



AMI[®] Data Center Manager (DCM)

User Guide

VERSION 6.0.0

NDA REQUIRED

AMI[®] Data Center Manager (DCM) User Guide

© Copyright 2025 AMI.

All rights reserved.

ami.com

This publication contains proprietary information that is protected by copyright. No part of this publication can be reproduced, transcribed, stored in a retrieval system, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, AMI.

All trademarks and trade names used in this document refer to either the entities claiming the marks and names or their products. AMI. disclaims any proprietary interest in trademarks and trade names other than its own.

Revision History

Date	Product Version	Revision	Description of Changes
30-Dec-2024	6.0.0	1.0	Initial Draft
23-Jan-2025	6.0.0	1.1	Reviewed the document format

Disclaimer

Although efforts have been made to assure the accuracy of the information contained here, AMI® expressly disclaims liability for any error in this information, and for damages, whether direct, indirect, special, exemplary, consequential or otherwise, that may result from such error, including but not limited to the loss of profits resulting from the use or misuse of the document or information contained therein (even if AMI has been advised of the possibility of such damages). Any questions or comments regarding this document or its contents should be addressed to AMI at marketing@ami.com.

AMI provides this publication “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a specific purpose.

Some states do not allow disclaimer of express or implied warranties or the limitation or exclusion of liability for indirect, special, exemplary, incidental or consequential damages in certain transactions; therefore, this statement may not apply to you. Also, you may have other rights that vary from jurisdiction to jurisdiction.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. AMI may make improvements and/or revisions in the product(s) and/or the program(s) described in this publication at any time.

Requests for technical information about AMI products should be made to your AMI authorized reseller or marketing representative.

Table of Contents

1	Getting Started	1
1.1	Overview	1
1.2	Software Requirements.....	1
1.3	Hardware Requirements	1
1.4	Installing AMI DCM Console	2
1.5	Launching AMI DCM Console.....	15
1.6	Setting Up Hierarchy	15
2	Licensing	16
3	Using AMI DCM Console	17
3.1	Dashboard.....	17
3.2	Hierarchy	18
3.3	Devices.....	25
3.4	Operations on Groups.....	34
3.5	Sustainability	40
3.6	Reliability	42
3.7	Events	45
3.8	GPUs.....	48
3.9	Settings	49
3.10	To integrate DCM Console in an iframe.....	54
3.11	RESTful APIs	55
3.12	Ansible Modules.....	56
3.13	Page Links.....	56
3.14	Command Line Tool.....	56
4	Working In a Scaled Environment	61
5	Renewing Passwords / Keys / Certificates	64
5.1	Renewing the Database Password.....	64
5.2	Renewing the Keystore Password	65
5.3	Renewing Keys	66
5.4	Renewing Certificates	67
5.5	Signing the AMI DCM Certificate with Certificate Authority (CA).....	68
5.6	Renewing Database Keys (High Availability mode).....	69

6	Failover	70
7	Data Streaming.....	71
7.1	Prerequisites	71
7.2	Enable and Configure Data Streaming	72
7.3	Event Logs	74
7.4	Troubleshooting	74
8	Appendix A: SNMP Traps OID Mapping	75
8.1	testTrap	75
8.2	alertPredefinedEvent.....	75
8.3	alertNotification.....	77
8.4	alertNotificationReturnToNormal.....	78
9	Glossary.....	79

Document Information

Technical Support

AMI provides technical support only for AMI products licensed directly from AMI.

Web Site

We invite you to visit our website at ami.com.

Purpose

This document is intended to be used for understanding how to use AMI DCM.

Audience

The intended audiences are data center admins / operators.

Chapter 1

1 Getting Started

1.1 Overview

AMI DCM is a powerful software solution designed to help organizations manage their data centers with greater efficiency and sustainability. Whether you are responsible for infrastructure management or IT operations. AMI DCM provides you with the tools to optimize performance, reduce operating costs, and manage your Data Center carbon footprint.

By leveraging real-time data collection, predictive analytics, and advanced reporting features, AMI DCM enables you to make data-driven decisions that improve the sustainability, reliability, and availability of your critical data center infrastructure.

With AMI DCM, you can achieve your sustainability goals while maximizing operational efficiency and minimizing environmental footprint.

1.2 Software Requirements

AMI DCM Console has been validated on the following operating systems (64-bit version) and web browsers:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2025
- Red Hat Enterprise Linux 8.10 Server x86_64
- Red Hat Enterprise Linux 9.4 Server x86_64
- Novell SUSE Linux Enterprise Server 12 SP5 x86_64
- Novell SUSE Linux Enterprise Server 15 SP6 x86_64
- Ubuntu Server 18.04.6 x86_64
- Ubuntu Server 20.04.6 x86_64
- Ubuntu Server 22.04.4 x86_64
- Ubuntu Server 24.04 x86_64
- Debian 11.10 x86_64
- Debian 12.6 x86_64
- Mozilla Firefox 133
- Google Chrome 131
- Microsoft Edge 131

1.3 Hardware Requirements

For best performance, install AMI DCM Console on a system with at least:

- A x86 dual-core Processor of 2.6 GHz or higher
- 16GB RAM
- 200GB of hard drive space
- 1 Gigabit network

Below is recommended configuration for a scaled environment (e.g., managing up to 60,000 IPMI based nodes):

- 2 * 16 core x86 Processor @ 2.60GHz or higher
- 192GB RAM
- 2TB SSD
- 10 Gigabit network

Here are the default network ports AMI DCM Console uses or connects to for different types of managed devices. Ports used by AMI DCM Console can be changed during the installation process. Ports used by managed devices can be changed when adding devices.

Protocol/Purpose	DCM Console	Managed devices
DCM Console web access	8643(TCP)	---
Collect SNMP trap from devices	1162(UDP)	---
RMI	1099(TCP)	---
IPMI	---	623(UDP) Optional: <ul style="list-style-type: none"> • 443 (TCP) for Redfish inventory/health • 22 (TCP) for some device management processor info, such HP iLO2/3/4 • 627(TCP) for firmware provisioning feature
SSH	---	22(TCP)
SNMP	---	161(UDP)
HTTP/WSMAN	---	443(TCP)
WMI	---	135(TCP)

1.4 Installing AMI DCM Console

There are two types of installers available, one is for AMI DCM Console with web GUI (e.g., "AMI_Data_Center_Manager_6_0_0.exe" as installer for Windows), the other for API based integration only (e.g., "AMI_Data_Center_Manager_API_6_0_0.exe" as installer for Windows). The installation process is quite similar. The only difference is the availability of web GUI.

Verifying the Installation Packages:

Before you install AMI DCM Console, verify the signature of installation package.

For the AMI DCM Console Windows installer:

1. Right click on the installer and select "Properties".
2. Verify its signature and the certificate chain in the "Digital Signatures" tab.

The same practice can be applied for installed executables / libraries as well.

For AMI DCM Console Linux installer, run following commands in the shell:

```
tar -xvzf AMI_Data_Center_Manager64_6_0_0.tar.gz
cd dcm64_package
openssl dgst -sha256 -verify public_key_6_0_0.pem -signature
AMI_Data_Center_Manager64.sig AMI_Data_Center_Manager64.sh
```

Note: Please ensure that the 'public_key_6_0_0.pem' file is either copied to the current folder or provide the full path to the file.

You should see the output as "Verified OK" if the signature is ok.

Installing on Windows:

Navigate to the directory containing the installation package, double-click the package to launch the installation program.

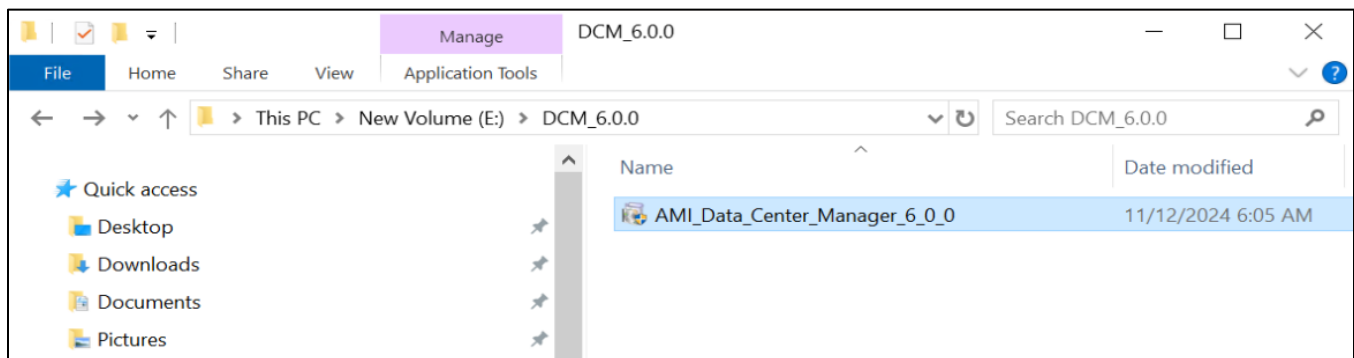


Figure 1 Installation

Note:

You may see a warning with the following message:

Windows Protected your PC

Windows defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

If you see this warning, press **More Info** link and click the **Run anyway** button below to continue the installation.

- Click **Next**.



Figure 2 InstallShield Wizard

- Enable **I accept the terms in the license agreement** and click **Next**.

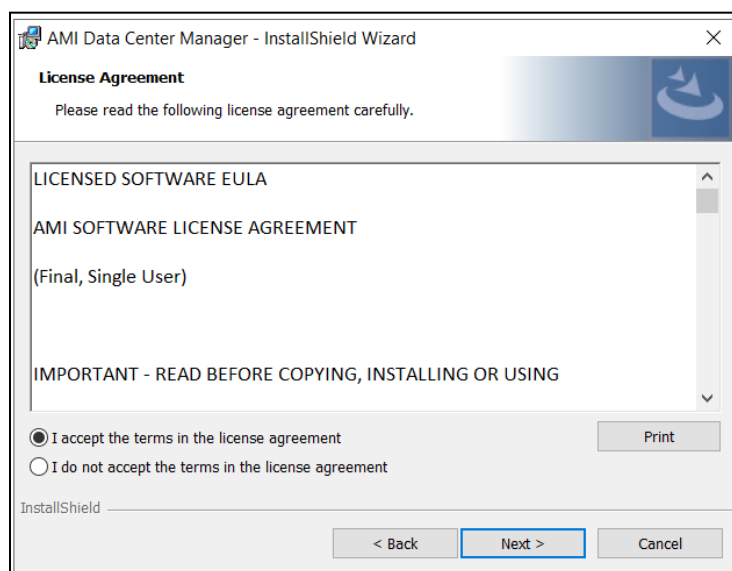


Figure 3 License Agreement

- Enter the **User Name** and **Organization**, and choose whether to install for all users or only the current user, and then click **Next**.

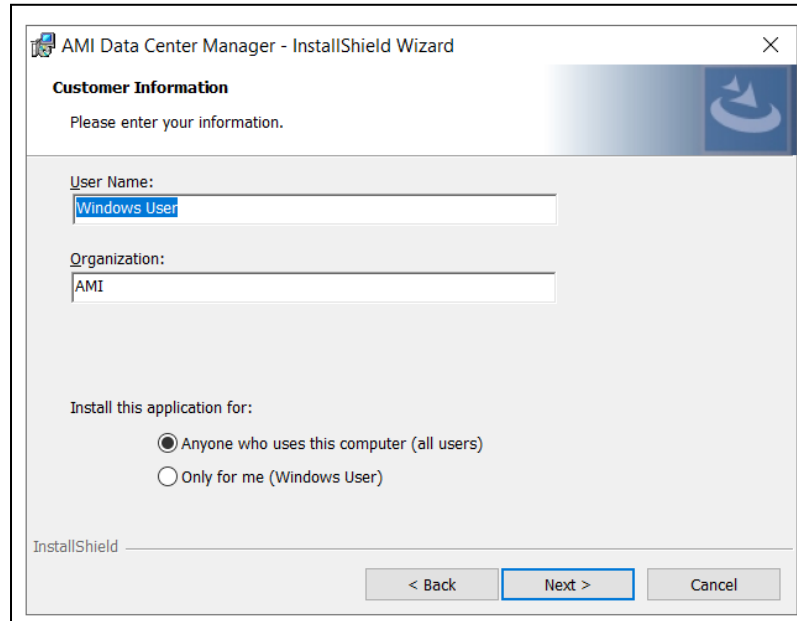


Figure 4 InstallShield Wizard

- For better troubleshooting, we highly recommend using the default installation path. If you want to change the path, click **Change**.

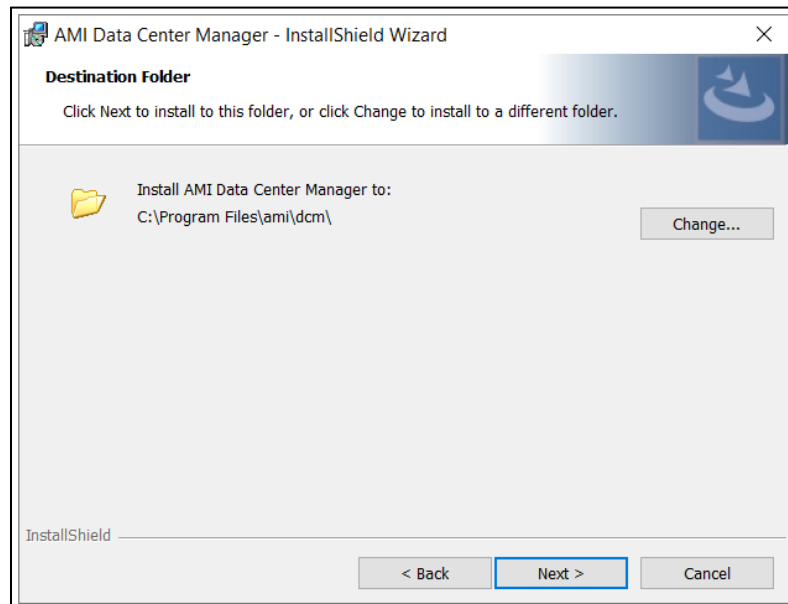


Figure 5 Destination Folder

- If you click **Change**, you can browse through the drop-down list or type the exact path in the text box. Click **OK**, and then click **Next** to continue the installation.

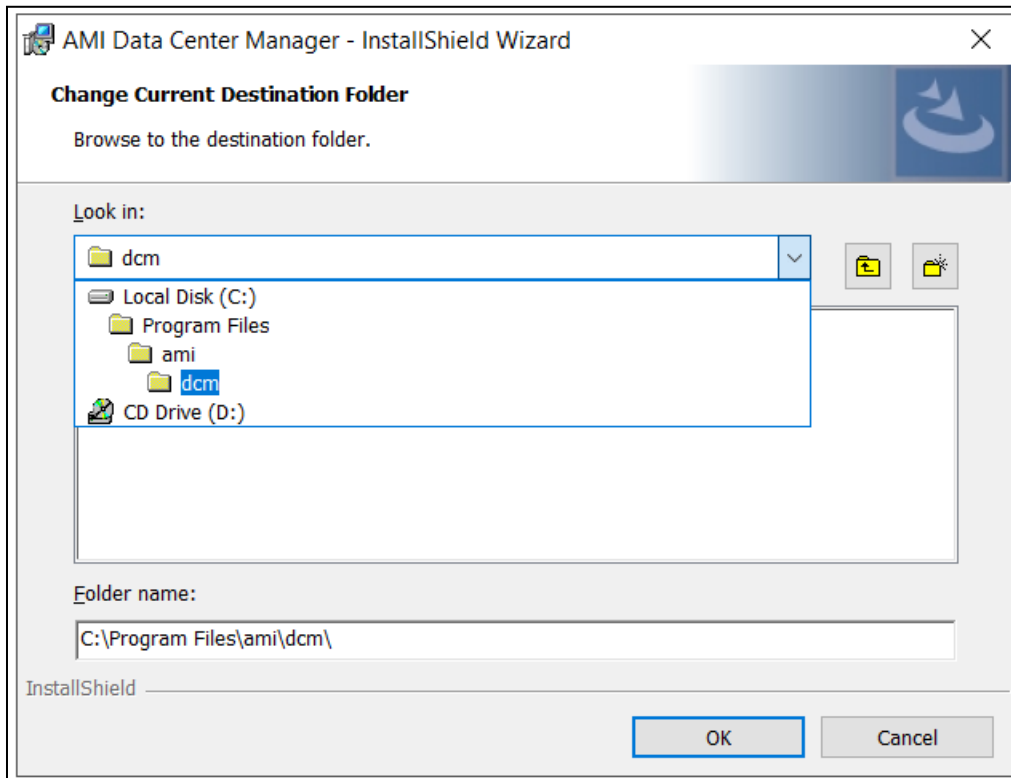


Figure 6 Change Current Destination Folder

- By default, AMI DCM Console dispatches SNMP traps to port 1162 and uses port 1099 for RMI communication. If there is any conflict with other network applications, please modify the default port numbers, then click **Next** to continue.

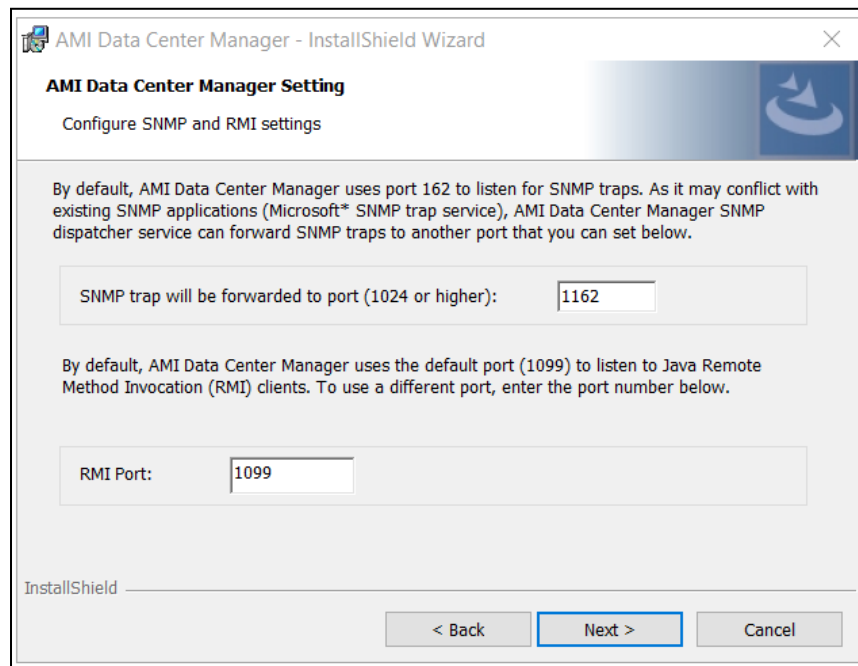


Figure 7 Configure SNMP and RMI Settings

Note: Please make sure that no other process uses the port you are setting before you change the value.

- TLS is required by default. The port number is configurable.

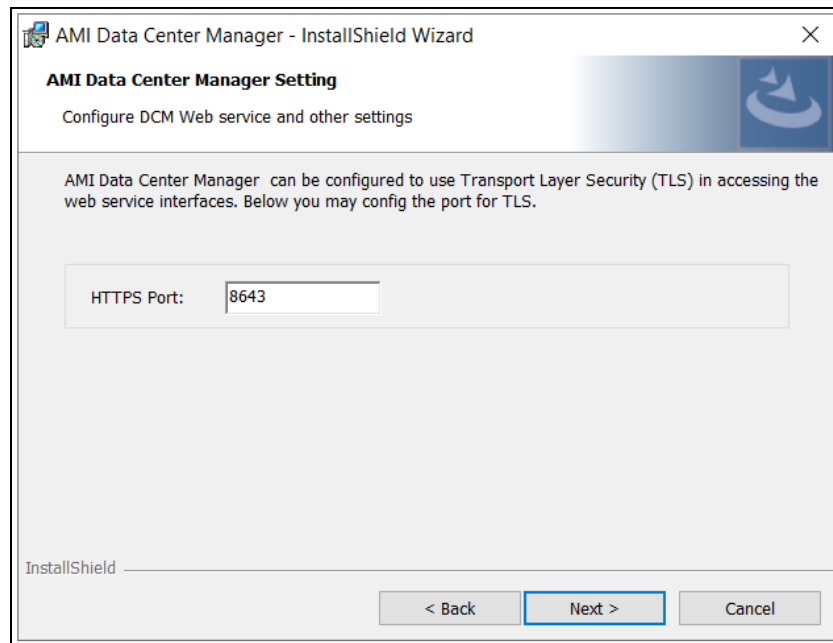


Figure 8 Config DCM Web Service

- Configure the **Sampling Interval** and **Data Granularity** settings, then click **Next**.

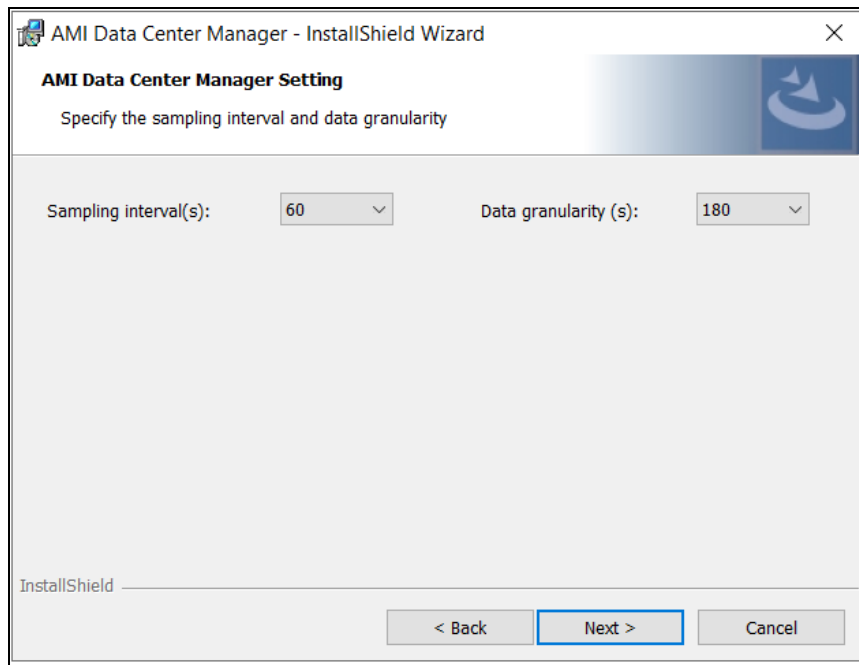


Figure 9 Sampling Interval and Data Granularity

Note:

Sampling Interval is the time interval between two consecutive sampling of power or thermal measurements that DCM collects from the managed devices. The default value is 60 seconds, and you need to make sure the sampling interval you set works for your device.

Data Granularity is the resolution of power/thermal data measurements stored in DCM database for query/metric usages. Valid measurement data granularity includes 30, 60, 180, 360, 600, 1800, and 3600 seconds, which must be a multiple of the Sampling Interval.

For a typical environment (e.g., 1~5000 IPMI based devices), we recommend 60 seconds as the Sampling Interval, and Data Granularity 180 seconds. For a scaled environment (e.g., 5000 ~ 60000 IPMI based devices), the recommended Sample Interval is 300 seconds, Data Granularity 300 seconds.

- Enter the **User Name** and **Password** for login, and click **Next**.

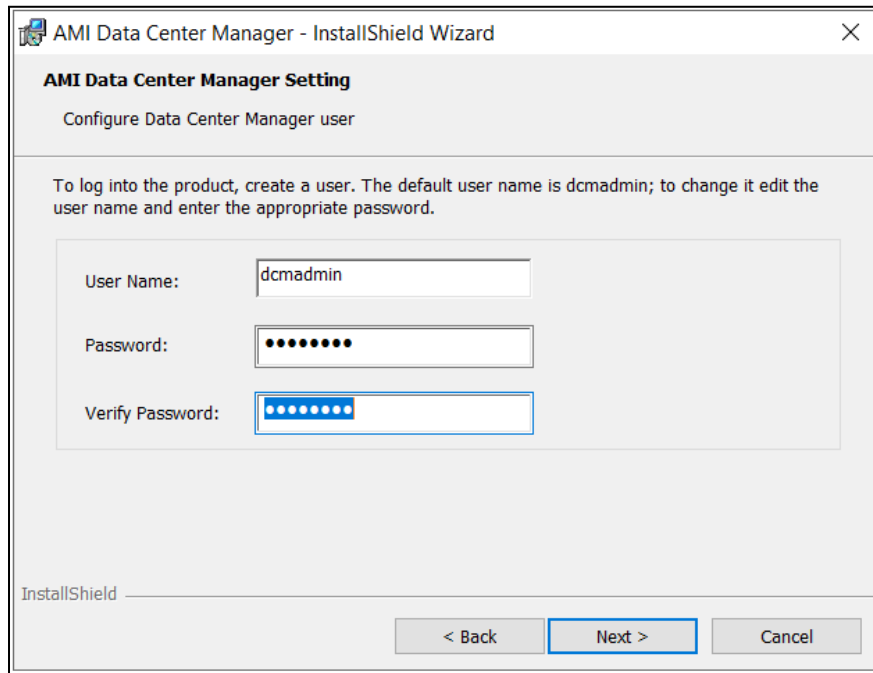
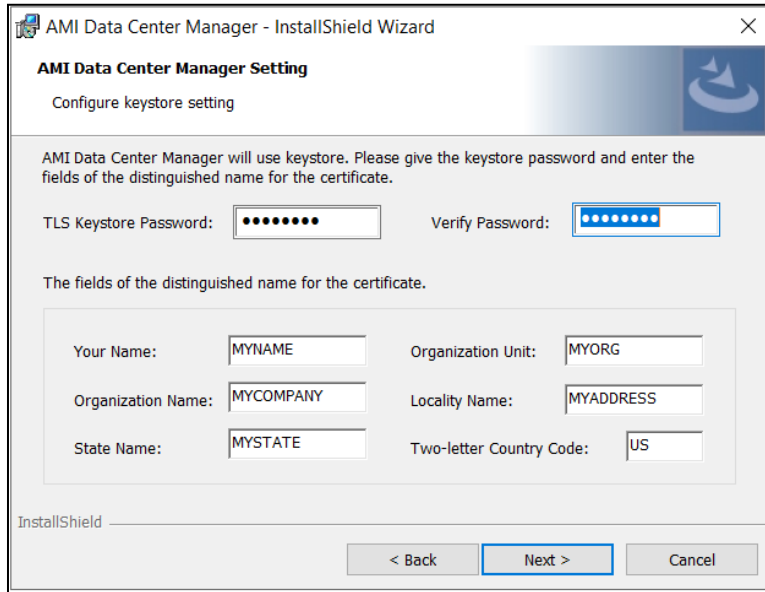


Figure 10 Config DCM User

Note:

For enhanced security, passwords must:

- Be a minimum of eight characters long.
- Not include the associated user ID or be a reverse of it.
- Not contain more than three of the same characters used consecutively.
- Meet at least three of the following criteria:
 - Include at least one lowercase alphabetic character.
 - Include at least one uppercase alphabetic character.
 - Include at least one numeric character.
 - Include at least one of the following special characters '!@#\$\$%^*()_+|.:?=-'
- Enter the **TLS Keystore Password** for DCM to access the keystore file. Then enter the corresponding information for the certificate. Click **Next** to generate a self-signed certificate for TLS communication. Please refer to [Renew Certificate](#) for additional information.



AMI Data Center Manager - InstallShield Wizard

AMI Data Center Manager Setting
Configure keystore setting

AMI Data Center Manager will use keystore. Please give the keystore password and enter the fields of the distinguished name for the certificate.

TLS Keystore Password: Verify Password:

The fields of the distinguished name for the certificate.

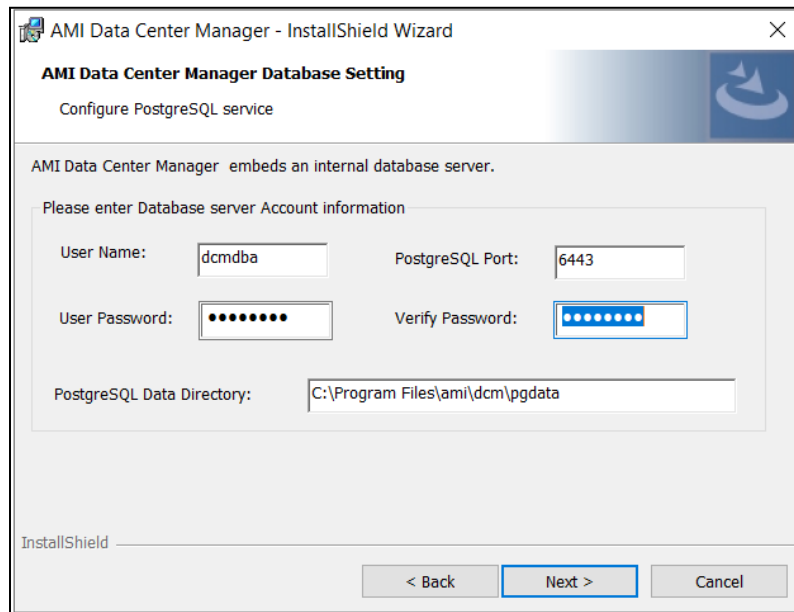
Your Name:	<input type="text" value="MYNAME"/>	Organization Unit:	<input type="text" value="MYORG"/>
Organization Name:	<input type="text" value="MYCOMPANY"/>	Locality Name:	<input type="text" value="MYADDRESS"/>
State Name:	<input type="text" value="MYSTATE"/>	Two-letter Country Code:	<input type="text" value="US"/>

InstallShield

< Back Next > Cancel

Figure 11 Config Keystore Setting

- Enter the required database settings, including the **User Name**, **PostgreSQL Port**, **User Password**, and the database directory. The default value of the **PostgreSQL Port** is 6443. If it is occupied, enter a different one. Then click **Next**.



AMI Data Center Manager - InstallShield Wizard

AMI Data Center Manager Database Setting
Configure PostgreSQL service

AMI Data Center Manager embeds an internal database server.

Please enter Database server Account information

User Name:	<input type="text" value="dcmdba"/>	PostgreSQL Port:	<input type="text" value="6443"/>
User Password:	<input type="password" value="••••••"/>	Verify Password:	<input type="password" value="••••••"/>

PostgreSQL Data Directory:

InstallShield

< Back Next > Cancel

Figure 12 PostgreSQL Service

- Click **Install** to begin the installation process or click **Back** if you want to change the installation settings.

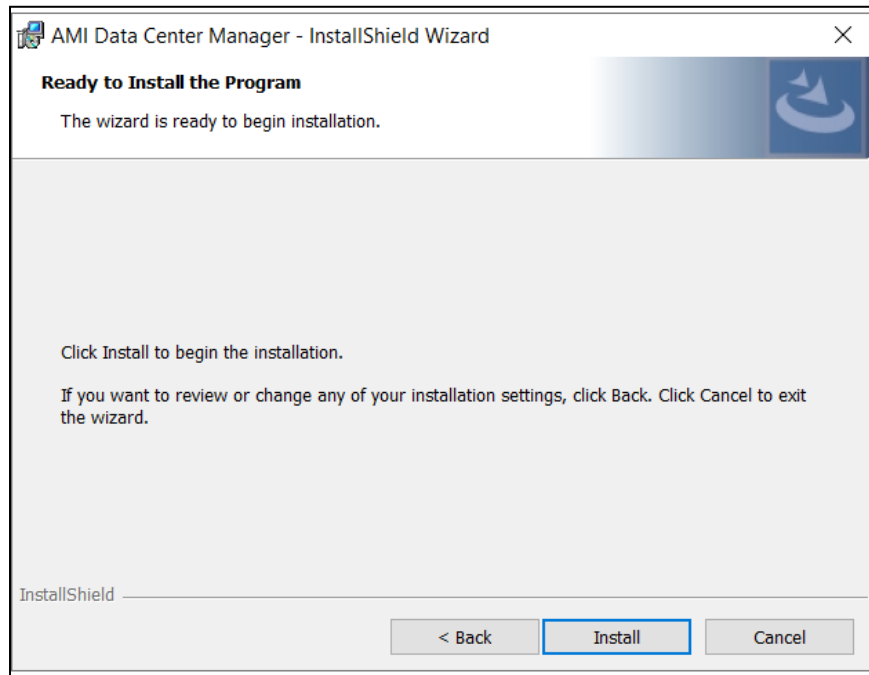


Figure 13 Ready to Install

- Once you click **Install**, you will see a status bar that notes the progress.

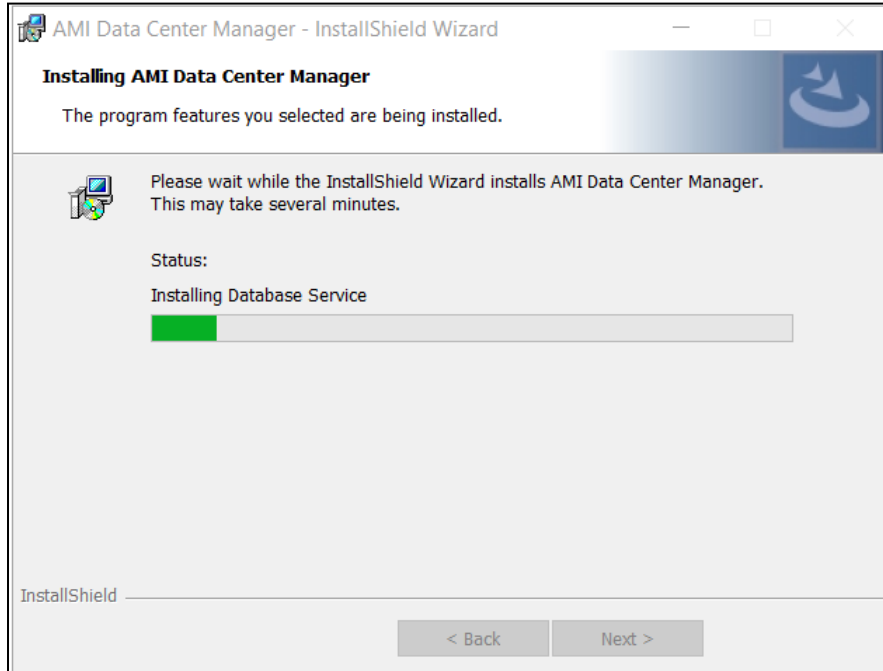


Figure 14 Installing Database Service

- Click **Finish** to complete the installation.

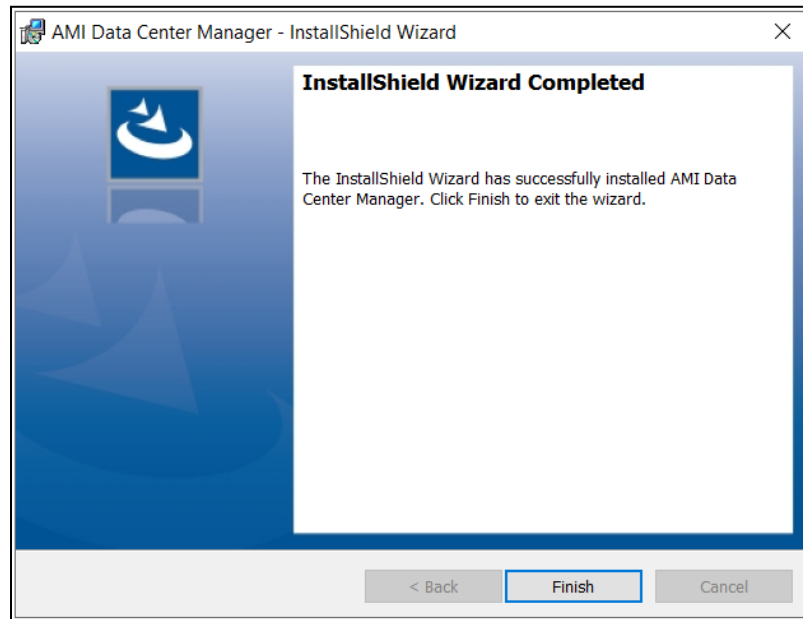


Figure 15 Finish

Installing on Linux:

The steps for installing AMI DCM Console on Linux are similar to those on windows, except that on Linux the installation is command-line based.

Use the following command to initiate the installation:

```
sudo ./AMI_Data_Center_Manager64.sh
```

Note:

Ensure to run with sudo permissions for installing AMI DCM.

Executing the Linux installer binary will launch the welcome page.

```
Step: Welcome
-----
Welcome to AMI Data Center Manager 6.0.0.
installation wizard
-----
You will complete the steps below during this installation:
- Preinstallation check
- End User License Agreement
- Installation location
- Installation configuration
- Installation
- Installation complete
-----
Press "Enter" key to continue or "q" to quit:█
```

Figure 16 Command

On Linux, AMI DCM Console supports High Availability. A Passive instance can replicate the database from an Active instance, and be converted into new Active instance manually in case of failover. To use the High Availability mode, you need to config a Network Time Protocol (NTP) service on each server for time synchronization.

You can select either Active mode or Passive mode during the installation process.

```
Step: AMI Data Center Manager Setting for High Availability
-----
At this step you can decide installing DCM Console
in "Active" mode (default) or "Passive" mode, Active
instance provides normal UI / API functions, Passive
instance will replicate database from Active instance,
and can be converted into new Active instance in case
of (manual) failover.
-----
1. Active mode
2. Passive mode

b. Back to the previous menu
q. Quit
-----
Please type a selection [1]:
```

Figure 17 Active or Passive Mode

After installing an Active instance, you can install a Passive instance to enable the High Availability support. When doing so, you will need to provide certain information like the address, PostgreSQL credentials, and port information of the Active instance during the installation.

```
Step: AMI Data Center Manager PostgreSQL Setting for High Availability
-----
Configure PostgreSQL for High Availability.
-----
1. Specify user name connect to PostgreSQL for High Availability : d_c_m_ha_user
2. Specify user Password connect to PostgreSQL for High Availability.

b. Back to the previous menu
q. Quit
-----
Please type a selection (Press Enter to next):
```

Figure 18 DCM PostgreSQL Settings

A Recovery Key will be generated from the installer of the Passive instance. It will be used for encrypting important information to be passed from the Active instance to the Passive instance.

```

Step: High Availability recovery key config
-----
Create recovery key for High Availability.

-----Begin Recovery Key-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEASzFQQYBZtwzXXRu5Rv+R2x+YFCwkFidkvFRt
tMHVn+zwLMxNqE2TleIYo1CwvYzBrF2mBkXRANK6VygFKzp+nU8UQpn31NI2BJU2MUcQBTJf0b5anQYr
5rDT0SXjcExI3x/0qfahLm9GTfs2IgfsgqL4KL iHJZtaIt504VBkrLpR3LbISAqwQn i1lUYyTJbG4hvz
EvywHk0NmvxFxBKL7segDB/RvUq5pqg5J6htJ85ls i/Rrk+9Bzs f5TQs5gYJAh01WHEBGgGKFc4WqMxr
dgFVNDzGeoTDwCiH17Gn0nuTd2G4yhpwN3/me i+1jLTFugqvAwIDAQAB5d1229d507f5a86be772faa1
c1ed601df2af7288220c55c8357f5fc7b434bc29
-----End Recovery Key-----
Command execute successfully
  
```

Figure 19 Recovery Key

The recovery key needs to be configured in Active instance: open the AMI DCM Console Web UI, enter the Recovery Key in **Settings → Miscellaneous → Recovery Key**, and click “**Save**”. Only in this way can the configurations be encrypted and replicated from Active instance to Passive instance.

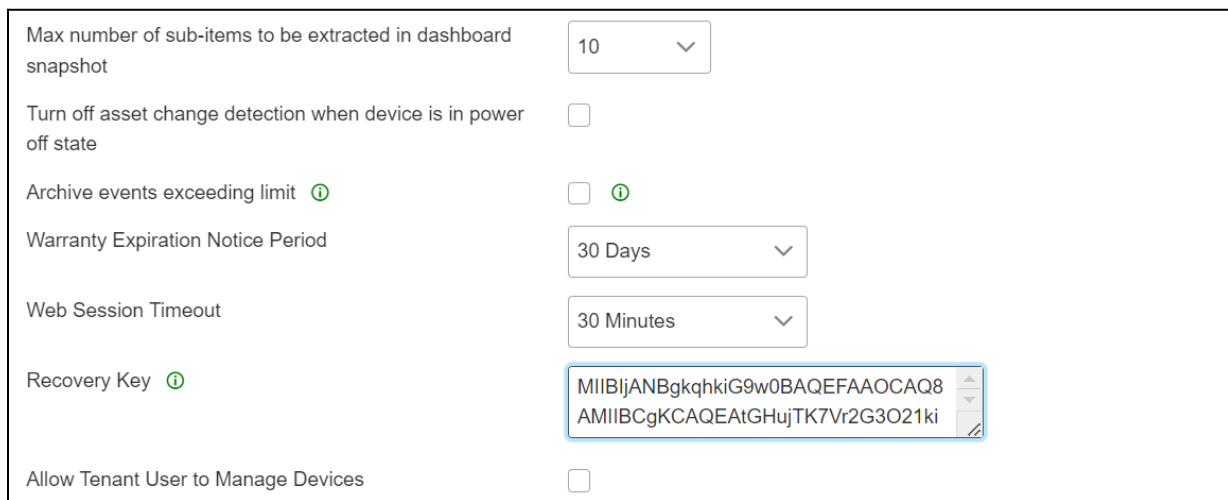


Figure 20

Note:

If the connection between the Active and Passive instances is not stable, the data to be replicated will be accumulated on Active instance until the connection becomes stable. Please reserve enough space (e.g., 1T in a scaled environment) on the Active instance to accommodate for such situations.

In the worst-case scenario where the Active instance is disconnected from the Passive instance for a long time, the data to be replicated will be recycled, and the Passive instance will no longer be able to re-connect to Active instance (no “Passive instance connected” event after “Passive instance disconnected” for a long time). If this happens, you can reinstall the Passive instance as follows:

- **Step 1:** On the Active instance, execute the commands below:

```
cd /opt/ami/dcm
export
LD_LIBRARY_PATH=/opt/ami/dcm/external/pgsql/lib
./external/pgsql/bin/psql -U dcmdba -p 6443 -d postgres
```

Input the password for dcmdba, then execute the SQL command below:

```
select pg_drop_replication_slot('dcm_ha_backup_slot');
exit;
```

- **Step 2:** Install a new Passive instance.

1.5 Launching AMI DCM Console

There are two ways to launch AMI DCM Console.

1. By typing the URL directly in the address bar of browsers.

- Enter the following default URL in your web browser:

<https://localhost:8643/DcmConsole/>

- Enter the **User Name** and **Password** you configured during installation to login.
- Once logged in, you will see the Dashboard which provides a wholistic overview of your data center's sustainability, power, health, thermals, capacity, etc.

Note: The letters of 'D' and 'C' in the default address are in capitals.

2. By clicking the shortcut in the Start menu (Windows only).

- Find the Data Center Manager folder.
- Click on Data Center Manager Console.

1.6 Setting Up Hierarchy

AMI DCM Console provides several ways to set up a data center hierarchy (data centers, rooms, rows, racks, and devices):

1. **Manually:** Click on “Hierarchy” (left menu) to start building a hierarchy manually.
2. **Discovery:** Click on “Devices” (left menu), then click on “Discovery and Import”. Then click on “Add Discovery Task” to discover devices in the same network. Discovered devices will appear in “All Devices”.
3. **Import:** Click on “Devices” (left menu), then click on “Discovery and Import”. Then click on “Add Import Task” to import devices or hierarchy from an excel file. Please refer to [Importing Devices](#) for more information on how to create an excel file.

To manage any device and see it's details, you must first add it to the hierarchy under “racks”.

Chapter 2

2 Licensing

AMI DCM Console is free of charge for the first 15 days. You can click **About** on the top right of the interface to check the license **Status** and **Expiration Date**.

The **Status** will change from **Valid** to **Expired** if a new license is not imported after the expiration date. AMI DCM Console will stop working, and an **Invalid license** notice will pop up for any operation in AMI DCM Console.

If you want to continue using AMI DCM Console after the expiration date, you can request a license from AMI to extend your use period.

To request a license:

- Click **About** on the top right of the interface.
- Select **Accept License Terms and Conditions** in the popup dialog and click **Generate License Request**.
- Email the generated license request file to dcm_sales@ami.com.
- Contact AMI to sign an agreement and complete payment correctly.
- Obtain license from AMI.

To view the features enabled by different license tiers:

- Click **About**.
- Click **License Tiers** in the popup dialog.

To import a new license:

- Click **About**.
- Click **Import new license** in the popup dialog.
- Select license file and then click **Open**.

Then your **Status** will change to **Valid** and the **Expiration Date** will be extended.

To upgrade from previous versions of AMI DCM to version 5.2 or later, you need to replace your existing license with a new one that includes newly introduced support details. To do so, follow the same steps mentioned above and contact dcm_sales@ami.com with the license request generated to get a new replacement license file.

For any questions or assistance required during the upgrade process, contact our dedicated support team at dcm_sales@ami.com.

Chapter 3

3 Using AMI DCM Console

3.1 Dashboard

The Dashboard provides a comprehensive overview of your environment, including carbon emissions, current power and cooling status, historical power and temperature trends, hotspots, power and space capacity, device status, and events.

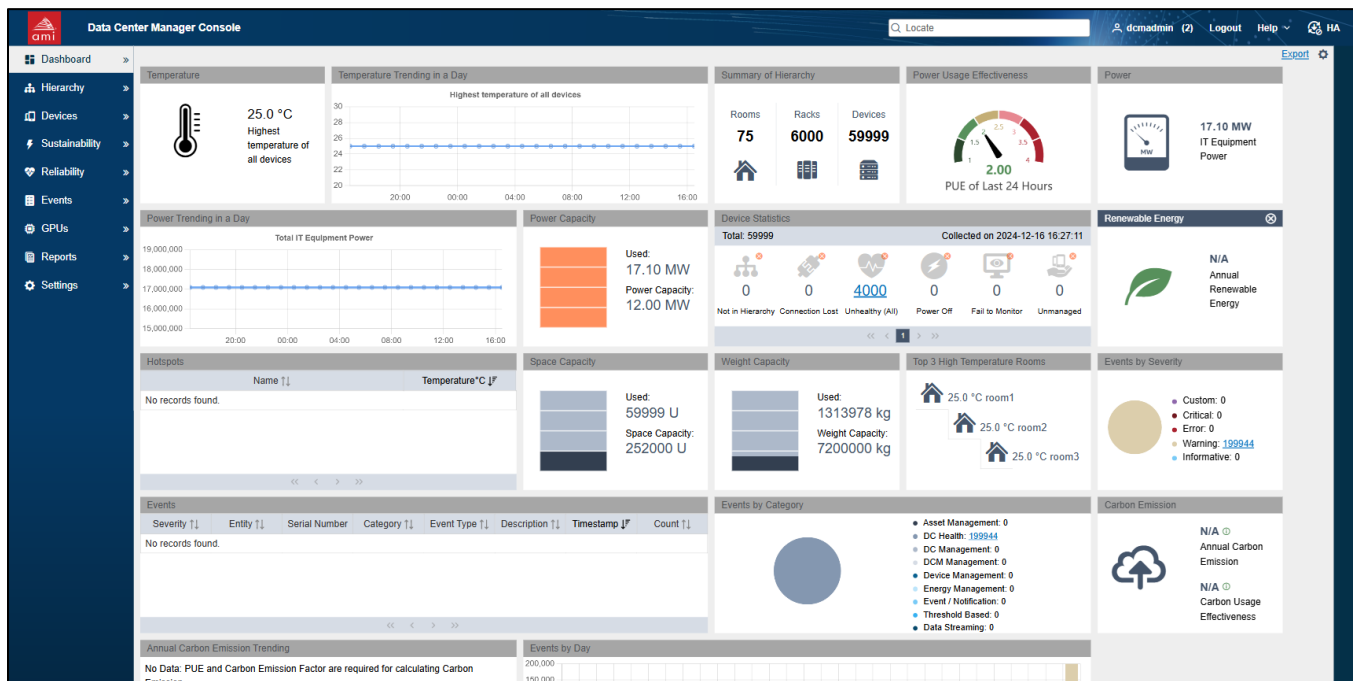


Figure 21 Dashboard

You can customize the dashboard by adding, deleting, or moving the gadgets in it.

- To add a gadget, click the 'Gear' icon on the top right corner. In the popup dialog, confirm the gadget you need and then click 'OK'.

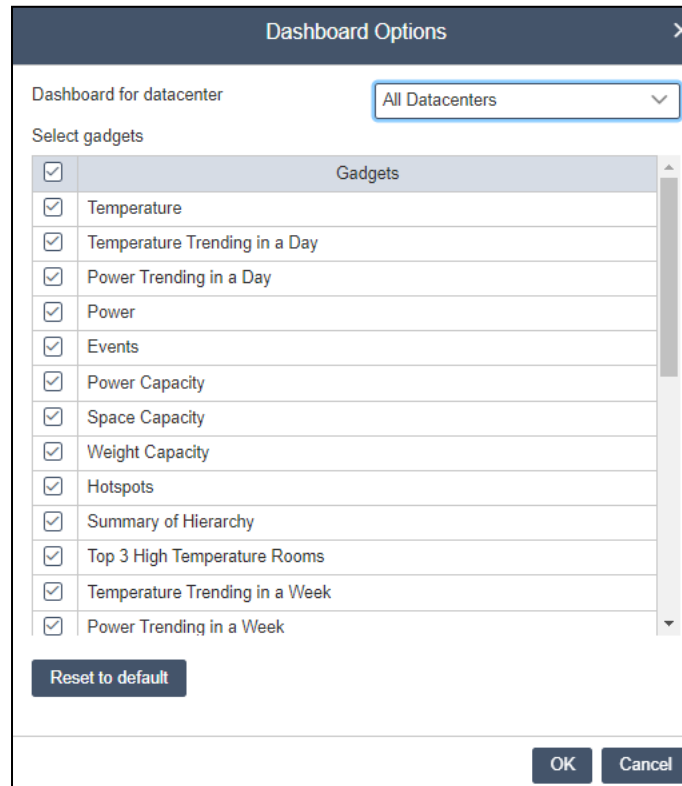


Figure 22 Dashboard Options

- To delete a gadget, deselect it.
- To move a gadget, drag the gadget to the desire location.
- To reset the dashboard to the default status, click the ‘Gear’ icon on the top right corner. In the popup dialog, click the **Reset to default** link.
- To view only one datacenter in the dashboard, you can choose that datacenter from the dropdown list **Dashboard for datacenter** under **Dashboard Options**.
- To specify gadget options, you can move your mouse to the gadget and click the spanner icon (which will appear if the gadget is configurable) on the top of the gadget. Then specify the gadget options in the popup dialog.

Most data in the dashboard will be refreshed automatically per minute.

The dashboard snapshot can be exported by clicking **Export**. It can also be sent through email by configuring **Email Subscription** in **Settings** page.

3.2 Hierarchy

AMI DCM Console manages entities through the following hierarchy structure:

Data Center > Room > Row > Rack > Device > Blade

When you are creating a hierarchy:

- You can only add Rooms to a data center.
- You can only add Rows to a room.
- You can only add Racks to a row.
- You can only add Devices to a rack.

- You can add Blades to either a rack or a chassis (displayed in Device list).

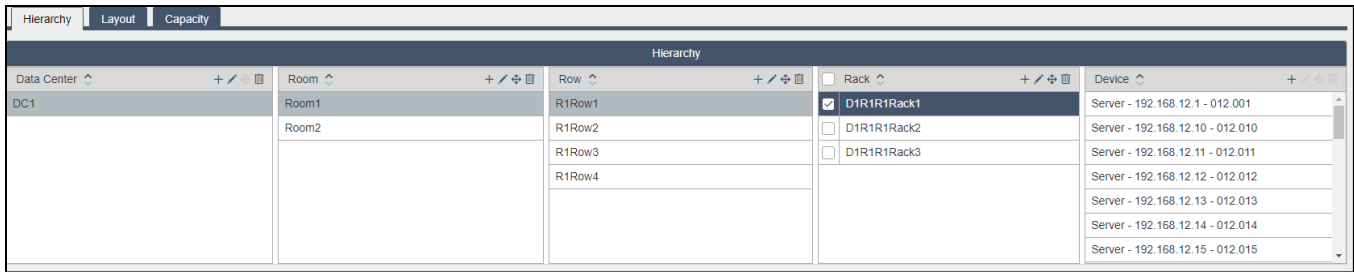


Figure 23 Hierarchy

Creating Hierarchy

On the **Hierarchy** page, click **+** in the **Data Center** list to add a DC. Specify the name in the popup dialog, then click **OK**.

Select a **DC** and click **+** in the **Room** list to add a room for it. Specify the name of the room in the popup dialog, then click **OK**.

Add rows to a room in the same way.

Select a row and click **+** in the **Rack** list to add a rack for it. Specify the name of the rack in the popup dialog, configure the space capacity and total power capacity. Check the box **“PDU Power as Rack Power”** if you want to take the power reading of PDU(s) in the rack as the IT equipment power of the rack, then click **OK**.

Note:

Name and Total Power Capacity are mandatory when you are adding a rack.

If **Total Power Capacity** is specified at Data Center, Room, or Row level, AMI DCM Console would use it to calculate the utilization percentage instead of the aggregated capacity from rack level.

PUE (Power Usage Effectiveness) is an optional property for data center and room to calculate **“Non IT Facility Energy”** and **“Energy Consumed (Total)”** metrics. If **Total Power Capacity** is not specified, AMI DCM Console would use PUE specified in the **Settings** page.

Adding Devices

Select a rack and click **+** on the **Device** tab. The popup dialog shows **“Devices not in Hierarchy”**. Select the devices you want to add to the rack, and then click **OK**.

You may also add a new device to a rack by navigating to the **Add New Device** tab in the popup dialog, and then specify the information of the device as described in [Adding a Device Manually](#).

Note: If you do not specify **Size of Device** and **Derated Power**, their values will be set by default (1 for **Size of Device** and 400 for **Derated Power**) after you click **OK**. The default values vary from different device types.

Hierarchy Management

In the **Hierarchy** tab on **Hierarchy** page, each entity can be edited or deleted (recursively with the sub-groups and devices) by clicking **Edit** or **Delete**.

To edit an entity:

- Select the entity.
- Click **Edit**, then click **OK**.

To delete one or more entities:

- Select the entity/entities.
- Click **Delete**, then click **OK**.

You may also click **Move** to change the hierarchy:

- Select the entity/entities, then click **Move**.
- In the popup dialog, select the destination, then click **OK**.

Note: You can refer to the **Hierarchy** tab by clicking the hyperlinks on entities. Almost all entities are linked to the **Hierarchy** tab.

Summary

The **Summary** widget on the **Hierarchy** tab displays detailed information about each entity, including temperature, power, space, and events, etc. You may export the selected hierarchy to an excel file at any level.

Summary of a Data Center

The **Summary** widget of a selected Data Center in the **Hierarchy** tab displays the following information:

- The highest inlet temperature
- The power capacity currently consumed against the power unused
- The space capacity currently consumed against the space unused
- The weight capacity currently consumed against the weight unused
- The total number of the racks and devices in the DC
- The total number of the processors, memory, and local hard disk in the DC
- The device status in the DC

The **Events** tab lists all the events of the DC.

Note:

The thermometer in the **Temperature** graph will turn red if the **Highest Inlet Temperature** exceeds 27 degrees.

The **pie charts** in the **Power** and **Space** graphs will turn red if the used amount surpasses the capacity configured.

Summary of a Room

The **Summary** widget of a selected room in the **Hierarchy** tab displays the following:

- The highest inlet temperature
- The power capacity currently consumed against the power unused
- The space capacity currently consumed against the space unused
- The weight capacity currently consumed against the weight unused
- The total number of the racks and devices in the room
- The total number of the processors, memory, and local hard disk in the room
- The device status in the room

The **Summary of a room** is similar to that of a DC.

The **Events** widget lists all the events of the room.

Summary of a Row

The **Summary** widget of a selected row in the **Hierarchy** page displays the following:

- The highest inlet temperature
- The power capacity currently consumed against the power unused
- The space capacity currently consumed against the space unused
- The weight capacity currently consumed against the weight unused
- The total number of the racks and devices in the row
- The total number of the processors, memory, and local hard disk in the row
- The device status in the row

The **Summary** of a row is similar to that of a DC.

The **Events** widget lists all the events of the row.

Summary of a Rack

The **Summary** widget of a selected rack in the **Hierarchy** tab displays the following:

- The highest inlet temperature
- The power capacity currently consumed against the power unused
- The space capacity currently consumed against the space unused
- The weight capacity currently consumed against the weight unused
- The total number of the devices in the rack
- The total number of the processors, memory, and local hard disk in the rack

The **Summary** of a rack is similar to that of a DC, except that the total number of the racks is not listed. You may click '**Rack View**' to see a visualized rack figure.

In '**Rack View**', the devices are color-coded by temperature, rectangles in white representing free space. When you move your mouse over a device, the detailed information of that device displays in tooltip.

By clicking the corresponding rectangle in the '**Rack View**', the device will be selected in the hierarchy, and it will be surrounded by blue dot line in the '**Rack View**'.

The **Events** widget lists all the events for the rack.

Summary of a Device

A selected device in the **Hierarchy** tab displays the following in the Summary widget:

- The highest inlet temperature
- Power
- Space
- Weight
- The details of the device

The **Summary** of a device is different from that of a group.

- The **Temperature** graph displays its highest inlet temperature.
- The **Power** graph shows its current power.
- The **Space** graph displays the space that it occupies.

The blue dashed line around a device in the visualized rack highlights the device selected. The empty rectangles with no color represent the free space. The **Events** widget lists all the events for the device.

Note: To refresh the properties and status of the selected device, click **Reconnect** on the Device Table widget.

Power/Temperature

Select an entity on the **Hierarchy** page and then check the **Power/Temperature** widget to see its details.

Power and temperature data are plotted in the figures with the corresponding data granularities. CPU utilization data is plotted if in-band OS information is specified for the given server.

The temperature figure shows:

- The Highest Inlet Temperature
- The Lowest Inlet Temperature
- The Average Inlet Temperature

The power figure shows:

- The Highest Power Consumption
- The Lowest Power Consumption
- The IT Equipment Power

You can view the power/temperature values by hovering your mouse over the data points in the curves.

By default, the power and temperature figures display the trending data in the past hour. You can click the arrow buttons “<” or “>” to view the data in the previous or future time window, or view them in different time windows by clicking the corresponding buttons.

To analyze the data more conveniently, you can save the measurement data to an excel file by clicking on **Export Data** at the top of the **Temperature/Power** widget.

Choose the start and end time for data exporting and then click **OK**.

Note: The corresponding data granularity varies from time window size and is shown in the figures.

The **Power/Temperature** widget also provides energy consumption metrics for the selected entity:

- **IT Equipment Energy** gives the total energy consumption of all the IT devices.
- **Non-IT Facility Energy**, obtained by multiplying IT Equipment Energy with a multiplier, estimates the energy consumption for cooling.
- **Energy Consumed (Total)** gives the total energy consumption of the IT devices and the cooling system.

Note: After enforcing a policy on the entity selected, the Requested Power Cap will be plotted in the power trending graph.

GPU Power and GPU temperature

Select an entity on the Hierarchy page, then check the GPU Power/Temperature widget to view its details. GPU power and temperature data are plotted in the figures with corresponding data granularities. By default, the power and temperature of all GPUs in the server are plotted. You can unselect the 'Total GPU' checkbox and select specific GPUs to view their power and temperature trending charts.

The GPU temperature figure shows:

- The highest inlet temperature of the whole server
- The lowest inlet temperature of the whole server
- The average inlet temperature of the whole server
- The instantaneous temperature of specified GPUs

The GPU power figure shows:

- The instantaneous power consumption of the whole server
- The instantaneous power consumption of specified GPUs

You can view the GPU power and temperature values by hovering your mouse over the data points on the curves. By default, the GPU power and temperature figures show trending data from the past hour. You can click the '<' or '>' arrow buttons to navigate to previous or future time windows, or switch to different time windows by clicking the corresponding buttons.

Note: Only licensed GPUs can be selected in the widget. To monitor GPUs via in-band SSH channel, inband information needs to be specified in server properties.

GPU Utilization and GPU Memory Utilization

Select an entity on the Hierarchy page, then check the GPU Utilization/Memory Utilization widget to view its details. GPU utilization and memory utilization data are plotted in the figures with corresponding data granularities.

The GPU utilization figure shows the instantaneous utilization of the selected GPUs.

The GPU memory utilization figure shows the instantaneous memory usage of the selected GPUs.

You can view the GPU utilization and memory utilization values by hovering your mouse over the data points on the curves. By default, the GPU utilization and memory utilization figures display trending data from the past hour. You can click the '<' or '>' arrow buttons to navigate to previous or future time windows, or switch to different time windows by clicking the corresponding buttons.

Note: Only licensed GPUs can be selected in the widget. To monitor GPUs via in-band SSH channel, inband information needs to be specified in server properties.

Layout

The layout tab demonstrates how racks are distributed in rooms. Every box in the layout represents the corresponding rack in the room. A red box indicates that the rack is hot. Detailed information about the rack, including its **Name**, **Capacity**, **Total power capacity**, **Weight Capacity**, **Temperature**, **Power**, **Grid X** and **Y** and so on, will appear once you move your cursor onto it. Right click the rack in the layout and choose **Go to the rack**, you will get detailed information about the rack.

To add a rack into the layout, you can either click **Add in Rack, Row, Room, Data center** in the Hierarchy and set **Grid X** and **Y**, or Right click the blank space in the Layout, and choose **Move rack** to the grid.

There are two ways to change the rack location in the layout. You can choose the specific rack in **Rack, Row, Room, Data center** in the **Hierarchy** and edit its **Grid X** and **Y**. And besides, you can also right click the rack in the layout and choose **Move the rack to drag** or **move the rack based on its current location** in the room.

You may rotate view angle of the room layout by editing the “**Layout Original Position**” of the room.

You may specify a row’s “**Rack Orientation**” by editing it in the hierarchy.

You may switch the data layer by clicking “**Layer**” icon. The data for temperature, power and capacity are color coded for the entire layout view.

When you select a row in the hierarchy, you can switch the layout view angle to Front (panel) view by clicking the “**Eye**” icon. In the “**Front view**” you may check the front panel temperature distribution for all the devices from the selected row. By switching the angle, you have the **2D orthogonal thermal map** for your datacenter.

You may check the historical data in the layout view by clicking the “**Clock**” icon. A new web browser window would pop up after you select an available timestamp. You may compare the data (temperature/ power/ capacity) to better optimize your datacenter energy efficiency.

What’s more, you can zoom in or out the layout view by moving the scroll wheel on the mouse. Right click the blank space and choose **Toggle full screen**, you will get a full and clear layout view. Whenever you go too far away from the layout, you can always get back to the original point by simply clicking **Go to the origin**.

You can set a layout background image by clicking **Select background image**.

Capacity

It shows the current power capacity, space capacity and weight capacity status.

You may specify device information to search for racks to install the device.

Type in **Size**, **Derated Power**, **Weight**, and then click **Search**.

Then the racks that meet your requirements will be listed.

You may plan (a what-if analysis) the way to install your new devices onto the racks by clicking the planning button.

3.3 Devices

All Devices

All Devices tab contains all the devices discovered, imported, or manually added.

On this page, you can edit device **Name**, **Description**, etc. You can also delete a device from the list or apply a filter to show specific devices.

Adding a Device Manually

Click **Add** to add a new device to the Device List.

Choose the device type in the drop-down list.

Specify **Name**, either **IP Address** or **Hostname** of the new device in the popup dialog. You may also need to provide certain additional information based on the **Device Type** you selected. For servers managed through IPMI protocol, you may specify in-band OS information to retrieve CPU utilization data along with the power and temperature data.

For example, if you chose Server as the Device Type, you must choose a protocol from IPMI, SSH, and WMI, then type in the related information.

Certain additional attributes are available for asset management purpose (e.g., Owner, Business Unit, Contact, Warranty Expiration). You can input customized attributes as well (need to be configured in **Settings** page first).

Note:

- You can choose to enter either **IP Address** or **Hostname**, not both.
- If you choose **Server** as the device type and **SSH** or **WMI** as the protocol, DCM will login the OS with the username and password. Then DCM will get the workload information from the OS to estimate power consumption dynamically.
- For **Network Devices**, DCM supports Cisco switches with Cisco EnergyWise technology enabled.

Redfish Supported Servers

If the server is Redfish enabled and you plan to monitor the device with this protocol, select HTTPs and then provide the authentication credentials during discovery or in the **Add New Device** tab.

PDU Configuration

If you add a PDU with outlet level power monitoring capabilities, you can associate unmanaged devices to that PDU. By doing this, you can get the power information of the devices without power monitoring capability from the PDU outlet power.

Click the **Device** tab and choose the **Outlet Management** link on the **PDU** summary page. Choose the unmanaged device from the drop-down list for the corresponding outlet. Then click **OK**.

Adding an Unmanaged Device

If you choose **Unmanaged server**, **Unmanaged network device**, **Unmanaged storage device**, or **Unmanaged Chassis** as the device type, you may need to specify Power Estimator(s) for the device(s) because these unmanaged devices do not have power monitoring capabilities. You can assign parameters to the estimator by specifying typical power or looking up in the power profile.

To look it up, you need to go to the **Hierarchy** page, select the **Hierarchy** tab, then add the unmanaged device to a rack.

Select the device, click the **Edit** link on the **Device Table** widget. DCM will fill in the **peak power** and **active idle power** automatically according to the device selected. Click **OK** to finish configuring **Power Estimator**.

If your device is not listed, and you know the typical power of your device, you can:

- Fill in the **peak power** and **active idle power** directly.
- Click **Add** in the popup dialog to add a power profile.

You can **Edit** or **Delete** a power profile by clicking the corresponding button.

You can also check, edit, and delete all the power profiles through the **Power Profile** tab on the **Settings** page.

Note:

- After you add an unmanaged device into a rack, an event will appear in the **Events** list to remind you to specify a power estimator for it.
- You can configure the **Power Estimator** for devices of the same type in batches.
- If you have specified an unmanaged device for a PDU, the information of the PDU will appear on the last line of the Device list. Take the screenshot below as an example, you can get its power information from Outlet1 of PDU with an IP address of 10.239.98.30. You can click the **Clear** link to disassociate this information.

Device Table	
Property	Value
Address	
Device Type	Unmanaged server
Device Model	
Capability	N/A
PDU Outlet	192.168.100.21, 2 Clear
Derated Power	400W
Protocol	
Platform ID	

Figure 24 Unmanaged Device

Filtering Devices

You can apply a filter to show specific devices only:

- Go to the **All Devices** tab on **Devices** page.
- Specify device name/address (partial or full).
- Click **Search**.

Advanced Search

You can search devices with combined conditions in the “**Advanced Search**” dialog by clicking the “Advanced Search” button.

Editing Devices

Click **Edit** to select the devices, and then click **OK**.

You can change the device name or optional information. Only common properties could be edited if you want to edit multiple devices.

Note: *IP Address/Hostname, Device Type, and Protocol information are based on the device configuration, which shall not be changed randomly.*

Deleting Devices

To delete device:

- Go to the **All Devices** tab on the **Devices** page.
- Select the device(s).
- Click **Delete**.
- Click **OK**.

Discovery and Import

Discovering Devices

Click ‘**Add Discovery Task**’ in the ‘**Discovery and Import**’ tab.

Select the protocol type from the drop-down list and input the IP range. The default ‘Subnet Mask’ is 255.255.255.0. You may need to provide some additional information based on the ‘Protocol type’ you choose.

Choose one from the seven protocol types in the drop-down list: IPMI, SNMPv1v2c, SNMPv3, WS-MAN, HTTPS, SSH, and INBAND.

Click **OK** to run the discovery task.

Add Discovery Task
✕

Please choose the protocol and enter the IP range, the subnet mask, and the credential.

Protocol	<input type="text" value="IPMI"/>		
First Address	<input type="text" value="Required"/>	Last Address	<input type="text" value="Required"/>
		Subnet Mask	<input type="text" value="255.255.255.0"/>
IPMI User Name	<input type="text"/>	IPMI Password	<input type="text"/>
Vendor	<input type="text" value="--ANY--"/>	IPMI Key	<input type="text"/>
	Memo	<input type="text"/>	

Figure 25 Add Discovery Task

Click **“Schedule”** to run the discovery task at a specific time or in a recurrent pattern.

Schedule Discovery Task
✕

Now
 Specific Time
 Recurrent

Figure 26 Schedule Discovery Task

Schedule Discovery Task
✕

Now
 Specific Time
 Recurrent

Hourly
 Daily
 Weekly
 Every day(s) on

Range of Recurrence:

Start

End

Figure 27 Discovery task

AMI DCM Console supports running multiple discovery tasks at the same time. However, if too many discovery tasks are running at the same time, the performance of AMI DCM Console could be impacted.

When the discovery progress reaches 100%, restart or remove the task by clicking the **'Run Again'** or **'Remove'** buttons.

The devices discovered will be added to the **'Device List'** automatically. For security reasons, AMI DCM Console will verify each device's identity during discovery by default. This can be disabled by modifying below (both) configuration files:

confconsole.config.xml:

```
<entry key="VALIDATE_AUTH_IN_DISCOVERY">false</entry>
```

confuser.config.xml:

```
<entry key="AUTHENTICATE_ENTITY_BY_DEFAULT">false</entry>
```

When it is enabled, you should provide device identity information to AMI DCM Console.

1. For SSH based devices, a file named "know_hosts" should be placed in the installation folder. It will take effect after restarting AMI DCM Console services. The host keys should be added in this file following below example:

```
192.168.10.10 ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBLka4e0TCDGzIAQAM+4tJf2Je
WB/LhOgCa/pk/LXYGqiY/7oBFnJGmvdosPoe0CpFNDz6/ubLPmNrp+xyWAoi+Y=
```

If a SSH based device has multiple host keys, AMI DCM Console will choose one key according to below order (key types)

```
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
ssh-rsa
ssh-dss
```

Click [here](#) for a detailed format explanation of this file.

2. For HTTPS based devices, you can use below command to import the device certificate to AMI DCM Console keystore:

```
external\jre\bin\keytool -import -keystore <keystore file path> -alias
<devicealiasname> -file <device cert file path>
```

Example:

```
external\jre\bin\keytool -import -keystore "C:\Program
Files\ami\dcm\keystore.ssl" -alias server001 -file
c:\temp\device_certs\server001.cer
```

You can verify the added device certificate by below command:

```
external\jre\bin\keytool -list -keystore <keystore file path>
```

- For WMI based devices, when AMI DCM Console is configured to verify device identity, they cannot be found through discovery process, and you need to manually add them in AMI DCM Console with FQDN specified. Refer to [Adding a Device Manually](#) section for details.

Note:

If some devices in the network you specified are not discovered or imported by AMI DCM Console, check the following:

- Network connectivity
- Device status
- Specified device credentials

Importing Devices

You can import devices with or without hierarchy information into AMI DCM Console. To import devices, you need to create either an Excel or a Csv (Comma separated values) file containing device and hierarchy information. Certain device types require specific columns to be included. For example, for IPMI based servers: Name, type, and Address are required, while other columns are optional.

Sample Excel file:

	A	B	C	D	E	F	G
1	name	type	address	username	password	snmpcommunitystring	snmpencryptionpassword
2	node manager	IPMI	10.239.43.42				
3	serverB	IPMI	10.239.43.19				
4	serverC	IPMI	10.239.43.27				
5	serverD	IPMI	10.239.43.48				
6	serverA	IPMI	10.239.43.7				
7	ibm	SSH	10.239.45.1	USERID	PASSWORD		
8	apc	SNMPv1v2c	10.239.43.236			public	
9	dell_cmc	WS_MAN	10.239.45.3	root	calvin		

	H	I	J	K	L	M	N	O	P
1	httpsport	sshport	distinguishedname	rack	row	room	dc	size	location
2				44444	3333	222	11		30
3				rack2	row1	room1	dc1		30
4				rack2	row1	room1	dc1		
5				rack2	row1	room1	dc1	1	
6				rack1	row1	room1	dc1	1	
7		22		rack2	row1	room1	dc1		
8				rack1	row1	room1	dc1		12
9				rack1	row1	room1	dc1	16	
10				rack1	row1	room1	dc1		

Sample CSV file:

```
name,type,address,serial_number,vendor,deratedpower,username,password,key,authenticateentity,
ServerA,HTTPS,192.168.1.37,0000C0A80125,INSPUR,400,dcm,user@123,,FALSE,,,,,443,,,r2,r1,r1,dc,
ServerB,HTTPS,192.168.1.32,0000C0A80120,LENOVO,400,dcm,user@124,,FALSE,,,,,443,,,r2,r1,r1,dc,
ServerC,HTTPS,192.168.1.33,0000C0A80121,LENOVO,400,dcm,user@125,,FALSE,,,,,443,,,r2,r1,r1,dc,
ServerD,HTTPS,192.168.1.34,0000C0A80122,LENOVO,400,dcm,user@126,,FALSE,,,,,443,,,r2,r1,r1,dc,
PDU1,SNMPv1v2c,192.168.11.19,MC22080838,VERTIV,10,,,TRUE,,,,,,CD_Rack_01_01_02,CD_Row_01_0
Storage1 - 192.168.11.23,SNMPv1v2c,192.168.11.24,4.51606E+11,NETAPP,400,,,TRUE,,,,,,Storage
NVSwitch,Unmanaged network device,,,,400,,,TRUE,,,,,,Oberon_GB200_NVL36,CD_Row_01_01,CD_Rc
```

The following table lists the description of each item.

Item	Description
name	Entity display name
description	Description of a device or a group.
type	Supported protocol types including IPMI, SNMPv1v2c, SNMPv3, WS_MAN, SSH, and INBAND_PROTOCOL. For unmanaged device, it should be "Unmanaged server", "Unmanaged network device", or "Unmanaged storage device".
address	IP address
username	Username to login. For HTTPS power meter, this field is used for Gateway UUID.
password	Password to login. For HTTPS power meter, this field is used for API Key.
snmpcommunitystring	Community string for accessing the SNMP-based platform via V1
snmpencryptionpassword	The SNMP-based platform user account password for encryption
snmpauthenticationprotocol	The authentication protocol for an SNMP v3 based device. It can be one of the options below: <ul style="list-style-type: none"> AuthMD5 AuthSHA1 AuthHMAC128SHA224 AuthHMAC192SHA256 AuthHMAC256SHA384 AuthHMAC384-SHA512
snmpencryptionprotocol	The encryption protocol for an SNMP v3 based device. It can be one of the options below: <ul style="list-style-type: none"> PrivDES Priv3DES PrivAES128 PrivAES192 PrivAES256
httpsport	The HTTPS port for the entity
sshport	The SSH port for the entity
distinguishedname	The UCS DN of the entity (used for identifying and discriminating UCS devices in DCM)
key	The IPMI key for the node
nameplatepower	Rated power capacity from nameplate.
deratedpower	De-rated power for both managed and unmanaged nodes
size	Size of the entity
location	Location of the physical entity
vendor	Import device from specified vendor only. It can be one of the options below: <ul style="list-style-type: none"> ANY ALTOS AMD APC ARISTA

	<ul style="list-style-type: none"> • AVOCENT • BAYTECH • BROCADE • CHATSWORTH • CISCO • CONTOSO • COOLIT • DELL • DIGITALFREAKS • EATON • EMC • EMERSON • ENLOGIC • EXTREMENETWORKS • F5 • FUJITSU • H3C • HITACHI • HOFFMAN • HP • HUAWEI • IBM • INSPUR • INTEL • KONTRON • LENOVO • MELLANOX • NETAPP • NETTRIX • ORACLE • PLANET • QCI • RARITAN • RSA • SERVERTECH • SIEMON • SUGON • SUN • SUPERMICRO • TRIPPLITE • VERTIV • ZTE • OTHERS <p>If not specified, devices from other vendors can be imported.</p>
authenticateentity	To decide whether to authenticate Dell CMC in WSMAN connection. Valid value: true, false
model	Device model for unmanaged devices
ostype	OS type for IPMI devices. Valid values: Windows, Linux, Xen, ESX
osaddress	OS IP address
osusername	OS user name
ospassword	OS password
typicalpower	Typical power used in power estimation
idlepower	Idle power used in power estimation
peakpower	Peak power used in power estimation

custom_mgmtconsoleurl	The customized management console URL for a device.
EPR	Action for Emergency Power Reduction. It can be one of the options below: <ul style="list-style-type: none"> Minimize Power Consumption Shutdown No Action
offline	Set to "Yes" to mark this device as in offline mode.
owner	Owner of the device
contact	Contact information associated with the device
warranty expiration	The warranty expiration date.
business unit	Business unit the device associated to
reportinlettemp	Option to decide whether a ChatsWorth PDU should report temperature (True / False)
rackcapacity	Capacity of a rack (in U)
rackpowercapacity	Power capacity of a rack (in W)
roompowercapacity	Power capacity of a room (in W)
rowpowercapacity	Power capacity of a row (in W)
cabinetpdupowercapacity	Power capacity of a cabinet pdu (in W)
gridx	The x axis of a rack in the room layout coordinate
gridy	The y axis of a rack in the room layout coordinate
width	The width of a chassis / blade (number of grids)
height	The height of a chassis / blade (number of grids)
start_x	The start position (in x-axle) of a blade in a chassis (start from 1)
start_y	The start position (in y-axle) of a blade in a chassis (start from 1)
dc	Data center
room	A physical group that includes all the rows from a physical room in the data center
rack	A physical group that includes all the devices from a physical rack in the physical data center.
row	A physical group that includes all the racks from a physical row in the physical data center
enclosure	An enclosure containing blade servers
group	A group that an entity belongs to.
birthday	The date when the device is used for the first time. Format : YYYY-MM-DD Example : 2024-05-10
creation_time	The time when the device is added into AMI DCM Console (for export only, will be ignored during import). ISO 8601 Format: YYYY-MM-DDTHH:MM:SS±HH:MM Example : 2024-05-10T22:44:27-08:00
weight_kg	device weight in kilograms
rowweightcapacity_kg	row weight capacity in kilograms
rackweightcapacity_kg	rack weight capacity in kilograms
rackweight_kg	rack weight in kilograms
rackmiscweight_kg	rack miscellaneous weight in kilograms
weight_lb	device weight in pounds
rowweightcapacity_lb	row weight capacity in pounds
rackweightcapacity_lb	Rack weight capacity in pounds
rackweight_lb	rack weight in pounds
rackmiscweight_lb	rack miscellaneous weight in pounds

Note:

If weight value is available both in kilograms and pounds in the import file, DCM will use the one matching the current weight unit setting.

Custom attributes can be imported as well. A '*' character should be appended for those not built-in attributes. Before importing devices with custom attributes, you should configure the custom attributes in **Settings** page, otherwise the custom attributes will be ignored.

To avoid issues caused by special characters in the password field, please add an extra leading single quote mark (') to the cell value. For example, if the intended password is \$%#123456, you can put '\$%#123456 in the password cell to ensure the intended value is used in import.

When running import task, you can check the progress or stop the task. For a completed import task, you can check the results or remove the task by clicking corresponding link and button.

Groups

The **Groups** tab will help you sort and group the devices you're interested in. You can manage, monitor, and configure the devices in the groups the same as in the **Hierarchy**.

3.4 Operations on Groups

Adding groups

1. Click **+** under **Group List** to add a group. Specify the name and give an optional description in the popup dialog, and then click **OK**.
2. Select a **Group**, click **+** at the right side of the "**Devices**" table to add a device.

Note:

If you want to add all the devices in an entity (Data Center/Room/Row/Rack) to a group, check the box for that entity, then click **OK**.

You can also click **search** to search devices and add them to the selected group.

Editing/deleting groups

You may click corresponding button to edit or delete a group in the **Group List**.

Summary/Power/Temperature/Events

These are similar to those of Hierarchy page.

Power On/Off

You may schedule power on/off tasks for a group of devices by clicking it.

Provisioning

Starting from AMI DCM Console version 3.3, this feature provides the capability to review and update firmware, provision system settings, and mount ISO images. The functions may vary depending on each servers' capabilities.

For Intel® Server Systems, this feature can be enabled during installation. AMI DCM Console can detect Intel® SDP Tool and generate the required configuration automatically. AMI DCM Console's provisioning features that based on Intel® SDPTool are only available for Linux. Below are the steps to enable provisioning after AMI DCM Console is installed without Intel® SDPTool.

1. Download and install Intel® SDP Tool
2. Run the command.

```
/opt/ami/dcm/dcm_util.sh enableprovisioning
```

Note:

The System Setting provisioning feature may not work if the server's BIOS Administrator password has been set.

The above procedure is applicable for provisioning Intel® Server Systems only.

Some of the servers requires Intel SDP Tool for provisioning capabilities. The SDP Tool can be downloaded from Intel web site: [Intel SDP Tool](#).

After you successfully enable the provisioning feature, you can find the BIOS version and BMC firmware versions of Intel® Server Systems in the Firmware Version column of All Devices.

You can select servers from All Devices or one server group from Groups, and then click Provisioning to update firmware, change system settings or mount ISO file.

Firmware Update

In the “**Firmware Update**” tab of the “**Provisioning**” dialog, you can create a “**Firmware Update**” task to run immediately or at a future time. You will need select the components first. For non- Intel® Server Systems, you need specify the file path for firmware update.

For Intel® Server Systems, if you use the “Preconfigured” mode to update firmware, the target firmware image files are pre-configured based on the server model and are mapped in the Intel® SDP Tool configuration file.

You can also upload your local firmware image file and get it updated to the selected servers which should be of the same model.

After the task is added, you can check its status in the Provisioning Status page. When the task is completed, you can check if it succeeded or failed in the result link.

System Settings

You can select one Intel® Server System to get its system settings. After the task is finished, you can download its system settings file in the task card.

For servers of the same model and firmware version, you can deploy the same settings by changing some values in the system settings file.

You can choose **Change Single System Setting** for all servers, such as enabling Intel Virtualization Technology.

Mount ISO

You can select some servers and mount an ISO file whose file path is specified in this dialog. The system on which AMI DCM Console is installed should have access to this file path. You can specify whether the servers will be automatically reset after the ISO file is mounted. After the task is finished, you can unmount the ISO file for all servers on the 'Mount ISO' task card. A new task will start to unmount the ISO file.

Checking the Latest Firmware Version

AMI DCM Console can check if there are newer firmware versions for Intel® Server Systems. The server on which AMI DCM Console is installed requires Internet connectivity. To enable this feature, perform the following steps:

1. Follow the ServerTools FWConnect API instructions [here](#).
2. After getting the required approvals, make sure that the checkbox under Scopes is unchecked during the Authorization step (not mentioned in the above link).

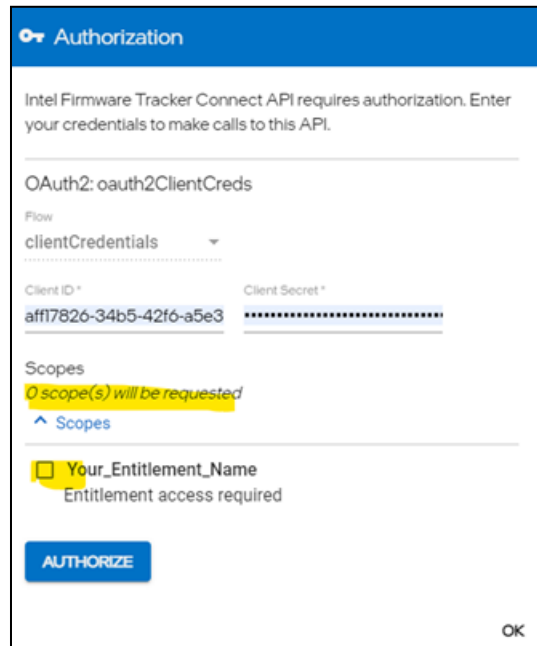


Figure 28 Authentication

3. Edit /etc/sdptool/sdptool.conf and enter **Client ID** and **Client Secret** as shown here:

```
[Global]
; SDPTool version
version=4.2-0
; Establish secure connections only
verifyCertificate=false
; SDPTool log directory
logRootPath=/usr/local/Log/SDPTool/Logfiles
; Enable full log capture
enableFullLog=true

[softwareinventory]
; Client ID for server tools API
ClientId= 94d36d4f-f4b7-42be-be31-fab0f71f9843
; Client Secret for server tools API
ClientSecret= X008Q~XRnjqHZjU3Fhc6NbFh1fZRizXf1V-myc-.

[cup_deploy]
staging=false
; Staging directory for CUP deploy
stagePath=/var/sdptool/cup
```

Figure 29 Config

4. Test if Intel® SDPTool is able to check the latest firmware versions available for different Intel® Server System models as shown below:

```

root@dms-ubuntu-nuc:/usr/local/SDPTool# SDPTool softwareinventory S2600BPB
Available BIOS Version ..: 02.01.0016
Available ME Version ....: 04.01.04.804
Available BMC Version ...: 2.88.71773d70
Available SDR Version ...: 1.49
Available FRU Version ...: 1.49
Available DCPMM Version ..: 1.2.0.5446
root@dms-ubuntu-nuc:/usr/local/SDPTool# SDPTool softwareinventory M50CYP2SBSTD
Available BIOS Version ..: 01.01.0007
Available ME Version ....: 04.04.04.202
Available BMC Version ...: 2.90.e5e4d391
Available SDR Version ...: 0.44
Available FRU Version ...: 0.44
Available CPLD Version ..: 4.2
Available PMeM Version ..: 2.2.0.1553
root@dms-ubuntu-nuc:/usr/local/SDPTool# SDPTool softwareinventory R1208WFTZSR
Available BIOS Version ..: 02.01.0016
Available ME Version ....: 04.01.04.804
Available BMC Version ...: 2.88.71773d70
Available SDR Version ...: 2.04
Available FRU Version ...: 2.04
Available PMeM Version ..: 1.02.00.5446
root@dms-ubuntu-nuc:/usr/local/SDPTool# SDPTool softwareinventory R2312WF0NPR
Available BIOS Version ..: 02.01.0016
Available ME Version ....: 04.01.04.804
Available BMC Version ...: 2.88.71773d70
Available SDR Version ...: 2.04
Available FRU Version ...: 2.04
Available PMeM Version ..: 1.02.00.5446
root@dms-ubuntu-nuc:/usr/local/SDPTool# █
    
```

Figure 30 Config

5. Edit DCM startdcm.sh script and enter your http_proxy and https_proxy details. If no proxy is required, replace those two lines with the following:

```
export NO_PROXY="localhost,127.0.0.1,:::1"
```

```

#!/bin/bash
#
# startdcm.sh:  AMI Datacenter Manager Server Daemon
#
#main function
export USE_DCM_SERVICE='USEDCMSERVICE'
CURRENT=$(dirname "$0")
export HOME=$(cd $(CURRENT) && pwd)

case "$1" in
start)
export http_proxy="http://proxy.company.com:1080"
export https_proxy="http://proxy.company.com:1080"
if [ "$USE_DCM_SERVICE" = '1' ]; then
systemctl start dcm
else
"$HOME/dcm_service.sh" start
fi
;;
    
```

Figure 31 Config

6. Edit the /etc/sudoers file and add the http_proxy and https_proxy (or no_proxy) variables as shown below:

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults    env_keep += "ftp_proxy http_proxy https_proxy no_proxy"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
```

Figure 32 Config

7. After restarting the AMI DCM Console, AMI DCM Console will be able to detect and notify you if there is any new firmware for an Intel® Server System as shown below:

Device Table		Property	Value
Address	192.168.12.3		Power Off Reconnect
Serial Number	012.003		
Device Type	Server		
Device Model	Node Manager 4.0 Intel Corporation - M50CYP2SBSTD		
Capability	power monitoring; temperature monitoring; power control		Edit
Provisioning Capability	Yes		
Mgmt Module Firmware Version	2.60 <i>New</i>		Provisioning More
Management Console URL	https://192.168.12.3:443		

Figure 33 Device Table

Note: If for any reason, AMI DCM Console is unable to lookup the latest firmware of an Intel® Server System, an event will be triggered as shown below:

Events Acknowledged Events						<input checked="" type="checkbox"/> Compressed View	Acknowledged
<input type="checkbox"/>	Severity	Type	Description	Time	Count		
<input type="checkbox"/>		NEW_FIRMWARE_DE...	Failed to detect new firmware	2023-1-31 15:56:18	2		

Figure 34 Events

3.5 Sustainability

Overview

In the **Overview** tab, the distribution of Annual carbon emissions among data centers and rooms is illustrated by a Pie chart. And a trending graph demonstrates the observed annual / monthly carbon emission data (as well as the projected data). You can specify a threshold for the annual / monthly carbon emissions by clicking the **Edit Threshold** link. If the threshold is exceeded, an event named Sustainability Issues will appear in a table.

Cooling Analysis

In the **Cooling Analysis** tab, the **Temperature Histogram** provides the real-time monitoring data of the inlet temperatures. The X-axis shows the temperature values, and the Y-axis gives the percentages of servers with the corresponding temperature values. **Sample Size** shows the number of devices whose temperature can be monitored in the selected room.

The current cooling status is evaluated with suggestions given, along with possible actions and the **Benefits** of taking these actions.

For example, when servers of inlet temperatures higher than 27 degrees are detected, they will appear in the **Hotspots** list.

Click **Refresh** on the top right to refresh the temperature data.

Low-Utilization Servers

Click **Analyze** on the **Low-Utilization Servers** tab to a list of low utilization servers for potential consolidation to improve energy efficiency. The timestamp of the analysis will show in the bottom-left corner of the screen.

Analyzing the utilization of many servers can be time-consuming. You can perform other tasks while the analysis is running in the background.

The **Daily Utilization Pattern** displays server utilization patterns based on historical monitoring data, which can assist with server consolidation. For instance, if one server is frequently busy at night but idle during the daytime, while another works quite the contrary, it may be beneficial to migrate workloads and shut one down.

Server Power Characteristics

To see the power consumption of different server models, go to the **Sustainability** page and click on the **Server Power Characteristics** tab. The bar diagram shows power values on the X-axis and server models on the Y-axis. The numbers next to the bars indicate the range of power consumption for each server model. As an example “**128 – 139**”, means that for all managed servers of a given model, the lowest power observed was 128 watts and the highest was 139 watts.

Advanced Power Model

You can add a power model for a server by selecting a server with both monitored power and utilization data, and at least 100 data points are required. Once added, you can predict its power consumption for a given workload.

Policies

Policies can be used to limit the power consumption of either a group or a device.

AMI DCM Console provides several policy types:

- **Custom Power Limit:** limits the total power consumption of an entity. When applied to a group, AMI DCM Console actively reallocates the power budgets to the individual servers within the group in each monitoring cycle. It attempts to minimize the gap between the power demands of each entity and the overall power allocation for the group to reduce the performance impact of the group power capping. AMI DCM Console monitors the power consumption data of the servers, estimates their power demand, and reallocates power budgets using a heuristic discriminative approach to solve a probabilistic model. In general, AMI DCM Console reacts quickly by allocating more power to servers to get new tasks running properly. If the total power demand of the group exceeds the group power constraint, AMI DCM Console implements a balanced power allocation. The policies are commonly applied to increase the server density with respect to power or cooling capacity.
- **Minimum Power:** throttles power consumption of an entity as much as possible to prolong business continuity in an emergency.

Creating Device Policies

To create a policy for a device, specify the policy name and select the policy type from the drop-down list in the popup dialog.

- If you choose **Custom Power Limit**, DCM will generate an alert when the actual power consumption is higher than the threshold you configured.
- If you choose **Minimum Power**, DCM throttles the device power to the minimum, so you do not need to specify a threshold.

To schedule the policy, navigate to the **Schedule** tab and click **OK**.

You may check the policy in the **Policies** tab or on the **Policies** page.

Note:

Reserve Budget is used for devices without power capping capability and is discounted from the total power limit.

Power Efficient policy type is supported for some old generation HP devices (e.g. iLO2/iLO3/iLO4), but it is not available by default as these devices require an insecure / outdated key exchange algorithm for SSH based communication. You can enable the insecure key exchange algorithms by appending the missing algorithm (e.g., `diffie-hellman-group14-sha1`) to the line beginning with "KexAlgorithms" in the "ssh_config" file under the "conf" folder (restarting AMI DCM Console services is required).

Creating Group Policies

You may configure the priorities of group members while enforcing Custom Power Limit at the group level. Excess power is distributed to the devices according to their priorities. You can choose one priority level for each member:

- Low
- Medium (Default)
- High
- Critical: DCM reserves the de-rated power for this entity.

Priority lists are policy-specific, and an entity may have different priorities in different policies. However, during policy calculation, a higher priority of an entity in one policy may override a lower priority of the same entity in another policy.

You may view all the policies on the **Policies** page to disable, edit, or delete policies.

Enabling/Disabling Policies

To enable/disable a policy:

- Click the policy's Enable/Disable link.
- The Status of the policy turns green/red.

Editing Policies

- Click **Edit** on the selected policy.
- Update policy details in the popup dialog.
- Click **OK**.

Deleting Policies

- Select the policies to delete by checking the boxes.
- Click **OK**.

3.6 Reliability

Unhealthy Devices

The Unhealthy Devices table lists all devices with health issues. Hovering over the state icon displays detailed information in a tooltip. Clicking the device hyperlink takes you to the Hierarchy to see the detailed device health info.

Anomaly Detection

Firmware Outlier shows firmware version outliers for servers of the same models.

Cooling Anomaly shows the details of cooling anomalies detected in rooms.

Fan Outlier shows anomalies of fan speeds, indicating potential issues with the fan.

SNMP Alerts

SNMP Alerts will appear only when “**Receive SNMP alerts**” is selected in **Settings** page.

SNMP alerts from managed devices can be viewed, acknowledged, and disabled in this table. They can also be forwarded through email / SNMP trap, with below option set to true in console.config.xml file, when “Email Subscription” / “SNMP Trap” are well configured in **Settings** page.

```
<entry key=" RELAY_DEVICE_SNMP_ALERT">true</entry>
```

Failure Indicator

The Failure Indicator helps determine whether a server model or component (such as memory, disk, or processor) is unhealthy based on failures observed over a long period of time, such as several months. It calculates the ratio of observed unhealthy status to successful observations and aggregates this data for each server model or location. However, this feature requires devices or components to support inventory and health monitoring to make it meaningful and available.

SSD

The first table on the SSD tab lists devices with unhealthy SSDs. This is determined by monitoring key attributes of SSDs. If any of these attributes fall below their corresponding failure thresholds, the SSD is marked as unhealthy, and its device will be added to this table.

The second table lists all the managed SSDs and their Estimated Life Span.

Note:

Currently, SSD related features in AMI DCM Console only support SATA SSDs on Linux based servers via SSH. These features rely on smartctl from the [smartmontools](#) package, which is usually included in mainstream Linux distributions. You can enable SSH root login and enter the root account credentials while adding the server to AMI DCM Console. You can also use non-root accounts, but they need to be added to the sudoer list.

The default sampling interval for SSDs is 1 hour which can be configured by adding the entry below in the console.config.xml file (30 minutes as an example).

```
<entry key="SMART_MONITOR_INTERVAL">1800</entry>
```

Unhealthy Sensor Thresholds

Thresholds for analog sensors can be set here to identify unhealthy components. To add a sensor threshold, click the plus button on the top right. A dialog box will appear, where you can input a sensor name, choose its type, set its condition, and give it a threshold as shown in the following example:

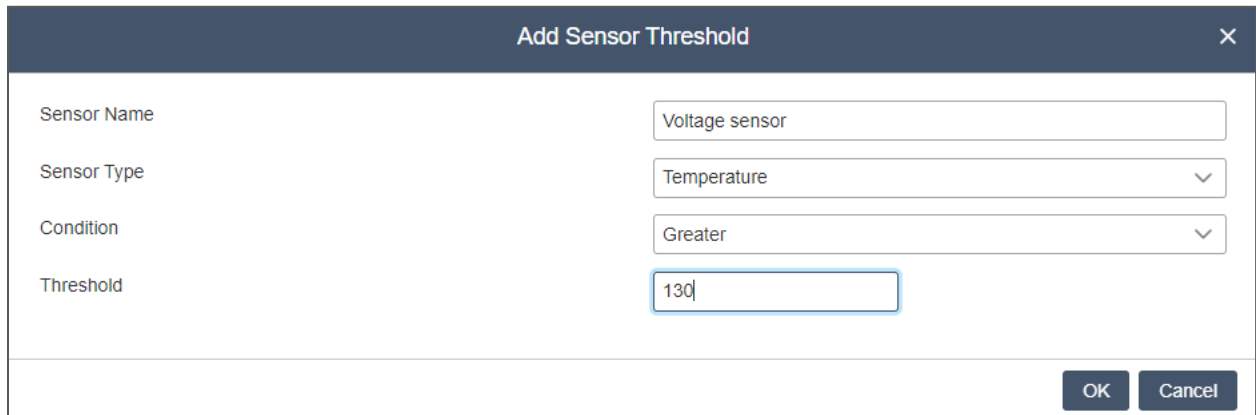


Figure 35 Add Sensor Threshold

Diagnostic Tools

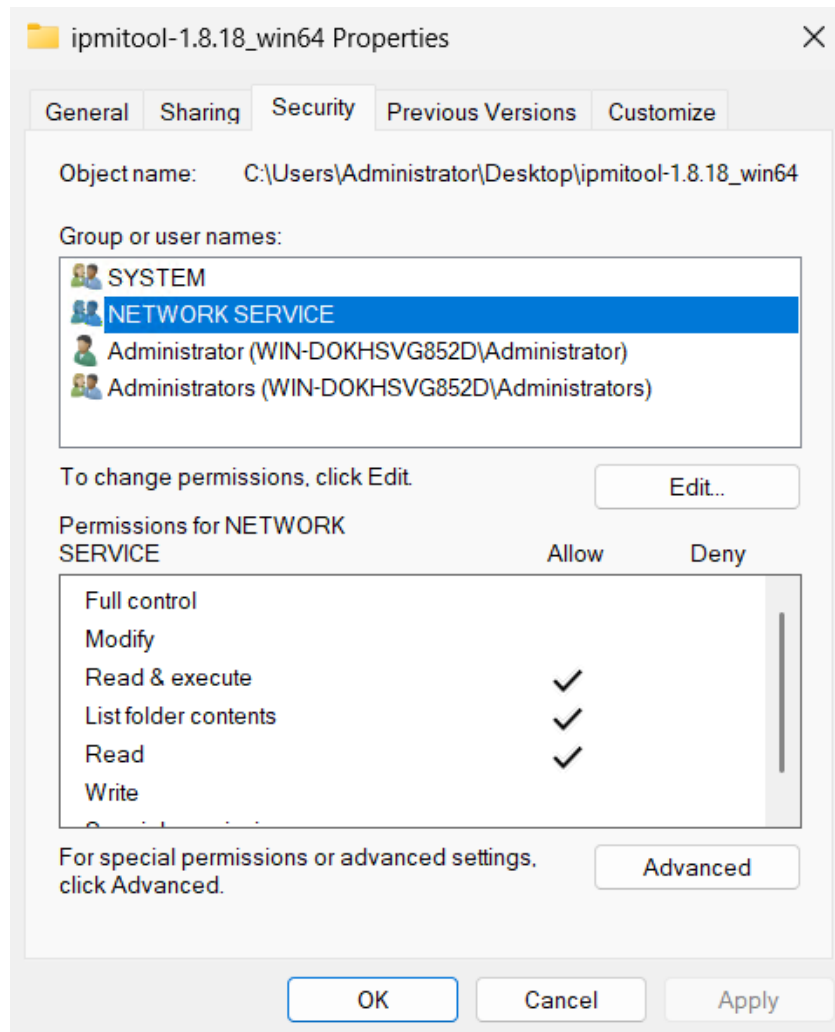
These are tools for troubleshooting Redfish, IPMI and SNMP issues.

Note:

1. To enable “IPMI Dump”, IPMITool should be installed on the AMI Data Center Manager server, with below configuration:
 - a. Modify \$installpath/conf/user.config.xml file, add entry for IPMITOOL_ABSOLUTE_PATH.
Example below:
 - Windows:


```
<entry key="IPMITOOL_ABSOLUTE_PATH"> C:/Home/ipmitool/ipmitool.exe</entry>
```
 - Linux:


```
<entry key="IPMITOOL_ABSOLUTE_PATH"> /usr/bin/ipmitool</entry>
```
 - b. Create NETWORK SERVICE permission on ipmitool folder (Windows only):



c. Restart DCM services

2. For SNMP walk, user must provide OID. For eg., OID can be as .1

3.7 Events

The **Events** and **Thresholds** tabs show the predefined events or custom events for DC management and all entity thresholds.

Note:






There are different **Events** tabs in AMI DCM Console:

- The **Events** page lists all the predefined events and custom events.
- The **Events** tab on the **Dashboard** page only lists the critical events and custom events.
- The **Events** tab in the **Hierarchy** page lists all the events applying to the specific group or device.

- The **Events** tab in the **Groups** page lists all the events applying to the specific group.

You can specify an e-mail address by clicking **E-mail Subscription** tab on the **Settings** page to receive messages through email when an event is triggered.

Click **Events** on left side of the interface to get the **Events** lists which can be filtered by time, severity level (defined below), Entity, Event Type, Description, or Serial Number.

Severity Level	Icon	Description
Custom		Associated with all custom events.
Critical		Errors that may cause DCM to stop working properly.
Error		Errors on specific nodes, or non-critical errors in AMI DCM.
Warning		An error may soon occur.
Informative		Events that do not report errors.

Customization option of severity for components health events

DCM uses the "*conf/eventSeverityMapping.csv*" file, located in the installation directory, to customize the severity of component fault events. The CSV file is structured with six columns, using commas to separate values, so commas should not be present within column content.

CSV Column Definitions:

Component Name:

Lists all supported components. The same component name can appear multiple times in the CSV.

Possible Values:

- ✓ BATTERY
- ✓ STORAGE
- ✓ ETHERNET_INTERFACE
- ✓ EVENT_SERVICE
- ✓ FAN
- ✓ FIRMWARE
- ✓ LOG_SERVICE
- ✓ MANAGEMENT_PORT
- ✓ MANAGER
- ✓ MEMORY
- ✓ NIC
- ✓ PCIE_DEVICE

- ✓ POWER_SUPPLY
- ✓ PROCESSOR
- ✓ STORAGE_CONTROLLER
- ✓ SWITCH
- ✓ SYSTEM
- ✓ TEMPERATURE
- ✓ VOLTAGE
- ✓ VOLUME

Device Model:

A regular expression to restrict the target device model name (as displayed in the DCM console device table) to which the rule should be applied.

Source Error Severity:

The severity string displayed in the target device's Redfish "Health" property.

Source Error Description:

Currently not used.

User Defined Severity:

The event severity displayed on the DCM console event page/widget. It should be one of the predefined values: "Critical", "Error", "Warning", or "Informative".

Enabled:

Indicates whether this rule is enabled. All existing rules are set to "FALSE" by default.

Note: Multiple rules with the same **Component Name** but different **Device Model** or **Source Error Severity** can coexist. When a component fault event is generated in DCM, all enabled rules are examined, and the first matching rule will take effect.

Exporting Events

- Click **"Export raw data"** to export the event data. The result is impacted by the filter applied.
- Click **"Export health report"** to export health report.

Acknowledging Events

Events can be acknowledged so that any new events of the same type, device, and description, don't appear again in the "Events" table.

To acknowledge events, select one or more events, click the "Acknowledge" button, and add notes if necessary, and then click "OK".

The acknowledged events can be found below the "Events" table. You can modify their notes by clicking the "Edit Notes" button. The events in this table can be filtered in the same way as in "Events" table.

The acknowledged events can be removed by clicking “Unacknowledge” in the “Acknowledged Events” table.

Deleting Events

AMI DCM Console automatically deletes old events if there are more than 20,000 events listed. You can also delete events manually.

To delete events:

- Go to the **Events** page.
- Select the check boxes.
- Click **Delete**.
- Click **OK**.

To delete all events:

- Go to the **Events** page.
- Click **Delete All**.

Thresholds

All thresholds are presented in a table and can be edited there. However, AMI DCM Console would not validate the input when you modify a threshold in the table as If you configure a power or temperature threshold on a group or device, and the "Condition" is met, custom events will be triggered. Here is an example on how to set a power threshold:

- Got to **Thresholds** tab and click '+'
- Select To single entity in hierarchy
- Pick an entity in the hierarchy
- Set IT Equipment Power as Threshold Type
- Choose the right value for **Condition**
- Enter the value of Threshold, and then click **OK**.

Once the power draw of the entity exceeds above the threshold you configured, an event will be triggered and listed in the **Summary** tab. You can check the details by hovering your mouse on **Description**.

You can also set threshold for multiple racks, rows or rooms at one time. Choose **Selection** as **To racks**, **To rows** or **To rooms**, and then select multiple racks, rows, or rooms to set the threshold.

3.8 GPUs

GPU List

All GPUs monitored by DCM are listed in the table. Unhealthy GPU components are indicated for each GPU.

When you hover over a warning icon, a detailed error message reported by the GPU is displayed.

You can select specific GPUs from the list and schedule management tasks, such as the following:

Add GPU Management Task
✕

Task Name:

Task Type:

Schedule: Now Specific Time Recurrent

Below task types are supported at the moment:

- Enable ECC
Enable GPU ECC mode.
- Disable ECC
Disable GPU ECC mode.
- Diagnose
Diagnose GPU.
- Reset
Reset GPU.
- Set application clocks
Set GPU application memory clock and graphics clock.
- Reset clocks
Reset GPU application memory clock and graphics clock to default value.
- Limit power
Set GPU power limit.

After adding a GPU management task, it will be displayed in the GPU Task tab page.

Note: Only licensed GPUs can be selected in the table. To monitor GPUs via in-band SSH channel, inband information needs to be specified in server properties.

GPU Task

This tab shows the status of all of GPU tasks. You can check the result of tasks, re-run, stop and delete a task.

3.9 Settings

User Management

In the **User Management** tab, you can create, edit, or delete users.

- **Administrator** has full access to the account and can manage devices, hierarchy, energy, reliability, event, settings, etc.
- **Power User** has similar permissions to an Administrator but cannot create, modify or remove the user account, power policy or power status.
- **Guest User** can only view information.

Tenant Users are designed for multi-tenant scenarios. They can manage devices and groups that belong to them but have limited management features.

- **Create User:** Initiates the process to create a new user account.

- Edit: Enables modification of a user's details.
- Delete: Permanently removes a user account.

AMI DCM Console supports Microsoft Active Directory user and group. You may assign a role for a Microsoft Active Directory user or group, and then login to AMI DCM Console with that account. You need to specify domain name and credentials to access the Active Directory server.

Note:

AMI DCM Console server communicates with Active Directory servers using the Transport Layer Security (TLS) channel which requires AD server certificate verification by default. Before adding an AD user or group to AMI DCM Console, import the AD server certificate into the keystore by following these steps:

- Get the AD server certificate or CA certificate from AD server admin.
- Run this command to import the certificate into keystore:

```
[Installation folder]/external/jre/bin/keytool -import --trustcacerts --alias  
adcert --file <certificate_file> --keystore "[Installation  
folder]/keystore.ssl"
```

Note:

If you want to disable secure transportation with AD server, you may change the 'conf/console.config.xml' file in AMI DCM Console installation folder. Add two entries: '<entry key="ENABLE_AD_TLS">False</entry>' and '<entry key="AD_PORT">389</entry>', save the file and then restart DCM services. It is highly recommended that you make this change only in a fully trusted network environment as the user credentials will be sent to the AD server in plain text.

AMI DCM Console also supports LDAP authentication. To enable LDAP authentication, you need to specify the correct LDAP configuration in **LDAP** tab under **Settings** page before adding an LDAP user.

AMI DCM Console tracks user operations for auditing purpose. The time, account, and action for user operations are logged in "action.log" file under "log" folder. Access to this file requires administrator or root privilege.

Passwords

This section allows you to update your password:

- Go to **User Management** tab in **Settings** page.
- Enter your old password.
- Enter the new password.
- Reenter the new password to ensure it matches.
- Click **Save**.

SNMP Traps

SNMP Traps allows you to assign a recipient to receive triggered events, which makes it easier to manage the events in 3rd-party event management systems. DCM events are defined in the Management Information Base (MIB) file which is installed at "<installation path>\ami\dcmlconf\DCMConsole-MIB-V1.mib".

You can refer to the DCM MIB file to configure or write your own SNMP receiver:

- If you are concerned about the events in alertCustomEventType, please listen to alertNotification and alertNotificationReturnNormal specific traps.
- If you are concerned about the events in alertPredefinedEventType, please listen to alertPredefinedEvent specific trap.
- In the threshold-based events, only the events of CarbonEmission and CarbonEmissionProjection belong to alertPredefinedEventType (others to alertCustomEventType), so please listen to alertPredefinedEvent trap for these two events.
- For the internal data structure and OID definition of each specific trap, please refer to the definition in DCM MIB.
- For SNMP traps OID mapping, please refer to Appendix A

To add a trap receiver:

- Go to the **SNMP Trap** tab in **Settings** page.
- Click Add Receiver.
- Fill in the Destination IP/Host, Port, and Community Name.
- Click **OK**.

To edit/delete/test a trap receiver:

- Go to the **SNMP Trap** tab in **Settings** page.
- Click **Edit/Delete/Test** in the **Action** column.

Email Subscriptions

In the "**Email Subscriptions**" tab in **Settings** page, you can subscribe to get event alerts by email.

To subscribe to an event:

- To Add Subscription, click **Add** icon.
- Fill in email server configuration.
- Check Subscribe threshold-based events only for threshold-based event.
- Click **OK**.

To edit/delete/test a subscription:

- Click **Edit/Delete** in the Action column.

Emails can be grouped to avoid flooding:

- Go to Email Subscriptions section
- Click the configuration button
- Check **Enable Email Group** to enable email grouping. The Parameters that impact email groups are listed below:
- Group By: The field(s) by which the events are grouped. It can be "All", "Event Type" (default), or "Entity", or "Entity" + "Event Type", or "Entity" + "Event Type" + "Description".
- Group Wait: The time to wait before sending a notification for a group.
- Repeat Interval: The time between sending consecutive emails.

Predefined Events

All predefined events are integrated in one form which includes the Predefined Event Type and event Severity. You can select the predefined events you are interested in by checking the corresponding boxes and then click **Save**.

SEL Rules

In the **SEL Rules** tab, user can open the **Add SEL Matching Rule** or **Edit SEL Matching Rule** dialogs to define or modify SEL rules by providing a rule name and details. Enable the **Regular Expression** checkbox to use Java regex for matching; if disabled, the system performs an exact string match. When an event log message matches the defined rule, a RULE_MATCHED_SEL event is generated.

Note: For security reasons, DCM automatically encodes angle brackets (< and >) in input strings. If you enter these characters, they will be displayed as < and > respectively. This measure is implemented to protect against potential security vulnerabilities, such as Cross-Site Scripting (XSS) attacks. SEL entries that contain < or > will not be matched.

Power Profiles

All the power profiles are listed in the **Power Profile** tab in the **Settings** page.

- Click **Add** to add a new power profile.
- Click **Delete** to delete an existing power profile.
- Click **More** to edit the corresponding power profile.

LDAP

AMI DCM Console can support LDAP authentication if you specify correct LDAP configuration in the settings before adding an LDAP user. You may need to consult your LDAP administrator to get the configuration information for the settings.

Note: Only LDAP over TLS is supported.

Emergency Power Reduction

In case of an emergency such as a data center level power failure, Emergency Power Reduction (EPR) can be enabled to reduce the power usage of devices and prolong their service time.

You can specify or modify the emergency power reduction (EPR) by adding or editing the device. Different devices can be in different EPR states when a room is under emergency power reduction.

There are three actions to choose from the drop-down list: Minimize power consumption (default), Shut down and No action. Choose No action for very critical devices and Minimize power consumption or Shutdown for others.

Note: Applying EPR may significantly reduce device performance. Please use this function only in emergencies and check the EPR action carefully before applying it.

Enabling EPR

- Choose a data center or a room, and then click **Save**.
- Click **OK** to confirm in the popup dialog.
- All devices with power capping capability in this group are throttled to the state specified by the manager. Edit the devices to specify EPR action.
- An icon for EPR will appear on the top right of the page.
- Click the icon to check the device list in EPR.

Disabling EPR

- To disable emergency power reduction, uncheck the specified groups, and then click Save.
- Click **OK** to confirm in the popup dialog.

Custom Attributes

AMI DCM Console supports custom attributes that can be associated with devices. You can manage (add / edit / delete) the custom attributes in this section.

Sustainability

Power Usage Effectiveness: Specify the PUE (Total Facility Energy / IT Equipment Energy) to estimate metrics on the Temperature/Power page.

- **Carbon Emission Factor:** The default factor for estimating Carbon Emission and can be overridden by DC-specific Carbon Emission Factor.
- **Annual Carbon Emission Starting Month:** Select the starting month from which the Annual Carbon Emission will be counted.
- **Enable Carbon Emission Projection:** Carbon emission projection will be enabled only when this checkbox is checked.

Miscellaneous

You may configure the following options to your preferences:

- **Maximum Healthy Temperature:** It will affect the dashboard color (blue or orange). The recommended value is 27 °C. And this setting will not impact the temperature-based thresholds.
- **Show Monitoring Status of Devices in Visualized Rack:** Check this box to indicate servers that are not monitored with an orange dot in the Datacenter Manager visualized rack.
- **Temperature Unit:** Specify the unit of temperature measurement.
- **Weight Unit:** Specify the unit of weight measurement.
- **Show advanced telemetry:** Enable advanced telemetry for some NM-enabled servers.
- **Receive SNMP Alerts:** Check this box to display SNMP alerts received from managed devices in the Reliability tab.
- **Email Health Alert to Device Vendor:** Check this box and provide SMTP server information to send health alert emails to device vendors (if their email is configured correctly for devices with health issues).

3.10 To integrate DCM Console in an iframe

DCM Console can be integrated in an iframe by another web application. Let's assume the URL of the DCM Console is `https://dcm-ip:8643/DcmConsole` and the URL of another web application is `https://app-ip:1234/myApp`.

The following integration steps should be followed:

- Add the following configuration to DCM Console configuration file(`console.config.xml`) then restart DCM service

```
<entry key="IFRAME_PARENT_URL_LIST">https://app-ip:1234</entry>
```

- Post login message with JSON format to the iframe content window with DCM Console

The message format is following:

```
{
  "action": "login",
  "user": string,
  "psw": string,
  "account": integer, //0--console user, 1--AD user,2--LDAP user
  "domain": string
}
```

Sample:

```
var msgObj = {action:"login", user: user, psw: psw, account: account,
domain: domain};
msg = JSON.stringify(msgObj);
document.getElementById("iframe").contentWindow.postMessage(msg, "*");
```

- Receive login result message

The host web application can receive the login result message from DCM Console like following example code:

```
if (typeof window.addEventListener != 'undefined') {
  window.addEventListener('message', onIframeMessage, false);
} else if(typeof window.attachEvent != 'undefined') {
  window.attachEvent('onmessage', onIframeMessage);
}

onIframeMessage = function(e) {
  var cmd = JSON.parse(e.data);
  if(cmd.action == 'login_result'){
    if(cmd.result_code != 0) {
      alert(cmd.result_desc);
    }else{
      //Show the iframe
    }
  }
};
```

- The login result message format is following:

```
{  
    "action": "login_result",  
    "result_code": string, // Same as DCM login API  
    "result_desc": string // Same as DCM login API  
}
```

Page Links:

The following links can be specified as the iframe source:

Dashboard(Title bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dcmconsole/dashboard>

Dashboard (Title bar and navigation bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dashboard>

Hierarchy(Title bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dcmconsole/hierarchy>

Devices(Title bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dcmconsole/devices>

Sustainability(Title bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dcmconsole/sustainability>

Reliability(Title bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dcmconsole/health>

Events(Title bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dcmconsole/events>

Report(Title bar will be hidden)

<https://dcm-ip:8643/DcmConsole/#/dcmconsole/report>

Note:

Tenant user is not supported.

A CA-signed certificate is required when deploying the DCM service to prevent the iframe from being blocked. If using a self-signed certificate, then users must access full DCM console to accept it.

3.11 RESTful APIs

Starting from version 3.6, AMI DCM Console provides RESTful APIs to facilitate automation and integration.

Please refer to DCM_RESTful_API.pdf file in the /doc folder for more details.

3.12 Ansible Modules

Starting from version 3.8, AMI DCM Console starts to provide Ansible Modules for automation. Refer to “ansible” folder for Ansible modules, document, and sample playbooks.

3.13 Page Links

Starting from version 4.1, AMI DCM Console provides the following page links to facilitate integration.

Dashboard

<https://localhost:8643/DcmConsole/#/dcmconsole/dashboard>

Hierarchy

<https://localhost:8643/DcmConsole/#/dcmconsole/hierarchy>

Hierarchy for Certain Specified Entity

<https://localhost:8643/DcmConsole/#/dcmconsole/hierarchy/goto/EntityId>

All Device List

<https://localhost:8643/DcmConsole/#/dcmconsole/devices>

Events

<https://localhost:8643/DcmConsole/#/dcmconsole/events>

Reports

<https://localhost:8643/DcmConsole/#/dcmconsole/report>

3.14 Command Line Tool

AMI DCM Console provides a command line tool to manage hierarchies which should be run on the same server where AMI DCM Console was installed. You can find the corresponding executable hman.bat (for Windows) and hman.sh (for Linux) in DCM bin folder. Please make sure that no EPR (Emergency Power Reduction) is enabled when you are using the command line tool.

Six commands are supported:

add, delete, update, list, move, and help.

For each command, there should be command options and command target.

help

command target: add, delete, update, list, and move. Help command shows the usage of the commands. The tool shows the usages of all the commands if the command target is not specified.

add

command options:

- hierarchylevel (data center, room, row, rack, device, blade)
- name
- description
- capacity (for rack only)
- powercapacity (for rack only)
- pdupowerasrackpower (for rack only)
- type (refer to the table in Importing Devices for possible types)
- address
- username
- password (password id string which cannot contain “:.”)
- snmpcommunitystring
- snmpencryptionpassword (password id string which cannot contain “:.”)
- snmpauthenticationprotocol
- snmpencryptionprotocol
- httpsport
- sshport
- distinguishedname
- key
- deratedpower
- size
- location
- authenticateentity
- model
- ostype
- osaddress
- osusername
- ospassword (password id string which cannot contain “:.”)
- typicalpower
- idlepower
- peakpower
- gridx
- gridy
- passwordfile (a file contains passwordid:password pair)

command target: full path name (Unix like full path name style, e.g., /dc1/room1/row1/rack1/) to which end user wants to add a new entity. If the command target is not specified for the add command, root (/) would be used by default.

delete

command target: full path name of the entity to be deleted.

update

command options:

- name
- description
- capacity
- powercapacity
- pdupowerasrackpower
- address
- username
- password (password id string which cannot contain “:”)
- snmpcommunitystring
- snmpencryptionpassword (password id string which cannot contain “:”)
- snmpauthenticationprotocol
- snmpencryptionprotocol
- httpsport
- sshport
- distinguishedname
- key
- deratedpower
- size
- location
- authenticateentity
- model
- ostype
- osaddress
- osusername
- ospassword (password id string which cannot contain “:”)
- typicalpower
- idlepower

- peakpower
- gridx
- gridy
- passwordfile (a file contains passwordid:password pair)

command target: full path name of the entity to be updated.

Examples (with below sample content in password file "dcmpassfile"):

mypassword_id1:6VAsH3Fa

mypassword_id2:iOLZh9yw

mypassword_id3:E6D1bAZQ

1. Set up hierarchy, create hierarchy "/DC9 SHANGHAI/Real Lab/Row/TmpRack"

```
C:\Program Files\ami\dcm\bin>hman.bat add -hierarchylevel dc -name "DC 9 SHANGHAI"
```

```
C:\Program Files\ami\dcm\bin>hman.bat add -hierarchylevel room -name "Real Lab" "/DC 9 SHANGHAI"
```

```
C:\Program Files\ami\dcm\bin>hman.bat add -hierarchylevel row -name "Row" "/DC 9 SHANGHAI/Real Lab"
```

```
C:\Program Files\ami\dcm\bin>hman.bat add -hierarchylevel rack -name "TmpRack" "/DC 9 SHANGHAI/Real Lab/Row"
```

2. Add an HP iLO rack server to a rack

```
C:\Program Files\ami\dcm\bin>hman.bat add -hierarchylevel device -name "My iLO" -type IPMI -address 192.168.0.1 -username myname -passwordfile "c:\dcmpassfile" -password mypassword_id1 "/DC9 SHANGHAI/Real Lab/Row/TmpRack"
```

3. Add an HP enclosure to DCM to a rack

```
C:\Program Files\ami\dcm\bin>hman.bat add -hierarchylevel device -name "My Enclosure" -type SSH -address 192.168.0.2 -username myname -passwordfile "c:\dcmpassfile" -password mypassword_id2 "/DC9 SHANGHAI/Real Lab/Row/TmpRack"
```

4. Add an HP blade to an Enclosure ("My Enclosure")

```
C:\Program Files\ami\dcm\bin>hman.bat add -hierarchylevel blade -name "My iLO blade to enclosure" -type IPMI -address 192.168.0.1 -username myusername -passwordfile "c:\dcmpassfile" -password mypassword_id3 "/DC9 SHANGHAI/Real Lab/Row/TmpRack/My Enclosure"
```

list

command target: full path name of the entity to be listed. The command lists all direct children of the command target. If the command target is not specified for the “list” command, root (/) would be used by default.

move

command target: the command takes two arguments, source, and destination. “Source” means the full path of an existing entity, while “Destination” refers to the full path to specify where to move ‘source’. You need to follow the rule of the hierarchy to move an entity.

Chapter 4

4 Working In a Scaled Environment

When working in a scaled environment (e.g., up to 60,000 devices), AMI DCM Console demands more resources to accomplish tasks. Below are the steps to enable those additional resources.

For **Linux** (recommended):

1. Increase the maximum number of open file descriptors, from default value (ULIMIT=20000) to (ULIMIT=150000) in below file:

```
/opt/ami/dcm/dcm_env
```

2. Change JVM heap size:

find string DCMXmsString="-Xms256m" and change to DCMXmsString="-Xms32768m", find string DCMXmxString="-Xmx8192m" and change to DCMXmxString="-Xmx65536m" in below file:

```
/opt/ami/dcm/dcm_env
```

find string TomcatXmsString="-Xms256m" and change to TomcatXmsString="-Xms512m", find string TomcatXmxString="-Xmx2048m" and change to TomcatXmxString="-Xmx12288m" in below file:

```
/opt/ami/dcm/dcm_env
```

3. Increase the "shared_buffers" from default value (128MB) to (2048MB) for postgresSQL database in postgresql.conf file under

```
/opt/ami/dcm/pgdata.
```

Ensure if the passive instance also reflects the same update after installation in High Availability mode.

4. Increase the health sampling interval to 1 hour: add <entry key="NODE_HEALTH_SAMPLING_FREQUENCY">3600</entry> in

```
/opt/ami/dcm/conf/user.config.xml.
```

5. Update the NiPluginConfig.xml(/opt/ami/dcm/bin/plugins) file content as below

```
<?xml version="1.0" encoding="utf-8"?>
<NiPluginConfig>
  <HttpLibSendThreadNum value='16' />
  <HttpLibReceiveThreadNum value='64' />
  <ShareThreadPool value='false' />
  <HttpLibConnectionLimit value='60000' />
</NiPluginConfig>
```

```
<HttpLibAuthConnectionLimit value='60000' />
<HttpLibMaxConnectionPerNode value='1' />
<HttpLibMaxAuthConnectionPerNode value='1' />
<HttpLibMaxSendQueueSize value='70000' />
<HttpLibMaxRecvQueueSize value='70000' />
<DefaultConnectionTimeout value='5' />
</NiPluginConfig>
```

6. Verify whether the `contrackd` package is installed. If not, install the `contrackd` package to apply the configuration changes for `contrackd`.

To Verify:

Linux:

```
dpkg -l | grep contrackd
```

Redhat:

```
rpm -qa | grep contrack-tools
```

The above command will display information about the installed `contrackd` packages.

Ensure if the passive instance also reflects the same update after installation in High Availability mode.

7. The default `nf_contrack` table size is 65536 on host where memory is larger than 4G. It is recommended to change this value to 262144.

```
####Verified on SUSE15/Ubuntu22####
```

- create file `/etc/modprobe.d/contrack.conf`
- add line "options `nf_contrack` hashsize=262144" into `contrack.conf`
- reboot server
- After startup, check `/proc/sys/net/netfilter/nf_contrack_buckets` content equals 262144

Reference: https://www.kernel.org/doc/Documentation/networking/nf_contrack-sysctl.txt

Ensure if the passive instance also reflects the same update after installation in High Availability mode.

8. For both IPv4 and IPv6, the default table sizes are typically set to 1024, which might be insufficient for large subnetworks. It is recommended to increase this value according to the size of subnetwork and change local port range to [1024, 65535].

```
####Verified on SUSE15/Ubuntu22####
```

- Create the file if it does not exist, and then edit `/etc/sysctl.conf`
- Add line " `net.ipv4.ip_local_port_range = 1024 65535`
`net.ipv4.neigh.default.gc_thresh1 = 65536`
`net.ipv4.neigh.default.gc_thresh2 = 65536`
`net.ipv4.neigh.default.gc_thresh3 = 65536`
`net.ipv6.neigh.default.gc_thresh1 = 65536`
`net.ipv6.neigh.default.gc_thresh2 = 65536`
`net.ipv6.neigh.default.gc_thresh3 = 65536`
`net.core.netdev_budget = 800`
`net.core.netdev_budget_usecs = 40000`" into `sysctl.conf`

- Run command `"sysctl -p"`

Ensure if the passive instance also reflects the same update after installation in High Availability mode.

9. To ensure proper functioning of the AMI DCM Console in scaled environment, it is essential to update the "max_wal_size" from default value (1G) to (10G) in the postgresql.conf file located under /opt/ami/dcm/pgdata then restart DCM services to take effect.

Ensure if the passive instance also reflects the same update after installation in High Availability mode.

Chapter 5

5 Renewing Passwords / Keys / Certificates

As a maintenance effort, password / key / certificate used in AMI DCM Console may require update on a regular basis. Please make sure the installed services are stopped before updating them.

For Windows: Stop “DatacenterManagerServer” and “DatacenterManager” service

For Linux: Run command “./startdcm.sh stopjsvc” to stop service

5.1 Renewing the Database Password

The database super user name is available as entry DB_SUPER_USER_NAME in conf\superUser.config.xml:

```
<entry key="DB_SUPER_USER_NAME">dcmdba</entry>
```

Follow the steps below to renew the database super user password.

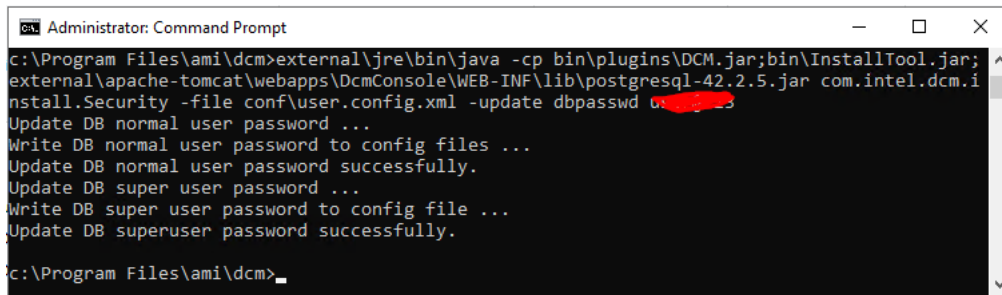
For Windows (in DCM installation folder):

```
external\jre\bin\java ^
-cp bin\plugins\DCM.jar^
;bin\InstallTool.jar^
;external\apache-tomcat\webapps\DcmConsole\WEB-INF\lib\postgresql-42.7.2.jar
^
com.intel.dcm.install.Security ^
-file conf\user.config.xml ^
-update dbpasswd yourpassword
```

For Linux (in DCM installation folder):

```
external/jre/bin/java \
-cp bin/plugins/Dcm.jar\
:bin/InstallTool.jar\
:external/apache-tomcat/webapps/DcmConsole/WEB-INF/lib/postgresql-42.7.2.jar
\
com.intel.dcm.install.Security \
-file conf/user.config.xml \
-update dbpasswd yourpassword
```

This command will also update database normal user with a random password and related config files (conf/user.config.xml, conf/console.config.xml and conf\ superUser.config.xml).



```

Administrator: Command Prompt
c:\Program Files\ami\dcm>external\jre\bin\java -cp bin\plugins\DCM.jar;bin\InstallTool.jar;
external\apache-tomcat\webapps\DcmConsole\WEB-INF\lib\postgresql-42.2.5.jar com.intel.dcm.i
ninstall.Security -file conf\user.config.xml -update dbpasswd u...
Update DB normal user password ...
Write DB normal user password to config files ...
Update DB normal user password successfully.
Update DB super user password ...
Write DB super user password to config file ...
Update DB superuser password successfully.
c:\Program Files\ami\dcm>
  
```

Figure 36 Command

5.2 Renewing the Keystore Password

Follow below steps to renew keystore password.

1. Renew keystore password.

Follow the instructions [here](#).

AMI DCM Console requires IDENTICAL passwords to protect both keystore and private key.

Refer to this link on how to renew keystore password (using “keytool –storepasswd” command) that is used for protecting keystore file. The private key password is also updated when keystore password is updated.

Alias associated to AMI DCM Console private key is datacentermanager.

The keystore file used by AMI DCM Console is keystore.ssl located under the installed folder.

Keytool is located under \external\jre\bin.

Note: Please run this Keytool command with root user permission.

2. Synchronize new password into AMI DCM Console configuration file.

For Windows (in DCM installation folder):

```

external\jre\bin\java ^
-cp bin\plugins\DCM.jar^
;bin\InstallTool.jar^
;external\apache-tomcat\webapps\DcmConsole\WEB-INF\lib\postgresql-42.7.2.jar
^
com.intel.dcm.install.Security ^
-file conf\user.config.xml ^
-update keystorepasswd yourpassword
  
```

For Linux (in DCM installation folder):

```

external/jre/bin/java \
-cp bin/plugins/Dcm.jar\
:bin/InstallTool.jar\
  
```



```
:external/apache-tomcat/webapps/DcmConsole/WEB-INF/lib/postgresql-42.7.2.jar
\
com.intel.dcm.install.Security \
-file conf/user.config.xml \
-update keystorepasswd yourpassword
```

This command will update both conf\user.config.xml and conf\console.config.xml.

3. Synchronize new password into Tomcat configuration file.

Please refer to [Tomcat document](#).

The Tomcat configuration file used in AMI DCM Console is external\apache-tomcat\conf\server.xml.

5.3 Renewing Keys

Run the following commands to renew the keys used by AMI DCM Console.

For Windows (in DCM installation folder):

```
external\jre\bin\java ^
-cp bin\plugins\DCM.jar^
;bin\InstallTool.jar^
;external\apache-tomcat\webapps\DcmConsole\WEB-INF\lib\postgresql-42.7.2.jar
^
com.intel.dcm.install.Security ^
-update rootkey ^
-file conf\user.config.xml
```

```
external\jre\bin\java ^
-cp bin\plugins\DCM.jar^
;bin\InstallTool.jar^
;external\apache-tomcat\webapps\DcmConsole\WEB-INF\lib\postgresql-42.7.2.jar
^
com.intel.dcm.install.Security ^
-update dbpasswdkey ^
-file conf\user.config.xml
```

```
external\jre\bin\java ^
-cp bin\plugins\DCM.jar^
;bin\InstallTool.jar^
;external\apache-tomcat\webapps\DcmConsole\WEB-INF\lib\postgresql-42.7.2.jar
^
com.intel.dcm.install.Security ^
-update consolekeys ^
-file conf\console.config.xml
```

For Linux (in DCM installation folder):

```
external/jre/bin/java \
```

```
-cp bin/plugins/Dcm.jar\  
:bin/InstallTool.jar\  
:external/apache-tomcat/webapps/DcmConsole/WEB-INF/lib/postgresql-42.7.2.jar\  
\ com.intel.dcm.install.Security \  
-update rootkey \  
-file conf/user.config.xml
```

```
external/jre/bin/java \  
-cp bin/plugins/Dcm.jar\  
:bin/InstallTool.jar\  
:external/apache-tomcat/webapps/DcmConsole/WEB-INF/lib/postgresql-42.7.2.jar\  
\ com.intel.dcm.install.Security \  
-update dbpasswdkey \  
-file conf/user.config.xml
```

```
external/jre/bin/java \  
-cp bin/plugins/Dcm.jar\  
:bin/InstallTool.jar\  
:external/apache-tomcat/webapps/DcmConsole/WEB-INF/lib/postgresql-42.7.2.jar\  
\ com.intel.dcm.install.Security \  
-update consolekeys \  
-file conf/console.config.xml
```

5.4 Renewing Certificates

Follow the steps below to renew the self-signed certificate when necessary (e.g. after expiration).

1. Delete old certificate

```
keytool -delete -alias datacentermanager -keystore keystore.ssl  
You will be required to input keystore password.
```

```
Then verify the entry with "datacentermanager" alias is removed from  
keystore.ssl  
keytool -list -v -keystore keystore.ssl
```

2. Create new certificate

```
keytool -genkeypair -alias datacentermanager -keyalg RSA -keystore  
keystore.ssl -dname "CN=MYDN,OU=MYORG,O=MYCMPY,L=MYADDRESS,S=MYCITY,C=CN" -  
validity 365 -storetype pkcs12 -keysize 3072
```

```
Also, verify the entry with "datacentermanager" alias is inserted into  
keystore.ssl  
keytool -list -v -keystore keystore.ssl
```

5.5 Signing the AMI DCM Certificate with Certificate Authority (CA)

Follow the steps below to sign the self-signed certificate with a CA to prevent browser warnings about insecure connections.

1. First, please make sure that the self-signed certificate in the DCM keystore has a Common Name (CN) matching the DCM server hostname. Renew the certificate if necessary to correct the CN.
2. Create the Certificate Signing Request (CSR) for the self-signed certificate, alias “datacentermanager” in the DCM keystore by:

```
[dcm_home]/external/jre/bin/keytool -certreq --keystore  
[dcm_home]/keystore.ssl --alias datacentermanager -keyalg rsa -file dcm.csr
```

3. Send the CSR (i.e., the file dcm.csr created in the previous step) to CA for signing. Besides the reply to the CSR, you also need to get CA certificate chain.
4. Import all certificates in the CA certificate chain, starting from the Root CA certificate one by one. Here are the command examples. Please replace the certificate file names with the actual ones. The aliases in the commands can be any strings containing only English letters.

```
[dcm_home]/external/jre/bin/keytool -importcert -trustcacerts --keystore  
[dcm_home]/keystore.ssl -alias RootCA -file "rootca.crt"
```

```
[dcm_home]/external/jre/bin/keytool -importcert -trustcacerts --keystore  
[dcm_home]/keystore.ssl -alias IntermediateCA -file "intermediateca.crt"
```

5. Import the certificate reply. Here is the command example. Please replace the certificate file name with the actual one. The alias in the command MUST be “datacentermanager”.

```
[dcm_home]/external/jre/bin/keytool -importcert -trustcacerts --keystore  
keystore.ssl -alias datacentermanager -file dcm.cer
```

6. Restart DCM services.

- For Linux, run:

```
[dcm_home]/startdcm.sh restart
```

- For Windows, restart services “AMI Data Center Manager Server” and “AMI DCM” from the Windows Services control panel (services.msc) or by running the following commands:

```
net stop DatacenterManager  
net stop DatacenterManagerServer  
net start DatacenterManagerServer  
net start DatacenterManager
```

Please refer to this [documentation](#) for detailed information on the keytool command.

5.6 Renewing Database Keys (High Availability mode)

If the Passive instance is installed and the Recovery Key is configured in the Active instance, AMI DCM Console will be working under High Availability mode. In this case, you need to renew keys for database after renewing the Certificate.

For the Active Instance:

Run below commands to renew keys for database.

```
cd /opt/ami/dcm
external/jre/bin/keytool -importkeystore -srckeystore ./keystore.ssl -
destkeystore ./pgdata.ssl -deststoretype PKCS12 -alias datacentermanager -
srcstorepass {keystore password} -deststorepass {keystore password}
openssl pkcs12 -in ./pgdata.ssl -out ./privkey.pem -nodes -passin
pass:{keystore password}
openssl rsa -in ./privkey.pem -out {postgresql data path}/server.key
chown dcmdba {postgresql data path}/server.key
chmod 600 {postgresql data path}/server.key
openssl x509 -in ./privkey.pem -out {postgresql data path}/server.crt
chown dcmdba {postgresql data path}/server.crt
chmod 600 {postgresql data path}/server.crt

rm -rf ./pgdata.ssl
rm -rf ./privkey.pem
./startdcm.sh restart
```

For the Passive Instance:

Copy server.key and server.crt from Active instance to {postgresql data path}, then run below commands.

```
chown dcmdba {postgresql data path}/server.crt
chmod 600 {postgresql data path}/server.crt
chown dcmdba {postgresql data path}/server.key
chmod 600 {postgresql data path}/server.key
./startdcm.sh restart
```

Chapter 6

6 Failover

When AMI DCM Console is working in High Availability mode, if the Active instance fails, the Passive instance can be manually promoted to become the new Active instance using the following commands. After that, a new Passive instance can be created, and its details and key are added in the new Active instance, and data replication continues as before.

```
cd /opt/ami/dcm
./ha_util.sh promote
```

Chapter 7

7 Data Streaming

- Data Streaming to Kafka is enabled by configuring DCM installed system as Kafka Producer Client with an existing Kafka broker.
- DCM collects and streams following data to user-configured Kafka periodically in Avro format.
 - Power
 - Temperature
 - Inventory
 - Device Health Status
 - Sensor Data Record (SDR)

7.1 Prerequisites

1. To enable Data streaming in DCM it is required to have:
 - a. Kafka Broker v3.6.x with SSL/Plaintext support
 - b. Confluent Schema Registry
2. Additionally, to enable SSL based data streaming, it requires:
 - a. SSL certificates for DCM system signed by Kafka broker
 - b. Kafka broker SSL Root certificate, Kafka broker trust store and DCM system's client keystore must be available under DCM_installation_folder/conf
 - c. File containing properties to establish SSL communication with broker must be placed under DCM_installation_folder/conf. This file may refer other files which should also be placed under DCM_installation_folder/conf.
 - d. For DCM (Linux), in addition to copying to conf location, group permission to be set as "chown root:dcm <DCM>/conf/<file>"
 - e. The password fields in this file should be UTF-8 Base64 encoded strings.
3. A Topic must be created for each type of data – namely, power, temperature, inventory, deviceHealth and sdr.
4. In the case of using Consumer, Avro schema must be uploaded to schema registry. The schema files are available under DCM_installation_folder/conf/kafka_schema

7.2 Enable and Configure Data Streaming

- Navigate to DCM installation folder. Edit kafka.properties under DCM_installation_folder/conf and configure as mentioned in the table.
- The configuration does NOT need service restart.
- All extra configuration files configured in kafka.properties under DCM_installation_folder/conf
- **Note:** To disable Data streaming feature anytime, set 'kafka.streaming.enabled=false'
- **Note:** By default, the pushing of data to kafka for inventory is 24 hours, health is 30 mins and sensor is 1 hour. This can be modified by user, by editing the <dcm_install_location>/conf/user.config.xml by adding the following keys:
 - NODE_INVENTORY_PUSH_INTERVAL for inventory
 - NODE_HEALTH_PUSH_INTERVAL for health.
 - NODE_ALL_SENSORS_PUSH_INTERVAL for sdr

Example: <entry key="NODE_INVENTORY_PUSH_INTERVAL">180</entry>

- NODE_HEALTH_PUSH_INTERVAL should be equal or larger than the sampling interval and be the multiple of sampling interval. By default, sampling interval is 30 mins. Sampling interval can be set using NODE_HEALTH_SAMPLING_FREQUENCY.

Field	Description	Mandatory
kafka.streaming.enabled	It is used to enable/disable overall data streaming feature. By default, it is set to false . i.e data streaming is disabled. To enable, set it to true .	Yes
kafka.ssl.enabled	It is used to enable SSL support for streaming. This should be enabled only when Kafka broker and DCM (Kafka client) has SSL support configured. By default, it is set to false and uses plaintext based communication. To enable, set it to true .	Yes
kafka.producer.client.properties	This should be a path to a file containing Kafka producer configuration. The path should point to a file located in /conf folder under DCM installed path. This file might be necessary to provide SSL properties or extra Kafka producer configuration. It should contain only Kafka supported Producer Configs. The password fields must be UTF-8 Base64 encoded. If the configuration file references another file path, that file should also be located within the conf folder under DCM installed path. For Example: if the file contains a property pointing to the location of a truststore, the path should be within the conf directory under DCM installed path. ssl.truststore.location=</DCM_home/conf/truststore> For DCM (Linux), the files copied to <i>conf</i> folder should be owned by the group called "dcm".	Optional (Mandatory if ssl support is required)
kafka.bootstrap.servers	This is a list of Kafka bootstrap servers. It is comma separated in the format <i>kafka.bootstrap.servers=host1:port1,host2:port2</i>	Yes
kafka.bootstrap.registry.url	This is Confluent Schema Registry URL. HTTP/ HTTPS can be used.	Yes
kafka.schema.*.enabled	It is used to enable/disable data streaming for specified type of data after enabling overall data streaming feature. By default, it is set to false , i.e. none of the data is streamed. Based on need a specific data can be enabled/disabled streaming. When it is set to true , given data will be streamed to Kafka. <i>For example, if kafka.schema.power.enabled=true, IT equipment power data will be streamed to Kafka, otherwise it will not be streamed.</i>	Yes

kafka.schema.*.topic	Configure the user created topics for each type of data. <i>For example, if kafka.schema.power.topic=ami.dcm.power, then IT equipment power data will be streamed to ami.dcm.power Kafka topic.</i>	Yes
kafka.schema.sdr.sensors	Configure the names of specific sensors if needed. By default, "ALL" pushes data from all sensors to Kafka. Sensor names are case-sensitive. <i>For example, kafka.schema.sdr.sensors=ALOM_Link_P6,02-CPU 1</i>	Yes

7.3 Event Logs

- Events related to Data streaming could be viewed in DCM Console UI in Events page under Data Streaming event type.
- Logs can be checked in *DCM_installation_folder/logs/DatacenterManager.log*

7.4 Troubleshooting

- In case of any Data Streaming related error, contact AMI and send the log file *DCM_installation_folder/logs/DatacenterManager.log* for further evaluation.

8 Appendix A: SNMP Traps OID Mapping

The SNMP traps supported by DCM Console are listed as follows.

Trap	OID	Description
testTrap	1.3.6.1.4.1.343.2.122.2.2.0.2	This is a test trap.
alertPredefinedEvent	1.3.6.1.4.1.343.2.122.2.2.0.3	DCM predefined events. Please select predefined events you are interested in settings, for retrieving them from the SNMP trap. Some predefined events with alertPredefinedEventType>100 are not listed in the DCM Console setting, but they are always enabled for sending SNMP trap.
alertNotification	1.3.6.1.4.1.343.2.122.2.2.0.5	DCM threshold-based events notification. This is an edge-triggered event. It happens only when the value was changed from out-range to in-range of the condition.
alertNotificationReturnToNormal	1.3.6.1.4.1.343.2.122.2.2.0.6	DCM threshold-based events return to normal notification. This is an edge-triggered event. It happens only when the value was changed from in-range to out-range of the condition.

8.1 testTrap

Trap OID = 1.3.6.1.4.1.343.2.122.2.2.0.2

Field	OID	Type	Possible Values
alertDisplayMessage	1.3.6.1.4.1.343.2.122.2.1.8	OCTET STRING	The display message of event. It is a Unicode encoded string.

8.2 alertPredefinedEvent

Trap OID = 1.3.6.1.4.1.343.2.122.2.2.0.3

Field	OID	Type	Possible Values
alertEntityName	1.3.6.1.4.1.343.2.122.2.1.1	OCTET STRING	The name of the entity to which the event applies. It is a Unicode encoded string.

Field	OID	Type	Possible Values
alertEntityID	1.3.6.1.4.1.343.2.122.2.1.2	INTEGER	The ID of the entity to which the event applies.
alertPredefinedEvent Type	1.3.6.1.4.1.343.2.122.2.1.3	INTEGER	The predefined event types defined by DCM. ipmiPowerUnit(1), snmpPowerUnit(2), ipmiPowerSupply(3), ipmiProcessorThermalTrip(4), ipmiFan(5),

		<p>bmcSelReachingFullCapacity(6), bmcSelAtFullCapacity(7), entityPropertyChanged(8), communicationWithNodeFailed(9), communicationWithNodeRestored(10), insufficientNodePermission(11), controlPolicyCannotBeMaintained(12), cantSetNodeEvent(13), controlPolicyApplied(14), controlPolicyEnded(15), internalError(16), configurationChanged(17), hierarchyChanged(18), controlPolicyChanged(19), customEventChanged(20), eventEvaluationFailure(21), collectionStateChanged(22), importHierarchyCompleted(23), dbMaintenanceStarting(24), dbMaintenanceEnded(25), dbConnectionFailed(26), dbConnectionRestored(27), controlPolicyPriorityConflict(28), dcmServerConnectionFailed(29), dcmServerConnectionRestored(30), clockNotSynchronized(31), powerOnMachineFailed(32), powerOffMachineFailed(33), dcmServerConflict(34), criticalDataSynchronizationStarting(35), criticalDataSynchronizationEnded(36), notificationChanged(37), notification(38), setPolicyToEntityFailed(39), removePolicyFromEntityFailed(40), communicationWithEnclosureFailed(41), communicationWithEnclosureRestored(42), upsBadBattery(43), upsLowBattery(44), upsBadTemperature(45), upsBadInput(46), upsBadOutput(47), upsOverload(48), upsOnBypass(49), upsBadBypass(50), upsSHutdown(51), upsChargeFailure(52), upsFanFailure(53), upsCommunicationLost(54), entityWithDuplicationPlatformId(55), pduLowLoad(56), pduHighLoad(57), pduOverload(58), pduOutletOn(59), pduOutletOff(60), entityCapabilitiesChanged(61), pduOutletLowLoad(62), pduOutletHighLoad(63), pduOutletOverload(64), platformOperationFailed(65), ipmiTestEvent(66), cmcSnmpEvent(67), idracSnmpEvent(68), serverComponentHighTemperature(69), pduSensorEvent(70), coolingAnomaly(71), predictiveFanFailure(72), deviceComponentFault(73), snmpEvent(74), disconnectForPeriod(75), assetChanged(76), ruleMachedSEL(77), networkDevicePortDown(78), contactSensorAlarmed(79), kafkaConfigurationMissing(80),kafkaConfigurationInvalid(81),kafkaSchemaMissing(82), kafkaSchemaInvalid(83), kafkaPublishFailed(84), kafkaPublishCompleted(85),missingFacilityPower(86), facilityPowerRestored(87), devicesWithoutPowerMonitoring(102), discoverySkipped(103), archiveEventFail(104), newDeviceDiscovered(105), warrantyExpiration(106), passiveInstanceConnected(107),</p>
--	--	--

			passiveInstanceDisconnected(108), newFirmwareAvailable(109), newFirmwareDetectionFailed(110), carbonEmissionThresholdExceed(111), carbonEmissionProjectionThresholdExceed(112)
alertDisplayMessage	1.3.6.1.4.1.343.2.122.2.1.8	OCTET STRING	The display message of event. It is a Unicode encoded string.
alertEntityAddress	1.3.6.1.4.1.343.2.122.2.1.9	OCTET STRING	The address of the device.
alertEntityPath	1.3.6.1.4.1.343.2.122.2.1.10	OCTET STRING	The full path of the entity. It is a Unicode encoded string.

8.3 alertNotification

Trap OID = 1.3.6.1.4.1.343.2.122.2.2.0.5

Field	OID	Type	Possible Values
alertEntityName	1.3.6.1.4.1.343.2.122.2.1.1	OCTET STRING	The name of the entity to which the event applies. It is a Unicode encoded string.
alertEntityID	1.3.6.1.4.1.343.2.122.2.1.2	INTEGER	The ID of the entity to which the event applies.
alertCustomEventType	1.3.6.1.4.1.343.2.122.2.1.4	INTEGER	The custom event types defined by DCM. maxPower(1), avgPower(2), minPower(3), maxAvgPower(4), totalMaxPower(5), totalAvgPower(6), totalMinPower(7), minAvgPower(8), maxInletTemperature(9), avgInletTemperature(10), minInletTemperature(11), avgWattsPerDimension(12), avgCoolingPower(13), inletTemperatureSpan(14), totalAvgPowerCap(15), itEquipmentPower(16), cpuTemperature(17), memoryTemperature(18), pchTemperature(19), iohTemperature(20), outletTemperature(21), cpuThermalMargin(22), memoryThermalMargin(23), iohThermalMargin(24), humidity(25), portUtilization(26), gpuPwr(27), gpuMaxTemp(28), gpuAvgTemp(29), gpuMinTemp(30), dynamicPUE(31)
alertCondition	1.3.6.1.4.1.343.2.122.2.1.5	INTEGER	greater(1), less(2)
alertThreshold	1.3.6.1.4.1.343.2.122.2.1.6	INTEGER	Threshold value
alertCurrentValue	1.3.6.1.4.1.343.2.122.2.1.7	INTEGER	Current value
alertDisplayMessage	1.3.6.1.4.1.343.2.122.2.1.8	OCTET STRING	The display message of event. It is a Unicode encoded string.
alertEntityAddresses	1.3.6.1.4.1.343.2.122.2.1.9	OCTET STRING	The address of the device.

Field	OID	Type	Possible Values
alertEntityPath	1.3.6.1.4.1.343.2.122.2.1.10	OCTET STRING	The full path of the entity. It is a Unicode encoded string.

8.4 alertNotificationReturnToNormal

Trap OID = 1.3.6.1.4.1.343.2.122.2.2.0.6

Field	OID	Type	Possible Values
alertEntityName	1.3.6.1.4.1.343.2.122.2.1.1	OCTET STRING	The name of the entity to which the event applies. It is a Unicode encoded string.
alertEntityID	1.3.6.1.4.1.343.2.122.2.1.2	INTEGER	The ID of the entity to which the event applies.
alertCustomEventType	1.3.6.1.4.1.343.2.122.2.1.4	INTEGER	The custom event types defined by DCM. maxPower(1), avgPower(2), minPower(3), maxAvgPower(4), totalMaxPower(5), totalAvgPower(6), totalMinPower(7), minAvgPower(8), maxInletTemperature(9), avgInletTemperature(10), minInletTemperature(11), avgWattsPerDimension(12), avgCoolingPower(13), inletTemperatureSpan(14), totalAvgPowerCap(15), itEquipmentPower(16), cpuTemperature(17), memoryTemperature(18), pchTemperature(19), iohTemperature(20), outletTemperature(21), cpuThermalMargin(22), memoryThermalMargin(23), iohThermalMargin(24), humidity(25), portUtilization(26)
alertCondition	1.3.6.1.4.1.343.2.122.2.1.5	INTEGER	greater(1), less(2)
alertThreshold	1.3.6.1.4.1.343.2.122.2.1.6	INTEGER	Threshold value
alertCurrentValue	1.3.6.1.4.1.343.2.122.2.1.7	INTEGER	Current value
alertDisplayMessage	1.3.6.1.4.1.343.2.122.2.1.8	OCTET STRING	The display message of event. It is a Unicode encoded string.
alertEntityAddress	1.3.6.1.4.1.343.2.122.2.1.9	OCTET STRING	The address of the device.
alertEntityPath	1.3.6.1.4.1.343.2.122.2.1.10	OCTET STRING	The full path of the entity. It is a Unicode encoded string.

9 Glossary

BMC	Board Management Controller
DC	Data Center
DCM	Datacenter Manager
IPMI	Intelligent Platform Management Interface
NM	Intelligent Power Node Manager
PDU	Power Distribution Unit
PUE	Power Usage Effectiveness
RMI	Remote Method Invocation
RAM	Random Access Memory
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security
UI	User Interface
UPS	Uninterruptible Power Supply
UCS	Universal Character Set
WMI	Windows Management Instrumentation