial license expires, you may have to import a permanent license.


## Topics:

- [About authentication](#)
- [Logging in](#)
- [Logging out](#)
- [Managing user roles and privileges](#)
- [Managing user accounts](#)
- [Viewing current user information](#)

## About authentication

OpenManage Power Center supports both OpenManage Power Center users and Windows and Linux users.

For cross-domain authentication, domains must be two-way transitively trusted by the domain in which the OpenManage Power Center server is installed. Authentication of user accounts in domains that are one-way trusted or not trusted by the domain in which the OpenManage Power Center server is installed is not supported and may fail.




 **NOTE:** The password must be a minimum of eight characters, with characters from at least three of the following categories: uppercase, lowercase, numeric, and non-alphanumeric. The password can include spaces.

## Logging in


OpenManage Power Center supports both OpenManage Power Center-managed users and authenticated Microsoft Windows and Linux users.

## Logging in with a user name and password

To log into OpenManage Power Center with a user name and password, use one of the following accounts:

- Power Center Account — You can create this account in OpenManage Power Center. When logging into OpenManage Power Center for the first time, you must use the Power Center user account created during installation.
  -  **NOTE:** Before logging into OpenManage Power Center using either the Windows domain or the Windows local account, you must add the account into OpenManage Power Center by accessing the **Settings > Users** screen. For further information, see [Adding A User Account](#).
  -  **NOTE:** You cannot log into OpenManage Power Center using SSO on the OpenManage Power Center server. You only can log into OpenManage Power Center using SSO remotely.
  -  **NOTE:** You must add the SSO user account to OpenManage Power Center before you can log in using SSO. You skip the login page and enter the **Home** page directly using SSO.
- Windows Domain Account — Windows domain account.

- Windows Local Account — Windows local account on the OpenManage Power Center server.
- Linux Local Account — Linux local account on the OpenManage Power Center server.

 **NOTE:** OpenManage Power Center requires that SSL is enabled at the LDAP server, if not, the authentication fails.

 **NOTE:** LDAP authentication must be enabled in the **Directory Settings** screen. See [Editing Directory Settings](#).

- LDAP Account

For more information on how to open the OpenManage Power Center management console, see [Launching Power Center In Windows](#) or [Launching Power Center In Linux](#).

## Logging in with a Power Center account

1. Enter the **User Name** and **Password** of the OpenManage Power Center account.
2. Select **OMPC Account** (default) from the **Login using** drop-down list.
3. Click **Login**.

## Logging in with a Windows domain account

1. Enter the **User Name** and **Password** of the Windows domain account.
2. Select **Windows Domain Account** from the **Login using** drop-down list.
3. Enter the **Domain** name for the Windows domain account.
4. Click **Login**.

## Logging in with a Windows local account

1. Enter the **User Name** and **Password** of the Windows local account.
2. Select **Windows Local Account** from the **Login using** drop-down list.
3. Click **Login**.

## Logging in with a Linux local account

1. Enter the **User Name** and **Password** of the Linux local account.
2. Select **Linux Local Account** from the **Login using** drop-down list.
3. Click **Login**.

## Logging in with an LDAP account

 **NOTE:** The LDAP Account type is only available when LDAP authentication has been enabled in [Directory Settings](#).

1. Enter the **User Name** and **Password** of the LDAP account.
2. Select **LDAP Account** from the **Login using** drop-down list.
3. Click **Login**.

## Logging in with Single Sign-on (SSO)

SSO uses centralized authentication servers that other applications and systems use for authentication purposes together with other techniques to ensure that you do not have to enter their credentials more than once. Kerberos SSO requires specific settings for web browsers. Configure your web browser for SSO support. For more information, see configuration steps for Internet Explorer 10 in [Configuring Web Browsers For Single Sign-on](#), or for instructions on SSO configuration in other web browsers, consult the appropriate browser help documentation. Additionally, for a list of OpenManage Power Center-supported web browsers, see [System Requirements](#).

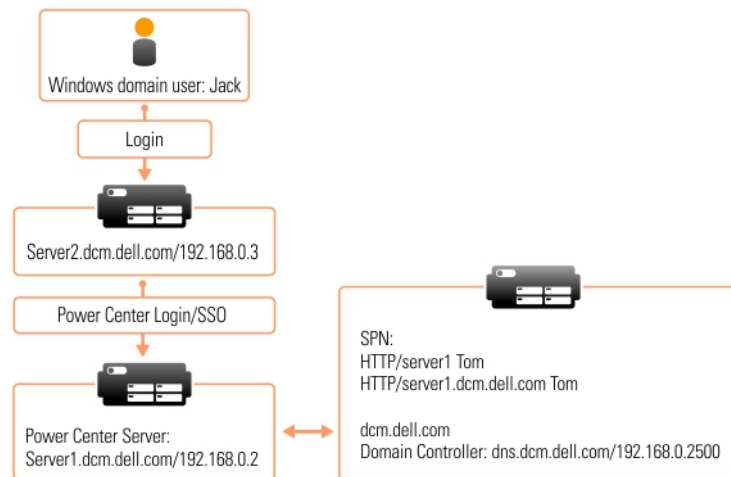
The following is an example of configuration steps in Microsoft Internet Explorer 10 or 11:

**NOTE:** Kerberos SSO may not work if you launch Power Center services using an account other than Network Service.

## Single domain environment

You can set up a single domain environment with the following components:

- Domain Controller — AD server that supports the domain (parent and child)
- Power Center Server — Server with Power Center installed
- Power Center Client — Client server that connects to the Power Center server



**Figure 2. Single domain environment**

To set up the Kerberos SSO single domain environment, install Power Center and [configure your web browser for SSO](#).

## Configuring web browsers for Single Sign-on

To enable Kerberos Single Sign-on (SSO), you must configure your web browser to support the feature. For more information, see your web browser Help documentation. For a list of OpenManage Power Center-supported web browsers, see [System Requirements](#).

**NOTE:** To correctly set up Kerberos SSO, the date and time on all involved computers must be consistent and DNS configuration must be correct.

To support SSO in Internet Explorer, you must add the OpenManage Power Center server as a local Intranet site.

The following is an example of the configuration steps in Microsoft Internet Explorer 10:

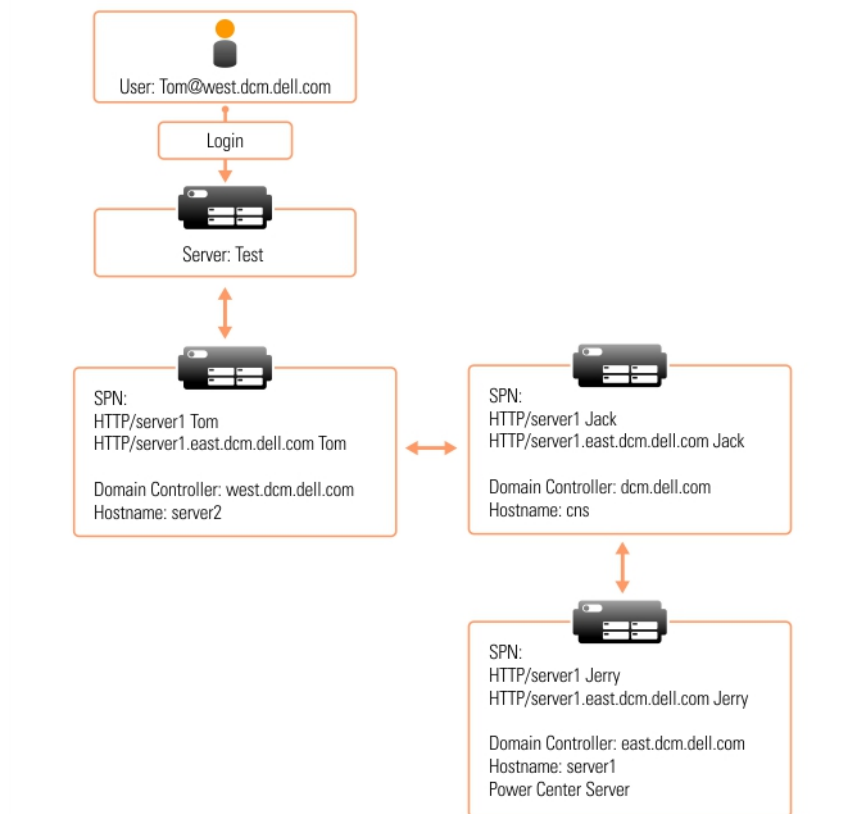
1. Go to **Internet Explorer 10 > Internet Options > Security > Local Intranet**, and click **Sites**. The **Local Intranet** window opens.
2. Click **Advanced**.
3. Add your Power Center site into **Local Intranet**—for example, *server1.dcm.dell.com*.

## Multiple domain environment

Set up a multiple domain environment with the following components:

- Domain Controller — There can be several Windows Active Directory (AD) domain controllers; for example, a parent domain and many child domains.
- Power Center Server — This is the server with Power Center installed. It is an AD domain controller.
- Power Center Client — The client server connects to the network of the Power Center server.





**Figure 3. Multiple domain environment**

To set up the Kerberos SSO multiple domain environment:

1. Install Power Center.
2. [Configure your web browser for SSO.](#)

## Windows NT LAN Manager (NTLM) authentication limitation

OpenManage Power Center supports Kerberos SSO for Windows domain user authentication. To enable this feature, OpenManage Power Center is configured to support the Windows integrated authentication option which includes two authentication mechanisms: Kerberos and NTLM .

NTLM is not supported in OpenManage Power Center. If the client's web browser uses NTLM to authenticate domain users for OpenManage Power Center, there are some limitations.

The web browser displays a message box requiring a Windows user name and password.

- If you click **OK** after entering a user name and password, whether the information is correct or not, the OpenManage Power Center login page is displayed and requires you may have to authenticate through the login page.
- If you click **Cancel**, an HTTP Status 401 failure displays, and you cannot log into Power Center.

See [Troubleshooting](#) for more information on how to resolve this issue.

## Logging out

To log out of OpenManage Power Center when not logged in through Kerberos SSO, click **Logout** at the upper right corner of the management console.

When logged in through Kerberos SSO, close the web browser or the OpenManage Power Center management console to log out. Clicking **Logout** does not work.

# Managing user roles and privileges

OpenManage Power Center supports three pre-defined roles:

- **Administrator:** All privileges
- **Power User:** All privileges except *Manage role/user* and *Manage license*
- **Guest:** *View device/group* privileges only


These pre-defined roles cannot be edited or deleted.

 **NOTE:** Only users with the *Role/User Management* privilege can add, edit, or delete a role or user or group account.

## Adding a custom role

1. In the left pane, click **Settings > Roles**.
2. Click **Add a Role**.  
The **Add Role** window is displayed.
3. Enter a name for the role in the **Role Name** text box. Ensure that the name does not exceed 50 characters.
4. Enter a description for the role in the **Role Description** text box. Make sure that the description does not exceed 1024 characters. This field is optional.
5. Under **Select Privileges**, select the check box next to the rights that you want to assign to the role. The available options are:
  - **Global Configuration**
  - **Manage Role/User**
  - **View Device/Group**
  - **Manage Device/Group**
  - **Manage Policy**
  - **Manage Event/Log**
  - **Manage License**
  - **Manage Report**
  - **Execute Power Task**
  - **Manage Power Task**
  - **Backup Database**
6. Click **Save** to add the custom role, or click **Cancel** to discard your changes and return to the **Roles** tab.

## Editing a role

 **NOTE:** You cannot edit a predefined role.

1. In the left pane, click **Settings > Roles**.
2. Select the check box next to the role you want to edit and click **Edit**.  
The **Edit Role** window is displayed.
3. Make the required changes to the **Role Name**, **Role Description**, and **Select Privileges** fields for this role.
4. Click **Save** to save your changes, or click **Cancel** to discard them and return to the **Roles** tab.

## Deleting a role

1. In the left pane, click **Settings > Roles**.
2. Select the check box next to the role you want to delete and click **Delete**.  
The following message is displayed.

Are you sure you want to delete the selected item(s)?

3. Click **Yes** to confirm the deletion, or click **No** to discard the delete task.

## Privileges

Each pre-defined role is associated with a set of specific *privileges*. Additionally, you can create custom roles with one or more of the following privileges:

- Global Configuration
- Manage Role/User
- View Device/Group
- Manage Device/Group
- Manage Policy
- Manage Event/Log
- Manage License
- Manage Report
- Execute Power Task
- Manage Power Task
- Database Backup

Every Power Center screen functions differently depending on the privilege level assigned to a user account:

- Fully functional—User can view and edit all.
- Partially functional—User can partially view or edit.
- Not functional—User sees a blank page.

## Global Configuration

The *Global Configuration* privilege enables a user to change the Power Center global configuration—for example, the sampling interval and database settings. Users without this privilege can only view part of the **Settings** page, and cannot make any changes (the **Edit** option is not available).

## Manage Role/User

Users with the *Manage Role/User* privilege can:

- Create roles
- Delete roles
- Update roles
- Create users
- Delete users
- Update users

Users without this privilege can only view their own user account information and update the password.

## View Device/Group

The *View Device/Group* privilege enables a user to view all device and group information. Users without this privilege cannot view device or group information; they can only view the **Settings** page.


Users with only the *View Device/Group* privilege have the following restrictions:

- The **Run Discovery** task is not available.
- Add/Edit/Delete functionality is disabled on the **Devices** screen.

## Manage Device/Group

The *Manage Device/Group* privilege enables a user to:

- Create groups
- Create a Data Center/Room/Aisle/Rack/Device
- Associate Data Center/Room/Aisle/Rack/Device/Group
- Manage a device
- Remove a device/group from the Device List


 **NOTE:** When you assign the *Manage Device/Group* privilege to a user, Power Center automatically assigns the *View Device/Group* privilege to this user as well.

Users without this privilege can view all devices and group information, but cannot add/delete/edit/manage the devices and groups.

## Manage Policy

The *Manage Policy* privilege enables a user to:

- Add/remove a policy
- Update a policy
- Start/stop Emergency Power Reduction on a device or group


 **NOTE:** To manage a policy, you must also have the *View Device/Group* privilege.

Users without this privilege cannot see the **Policies** screen.

## Manage Event/Log

The *Manage Event/Log* privilege enables a user to:

- Add/Remove an event condition (threshold)
- Update an event condition (threshold)
- Remove an event
- Manage event logs

 **NOTE:** To manage an event, you must also have the *View Device/Group* privilege.

Users without this privilege can view event information and add comments to events, but cannot delete events or see the **Thresholds** values from the **Devices** screen.

## Manage License

The *Manage License* privilege enables a user to:

- Manage a license
- Purchase a license if required
- Import a license
- Delete a license

## Manage Report

The *Manage Report* privilege enables a user to:

- Manage reports
- Add reports
- Delete reports
- Export reports

## Execute power task

The *Execute Power Task* privilege enables a user to:

- Create power control tasks
- Perform power control task

## Manage power task

The *Manage Power Task* privilege enables a user to:

- Manage power control tasks
- View power control task
- Edit power control task
- Re-run power control task
- Stop power control task
- Delete power control task

## Backup Database

The *Backup Database* privilege enables a user to:

- Manage database policies
- Schedule database purge
- Configure and schedule database backup

# Managing user accounts

You can create users and assign them to different roles.

If you have the *Manage Role/User* privilege, you can add, edit, or delete a user in OpenManage Power Center.

## Adding a user account

1. In the left pane, click **Settings > Users**.



**NOTE:** If OpenManage Power Center is installed on a Windows Active Domain Controller server, every user account added on this server should be a **Windows Domain Account**.

2. Click **Add a User/Group**.  
The **Add a User or Group Account** window is displayed.
3. Select the **A user** option.

4. Select **Account Type** and enter the required credentials:


The available options are:

*For both Windows and Linux installations:*

- OMPC Account
  - Enter a unique **User Name** for the account.
  - Enter a **Password** that is at least eight characters long and includes characters from at least three of the following categories: uppercase, lowercase, numeric, and nonalphanumeric.
  - Re-enter the password in the **Verify Password** text box to confirm.

*For a Windows installation:*

- Windows Local Account — Enter a unique **User Name** for the account.


 **NOTE:** If Power Center is installed on a Windows 2012 Essential server and the server is configured as a Domain controller, all user accounts on the server must be Windows Domain Accounts, and not Windows Local Accounts.

- Windows Domain Account


- Enter a unique **User Name** for the account.
- Enter a valid Windows **Domain Name**.

*For a Linux installation:*

- Linux Local Account — Enter a unique **User Name** for the account.

 **NOTE:** While Linux Local Accounts can be changed from the Linux server, these changes are not mirrored in the same local account that was added to Power Center, and Power Center authentication attempts on this account fails. To keep the Linux Local Account in sync between Power Center and the Linux server when the local account is changed from Linux, the original account must be deleted from Power Center and the changed account must be created in Power Center as a new Linux Local Account.

- LDAP Account — Enter a unique **User Name** for the account.

 **NOTE:** A user description is useful when there are two users with the same user name. Two user accounts with the same user name are only possible where the user types are different.

5. Enter a description of this user account (optional) in the **Description** text box.
6. From the **Roles** drop-down list, select the user and group roles. If the role you want is not available in the drop-down list, click **Create New** to open the **Add Role** wizard. For more information, see *OpenManage Power Center User's Guide*.
7. Click **Save** to add the user account, or click **Cancel** to discard your changes.


## Adding a group account

1. In the left pane, click **Settings > Users**.
2. Click **Add a User/Group**.  
The **Add a User or Group Account** window is displayed.
3. Select the **A group** option.
4. Select a group **Account Type**.  
The available options are:
  - *Windows Local Group*
  - *Windows Domain Group*
5. Enter a unique group user name in the **User Name** text box.
6. Enter a description of the group account (optional).
7. If you select the **Windows Domain Group** account type, enter a valid Windows domain name in the **Domain** name text box.
8. Select between one and four user roles and privileges. If the role you want is not available in the drop-down list, click **Create New** to open the **Add Role** wizard. For more information, see *OpenManage Power Center User's Guide*.
9. Click **Save** to add the new group, or click **Cancel** to discard your changes.

## Editing a user or group account

1. In the left pane, click **Settings > Users**.
2. Select the check box next to the user or group account that you want to edit, then click **Edit**.  
The **Edit a User or Group Account** window is displayed.
3. Make the required changes, then click **Save** to save your changes, or click **Cancel** to discard them and return to the **Users** tab.

## Deleting a user or group account

 **NOTE:** You cannot delete the Power Center managed user (super user) created during installation.

1. In the left pane, click **Settings > Users**.
2. Select the check box next to the user or group account you want to delete.
3. Click **Delete**.  
The following message is displayed: **Are you sure you want to remove the selected item(s)?**
4. Click **Yes** to proceed or **No** to return to the **Users** tab.

## Changing a user account password

Do one of the following:

- Change the password of the current user.
  1. In the top right hand-side of the OpenManage Power Center screen, click the user account name with which you are currently logged in. The **Current User** window is displayed.
  2. Enter the current password in the **Current Password** text box.
  3. Enter the new password in the **New Password** text box.
  4. Enter the new password again in the **Verify Password** text box to confirm.
  5. Click **Save** to apply the new password or click **Cancel** to discard your changes.
- Change any user or group account password on the **Settings > Users** screen.
  1. Click **Settings > Users** and select the check box next to the user account whose password you want to change.
  2. In the task menu, click **Edit**.
  3. Enter the new password in the **Password** text box.
  4. Enter the new password again in the **Verify Password** text box to confirm.
  5. Click **Save** to change the password, or click **Cancel** to discard your changes.

## Viewing current user information

You can view current user information and update the current user's password.

To view current user information, click the login user name in the upper-right corner of the OpenManage Power Center screen, or go to **Settings > Users**.

To change the current user password, see [Changing A User Or Group Account Password](#).

# Task management

The Tasks feature enables you to perform device discovery and power control tasks such as power-on and power-off, on a specific device or a group of devices.


In the left pane, click **Tasks**. The **Tasks** screen comprises the following tabs:

- Discovery Tasks
- Power Control Tasks

By default, the **Discovery Tasks** tab is displayed.

On the **Tasks** screen you can:

- Create new discovery and power control tasks
- Edit or delete discovery and power control tasks
- Start, stop, or re-run discovery and power control tasks
- Refresh the list of discovery or power control tasks
- View the summary of the discovery or power control tasks

 **NOTE:** If you schedule a task at a non-existent time when the daylight saving is effective, the Web browsers align themselves to the accurate time.

## Topics:

- [Discovery tasks](#)
- [Power control tasks](#)
- [Protocol profile](#)

## Discovery tasks

The *Device Discovery* privilege enables you to discover network devices. Users without this privilege can view the **Devices** screen, but cannot make any changes.


To manage devices in OpenManage Power Center, you must have *Manage Device/Group* privileges, and you must first add the devices to the OpenManage Power Center management console. OpenManage Power Center discovers devices using IP ranges and collects basic information about each device, such as:


- Device name
- Connection status
- Device type
- Device model
- IP address
- Hostname

This information enables you to track device status and data center information. You can also manage these discovered devices in Power Center. If there is a new or changed device in your data center, you can use the device discovery function to rediscover the devices.

There are two ways to add a device in Power Center:

- Using a single IP address or IP ranges or host names to discover devices on the network, at the scheduled time.
- Using the OpenManage Power Center management console to specify device properties and discover devices.

 **NOTE:** If you use a network security policy, the discovery function may not work properly.

 **NOTE:** When you use multiple IPMI protocols to discover 13th generation PowerEdge systems, ensure that the credentials for the protocols are correct. In case you enter an incorrect credential, use a valid credential and wait for sometime before running the discovery task again.



After a device is discovered, it is automatically added to the **Devices > All Devices** tab. The device can be assigned to a group and managed by OpenManage Power Center.

After you have created a discovery task, you can also re-run the task when needed. Discovery tasks can also be scheduled to run later or run immediately.


## Creating discovery tasks


You can create discovery tasks using the **New Discovery Task** wizard.

1. In the left pane, click **Tasks > Discovery Tasks > New Discovery**.  
The **New Discovery Task** wizard is displayed.
2. In the **Discovery Task** tab, enter a name for the discovery task.
3. If you want the discovery to cover a range of systems, select the **IP-Address Range** and specify the Subnet Mask. Else, select the **Single Device** option to run the discovery task for a single device and specify the IP address or host name of the device.

You can also select **Exclude Range** option to exclude the systems within a range. Specify the range of IPs to be excluded in **Beginning** and **End** text boxes.

You can add multiple ranges or host names (devices).

 **NOTE:** The Subnet Mask is not required for single devices.

 **NOTE:** You can also create the group hierarchy by selecting the **Replicate Device Path** option.

4. Click **Add**. The IP address range is specified at the bottom part of the screen.
5. Click **Next** to view the **Connection Protocol** tab.
6. Select the check box next to a protocol profile from the list for the discovery task or click **Add** to create a profile and click **Next**. For more information, see [Protocol Profile](#).
7. In the **Schedule Task** tab, select the **Run Now** option to start the discovery task immediately.


Alternately, you can select the **Set Schedule** option to start the discovery task at a specific interval. The possible options are:

- **Run Once** — Specify the date and time when you want the discovery task to begin.
  - **Periodic** — Specify if you want the discovery task to start hourly, daily, weekly, or at a specific interval.
- a. Select or clear the **Activate** check box to enable or disable the scheduling of the task. By default, the check box is selected. You can save an inactive task, but it is not scheduled to run.

 **NOTE:** You can edit the task to clear or select the **Activate** check box and view the status of the task in the **Discovery Tasks** tab.

- b. Under the **Range of recurrence** option, select the start and end date for the task, or select the **No End Date** option to run the task for an unlimited period.
- c. Click **Next** to view the summary of the discovery task in the **Summary** tab.

The summary comprises the name of the task, protocol used, IP ranges, and schedule.

 **NOTE:** Make sure that the browsers used for scheduling discovery tasks are daylight saving-compliant.

8. Click **Finish** to create the discovery task and return to the **Discovery Tasks** tab.

## Re-running recent discovery tasks

1. In the left pane, click **Tasks**.  
The **Tasks** window is displayed.
2. On the **Discovery Tasks** tab, select the discovery task by clicking on the checkbox.
3. Click **Re-Run**.
4. After the discovery job completes, go to the **Devices** screen, and make sure the correct devices are listed.


# Power control tasks

Power control tasks help you to manage the power-on or power-off of devices. You can schedule the time at which the power control tasks must be performed on the devices or device groups.

## Creating power tasks

You can create power tasks using the **Power Task** wizard.

1. In the left pane, click **Tasks > Power Control Tasks > New Task**.  
The **Power Task** wizard is displayed.
2. In the **Power Task** tab, enter a name for the power control task and select one of the following options:
  - **Power On**
  - **Power Off**
  - **Graceful Shutdown**
  - **Reset System (warm boot)**
  - **Power Cycle System (cold boot)**


 **NOTE:** Restarting a system forcefully is called **warm boot** while closing all the programs and shutting down a system is called **cold boot**.
3. Select the **Perform random power on commands** check box, specify the interval (in minutes) and the number of devices to which you want to apply the power task, and click **Next**.
4. In the **Associated Devices/Groups** tab, select the devices in the **All Devices** tab or in the **Groups** tab, select the device groups that you want to manage and click **Next**.
5. In the **Schedule Task** tab, select the **Run Now** option to start the power control task immediately.  
Alternately, you can select the **Set Schedule** option to start at a specific interval. The possible options are:
  - **Run Once** — Specify the date and time when you want the power control task to begin.
  - **Period** — Specify if you want the power control task to run the power control task daily, weekly, or at a specific period.
  - a. Select or clear the **Activate** check box to enable or disable the task. By default, the check box is selected. You can save a disabled task, but cannot run it.
  - b. Under the **Range of recurrence** option, select the start and end date for the task, or select the **No End Date** option to run the task for an unlimited period.
  - c. Click **Next**. Enter the iDRAC/IPMI user name and password of the device on which you want to run the power control task.
6. Click **Finish** to create the power control task and return to the **Power Control Tasks** tab.

## Protocol profile

Power Center server uses a protocol profile to communicate with devices. The protocol profile specifies the connection protocol and credential information of a device. You select a protocol profile when you discover a new device.

You can set up multiple protocol profiles for each device. Also, you can add a profile, edit an existing profile, or delete a profile.

Power Center supports the following connection protocol types, and includes several optional settings:

 **NOTE:** Get the correct protocol type and credential information from your system administrator. The user name and password for the IPMI/WS-MAN protocol must be the same as those used for the iDRAC/CMC Web console.

- **IPMI:** Select IPMI protocol for the server.
  - **IPMI User Name** — Maximum length is 16 characters
  - **IPMI Password** — Maximum length is 255 characters
  - **IPMI Key** — A string of 40 hex digits
- **Redfish:** You can also select the Redfish protocol for the server.
  - **User Name** — Maximum length is 16 characters.
  - **Password** — Maximum length is 255 characters.

- **Port** — A string of 40 hex digits.
- **Validate Certificate** — (Optional) Enables certificate validation.

**NOTE:** By default, OpenManage Power Center uses port 8643 for power center application and port 8644 for redfish HTTPS events. You also have the option to use a different port apart from the default port.

**NOTE:** In OMPC 4.0, there are restrictions in using Redfish protocol with the lockdown feature of iDRAC enabled. For more information, see [Troubleshooting](#) chapter.

- **WS-MAN:** Select the WS-MAN protocol for the chassis.

- **WS-MAN User Name** — HTTP basic user name; maximum length is 255 characters.
- **WS-MAN Password** — HTTP basic password; maximum length is 255 characters.
- **WS-MAN Port** — Default value is 443, or enter a port number from 1 to 65535.
- **WS-MAN Validate Certificate** — (Optional) Enables device certificate validation.

**NOTE:** A trusted certificate must be imported into the system before the WS-MAN Validate Certificate option is enabled, or communication may fail. For more information on how to install the certificate using the Chassis Management Controller, see the white paper *Using Windows Remote Management (WinRM) to Remotely Manage PowerEdge M1000e Using the Chassis Management Controller (CMC)* available at [delltechcenter.com/page/dcim.modular.cmc.winrm](http://delltechcenter.com/page/dcim.modular.cmc.winrm). For more information on how to import the certificate to Power Center, see [Managing Certificates](#).

- **SNMP v1v2c (UPS/PDU):** Select an SNMP protocol version from SMMPv1 or SNMP v2/v2c for the PDU or UPS.

- **SNMP Community string** — (Required) Maximum length is 255 characters.

- **SNMP v3 (UPS/PDU):** Select SNMP v3 for the PDU or UPS.

- **SNMP User Name** — (Required) Maximum length is 255 characters.
- **SNMP Authentication Password** — (Required) Maximum length is 16 characters.
- **SNMP Encryption Password** — Maximum length is 255 characters. When the **SNMP Authentication Password** is empty, the **SNMP Encryption Password** is also empty.

- **HTTPs** — Select the HTTPs based device communication for managing MX7000, third-party enclosures, or hypervisors.

- **HTTPs User Name** — The user name for HTTPs-based device communication. Maximum length is 255 characters.
- **HTTPs Password** — The password for HTTPs-based device communication. Maximum length is 255 characters.
- **HTTPs Port** — The port for HTTPs-based device communication. Enter a port number from 1 to 65535. The default port 443.
- **Validate Certificate** — (Optional) Enables device certificate validation.

- **SSH** — Select the SSH-based device communication for managing third-party enclosures.

- **SSH User Name** — The user name for SSH-based device communication for managing third-party enclosures. Maximum length is 255 characters.
- **SSH Password** — The password for SSH-based device communication. Maximum length is 255 characters.
- **SSH Port** — The port for SSH-based device communication. Enter a port number from 1 to 65535. The default port is 22.
- **Validate Host Key** — Enables host key validation.

- **WMI** — Select the WMI-based device communication for managing hypervisors.

- **Domain** — This field displays the domain for the hypervisor.
- **SSH User Name** — The user name for WMI-based device communication for managing third-party enclosures. Maximum length is 255 characters.
- **SSH Password** — The password for SSH-based device communication. Maximum length is 255 characters.
- **WMI Port** — The port for WMI-based device communication. The default port is 443.
- **Validate Certificate** — (Optional) Enables device certificate validation.

**NOTE:** You can change the protocol timeout settings in the **Settings > General** tab.

## Redfish protocol support

You can discover devices by using the Redfish protocol. The tasks that you can perform by using the Redfish protocol depends on the roles defined by the Distributed Management Task Force (DMTF) standard, namely Administrator, Operator, and ReadOnly. For example, with the administrator role, you have access to all the iDRAC privileges, with the ReadOnly role, you


have access only to the iDRAC login privilege. For more information on the roles and iDRAC privileges, see the iDRAC Redfish reference guide.


In OMPC, you can discover and manage devices by using multiple protocols. For example, to manage servers—you can use the IPMI or the Redfish protocol. OMPC does not change the protocol in use for devices discovered earlier. If you want to change the protocol to manage a device, you have to delete the device discovered using a protocol and rediscover with the other protocol.

 **NOTE:** You cannot discover the Non-Dell servers through the Redfish protocol.

## Limitations in using OMPC with Redfish protocols and devices

- You cannot discover Non-Dell servers through the Redfish protocol.
- Power capping and iDRAC location update functionality is supported only on Dell's 14th generation of PowerEdge servers.
- CUPS metrics, CFM metrics, and subsystem power metrics information are not available on devices discovered through the Redfish protocol.
- The following features are not supported by the Redfish protocol:
  - iDRAC location update
  - Calculating average power
  - Power Capping
  - CUPS
  - Airflow
  - Outlet Thermal
  - PEC Chassis Information—only for C6320
  - Graceful shutdown and graceful restart
- The following features are not supported on **iDRAC9** by the Redfish protocol:
  - CUPS
  - Airflow
  - Outlet Thermal
  - Slot number in chassis—only for C6420
  - Graceful shutdown and graceful restart


 **NOTE:** In OMPC 4.0, there are restrictions in using Redfish protocol with the lockdown feature of iDRAC enabled. For more information, see [Troubleshooting](#) chapter.

 **NOTE:** By default, the Redfish events are not logged into the event list. For more information, see [Troubleshooting](#) chapter.

## Adding a protocol

1. In the left pane, expand **Tasks**, and click **Protocols**.  
The **Protocols** screen is displayed.
2. In the task menu, click **Add**.  
The **Add Protocol** window is displayed.
3. In the **Profile Name and Description** section, enter a name and a description for the protocol.
4. In **Protocol Information**, select one of the following options:
  - Server
    - IPMI Protocol
    - Redfish Protocol
  - Chassis
    - WS-MAN Protocol
    - HTTPs Protocol
    - SSH Protocol
  - PDU/UPS
    - SNMPv1v2c
    - SNMPv3

- Hypervisor
  - HTTPs Protocol
  - WMI Protocol

 **NOTE:** By default, OpenManage Power Center uses port 8643 for power center application and port 8644 for redfish HTTPS events. You also have the option to use a different port apart from the default port.

5. Click **Finish**.

## Editing a protocol

You can edit the protocol information of a device.

1. In the left pane, expand **Tasks** and click **Protocols**.  
The **Protocols** screen is displayed.
2. Select the check box next to the protocol profile name you want to edit.
3. In the task menu, click **Edit**.  
The **Edit Protocol** window is displayed.
4. Make the required changes.
5. Click **Finish** to save your changes, or click **Cancel** to discard them.

## Deleting a protocol

1. In the left pane, expand **Tasks**, and click **Protocols**.  
The **Protocols** screen is displayed.
2. Select the check box next to the connection protocol that you want to delete.
3. In the task menu, click **Delete**.  
The following message is displayed: **Are you sure you want to delete the selected protocol(s)?**
4. Click **Yes**.  
The selected protocols are deleted.

# Device Management

The Devices feature enables you to view and manage the network-discovered devices and devices added manually. You can also categorize the devices into groups.

In the left pane, click **Devices**. The **Devices** screen is displayed and comprises the following tabs:

- **All Devices**
- **Managed Groups**

By default, the **All Devices** tab is displayed.

You can also view the details of a specific device or device group at the bottom section of the **Devices** screen. The details are categorized into the following tabs:

- **IP Address/Hostname**
- **Serial Number or Service Tag**
- **Device Model**
- **Protocol**
- **Power Capability**
- **Time of Discovery**

## Topics:

- [Adding a new device](#)
- [Adding an existing group](#)
- [Adding a device from the network](#)
- [Viewing resource utilization history](#)
- [Filtering devices](#)
- [Editing a device](#)
- [Deleting devices using a filter](#)
- [Sorting devices](#)
- [Updating Device location](#)
- [Chained PDU Support](#)
- [Managing groups](#)

## Adding a new device

The **Add New Device** window enables you to manually add a new device to the device list. You can add only unsupported devices and create a group structure to build the data center.

OpenManage Power Center cannot discover or manage all device types, and you must manually add unsupported devices to complete the data center group structure. For supported devices:

- Discover and add a supported device to the system.
- Perform management functions including discovery, adding to the group structure, monitoring power and temperature, applying power management policies, and sending events.

For unsupported devices:

- OpenManage Power Center does not communicate with unsupported devices, therefore connection protocol and credential information is not necessary.
- Unsupported devices cannot be discovered; they can only be added manually to the system.
- OpenManage Power Center adds the unsupported device to the group structure, but cannot manage it using the available management functions.

1. In the left pane, click **Devices** > **All Devices** > **Add New**.

The **Add New Device** window is displayed.

2. Enter the name of the device you want to add in the **Device Name** text box.
3. Enter a valid IP address in the **IP Address** text box or the hostname and device model number in the **Hostname** and **Model** text box respectively.
4. From **Additional Information (Optional)** > **Size of Device (U)** drop-down list, select the size of the device you want to add, in rack units (U).
5. Enter a description for the device in the **Device Description** text box.
6. Enter the maximum power estimate, in watts, for the device in the **Estimated Max Power (W)** text box.
7. Click **Finish** to add the device, or click **Cancel** to discard your changes.  
The device is displayed in the **All Devices** tab.


## Adding an existing group

You can use the Managed Groups feature to add sub-groups to an existing group. The sub-groups can be new or existing ones.

1. In the left pane, click **Devices** > **Managed Groups**.
2. Click the group to which you want to add a sub-group.
3. In the task menu, click **Add New**.  
The **Add New Device/Group** window is displayed. For more information on adding a new group to an existing group, see [Creating A New Group](#).
4. Click the **Add Existing Group** tab.  
By default, the group in the recent hierarchy navigation is selected.
5. In the list of existing groups, select the check box next to the existing groups that you want to add, and click **Save**.

## Adding a device from the network

You can use the Power Center management console to discover a device from the network.

-  **NOTE:** Power Center server tries to get device names from the DNS server specified in the network configuration of the operating system. This may cause the device name to be different from the actual one if the DNS server resolves the device IP address to a different device name.

Before adding a device from the network, make sure the DNS server is set up correctly. Specifically, make sure that:

- There is a DNS server running on the Power Center network.
- The specified DNS server has a reverse DNS zone for the network on which you are trying to discover the devices.

## Viewing resource utilization history

OpenManage Power Center enables you to view a graphical representation of the utilization of resources.


1. In the left pane, click **Devices** > **All Devices**.
2. Select a device from the list of devices in the **All devices** tab.  
The details of the selected device are displayed in the **Details** section.
3. Click **Details** > **Resource Utilization History**.  
The **Resource Utilization History-<Entity>** window is displayed, where an **<Entity>** is the selected device.
4. Click **X** in the upper-right corner to return to the **Managed Groups** tab.


## Filtering devices


The filter feature in the **All Devices** tab helps you to view devices that share a certain attribute. For example, you can view devices of a certain device type or devices that share an IP range.


1. In the left pane, click **Devices**.  
The **All Devices** tab is displayed by default.


2. In the task menu, click **Filter**.  
The **Device Filter** window is displayed.
3. Select the filter by clicking **Select Filter** drop-down list.
4. (Optional) Enter a name for the filter in the **Filter Name** text box.
5. Do one of the following:
  - Select the **IP Range** check box, and enter the start and end IP address of devices.
  - Select the **Date Range** check box, and enter the start and end date of device discovery. Enter the dates manually following the format MM/DD/YYYY, or select the dates from the calendar. Devices discovered from 00:00:00 of start date to 00:00:00 of the next day after the end date are displayed. For example, if you enter the filtering option 01/01/2015 as both start date and end date, all devices discovered between 00:00:00 of 01/01/2015 and 00:00:00 of 01/02/2015 are displayed.
  - Select the **Device Type** check box, and select the device type from the drop-down list. The available options are:
    - **Server**
    - **Chassis**
    - **PDU**
    - **UPS**
    - **Unsupported**

 **NOTE:** You can select multiple device types.
  - Select the **Power Capability** check box, and select the power capability of the device from the drop-down list. The available options are:
    - **Unknown** — Indicates that the power capability of the device is unknown.
    - **None** — Indicates that the device does not have power capability.
    - **Monitor** — Indicates that the device has aggregate power monitoring capability.
    - **Monitor and capping** — Indicates that device has aggregate power monitoring and power capping capability.
    - **Monitor, upgradeable** — Indicates that the device can be upgraded with the iDRAC enterprise license for power capping.
    - **Instantaneous power** — Indicates that the device has instantaneous power monitoring capability.
    - **Outlet Power** — Indicates that the devices are filtered based on the specified outlet power.
    - **Monitor through PDU** — Indicates the devices that can be monitored using PDU.

 **NOTE:** You can select multiple power capabilities.
  - Select the **Protocol** check box, and select the protocols used for communication. The available options are:
    - **IPMI (Server)**
    - **WS-MAN (Chassis)**
    - **SNMPv1v2c (UPS/PDU)**
    - **SNMPv3 (UPS/PDU)**
    - **HTTPS**
    - **SSH**
    - **Redfish**

 **NOTE:** You can select multiple protocols.
  - Select the **Status** check box, and select device status from the drop-down list. The available options are:
    - **Connected**
    - **Lost Connection**
    - **NA**

 **NOTE:** You can select multiple status.
  - Select the **Device Model** check box, and choose a model from the drop-down list. The device model is the specific model information of a device type, for example, *PowerEdge M610*.  

 **NOTE:** If you select both **Device Type** and **Device Model**, ensure that the device type and the device model match. Otherwise, the results may not be displayed.
  - Select the **Estimated Max Power (W)** check box and enter the maximum power for device. The estimated max power is considered as the peak power consumption by a device.
6. Click **Save and Run** to save the filter.



OR

- Click **Run Once** to view a filtered list of devices.

OR

- Click **Cancel** to return to the **All Devices** tab.


You can use the saved filters later.

## Editing a device

You can edit devices or device groups from the **Devices** screen.

1. In the left pane, click **Devices**.
2. Select the check box next to the device or device group that you want to edit.
3. Click **Edit**.  
The **Edit Entity** screen is displayed.
4. Make the required changes.

For devices, you can edit the name of the device, device description, size of the device, and estimated maximum power. For device groups, you can edit the group type, group name, group description, and power capacity.

 **NOTE:** For PDUs, you have an option to replicate the rack association relationship.

5. Click **Finish** to save your changes, or click **Cancel** to return to the **Devices** screen without saving your changes.

## Deleting devices using a filter

You can also delete devices using the Filter feature.

1. In the left pane, click **Devices**.
2. In the task menu, click **Filter**.  
The **Device Filter** window is displayed.
3. Select the filter by which you want to sort the devices list.
4. Select the check boxes next to the devices that you want to delete.
5. In the task menu, click **Delete**.  
The following message is displayed.

Are you sure you want to delete the selected item(s)?

6. Click **Yes** to proceed with the deletion.

## Sorting devices

By default, the devices in the **All Devices** tab, are listed by **Name** in alphabetical order (A-Z). But you can sort the list as per your requirement.

1. In the left pane, click **Devices** to view the list of all devices.
2. To sort the devices, click the 'up' or 'down' arrow next to one of the following column headers:
  - **Status**
  - **Device**
  - **Device Type**
  - **Device Size**
  - **Device Model**


The 'up' or 'down' arrow is displayed next to the column header by which the display is sorted.

# Updating Device location


OMPC enables you to replicate and update the physical organization and hierarchy of a data center.

Using OMPC you can place servers in the hierarchy specified on iDRAC/CMC. Only servers for which the values have been populated in the following hierarchy — Data Center, Room, Aisle, and Rack fields are automatically assigned in OMPC. The servers remain unassigned, if any of the values are missing in the hierarchy.

The iDRAC/CMC location can be updated from a group level following the physical hierarchy — Data center, Room, Aisle, and Rack. OMPC updates the location of the devices present in a particular group, such as a data center, room, aisle, or a rack.

 **NOTE:** The location can be updated only for chassis, rack, and tower (only Dell servers).

1. In the left pane, click **Devices > Managed Group**
2. From the list of device groups, select a data center, room, aisle, rack, or a device in the rack.  
The details of the device are displayed in the **Details** section
3. Click **Update Device Location**.  
The **Device Location Update Window** is displayed.
4. Click **Update** to update the device location with the iDRAC/CMC location.

 **NOTE:** If the iDRAC/CMC path and the device path are not synchronized, a warning message is displayed in the **Details > Device Details** section. You may have to update the device path to ensure that it is synchronized with the iDRAC/CMC path.


A table is displayed providing information about the successful location update. If the update is not successful, you can view the application logs for details about the failure.


5. Click **Close**.

## Chained PDU Support

In a data center, you can use any number of PDUs for power distribution, depending on the infrastructural requirements. The PDUs can be connected in a daisy chain manner to further enhance and improve the power distribution in the data center. In the daisy chain arrangement of PDUs, a master PDU discovers and monitors the subordinate PDUs. Currently, only the master PDUs are discovered, but the subordinate PDUs connected are not discovered, hence monitoring the power aspects of those PDUs are not possible.

Starting OMPC 3.2, you can also discover, monitor, and perform all operations on the subordinate PDUs as it is done on a master PDU. The daisy chained PDUs are discovered using the IP address, irrespective of whether the same SNMP port is used (for both master and the subordinate) or not. Adding a daisy chained PDU to a rack automatically associates the subordinate PDUs to that particular rack. However, you can also associate or disassociate a subordinate PDU from the master PDU individually.

 **NOTE:** If you disassociate a subordinate PDU from the master PDU, it is removed only from that particular daisy chain arrangement.

 **NOTE:** Deleting a master PDU does not delete the associated subordinate PDUs.

## Viewing chained PDUs

1. In the left pane, click **Devices > All Devices**.
2. From the list of devices, select a PDU device.
3. If the selected PDU is a Master PDU, **Associate Subordinate PDU** option is displayed.
4. Click on the **Associate Subordinate PDU** option to view the associated subordinate PDU.  
The sequence of the associated PDUs, PDU name, PDU model, Service tag, and the time of discovery is displayed.
5. If the selected PDU is a subordinate PDU, **Associate Master PDU** option is displayed.
6. Click on the **Associate Master PDU** option to view the associated master PDU.  
The PDU name, PDU model, Service tag, and the time of discovery is displayed.

# Managing groups

OpenManage Power Center enables you to create groups for organizing devices, so that you can manage them more efficiently. The groups can be of the following types:

- Datacenter
- Room
- Aisle
- Rack
- Custom

In the left pane, click **Devices > Managed Groups**. In this tab, you can:


- View details of a specific device group
- Add groups
- Edit groups
- Delete groups
- Refresh the list of device groups
- Move devices from one group to another
- Manage racks
- Enable or disable Emergency Power Reduction (EPR)
- View rack utilization graphs

## Mapping Group Structure Information

OpenManage Power Center supports group structure mapping for PowerEdge rack servers and tower servers.

After you create or update the group structure, Power Center automatically updates the location information in the firmware of supported devices using the following mapping structure:


- Data Center — Data center and room information in Power Center; format: <Data Center - Room>
- Aisle — Aisle information in Power Center
- Rack — Rack information in Power Center
- Rack Slot — Rack slot information in Power Center
- Custom — Customize the device group

 **NOTE:** To view updated location information on supported device, you must make sure the device status has a *Connected* status in Power Center. It may take a few minutes for location information to update in device firmware.

## Creating a new group

A group can represent the actual structure of a data center, room, aisle, rack, or custom. You can nest groups in parent-child relationships to represent how the devices in your data center are physically configured.

1. In the left pane, click **Devices > Managed Group**.
2. In the task menu, click **Add New**.  
The **Add New Group** window is displayed. By default, the group used previously is selected.
3. Enter a name for the group in the **Name** text box.


 **NOTE:** The name must be unique across groups and devices under the parent group.

4. From the **Type** drop-down list, select the group type.  
The available options are:

- **Datacenter**
- **Room**
- **Aisle**
- **Rack**
- **Custom**

For racks,

- Select the space capacity from the **Space Capacity (U)** drop-down list.
  - Enter the power capacity in the **Power Capacity (W)** text box. The power capacity is determined by the power distribution to the rack.
  - (Optional) Select the **Use PDU Power Consumption** check box. By default, this check box is cleared.
5. Enter a description for the group in the **Description** text box.
  6. Select the **Replicate Group Count** option if you want to replicate a device.
 

 **NOTE:** These steps are applicable only if you chose the **Replicate Group Count** option.

    - a. Provide the start index from where the devices are to be replicated, for example, from serial number 1, serial number 2, or so on.
    - b. Provide the number of instances the device has to be replicated, for example, choose 3 to replicate the selected device three times, that is, *<device (001)>*, *<device (002)>*, *<device (003)>*.
  7. Click **Save** to save the new group or click **Cancel** to return to the **Devices > Managed Group** screen without saving the changes.

## Moving device groups or devices

You can move a manually added device to an existing group as well as move groups of devices from one group or rack to another. You can also move a group of devices from one slot to another slot in a rack.

To move a device from one slot to another within a rack, see [Manage Racks](#).

 **NOTE:** Any power policies in effect is recalculated after moving a group.

1. In the left pane, click **Devices > Managed Groups**.
2. Select the device group you want to move.
3. In the task menu, click **Move**.  
The **Move To Group** window is displayed with the list of groups. The **Current Entity** field displays the name of the group with which the devices are currently associated.  
The **Move To** displays the **Other** option that is selected by default.
4. Select the group to which you want to move the group or device.
5. Click **Finish** to return to the **Devices** screen, or click **Cancel** to discard your changes.
6. Confirm the move:
  - a. Click the **Devices > Managed Groups**.
  - b. Using the device tree, select the group to which you added the group or device, and check to make sure that the device is listed as expected.

## Viewing devices in a chassis

OpenManage Power Center enables you to view the installed devices in a chassis. Further, if you have physically added, removed, or changed the devices in a chassis, you can update the device information in Power Center.

1. In the left pane, click **Devices > All Devices** or **Devices > Managed Group**.
2. From the list of devices, select a chassis.  
The details of the chassis are displayed in the **<Device> Details > Summary** tab.

## Managing Racks

OpenManage Power Center enables you to manage racks and the slotted and associated devices that have been added to the Power Center system.

The **Manage Rack** wizard comprises of the following tabs.

- Rack Contents
- Associated Devices

In the **Rack Contents** tab you can configure a rack selected in the **Devices** screen in the following ways:

- Add devices to rack slots

- Rearrange devices within rack slots
- Remove devices from rack slots
- Edit devices

In the **Associated Devices** tab you can manage devices such as PDUs that are not added to a rack slot, but are associated with the rack, in the following ways:

- Add an associated device to the rack
- Edit an associated device that has already been added to the rack
- Remove an associated device from the rack

## Adding a device to a rack slot

1. In the left pane, click **Devices > Managed Groups**.
2. From the list of devices, select a rack device.
3. From the devices menu, click **Manage Rack**.  
The **Manage Rack** window is displayed. By default, the **Rack Contents** tab is displayed.
4. In the **Rack Contents** tab, click **Add to Rack Slot**.  
The **Add to Rack Slots** wizard is displayed.
5. Select the check boxes next to the devices you want to add to the rack and click **Next**.
6. From the **Select** drop-down list next to the devices you want to add to the rack, select the slots into which you want to place the devices.
7. Click **Finish** to return to the **Manage Rack** screen and review your changes.

## Adding an associated device to a rack

1. In the left pane, click **Devices > Managed Groups**.
2. From the list of devices select a rack device.
3. In the task menu, click **Manage Rack > Associated Devices > Add To Rack**.  
The **Associate a Device with a Rack** window is displayed.
4. Select the check box next to the device that you want to associate with the rack.
5. Click **Finish** to return to the **Manage Rack** screen and review your changes, or click **Cancel** to return to the previous screen.

## Editing a rack-associated device

1. In the left pane, click **Devices > Managed Groups**.
2. From the list of devices select a rack device.
3. In the task menu, click **Manage Rack > Associated Devices > Add To Rack**.
4. Select the check box next to the device that you want to associate with the rack.
5. Click **Finish** to return to the **Manage Rack** screen.
6. From the list of devices, select the device you want to edit, and click **Edit**.
7. Make the desired changes.
8. Click **Finish** to return to the **Manage Rack** screen and review your changes, or click **Cancel** to return to the previous screen.

## Rearranging devices in a rack

1. In the left pane, click **Devices > Managed Groups**.
2. From the list of devices select a rack device.
3. In the task menu, click **Manage Rack**.  
The **Manage Rack** window is displayed. By default, the **Rack Contents** tab is displayed.
4. In the **Rack Contents** tab, click **Rearrange Rack**.  
The **Move In Rack** window is displayed with the list of slotted devices.

5. From the **New Slot** drop-down list next to the devices you want rearrange, select the slots into which you want to move the devices.


 **NOTE:** You can add devices with size up to **42U**.

6. Click **Finish** to return to the **Manage Rack** screen and review your changes.

## Removing a rack-associated device


1. In the left pane, click **Devices > Managed Groups**.
2. From the list of devices select a rack device.
3. In the task menu, click **Manage Rack > Associated Devices**.
4. From the list of devices, select the device you want to remove.
5. In the task menu, click **Remove**.  
The following message is displayed: **The device will not be deleted, but will remain in the Devices List.**
6. Click **Yes** to proceed with the removal.

## Removing slotted devices from a rack

1. In the left pane, click **Devices > Managed Groups**.
2. From the list of devices select a rack device.
3. In the task menu, click **Manage Rack**.  
The **Manage Rack** window is displayed. By default, the **Rack Contents** tab is displayed.
4. From the list of devices in the rack slots, select the device you want to remove and click **Remove from Rack**.
5. The following message is displayed:  
**The device will not be deleted, but will remain in the Devices List.**  
 **NOTE:** The device is immediately removed from the rack when you click **Remove from Rack**. The device is removed only from the rack slot, and not from the device list. But you can add the device back if you removed the device by mistake.
6. Click **Yes** to proceed with the removal.

## Viewing a rack utilization graph

OpenManage Power Center enables you to view a graphical representation of different aspects of rack utilization for custom and physical entities within the Power Center system. This information can help you determine the availability of space and power within specific racks to add new devices.

1. In the left pane, click **Devices > Managed Group**.
2. From the list of device groups, select a group that contains a rack device.  
The details of the device are displayed in the **Details** section.
3. Click **Details > Rack Utilization**.  
The **Rack Utilization** window is displayed.  
 **NOTE:** The **Rack Utilization** option is available only for groups of the types — datacenter, room, and aisle.
4. Click the **Power Utilization** or **Space Utilization**, and the **Actual** or **Percentage** options to change the data viewed.
5. Click **X** in the upper-right corner to return to the **Managed Groups** tab.

A rack may not be displayed in the rack utilization graph if:

- The actual power of a device or devices in the rack exceeds the specified power capacity.
- The estimated maximum power for a device in the rack is not set.

## Deleting a group

1. In the left pane, click **Devices > Managed Groups**.
2. In the **Managed Groups** tab, select the group that you want to delete.

3. In the task menu, click **Delete**.  
The **Delete Group** window is displayed with the details of the managed group that you want to delete.
4. Click **Confirm** to proceed with the deletion.

## Emergency Power Reduction

When there is an emergency situation — for example, a power failure and your devices are running on UPS, you can initiate Emergency Power Reduction to reduce the power consumption of your managed devices.

### CAUTION:

**Applying emergency power reduction will throttle power on the devices down to an extremely low level, which will impact performance. All devices with Monitor & Capping power capability are impacted. Use this only in an emergency situation.**


All of the devices with the Monitor & Capping power capability within this group are set to the minimal power consumption state. The **Emergency Power Reduction** button appears in the upper-right corner of all pages. The devices impacted by emergency power reduction are marked with **EPR** in the **Devices** screen.


## Enabling Emergency Power Reduction


1. In the left pane, click **Devices > All Devices** or **Devices > Managed Groups**.
2. From the list of devices, select the device (data center, room, aisle, rack, or chassis) to which you need to apply the Emergency Power Reduction.
3. In the task menu, click **Enable EPR**.  
The following message is displayed: **Applying Emergency Power Reduction will throttle power down to an extremely low level, and impact performance. Do you want to continue?**
4. Click **Yes** to proceed.  
Again a message is displayed to confirm if you are opting to compromise with the performance by reducing power.
5. Click **Yes**.

## Disabling Emergency Power Reduction

Disabling Emergency Power Reduction (EPR) restores device power to its full state.

 **NOTE:** For instructions on applying EPR to an entity, see [Enabling emergency power reduction](#).

 **NOTE:** It may take a few moments for the Power Center console to reflect the disabling of EPR. You can manually refresh your screen to see the updated EPR status notification in the upper right corner of the screen.


 **NOTE:** The red EPR status notification icon only appears in the upper right corner of the screen when EPR has been applied to a device.

1. From any screen within Power Center, click the red EPR status notification in the upper right corner of the screen or in the left pane, click **Devices > All Devices**, or **Devices > Managed Groups**.

 **NOTE:** If the devices on which you enabled EPR do not appear on the list, click **Refresh**.

A pop-up window opens listing the **Name** of the entity under EPR and a **Timestamp** reflecting the time EPR went into effect.

2. Click the **View EPR** button.  
The **Emergency Power Reduction** window is displayed.
3. Select the entity (data center, room, aisle, rack, or chassis) for which you want to disable EPR.
4. In the task menu, click **Disable EPR**.

 **NOTE:** The **Disable EPR** option is displayed only if you select a device.

The following message is displayed: **You are about to disable Emergency Power Reduction. Are you sure you want to perform this action?**

5. Click **Yes** to disable the EPR.

# Virtual machines

OMPC monitors the devices, manages the power consumption, and aggregates the observations in the form of a report. However, only physical devices such as server, chassis, UPS, or PDU are monitored. Currently, the power consumption of virtual machines is not monitored.


You can discover hypervisors, enumerate virtual machines on the hypervisor, manage power tasks, evaluate, and generate power consumption reports.

The metrics from the report enable data center administrators to:

- Compute power utilization of the virtual machines.
- Identify a potential problem.
- Prioritize the workload based on actual power consumption.
- Provide usage chargeback.

After you discover the devices, the hypervisors associated with that particular device are displayed in the **Virtual Machines** feature tab. Only the hypervisors associated with a physical device that was discovered, is selected for processing. If you remove a physical server from OMPC, all the associated hypervisors and virtual machines are deleted.

You can move a virtual machine from one physical host to another. The virtual machine is allocated a unique identifier, through which it can be identified in the physical host after the migration. In this way, all the information related to the virtual machine is preserved even after the virtual machine is migrated to a different physical host.

 **NOTE:** You cannot delete a discovered virtual machine. However, you can delete the device with which the virtual machine has been associated, that eventually deletes the corresponding hypervisors and virtual machine.

## Topics:

- [Filtering virtual machines](#)
- [Creating a new virtual machine group](#)
- [Adding a virtual machine to an existing group](#)
- [Moving a virtual machine group](#)
- [Viewing a virtual machine power history graph](#)
- [Viewing a virtual machine power distribution graph](#)
- [Deleting a VM group](#)


## Filtering virtual machines


The filter feature in the **Virtual Machines** tab helps you to view the virtual machines that share a certain attribute. For example, you can filter and view the virtual machines based on the IP range or the status.

1. In the left pane, click **Virtual Machines**.  
The **Virtual machines** tab is displayed by default.
2. From the task menu, click **Filter**.  
The **Virtual Machines Filter** window is displayed.
3. Select the filter from the **Select Filter** drop-down list. The available options are **All VMs**, **VMware ESXi**, and **Microsoft Hyper-V**.
4. Enter a name for the filter in the **Filter Name (Optional)** text box.
5. Do one of the following:
  - Select the **Hypervisor IP Range** check box, and enter the start and end IP address of the hypervisor.
  - Select the **Virtual Machine Date Range** check box, and enter the start and end date of virtual machine discovery. Enter the dates manually following the format MM/DD/YYYY, or select the dates from the calendar. Devices discovered from 00:00:00 of start date to 00:00:00 of the next day after the end date are displayed. For example, if you enter the filtering option 01/01/2015 as both start date and end date, all devices discovered between 00:00:00 of 01/01/2015 and 00:00:00 of 01/02/2015 are displayed.




- Select the **Hypervisor host** check box, and select the hypervisor type from the drop-down list. The available options are:
    - **VMware ESXi**
    - **Microsoft Hyper-V**

 **NOTE:** You can select both the options.
  - Select the **Status** check box, and select the status of the virtual machine from the drop-down list. The available options are:
    - **Online**
    - **Offline**
    - **Suspended**
    - **Unknown**

 **NOTE:** You can select multiple statuses.
6. Click **Save and Run** to save the filter. You can use the saved filters at a later time.
- OR
- Click **Run Once** to view a filtered list of virtual machines.
- OR
- Click **Cancel** to return to the **All Devices** tab.

## Creating a new virtual machine group

A virtual machine group can represent the structure of a data center, room, aisle, rack, or custom. You can nest groups in parent-child relationships to represent how the virtual machines in your data center are configured.

1. In the left pane, click **Virtual Machines > VM Groups**.
2. From the task menu, click **Add New**.  
The **Add New VM/Group** window is displayed. By default, the group used previously is selected.
3. Enter a name for the group in the **Name** text box and provide an optional description for the group.  
 **NOTE:** The name must be unique across groups and devices under the parent group.
4. Click **Save**.  
A new VM group is created successfully.
5. In the **Add Existing VM** tab, select the virtual machines to add to the VM group.
6. Click **Save**.  
The selected VMs are added successfully.

## Adding a virtual machine to an existing group

After a virtual machine is discovered or manually added to OpenManage Power Center, you can add it to a VM group.

1. In the left pane, click **Virtual Machines > VM Groups**.
2. Select the VM group to which you want to add the virtual machine and click **Add Existing VM** tab.
3. Select the virtual machines that you want to add to the selected VM group and click **Save**.  
The selected VMs are added successfully.

## Moving a virtual machine group

After creating a virtual machine group, you can move the group to another existing virtual machine group.

1. In the left pane, click **Virtual Machines > VM Groups**.
2. Select **Move** to move a VM group to another VM group.

The current VM group is displayed as **Current Entity**.


3. The available VM groups to which you can move is listed as **Move to**. Choose the VM group to which you want to move.
4. Click **Save**.  
The VM group is moved to the selected group.

## Viewing a virtual machine power history graph

OpenManage Power Center provides a visual representation of the power history of a virtual machine or a group of virtual machines.

1. In the left pane, click **Virtual Machines > All Virtual Machines** or **Virtual Machines > Virtual Machine Groups**.
2. From the list of devices, select a virtual machine or a group of virtual machine.
3. In the **Details** tab, click **Power History**.  
The **Power History-<VM Name>** page is displayed.
4. Select the time period and attributes displayed:
  - a. To select the time period represented in the graph, click the buttons along the top of the graph.
  - b. To add or delete attributes, select from the listed options; click the option to toggle its addition or removal from the graph:
    - Estimated VM Power
    - Hypervisor Power

 **NOTE:** If you select a group, only **Estimated VM Group Power** attribute is displayed.

 **NOTE:** To view specific numbers related to each attribute displayed in any section of the graph, move the pointer over the graph.

5. To move along the data stream over time, click the navigation arrows below the graph.

## Viewing a virtual machine power distribution graph

OpenManage Power Center provides a visual representation of the power distribution of a group of virtual machines.

1. In the left pane, click **Virtual Machines > Virtual Machine Groups**.
2. From the list of devices select a group of virtual machine.
3. In the **Details** tab, click **Power Distribution**.  
The **Estimated VM Power for Group:<Virtual Machine Name>** page is displayed.
4. To move along the data stream over time, click the navigation arrows below the graph.

## Deleting a VM group

After creating a virtual machine group, you can delete that group.

1. In the left pane, click **Virtual Machines > VM Groups**.
2. Select the VM group that you want to delete and click **Delete**.
3. A message asking for a confirmation to delete the VM group is displayed. Click **Yes**.  
The selected VM group is deleted successfully and the virtual machines associated with the VM group is disassociated.

# Power Monitoring

Power Center enables the monitoring of current or historical power-related metrics (for example, power consumption or cost). This can help you understand the power status in the data center and plan for additional power infrastructure, cooling, and facility needs.

You can monitor power at different device and/or group levels. You can configure power monitoring settings to meet your monitoring needs, and you can print the power status graph.

## Topics:

- [Power monitoring levels](#)
- [Power thresholds](#)
- [Viewing power details](#)
- [Viewing Energy Consumption](#)
- [Viewing a power history graph](#)
- [Viewing system airflow graph](#)
- [Monitoring PDU](#)
- [Monitoring UPS Power](#)

## Power monitoring levels

OpenManage Power Center provides power monitoring at the following levels for groups:

- Rack
- Aisle
- Room
- Data center
- Custom

## Power thresholds

It is useful to monitor thresholds when you want to be notified when the power of a group and/or device exceeds the set limits.

1. In the left pane, Click **Devices**.
2. From the **Managed Groups** tab, select the group or device for which you want to set the threshold.
3. In the details section of the screen, click **Thresholds**.
4. Under **Power Alert Thresholds (W)**, enter values in the **Upper Warning** and **Upper Critical** text boxes.  
When the power exceeds the upper warning value, a warning-level event alert is sent. When the power exceeds the upper critical value, a critical-level event alert is sent.
5. Click **Save**.

For more information on configuring the device/group range and sampling interval, see [Monitoring Settings](#).

For more information on configuring default units and energy consumption, see [Configuring Energy Consumption Cost Settings](#).

## Viewing power details

In the left pane, click **Devices > All Devices** or **Devices > Managed Groups**. Click the icon for a device or group, then refer to the power detail section of the screen. While OpenManage Power Center does provide power information for PDU and other devices and groups, Power Center does not provide power details for UPS devices.

For devices and groups (excluding PDU and UPS), by default, the **Power** graph displays the power details for the previous hour. Refer to [Viewing Power History Graph](#) for details on accessing a device or group graph.

**NOTE:** CMC infrastructure power adjustments are not considered when OMPC reports the modular server power reading. It is recommended to view the total power from a chassis level.

## Power details for the current time window

You can view power details for the current time window by clicking a time window tab. The following table describes the time windows and their associated intervals:

**Table 4. Time windows and intervals**

Time Window	Description	Interval
15Min	15 minutes	1 minute
1H	1 hour	3 minutes
1D	1 day	1 hour
1W	1 week	6 hours
1M	1 month	1 day
3M	3 months	1 week
1Y	1 year	2 weeks

**NOTE:** This table lists the interval when the sampling interval is at the default value (1 minute). Changing the sample interval results in interval changes for the 15Min and 1H time windows. If you change the sampling interval to 3 minutes, the interval of the 15Min time window is 3 minutes. If you change the sampling interval to 6 minutes, the interval of the 15Min time window is 3 minutes and the interval of the 1H time window is 6 minutes.

## Power details for a different time window

Click the arrows < > to view the details for the previous/next sampling time, or click the double arrows << >> to view the details for the previous/next page of results for the current time window. You can click Average, Maximum, or Minimum to display the selected value.

- **Average:** The average value from the previous time point to the current time point.
- **Maximum:** The maximum value from the previous time point to the current time point.
- **Minimum:** The minimum value from the previous time point to the current time point.

For example, you view power details in the 1H (1 hour) window and the maximum value at 15:00 shows 500W and the time interval is 6 minutes. This value would represent that the maximum power consumption from 14:54 to 15:00 is 500W.

**NOTE:** It is common to see that some instantaneous values exceed the Power Cap value in the **Maximum** line. Power Center monitors this value and controls it to the normal power range with this happens. You only need to pay attention when the Average power value exceeds the Power Cap value.

**NOTE:** You can set the time interval (the period from a time point to the next time point) in the **Settings** page. For information on configuring the interval, see [Monitoring Settings](#).

## Power details for racks

For racks, you can click **Devices > Managed Group > Details** to display PDU power consumption for all rack PDUs.

You can also click **Devices > Managed Group > Policies** to change a power policy.

You can view the following power details of PDU devices. For more information on supported PDU devices, see [System Requirements](#).

- PDU device information, including PDU name, model, and IP address.
- PDU outlet information, including outlet number, power (W), voltage (V), amps (A), and the time of the information recorded, following the format <YYYY-MM-DD HH:MM:SS>. The table lists the information for each outlet and the total power consumption for all outlets.

## Viewing Energy Consumption

Details of each device and device group power consumption are available in the power history graph.

- **IT Equipment Energy** — The total energy consumption and cost for all managed devices in the selected device or device group.

**NOTE:** Power Center can read the power consumption of a device when it is at S0 (On) state. For devices in S4/S5 state, Power Center uses a fixed value (30W) to calculate the power consumption.

- **Cooling Energy** — The estimated energy consumption and cost needed to cool the selected device/group.

$\text{Cooling Energy} = \text{IT Equipment Energy} * \text{Cooling Multiplier}$

You can configure the cooling multiplier on the **Settings > Monitoring** screen, in the **Energy Consumption Cost** section.

- **Energy Consumed (Total)** — The combined energy consumption and costs for the IT equipment and cooling energy. The formula is:

$$\text{Cost} = (\text{IT Equipment Energy } T1 * \text{Cooling Multiplier}) * \text{Flat Rate } T1 + (\text{IT Equipment Energy } T2 * \text{Cooling Multiplier}) * \text{Flat Rate } T2 + \dots + (\text{IT Equipment Energy } Tn * \text{Cooling Multiplier}) * \text{Flat Rate } Tn$$

**NOTE:** T1/T2/.../ Tn is the time period (in hours) at a certain flat rate.

**NOTE:** By default, the **Cost** column displays 0. You must configure the cost rate to see the cost. The rate is a global setting, and can be set on the **Settings > Monitoring** page.

**NOTE:** The **Energy Consumption Cost** section displays information based on the values configured in the **Settings** screen. This information should be used as an estimate only.


**NOTE:** When a device or group is newly-added or created in Power Center, the power and energy consumption data displayed in the "1W" and "1M" time windows are different if the monitored time is less than 1 week, and the data displayed in the "1H" and "1D" time windows are different if the monitored time is less than 1 day. This occurs because Power Center uses different sampling intervals for different time windows. For example, a device is added into Power Center at 2011-10-15 09:00, and the current time is 2011-10-17 11:10. For the 1M time window (sampling interval is 1 day), the power and energy consumption is calculated from 2011-09-17 00:00 to 2011-10-17 00:00. For the 1W time window (sampling time is 1 hour), the power and energy consumption is calculated from 2011-10-10 11:00 to 2011-10-17 11:00. There is an 11 hour gap; therefore, the data displayed in the two time windows are not the same.

## Viewing a power history graph

OpenManage Power Center provides a visual representation of the power history of the system devices.

1. In the left pane, click **Devices > All Devices** or **Devices > Managed Group**.
2. From the list of devices, select a device.  
The details of the device are displayed in the **Details** section.
3. In the **Details** section, click the **Thresholds** tab.

4. Click **View History** next to **Power Alert Thresholds**.  
The **Power History — <device>** window is displayed.
5. Select the time period and attributes displayed:
  - a. To select the time period represented in the graph, click the buttons along the top of the graph.
  - b. To add or delete attributes, select from the listed options; click the option to toggle its addition or removal from the graph:
    - Power
    - Upper Warning
    - Upper Critical


 **NOTE:** To view specific numbers related to each attribute displayed in any section of the graph, move the pointer over the graph.


6. To move along the data stream over time, click the navigation arrows below the graph.

## Viewing system airflow graph

iDRAC provides an accurate calculation of the server's Cubic Feet Per Minute (CFM) value. The CFM value is a measure of the net system airflow to the servers. This value is used in Power Thermal Aware Scheduling (PTAS), balancing the data center workload, efficient server utilization, and thermal management from a rack level. CFM or the system airflow graph is useful from a group level (data center, room, aisle, rack, or custom groups). The values are collected only from the devices that support this feature.

1. In the left pane, click **Devices > Managed Group**
2. Select the required data center, room, aisle, or rack in the data center.  
The details of the selected entity are displayed in the **Details** section
3. Click **System Airflow History**.  
The **System Airflow History — <data center name>** window is displayed.
4. Select the time period and attributes displayed:
  - a. To select the time period represented in the graph, click the buttons along the top of the graph.

 **NOTE:** To move along the data stream over time, click the navigation arrows below the graph.

 **NOTE:** A rack may not be displayed in the rack utilization graph if:

- The actual power of a device or devices in the rack exceeds the specified power capacity.
- The estimated maximum power for a device in the rack is not set.

## Monitoring PDU

Using OMPC, you can view the PDU socket connection mapping with the devices. Starting OMPC 3.2, you can also monitor the temperature, humidity, and other necessary metrics in a data center by using environmental sensors.

To monitor a PDU, click **Devices** in the left pane, navigate to the required PDU, view the **Details** section of the screen.

The instantaneous power value of the PDU is displayed, and the details section of the screen also lists the PDU details read from the device. It displays NA when the data is not provided on the PDU device.

You can also generate reports and view the details. For more information on creating PDU reports, refer [Managing Reports](#).

## Monitoring UPS Power

To monitor UPS power, click **Devices** in the left pane, and then select the UPS. The UPS details are displayed in the **Details** section of the screen.

The instantaneous power value of the UPS is shown, as well as the UPS details read from the device. It displays NA when the data is not provided on the UPS.

# Temperature Monitoring

OpenManage Power Center enables monitoring of the current and historical server inlet temperature of the data centers in Power Center. This can help you understand the temperature status and identify hot spots in the data center.

You can monitor the temperature status at different device/group levels. You can configure the temperature monitoring settings to meet your monitoring needs, and you can print the temperature status graph.

## Topics:

- [Temperature Monitoring Level](#)
- [Viewing Temperature Details](#)
- [Viewing a temperature history graph](#)
- [Monitoring the Temperature of the Chassis/Blade Server](#)
- [Applying circuit breaker limits to chassis](#)
- [Monitoring the Temperature of Devices/Groups](#)

## Temperature Monitoring Level

Power Center provides temperature monitoring at the following levels:

- Device level — You can monitor temperature-related metrics for devices.
- Physical group level — You can monitor temperature-related metrics at the physical group level (data center, room, aisle, chassis modular).
- Logical group level — You can monitor temperature-related metrics at the logical group level.

## Viewing Temperature Details

Click **Devices** in the left navigation pane, then select the **Managed Groups** tab. Click the icon for the group or device, then refer to the **Details** section of the screen.

Click **View History** under the **Present Power** heading to access the **Temperature Details** graph. By default, the **Temperature Details** graph displays the temperature details for the previous hour.

## Temperature Details for the Current Time Window

You can view temperature details for the current time window by clicking a time window tab. The following table describes the time windows and their associated intervals:

**Table 5. Time Windows and Intervals**

Time Window	Description	Interval
15Min	15 minutes	1 minute
1H	1 hour	3 minutes
1D	1 day	1 hour
1W	1 week	6 hours
1M	1 month	1 day
3M	3 months	1 week

**Table 5. Time Windows and Intervals (continued)**

Time Window	Description	Interval
1Y	1 year	2 weeks

**NOTE:** This table lists the interval when the sampling interval is at the default value (1 minute). Changing the sample interval results in interval changes for the 15Min and 1H time windows. If you change the sampling interval to 3 minutes, the interval of the 15Min time window is 3 minutes. If you change the sampling interval to 6 minutes, the interval of the 15Min time window is 3 minutes and the interval of the 1H time window is 6 minutes.

## Temperature Details for a Different Time Window

Click the arrows < > to view the details for the previous/next sampling time, or click the double arrows << >> to view the details for the previous/next page of results for the current time window. You can click Average, Maximum, or Minimum to display the selected value.

- **Average:** The average value from the previous time point to the current time point.
- **Maximum:** The maximum value from the previous time point to the current time point.
- **Minimum:** The minimum value from the previous time point to the current time point.

For example, you view temperature details in the 1H (1 hour) window and the maximum value at 15:00 shows 40°C and the time interval is 6 minutes. This value would represent that the maximum temperature from 14:54 to 15:00 is 40°C.

## Chassis Details

The **Chassis Details** table appears when you select a chassis on the Devices screen. **Chassis Details** lists all blade servers within the chassis and their temperature details in a table, including:

- **Device:** Device name.
- **Average:** The average value of the latest sampling interval.
- **Maximum:** The maximum value of the latest sampling interval.
- **Minimum:** The minimum value of the latest sampling interval.

**NOTE:** You can set the time interval (the period from a time point to the next time point) in the **Settings > General** page. For information on configuring the interval, see [Monitoring Settings](#).

**NOTE:** The **Average**, **Maximum**, or **Minimum** field displays **NA** if no data is available—for example, when the blade server is an Unsupported device.


## Viewing a temperature history graph

OpenManage Power Center provides a visual representation of the temperature history of your system devices.

1. In the left pane, click **Devices > All Devices** or **Devices > Managed Group**.
2. From the list of devices, select a device.  
The details of the device are displayed in the **Details** section.
3. In the **Details** section, click the **Thresholds** tab.  
Alternately, you can also click **Thermal History** in the **Summary** tab.
4. Click **View History** next to **Average Inlet Temperature Alert Thresholds**.  
The **Thermal History — <device> Group** window is displayed.
5. Select the time period and attributes displayed:
  - a. To select the time period represented in the graph, click the buttons along the top of the graph.
  - b. To add or delete attributes, select from the listed options; click the option to toggle its addition or removal from the graph:



- Minimum
- Maximum
- Average

 **NOTE:** To view specific numbers related to each attribute displayed along any portion of the graph, move the pointer over the graph.

6. To move along the data stream over time, click the navigation arrows below the graph.

## Monitoring the Temperature of the Chassis/Blade Server


You can monitor the inlet temperature at the blade server level.

You can also monitor the inlet temperature at the chassis level, including average, maximum, and minimum details.

## Applying circuit breaker limits to chassis

OpenManage Power Center enables you to place circuit breaker, or static power cap limits on chassis that support M1000E 4.4 or later and VRTX 1.35 or later.

1. In the left pane, click **Devices > All Devices** or **Devices > Managed Groups**.
2. From the list of devices, select a specific chassis.  
The details of the selected chassis are displayed in the **<Device> Details > Summary** section.
3. Click **Edit** next to **Chassis Circuit Breaker**.  
The **Edit Chassis Circuit Breaker** window is displayed.
4. Enter the **Chassis Circuit Breaker Cap**, **Chassis Lower Bound**, and **Chassis Upper Bound** values for the selected chassis.

 **NOTE:** The power cap range for MX7000 device changes dynamically when you add new blades. It is recommended to create a periodic discovery task to rediscover the MX7000 device. After you discover the device, the chassis circuit breaker lower and upper bound limits are updated.

5. Click **Save** to apply your changes, or click **Cancel** to discard your changes.

## Monitoring the Temperature of Devices/Groups

Power Center supports temperature monitoring of the inlet temperature span for devices and groups. The inlet temperature span is the average inlet temperature differential between the maximum and minimum temperature reading for a device in a group (Celsius or Fahrenheit). You can calculate this value according to the maximum and minimum temperature from the **Temperature Details** graph.

# Policies

A power policy is a set of configurations to manage the power cap for a device or group. A policy is useful for power management in different situations. For example, you can create a policy to:

- **Power Cap** — Make sure that power consumption does not exceed the capacity of the circuit.
- **Control Power Usage** — Schedule power usage according to the workload of the device or group. For example, you can set an aggressive cap when the workload is low, enabling a reduction of power use for your data center.
- **Increase rack density** — For example, monitor the current power consumption of a rack with 10 devices to estimate how many more devices you can add to the rack.

Power Center supports three power cap policy types:

- **Static** — Manually set the power cap for each device in a rack or chassis.
- **Dynamic** — Power Center dynamically allocates the power cap for each device in a group (data center, room, aisle, rack, or chassis).
- **Temperature Triggered Policy** — The power cap is allocated depending on the changes in the temperature, based on the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) standards.

From the **Policies** screen, you can:

- Create a power policy
- Edit a power policy
- Enable or disable a power policy
- Delete a power policy
- Refresh the list of policies
- Filter power policies so only certain policies are displayed
- Sort the list of policies

## Topics:

- [Dynamic power caps](#)
- [Power Policy Capabilities](#)
- [Upgrading Device Power Policy Capability](#)
- [Creating a policy](#)
- [Policy Priority Levels](#)
- [Policy Modes](#)
- [Enabling or disabling a policy](#)
- [Viewing policies in the power details graph](#)
- [Editing a policy](#)
- [Deleting a policy](#)
- [Filtering policies](#)

## Dynamic power caps

The following terms are helpful for understanding how a dynamic power cap works:

- **Consumption** — The amount of power a device is using.
- **Power Cap** — The maximum amount of power that a device is allowed to consume (may not be equal to its demand).

- **Headroom** — The difference between rack power capacity (specified by the user when the rack is added to OpenManage Power Center system) and rack power consumption (determined by the actual power consumption by PDUs added or associated with the rack).
- **Demand** — Amount of power a device requests to accommodate its workload.
- **Estimated maximum power (Estimated max power)** — The maximum power consumption allocation estimated for a device. The estimated max power is considered the peak power consumption by a device.

Dynamic power caps enable all devices to execute workloads without requiring more power than the overall power cap assigned to the group. When choosing a dynamic power cap, remember:

- If lower-priority devices require more power to maintain their cap, they may receive more power than higher-priority devices.
- If the power cap is too restrictive and the group power consumption exceeds the power cap, an error event occurs for the policy. If this occurs frequently, reconsider your power allocations, or adjust workloads accordingly.
- If fluctuations in device power requirements occur after the power cap is successfully established, then a device that requires more power may not receive it if the power cap of another device in the policy would be violated. To force one or more devices in a policy to a lower cap, create a static power policy for the device at a lower level (rack or chassis). The most restrictive power cap of the overlapping policies is applied to the device.
- If there is excess available power (known as headroom) after all power capping requirements are met, the excess power is dynamically allocated according to the priority and demand of each device in the power policy.

## Power Policy Capabilities

Power Center defines the following statuses of power policy capabilities for the devices:

- **Unknown** — Shown for unsupported devices or devices that were never connected to Power Center.
- **None** — No power policy capability. You cannot set any policy on the device.
- **Monitor** — With power monitoring capability only.
- **Monitor & Capping** — With power monitoring and capping capabilities.
- **Monitor and Upgradable** — With power monitoring capability, and can be upgraded to have power capping capability.

You can find this power policy capability status in the **Power Capability** column of the **Devices** page.

For servers that comply with iDRAC7, when there is a power policy capability change due to a license change, Power Center changes its information in the management console within 24 hours. There are two scenarios:

### Scenario 1 — The license expires or is not imported

In this case, the following happens:

- If a policy exists on the devices, a "Server Capabilities Changed" event is generated.
- The **Policies** tab of the devices is set to disabled in the **Groups** page.
- The power capability status of the devices is set to "None" in the **Devices** page.
- You cannot edit the policy of this device from the **Policies** page; you can only delete it.

### Scenario 2 — You try to import a license on a device without a license imported

In this case, the following happens:

- If a policy exists on the devices, a "Server Capabilities Changed" event is generated.
- The **Policies** tab of the devices is set to **Enabled** in the **Groups** page.

The power capability status of the devices is changed in the **Devices** page.

The policy of the devices is editable. You can access it from the **Policies** page.

## Upgrading Device Power Policy Capability

The power policy capability of some devices can be upgraded to include capping of power consumption—for example, PowerEdge M620. These devices show **Monitor and Upgradable**. To upgrade the device so that its power consumption can be capped, go to the **Devices** page and click **Upgrade** next to the device, then follow the instructions on the pop-up help page to upgrade the device power capability. Once the upgrade is completed, the power capability status changes to **Monitor & Capping** within 24 hours.


## Creating a policy

You can create static power policies for a rack, chassis, or device. You can create dynamic power policies for any group or device, and temperature triggered policy to monitor the temperature.. Power policies apply only to the groups and devices that have monitoring and capping power capabilities.


 **NOTE:** You can also create policies from the **Devices > All Devices > Policies** or **Devices > Managed Groups > Policies** tabs.


1. In the left pane, click **Policies**.  
The **Policies** screen is displayed.
2. In the task menu, click **New Policy**.  
The **Create New Policy** wizard is displayed.
3. In the **Select a Group or Device** window, enter a name for the policy in the **Policy Name** text box. The name should be fewer than 25 characters in length.
4. In the **Grouped Devices** tab, select the device group or in the **Unassigned** tab, select the devices to which you want to apply the policy.
5. Click **Next** to continue, or click **Cancel** to return to the **Policies** screen.
6. In the **Power Cap Values** window, select the type of the policy from the **Policy Type** drop-down list.  
The available options are:
  - STATIC
  - DYNAMIC
  - TEMPERATURE TRIGGERED POWER POLICY

 **NOTE:** This step is applicable only to racks and chassis.

 **NOTE:** The following steps are applicable if you select **STATIC** or **DYNAMIC** power policy.

7. From the **Power monitoring values are for a fixed time period** drop-down list, select the power cap values.  
The possible options are:
  - Previous hour
  - Previous day
  - Previous week
  - Previous month
  - Previous quarter
8. Enter a value in the **Power Cap Value** text box.
9. Click **Next** to continue, click **Back** to return to the previous screen, or click **Cancel** to discontinue the task.
10. In the **Power Cap Priorities** window, select an option from the **Priority** drop-down list to set the capping priority for each device in the group.  
The available options are:
  - Low
  - Medium
  - High

 **NOTE:** The **Power Cap Priorities** window is accessible only when you select a device group.

11. Click **Next** to continue, click **Back** to return to the previous screen, or click **Cancel** to discontinue the task.
12. In the **Power Policy Schedule** window, set the monitoring schedule for the policy.
  - **Time Span** — Always or a range (enter start and end time in the format hh:mm using 24-hour time)
  - **Recurrence Pattern** — Always or specific days of the week
  - **Recurrence Range** — Always or a range (enter start and end dates)
13.  **NOTE:** The following steps are applicable only if you choose **TEMPERATURE TRIGGERED POWER POLICY** option. If you choose **STATIC** or **DYNAMIC** power policy, you can skip the 13th, 14th, and the 15th step.

Select the time period to monitor the temperature. The available options are **Previous hour**, **Previous day**, **Previous week**, **Previous month**, **Previous quarter**.
14. Select the required ASHRAE class from the drop-down menu.

The temperature threshold for the selected ASHRAE class is populated automatically.
15. Click **Next** to schedule the policy. The available options are **Always** and **Range**.
16. Click **Next** to view the summary of the policy you created.
17. In the **Summary** window, click **Finish** to save the policy, click **Back** to review the policy information, or click **Cancel** to discard the changes.

The new policy is effective immediately.

## Policy Priority Levels

When you create or update a policy, you can select different priority levels for each device/group. For example, you can set priority levels based on the service level agreements associated with workloads running on a device/group.

Power Center tends to reserve more power to the devices/groups with higher priority when the power cap for devices/groups is not fully utilized.

For each device/group, you can set one of the three priority levels:

- Low
- Medium (Default)
- High

Priority lists are policy-specific; however, a device/group may have different priority levels in different policies. A higher-priority value of a device/group in a policy overrides the lower-priority value of the same node in another policy.

For example, you created Policy1 for device <A, B, C> and Policy2 for device <B, C, D>, and you configured different priorities or power caps for the policy with the same time slot. In this case, Power Center follows these rules:

- If there are overlapping policies on an entity, the policy with the lowest power cap is applied.
- If there are overlapping dynamic policies on an entity and both are currently active, the highest priority (High > Medium > Low) of this entity is applied.

## Policy Modes

The policy mode is shown in the Enabled and Active columns in the **Policies** page. A green symbol indicates Enabled or Active. Power Center supports three policy modes:

**Table 6. Policy Modes**


Enabled Column	Active Column	Mode	Description
Green	Green	Enabled and active	The policy is in use now.
Green	NA	Enabled but not active	The policy is available but not in use now.

**Table 6. Policy Modes (continued)**

NA	NA	Disabled	The policy is created but not available for use.
----	----	----------	--

## Enabling or disabling a policy

1. In the left pane, click **Policies**.  
The **Policies** screen is displayed.
2. In the list of policies, select the check box next to the policy or policies that you want to enable or disable.
3. In the task menu, click **Enable** or **Disable**.

 **NOTE:** The **Enable** and/or **Disable** menu options are available only when you select a policy.


## Viewing policies in the power details graph

1. In the left pane, click **Devices** > **All Devices** or **Devices** > **Managed Groups**.
2. Select the check box next to a device or device group.  
The details of the selected device or device group are displayed in the bottom section of the screen.
3. Click the **Policies** tab to view the policies associated with the device or device group.

## Editing a policy

You can edit only one policy at a time.


1. In the left pane, click **Policies**.  
The **Policies** screen is displayed.
2. In the list of policies, select the check box next to the policy that you want to edit.
3. In the task menu, click **Edit**.  
The **Edit Policy** wizard is displayed.
4. Make the required changes.

 **NOTE:** You cannot change the selected device or group while editing a policy.

5. In the **Summary** screen, review the changes and click **Finish** to save the changes, click **Back** to return to the previous screen, or click **Cancel** to discard the changes.

## Deleting a policy

1. In the left pane, click **Policies**.  
The **Policies** screen is displayed.
2. In the list of policies, select the check box next to the policy that you want to delete.

 **NOTE:** You can select more than one policy to at a time.

3. In the task menu, click **Delete**.  
The following message is displayed : **Are you sure you want to delete the selected item(s)?**
4. Click **Yes**.

## Filtering policies

You can filter policies so they display according to type, power cap, status, and/or other attributes.

1. In the left pane, click **Policies**.


The **Policies** screen is displayed.

2. In the task menu, click **Filter**.

The **Policy Filter** window is displayed.

 **NOTE:** The **Policy Filter** wizard is displayed only if you have at least one policy.

3. Select an existing filter from the **Select Filter** drop-down list and run it or proceed to step 4.
4. Under **Quick View**, select the **Policy Type** check box and then select the **Static**, **Dynamic**, or **Temperature** option.
5. Select one or more of the following options:
  - Select the **Power Cap** or **Temperature Threshold** check box and then enter values in the **Minimum** and/or **Maximum** text boxes.
  - Select the **Policy Enabled** check box and then select the **Yes** or **No** option.
  - Select the **Policy Activated** check box and select the **Yes** or **No** option.

 **NOTE:** Policy filters stay in effect until they are cleared or until you close the session.

 **NOTE:** **Power Cap** and **Temperature Threshold** options are displayed based on the chosen policy type.

6. Click **Run Once** to view a filtered list of policies.

OR

- Enter a name for the filter in the **Filter Name (Optional)** text box and click **Save and Run** to save the filter and sort the policies based on the filter criteria.

OR

- Click **Cancel** to discard the selections and return to the **Policies** screen.

You can use the saved filters later.

# Analysis

This chapter provides information about various graphs and helps in analyzing the artifacts derived from the observation.

The Analysis feature enables you to view a graphical representation of the server characteristics, power or thermal characteristics, and also the underutilized servers. You can export the report in XML or CSV format. The graphs are useful in analyzing the power and thermal issues, to measure the server characteristics and utilize them efficiently.

In the left pane, click **Analysis**. On this screen, you can:

- View server power characteristics
- View peak power and idle power distribution
- View underutilized servers
- View power and thermal information

## Topics:

- [Server characteristics](#)
- [Underutilized servers](#)
- [Power Analysis](#)
- [Cooling Analysis](#)

## Server characteristics

Using OMPC you can view the power consumption at a single-server level. The power consumption reading from a single-server perspective is useful in capacity planning of a data center.

Currently, to view the server power characteristics, the dependency is on the nameplate of the server or an estimated value, which may vary from the actual value. OMPC collects information about the power consumption of all servers. Using the server power characteristics feature, OMPC classifies and represents the overall power consumption of each device based on the actual usage.

**NOTE:** All the servers (Dell and non-Dell) are categorized based on the support provided for the power monitoring capability feature along with the servers which provide instantaneous power.

**NOTE:** Chassis or any of the enclosure devices are not considered for the analysis as the number of blades used in the enclosure may vary.

## Viewing server power characteristics graph

OMPC enables you to view the details about the server power consumption from a single server perspective.

1. In the left pane, click **Analysis > Server Characteristics**.
2. In the task menu, click **Graphical View**.  
The **Server Power Characteristics** graph is displayed. The graph displays the minimum and the maximum power consumption of all server models.

## Viewing peak power distribution graph

OMPC enables you to view the details about the distribution of peak power for the servers.

1. In the left pane, click **Analysis > Server Characteristics**.
2. In the task menu, click **Peak Power**.  
The **Peak Power Distribution — <Server>** graph is displayed.



3. Set the power range distribution value by typing the value in **Set Y-axis Power Range Granularity** text box and click **Apply**.  
The graph with the minimum and the maximum power distribution of the server models is displayed.

## Viewing active idle power distribution graph

OMPC enables you to view the details about the distribution of idle power that is the lowest power observed for a specific time duration.

1. In the left pane, click **Analysis > Server Characteristics**.
2. In the task menu, click **Active Idle Power**.  
The **Active Idle Power — <Server>** graph is displayed.
3. Set the distribution range value by typing the value in **Set Y-axis Power Range Granularity** text box and click **Apply**.  
The graph with the minimum and the maximum active idle power distribution of the server models is displayed.

## Exporting server power report

OMPC enables you to export the server power report to a local drive on your system.

1. In the left pane, click **Analysis > Server Characteristics**.
2. In the task menu, click **Export All**.  
The report downloads to your local system in \*.CSV format. The filename includes the date and time. For example, ServerPowerCharacteristics-20150513-124005.csv

## Underutilized servers

OMPC helps you in identifying the servers that are not utilized efficiently. The observed data is important in understanding the overall utilization of servers in a data center and helps in distributing the workload efficiently.

The server utilization in a data center is calculated using the formula,

- `Maximum value of CUPS indices for CPU, Memory bandwidth and I/O bandwidth, if available`

or,

- `(Current Power - Idle Power) / (Power Capacity - Idle Power)`

where,

- Current power is the power used by the server
- Idle power is the power consumption when server is idle
- Power capacity is the maximum of (2 \* idle power, observed maximum power).

The following formulae is used in calculating the underutilization value of a server,

`Servers with an average utilization of less than or equal to <X>`

, where <X> represents a utilization percentage. The range is between 80% to 20%, by default the value is set to 15.

`Servers with <Y> percentile utilization being less than or equal to <X>.`

, where <Y> is the percentile. The range is between 0% to 20%, by default the value is set to 95.

## Configuring underutilized servers settings

OMPC enables you to view the underutilized servers based on the power consumption.

1. In the left pane, click **Analysis > Underutilized Servers** and then click .

2. Enter a value in **Power Utilization (X)** text box and **Percentile Utilization (Y)** text box.

**NOTE:** The range for **Power Utilization** is 0–20. By default, the value is set to 15.

**NOTE:** The range for **Percentile Utilization** is 80–100. By default, the value is set to 95.

3. Click **Save**.

## Power Analysis

OMPC helps you in monitoring and managing power in a data center. The observed monitoring data is helpful in planning capacity expansion, placement suggestions.

In the left pane, click **Analysis > Power Analysis**. The **Power Analysis** screen is displayed. On this screen, you can:

- Perform data center capacity expansion planning
- Analyze and view the placement suggestions
- Analyze and view power and space gains from underutilized servers

## Analyzing capacity expansion

1. In the left pane, click **Analysis** and then click **Power Analysis**.  
The **Power & Space Analysis** page is displayed.
2. In the **Capacity Planning** tab, select applicable check box against the device group.
3. Select the required server model for analysis from the **Select Server Model** section.  
Provide the number of servers and the priority of those servers in the respective fields.
4. Click **Analyze** to analyze the capacity for selected servers.  
You can view the details of the analysis in **Resource Availability** section.



You can also export the report to the required location on the system.

## Viewing placement suggestions



1. In the left pane, click **Analysis** and then click **Power Analysis**.  
The **Power & Space Analysis** page is displayed.
2. In the **Placement Suggestions Based on Available Power and Space** section, click **Launch**.  
**Placement Suggestion** window is displayed.
3. From the **Group Selection** tab, select the data centers by clicking **+** to analyze the availability of power and space. Click **Next**.
4. In the **Placement Type** tab, select the type of placement required from the drop-down list. The available options are **Auto** and **Manual**. By default, **Auto** option is selected.
5. Select the server model from the **Server Model** drop-down list for which you require placement suggestions.
6. Enter the number of servers in the **Server Count** text field.
7. Select the criteria in which the racks are selected and click **Next**. The available options are:

**Table 7. Placement Suggestions options**

Option	Description
<b>Equal rack priority</b>	Select racks with equal priority
<b>Highest space headroom</b>	Select racks with higher space headroom
<b>Highest power headroom</b>	Select racks with higher power headroom
<b>Lowest space headroom</b>	Select racks with lowest space headroom
<b>Lowest power headroom</b>	Select racks with lowest power headroom

8. In the **Rack Placement** tab, information about the availability of power and space before and after allocation is displayed. You can set the weightage of the racks by typing the required value in **Weightage** column of the **Set the rack placement priority** section and click **Next**.
9. The placement suggestions are provided in the **Rack Placement Result** section. Analyze the result and click **Next**.  
 **NOTE:** Click **Add Another Model** to repeat the same procedure with a different server model.
10. The summary of the analysis is displayed in the **Summary** screen. Click **Finish**.  
 **NOTE:** You can also export the report to the required location on the system.

## Viewing resource suggestions

1. In the left pane, click **Analysis** and then click **Power Analysis**. The **Power & Space Analysis** page is displayed.
2. In the **Power and Space Gains from Underutilized Server(s)** section, click **Launch**. **Power and Space Savings** window is displayed.
3. From the **Server Selection** tab, details about the underutilized servers are displayed. Select the servers by clicking the check box next to each server. You can also select all the servers by selecting **Consider all underutilized servers** option. Click **Next**.
4. The summary of the analysis is displayed in the **Summary** screen. Click **Finish**.  
 **NOTE:** You can also export the report to the required location on the system.  
 **NOTE:** The estimated data should be used as a reference for planning as the final value may change during plan execution.



## Cooling Analysis

OMPC helps you in monitoring the temperature sensors of the supported devices in a data center. The observed data is helpful in identifying the potential cooling issues of all the rooms in a data center.

In the left pane, click **Analysis > Cooling Analysis**. The **Cooling Analysis** screen is displayed. On this screen, you can view:

- Hot spot room
- Over cooled room
- Large temperature span room
- Hot outlier room

## Configuring cooling analysis settings

1. In the left pane, click **Analysis** and then click **Cooling Analysis**. The **Data center Cooling Analysis** page is displayed.
2. Click . **Cooling Analysis Settings** window is displayed.
3. Select the threshold temperature from the drop-down list to classify a room as Hot Room.  
 **NOTE:** Values for **Over Cooled Rooms** and **Large Temperature Span Rooms** are present by default.
4. In the **Hot Outlier Devices** section, type a value in the text box to classify a device as a **Hot Outlier Device**. A device is classified as a **Hot Outlier Device** if it exceeds the defined value.

## Viewing a hot spot room

1. In the left pane, click **Analysis** and then click **Cooling Analysis**. The **Datacenter Cooling Analysis** page is displayed.

2. In the **Hot Spot Room** section, you can view the rooms that are the hottest in the data center. Click on any room that is listed.  
**Room <number>: Device(s) Under Hot Spot Room** window is displayed. The details of the devices are displayed.
3. Click **Close**.

## Viewing an over cooled room

1. In the left pane, click **Analysis** and then click **Cooling Analysis**.  
The **Data center Cooling Analysis** page is displayed.
2. In the **Over Cooled Rooms** section, you can view the rooms that are the coolest in the data center. Click on any room that is listed.  
**Room <number>: Over Cooled Room** window is displayed. The details of the devices are displayed along with the reason for the scenario along with the resolution.
3. Click **Close**.

## Viewing devices under large temperature span room

1. In the left pane, click **Analysis** and then click **Cooling Analysis**.  
The **Data center Cooling Analysis** page is displayed.
2. In the **Large Temperature Span Rooms** section, you can view the rooms with a large temperature difference between the inlet temperature and over cooling threshold value. Click on any room that is listed.  
**Room <number>: Devices Under Large Temperature Span Room** window is displayed. The details of the devices are displayed along with the reason for the scenario along with the resolution.
3. Click **Close**.

## Viewing devices under hot outlier room

1. In the left pane, click **Analysis** and then click **Cooling Analysis**.  
The **Data center Cooling Analysis** page is displayed.
2. In the **Hot Outlier Devices** section, you can view the rooms in which are classified as hot outlier room.  
**Room <number>: Devices Under Hot Outlier Room** window is displayed. The details of the devices are displayed along with the reason for the scenario along with the resolution.
3. Click **Close**.

## Managing reports

This chapter provides information on periodically generating reports for inventory and monitoring and managing the reports.

Pre-defined templates are provided to help you generate the reports. By default, the reports are generated in HTML format. You can download the reports in XML or CSV format.

In the left pane, click **Reports**. The **Reports** screen is displayed. On this screen, you can:

- View report details
- Create reports
- Edit reports
- Delete reports
- Refresh the reports list
- Add or edit report groups
- Set estimated max power
- Filter reports

The following types of reports can be generated using OpenManage Power Center:

- **Power Hoarders** — The Power Hoarder report displays the devices that are the largest consumers of power. The result is calculated considering the highest average power consumption of the devices over a specific time period.
- **Power Frugal** — The Power Frugal report displays the devices that are the least consumers of power. The result is calculated considering the lowest average power consumption of the devices over a specific time period.
- **Power Data** — The Power Data report displays the power consumption data for the selected devices or device groups. The data comprises of the minimum, maximum, highest or lowest average power consumption.
- **Power Headroom** — The Power Headroom report displays the total power consumption and the unused power data for the selected devices or device groups.
- **General Inventory** — The General Inventory report displays the inventory data for the selected devices or device groups.
- **Power Hoarders Rack** — The Power Hoarders Rack report displays the rack devices that are the maximum power consumers. The result is calculated considering the lowest headroom of the devices over a specific time period.
- **Power Frugal Rack** — The Power Frugal Rack report displays the rack devices that are the least power consumers. The result is calculated considering the highest headroom of the devices over a specific time period.
- **Raw Monitoring Data** — The Raw Monitoring Data report displays the monitoring data for the selected devices or device groups.
- **Comparison Report** — The Comparison report displays the result obtained on comparing a minimum of two or a maximum of three devices or device groups.
- **Thermal Data** — The Thermal data report displays the observed temperature values for the selected devices or device groups.
- **Power Utilization** — The Power utilization report displays the power utilization for the selected devices or device groups.
- **Power Threshold Violations** — The Power threshold violation reports displays the information about the power threshold violations for the selected devices or device groups.
- **Power Cap Violations** — The Power cap violations report displays the violations observed in the device or the device group power cap level.
- **Power Cap Settings** — The Power cap settings report displays the settings of the device or the device group power cap level.
- **Threshold Settings** — The Threshold settings report displays the threshold settings of the device or the device group.
- **Rack Fragmentation Hoarders** — The Rack fragmentation hoarders report displays the racks that are the most fragmented.
- **Rack Space Hoarders** — The Rack space hoarders report displays the racks with the highest rack space utilization.
- **Rack Space Frugal** — The Rack space frugal report displays the racks with the lowest rack space utilization.
- **Highest Temperature** — The Highest temperature report displays the devices that has the highest temperature.
- **Lowest Temperature** — The Lowest temperature report displays the devices that has the lowest temperature.
- **Events Reports** — The Events report displays the events with a specified severity level for a specified time-period.
- **PDU Outlet Assignment** — The PDU outlet assignment report displays the PDU name, PDU IP, PDU location, PDU outlet assignment and other relevant details.
- **PDU Sensor Report** — The PDU sensor report displays the PDU environment sensors information and other relevant details.

- Thermal Event Policy — The thermal event policy report displays the thermal event based policy settings and other relevant details.
- VM Power Hoarders — The VM Power Hoarders report displays the details of virtual machines that consume more power.
- VM Power Frugal — The VM Power Frugal report displays the details of the virtual machines that consume the least power.
- VM General Inventory— The VM General Inventory report displays the inventory details of the virtual machines.

### Topics:

- [Viewing Report Details](#)
- [Creating reports](#)
- [Editing reports](#)
- [Deleting reports](#)
- [Adding report groups](#)
- [Editing report groups](#)
- [Deleting report groups](#)

## Viewing Report Details

You can view the details of a particular report in the Reports list, in the bottom section of the **Reports** screen.

On the **Reports** screen, click the report name whose details you want to view. The details are displayed in the following tabs.

- Summary — Displays information such as the name, description, report group, and selected attributes of the report.
- Results — Displays the results for the attributes that were selected while creating the report.

You can export the report in CSV or XML format to the required location on your system.

## Creating reports

1. In the left pane, click **Reports > New Reports**.
2. Select a report type from the drop-down list. The available options are:
  - Power Hoarders
  - Power Frugal
  - Power Data
  - Power Headroom
  - General Inventory
  - Power Hoarders Rack
  - Power Frugal Rack
  - Raw Monitoring Data
  - Comparison Report
  - Thermal Data
  - Power Utilization
  - Power Threshold Violations
  - Power Cap Violations
  - Power Cap Settings
  - Threshold Settings
  - Rack Fragmentation Hoarders
  - Rack Space Hoarders
  - Rack Space Frugal
  - Highest Temperature
  - Lowest Temperature
  - Events Report
  - PDU Assignment Report
  - PDU Sensor Report
  - Thermal Event Policy
  - VM Power Hoarders
  - VM Power Frugal

- VM General Inventory


The **New Report** wizard is displayed.


3. Enter a name for the report in the **Name** text box.

4. Under **Duration**, select one of the following options

- **Last One** — Select one of the following options from the drop-down list:
  - Hour(s)
  - Day(s)
  - Week(s)
  - Month(s)
- **Last** — Enter the number of days in the past for which you want to create the report.
- **Date Range** — Enter the start and end dates of the range for which you want to create the report.

5. Select the **Report Aggregation Period** check box to collate power or thermal related data from the database for a specific period.

 **NOTE:** This option is available only for Power Data, Raw Monitoring data, and Thermal data report types.

 **NOTE:** The power aggregation value for a device or group is calculated accurately, only if the power data for the specified **Report Aggregation Period** is available in the database.

6. Select an option from the **Report Aggregation Type** drop-down list. The available options are:

- Hour
- Day
- Week
- Month

 **NOTE:** This option is available only for Power Data, Power Headroom, and Raw Monitoring data report types.

7. Enter the report aggregate value in the **Report Aggregation Value** text box and click **Next**.

 **NOTE:** This option is available only for Power Data, Power Headroom, and Raw Monitoring data, and Thermal data report types.

8. In the **Associated Devices/Groups** tab, select the devices or groups for which you want to generate the report.

a. Click the 'plus' icon to add them to the **Selected Devices/Groups** list and click **Next**.

 **NOTE:** This option is displayed only for Power Headroom, General Inventory, Raw monitoring data, Comparison report, PDU outlet assignment, and PDU sensor report types.

 **NOTE:** Starting OMPC 3.2, the **Select All Devices** and **Select All Groups** options are available.

9. In the **Report Attributes** tab, select one or more attributes that you want to include in the report. The attributes displayed are based on the report type you select.

a. From the **Limit Output to** drop-down list, select the output limit for the report. The available options are:

- 10
- 50
- 100
- All

b. From the **Sort by** drop-down list, select an attribute by which you want to sort the report. Select the **Ascending** or **Descending** option to sort the report in that order and click **Next**.

10. In the **Save/Run** tab, do one of the following:

- Select the **Save Only** option to save the report.
- Select the **Save and Run** option to save and run the report and select the **CSV** or **XML** format to export the report in the selected format.

11. Click **Finish** to save the report or save and run the report.

## Editing reports

1. In the left pane, click **Reports**.
2. Select the check box next to the report that you want to edit.
3. In the task menu, click **Edit**.  
The **Edit Report** wizard is displayed.
4. Make the required changes.
5. Click **Finish** to save the changes or click **Cancel** to return to the **Reports** screen without saving the changes.

## Deleting reports

1. In the left pane, click **Reports**.
2. Select the check box next to the report that you want to delete. To delete multiple reports, select the check box next to the **Name** header.
3. In the task menu, click **Delete**.  
The following message is displayed : **Are you sure you want to delete this report(s)? All running instances will be deleted along with this report(s)?**
4. Click **Yes**.

## Adding report groups

The Report Groups feature enables you to classify the reports into different groups. For example, you can create two reports based on the available power data and add them to different groups. This helps you filter and find specific reports.

1. Click **Reports > Report Group**.  
The **Add/Edit/Delete Report Groups** window is displayed.
2. To create a report group, select **New** from the **Group** drop-down list.
3. Enter a name for the report group in the **Name** text box.
4. Enter a description for the report group in the **Description** text box.
5. Click **Save** to save the group or click **Cancel** to return to the **Reports** screen.

## Editing report groups

1. Click **Reports > Report Group**.  
The **Add/Edit/Delete Report Groups** window is displayed.
2. Select the group that you want to edit from the **Group** drop-down list.  
You can edit the name and description of the report group.
3. Click **Save** to save the changes or click **Cancel** to return to the **Reports** screen without saving the changes.

## Deleting report groups

1. Click **Reports > Report Group**.  
The **Add/Edit/Delete Report Groups** window is displayed.
2. Select the group that you want to delete from the **Group** drop-down list.
3. Click **Delete**. The following message is displayed.

Are you sure you want to delete this group? If you delete the group, all reports under this group will be deleted.

4. Click **Yes** to proceed.



# Event Management

This chapter provides information on event types, severity levels, supported UPS/PDU events, and how to manage Power Center events.

You can receive events indicating an abnormal power/temperature situation in the data center. Power Center detects:

- Pre-defined events
- Custom events

Power Center uses port 6553 to listen for internal events. If another application is configured to use port 6553, you must change it to reserve port 6533 for Power Center.

Power Center uses port 162 to listen for events from external devices. If the SNMP Trap service exists and uses port 162, Power Center automatically uses port 1162 to receive external events forwarded by the SNMP trap service.

In the left pane, click **Events**. The **Events** screen is displayed. On this screen, you can:

- Acknowledge Events
- Add a note to an event
- Delete events
- Sort events
- Filter events
- Export events

## Topics:

- [Pre-defined events](#)
- [Custom events](#)
- [Application log events](#)
- [Supported PDU and UPS events](#)
- [Event severity levels](#)
- [Viewing events](#)
- [Sorting events](#)
- [Adding comments to events](#)
- [Deleting events](#)
- [Filtering events](#)
- [Sending test events from an IPMI device](#)

## Pre-defined events

A predefined event is an event that Power Center defines based on system conditions. Device support for events includes:

- UPS/PDU devices – To receive events, you must subscribe to the event from the console of that PDU or UPS.
- PowerEdge tower and rack servers – Support all IPMI events (IPMI Power Unit, IPMI Power Supply, IPMI Processor Temperature Trip, IPMI Fan).
- PowerEdge blade servers – Only support IPMI Processor Temperature Trip events.
- Integrated Dell Remote Access Controller (iDRAC) – Only supports the IPMI trap format. To receive events from an iDRAC device, make sure the alert function is enabled and the IPMI trap format is selected for all Power Center-supported events in the iDRAC management console (IPMI Power Unit, IPMI Power Supply, IPMI Processor Temperature Trip, IPMI Fan). For example, in the iDRAC7 management console, you must select IPMI trap for all PWR/PSU/CPU/Fan-related alerts.

 **NOTE:** For more information on using the iDRAC management console, see iDRAC documentation.

**Table 8. Power Center events and severity levels**

Type	Description	Severity Level
Blades Change In Chassis	Some blades in a chassis have changed; you must manually rediscover the chassis. Power Center detects chassis changes once every 15 minutes	Informative
Cannot Register for Events	The device cannot register device events to the Power Center server automatically.	Warning
Chassis Power Control Capabilities Changed	The circuit breaker power control (system input power cap) capability on the chassis no longer exist.	Critical
CMC SNMP Event	Event received from chassis	Critical or Warning
Communication with Chassis Failed	Power Center lost communication with the chassis.	Warning
Communication with Chassis Restored	Power Center restored communication with the chassis.	Informative
Communication with Device Failed	Power Center lost communication with the device.	Warning
Communication with Device Restored	Power Center restored communication with the device.	Informative
Device Hostname Changed	Device hostname is changed.	Informative
Entity Capabilities Changed	Entity capabilities changed.	Warning
Failed to Set Sampling Interval on Device	Failed to set sampling interval for the device. The sample interval might not be supported by device.	Warning
iDRAC SNMP Event	Event received from iDRAC.	Critical or Warning
IPMI Fan	Events related to the server fan.	Critical
IPMI Power Supply	Events related to the server.	Critical
IPMI Power Unit	Events related to the server power unit.	Critical
IPMI Processor Temperature Trip	Events related to the server processor temperature trip.	Critical
IPMI Test	An IPMI test event was received.	Informative
MPCM Configure Failed	Failed to set MPCM on the chassis.	Warning
MPCM Not Supported	The Dell chassis does not support MPCM. Upgrading firmware on the chassis might be required.	Warning
PDU High Load	The PDU power is greater than the high load threshold.	Warning

**Table 8. Power Center events and severity levels (continued)**

Type	Description	Severity Level
PDU Low Load	The PDU power is lower than the low load threshold.	Warning
PDU Outlet High Load	The PDU outlet power is greater than the high load threshold.	Warning
PDU Outlet Low Load	The PDU outlet power is lower than the low load threshold.	Warning
PDU Outlet Off	The PDU outlet is Off.	Informative
PDU Outlet On	The PDU outlet is On.	Informative
PDU Outlet Overload	The PDU outlet is overloaded.	Critical
PDU Overload	The PDU is overloaded.	Critical
Protocol Operation Failed	Device protocol operation failed.	Warning
Server Capabilities Changed	The server capabilities have changed, for example, a license change. This event is only applicable to a device that has a policy applied. When you see such an event, check the policy on the device.	Warning
Unsupported Sampling Interval	Cannot set sampling interval to device. iDRAC 6 devices with a BMC firmware version older than version 1.5 only support a 1-minute sampling interval. Use a 1-minute sampling interval for such device, or upgrade the BMC firmware to newer version.	Warning
UPS Battery Failed	Events related to battery failure in the UPS.	Critical
UPS Battery Low	Events related to low battery limits and exceeded thresholds in the UPS.	Critical
UPS Bypass Failure	Events related to bypass failure in the UPS.	Critical
UPS Charge Failure	Events related to charge failure in the UPS.	Critical
UPS Communication Lost	Events related to communication lost in the UPS.	Warning
UPS Fan Failure	Events related to power fan failure in the UPS.	Critical
UPS Input Power	Events related to power input failure in the UPS.	Critical
UPS On Bypass	Events related to on bypass in the UPS.	Informative
UPS Output Power	Events related to power output failure in the UPS	Critical

**Table 8. Power Center events and severity levels (continued)**

Type	Description	Severity Level
UPS Overload	Events related to output power load limits and exceeded thresholds in the UPS.	Critical
UPS Shutdown	The UPS has shutdown.	Informative
UPS Temperature Threshold	A UPS temperature threshold was exceeded.	Critical

## Custom events

Custom events that you have set up are automatically triggered when the custom condition threshold is reached.

**Table 9. Power Center custom events**

Type	Description	Severity Level
Average Inlet Temperature	Average temperature is greater or less than the average value you set in the Thresholds	Critical or Warning; depends on the threshold type
Policy Cannot Be Maintained	Policy cannot be maintained because average power consumption of devices with power capping capability that relate to this policy exceed the power cap value of this policy	Critical or Warning
Policy Return To Normal	Policy can now be maintained, because power consumption is less than the power cap value	Informative
Power	Average power consumption is greater than the average value you set in the Thresholds.	Critical or Warning
Power Return To Normal	Power consumption returned to the normal range you set in the Thresholds	Informative
Temperature Return To Normal	Temperature returned to the normal range you set in the Thresholds	Informative

When the following changes occur, then corresponding *Critical* events become *Informative* events:

- Device/group is removed from Power Center.
- Event condition is removed from Power Center; for example, the Threshold settings.
- Event condition is updated in Power Center; for example, the Threshold settings.
- Power policy is removed or disabled.
- *Policy Return To Normal* event is triggered.

For example, when the *Power/Temperature Return to Normal* event is triggered, the corresponding *Critical* or *Warning* event becomes an *Informative* event. Using the Average Inlet Temperature as an example: If you set 50 °C as the *Critical* threshold and 40 °C as the *Warning* threshold, then *Critical* and *Warning* events are sent when the average temperature reaches 60 °C. When the average temperature returns to 45 °C, the *Critical* event automatically becomes *Informative*. When the average temperature returns to 35 °C, the *Warning* event automatically becomes *Informative*.

# Application log events

The application log contains information about informational or unexpected events, or internal errors that occur in OpenManage Power Center.

**Table 10. Application log events**

Type	Severity	Functional area	Description
Internal Error	Warning	Service	Power Center internal error.
Duplicated Managed Devices	Warning	Discovery	Duplicated device identified.
Group Structure Change Policy	Warning	Policy	A group structure has affected a policy.
Database Maintenance Successful	Informative	Service	Database maintenance was successful.
Protocol Timeout Change Failed	Warning	Monitor	The protocol timeout change failed.
Duplicate Device Deleted	Informative	Discovery	The duplicated device has been deleted.
Email Failure	Warning	Event	The email alert for the event has failed. SMTP or Alert Settings might be incorrect.
Internal Database Operation Error	Warning	Service	Internal database operation failed.
Discovery In Progress	Warning	Discovery	Current round of scheduled discovery task is skipped because a previously scheduled instance is still underway.
Chassis Inventory In Progress	Warning	Discovery	Current round of chassis inventory task is skipped because a previously instance is still underway.
Re-run Running Discovery Task	Warning	Discovery	Previous discovery task is stopped as a user has re-run this task.
License Violation Detected	Critical	License	License violation has been detected.
License Violation Rectified	Informative	License	License violation has been rectified.
Policy On Non Power Capping Device	Warning	Policy	The device's power capping capability is removed.
Application Logs Cleared	Informative	Log	All application logs have been removed.
Require License For Power Policy	Warning	License	Failed to set power policy due to insufficient license.


# Supported PDU and UPS events

Power Center supports events for different PDU and UPS devices. The following table lists the events that are validated by Power Center for specific devices. There may be other events not mentioned in this table.


**Table 11. PDU and UPS events**

PDU/UPS Model	Supported Events
Dell UPS	UPS Low Battery, UPS Bad Input
APC UPS	UPS Low Battery, UPS Shutdown, UPS On Bypass
Eaton UPS	UPS Low Battery, UPS Bad Input, UPS Bad Battery




**Table 11. PDU and UPS events (continued)**

Emerson UPS	UPS Low Battery
Dell PDU	PDU Low Load, PDU High Load, PDU Overload, PDU Outlet Low Load*, PDU Outlet High Load*, PDU Outlet Overload*, PDU Outlet On*, PDU Outlet Off*   <b>NOTE:</b> Events marked with * are only supported on Dell Managed Rack PDU 6605.
APC PDU	PDU Low Load, PDU High Load, PDU Overload
ServerTech PDU	PDU High Load, PDU Outlet On, PDU_Outlet Off
Emerson PDU	PDU Low Load, PDU High Load, PDU Overload

## Event severity levels

 **NOTE:** Severity levels defined in Power Center may be inconsistent with the levels defined on monitored devices. For example, an event defined as severe on a device might be considered a warning event in Power Center.

**Table 12. Power Center event severity levels**

Severity Level	Icon	Description
Critical		Errors that cause managed devices or Power Center to stop working properly. You must take action to resolve the issue.
Warning		Errors requiring attention. You should look into the root cause to determine whether to take action.
Informative		Event that is not an error or warning. This is an informational event; you do not need to take action.


## Viewing events

The number of events is displayed at the top-right corner on the OpenManage Power Center screen.

There are several ways to view Power Center events:

- *Using the left pane:* — In the left pane, click **Events**.
- *Using the Critical Event Notification icon:*
  1. Click the Critical Event Notification icon in the upper right corner of the OpenManage Power Center screen.  
A list of the recent critical events is displayed.
  2. Click **View Events**.  
The **Events** screen with the list of events is displayed.
- *From the Home screen:*
  1. In the left pane, click **Home**.  
The **Events (Overall)** and **Events (Top 5 Groups)** graphs are displayed.
  2. Click **View Events**.

The **Events** screen with the list of events is displayed.

 **NOTE:** By default, the protocol error events are hidden. To view these events, click **Settings > Database**. In the **Events Logs Settings** section, uncheck the **Ignore Protocol Operation Events(s)** option.

## Sorting events


1. In the left pane, click **Events**.  
By default, events are listed by **Date** in descending order (from most recent to older).
2. To sort the list by fields other than the date, click the 'up' or 'down' arrow next to one of the following column headers.
  - Severity
  - Entity
  - Event Type
  - Acknowledged By
  - Date
  - Notes

The 'up' or 'down' arrow is displayed next to the column header by which the display is sorted.

## Adding comments to events

1. In the left pane, click **Events**.
2. In the **Notes** column for the event for which you want to comment, click .  
The **Add Comment** window is displayed.
3. Enter your comment in the **Note** text box. The maximum length for a comment is 512 characters.  
If other users have commented on the event, their comments are displayed below the **Note** text box. The name of the user, timestamp of the comment, and description of the comment are displayed.

 **NOTE:** You cannot edit or delete a comment after you save it; you can only add additional comments.
4. Click **Add** to save your comment, or click **Cancel** to discard your changes and return to the **Events** screen.  
Power Center automatically adds the **User Name** and **Time Stamp** information to each comment.

After a comment is added for an event,  is displayed in the **Notes** column for the event.

## Deleting events

1. In the left pane, click **Events**.  
The **Events** screen is displayed.
2. Select the check box next to the event or events that you want to delete.  
If you want to delete all the events in the list, select the check box next to **Severity**.
3. In the task menu, click **Delete**.  
The following message is displayed.

Are you sure you want to delete the selected item(s)?

4. Click **Yes** to proceed with the deletion.

 **NOTE:** You also have the option to delete all the events by clicking **Delete All**.

# Filtering events

The Events Filter feature helps you to view events of specific types, severity levels, Acknowledged By user name, and/or events that occur within a specific time period.

1. In the left pane, click **Events**.
2. In the task menu, click **Filter**.  
The **Events Filter** window is displayed.
3. Do one or more of the following:
  - Select an **Entity Type** from the drop-down list. The available options are:
    - Server
    - PDU
    - UPS
    - Chassis
    - Data Center
    - Room
    - Aisle
    - Rack
    - Custom
    - Hypervisor
  - Select an **Event Type** from the drop-down list. The available options are:
    - Entity Capabilities Changed
    - Cannot Register for Events
    - Communication with Device Failed
    - Communication with Device Restored
  - Select a **Severity** level. The available options are:
    - Critical
    - Warning
    - Information
  - Enter the start and end dates in the **Date From** and **Date To** fields respectively. Use the format MM/DD/YYYY. Only events from 00:00:00 of the start date to 00:00:00 of the day after the end date are displayed. For example, if you enter the filtering option 01-01-2013 as both the start date and end date, then all events from 00:00:00 of 01-01-2013 to 00:00:00 of 01-02-2013 are displayed.
  - Select a user name from the drop-down list in the **Acknowledged By** field to sort by that user name.
4. Click **Run Once** to view a filtered list of events.  
OR
  - Enter a name for the filter in the **Filter Name (Optional)** text box and click **Save and Run** to save the filter and sort the events based on the filter criteria.  
OR
  - Click **Cancel** to discard your selections and return to the **Events** screen.

You can use the saved filters later.

# Sending test events from an IPMI device

Power Center enables you to view test events sent from an IPMI device, therefore, you can verify the event channel between the IPMI device and Power Center server.

Before sending a test event, make sure:


- The IPMI device is added on the **Devices** page.
- The network connection status of the IPMI device is *Connected*.
- The Power Center server address is added in the event destination list of the IPMI device.

To send a test event from an IPMI device, see the following example for a PowerEdge M610 server:



1. Open the iDRAC management console of the M610, and go to the page related to SNMP trap settings.
2. Click **Send** next to the Power Center server address to send a test event.
3. Open the Power Center management console, and click **Event Logs** in the left pane.

The informative event *IPMI Test* appears on the **Event Logs** page.

 **NOTE:** For more information on steps 1 and 2, see the IPMI device documentation.

## Security

Power Center is designed to ensure data confidentiality, data integrity, and the security of user authentication. Power Center not only provides authentication and access control to user accounts (see [Access Control](#)), but also protects all of the communication channels to the Power Center server and the stored sensitive data (for example, passwords) on the Power Center server.

To enhance security for your Power Center system:

- Start services with a normal Windows operating system (OS) user account: After installation, Power Center services are logged on with the Network Service account by default. You can use a normal Windows OS user account instead of the Network Service account to provide better security.
- OS hardening: You can apply [OS hardening](#) on the system where Power Center is installed. By doing so, the minimum security foundation is set up for Power Center security-related configurations.
- Audit log: Power Center tracks the action log for critical user operations, including user login/logout, emergency power reduction, start/stop network discovery, security configuration, and policy change.
- Certificate management: To enforce communication confidentiality and data integrity, Power Center enables SSL/TLS communication between the Power Center management console and the Power Center server and between the Power Center server and managed chassis. The SSL/TLS authentication is certificate-based. Power Center uses a Keystore file to manage certificates.

### Topics:

- [Starting Services with a Windows operating system standard user account](#)
- [Operating system hardening](#)
- [Audit log](#)
- [Managing certificates](#)

## Starting Services with a Windows operating system standard user account

To configure a standard Windows user account, follow these steps:

1. Stop all Power Center services.
2. Go to **Control Panel > User Accounts > Manage User Accounts**, and add a new standard user (either local or domain), or select an existing standard user.
3. Grant **Full Control** permission of the following directories or files to the user account.

Directory:

- Dell\OpenManagePowerCenter\bin
- Dell\OpenManagePowerCenter\external\apache-tomcat
- Dell\OpenManagePowerCenter\external\pgsql\bin
- Dell\OpenManagePowerCenter\logs
- Dell\OpenManagePowerCenter\pgdata

File:

- Dell\OpenManagePowerCenter\conf\user.config.xml
- Dell\OpenManagePowerCenter\conf\app.config.xml
- Dell\OpenManagePowerCenter\external\apache-tomcat\conf\context.xml
- Dell\OpenManagePowerCenter\external\apache-tomcat\conf\server.xml

- Dell\OpenManagePowerCenter\external\apache-tomcat\conf\tomcat-users.xml
  - Dell\OpenManagePowerCenter\external\apache-tomcat\conf\web.xml
  - Dell\OpenManagePowerCenter\keystore.ssl
  - Dell\OpenManagePowerCenter\pgdata\pg\_hba.conf
  - Dell\OpenManagePowerCenter\pgdata\postgresql.conf
4. Delete all content under Dell\OpenManagePowerCenter\external\apache-tomcat\work.
  5. Update the **Properties** of the Power Center services to use the normal user account to log into the service. When the system notifies that "The account .\A has been granted the Log On As A Service right," click **OK** to confirm.
  6. Start all Power Center services for these changes to take effect.

## Operating system hardening

Before deploying OpenManage Power Center on a virtual appliance, you must configure the operating system (OS) as follows to prevent data conflicts and errors:

- Installation Settings
  - Do not install Power Center and its database in the system volume or domain controller.
- Service Pack and Hotfix Settings
  - Install all critical or important service packs and hot fixes.
- Hardening requirements recommended by Center for Internet Security (CIS)
  - Apply the hardening requirements recommended by CIS for OpenManage Power Center supported Windows OS. For more information on CIS benchmark, visit [www.cisecurity.org](http://www.cisecurity.org).

## Audit log

Power Center tracks critical operations and stores related information in a log file for auditing purposes. Each log includes the following basic information:

- User name
- Time
- Action
- Details (Depends on the action; see the following table for audit log details).

**Table 13. Audit log details**

Action	Tracked Information
Successful/failed user login/logout	Source IP
Add/remove emergency power reduction	Impacted single device/group
Set/update/remove power policy	Impacted single device/group
Start/stop network discovery	Network discovery information; includes protocol profile, IP range
Change session timeout	Old/new value of timeout
Change password for Power Center managed user	User name
Update role privilege	Role name, old/new value of privileges
Add/remove user to role	User name, old/new value of role name
Add/remove user	User name

The event logs are kept in the log file. You can find the log file(s) in: <InstallDir>\OpenManagePowerCenter\logs\Audit.log.x. Where x is the incremental number, if applicable (shown below.)

The total size of all audit log files is limited to 20 MB. Power Center keeps up to three audit log files of approximately 6.67 MB each. If a new log causes the file size to exceed the limitation for a single log file, Power Center renames the log file to a new name and stores the new log in a new log file with the original file name.


When generating an audit log file, the naming rules are as follows:

- audit.log — The first audit log file name. This file always logs the latest actions.
- audit.log.1 — The second audit log file name. This is copied from audit.log when it exceeds the file size limitation.
- audit.log.2 — The third audit log file name. This is copied from audit.log.1 when audit.log exceeds the file size limitation.


## Managing certificates

Power Center uses Keytool— a key and certificate management utility from the Java Runtime Environment (JRE)—to generate a key pair (a public key and an associated private key) that is used to create a self-signed certificate during installation.

Keytool is installed at <InstallDir>\external\jre\bin\keytool.exe. The private key and the self-signed certificate are stored in the keystore file at <InstallDir>\keystore.ssl. The self-signed certificate expires three months after installation.

 **NOTE:** It is strongly recommended to update the private key and self-signed certificate.

You can manage Power Center certificates in Keytool. Common scenarios include:

- Scenario 1 — Generate a key pair and self-signed certificate. During Power Center installation, a key pair and self-signed certificate are generated for the Power Center server.  
 **NOTE:** When you delete an entry from the keystore file, make sure you leave at least one key pair entry in the keystore file; otherwise, Power Center does not work.
- Scenario 2 – Replace the self-signed certificate with a signed certificate issued by a Certification Authority (CA). A certificate signed by a CA is more likely to be trusted by the Web browsers. To sign your certificate by a CA, do the following:
  - Generate a Certificate Signing Request (CSR) and submit to the CA.
  - Import a certificate for your CA.
  - Import the Certificate Reply from the CA.
- Scenario 3 – Import a new Trust Certificate. Some devices (for example, chassis and the exposed management interface through WS-MAN) or web service providers may provide a certificate for Power Center validation when establishing communication. If you validate the certificate and Power Center fails to verify it by building a trust path from the trust certificate in the keystore file, then communication fails. In this scenario, you may need to import a new trust certificate to make sure a trust path can be built to verify the certificate.

For more information on how to manage certificates, see Keytool documentation.

## Configuring settings

You configure the OpenManage Power Center settings in the **Settings** screen. The **Settings** screen comprises the following tabs:

- **General** — Configure the timeout for console and device communication.
- **Monitoring** — Configure the power/thermal units and energy consumption parameters.
- **Alerts** — Configure alerts for SNMP traps, enable or disable sending alerts through emails, configure email recipients, and event severity-level.
- **SMTP** — Configure SMTP parameters for sending alert emails.
- **Database** — Configure database compression and purging policy.
- **Directory** — Configure Lightweight Directory Access Protocol (LDAP) settings to support authentication through LDAP. This tab is displayed only on systems running the Linux operating systems where OpenManage Power Center is installed.
- **Users** — Manage user or group accounts for accessing OpenManage Power Center.
- **Roles** — Managing roles and rights.
- **Licensing** — Manage the issued licenses.
- **Inventory** — Track chassis inventory.

Some settings are activated immediately; some settings are activated during the subsequent time duration. See the following sections for more specific information.

### Topics:

- [General settings](#)
- [Monitoring settings](#)
- [Database policy settings](#)
- [Directory](#)
- [Alerts](#)
- [Editing SMTP settings](#)
- [Licensing](#)
- [Inventory](#)

## General settings

In the left pane, click **Settings**. By default the **Settings > General** tab is displayed.

In the **General** tab, you can view and configure the timeout of console sessions and protocols.

## Configuring console session timeout

1. In the left pane, click **Settings**.  
The **General** tab of the **Settings** screen is displayed.
2. Under **Console Session Timeout**, enter the time, in minutes, after which you want the console session to expire, in the **Session Timeout** text box.  
The default time is 20 minutes.
3. Click **Save** to save the changes or click **Reset** to revert to the previously saved settings.

## Setting protocol timeout periods

1. In the left pane, click **Settings**.  
By default, the **General** settings screen is displayed.

2. In the **Protocols Timeout** section, enter the time in seconds for the specified communication protocol (*IPMI, SNMP, WS-MAN, HTTPS, or SSH*).

OpenManage Power Center considers the device not reachable if it cannot get any response from the device within the timeout period.

3. Click **Save** to apply your settings, **Reset** to revert to the previously saved settings.

The new settings take effect the next time when Power Center communicates with the device.

## Monitoring settings

These settings are used to enable/disable monitoring and set the sampling interval:

- **Monitor all devices and groups** – Enables or disables monitoring of all devices and groups. By default, the check box is selected. If you clear the check box, you cannot view the device or group power and temperature details.
  - **Power sampling interval** – Power Center gets power data according to the sampling interval you set (1, 3, 6, or 10 minutes). You can view power data on the **Power Details** page. The default is 1 minute.
  - **Temperature sampling interval** – Power Center gets temperature data according to the sampling interval you set (1, 3, 6, or 10 minutes). You can view temperature data on the **Temperature Details** page. The default is 1 minute.
- **Monitoring Units**
  - **Power Units** — The power consumption of a device or device group is displayed in the unit option you select (Watts or BTU/hr). By default, the power consumption is displayed in Watts.
  - **Temperature Units** — The temperature data of a device or device group is displayed in the unit option you select (Celsius, Fahrenheit). By default, the temperature data is displayed in Celsius.
- **Energy Consumption Cost** — The power consumption cost comprises the following components:
  - **Flat Rate** — It is the cost of power used per kilowatt hour in the specified currency.
  - **Cooling Multiplier** — It is used to estimate the energy required to cool the device or device group.
  - **Currency** — Select the currency in which you want to calculate the energy consumption cost from the drop-down list.

## Recommended sampling intervals for performance tuning and scaling

It is important to configure appropriate Power and Temperature Sampling Intervals in Power Center, because sampling intervals impact the system performance and footprint significantly, including network bandwidth consumption, database size, and trend graph display latency.

The default power and temperature intervals in Power Center are 1 minute. This value is appropriate for small- or medium-sized environments where the device number is less than 1000; however, when the environment has more managed devices, it is recommended to adjust the values to 3 or 6 minutes.

 **NOTE:** The device number includes only supported devices. Unsupported devices are not counted.

## When are the settings effective?

- Monitor all devices and groups — Immediately
- Power/Temperature sampling interval — Every 30 minutes, for example, 08:00, 08:30, 09:00, and so on.

## Configuring the power and temperature sampling intervals


1. On the **Settings** screen, click the **Monitoring** tab. Select the **Monitoring all devices and groups** check box to enable the power and thermal monitoring of all devices and groups.
2. Enter values in the **Power Sampling Interval** and **Temperature Sampling Interval** text boxes.

The default power and temperature sampling interval is one minute.
3. Click **Save** to apply the settings, or click **Reset** to revert to the previously saved settings.

## Configuring the power and temperature monitoring units

1. Under **Monitoring > Power Units** settings, select the unit of measurement in which the power consumption must be displayed.  
The available options are:
  - **Watts**
  - **BTU/hr**
2. Under **Temperature Units**, select one of the following options in which the temperature monitoring must be displayed.  
The available options are:
  - **Celsius**
  - **Fahrenheit**
3. Click **Save** to apply the settings, or click **Reset** to revert to the previously saved settings.

## Configuring energy consumption cost settings

1. In the left pane, click **Settings > Monitoring**.
  2. In the **Energy Consumption Cost** section, enter values in the **Flat Rate** and **Cooling Multiplier** text boxes.  
**Flat rate** is the cost of power used per kWh in the specified currency.  
**Cooling Multiplier** is used to estimate the energy needed to cool the device or device group.
  3. From the **Currency** drop-down list, select the currency in which the energy consumption cost must be displayed.
  4. Click **Save** to apply your settings, or click **Reset** to revert to the previously saved settings.
-  **NOTE:** Changes to the **Cooling Multiplier** take effect immediately. But, changes to the **Flat Rate** take effect at the beginning of the next hour.

## Database policy settings

Database policy settings are used to configure the database maintenance policy.

OpenManage Power Center stores monitoring data for your data center in a database file, using compressed power/temperature data to optimize for higher query performance and smallest database size. It stores both power/temperature compressed data and non-compressed data in the database. Data compression helps improve data query efficiency by aggregating and saving monitoring data using a bigger granularity (hourly or daily), but not the original granularity decided by the Sampling Interval.

By default, OpenManage Power Center keeps compressed power/temperature data and event data up to 365 days and non-compressed power/temperature data up to 14 days. You can configure the duration for which OpenManage Power Center retains compressed and non-compressed data using the **Data compression** and **Purge data (older than)** fields. Data that exceeds its duration or is older than the purge date is deleted. This improves the efficiency of the data query. You can automatically purge data by using the **Schedule Purge** field, or you can trigger it manually to start purging data immediately (see "Purge Database Now," below).


You can set the following for database maintenance:

- **Data compression** — Set the number of the days (1-14) to keep the non-compressed data. The default is 7 days.
- **Purge data (older than)** — Set the number of the days (1-365) to keep the compressed data and the event logs. The default is 365 days.
- **Schedule Purge** — Set the time of day to start database purging (00:00:00 - 23:00:00). The default is 23:00:00. You can also purge the data immediately by clicking **Purge Now**. Power Center immediately purges the database based on the settings in **Purge data (older than)**. After the data is purged an informative event, *Database Maintenance Success*, is displayed on the **Events** screen.
- **Application Logs Settings** — Enter the maximum size for the OpenManage Power Center application log stored in the database, in the **Maximum log size** text box. The default is 100000 entries. After reaching the specified log size, a new application log is created.

- **Events Logs Settings** — Enter the maximum size for the OpenManage Power Center event log stored in the database, in the **Maximum log size** text box. The default is 100000 entries. After reaching the specified log size, a new event log is created.

## Setting or editing the database policy

1. In the left pane, click **Settings > Database**.
2. From the **Data compression** drop-down list, select the number of days (1-14) for which you want to keep the non-compressed data (the default is 7 days).
3. From the **Schedule Purge** drop-down list, select the time at which the data must be purged. The default time is 23:00.
4. In the **Purge data (older than)** text box, enter the number of days to remove the data automatically from the database after the specified period. The default is 365 days.
5. In the **Applications Logs Settings > Maximum log size** text box, enter the maximum number of entries for the application log. The default size is 100000 entries.

 **NOTE:** To ignore the events from the protocol operation select **Ignore Protocol Operation Events (s)** option.


6. In the **Events Logs Settings > Maximum log size** text box, enter the maximum number of entries for the event log. The default size is 100000 entries.
7. Click **Save** to apply your changes, or click **Reset** to revert to the previously saved settings.

## Configuring database backup


OMPC enables you to schedule a database backup of the power monitoring data. The backup data can be used on a different OMPC server or can be used as a restore point in case of a disk failure.

You can also backup the database using CLI commands, for more information on the CLI commands used for database backup, see the **backup\_database** section in [Command Line Interface commands](#).


1. In the left pane, click **Settings > Database**.
2. Click **Advanced Settings** to configure the database backup.
3. Click **Enable Database Backup**. By default, this option is disabled.

 **NOTE:** Data in the backup folder may be overwritten by a subsequent backup.


4. In the **Backup Path** text box, enter the location of the OMPC server to save the backup files.

 **NOTE:** If the backup location does not exist, the service account (**NETWORK SERVICE** in Microsoft Windows operating system and **dcm** in Linux operating system) must have the appropriate network permissions to create a backup location and copy the files to and from the location.


5. In the **Encryption Password** text box, enter the password to encrypt the backup data.

 **NOTE:** The encryption password must be at least eight characters in length and should comply with at least three of the following categories: an uppercase letter, a lowercase letter, a numeric or a non-alphanumeric character.


6. Click **Set Schedule** to schedule the database backup.

 **NOTE:** Click **Run Now** to back up the files from the database immediately.

- Click **Run Once** option to schedule one time database backup. Specify the date and time of the schedule.
- Select **Periodic** option and specify if the database backup has to happen daily, weekly, or on a specific day.


 **NOTE:** Under the **Range of recurrence** option, select the start and end date for the task, or select the **No End Date** option to run the task for an unlimited period.

7. Click **Apply** to save the changes or click **Cancel** to revert to the previously saved settings.

 **NOTE:** After the database backup is complete, you can view the application log details about the completion of the database backup by clicking **Click here** link.



# Directory

 **NOTE:** The **Directory** settings screen is available only in the Linux environment.

On the **Directory** settings screen, you can configure LDAP settings to manage user authentication and certificate validation on systems running Linux, where OpenManage Power Center is installed. The following table lists the options available on this screen.

**Table 14. Directory settings options**

Option	Description
<b>Enable LDAP User Authentication</b>	Select the check box to enable the LDAP user authentication. The following fields are enabled only when you select this check box. <ul style="list-style-type: none"><li>• <b>LDAP Server Address</b></li><li>• <b>Bind Distinguished Name</b></li><li>• <b>Bind Password</b></li><li>• <b>Base Distinguished Name to Search</b></li><li>• <b>Attribute of User Login</b></li></ul>
<b>LDAP Server Address (Enter single DNS names or IP addresses, or multiple ones separated by a comma)</b>	Enter the IP address or the DNS name of the LDAP server. You can enter multiple IP addresses or names, separating them using a comma. For example: 192.125.46.89, 192.25.47.68
<b>Bind Distinguished Name</b>	Enter a user name for the Bind search. If a name is not entered, OpenManage Power Center uses an anonymous Bind to search for the user's login Distinguished name. For example: uid=mark, ou=manager, dc=dell, dc=com
<b>Bind Password</b>	Enter a password for the Bind Distinguished name you provided.
<b>Base Distinguished Name to Search</b>	The Distinguished name of the directory branch from where search begins. For example: ou=ccr, dc=dell, dc=com
<b>Attribute of User Login</b>	Specify a user login attribute for the search. If an attribute is not provided, the default search string, 'uid', is used. The attribute must be unique.
<b>Advanced Settings</b>	Select this check box to enable advanced LDAP settings. The following fields are enabled only when you select this check box. <ul style="list-style-type: none"><li>• <b>LDAP Server Port</b></li><li>• <b>Search Filter</b></li><li>• <b>Network Timeout</b></li><li>• <b>Search Timeout</b></li><li>• <b>Enable Certificate Validation</b></li></ul>
<b>LDAP Server Port</b>	Enter a port number for the LDAP server over SSL. The default port number is 636.
<b>Search Filter</b>	Specify a valid LDAP search filter if you cannot uniquely identify the login user with the specified Base Distinguished Name. If a search filter is not provided, the default filter (objectClass=*) is used and all objects in the tree are searched. The maximum length of this filter is 1024 characters.
<b>Network Timeout</b>	Specify the time, in seconds, for which OpenManage Power Center LDAP must wait for connecting to the LDAP server. The default timeout is 30 seconds.
<b>Search Timeout</b>	Specify the time, in seconds, after which the OpenManage Power Center LDAP stops waiting for a response to the search request. The default timeout is 120 seconds.
<b>Enable Certificate Validation</b>	Select this check box to enable the LDAP certificate validation. The following fields are enabled only if this check box is selected. <ul style="list-style-type: none"><li>• <b>Upload Directory Service CA Certificate</b></li></ul>

**Table 14. Directory settings options (continued)**

Option	Description
	<ul style="list-style-type: none"> <li><b>Directory Service CA Certificate Information</b></li> </ul>
<b>Upload Directory Service CA Certificate</b>	Click <b>Choose File</b> to navigate to the location on the system where the CA certificate is located, select the file and then click <b>Open</b> to upload the file. The name of file you selected is displayed.
<b>Directory Service DA Certificate Information</b>	Displays information about the CA certificate that is in effect.

From this screen you can:

- [View](#) directory settings
- [Edit](#) directory settings

## Editing directory settings

 **NOTE:** Directory settings are only applicable to OpenManage Power Center installations in a Linux environment.

1. In the left pane, click **Settings > Directory**.
2. To enable LDAP authentication, select the **Enable LDAP User Authentication** check box, then provide the following information:
  - **LDAP Server Address** (required) — Enter single DNS names or IP addresses, or multiple names or addresses. Use comma to separate multiple names or addresses. For example:
 

```
192.25.46.89,192.25.47.68
```
  - **Bind Distinguished Name** (optional) — If a Bind Distinguished Name is not provided, Power Center uses an anonymous bind to search for the login Distinguished Name of the user. For example:
 

```
uid=mark,ou=manager,dc=dell,dc=com
```
  - **Bind Password** (optional unless a Bind Distinguished Name is provided). — Password of the **Bind Distinguished Name**.
  - **Base Distinguished Name to Search** (required) — The Distinguished Name of the branch of the directory from which the search starts. For example:
 

```
ou=ccr,dc=dell,dc=com
```
  - **Attribute of User Login** (optional) — Specify an attribute to search. If this field is not configured, the default search string used is “uid”. The User Login attribute must be unique.
3. To configure advanced LDAP settings, select the **Advanced Settings** check box, then provide the following information:
  - **LDAP Server Port** (required) — Enter the port number for the LDAP server over SSL. The default port number is 636.
  - **Search Filter** (optional) — Specify a valid LDAP search filter if you cannot uniquely identify the login user within the chosen Base Distinguished Name. If a search filter is not provided, the default filter is used (objectClass=\*) and searches all objects in the tree. The maximum length of this property is 1024 characters.
  - **Network Timeout (seconds)** — Specify the time, in seconds, for which OpenManage Power Center LDAP must wait for connecting to the LDAP server. The default timeout is 30 seconds.
  - **Search Timeout (seconds)** — Specify the time, in seconds, after which the OpenManage Power Center LDAP stops waiting for a response to the search request. The default timeout is 120 seconds.
  - **Enable Certificate Validation** — If this option is selected, Power Center uses the CA certificate to validate the LDAP server certificate during the SSL handshake.

- **Upload Directory Service CA Certificate** (optional unless Certificate Validation is enabled) — Click **Browse** and navigate to the CA certificate you want to upload, then click **Open** to upload the new certificate.
- **Directory Service CA Certificate Information** — Displays information about the CA certificate that is in effect.

4. Click **Save** to save your settings, or click **Reset** to revert to the previously saved settings.

## Viewing directory settings

In the left pane, click **Settings > Directory**.

You can also [edit](#) the directory settings from this screen.

## Alerts

On the **Alerts** settings screen, you can enable or disable SNMP trap forward and email alerts. The following table lists the options available on this screen.

**Table 15. Alerts settings options**

Option	Description
<b>Enable SNMP Traps</b>	Select the check box to enable SNMP trap forward. Enter the <b>Destination IP/Host, Port,</b> and <b>Community Name</b> details.
<b>Enable Email Alerts</b>	Select the check box to enable alerts based on severity. The available severity levels are: <ul style="list-style-type: none"> <li>● <b>Critical</b> — Select the check box to send emails for critical events.</li> <li>● <b>Warning</b> — Select the check box to send emails for warning events.</li> <li>● <b>Info</b> — Select the check box to send emails for information events.</li> </ul>
<b>Email Recipients</b>	Enter the email IDs of recipients who must receive the emails for event alerts based on severity. Use a semi colon (;) to separate the email IDs.

## Setting SNMP traps

Configure SNMP trap settings to [send custom events](#) to preferred third-party applications. You can add up to three SNMP trap receivers for the following types of events:

- Power
- Average Inlet Temperature
- Email Failure
- Server Capabilities Changed
- Failed to Set Sampling Interval to Device
- Cannot Register for Events
- Communication with Device Failed
- Communication with Device Restored
- Policy Cannot Be Maintained
- Policy Return To Normal
- Power Return To Normal
- Temperature Return To Normal

The SNMP traps enable you to identify OpenManage Power Center-specific alerts on the third-party consoles.

1. In the left pane, click **Settings > Alerts**.
2. Select the **Enable SNMP Traps** check box.
3. Enter the following information:
  - The IP address or hostname (**Destination IP/Host**) of the destination device to which events are sent. The maximum length is 255 characters.
  - The port number (**Port**) of the destination device. You can enter any available port between 1 - 65535 (default is 162).
  - The community name (**Community Name**) that describes the community; for example, *Public*. The maximum length is 255 characters.
4. Click **Save** to apply the changes, or click **Reset** to revert to the previously saved settings.

## Sending SNMP traps to a Third-Party Application

1. Locate the Power Center MIB file (DellOpenManagePowerCenter-MIB.mib) at <InstallationDirectory>
2. Import the MIB file into the third-party application.
3. Make sure the [SNMP trap settings](#) are configured as required in OpenManage Power Center.

## Editing email alert settings

1. In the left pane, click **Settings > Alerts**.
2. Select the **Enable SNMP Traps** check box.
3. Enter the destination IP address or hostname, port, and community name.
4. Select the **Enable Email Alerts** check box.
5. Under **Severity Level**, select the severity level of event log alerts you want to forward.
6. Enter the email addresses of alert recipients. Separate multiple addresses with a semicolon.
7. Click **Test Email** to send a test email to the list of email recipients, and verify that the email is sent successfully.
8. Click **Save** to save your settings, or click **Reset** to revert to the previously saved settings.

## Viewing alert forward settings

In the left pane, click **Settings > Alerts**.

You can also [edit](#) the alert forward settings on this screen.


## Editing SMTP settings

Add the SMTP information that OpenManage Power Center uses to forward event alert messages.

1. In the left pane, click **Settings > SMTP**.
2. Enter the SMTP server address or hostname, server port, and reply address.
3. Select the **Enable SSL** check box to secure sensitive information such as login credentials.
4. Select the **Use Credentials** check box to use the user credentials for accessing the SMTP server.

## Licensing

OpenManage Power Center requires a valid license for capping the 13th and 14th generation of PowerEdge systems (advanced power capping).

 **NOTE:** Starting OpenManage Power Center 4.0, you do not require a license to monitor a Non-Dell device (third-party power monitoring), as the support is in-built with the software. If a Non-Dell license exists, the status is displayed as *Obsolete*.


The licenses are of three types:

- Trial — These licenses are valid for a limited duration only.
- Perpetual — These licenses do not expire, but they can be used only for the number of nodes mentioned while obtaining the license.
- Site — These licenses do not expire, can be used for unlimited nodes.

 **NOTE:** Only users with the Manage License privilege can import the license.

On the **Licensing** settings screen, you can:

- View the summary and details of the licenses obtained.
- Import and delete licenses

 **NOTE:** The **Home** screen displays a warning message when the licensing terms are violated.


To obtain a Power Center license, visit <https://www.dell.com/en-in/work/shop/cty/pdp/spd/dell-openmanage-power-center>.

## Importing a License

You must purchase, download, and import a license to continue using the product after the trial period.

1. In the left pane, click **Settings > Licensing**.
2. Under the **License Details** pane, click **Import License**.
3. In the **Import License** window, click **Browse** next to **Select the license file** text box to navigate to the location where you have stored the license file **or** enter the path where the license file is located, in the **Select the license file** text box.

 **NOTE:** If you have not purchased a license, click **License Self Service Portal** to purchase a license.

 **NOTE:** You can import only one license in the OpenManage Power Center console at a time.

After the license is uploaded the following message is displayed.

File uploaded successfully

4. Click **Browse** to upload more licenses or click **Close** to close the **Import License** window and return to the **Licensing** tab. You can view the license information in the **Licensing** tab.

## Inventory

On the **Inventory** settings screen, you can track the inventory of a chassis. By default, the inventory check is run every 30 minutes. But, you can trigger the inventory immediately by clicking **Run Now** on the **Inventory** settings screen.


## Configuring inventory settings

1. In the left pane, click **Settings > Inventory**.
2. In the **Schedule chassis inventory search on every** text box, enter the interval, in minutes, at which you want to run the chassis inventory check.  
The default interval is 30 minutes.

3. Click **Run Now** to run the inventory check immediately.

The **Last search for chassis inventory run at** displays the timestamp at which the inventory check was last run.

4. Click **Save** to apply your changes or click **Reset** to revert to the previously saved settings.

 **NOTE:** The chassis inventory operation is applicable only to the chassis that is discovered and added to a managed group.

# Logs

The Logs feature displays information about unexpected or informational events, or internal errors that occur in OpenManage Power Center. The latest application log is displayed on the top of the list. A log can have a maximum of 1,00,000 entries.

In the left pane, click **Logs**. The **Application Logs** screen is displayed. On this screen you can:

- Delete logs
- Export logs
- Refresh the logs list
- Filter logs
- Clear existing filters
- Sort the logs list
- Specify the maximum number of logs

## Topics:


- [Sorting the logs display](#)
- [Setting the application log size](#)

## Sorting the logs display

1. In the left pane, click **Logs** to view the list of application logs.
2. To sort the logs, click the 'up' or 'down' arrow next to the following column headers:
  - Severity
  - Time
  - Entity Name
  - Entity Type
  - Source/Feature

The 'up' or 'down' arrow is displayed next to the column header by which the display is sorted.

## Setting the application log size

1. On the **Application Logs** screen, click . The **Application Log Settings** window is displayed.
2. Enter the number of entries for the log file in the **Maximum log size** text box. The default value is 1,00,000.
3. Click **Save** to save the changes or click **Cancel** to return to the **Application Logs** screen without saving the changes.

## Troubleshooting

This chapter lists some of the known issues you may encounter when working with Power Center.

### Why am I being required to log in more than once by Power Center?

**Possible Cause:** This occurs when one of the following elements of Kerberos SSO is not correctly configured: the Power Center server, the web browser, or the AD domain controller configuration.

**Resolution:** Correctly configure your Power Center server and [web browser](#) for Kerberos SSO. For more information, see your web browser's Help documentation.

### Why can't I access the Power Center management console from a Web browser, even though the Power Center server is running normally?

**Possible Cause:** A proxy setting may prevent the browser from accessing the Power Center server on the network.

**Resolution:** Check your proxy server settings to make sure they are properly configured.

### Why was I automatically logged out of Power Center?

**Possible Cause:** The network connection was lost.

**Resolution:** Check your network connection status; make sure that it is connected to the Power Center server.

**Possible Cause:** The console session timed out.

**Resolution:** Check the **Settings > General > Console Sessions Timeout** settings.

**Possible Cause:** Your user account was deleted.

**Resolution:** Check your user account status to make sure it was not deleted by another user with higher privileges.

### Why did my connection to iDRAC6 devices (PowerEdge Servers) fail, when the network connection status is *Connected*?

**Possible Cause:** iDRAC6 devices are limited to three concurrent connection sessions, and you have reached the limit. There are various reasons that may cause the session to be occupied for a while until it is relinquished—for example, you used incorrect credential information to connect with iDRAC6 devices for three times or more within a short period.

**Resolution:** Wait one minute or more for iDRAC6 devices to release the connection sessions, then try again.

## Why can't Power Center receive events sent from devices?

**Possible Cause:** Power Center is not the destination host of the events sent from devices.

**Resolution:** Make sure the Power Center server's IP address is registered on the device as the destination for events.

**Possible Cause:** There is a network connection problem.

**Resolution:** Make sure the device network and the Power Center server are connected and packets can be routed.


**Possible Cause:** Essential services are not started.

**Resolution:** Make sure that if the Windows SNMP trap service is installed on the Power Center server, this service and the OpenManage Power Center SNMP Dispatcher are started on the Power Center server.

## Why are previously-existing power policies (including EPR) still effective on devices when Power Center is corrupted or has been uninstalled?

**Possible Cause:** Even if Power Center is corrupted or uninstalled, the Power Cap Values of existing power policies (including EPR) on the devices still remain effective.

**Resolution:**

 **NOTE:** Check your data center power capacity to avoid tripping the breaker before performing the following steps.

- If you intend to uninstall Power Center, make sure to remove all devices first.
- If Power Center is corrupted, do one of the following to remove the power policies:
  - If the device number is small, access the iDRAC management console, and manually remove the power policies.
  - If the device number is large, perform the following steps. Power Center removes the policies first, and then remove the devices.
    1. Install Power Center.
    2. Add all the devices to the Power Center management console.
    3. Create a logical group that contains all of the devices, and then create a power policy for this group.
    4. Remove all of these devices from the Power Center management console.

## Why do I see the PostgreSQL error log "FATAL: terminating connection due to administrator command" in the Windows event log?

**Possible Cause:** This error is caused by Power Center server shutdown. Normally, the Power Center database service (Dell OpenManage Power Center Database Server service) stops after other Power Center services; however, if the Power Center server has been shut down quickly, the Power Center database service is forced to stop when other Power Center services are not yet stopped. In this case, the database connection sessions that cannot be closed by other Power Center services is closed by the Power Center database service, and this error is generated. Since such an error is caused by Windows when it shuts down the services quickly, Power Center protects the important data through transaction; therefore, this kind of error does not impact Power Center.

**Resolution:** No action is required.



## Why I can't open power center login page when I access it through Firefox 31?

**Possible Cause:** During the installation of power center, a self-signed certificate is created for power center. If end user has replaced this self-signed certificate with a certificate signed by a well-known CA(Firefox recognize this CA), then you do not encounter this issue. Mozilla has improved its certificate verification process. For more information, visit [www.wiki.mozilla.org/SecurityEngineering/Certificate\\_Verification](http://www.wiki.mozilla.org/SecurityEngineering/Certificate_Verification). As a consequence of this improvement, when end users access power center through Firefox 31, they may get an "sec\_error\_ca\_cert\_invalid" error.

**Resolution:** Following are the solutions recommended to handle this issue:

1. Use a different web browser
2. Replace power center's self signed certificate with a well-known CA signed certificate.
3. Search Mozilla Firefox official documents for solution.

If the above solutions do not work, you can try the following procedure.

1. Delete all Firefox 31 remembered self-signed certificates.
2. Delete all Firefox 31 remembered histories.
3. Restart Firefox31.
4. Try open power center again.

## Why I encounter an error, "An internal error occurred. Contact the technical support for help: subordinate error code: 0x8f0c1301", the Home page when OpenManage Power Center server is installed on SUSE Linux Enterprise Server 11 SP2?

**Possible Cause:** SUSE Linux Enterprise Server 11 SP2 has a known time zone issue which cause power center fail to get the right time zone of server. For more information, visit [www.suse.com/support/update/announcement/2012/suse-ru-20121258-1.html](http://www.suse.com/support/update/announcement/2012/suse-ru-20121258-1.html).

**Resolution:** To handle this issue, it is recommended that you install the patch provided by SUSE Linux.

## Why do I encounter a network exception while adding a LDAP user?

**Possible Cause:** If a wrong LDAP server address is set, OpenManage Power Center tries to connect to the LDAP server till network time out. But, if the web server timeout occurs before the network timeout, the network exception is displayed.

**Resolution:** To handle this issue, it is recommended that you provide the correct LDAP server address.

## Why do I encounter a network exception while adding a chassis to a group?

**Possible Cause:** The chassis platform response could be slow. The web server may timeout before the chassis responds to OpenManage Power Center, resulting in the network exception.

**Resolution:** The chassis is added to the group at the back-end, but the GUI times out before the chassis responds to OpenManager Power Center.

## In the compare report, why is the average power value of a device different when the service is stopped for a few hours?

**Possible Cause:** There may be an inconsistency in the logic for **All Devices** and **Managed Groups**.

**Resolution:** You can select the device from the **Managed Groups** where the power value calculation is more accurate.

## Why is the “policy return to normal” event not displayed when the only device in the Chassis Management Controller (CMC) is deleted?

**Possible Cause:** When the last blade in the chassis is deleted, the power value returns to “-1” as there is no device in the chassis. The comparison between the power value and the policy capping fails and the “policy return to normal” event is not triggered.

**Resolution:** You can add a blade to the chassis if the power value does not exceed the power capping value. The “policy return to normal” event is triggered. You can delete the events manually.

## After discovering the devices, incorrect device information is displayed? Why is this happening?

**Possible Cause:** It may be due to the IPMI privilege level limit set to operator/user level in iDRAC.

**Resolution:** Ensure that in the iDRAC page, the channel privilege level limit in the IPMI settings section is set to Administrator.

## I am not able to view the power headroom graph on the home screen. How do I troubleshoot?

### Scenario 1

**Possible Cause:** The Estimated Max Power for some unsupported devices is not available.

**Resolution:** Configure the Estimated Max Power and then view the graph.

### Scenario 2

**Possible Cause:** The peak power of a group is not available.

**Resolution:** Add devices to the group and assign power before viewing the graph.

### Scenario 3

**Possible Cause:** The Power Capacity of the group is not available.

**Resolution:** Configure the power capacity of the group or add rack (for which the power capacity is mandatory) in a group, so that the power capacity of the group can be calculated from the power capacity of the racks in that particular group.

### Scenario 4

**Possible Cause:** The monitored peak power of the group is higher than the power capacity of the group.

**Resolution:** Configure the power capacity of the group or the racks in the group.

# I am not able to manage the servers discovered by OMPC through the Redfish protocol. Events are also not logged. How do I troubleshoot and resolve the issue?

In OMPC 4.0, you may not be able to use certain features when you discover the servers through Redfish protocol with the lockdown feature of iDRAC enabled. The below matrix lists the restrictions:

Table 16.

Protocol	Monitoring (Devices)	Managing ( Device, task, and reports)	Set iDRAC location	Event subscription
IPMI	Supported	Supported	Supported	Supported
Redfish	Not Supported	Not Supported	Not Supported	Not Supported

To resolve the issue or overcome the restrictions, turn off the lockdown feature in the iDRAC interface or discover the servers using IPMI.

# I discovered a server through the Redfish protocol. When I tried to manage the server, the events are not logged in the event list. What do I do now?

By default, the Redfish events are not logged into the event list due to security restrictions. You may choose to receive the events by following the steps provided here.

- Open `service.xml` file from `[OMPC installation folder]/external/apache-tomcat/conf` location.
- Change the value of `clientAuth` value to `false`.
- Restart OMPC services to start receiving the Redfish events.

# On the **Devices** page, after device discovery, for the MX7000 chassis device, I see the **Device Model** as Dell EMC, however, relevant details are not available. The status of the device is displayed as **Lost Connection**. What should I do to retrieve the device details?

To resolve the issue, it is recommended to configure the MX7000 chassis device with the DNS name and use the same name as the hostname during device discovery or you should discover the device using the IP address of the device.

# Upgrade failure recovery on Microsoft Windows operating system

## Check OMPC status

If the installer process is stopped or server is switched off during upgrade, the upgrade fails. Follow the steps to troubleshoot the upgrade failure scenario:

1. Run `wmic product where name='Dell OpenManage Power Center' get version` command on the windows command line interface to get the current version OMPC.
2. If the OMPC old version is displayed, for example 3.1.0.XXXX, it means OMPC upgrade operation has not been started, see **Recover OMPC** section.
3. If the OMPC new version is displayed, for example "3.2.0.XXXX", it means OMPC upgrade has been started, see **Check OMPC database service status** section.
4. If neither old nor new version is displayed, see **Rollback to previous OMPC version** section.
5. See **OMPC database upgrade status** to view the upgrade status.

## Recover OMPC



1. Check All OMPC services, if one or more services does not exist, see **Recover OMPC** section. If not, proceed with the next step.
2. Start All OMPC services if they was not started.
  - NOTE:** If **Dell OpenManage Power Center Database Server** service cannot be started, check **[DataDir]**. If it has been renamed to **[DataDir]bak** (for example, pgdatabak), then you may need to rename it to **[DataDir]** (for example, pgdata) and restart this service again.
  - NOTE:** If you renamed **[DataDir]** folder, you should give Network Service full control privilege to this folder. if the service still could not get started, see **Rollback to previous OMPC version** section.
3. Remove **[LocalAppData]\ompc\ompcold** if it exists.

## Check OMPC database service status

If OMPC database services can be started, and you can successfully login to the OMPC database **dcmapp** using the OMPC database privileges , see **OMPC database upgrade status** to check OMPC database upgrade status. See **Rollback to previous OMPC version** to recover old OMPC.

## Rollback to previous OMPC version

1. Uninstall the new OMPC using `msiexec /x {79427712-CD0A-4114-A571-6BCA07F2EE0A} NOWARNING=1 REMOVEINSTALLDIR=0`.
  - NOTE:** In some case (Power off or killed OMPC installer program), there is still a corrupt OMPC in the Windows OS. It may not be able to uninstall by the above command and will block any new OMPC installed. In this case, you need to remove OMPC manually.
    - a. Open register table using the **regedit** command and search all key or value include **{79427712-CD0A-4114-A571-6BCA07F2EE0A}**. Remove all key or value found.

- b. Stop all OMPC services if they exist.
  - c. Delete all OMPC services if they exist with below command:
    - i. Sc.exe delete "DatacenterManager"
    - ii. Sc.exe delete "DatacenterManagerSnmp"
    - iii. Sc.exe delete "DatacenterManagerServer"
    - iv. Sc.exe delete "Dell OpenManage Power Center Database Server"
2. Run the command in windows command line to reinstall old OMPC: (app.exe or app64.exe depending on 32-bit or 64-bit OS ): "[LocalAppData]\ompc\ompcold\App.exe" /V"/qb! INSTALLDIR=\"%[InstDir]\" PGSQLDATADIR=\"%[DataDir]\" USEDDBSERVER=0"
-  **NOTE:** If you get an error message **Another installation is in progress; complete that installation before continuing this one**, reboot server and retry upper command line:
3. Stop All OMPC services.
4. If **[DataDir]bak** exists, then remove **[DataDir]**, and rename **[DataDir]bak** to **[DataDir]**.
   
 **NOTE:** If you renamed **[DataDir]** folder, you should give Network Service full control privilege to this folder.
5. Start all OMPC services.

## Check OMPC database upgrade status

1. Use PGAdmin to login OMPC database **dcmapp** with OMPC database user.
2. Check upgrade log file (%LOCALAPPDATA%\ompc\ompcupgrade.log) and if **Reuse and Upgrade completed** exists the upgrade was successful. Otherwise upgrade to new version was failed.
3. If OMPC database upgrade was success, you only need to forward OMPC to new version. See **Upgrade OMPC to new version**.
4. If OMPC database upgrade failed, you should recover OMPC to old version. See **Recover OMPC to previous version**.

## Update OMPC to next version

1. Check if all the OMPC services are started. If not, start them.
2. Clean the database and delete the previous data if they exist.
3. Use PGAdmin to login OMPC database **dcm** with OMPC database user.
4. Execute below SQL to clean old database: **DROP DATABASE IF EXISTS dcm\_old** and **DROP DATABASE IF EXISTS dcmapp\_old**.
5. Remove **[DataDir]bak** and **[LocalAppData]\ompc\ompcold** if they exist.

## Recover OMPC to old version

1. Use PGAdmin to login OMPC database **dcm** with OMPC database user.
2. Execute below SQL to clean old database: **DROP DATABASE IF EXISTS dcm\_tmp** and **DROP DATABASE IF EXISTS dcmapp\_tmp**.
3. Recover other disk files. Follow the process specified in **Rollback to previous OMPC version**.

# Upgrade failure recovery on Linux operating system

Use `install.sh` command in the new OMPC version package to do upgrade or install OMPC. The `install.sh` command detects the version of OMPC. If there is an old version installed, upgrade process is initialized. If not, then a new version is installed.

**NOTE:** If you use `rpm -U` during the OpenManage Power Center installation or upgrade, many warning messages will get displayed. You can ignore these warning messages as the upgrade operation will continue as expected. To resolve this issue, it is recommended that you use `install.sh` instead of `rpm -U`.

## Check OMPC status

If the installer process is stopped or server is switched off during upgrade, the upgrade fails. Follow the steps to troubleshoot the upgrade failure scenario:

1. Run `rpm -q OpenManage_PowerCenter` command on the command line interface to get the current version OMPC.
2. If the OMPC old version is displayed, for example 3.1.0.XXXX, it means OMPC upgrade operation has not been started, see **Recover OMPC** section.
3. If the OMPC new version is displayed, for example "3.2.0.XXXX", it means OMPC upgrade has been started, see **Check OMPC database daemon status** section.
4. If neither old nor new version is displayed, see **Rollback to previous OMPC version** section.
5. See **OMPC database upgrade status** to view the upgrade status.

## Recover OMPC

1. Copy any files in `/etc/ompc/backup/[OMPCFODLER]` back to the `[InstDir]` with the same folder structure: `cp -rf /etc/ompc/backup/[OMPCFODLER] [InstDir]`.
2. Move the backup pgdata folder (e.g. `/opt/dell/pgdatabak`) back to `[InstDir]`, rename it to the original name (e.g. `pgdata`) if changed.

```
rm -r -f /opt/dell/ompc/pgdata
```

and

```
mv -f /opt/dell/pgdatabak /opt/dell/ompc/pgdata
```

3. Run the `[InstDir]/startup.sh` command to start the old OMPC daemons.
4. Remove `/etc/ompc` if they exist.

## Check OMPC database daemon status

Check if the file `upgradeok` exists in `/etc/ompc`. If yes, it means that the upgrade is completed successfully. If not, run `[InstDir]/ompcstatus` command to check OMPC database daemon status.

1. Run `[InstDir]/tools/ompc-pgsql-daemon start` command to start the database daemon.

**NOTE:** If the OMPC database daemon cannot be started, it means that the OMPC upgrade has failed, see **Rollback to previous OMPC version**.

2. Check the database version:

- a. [PGSQLDRV]= postgresql-9.3-1102.jdbc4.jar if target version is above or equals to 3.1;
- b. [PGSQLDRV]= postgresql-8.3-603.jdbc4.jar if target version below 3.1;

You can get the current database version by the **DB\_VERSION** item in **[InstDir]/dbinfofor.tmp**. Check the availability of **/etc/ompc/upgradeok**:

If it exists, it means upgrade completed. If not, new OMPC installed but upgrading yet to be completed.

## Rollback to previous OMPC version

1. Launch roll back script: `/etc/ompc/backup/ompcrollback.sh`.
2. Use PGAdmin to login OMPC database **dcmapp** with OMPC database user.
3. Execute below SQL to clean old database: ***DROP DATABASE IF EXISTS dcm\_old*** and ***DROP DATABASE IF EXISTS dcmapp\_old***.

## Completing OMPC upgrade

1. Restart OMPC daemons using **[InstDir]/stop.sh** and **[InstDir]/startup.sh**.
2. Use PGAdmin to login OMPC database **dcmapp** with OMPC database user.
3. Execute below SQL to clean old database: ***DROP DATABASE IF EXISTS dcm\_old*** and ***DROP DATABASE IF EXISTS dcmapp\_old***.
4. If an older version exists, run **rpm -e OpenManage\_PowerCenter-[OLDVER]-1** command. Remove **/etc/ompc** if it exists.