



System Management Module 3 User Guide



Note

Before using this information and the product it supports, be sure to read and understand the safety information and the safety instructions, which are available at:

http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html

In addition, be sure that you are familiar with the terms and conditions of the Lenovo warranty for your solution, which can be found at:

<http://datacentersupport.lenovo.com/warrantylookup>

First Edition (February 2025)

© Copyright Lenovo 2025.

LENOVO and THINKSYSTEM are trademarks of Lenovo. All other trademarks are the property of their respective owners.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Contents	i
-----------------	----------

Chapter 1. Introduction	1
--------------------------------	----------

Scope of This Document	1
------------------------	---

Chapter 2. Opening and Using the System Management Module Web Interface	3
--	----------

Logging in to the SMM3	3
------------------------	---

Description of SMM3 functions on web interface	6
--	---

Chapter 3. Home page	9
-----------------------------	----------

Chapter 4. Events	11
--------------------------	-----------

Event Logs	11
------------	----

Audit Logs	11
------------	----

Debug Logs	12
------------	----

Notification (Email/SNMPv2c/PEF)	12
----------------------------------	----

Chapter 5. Systems	15
---------------------------	-----------

Inventory	15
-----------	----

Nodes	16
-------	----

Voltage	17
---------	----

Cooling	17
---------	----

Chapter 6. Power	19
-------------------------	-----------

Power overview	19
----------------	----

Power meter	19
-------------	----

Power configuration	19
---------------------	----

Power capping	20
---------------	----

Chapter 7. Operations	21
------------------------------	-----------

Firmware	21
----------	----

SMM	21
-----	----

SMM Firmware Update	21
---------------------	----

PCS Firmware Update	22
---------------------	----

Enclosure and SMM	22
-------------------	----

Enclosure	22
-----------	----

SMM	22
-----	----

Session	22
---------	----

Chapter 8. Setting	23
---------------------------	-----------

User	23
------	----

Account policy settings	23
-------------------------	----

Add or Edit User	24
------------------	----

Network interface	25
-------------------	----

General setting (Hostname, DNS Domain Name, VLAN)	26
---	----

IPv4 configurations	26
---------------------	----

IPv6 configurations	27
---------------------	----

Network service	28
-----------------	----

HTTPS Certificates	28
--------------------	----

Service and Port	29
------------------	----

SMTP Server	29
-------------	----

Backup and Restore	29
--------------------	----

Backup SMM Configuration	30
--------------------------	----

Restore SMM from Configuration File	30
-------------------------------------	----

VPD	30
-----	----

Reset SMM to Factory Defaults	30
-------------------------------	----

Date and time	30
---------------	----

Chapter 9. System Management Module 3 Redfish REST API	31
---	-----------

Chapter 10. IPMI Command	33
---------------------------------	-----------

IPMI Command Contents	34
-----------------------	----

SMTP Configuration Parameters	54
-------------------------------	----

Parameter in IPMI Command	58
---------------------------	----

Parameter in IPMI Command Contents	58
------------------------------------	----

IPMI Parameter - LAN Configuration Parameters	59
---	----

Index	61
--------------	-----------

Chapter 1. Introduction

This section summarizes the functions of the System Management Module 3 (SMM3) firmware built-in web pages. It supports the Transport Layer Security 1.3 for data encryption over the network and certificate management.

The SMM3 performs the following tasks:

1. Node status report
2. Enclosure power status report
3. Enclosure power configuration management
4. Enclosure Vital Product Data (VPD) information report
5. Enclosure event log Display, Save, and Clear
6. SMM3 configuration and settings Backup or Restore

Scope of This Document

This user guide provides the process of operating SMM3 and detailed WebGUI. The descriptions include how to check the status, component information and show you how to modify the configuration. It offers the detailed explanation and definition for each function tabs of the SMM3 web pages.

The user guide supports the following enclosures and trays:

- ThinkSystem N1380 Neptune DWC Enclosure Type 7DDH (N1380 Enclosure), compatible with the following tray
 - ThinkSystem SC750 V4 Compute Node Type 7DDJ (SC750 V4 Tray)

Notes:

- Before using this information and the product it supports, be sure to read and understand the safety information and the safety instructions, which are available at:
http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html
- Be sure that you are familiar with the terms and conditions of the Lenovo warranty for your solution, which can be found at:
<http://datacentersupport.lenovo.com/warrantylookup>

Chapter 2. Opening and Using the System Management Module Web Interface

This topic describes the login procedures and the actions that you can perform from the System Management Module web interface.

You must first log in using the System Management Module web interface to access the System Management Module remotely. This chapter describes the login procedures and the actions that you can perform from the System Management Module web interface.

Notes:

- The SMM website only supports English settings.
- The web pages can be displayed on mobile browsers but may not be optimized. For example, if some tablets are in vertical mode, the resolution width is 768 pixels, and SMM Web content cannot be displayed correctly.
- The display in browser and system zoom mode will not be optimized.

Logging in to the SMM3

Use the information in this topic to access the SMM3 through the SMM3 web interface.

To log in to the SMM3 web interface, complete the following steps:

1. Open a web browser. In the address or URL field, type the IP address or host name of the SMM3 to which you want to connect.

The following out-of-factory default network settings are applied when you first access the SMM3:

- a. SMM3 attempts to use DHCP to acquire an IP address. If SMM3 cannot acquire IP address from the DHCP server in two minutes, it will use the static IP address.
- b. The default static IP is 192.168.70.100 (IPv4 enabled).
- c. Using Hyper Text Transfer Protocol Secure (HTTPS). (For example, <https://192.168.70.100>)
- d. IPv6 enabled with local link address (LLA) IP

Notes: To calculate LLA IP, follow the procedures below:

- 1) Split the MAC address of SMM3 (39-A7-94-07-CB-D0) into two parts and insert FF-FE in the middle. For example, 39-A7-94-FF-FE-07-CB-D0
 - 2) Convert the two hexadecimal digits at the left end of the string to binary. For example, 00111001-A7-94-FF-FE-07-CB-D0
 - 3) Invert the value for bit 1 of the first byte. For example, 00111011-A7-94-FF-FE-07-CB-D0
 - 4) Convert the binary digits at the left end of the string back to hexadecimal. For example, 3B-A7-94-FF-FE-07-CB-D0
 - 5) Combine the hexadecimal digit pairs into 4-digit groups. For example, 3BA7-94FF-FE07-CBD0
 - 6) Replace dash (-) separators with colon (:) separators. For example, 3BA7:94FF:FE07:CBDO
 - 7) Add FE80:: to the left of the string. For example, FE80::3BA7:94FF:FE07:CBDO
2. Type your username and password (assigned by the system administrator) in the SMM3 Login window. The SMM3 is set initially with a username of USERID and password of PASSWORD (with a zero, not the letter O). The Login window is shown in the following illustration.

Note: User can click the “eye” icon on the right of the password input box to show or hide the password text.

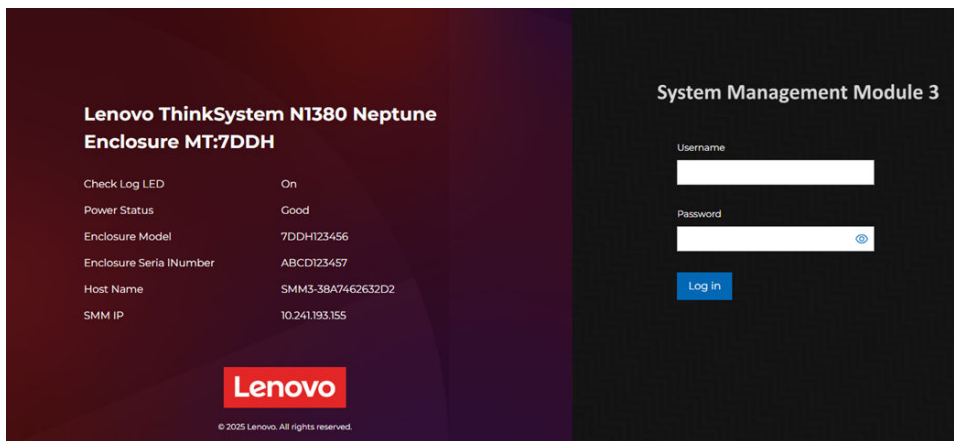


Figure 1. Login page

3. Click the Log in button to start the session.
4. Change the password for the first login.

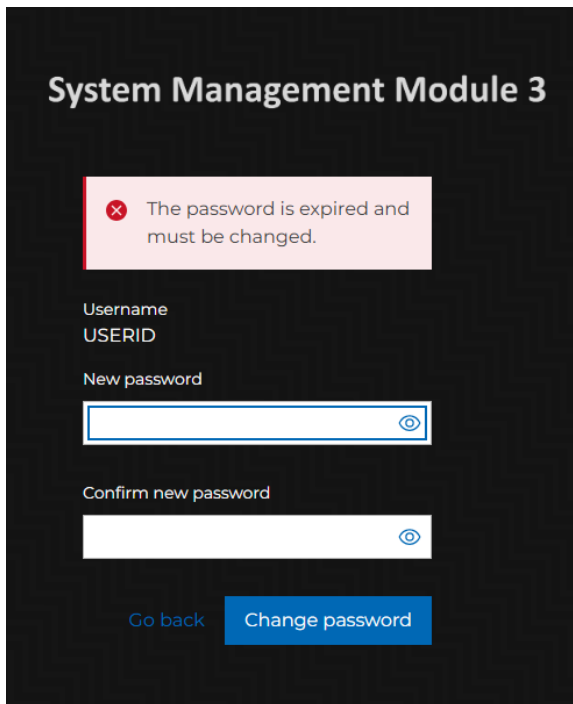


Figure 2. Changing password for the first login

Notes:

- Default password complexity rules:
 - At least ten characters in length
 - Must contain at least one number (0 through 9)
 - Must contain at least two of the following three categories:
 - An uppercase letter (**A** through **Z**)
 - A lowercase letter (**a** through **z**)

- A non-alphabetic characters such as !@#\$%^*_+={}~|?`\"
 - Alternatively, you can use the following REST API command to change the password: `curl -k -H "Content-Type:application/json" -X PATCH -d '{"Password": "[NEW PASSWORD]"}' https://USERID:[PASSWORD]@[SMM3_IP]/redfish/v1/AccountService/Accounts/USERID`
5. The browser opens the SMM3 home page, as shown in the following illustration.

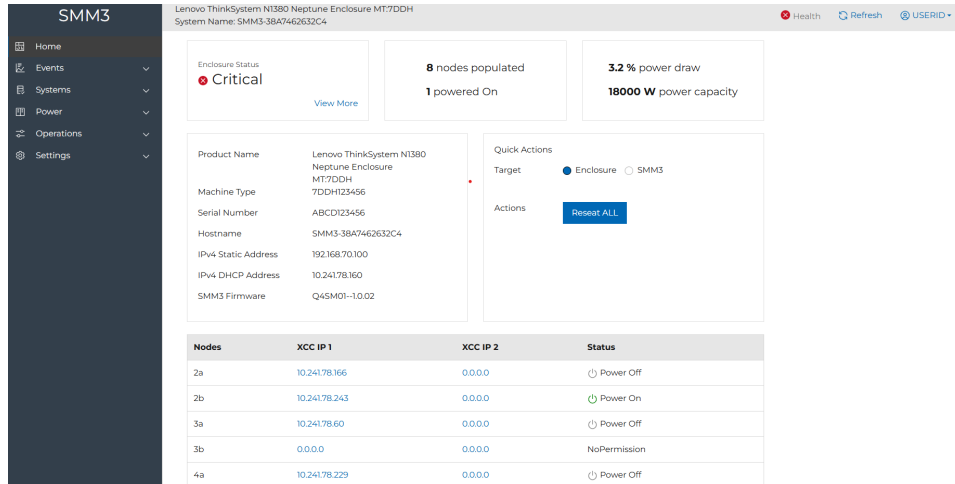


Figure 3. Webpage after login

The webpage is essentially divided into three sections. The first section is the left navigation panel, which is a set of topics that allow you to perform the actions shown in “Description of SMM3 functions on web interface” on page 6.

The second section is the top bar, which show the following system information from left to right:

- **Product name**
- **System name**
- **Health:** Select which health status to show. The health status includes the following:
 - **Health**: Indicate that there is only normal level SEL.
 - **Health**: Indicate that there is a warning level SEL without any critical level SEL.
 - **Health**: Indicate that there is a critical level SEL.
- **Refresh:** Refresh the current page content.
- **Login name:** Display the login username. Click the user icon to show the following list:
 - **Profile settings:** Configure user information. Change the user password or select the time zone display preference throughout the application.
 - **Help:** Click the link to navigate to https://pubs.lenovo.com/mgt_tools_smm3/.
 - **Open Source Licenses:** Click the link to export SMM3 open-source list to the download folder. The export file name will be named: **open_source_licenses.txt** by default.
 - **Log out:** Click the link to log out from the current user and you will be redirected to login page.

The third section is the enclosure and node overall status and information provided to the right of the navigation panel. For more information, see Chapter 3 “Home page” on page 9.

Note: The content in the third section might be different depends on the tab you select in the navigation panel.

Description of SMM3 functions on web interface

The information in this topic explains the SMM3 functions on the web interface.

The following is a table that describes the System Management Module 3 functions in the left navigation panel.

Tab	Selection	Description
Home	Enclosure status	Show enclosure health information.
	Node status	Show the number of nodes installed in the enclosure and the number of powered-on nodes.
	Power status	Show system power usage status.
	Enclosure Information	Show enclosure product name, machine type, hostname, network information and firmware version.
	Quick Actions	Provide enclosure and SMM3 quick actions.
	Nodes Information	Provide enclosure installed nodes information.
Events	Event logs	The Event Log page displays entries that are currently stored in the SMM event log. All events in the log are time stamped, using the SMM date and time settings. Some events also generate alerts, if they are configured to do so. You can sort and filter events in the event log and export them to a file.
	Audit Logs	The Audit Log page displays entries that are currently stored in the SMM audit log. The log includes a text description of system events that are reported and remote access attempts.
	Debug logs	Generate and download the debug log for advance service support.
	Notification	Include PEF configuration for sent notification condition. This page allows you to manage who will be notified of system events. It allows you to configure Email/SNMPv2c recipient. You can also generate a test event to verify notification feature operation. Edit trap receiver and email receiver while PEF condition happened.

Tab	Selection	Description
Systems	Inventory	The inventory page displays the all the components in the system, along with their status and key information. You can click on a device to display additional hardware information for it.
	Nodes	Show enclosure node information, include XCC IP, power status and restore policy. Provide restart XCC3 or reseal node action.
	Voltage	Display system voltage relative sensor.
	Cooling	Show cooling configuration and Leakage sensor status
Power	Power Overview	Show Power relative information.
	Power Meter	Displays PCSs status and related power data.
	Power configuration	Configure PCS policy. Allow user to configure the power redundancy mode.
	Power Capping	Edit entire enclosure power capping and node power capping.
Operations	Firmware	The Server Firmware page displays firmware information and allows you to update the SMM or PCS firmware.
	Enclosure and SMM	Support enclosure virtual reset, SMM restart, SMM locator led control and some information.
	Session	Configure maximum session number and timeout value. List all session connect to this SMM system.
Setting	User	List all available user. It allows you to add/edit/delete local user. Configure advance user setting, which includes password complex rule and lock out user period, etc.
	Network interface	SMM network interface information, include IPv4, IPv6 Configuration.
	Network service	It allows you add/replace HTTPS configuration, enable/disable IPMI service and setup SMTP server configuration.
	Backup and restore	Allow you to backup or restore SMM configuration and VPD info and reset the configuration of the SMM to the factory defaults. Attention: When you click Reset SMM to Factory Defaults , all modifications that you have made to the SMM will be lost.

Tab	Selection	Description
	Date and time	Configure SMM date and time

Chapter 3. Home page

Home page displays enclosure overall status and information.

After logging into the SMM3 web interface, the home page is displayed. From this page, you can view the Enclosure status, enclosure node, enclosure power, enclosure information, quick actions, and each nodes information.

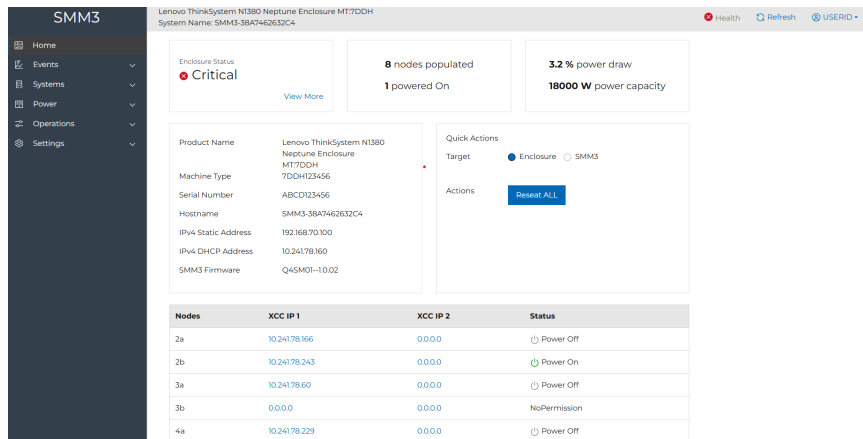


Figure 4. Home page

Viewing the overall status

The overall information panel is located to the upper of the home page provides a summary of common server information, which includes the following:

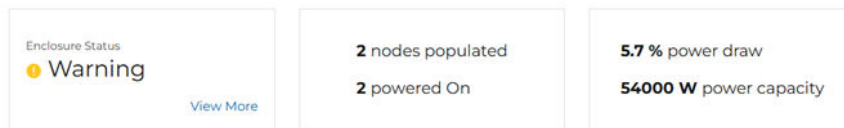


Figure 5. Overall information

- **Enclosure status:** Represent the enclosure overall health status which includes the following:

- **Normal** : Indicate the enclosure in Normal status.
- **Warning** : Indicate the enclosure is in Warning status.
- **Critical** : Indicates the enclosure is in Critical status.

Click the “**View More**” link to be navigated to the “**Event Logs**” on page 11 page.

- **Node status:**

- **Nodes populated:** Show the number of present nodes.
- **Powered On:** Show the number of powered on nodes.

- **Power status:**

- **Power draw:** Show current power loading.
- **Power capacity:** Maximum power capacity.

Viewing the Enclosure information

Show the enclosure information which includes the following:

Product Name	Lenovo ThinkSystem N1380 Neptune Enclosure MT:7DDH
Machine Type	7DDH123456
Serial Number	ABCD123456
Hostname	SMM3-6AE74DEFA74D
IPv4 Static Address	192.168.70.100
IPv4 DHCP Address	10.241.70.100
SMM3 Firmware	Q4SM01A-1.0.00

Figure 6. Enclosure information

- **Product Name:** Product name
- **Machine Type:** Machine type
- **Serial Number:** Serial number
- **Hostname:** Hostname, default is SMM3-[MAC-Address]
- **IPv4 Static Address:** Display the current configured static IPv4 address
- **IPv4 DHCP Address:** Display the IPv4 address assigned by the DHCP server
- **SMM3 Firmware:** Show current firmware version

Quick Actions

The quick actions section on the SMM3 home page provided two relative targets, Enclosure and SMM3. You can select one of the following targets to show the related action:

- **Enclosure:** “Reseat ALL”.SMM3 will reseat the whole enclosure including the SMM3 and all nodes.
- **SMM3:** “Restart”. Restart SMM3.

Viewing the Node information

The node information panel located to the bottom of the home page provides a summary of common node information, which includes the following:

Nodes	XCC IP 1	XCC IP 2	Status
1a	10.241.78.102	0.0.0.0	 Power Off
1b	10.241.78.238	0.0.0.0	 Power On

[View More](#)

Figure 7. Node information

- **XCC IP 1/ XCC IP 2 link:** Click the IP link to open XCC webpage.
- **View more:** Redirect to [“Nodes” on page 16](#).

Chapter 4. Events

Use the information in this topic to understand how to view and monitor information for the server that you are accessing.

Event Logs

The **Event Log** page provides a historical list of all hardware and management events.

The SEL (System Event Log) records enclosure-level information, warnings, and critical events, allowing user to review what has happened in the enclosure. A maximum number of 4090 event entries can be logged.

By default, the latest entry appears on the first page as events are sorted in descending order from the most recent to the earliest. Click on **Date** to reorder the event from earliest to latest.

The following is a description of the actions that can be performed in the **Event Log** page.

- **Search:** Allow users to enter search keywords and display only relevant results in the table. Filters data if that keyword appears in the Severity, Date, or Description columns. Note that the input is case-insensitive.
- **Time filter:** Filter or select data within a specific time range. You can input the specific date in the input box directly or click the calendar icon on the right side to select the time interval for the events you want to display.
- **Filter:** Filter SEL entries with event severity. Click the Filter button to display a severity list with the following options. User can select multiple severities to filter the SEL entries.
 -  **Normal** : Indicates **Normal** type of events.
 -  **Warning** : Indicates **Warning** type of events.
 -  **Critical** : Indicates **Critical** type of events. The Check Log LED will be lit when error events occur.
- **Delete all:** Click the button to delete all system event logs.
- **Export all:** Export all SMM3 SEL data to local storage. The default format of the file name is: all_event_logs_YYYY-MM-DD_HH-MM-SS.json. For example, all_event_logs_2025-03-14_11-34-00.json.

Note: Currently, a new event cannot be written into the log when it is full. Please manually clear the log to allow the latest event to be recorded.

Audit Logs

The **Audit Logs** provides a historical record of user actions, including logging in to the SMM3, creating users, and updating passwords.

The latest 1024 audit entries will be displayed.

Both the event log and the audit log support similar maintenance and viewing actions. To see the description of the display and filtering actions that can be performed on the Audit Log page, see [“Event Logs” on page 11](#).

Notes:

- The audit logs will remain after the SMM3 restore to factory default setting.

Debug Logs

The **Debug Logs** instantly collects information about events and conditions that might lead up to a failure. It was formerly called FFDC (Fast Failure Data Collection).

If there is no available debug log file, the SMM debug log table shows “No items available”.

The following actions items can be performed in the **Debug Logs** section.

- **Initiate debug log:** Click the button to start generating debug log, it might take some time to complete.

Note: Make sure to refresh the web page to check if the file has been generated completed.

Once the file is generated, it will appear in the debug log table with option to download or delete.

- **Download icon:** Download the debug log file to the local storage. The default file format is: **[Machine-Type_SerialNumber-smm3_DebugLog_YYMMDD_HHMMSS.tgz]**. For example, 7DDH123456_ABCD123456_smm3_DebugLog_241218_110258.tgz
- **Delete:** Delete the debug log to free up the storage space.

Notification (Email/SNMPv2c/PEF)

Use the information in this topic to add and modify e-mail, SNMPv2c trap or PEF. Configured email and SNMPv2c traps allow users to monitor the enclosure status. Email and SNMPv2c trap will be sent according to the PEF (Platform Event Filters) setting.

The following is a description of the actions that can be performed in the **Notification** tab.

Email

You can enable, configure and test email alert in this section.

- **Sender Information:** Sender email address
- **Edit Recipient:** Edit the email alert configuration.
 - Enabled or Disabled
 - Email Subject
 - Recipient
- **Clear Recipient:** Clear selected email alert setting.
- **Sent Test Email:** Send testing email alerts with selected configuration.

Notes:

- Before sending an Email alert, make sure that the changes of the following items have been saved successfully:
 - **Events → Notification → PEF section:** Global Alerting is “Enabled”.
 - **Events → Notification → Email section:** Recipients is set as valid Email address, and the status is “Enabled”.
 - **Setting → Network service → SMTP Server:** SMTP Server Configuration server is connected successfully.
- When the SMM3 SEL is full, no new event entry can be added to the SEL. Email alert will not be generated until the log is cleared.

SNMPv2c Trap

- **Community:** Click the pencil icon to edit the community name of SNMPv2c Trap.

Note: Default value: public.

- The following actions can be performed in the SNMPv2c Trap section:
 - **Edit Trap:** Click the button to edit the setting the SNMv2c trap destination.
 - **Disabled or Enabled:** Select to enable or disable the SNMP Trap status. If **Disabled** is selected, the setting will remain configured but no SNMPv2 traps will be sent. All traps are disabled by default.
 - **Destination SNMPv2c Trap Address:** Enter an IPv4 or IPv6 destination trap address, such as 10.24.195.66 or 2001::30.
 - **Clear Trap:** Click the button to clear the previous configuration of the selected SNMP.
 - **Send Test Trap:** Click the button to send a test SNMP trap using the selected trap configuration.

Notes:

- Before sending a test trap, make sure that the changes to the following items have been saved successfully:
 - **Target Destination** and **Community String** have been setup.
 - **Events → Notification → PEF section:** Global Alerting is “Enabled”.
- When the SMM3 SEL is full, some PEF alerts might be missing or be sent repeatedly.
- All the events would be sent to the destination IP address when **Global Alerting Enable** is enabled on the PEF section.
- For SNMP trap type, check the Generate PEF box for targeted types of events. See [“PEF section” on page 13](#) below for configuration details.

Platform Event Filtering (PEF) List

You can set SMTP/SNMP trap event types in this section. The following information provides the default values:

- Global Alert status:
 - The global setting applies to all SNMPv2c trap and email recipients. The setting will be configured directly after clicking the button.
 - If enabled, system will send SNMPv2c trap, or an email alert based on the configuration in SNMPv2c Trap and Email section.
 - If disabled, the settings will remain configured but no SNMPv2c trap or an email alert will be sent.
 - Disabled by default.
- All the filters are set as Enabled and selected by default. Select the types of events that will be cause Traps to be sent. If you click the checkbox next to the filter you can select or deselect notifications for specific components in the category. Make sure to click “Save” button after the configuration.

Chapter 5. Systems

Use the information in this chapter to understand the options available for system configurations.

Inventory

Use the information in this page to view or edit the vital product data for the system.

Notes: Click the pencil icon to configure the following VPD information:

- **Enclosure UUID:** UUID format data: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx where x is a hexadecimal character.
- **Enclosure Serial Number:** Up to 10 characters using alphanumeric characters a-z, A-Z and 0-9.
- **Enclosure Model:** Up to 10 characters using alphanumeric characters a-z, A-Z and 0-9.
- **Interposer UUID:** UUID format data: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx where x is a hexadecimal character.

The page provides the fixed VPD (Vital Product Data) information.

- **“Enclosure” on page 15:** Show enclosure inventory.
- **“Interposer” on page 15:** Show interposer inventory.
- **“SMM3” on page 16:** Show SMM3 inventory.
- **“Power Conversion Stations (PCS)” on page 16:** Show PCS inventory.

Enclosure

The following information is available for the enclosure:

- Name
- Serial number
- Model
- UUID
- Manufacturer
- Hardware version

Interposer

The following information is available for the interposer:

- Name
- Serial number
- EC Level
- Part number
- FRU part number
- UUID
- Manufacturer
- Manufacturer date
- Hardware version

SMM3

The following information is available for the SMM3:

- Name
- Serial number
- EC Level
- Part number
- FRU part number
- UUID
- Manufacturer
- Manufacturer date
- Hardware version

Power Conversion Stations (PCS)

The power supply ID and status will be displayed in this section:

- Name
- Model
- Power capacity
- Serial number
- Part number
- FRU part number
- Header code
- Barcode
- Manufacturer
- Manufacturer revision
- Manufacturer model
- Manufacturer location
- Package version
- Primary firmware revision
- Secondary firmware revision

Nodes

Display nodes information, configure node restore policy, and provide restart XCC and reseal node actions.

- **Node checkbox:** Launch selected node to show available action item: restart XCC / Reseat Node.
- **Nodes:** Indicates server slot numbering and show the information of the present node. Depending on the type and the location of the node installed, the number is from 1a to 8d.
- **XCC IP 1 / XCC IP 2:** Show XCC IP information. Click the XCCIP link to open the XCC webpage.
- **Status:**
 - **No Permission:** Indicates node has not granted power permission and cannot power on.
 - **Fault:** Indicates node has power fault and cannot be powered on.
 - **Power On:** Indicates node is power on.
 - **Power Off:** Indicates node is power off.

- **Edit:** To configure power restore policy. Select either “**Power off**” or “**Last State**” for the restore policy. It indicates the mode of the operation after the power failure occurred.
 - Power off: Node remains power off when power is restored.
 - Last State: Node will be powered on automatically and restore to the status before the power failure occurred.

Make sure to click on “**Save**” to activate the setting.

Note: Use this configuration when ‘Current Power Status’ is Good.

To perform Restart XCC, Reseat Node through System Management Module 3 click the following button:

- **Restart XCC:** Click the “Restart XCC” button to restart node’s XCC.
- **Reseat Node:** Click the “Reseat Node” button to power cycle entire node.

Note: After these actions, the node’s XCC requires at least two minutes to be ready.

Voltage

Voltage page provides the voltage sensor of the SMM3 board.

When the sensor’s critical threshold is reached, SMM3 will generate an SEL.

Cooling

The Cooling tab shows the system cooling information and leak detector instance.

Element	Behaviors
Equipment Type	Shows “CDU”
Leakage Protection Power Off Mode	Shows “Soft Off” or “Hard Off”
Leakage Protection Power Off Time	The time in seconds the enclosure will power off while a water leak is detected.
Water Loop	Shows “Serial” or “Parallel”
Name	Shows detector name
Leak Detector Type	Shows “Moisture”
Status	Shows “Not present”, “Normal”, “Warning”, or “Critical”

Chapter 6. Power

Use the information in this topic to view power management information and perform power management functions

Power overview

This page displays enclosure power consumption, node power consumption, and the power consumption of power sub-systems, such as power conversion station.

Notes:

1. The enclosure and power supply power consumption samples every second and choose the maximum, minimum, average value among the latest 30 readings.
2. The node power consumption includes the power consumption of corresponding add-on tray such as a GPU tray

Power meter

This page displays the overall PCS status and related information.

It can be used for status monitoring, power configuration or as a reference for power capping solution.

Power configuration

This page allows users to set the redundancy mode, and zero output mode for power conversion station configuration.

Available fields in this section include the following:

- **Minimum PCS Count:** Click the pencil icon to edit and enter a minimum PCS count ranging from 1 to 4.
- **Redundancy Mode:** Offer three modes for users to choose from.
 - **None:** System could be throttled or shut down if one or more power supplies are in faulty condition.
 - **N+1:** There is one properly installed power supply as redundant power supply, so there is no impact to system operation or performance if any one of the power supplies is in faulty condition given that Oversubscription mode is not enabled.
 - **N+N:** N PCS active, and N PCS in standby mode.
- **Oversubscription Mode:** Grants users' access to extra power from the redundant power supply. When the redundancy fails, however, the power supply will shut down within one second if system power loading is not corrected. SMM3 takes the action of node throttling at such power emergency, while enclosure performance could be impacted.
 - Oversubscription mode is applied with N+1 and N+N redundancy mode enabled.
 - When enabled with N+1 redundancy mode, the total available power will be equivalent to 1.2 times of the total capacity of the N+1 redundancy mode.
- **Zero Output mode:** Put PCS into sleep mode when power requirement is low.
 - The **Zero Output** mode is disabled by default and only applied with N+1 and N+N redundancy mode enabled.
 - Disabling **Zero Output** mode will keep all power supplies always active.

- Three scanning period are offered: **Disabled/10/30/60 minutes**. Some PCS may enter hibernate mode to maintain the workload on the remaining active PCS at 50%, which makes the best efficiency out of PCS. When less time is chosen, SMM3 responds to workload changes more quickly

Click **Save** to activate the power configuration setting.

Power capping

To configure the power capping policy, use the information in this topic.

Power capping allows users to set a wattage limit on power consumption. When applied on individual node, the node power consumption is capped at assigned level and when applied on enclosure, the whole enclosure power consumption is capped.

You can choose one of the following power capping types:

- **Enclosure Power Capping**
- **Node Power Capping**

Total Power Capacity is being calculated based on power redundancy mode and number of PCS's installed in the system. The manual setting of maximum power limit can be over the actual power capacity.

When power capping is enabled, the system may be throttled in order to maintain the power limit. You can choose to enable or disable the power capping function. By clicking the pencil icon, you can change the power capping value. Input the value in the input box, ensure that the input value must be within the specific range.

Click **Save** after making the configuration changes.

Chapter 7. Operations

Operations that are used to manage the SMM3 module.

There are three pages:

- **Firmware**
- **Enclosure and SMM**
- **Session**

Firmware

The page provides firmware information and firmware update.

This page provides three main functions:

- [“SMM” on page 21](#)
- [“SMM Firmware Update” on page 21](#)
- [“PCS Firmware Update” on page 22](#)

SMM

An overview of the active and inactive firmware information is provided.

- **Active Firmware:** Overview of active firmware information.
- **inactive Firmware:** Overview of inactive firmware information.

SMM Firmware Update

The firmware update process comes in three steps.

- **Step 1:** Click **“Add file”** and select a firmware image file, then click **“Upload”**.
- **Step 2:** Once the valid firmware image has been uploaded, the firmware information will be displayed. Select **“SMM_Primary”** or **“SMM_Backup”** as the target that will be used for the update process.

The following actions can also be performed:

- **Enable Secure Rollback:** Click the checkbox to roll back to the previous firmware version. The function is set as “Disabled” by default.
- **Preserve Settings:** Check to preserve the setting. The configuration will be kept and SMM3 will be reboot after the firmware is updated. If you unclick the checkbox, SMM3 configurations will be reset to factory default setting after the firmware is updated.

Attention: Do not close the browser or change to another page during the upload process.

- **Step 3:** Click **“Update”** to start the update. The update progress will be shown and may take about 3-5 minutes to complete the update.

Attention:

- Do not close the browser during the update process, once the progress reaches 100%, SMM3 will atomically restart and users need to log in again to access the SMM3 web interface.

PCS Firmware Update

Steps to update PCS firmware. To manually apply update for PCS firmware, complete the following steps:

- **Step 1:** Click “**Add file**” and select a firmware image file, then click “**Upload**”.
- **Step 2:** Once the valid firmware image has been uploaded, the firmware information will be displayed. Check the PCS’s that will be used as the target for the update process. All the available PCS will be selected by default.

Attention: Do not close the browser during the upload process.

- **Step 3:** Click “**Update**” to start the update. The update progress will be shown and may take a few minutes depending on the number of PCS number that needs to be updated.

Attention: Do not close the browser during the update process.

Enclosure and SMM

Use the information in this topic to understand the enclosure and SMM settings.

Enclosure

Click the **Reset Enclosure** button, the enclosure will be powered off immediately and be powered on after 10 seconds.

Note: When you reset the enclosure, your web browser will lose contact with the SMM for several minutes.

SMM

When configuring the SMM, following options are available:

- **Check Log Status LED:** Shows “On” when critical event occurs and “Off” when system critical event is de-asserted.
- **Locator LED Accept Mode:** Show “On” or “Off”.
- **Locator LED:** Choose Locator Led behavior, click **Launch** button after making configuration changes.
 - **Turn Off:** Turn off the ID LED on all the compute nodes in the enclosure and enter accept mode, in which the LED behavior is determined by the node ID LEDs.

Note: Locator LED is set as accept mode by default.

- **Turn On:** All the node ID LEDs will be on except the blinking ones, which will remain blinking.
 - **Blink:** All the node ID LEDs will be blinking regardless of previous status.
- **Restart SMM:** Click the **Restart** button to restart the SMM, your web browser will lose contact with the SMM for 2 to 3 minutes. When the SMM is back online, you may need to log in again.

Session

This page displays the current session list and allows you to configure session settings.

The following fields are available on the session page:

- **Max session number:** Click the edit icon; then, enter the maximum number of sessions from 1 to 16.
- **WEB Session Timeout:** Choose a timeout value from the drop-down menu.
- **Disconnect:** Click **Disconnect** to terminate the selected session.

Chapter 8. Setting

Configure settings are used to manage the SMM3 module.

There are five pages:

- **User**
- **Network interface**
- **Network service**
- **Backup and restore**
- **Date and time**

User

Use the information in this topic to view or change the user settings.

This page lists all local user account, account policy configuration settings and allows you to add, edit, or delete users.

Available fields in this section include the following:

- **Account policy settings:** Account policy settings page allows you to set different values based on the following rules. See [“Account policy settings” on page 23](#) for more information.
- **Add User:** Click **Add User** to create a new user. See [“Add or Edit User” on page 24](#) for more information.
- **Edit User:** Click **Edit User** to change settings for this user. See [“Add or Edit User” on page 24](#) for more information.
- **Delete User:** Click **Delete User** on the row of the user that you wish to remove.

Account policy settings

Element	Behaviors	Default settings
Force to change password on first access	Check to enable this requirement.	Checked (Enabled)
IP address block for 300 seconds after 10 login failures	Check to enable this requirement.	Checked (Enabled)

Element	Behaviors	Default settings
Password Complex Rules	Value from 0-5. 0. Disable password complexity rule. 1. Contains at least one letter. 2. Contains at least one number. 3. Contain at least 2 of the following: (a) An upper case letter. (b) A lower case letter. (c) A special character.. 4. Cannot be a repeat or reverse of the corresponding username. 5. Contain at most 2 consecutive occurrences of the same character. Note: When a higher number of password complex rule is followed, all the preceding rules are also required to be automatically included.	4
Password expiration period	0~365 (days)	0
Password expiration warning period	0~365 (days)	0
Minimum password length	8~20 (characters)	10
Minimum password reuse cycle	0~10 (times)	5
Minimum password change interval	0~240 (hours)	1
Maximum number of login failures	0~10 (times)	5
Lockout period after maximum login failures	0~2880 (minutes)	60
Save	Save account policy settings.	

Add or Edit User

Note: You cannot modify the username and status of your own account.

Element	Behaviors
Account status	Manually enable or disable this account.
Privilege	Select from drop-down menu: • Administrator: Full access to all of the web pages and authorized to modify all of the settings and configurations. • Operator: Full access to all of the web pages except for the User page. Operator can only see his/her own account on the User page and no modification on the account page is allowed. • ReadOnly: The Read Only role can display server information but cannot perform operation that affects the state of the system, such as save, modify, clear, reboot, and update firmware.
Access Method	There are three options: • "IPMI" • "Redfish, WebUI" • "IPMI, Redfish, WebUI"
Password Complex Rules	Value from 0-5. • 0. Disable password complexity rule. • 1. Contains at least one letter. • 2. Contains at least one number. • 3. Contain at least 2 of the following: – (a) An upper case letter. – (b) A lower case letter. – (c) A special character.. • 4. Cannot be a repeat or reverse of the corresponding username. • 5. Contain at most 2 consecutive occurrences of the same character. Note: When a higher number of password complex rule is followed, all the preceding rules are also required to be automatically included.
User Password	Enter a password that matches the password complex rules.

Network interface

Use the information in this topic to view or change the network interface settings.

Click **Network interface** under **Setting** to modify System Management Module Ethernet settings.

The following network parameters can be modified in the **Network interface** section:

- ["General setting \(Hostname, DNS Domain Name, VLAN\)" on page 26](#)
- ["IPv4 configurations" on page 26](#)
- ["IPv6 configurations" on page 27](#)

General setting (Hostname, DNS Domain Name, VLAN)

Notes:

- Changing the network settings may change IP address settings.
- Each change to settings may cause a loss in connectivity and the termination of all sessions.
- Changes may not take effect immediately.
- Default settings for **General Settings**:
 - Dynamic DNS: Disabled
 - DHCP for DNS Domain Name: Disabled
 - Host-name = SMM3-[SMM3-MAC-ADDR]
 - Domain Name = lenovo.com
 - Enable VLAN = Disabled

Element	Behaviors
Dynamic DNS	Enable or disable dynamic DNS service. Changes take effect immediately.
DHCP for DNS Domain Name	Enable or disable DHCP for DNS Domain Name. Changes take effect immediately.
Hostname	SMM3 Hostname. Click Apply to update the configuration.
Domain Name	SMM3 Domain name. Click Apply to update the configuration.
Enable VLAN	There are two options: • Disable VLAN: Set by default. • Enable VLAN: Input the VLAN ID in the input box. Ensure that the input value must be within the specific range of 1 to 4095. Click “Apply” to update the configuration.

IPv4 configurations

Element	Behaviors
IP Source	There are three options: • First DHCP, then static IP address: Use address from DHCP server first, then static IP address. • Obtain IP from DHCP: Obtain an IP address from DHCP and display the assigned IPv4 address. • Use static IP address: Use a static IP address. Allows user to configure the “IPv4 Static Address”, “IPv4 Static Netmask”, and “IPv4 Static Gateway.”
• IPv4 Static Address • IPv4 Static Netmask • Ipv4 Static Gateway	IPv4 Static address configuration. • When IP Source is set to ‘First DHCP, then static IP address’ or ‘Obtain IP from DHCP’, display information assigned by the DHCP Server. • When IP Source is set to ‘Use static IP address’, allows user to edit for user configuration.

Element	Behaviors
DNS Source	There are two options: • DHCP: Display DNS address information obtained from the DHCP Server • Static: Display an input box allowing the user to configure the DNS address manually.
• DNS Server 1 • DNS Server 2	DNS Server configuration. • When DNS Source is set to 'DHCP', it will display the DNS server assigned by the DHCP Server. • When DNS Source is set to 'Static' these fields are editable for user configuration.
Apply	Save IPv4 configuration

IPv6 configurations

Element	Behaviors
IP Source	Click the checkbox to enable or disable the DHCP: • Enabled DHCP: Show IPV6 address information. • Disabled DHCP: Allows user to specify “IPv6 Static Address 1”, “IPv6 Static Address 2”, and “Default Gateway”. Click the checkbox to enable or disable the Stateless: • Disabled Stateless: When this checkbox is checked, the name will change to “Enabled Stateless” and show IPv6 address from DHCP Server. • Enabled Stateless: When this checkbox is checked, the name will change to “Disabled Stateless” and show stateless address.
Link Local Address	Show Link local address.
• IPv6 Static Address 1 • IPv6 Static Address 2	Specify an IPv6 address and prefix length information. Available format: [IPv6-Address]/[Prefix-length] Example: 2001::31/64 Note: need disable DHCP checkbox first
Default Gateway	Default gateway. Specify an available IPv6 address.
DNS Source	There are two options: • DHCP: Display DNS address information obtained from the DHCP Server • Static: Display an input box allowing the user to configure the DNS address manually.

Element	Behaviors
- DNS Server 1 - DNS Server 2	Configure IPv6 DNS Server IP. - When DNS Source is set to 'DHCP', it will display the DNS server assigned by the DHCP Server. - When DNS Source is set to 'Static' these fields are editable for user configuration.
Apply	Save IPv6 configuration

Network service

Use the information in this topic to view or change the network service settings.

The following network parameters can be modified in the **Network service** section:

- “[HTTPS Certificates](#)” on page 28
- “[Service and Port](#)” on page 29
- “[SMTP Server](#)” on page 29

HTTPS Certificates

Use Self-signed Certificate

- Click the “**Use Self-signed Certificate**” button to fill in the certification request information.
- Click the “**Self-signed Certificate**” button will use customized input data for certificate.

Notes:

- Uploading a certificate will restart the web service, leading to the termination of the current Web GUI session and temporary unavailability of the web server.
- You can import the certificate when the CA responds with a signed certificate. Importing certificates in PEM format is supported. You can convert your DER certificate to PEM format by `openssl x509 -inform der -in certificate.cer -out certificate.pem`. After the certificate has been imported, it is required to reconnect to the SMM3 web.

Generate Certificate Signing Request (CSR)

- Click the “**Generate CSR**” button to fill in the certification request information and download the CSR.
- Click the “**Generate CSR**” button will show the Certificate Signing Request (CSR) content.
- Click “**Download**” to download the content to file (default filename: certificate.csr), or click “**Copy**” to copy the content.

Note: Generating a self-signed certificate will restart the web service, leading to the termination of the current WebGUI session and temporary unavailability of the web server.

Replace certificate

- Click the “**Replace**” button, then click the “**Add file**” button to add a CA file.
- Click the “**Replace**” button to replace current selected certificate with the new certificate file.

Note: Uploading a certificate will restart the web service, leading to the termination of the current Web GUI session and temporary unavailability of the web server.

Service and Port

- **HTTPS Status:** Read-only switch. HTTPS service is always enabled.
- **IPMI Status:** Click the switch to enable or disable IPMI service.

SMTP Server

Element	Behaviors
SMTP server address	SMTP server address. Support IPv4 address.
Port	SMTP Port number.
SMTP encryption	SMTP encryption. After clicking, a dropdown menu will appear with options. • None • AutoDetect • StartTLS
SMTP authentication	SMTP authentication. After clicking, a dropdown menu will appear with options. • None • AutoDetect • Plain • Login • CRAM_MD5
Username	Access SMTP account username.
Password	Access SMTP account password. Note: Click the eye-icon to show the password in plain text.
Save	Save SMTP Server configuration.

Backup and Restore

You can backup or restore the configuration, that is encrypted or decrypted by user specific password, to or from a local device.

If a USB storage device is inserted and detected, it can be used for SMM3 to preserve user configurations. SMM3 only keeps the latest configuration file in the USB storage device for backup and restore.

Note: The storage device can be a USB device depending on the machine types. The storage capacity of the USB storage device should be higher than 1 GB. The support file system is FAT32.

The following actions can be performed in the “Backup and Restore” section:

- [“Backup SMM Configuration” on page 30](#)
- [“Restore SMM from Configuration File” on page 30](#)
- [“VPD” on page 30](#)
- [“Reset SMM to Factory Defaults” on page 30](#)

Backup SMM Configuration

Allows users to backup the following enclosure configurations to SMM USB storage or customer's storage space:

- Power supply redundancy policy
- Oversubscription mode
- Zero Output
- Enclosure capping/saving or compute node capping/saving.
- Power restores policy

Restore SMM from Configuration File

Allows users to restore and apply the configurations stored in a local device or USB storage device to SMM3. Make sure to insert the USB to SMM3 USB port in advance.

Note: Default password complexity rules: Must contain at least 8 letters

VPD

Provides users to backup or restore VPD information. Make sure to insert the USB to SMM3 USB port in advance. Click “Apply” button to complete.

Note: Default password complexity rules: Must contain at least 8 letters

Reset SMM to Factory Defaults

Restore the SMM3 to factory default settings.

You will lose all information and settings that are currently in the SMM, including: local users, network settings, power settings, events log, notification targets, imported certificates, etc. The SMM will restart automatically with factory default settings. You will have to reconnect to this SMM with a DHCP assigned IP address or the default address of 192.168.70.100. The login password will also be reset to factory default.

Notes:

- By pressing the hardware reset button for more than four seconds, all settings (except for **Time Setting**) can be restored to out-of-factory default settings.
- Only user with Administrator privilege can perform this function.
- When Ethernet connections are temporarily dropped, you must log in to the SMM to access the SMM web interface.
- When you use the **Reset SMM to Factory Defaults** option, you will lose all modifications that you have made to the SMM.

Date and time

Use the information in this topic to configure the SMM3 date and time.

- **Manual:** Specify the date and time directly.
- **NTP:** Synchronize the SMM3 clock with the specified NTP server.

Chapter 9. System Management Module 3 Redfish REST API

The System Management Module provides a Redfish compliant set of easy-to-use REST APIs that can be used to access System Management Module data and services from applications running outside of the System Management Module framework.

This allows for easy integration of System Management Module capabilities into other software, whether the software is running on the same system as the System Management Module server, or on a remote system within the same network. These APIs are based on the industry standard Redfish REST API and are accessed via the HTTPS protocol.

The System Management Module Redfish REST API user guide can be found here: <https://pubs.lenovo.com/smm3-restapi/>.

Lenovo provides open source sample Redfish scripts that can be used as reference for developing software that communicates with Lenovo Redfish REST API. These sample scripts can be found here:

- Python: <https://github.com/lenovo/python-redfish-lenovo>
- PowerShell: <https://github.com/lenovo/powershell-redfish-lenovo>

DMTF specifications related to the Redfish API are available at: <https://redfish.dmtf.org/>. This website provides general specifications and other reference material on the Redfish REST API.

Chapter 10. IPMI Command

The section includes information about IPMI commands.

Note: The IPMI via RMCP+ or RMCP is available through OOB communication via the physical interface, the Ethernet port.

Table 1. IPMI command list

NetFn	CMD	Name	NetFn	CMD	Name
0x32	0x90	"GET PCS COLLECTED DATA" on page 34	0x32	0xA9	"SET NODE RESTORE POLICY" on page 45
0x32	0x91	"GET PCS STATUS" on page 34	0x32	0xAA	"GET NODE RESTORE POLICY" on page 45
0x32	0x93	"GET CHASSIS MONITORING STATUS" on page 35	0x32	0xAB	"SET PCS ZERO OUTPUT MODE" on page 46
0x32	0x96	"GET SYS LED" on page 37	0x32	0xAC	"GET PCS ZERO OUTPUT MODE" on page 46
0x32	0x97	"SET SYS LED" on page 37	0x32	0xAD	"SMM3 RESET TO DEFAULT" on page 47
0x32	0x98	"GET NODE POWER READING" on page 38	0x32	0xAF	"SET VPD" on page 47
0x32	0x99	"GET NODE SIZE" on page 38	0x32	0xB0	"GET VPD" on page 49
0x32	0x9D	"GET CAP BOUNDARY" on page 38	0x32	0xB1	"FFDC DUMP" on page 49
0x32	0x9E	"SET CAPPING VALUE" on page 39	0x32	0xB2	"SET SMTP CONFIG PARAMETERS" on page 50
0x32	0x9F	"SET CAPPING STATE" on page 39	0x32	0xB3	"GET SMTP CONFIG PARAMETERS" on page 51
0x32	0xA0	"GET CAPPING STATE" on page 40	0x32	0xC3	"GET PCS DATA" on page 51

Table 1. IPMI command list (continued)

0x32	0xA1	"SET DATE TIME" on page 41	0x32	0xF0	"GET WEB STATE" on page 52
0x32	0xA2	"GET PCS POLICY OVS" on page 41	0x32	0xF1	"SET WEB STATE" on page 52
0x32	0xA4	"SET NODE RESET / RESEAT" on page 42	0x32	0xF5	"ENCLOSURE VIRTUAL RESEAT" on page 52
0x32	0xA5	"SET NODE RESET / RESEAT" on page 42	0x32	0xF6	"SET SYSTEM ENCLOSURE LRU" on page 52
0x32	0xA6	"BACKUP / RESTORE" on page 43	0x32	0xFA	"GET SECURITY OPTION" on page 53
0x32	0xA7	"GET NODE STATUS" on page 43	0x32	0xFB	"SET SECURITY OPTION" on page 54
0x32	0xA8	"GET SMM3 STATUS" on page 44			

IPMI Command Contents

The section provides detailed IPMI command contents.

GET PCS COLLECTED DATA

NetFn	0x32
CMD	0x90
Request data	Byte 1
Response data	- Byte 1 - Type - Byte [3:2] - Summary of minimum reading - Byte [5:4] - Summary of average reading - Byte [7:6] - Summary of maximum reading
Comments	[Request data] Byte 1 - Type 0x01 - AC-In 0x02 - PCS power consumption Note: The unit is 1 Joule.

GET PCS STATUS

NetFn	0x32
CMD	0x91

Request data	N/A
Response data	• Byte [2:1] - PCS EPOW • Byte [4:3] - PCS Throttle • Byte [6:5] - PCS Present • Byte [8:7] - PCS Power Good • Byte 9 - EPOW Out • Byte 10 - Throttle Out • Byte [12:11] - PCS Type • Byte [14:13] - Total Power Bank
Comments	[Response data] Bit [0:3] - For PCS 1 to 4 • 0b - Not trigger • 1b - Trigger

GET CHASSIS MONITORING STATUS

NetFn	0x32
CMD	0x93
Request data	N/A

Response data	• Byte 1 - Chassis Leakage Sensor Status • Byte 2 - Tray Leakage Sensor Present • Byte 3 - Tray Leakage Sensor Health • Byte 4 - Tray Leakage Sensor Alert • Byte 5 - Tray Spike Alert • Byte 6 - Tray PIB Power Fault • Byte 7 - PCS Leakage
Comments	[Response data] Byte 1 - Chassis Leakage Sensor Status • Bit 0: Present – 0b - Not trigger – 1b - Trigger • Bit 1: Health – 0b - Abnormal – 1b - Normal • Bit 2: Alert – 0b - Normal – 1b - Abnormal Byte 2 - Tray Leakage Sensor Present • 0b - Not Present • 1b - Present Byte 3 - Tray Leakage Sensor Health • 0b - Abnormal • 1b - Normal Byte 4 - Tray Leakage Sensor Alert • 0b - Normal • 1b - Leakage Byte 5 - Tray Spike Alert • 0b - Normal • 1b - Spike Alert Byte 6 - Tray PIB Power Fault • 0b - Normal • 1b - PIB Power Fault Byte 7 - PCS Leakage • 0b - Normal • 1b - Leakage

GET SYS LED

NetFn	0x32
CMD	0x96
Request data	N/A
Response data	• Byte 1 - ID LED for Enclosure • Byte 2 - Check Log LED
Comments	[Response data] Byte 1 - ID LED for Enclosure • 0x00 - Off • 0x01 - On • 0x02 - Blink • 0x03 - Accept mode - Off • 0x04 - Accept mode - On • 0x05 - Accept mode - Blink Byte 2 - Check Log LED • 0x00 - Off • 0x01 - On

SET SYS LED

NetFn	0x32
CMD	0x97
Request data	• Byte 1 - LED type • Byte 2 - Function
Response data	• Byte 1 - LED type • Byte 2 - Function
Comments	[Request data] Byte 1 - LED type • 0x01 - ID LED for the Enclosure Byte 2 - Function • 0x00 - Off • 0x01 - On • 0x02 - Blink Notes: • While the ID LED has been set to Off, SMM3 will enter the accept mode, in which the LED behavior is determined by the node ID LEDs. • When SMM3 receives various settings from XCC in the accept mode, the Blink will be given the highest priority over On and Off (Off will be given the lowest priority).

GET NODE POWER READING

NetFn	0x32
CMD	0x98
Request data	Byte 1 - Node number
Response data	- Byte 1 - Node number - Byte [3:2] - Compute node minimum power reading - Byte [5:4] - Compute node average power reading - Byte [7:6] - Compute node maximum power reading - Byte [9:8] - GPU node minimum power reading - Byte [11:10] - GPU node average power reading - Byte [13:12] - GPU node maximum power reading
Comments	[Request data] Byte 1 - Node number - For Tray 1 Node A: 0x1A ... - For Tray 8 Node B: 0x8B Notes: - The unit is 1 watt. - The chassis power reading is the summary of populated nodes.

GET NODE SIZE

NetFn	0x32
CMD	0x99
Request data	Byte 1 - Node number
Response data	- Byte 1 - Node number - Byte 2 - Node physical width - Byte 3 - Node physical height - Byte 4 - Add-on valid - Byte 5 - Add-on width - Byte 6 - Add-on height
Comments	[Request data] Byte 1 - Node number - For Tray 1 Node A: 0x1A ... - For Tray 8 Node B: 0x8B

GET CAP BOUNDARY

NetFn	0x32
CMD	0x9D
Request data	Byte 1 - Node number

Response data	• Byte 1 - Node number • Byte [3:2] - Minimum capping Value • Byte [5:4] - Maximum capping Value • Byte [7:6] - Protective Power capping Value • Byte [9:8] - User Power capping Value • Byte [11:10] - Thermal Power capping Value
Comments	[Request data] Byte 1 - Node number • For Chassis: 0x00 • For Tray 1 Node A: 0x1A ... • For Tray 8 Node B: 0x8B Notes: • The Power Capping will only be applied in OS-runtime. • The unit is 1 watt.

SET CAPPING VALUE

NetFn	0x32
CMD	0x9E
Request data	• Byte 1 - Node number • Byte [3:2] - Capping value
Response data	• Byte 1 - Node number • Byte [3:2] - Capping value
Comments	[Request data] Byte 1 - Node number • For Chassis: 0x00 • For Tray 1 Node A: 0x1A ... • For Tray 8 Node B: 0x8B Note: The unit is 1 watt.

SET CAPPING STATE

NetFn	0x32
CMD	0x9F
Request data	• Byte 1 - Node number • Byte 2 - Capping mode • Byte 3 - Saving mode

Response data	• Byte 1 - Node number • Byte 2 - Capping mode • Byte 3 - Saving mode
Comments	[Request data] Byte 1 - Node number • For Chassis: 0x00 • For Tray 1 Node A: 0x1A ... • For Tray 8 Node B: 0x8B Byte 2 - Capping mode • 0x00 - Disable • 0x01 - Enable Byte 3 - Saving mode • 0x00 - Disable Note: Byte 3 is reserved for backward compatible.

GET CAPPING STATE

NetFn	0x32
CMD	0xA0
Request data	• Byte 1 - Node number
Response data	• Byte 1 - Node number • Byte 2 - Capping mode • Byte [4:3] - Capping value • Byte 5 - Saving mode
Comments	[Request data] Byte 1 - Node number • For Chassis: 0x00 • For Tray 1 Node A: 0x1A ... • For Tray 8 Node B: 0x8B
	[Response data] Byte 2 - Capping mode • 0x00 - Disable • 0x01 - Enable Byte 5 - Saving mode • 0x00 - Disable • 0x01 - Enable

SET DATE TIME

NetFn	0x32
CMD	0xA1
Request data	• Byte [1:2] - Year • Byte 3 - Month • Byte 4 - Date • Byte 5 - Hour • Byte 6 - Minute • Byte 7 - Second
Response data	• Byte [1:2] - Year • Byte 3 - Month • Byte 4 - Date • Byte 5 - Hour • Byte 6 - Minute • Byte 7 - Second
Comments	[Request data] Example: 2037/12/31 23:59:59 • Byte 1 - 0x20 • Byte 2 - 0x37 • Byte 3 - 0x12 • Byte 4 - 0x31 • Byte 5 - 0x23 • Byte 6 - 0x59 • Byte 7 - 0x59

GET PCS POLICY OVS

NetFn	0x32
CMD	0xA2
Request data	N/A
Response data	• Byte 1 - PCS policy • Byte 2 - OVS mode
Comments	[Response data] Byte 1 - PCS policy • 0x00 - No redundant • 0x01 - N+1 policy • 0x02 - N+N policy Byte 2 - OVS mode • 0x00 - Disable • 0x01 - Enable

SET PCS POLICY OVS

NetFn	0x32																																	
CMD	0xA3																																	
Request data	- Byte 1 - PCS policy - Byte 2 - OVS mode																																	
Response data	- Byte 1 - PCS policy - Byte 2 - OVS mode	Note: <table border="1"> <thead> <tr> <th></th><th>1 PCS</th><th>2 PCS</th><th>3 PCS</th><th>4 PCS</th></tr> </thead> <tbody> <tr> <td>N+0</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr> <td>N+1</td><td>x</td><td>x</td><td>x</td><td>x</td></tr> <tr> <td>N+1 w/ OVS</td><td>x</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr> <td>N+N</td><td>x</td><td>x</td><td>x</td><td>x</td></tr> <tr> <td>N+N w/ OVS</td><td>x</td><td>x</td><td>x</td><td>✓</td></tr> </tbody> </table>				1 PCS	2 PCS	3 PCS	4 PCS	N+0	✓	✓	✓	✓	N+1	x	x	x	x	N+1 w/ OVS	x	✓	✓	✓	N+N	x	x	x	x	N+N w/ OVS	x	x	x	✓
	1 PCS	2 PCS	3 PCS	4 PCS																														
N+0	✓	✓	✓	✓																														
N+1	x	x	x	x																														
N+1 w/ OVS	x	✓	✓	✓																														
N+N	x	x	x	x																														
N+N w/ OVS	x	x	x	✓																														
Comments	[Request data] Byte 1 - System PCS policy 0x00 - No redundant 0x01 - N+1 policy 0x02 - N+N policy Byte 2 - System OVS mode 0x00 - Disable 0x01 - Enable Byte 3 - Status 0x00 - OK 0x01 - Present error 0x02 - Insufficient Bank Byte 4 - User PCS policy Byte 5 - User OVS mode																																	

SET NODE RESET / RESEAT

NetFn	0x32
CMD	0xA4
Request data	- Byte 1 - Node number - Byte 2 - Reset mode
Response data	- Byte 1 - Node number - Byte 2 - Reset mode
Comments	[Request data] Byte 1 - Node number - For Tray 1 Node A: 0x1A ... - For Tray 8 Node B: 0x8B Byte 2 - Reset mode - Reset (BMC reset) - Reseat (AC cycle) Note: The response D5h indicates the node is not present.

BACKUP / RESTORE

NetFn	0x32
CMD	0xA6
Request data	• Byte 1 - Action • Byte 2 - Password Length • Byte [3:N] - Password String
Response data	Byte 1 - Status
Comments	[Request data] Byte 1 - Action • 0x00 - Get backup or restore status • 0x01 - Backup to storage device • 0x02 - Restore from storage device Byte 2 - Password length Note: Support when Action is 0x01 or 0x02 Byte [3:N] - Password string Note: Support when Action is 0x01 or 0x02
	[Response data] Byte 1 - Status • 0x00 - COMMAND OK • 0x01 - BACKUP RESTORE RUNNING • 0x31 - BACKUP FINISHED • 0x32 - BACKUP FAIL • 0x41 - RESTORE FINISHED • 0x42 - RESTORE FAIL Notes: • This command is used to backup/restore configuration to/from an external storage device, such as USB dongle. The status will be fault when the storage device is not inserted. • When Request Action is 0x01/0x02, Password string must use a minimum of eight (up to 20) printable US-ASCII (Code: 33-126) characters and contain characters from three of the following four categories: – English uppercase characters (A through Z) – English lowercase characters (a through z) – Base 10 digits (0 through 9) – Non-alphabetic characters (for example, !, \$, #, %) Note: If the password validation fails, the command will reply 0xCC status code.

GET NODE STATUS

NetFn	0x32
CMD	0xA7

Request data	Byte 1 - Node number
Response data	• Byte 1 - Node number • Byte 2 - Power state • Byte 3 - Width • Byte 4 - Height • Byte 5 - Permission state
Comments	[Request data] Byte 1 - Node number • For Tray 1 Node A: 0x1A ... • For Tray 8 Node B: 0x8B Byte 2 - Power state • 0x00 - Permission to standby • 0x01 - First permission fail • 0x02 - Second permission fail • 0x03 - Permission pass • 0xFF - Initial not done

GET SMM3 STATUS

NetFn	0x32
CMD	0xA8
Request data	N/A
Response data	• Byte 1 - Platform ID • Byte 2 - Firmware Major Version • Byte 3 - Firmware Minor Version • Byte 4 - PSOC Patch Version • Byte 5 - FPGA Major Version • Byte 6 - FPGA Minor Version • Byte 7 - Boot Flash Number • Byte [8:14] - Firmware Build ID • Byte 15 - Minimum power supplies installed required
Comments	[Response data] Byte 1 - Platform ID • 0x00: For N1380 Byte 7 - Boot Flash Number • 0x01 - primary section • 0x02 - backup section Byte [8:14] - Firmware Build ID • Plain text in ASCII code. Byte 15 - Minimum power supplies installed required, 1~4

SET NODE RESTORE POLICY

NetFn	0x32
CMD	0xA9
Request data	• Byte 1: Tray 1 Restore Policy • Byte 2: Tray 2 Restore Policy • Byte 3: Tray 3 Restore Policy • Byte 4: Tray 4 Restore Policy • Byte 5: Tray 5 Restore Policy • Byte 6: Tray 6 Restore Policy • Byte 7: Tray 7 Restore Policy • Byte 8: Tray 8 Restore Policy
Response data	• Byte 1: Tray 1 Restore Policy • Byte 2: Tray 2 Restore Policy • Byte 3: Tray 3 Restore Policy • Byte 4: Tray 4 Restore Policy • Byte 5: Tray 5 Restore Policy • Byte 6: Tray 6 Restore Policy • Byte 7: Tray 7 Restore Policy • Byte 8: Tray 8 Restore Policy
Comments	[Request data] Byte N: Tray N Restore Policy • Bit [7:6]: Node D – 01b: Last state – 00b: Off • Bit [5:4]: Node C • Bit [3:2]: Node B • Bit [1:0]: Node A

GET NODE RESTORE POLICY

NetFn	0x32
CMD	0xAA
Request data	N/A

Response data	• Byte 1: Tray 1 Restore Policy • Byte 2: Tray 2 Restore Policy • Byte 3: Tray 3 Restore Policy • Byte 4: Tray 4 Restore Policy • Byte 5: Tray 5 Restore Policy • Byte 6: Tray 6 Restore Policy • Byte 7: Tray 7 Restore Policy • Byte 8: Tray 8 Restore Policy
Comments	[Response data] Byte N: Tray N Restore Policy • Bit [7:6]: Node D – 01b: Last state – 00b: Off • Bit [5:4]: Node C • Bit [3:2]: Node B • Bit [1:0]: Node A

SET PCS ZERO OUTPUT MODE

NetFn	0x32
CMD	0xAB
Request data	Byte 1 - User Output Mode
Response data	N/A
Comments	refer to “GET PCS ZERO OUTPUT MODE” on page 46. Note: If any power supply is not support or the power supplies are mismatched, the zero output mode will be disabled.

GET PCS ZERO OUTPUT MODE

NetFn	0x32
CMD	0xAC
Request data	N/A
Response data	• Byte 1 - User Output Mode • Byte 2 - Zero output status
Comments	[Response data] Byte 1 - User configuration • 0x00: Disable • 0x01: Update per 10 mins • 0x02: Update per 30 mins • 0x03: Update per 60 mins Byte 2 - Status • 0x00: Disable • 0x01: Zero output is running • 0x02: Zero output mode is deactivate

SMM3 RESET TO DEFAULT

NetFn	0x32
CMD	0xAD
Request data	N/A
Response data	Byte 1 - Status code
Comments	[Response data] Byte 1 - Status code • 0x00 - Running

SET VPD

NetFn	0x32
CMD	0xAD
Request data	• Byte 1 - VPD type • Byte 2 - Device ID • Byte [3:N] - VPD data

Response data	- Byte 1 - VPD type - Byte 2 - Device ID					
Comments	[Response data] Byte 1 - VPD type 0x00 - SMM3 0x05 - Enclosure 0x08 - Interposer Byte 2 - Device ID					
	Code	De-scrip-tion	Bytes	Enclo-sure	SMM3	Inter-poser
	0x00	Machine type Model	10 bytes	√		
	0x01	Machine serial Number	10 bytes	√		
	0x02	Compo-nent part Number	12 bytes	√	√	√
	0x03	Compo-nent FRU Number	12 bytes	√	√	√
	0x04	Compo-nent Serial Number	12 bytes	√	√	√
	0x05	Manu-facture ID	4 bytes	√	√	
	0x06	Hard-ware Revision Level	1 byte		√	√
	0x07	Manu-facture Date	4 bytes	√	√	√
	0x08	UUID	16 bytes	√	√	√
	0x09	IANA Enter-prise Number	4 bytes	√		
	0x0A	Product ID	2 bytes	√		
	0x0B	Compo-nent Name	11 bytes	√		

	0x0C	GLID	11 bytes	√		
	0x0D	EC Level	10 bytes	√	√	√

GET VPD

NetFn	0x32
CMD	0xB0
Request data	- Byte 1 - VPD type - Byte 2 - Device ID
Response data	- Byte 1 - VPD type - Byte 2 - Device ID - Byte [3:N] - VPD data
Comments	Refer to “SET VPD” on page 47 .

FFDC DUMP

NetFn	0x32
CMD	0xB1
Request data	- Byte 1 - Function - Byte [2:N] - Data (option)
Response data	Byte 1 - Status
Comments	[Request data] Byte 1 - Function 0x00: Query status 0x01: FFDC dump to TFTP Server. 0x02: FFDC dump to USB. Byte [2:N] - Data (option) - For TFTP server only: ASCII string of TFTP server address and path, separated by “/”. The path can be empty.

	[Response data] Byte 1 - Status - For Query Status: 0x00: Finished 0x01: Running 0x02: Reserved 0x03: No USB 0x04: Tar fail 0x0E: Upload fail 0x0F: TFTP server not found - For FFDC dump to TFTP Server: 0x00 - Done - For FFDC dump to USB: 0x00 - Done Note: The maximum length of the field is 64 characters. Follow steps illustrate how to dump FFDC over IPMI: - Run FFDC dump to TFTP server: Set TFTP server address where the IP is in HEX, the example below is set TFTP server address as 192.168.1.1. <pre>ipmitool -H SMM3_IP -U USERID -P PASSWORD -I lanplus raw 0x32 0xB1 0x01 0x31 0x39 0x32 0x2E 0x31 0x36 0x38 0x2E 0x31 0x2E 0x31</pre> - Query FFDC dump status: <pre>ipmitool -H SMM3_IP -U USERID -P PASSWORD -I lanplus raw 0x32 0xB1 0x00</pre> - Run FFDC dump to USB: <pre>ipmitool -H SMM3_IP -U USERID -P PASSWORD -I lanplus raw 0x32 0xB1 0x02</pre> Note: The FFDC log file name is SMM3-MAC_addr-FFDC-YYYY-MM-DD-HHMMSS.tgz
--	--

SET SMTP CONFIG PARAMETERS

NetFn	0x32
CMD	0xB2
Request data	- Byte 1 - Parameter selector - Byte [2:N] - Data
Response data	- Byte 1 - Parameter selector - Byte [2:N] - Data
Comments	Refer to Table - “SMTP Configuration Parameters” on page 54 for Parameter Selector and Data.

GET SMTP CONFIG PARAMETERS

NetFn	0x32
CMD	0xB3
Request data	- Byte 1 - Parameter selector - Byte 2 - Set selector - Byte 3 - Block selector
Response data	- Byte 1 - Parameter selector - Byte [2:N] - Data
Comments	[Request data] Byte 2 - Set Selector 0x00: Parameter doesn't require a Set Selector. Byte 3 - Block Selector 0x00: Parameter doesn't require a Block Selector. Note: Refer to Table - "SMTP Configuration Parameters" on page 54 for parameter/set/block selectors and data.

GET PCS DATA

NetFn	0x32
CMD	0xC3
Request data	Byte 1 - PCS number
Response data	- Byte 1 - PCS number - Byte [3:2] - Fan A speed - Byte [5:4] - Fan B speed - Byte [7:6] - VIN - Byte [9:8] - PCS type
Comments	[Request data] Byte 1 - PCS number - For N1380 Enclosure - PCS 1 ~ 4: 0x01 ~ 0x04
	[Response data] Byte [3:2] - Reserved Byte [5:4] - Reserved Byte [7:6] - VIN - The unit is 1 voltage. Byte [9:8] - PCS type - The unit is 1 watt. Note: Fan B speed will be 0x00 for single fan PCS.

GET WEB STATE

NetFn	0x32
CMD	0xF0
Request data	N/A
Response data	Byte 1 - State
Comments	[Response data] Byte 1 - State • 0x00 - Disabled • 0x01 - Enabled

SET WEB STATE

NetFn	0x32
CMD	0xF1
Request data	Byte 1 - State
Response data	Byte 1 - State
Comments	[Request data] Byte 1 - State • 0x00 - Disabled • 0x01 - Enabled

ENCLOSURE VIRTUAL RESEAT

NetFn	0x32
CMD	0xF5
Request data	N/A
Response data	Byte 1 - Status
Comments	[Response data] Byte 1 - Status • 0x00 - Proceeding

SET SYSTEM ENCLOSURE LRU

NetFn	0x32
CMD	0xF6
Request data	• Byte 1 - Function • Byte 2 - LRU

Response data	• Byte 1 - Function • Byte 2 - Current LRU • Byte 3 - Previous LRU (Option for Read)
Comments	[Request data] Byte 1 - Function • 0x00 - Write • 0x01 - Read Byte 2 - LRU • Enclosure LRU

GET SECURITY OPTION

NetFn	0x32
CMD	0xFA
Request data	Byte 1 - Type
Response data	• Byte 1 - Type • Byte 2 - Setting • Byte 3 - Setting (option)
Comments	[Request data] Byte 1 - Type • 0x00 - Minimum password length • 0x01 - Force user to change password on first access • 0x02 - Password expiration period (in days) • 0x03 - Password expiration warning period (in days) • 0x04 - Minimum password change interval (in hours) • 0x05 - Minimum password reuse cycle • 0x06 - Maximum number of login failures • 0x07 - Lockout period after maximum login failures (in minutes) • 0x08 - Enable IP address block for 300 seconds after 10 login failures • 0x09 - Password Complexity Rule • 0x0A - Enable Secure Rollback Byte 2 - LRU • Enclosure LRU

	[Response data] Byte 3 - Configuration setting (option) • MSB for two bytes data Byte 2 - LRU • Enclosure LRU Notes: • Password Complexity Rules: (Rules should be enabled starting with rule 1, and up to the number of rules specified) 0x00: Password Complexity Rules disabled. – 0x00 - Password Complexity Rules disabled. – 0x01 - contains at least one letter – 0x02 - contains at least one number – 0x03 - contains at least two of the following: – An uppercase letter – A lowercase letter – A special character: !@#\$%^*_+=().:~'<>/[]{}; – 0x04: Cannot be a repeat or reverse of the corresponding user-name – 0x05: May contain at most 2 consecutive occurrences of the same character • Password does not allow white-space and the special characters below: ~'<>/[]{};
--	--

SET SECURITY OPTION

NetFn	0x32
CMD	0xFB
Request data	• Byte 1 - Type • Byte 2 - Setting • Byte 3 - Setting (option)
Response data	• Byte 1 - Type • Byte 2 - Setting • Byte 3 - Setting (option)
Comments	Refer to “GET SECURITY OPTION” on page 53.

SMTP Configuration Parameters

The below table is detail parameters for [“SET SMTP CONFIG PARAMETERS” on page 50](#) and [“GET SMTP CONFIG PARAMETERS” on page 51.](#)

Sender Information

Parameter selector	#	Parameter data (non-volatile)
Sender Information	0	Assigns the send from. The field is default filled with <host name>@<domain name> automatically. If the field is OEM set, it must follow the following rules: 1. It must not consist of only space characters. 2. It must be the combination of alphanumeric characters a-z, A-Z and 0-9,space characters, non-alphabetic characters. 3. The maximum length of the field is 254 characters. • Data 1: String length • Data [2:N]: The sting of <host name>@<domain name>

Destination Email Addresses

Parameter selector	#	Parameter data (non-volatile)
Destination Email Addresses	1	Data 1: Set selector = Field selector, 0 based. • [7:2] - Reserved • [1:0] - Field selector – 00b - Field 1 - Enable/Disable – 01b - Field 2 - Destination Email Address – 10b - Field 3 - Email Description – 11b - Field 4 - Send Alert (Set only) Data 2: Block selector = Target of Email Alert selector, 0 based. • [7:2] - Reserved • [1:0] - – 00b - Email Alert 1 – 01b - Email Alert 2 – 10b - Email Alert 3 – 11b - Email Alert 4 Set selector = 0 • Data 3: – [7:1] - Reserved – [0] - – 0b - Disable – 1b - Enable Set selector = 1 • Data 3: String length, Max = 64. • Data [4:N]: The sting of Destination Email Address Set selector = 2 • Data 3: String length, Max = 254. • Data [4:N]: The sting of Email Description.

SMTP (email) Server Settings

Parameter selector	#	Parameter data (non-volatile)
SMTP (email) Server Settings	2	Data1: Set selector = Field selector, 0 based. • [7:1] - Reserved • [0] - Field selector – 0b - Field 1 - SMTP IP Address – 1b - Field 2 - SMTP Port Number Set selector = 0 • Data 2: String length, Max = 254. • Data [3:N]: The sting of IPV4, IPV6 or FQDN. Set selector = 1 • Data [2:3]: Port number. LS-byte first.

SMTP Authentication

Parameter selector	#	Parameter data (non-volatile)
SMTP Authentication	3	Data 1: Set selector = Field selector, 0 based. • [7:3] - Reserved • [2:0] - Field selector – 000b - Field 1 - Username – 001b - Field 2 - Password (set only) – 010b - Field 3 - STARTTLS Mode – 011b - Field 4 - SASL Mode – 100b - 111b - Reserved Set selector = 0 • Data 2: – [7:1] - Reserved – [0] - – 0b - Disable – 1b - Enable Set selector = 1 • Data 2: String length, Max = 254. • Data [3:N]: The sting of Username. Set selector = 2 • Data 2: String length, Max = 254. • Data [3:N]:The sting of Password. Set selector = 3 • Data 2: – [7:2] - Reserved – [1:0] - – 00b - AUTO – 01b - OFF – 10b - ON – 11b - Reserved Set selector = 4 • Data 2: – [7:3] - Reserved – [2:0] - – 000b - NONE – 001b - AUTO – 010b - PLAIN – 011b - LOGIN – 100b - MD5 – 101b - 111b - Reserved

Parameter in IPMI Command

The section includes information about parameters in IPMI commands.

Table 2. List of parameters in IPMI commands

NetFn	CMD	Name	Parameter	Parameter name
0x0C	0x01	SET LAN CONFIG PARAM	0xC3	Host name
			0xC4	Domain name
			0xC5	DHCP option 12
			0xC6	DHCP option 60
	0x02	GET LAN CONFIG PARAM	0xC3	Host name
			0xC4	Domain name
			0xC5	DHCP option 12
			0xC6	DHCP option 60

Parameter in IPMI Command Contents

The section provides detailed parameters in IPMI command contents.

SET LAN CONFIG PARAM

NetFn	0x0C
CMD	0x01
Request data	- Byte 1 - Channel number - Byte 2 - Parameter Selector - Byte [3:N] - Configuration Parameter
Response data	Byte 1 - Completion Code
Comments	[Request data] Byte 2 - Parameter Selector Byte [3:N] - Configuration Parameter Refer to Table - “IPMI Parameter - LAN Configuration Parameters” on page 59.
	[Response data] Byte 1 - Completion Code 0x80: Parameter not supported. 0x81: Attempt to set the ‘set in progress’ value when not in the ‘set complete’ state. 0x82: Attempt to write read-only parameter. 0x83: Attempt to read write-only parameter.

GET LAN CONFIG PARAM

NetFn	0x0C
CMD	0x02

Request data	• Byte 1 - Channel number • Byte 2 - Parameter Selector • Byte 3 - Set Selector • Byte 4 - Block Selector
Response data	• Byte 1 - Completion Code • Byte 2 - Parameter Revision • Byte [3:N]: Configuration Parameter
Comments	[Request data] Byte 2 - Parameter Selector • Refer to Table - “IPMI Parameter - LAN Configuration Parameters” on page 59. Byte 3 - Set Selector • 0x00: if parameter doesn’t use a set selector. Byte 4 - Block selector • 0x00: if parameter doesn’t use a block selector.

IPMI Parameter - LAN Configuration Parameters

The following table provides detailed IPMI parameters in LAN configuration.

Table 3. IPMI parameters - LAN configuration parameters

Parameter selector	#	Parameter data (non-volatile)
Address Source	0x04	IP address source Byte 1 - Obtain IP address method • 0x01: Static IP address • 0x02: DHCP only • 0x04: First DHCP, then static IP address
Host Name	0xC3	BMC hostname • Byte 1: String length, maximum is 63. • Byte [2:N]: The plain string of BMC hostname.
DNS Domain Name	0xC4	DNS Domain Name. Set operation implicates using static for DNS Domain Name. Note: The setting of “Use DHCP for DNS Domain Name” will be disabled • Byte 1: String length, maximum is 237. • Byte [2:N]: The plain string of DNS Domain name.
DHCP Send Hostname Option	0xC5	Byte 1: • 0x00 - Disabled • 0x01 - Enabled
DHCP Send Vendor Class Information Option	0xC6	Byte 1: • 0x00 - Disabled • 0x01 - Enabled

Index

C

Configuration 23

E

enclosure
 VPD 15
Enclosure 22
enclosure VPD 15
Event
 Log 11
Event Log 11

F

Firmware 21

G

GET_SMTP_CONFIG_PARAMETERS 54

I

IPMI Command 33, 58
IPMI command contents 34, 58

L

LAN configuration parameters 59

N

Network 25
Network service 28

O

Operations 21
Overview 6

P

power
 consumption 19
Power 19
Power consumption overview 19
PSU
 Configuration 19
PSU Configuration 19

S

server power 19
Session 22
SET_SMTP_CONFIG_PARAMETERS 54
SMM 22
SMM3
 Recovery 29
SMM3 Recovery 29
SMTP Configuration Parameters 54
System Management Module
 web interface 3

U

Update 21
User 23

W

web interface, opening and using 3

