Management Plug-in for SCOM

User's Guide

Revision 2.1.0

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision: 2.1.0
Release Date: September 6, 2024

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2024 Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Revision History

Date	Rev	Description
2020/12/30	2.0.0	1. Initial release for SCOM-Plugin 2.0 2. This release contains following new features Monitoring Functions: - Asset Info - Sensor Reading - Health Event Log - Maintenance Event Log Management Functions: - BMC Cold Reset - UID LED Control - Chassis Intrusion Reset/Status - Fan Mode Control
2024/09/06	2.1.0	1. Add support 14 generation platform 2. Add assertion and deassertion to the description of Health Event Log 3. Rename the FRU tab to Detail and update the content

Contents

1 Overview 6

1.1 New Features 6

1.2 Components 7

2 Prerequisites and Installation 8

2.1 Hardware Requirements 8

2.2 Software Requirements 8

2.3 Installing Management Plug-in for SCOM 8

2.4 Installing Supermicro Redfish Management Pack 9

3 Supermicro Redfish Connector Service 10

3.1 Supermicro Redfish Connector Architecture 10

3.2 Using Supermicro Redfish Connector 11

4 Using Management Plug-in 12

4.1 First-Time Use 12

4.2 Accessing Asset Management Dashboard 13

4.3 Creating a Credential 14

4.4 Adding a System to the Asset List 14

4.4.1 Single Search 14

4.4.2 Range Search 15

4.4.3 Viewing Search Results 16

4.5 Viewing the Details of the System 17

4.5.1 Detail 17

4.5.2 Component Information 17

4.5.3 Power Supply Summary 18

4.5.4 Sensor 18

4.5.5 Health Event Log 19

4.5.6 Maintenance Log 19

4.6 Management Functions 21

4.6.1 BMC Cold Reset 21

4.6.2 UID Locate 21

4.6.3 Chassis Intrusion Reset 22
4.6.4 Fan Mode 22
4.6.5 Deep 22
4.6.6 Launch BMC Web 22
Appendix A. Third-Party Software 24
Contacting Supermicro 25

1 Overview

Data centers use Microsoft SCOM as a single point of system management. The Management Plug-in for SCOM integrates with the current SCOM interface, providing extended capability of SCOM to monitor and manage Supermicro servers.

1.1 New Features

- Managing Supermicro Servers X10 DP platforms and later, with calling Redfish APIs through the plug-in on SCOM directly and operating independently from SSM.
- Monitoring and managing through the plug-in on the Operation Manager console:
  - Monitoring:
    - Asset Info
    - Sensor Reading
    - Health Event Log
    - Maintenance Event Log
  - Management:
    - BMC Cold Reset
    - UID LED Control
    - Chassis Intrusion Reset/Status
    - Fan Mode Control
- Reviewing the hardware information of the managed Supermicro servers through the plug-in's Dashboard View on the Operation Manager console.
- Configuring BMC settings through the link of BMC Web.
- Running the plug-in on the below Microsoft SCOM server:
  - SCOM 2019/2022
- Retrieving events in the Maintenance Event Log, when:
  - accessing the BMC currently in the account locked out mode.
  - accessing the BMC currently enabled system lockdown mode. In addition, retrieving events of system lockdown in the Maintenance Event Log is allowed when the function is enabled and disabled.

1.2 Components

The Management Plug-in for SCOM includes the following components:

- **Supermicro Redfish Connector Service**
  - A backend Windows service for Supermicro Redfish Management Pack to communicate with Supermicro Servers.
- **Supermicro Redfish Management Pack**
  - The extended capability of SCOM to monitor/manage Supermicro Servers

2 Prerequisites and Installation

2.1 Hardware Requirements

- Processor (minimal): 4-Core 2.66 GHz CPU
- Memory (minimal): 16GB
- Disk space (minimal): 20GB

2.2 Software Requirements

- Microsoft System Center Operation Manager 2019/2022

2.3 Installing Management Plug-in for SCOM

1. This software must be installed on a Management Server (MS) in SCOM resource pool.
2. Log in the managed server as the administrator.
3. Run **Supermicro_SCOM_Management_Plug-in_<VER>_build.<BUILD>_Installer.exe** with the administrator privilege to start the installation.
4. Click the **Browse** button to select the destination folder, and then click the **Install** button to continue.

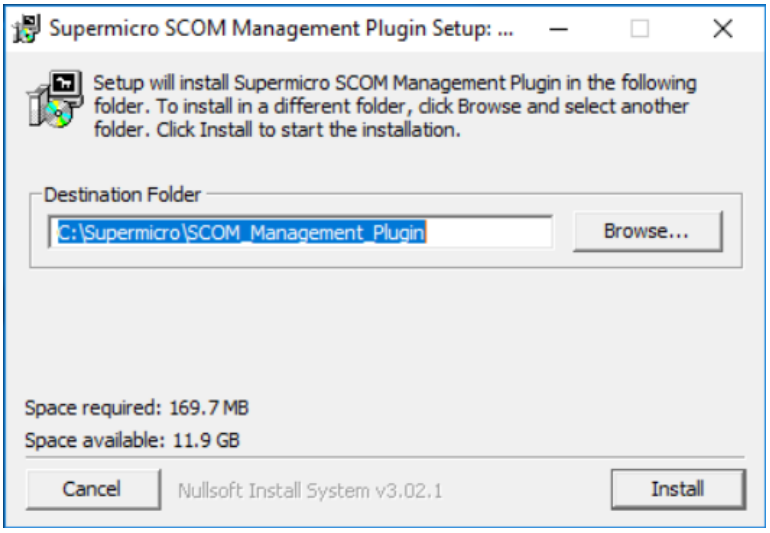


Figure 2- 1

5. After the installation is completed, click the **Close** button to finish.
6. Open Windows Services Manager, and check if Supermicro Redfish Connector is running.

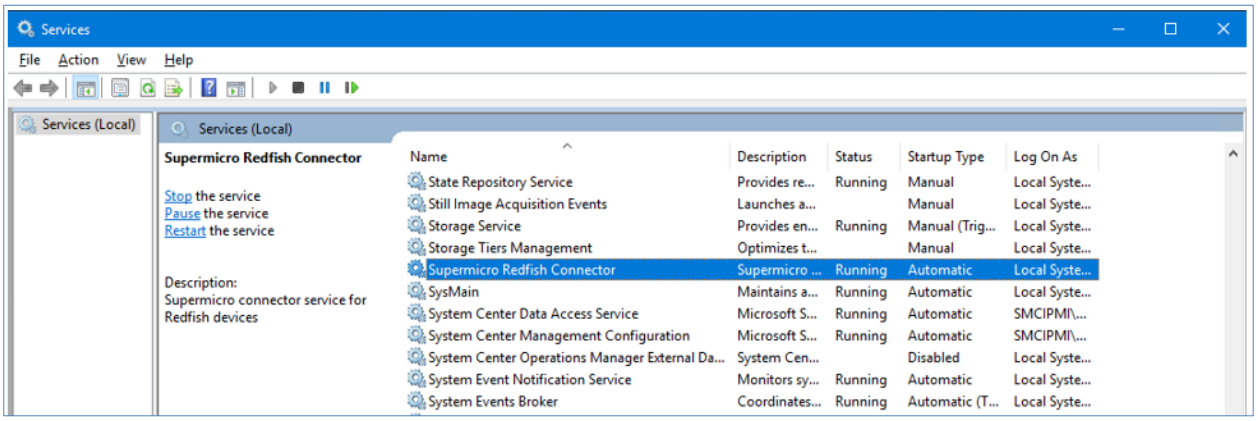


Figure 2- 2

2.4 Installing Supermicro Redfish Management Pack

The installer does not automatically import management packs into SCOM, and the management packs are available at **installation-folder**\MPs. Follow these steps to start the installation.

1. Find the management pack file **Supermicro_SCOM_REDFISH_ManagementPack_<VERSION>.mpb** and import it into SCOM Management Packs.

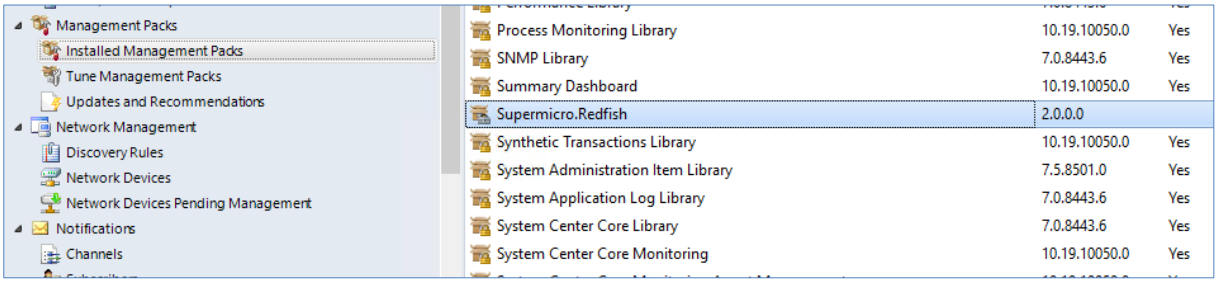


Figure 2- 3

2. You will find the Asset Management program under the Supermicro Plug-in folder in **Monitoring** dashboard.

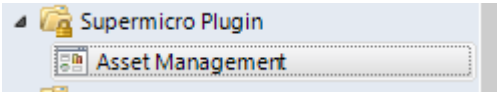


Figure 2- 4

3 Supermicro Redfish Connector Service

Supermicro Redfish Connector is windows-based service, providing backend service for Supermicro Redfish Management Pack to communicate with BMC of Supermicro Servers via Redfish API.

You can find the Supermicro Redfish Connector service in Windows Services Manager.

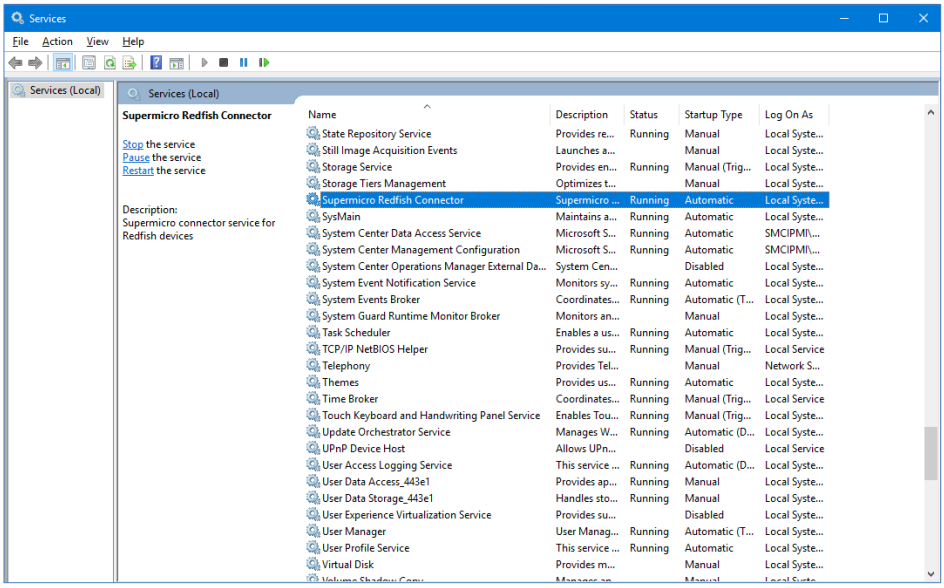


Figure 3- 1

3.1 Supermicro Redfish Connector Architecture

The figure shows how the Supermicro Redfish Connector service interacts with the related components.

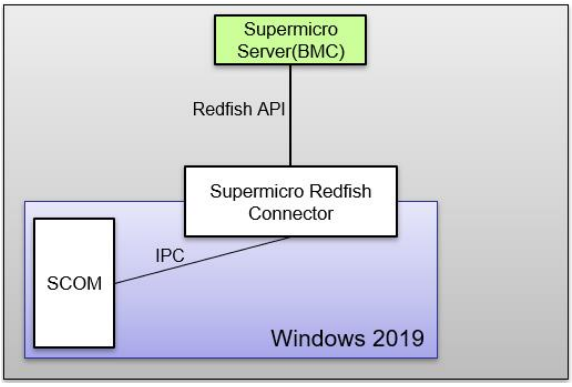


Figure 3- 2

3.2 Using Supermicro Redfish Connector

In order to communicate with BMC of Supermicro Servers, BMC credentials are needed for logging to Supermicro Servers. The credentials are stored in the Windows Credential Manager of the account (Local System by default). You can change the default logon user by following steps:

Note: Please keep your login account secure. The elevated user will be able to access Windows Credential Manager.

1. Open Windows Services Manager.
2. Select **Supermicro Redfish Connector**, right-click it and select **Properties**.
3. Select the **Log On** tab.
4. Select **This account**, input the account and password, and then click **Apply**.
5. Close the Operation Manager console
6. Restart the Supermicro Redfish Connector in order for the new setting to take effect.

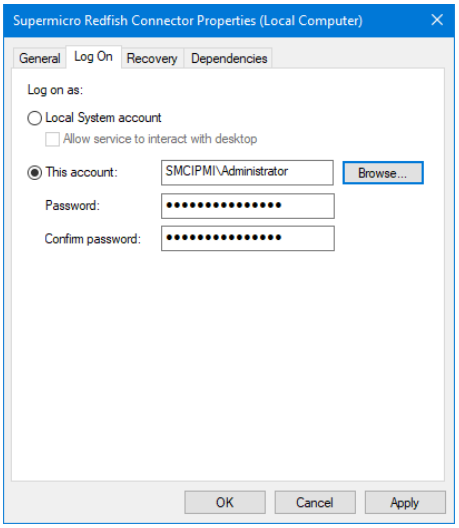


Figure 3- 3

4 Using Management Plug-in

4.1 First-Time Use

The Asset Management Dashboard is a WPF user control and in Html format. Because of the enhanced security of Internet Explorer in Windows Server, a warning dialog box may appear when you access the Management Plug-in for the first time.

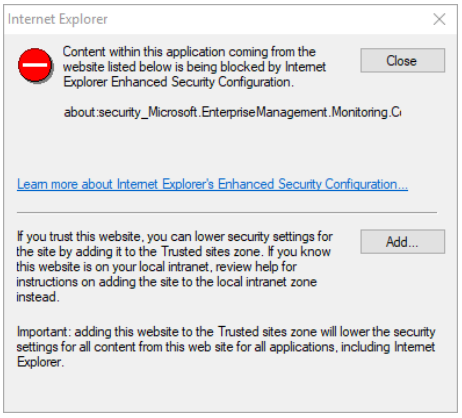


Figure 4- 1

Click the **Add** button to add it to the trusted zone and restart the Operation Manager console.

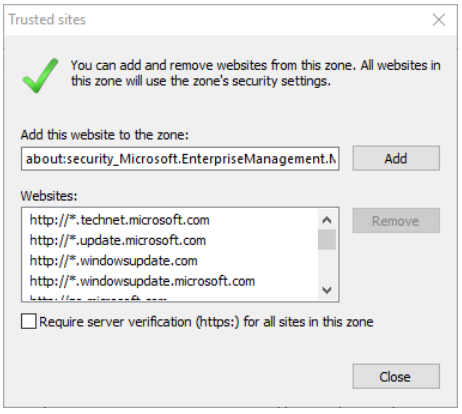


Figure 4- 2

4.2 Accessing Asset Management Dashboard

In Asset Management, select the **Supermicro Plug-in** folder in the navigation pane and click **Asset Management**.

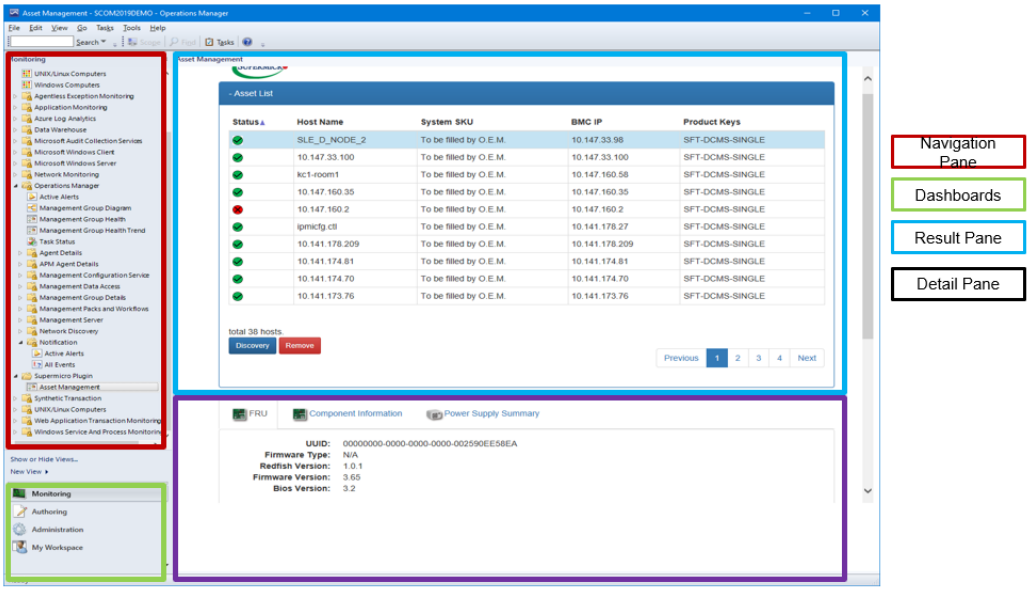


Figure 4- 3

- **Status:** Shows the status and health of this system.

Icon	Description
	Busy, Deep, Cold Reset
	System Absent
	System Health OK
	System Health Warning
	System Health Critical

- **Host Name:** Shows the DNS host name without any domain information of the BMC.
- **System SKU:** Shows the manufacturer SKU for this system.
- **BMC IP:** Shows the BMC IP address of this system.
- **Product Keys:** Displays currently activated licenses on this system.

Note: The Asset List is empty for the first-time use, and you need to add some systems to build your list. For more information, please refer to *Create a Credential* and *Adding a System to the Asset List*.

4.3 Creating a Credential

A credential is required to login BMC for monitor/manage. It will be added to Windows Credential Manager. To create a credential, follow these steps.

1. Click the **Discovery** button in the Result pane (Figure 4-3), and click **Credential Management**.

Figure 4- 4

2. Click **New**, enter the necessary information, and then click **Add**.

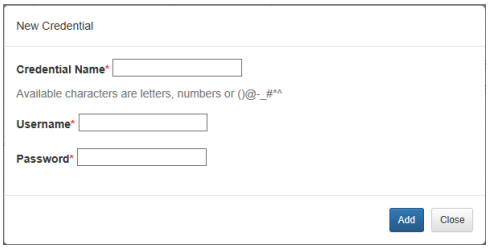


Figure 4- 5

4.4 Adding a System to the Asset List

Two methods are available for you to add a system to the Asset List.

4.4.1 Single Search

Use Single search to search for a specific IP address of a Supermicro Server. Follow these steps.

1. Click the **Discovery** button in the Result pane (Figure 4-3), and click **Single Search**. A dialog box appears.

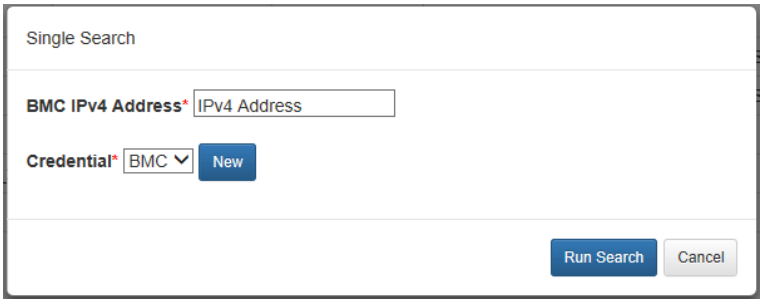


Figure 4- 6

2. Enter the IP address, and use the Credential drop-down list to select a credential. Note that you can add a new credential here by clicking the **New** button.
3. Click **Run Search**. The result then shows up on the Search Result page.

4.4.2 Range Search

Use Range search to search for the Supermicro Servers within a certain range of IP addresses. Follow these steps.

1. Click the **Discovery** button in the Result pane (Figure 4-3), and click **Range Search**. A dialog box appears.

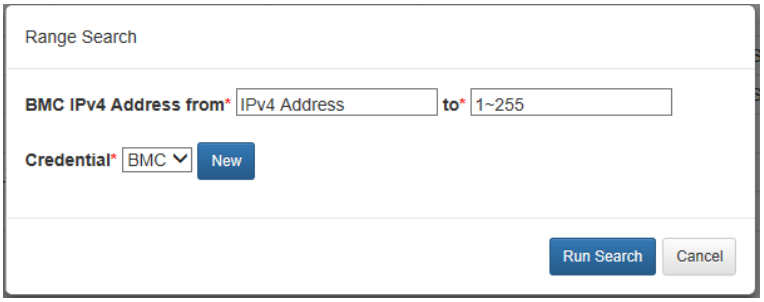


Figure 4- 7

2. Enter the IP addresses within your desired range, and use the Credential drop-down list to select a credential. Note that you can add a new credential here by clicking the **New** button.
3. Click **Run Search**. The result then shows up on the Search Result page.

4.4.3 Viewing Search Results

The Search Result page displays the searching progress and status. The search results will be kept until the next search is performed or the Supermicro Redfish Connector service is restarted. Only the valid system with a green State icon can be added to the asset list.

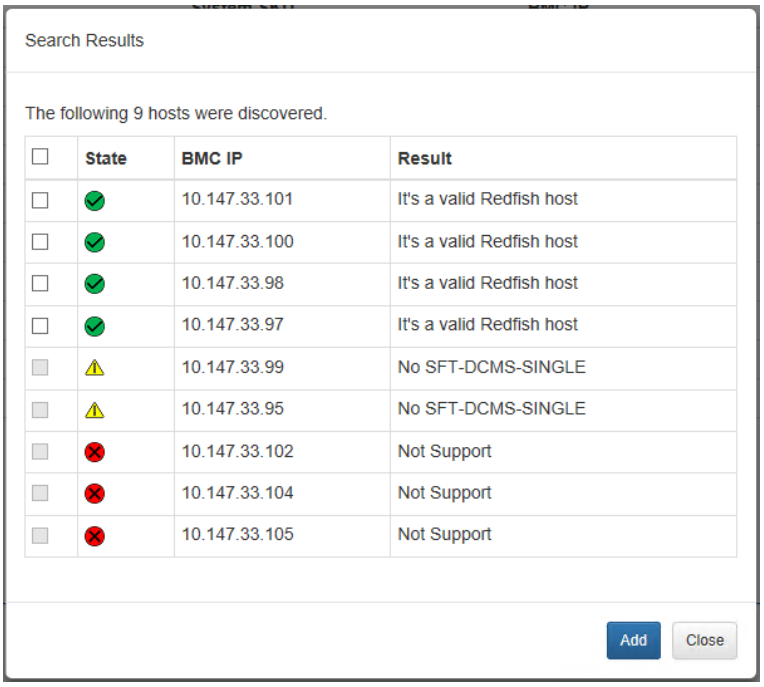


Figure 4- 8

4.5 Viewing the Details of the System

Click on any of the system in asset list table to view more information. Six types of information are listed by tab at the bottom: FRU, Component Information, Power Supply Summary, Sensor, Health Event Log and Maintenance Log. Click each tab to view the details.

4.5.1 Detail

Use this tab to view the detail information of the selected system.

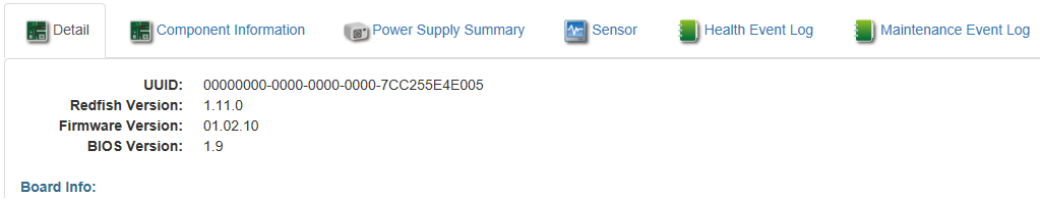
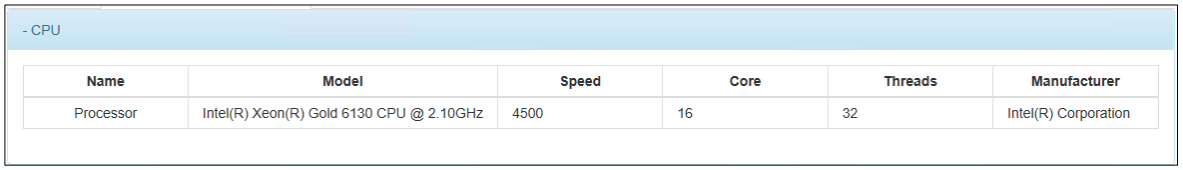


Figure 4- 9

4.5.2 Component Information

Use this tab to view the details about CPU and memory modules of the selected system.

4.5.2.1 CPU

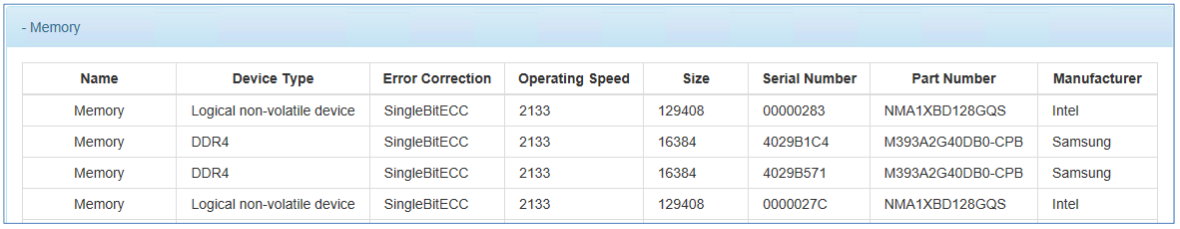


- CPU

Name	Model	Speed	Core	Threads	Manufacturer
Processor	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz	4500	16	32	Intel(R) Corporation

Figure 4- 10

4.5.2.2 Memory



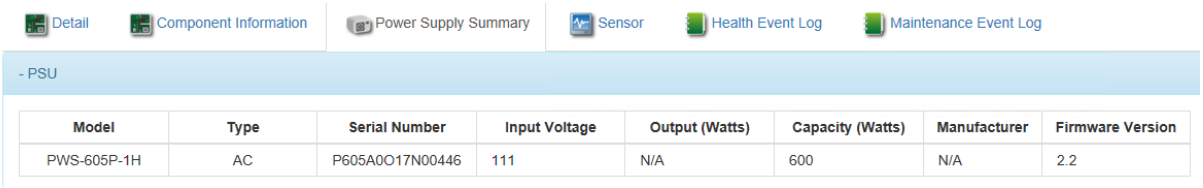
- Memory

Name	Device Type	Error Correction	Operating Speed	Size	Serial Number	Part Number	Manufacturer
Memory	Logical non-volatile device	SingleBitECC	2133	129408	00000283	NMA1XBD128GQS	Intel
Memory	DDR4	SingleBitECC	2133	16384	4029B1C4	M393A2G40DB0-CPB	Samsung
Memory	DDR4	SingleBitECC	2133	16384	4029B571	M393A2G40DB0-CPB	Samsung
Memory	Logical non-volatile device	SingleBitECC	2133	129408	0000027C	NMA1XBD128GQS	Intel

Figure 4- 11

4.5.3 Power Supply Summary

Use this tab to view the information of the power supply unit of the selected system.



Model	Type	Serial Number	Input Voltage	Output (Watts)	Capacity (Watts)	Manufacturer	Firmware Version
PWS-605P-1H	AC	P605A0O17N00446	111	N/A	600	N/A	2.2

Figure 4- 12

4.5.4 Sensor

This tab provides the sensor information of the selected system.

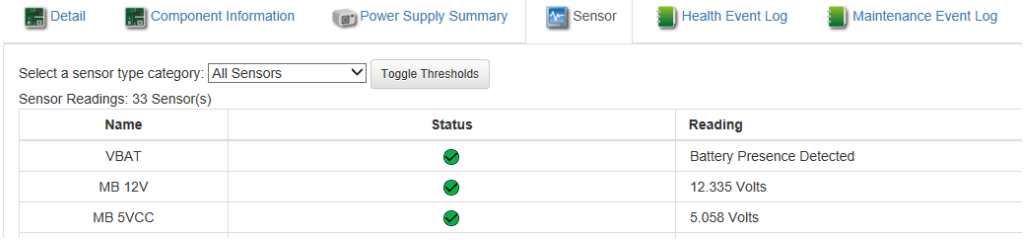


Figure 4- 13

- **Name:** The name of the monitored item.
- **Status:** The status of the sensor item.

Icon	Description
	Sensor Absent
	Sensor Status OK
	Sensor Status Warning
	Sensor Status Critical

- **Reading:** The readings of the sensor.

4.5.4.1 Accessing the Additional Information

Click the **Toggle Thresholds** button to access the additional information:

- **Low NR (Low Non-Recoverable):** This is the low threshold for a non-recoverable item. Any item with a reading below this point will not be recovered.
- **Low CT (Low Critical-Threshold):** This is the low threshold for a critical item. Any item with a reading below this threshold is in a critical state.
- **High CT (High Critical-Threshold):** This is the high threshold for a critical item. Any item with a reading above this threshold is in a critical state.

- **High NR (High Non-Recoverable):** This is the high threshold for a non-recoverable item. Any item with a reading above this point will not be recovered.

4.5.5 Health Event Log

This tab provides a record of events occurred on the managed system for you to diagnose or detect any potential issues.

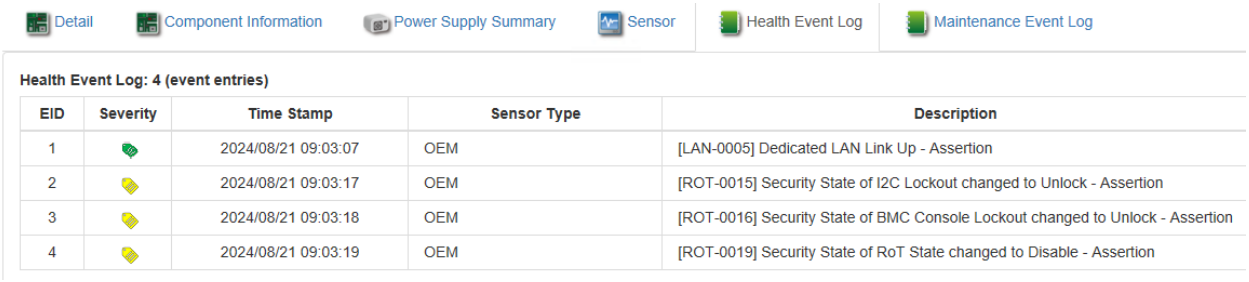


Figure 4- 14

- **EID:** The event ID of this event.
- **Severity:** The severity level of this event.

Icon	Description
	Event Log Severity OK
	Event Log Severity Warning
	Event Log Severity Critical
N/A	No specific severity information is available.

- **Time Stamp:** The time when the event takes place.
- **Sensor Type:** The type of the event.
- **Description:** A brief description of the event.

4.5.6 Maintenance Log

This page displays the record of maintenance events such as administrative events. Event log table shows below details about each log entries.

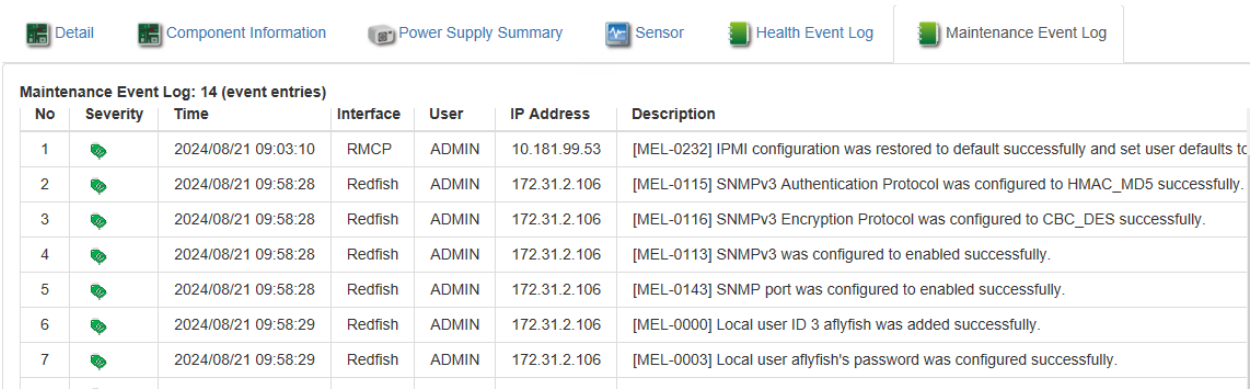


Figure 4- 15

- **No:** Index of the event log.
- **Severity:** Indicates severity of the events.

Icon	Description
	Event Log Severity OK
	Event Log Severity Warning
	Event Log Severity Critical
N/A	No specific severity information is available.

- **Time:** Time stamp of the event occurrence.
- **Interface:** Interface that triggered the event (e.g., RMCP, Redfish, Web).
- **User:** Name of the user that triggered the event.
- **IP Address:** Source that triggered the event.
- **Description:** Basic description of the event.

4.6 Management Functions

Right-clicking the desired item in the Asset List to select one of the management functions.

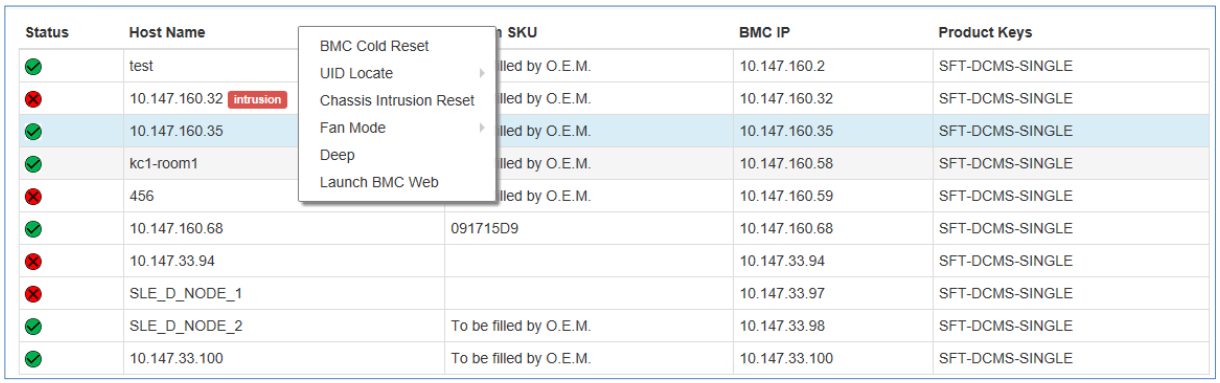


Figure 4- 16

4.6.1 BMC Cold Reset

Use this function to reset the selected BMC device. The status icon will change, and it takes a few minutes to re-sync the system status.

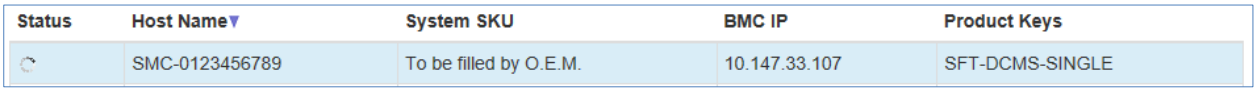


Figure 4- 17

4.6.2 UID Locate

You can turn the UID on or off to assist in identifying the desired system. To turn the UID on or off, right-click the desired system, select **UID Locate**, and then select **On** or **Off** to suit your need.

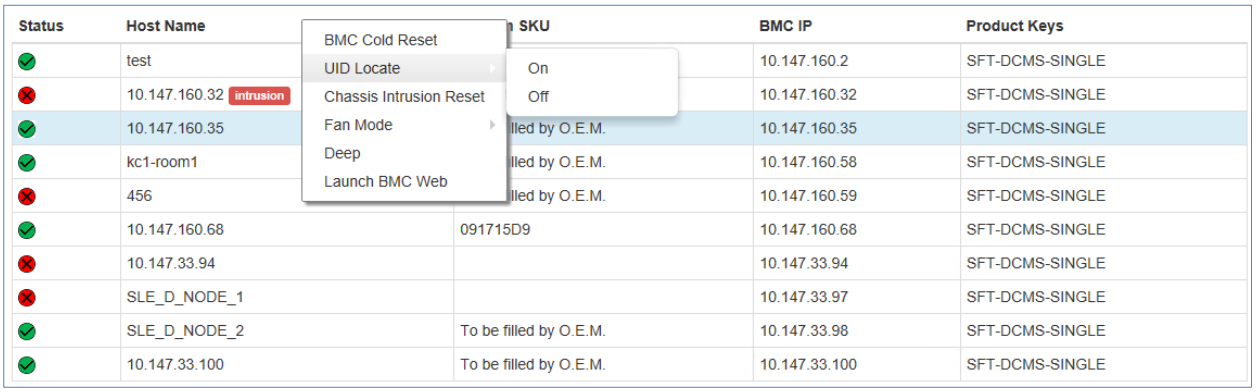
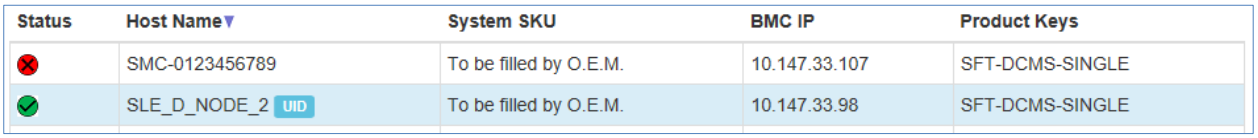


Figure 4- 18

If the UID is turned on, an UID badge appears next to the selected system in the Asset List.

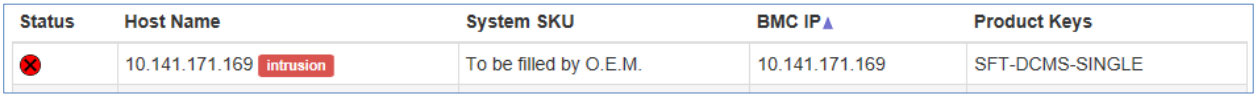


Status	Host Name	System SKU	BMC IP	Product Keys
	SMC-0123456789	To be filled by O.E.M.	10.147.33.107	SFT-DCMS-SINGLE
	SLE_D_NODE_2 UID	To be filled by O.E.M.	10.147.33.98	SFT-DCMS-SINGLE

Figure 4- 19

4.6.3 Chassis Intrusion Reset

When chassis is intruded, an intrusion badge appears next to the related system in the Asset List. You can use this function to reset the chassis intrusion alarm after you clear it out.

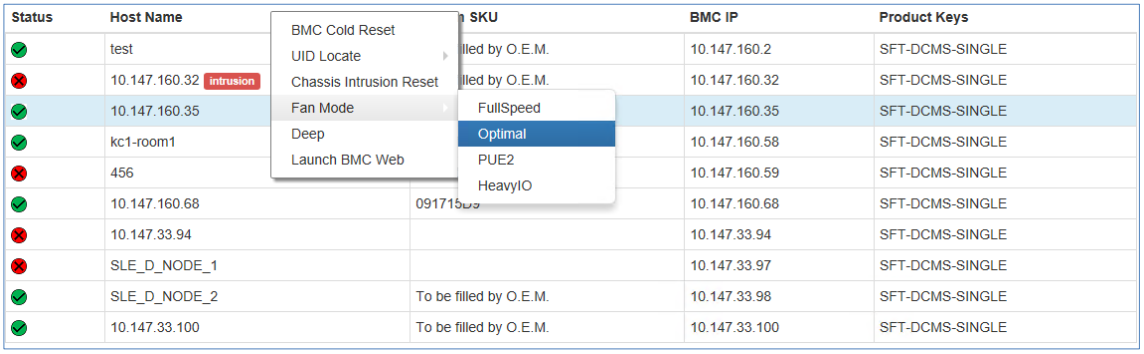


Status	Host Name	System SKU	BMC IP	Product Keys
	10.141.171.169 intrusion	To be filled by O.E.M.	10.141.171.169	SFT-DCMS-SINGLE

Figure 4- 20

4.6.4 Fan Mode

Use this function to control fan speed of the desired system. Note that the available options may vary depending on the selected system. The current fan speed mode is displayed highlight color in the Fan Mode submenu.



Status	Host Name	SKU	BMC IP	Product Keys
	test	lled by O.E.M.	10.147.160.2	SFT-DCMS-SINGLE
	10.147.160.32 intrusion	lled by O.E.M.	10.147.160.32	SFT-DCMS-SINGLE
	10.147.160.35		10.147.160.35	SFT-DCMS-SINGLE
	kc1-room1		10.147.160.58	SFT-DCMS-SINGLE
	456		10.147.160.59	SFT-DCMS-SINGLE
	10.147.160.68	0917	10.147.160.68	SFT-DCMS-SINGLE
	10.147.33.94		10.147.33.94	SFT-DCMS-SINGLE
	SLE_D_NODE_1		10.147.33.97	SFT-DCMS-SINGLE
	SLE_D_NODE_2	To be filled by O.E.M.	10.147.33.98	SFT-DCMS-SINGLE
	10.147.33.100	To be filled by O.E.M.	10.147.33.100	SFT-DCMS-SINGLE

Figure 4- 21

4.6.5 Deep

Use this function to rescan the Redfish API resources and actions of the selected system. The API resources are used by Supermicro Redfish Connector service to monitor and manage the Supermicro Servers. By default, every monitored system will do deep function one time. After then, you may need to manually run deep function again if there're any hardware components change.

4.6.6 Launch BMC Web

To configure the BMC settings, use this function to open a new Internet Explorer browser and navigate the BMC web console. Because of the enhanced security of Internet Explorer in Windows Server, you

need to add it to the trusted zone, and then restart the Operation Manager console for the changes to take effect.

Appendix A. Third-Party Software

The following open source libraries are used in Management Plug-in for SCOM package

Library	License
jQuery 3.5.1	MIT
Bootstrap 3.4.1	MIT
Credential Management 1.0.2	Apache-2.0

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Web Site:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Web Site:	www.supermicro.com.tw

Technical Support:

Email:	support@supermicro.com.tw
Tel:	+886-(2)-8226-3990