



J4108-01-35X

**4U108 12G JBOD
User's Manual**

Table of Contents

Preface	i
Safety Instructions	ii
About This Manual	iv
Chapter 1. Product Features	1
1.1 Box Contents	1
1.2 Specifications	2
1.3 Feature	2
Chapter 2. Hardware Setup	7
2.1 Top Cover	7
2.1.1 Installing/Removing the Top Cover A & B	8
2.1.2 Installing/Removing the Top Cover C & D	9
2.2 Disk Drive	10
2.2.1 Installing the Hard Disk Drive	10
2.2.2 Removing the HDD from the Tray	11
2.2.3 Installing the 2.5" Hard Disk Drive (Optional)	12
2.2.4 Installing/Removing the HDD Tray	13
2.3 Fan Module	14
2.3.1 Installing the Fan	14
2.3.2 Removing the Fan	14
2.4 Drive Backplane Module	15
2.4.1 Installing the HDD Backplane	15
2.4.2 Removing the HDD Backplane	15
2.5 Power Supply Unit Module	17
2.5.1 Installing the Power Supply Unit	17
2.5.2 Removing the Power Supply Unit	17
2.6 Expander Module	18
2.6.1 Installing the Expander	18
2.6.2 Removing the Expander	18
2.7 Cable Cover	19
2.7.1 Installing the Cable Cover	19
2.7.2 Removing the Cable Cover	19
2.8 Bridge Board Module	20
2.8.1 Installing the Bridge Board	20
2.8.2 Removing the Bridge Board	20
2.9 Rear Handle	21
2.9.1 Installing the Rear Handle	21
2.9.2 Removing the Rear Handle	21
2.10 Slide Rail	22
2.11 Standard Cabling	24
2.11.1 Single expander JBOD and 1 host server with 1 HBA card	24
2.11.2 Dual expander JBOD and 1 host server with 2 HBA cards	24
2.11.3 Dual expander JBOD and 2 host servers with 1 HBA card each	25
Chapter 3 Sub-system Configuration Setup	26
3.1 Supported Configuration and Unsupported Feature	26
3.1.1 Supported Configuration	26
3.1.2 Unsupported Feature	26
Chapter 4. BMC Configuration Settings	27
4.1 Login	27

4.2 Sensor's Location for Fan and Temperature	31
4.3 Expander Setting via Java SOL	32
4.3.1 Java SOL.....	32
4.3.2 Configure Serial Command Line Interface	37
4.3.2.1 How to enable/disable T10 zoning.....	37
4.3.2.2 How to configure T10 zoning.....	37
4.3.2.3 How to get all revisions in AIC® SAS 12G Expander	43
4.3.2.4 How to configure enclosure address (HUB only)	43
4.3.2.5 How to configure standby timer for all disk drives(EDGE only).....	43
4.3.2.6 How to configure wide port checker	44
4.3.2.7 How to power off/on all disk drives automatically.....	44
4.3.2.8 How to configure EDFB (EDGE only)	44
4.3.2.9 How to configure power setting (HUB only)	45
4.3.2.10 How to configure zone count	45
4.3.2.11 How to configure zoning of the wide port (HUB only)	51
4.3.2.12 How to configure zoning of the disk slot (EDGE only)	51
4.3.3 SES Inband Features.....	52
4.3.3.1 SES Pages.....	52
4.3.3.2 SES Elements.....	52
4.3.3.3 Implementation on SES Pages	53
4.3.3.4 Implementation on SES Elements	55
4.3.3.5 SES Element Control Functions.....	63
4.4 Web UI for AST2520	77
4.4.1 User Name and Password	77
4.4.2 Menu Bar.....	78
4.4.3 Quick Button and Logged-in User.....	79
4.4.4 Dashboard	80
4.4.5 Sensor	81
4.4.5.1 Sensor Detail.....	82
4.4.6 FRU Information	83
4.4.7 Logs & Reports	85
4.4.7.1 IPMI Event Log.....	86
4.4.7.2 Audit Log.....	87
4.4.8 Settings.....	88
4.4.8.1 Date & Time.....	89
4.4.8.2 Log Settings	90
4.4.8.3 Network Settings	93
4.4.8.4 Platform Event Filter.....	99
4.4.8.5 Services.....	108
4.4.8.6 SMTP Settings	111
4.4.8.7 System Firewall	114
4.4.8.8 User Management	123
4.4.8.9 Power Restore Policy	128
4.4.8.10 Zone Configurations.....	129
4.4.9 Remote Control	130
4.4.10 HDD Management.....	131
4.4.11 Power Control.....	132
4.4.12 Maintenance Group.....	133
4.4.12.1 Backup Configuration.....	134
4.4.12.2 Firmware Image Location	135

4.4.12.3 BMC Firmware Information	136
4.4.12.4 BMC Firmware Update	137
4.4.12.5 Preserve Configuration	143
4.4.12.6 Restore Configuration	145
4.4.12.7 Expander Update	147
4.4.12.8 BMC Reset	149
4.4.13 Sign Out	150
4.5 Web UI for AST1250	151
4.5.1 Dashboard	151
4.5.2 FRU information	152
4.5.3 Hard Disk Status	153
4.5.4 Storage Health.....	154
4.5.4.1 Sensor Readings.....	154
4.5.4.2 Event Log.....	155
4.5.5 Configuration.....	156
4.5.5.1 DNS.....	156
4.5.5.2 Network Settings	158
4.5.5.3 Network Link.....	160
4.5.5.4 NTP.....	161
4.5.5.5 PEF	162
4.5.5.6 SMTP	163
4.5.5.7 Schedule Power ON/OFF	165
4.5.5.8 User	166
4.5.6 Remote Control	167
4.5.6.1 Storage power control.....	167
4.5.6.2 Zone Setting.....	168
4.5.7 Maintenance Control.....	170
4.5.7.1 Preserve Configuration	170
4.5.7.2 Restore Configuration	174
4.5.8 BMC Firmware Update.....	176
4.5.8.1 Requirement.....	176
4.5.8.2 Web update.....	176
4.5.8.3 Image Transfer Protocol	182
4.5.9 Expander Firmware/MFG Update.....	183
Chapter 5. Technical Support	191



Copyright © 2018 AIC®, Inc. All Rights Reserved.

This document contains proprietary information about AIC® products and is not to be disclosed or used except in accordance with applicable agreements.

Document Release History

Release Date	Version	Update Content
July, 2018	1	Release to public.
October, 2018	1.1	1. Update BMC 2. Update Java Sol 3. New cover
March, 2019	1.2	Update Slide Rail QIG
October, 2019	1.3	Update slide rail.
December, 2019	1.6	BMC update
February, 2020	1.7	BMC Expander update
April, 2020	1.8	BMC Expander update
May, 2020	2	BMC update
May, 2021	2.1	Fan sensor update
June, 2021	2.2	BMC update
January, 2022	2.3	Datasheet spec update
April, 2022	2.4	BMC Section 4.3.2.8 update
December, 2022	2.5	Add Standard cabling and T10 zoning NOTE.
July, 2024	2.6	Update specification content (AC input).
October, 2024	2.7	Add 3.5" HDD removal info.
June, 2025	2.8	Update front panel and add 8644 LED indicator.
October, 2025	2.9	Add Zone Count 3 information.
June, 2026	3	Update BMC content: 4.1/4.3.1/4.3.4, add 4.7 section.
August, 2026	3.1	Add 4.4.8.5 Services NOTE.

Preface

Copyright

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photo-static, recording or otherwise, without the prior written consent of the manufacturer.

Trademarks

All products and trade names used in this document are trademarks or registered trademarks of their respective holders.

Changes

The material in this document is for information purposes only and is subject to change without notice.

Warning

1. A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.
2. Use only shielded cables to connect I/O devices to this equipment.
3. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Disclaimer

AIC® shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither AIC® or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice.

Instruction Symbols

Special attention should be given to the instruction symbols below.



NOTE

This symbol indicates that there is an explanatory or supplementary instruction.



CAUTION

This symbol denotes possible hardware impairment. Upmost precaution must be taken to prevent serious hardware damage.



WARNING

This symbol serves as a warning alert for potential body injury. The user may suffer possible injury from disregard or lack of attention.

Safety Instructions

Before getting started, please read the following important cautions:

- All cautions and warnings on the equipment or in the manuals should be noted.
- Most electronic components are sensitive to electrical static discharge. Therefore, be sure to ground yourself at all times when installing the internal components.
- Use a grounding wrist strap and place all electronic components in static-shielded devices. Grounding wrist straps can be purchased in any electronic supply store.
- Be sure to turn off the power and then disconnect the power cords from your system before performing any installation or servicing. A sudden surge of power could damage sensitive electronic components.
- Do not open the system's top cover. If opening the cover for maintenance is a must, only a trained technician should do so. Integrated circuits on computer boards are sensitive to static electricity. Before handling a board or integrated circuit, touch an unpainted portion of the system unit chassis for a few seconds. This will help to discharge any static electricity on your body.
- Place this equipment on a stable surface when install. A drop or fall could cause injury.
- Please keep this equipment away from humidity.
- Carefully mount the equipment into the rack, in such manner, that it won't be hazardous due to uneven mechanical loading.
- This equipment is to be installed for operation in an environment with maximum ambient temperature below 35°C.
- The openings on the enclosure are for air convection to protect the equipment from overheating. DO NOT COVER THE OPENINGS.
- Never pour any liquid into ventilation openings. This could cause fire or electrical shock.
- Make sure the voltage of the power source is within the specification on the label when connecting the equipment to the power outlet. The current load and output power of loads shall be within the specification.
- This equipment must be connected to reliable grounding before using. Pay special attention to power supplied other than direct connections, e.g. using of power strips.
- Place the power cord out of the way of foot traffic. Do not place anything over the power cord. The power cord must be rated for the product, voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product.
- If the equipment is not used for a long time, disconnect the equipment from mains to avoid being damaged by transient over-voltage.
- Never open the equipment. For safety reasons, only qualified service personnel should open the equipment.

- If one of the following situations arise, the equipment should be checked by service personnel:
 1. The power cord or plug is damaged.
 2. Liquid has penetrated the equipment.
 3. The equipment has been exposed to moisture.
 4. The equipment does not work well or will not work according to its user manual.
 5. The equipment has been dropped and/or damaged.
 6. The equipment has obvious signs of breakage.
 7. Please disconnect this equipment from the AC outlet before cleaning. Do not use liquid or detergent for cleaning. The use of a moisture sheet or cloth is recommended for cleaning.
- Module and drive bays must not be empty! They must have a dummy cover.

**CAUTION**

The equipment intended for installation should be placed in Restricted Access Location.

**CAUTION**

This unit may have more than one power supply. Disconnect all power sources before maintenance to avoid electric shock.



About This Manual

Thank you for selecting and purchasing J4108-01-35X.

This user's manual is provided for professional technicians to perform easy hardware setup, basic system configurations, and quick software startup. This document pellucidly presents a brief overview of the product design, device installation, and firmware settings for J4108-01-35X. For the latest version of this user's manual, please refer to the AIC® website: <https://www.aicipc.com/en/productdetail/40912>.

Chapter 1 Product Features

J4108-01-35X is an ideal SAS JBOD that is specifically designed to accommodate diverse corporations and enterprises who pursue flexibility, easy control, and density in external or backup storage. This product supports hot swap designs and is easily deployed for your benefit.

Chapter 2 Hardware Setup

This chapter displays an easy installation guide for assembling the main components of the JBOD. Utmost caution for proceeding to set up the hardware is highly advised. Do not endanger yourself by placing the device in an unstable environment. The consequences for negligent actions may be extremely severe.

Chapter 3 Sub-system Configuration Setup

This chapter provides details about the supported features and unsupported configurations about your host(s) and expander controller connection.

Chapter 4 BMC Configuration Settings

This chapter illustrates the diverse functions of IPMI BMC, including the details on logging into the web page and assorted definitions. These descriptions are helpful in configuring various functions through Web GUI without entering the BIOS setup.

Chapter 5 Technical Support

For more information or suggestion, please contact the nearest AIC® corporation representative in your district or visit the AIC® website: <http://www.aicipc.com/en/index>. It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

J4108-01-35X is a high performance JBOD product that includes 108 x 3.5" hot swap drive bays and single/dual expander module(s). For more information about our product, please visit our website at <http://www.aicipc.com/en/index>.

Before removing the subsystem from the shipping carton, visually inspect the physical condition of the shipping carton. Exterior damage to the shipping carton may indicate that the contents of the carton are damaged. If any damage is found, do not remove the components; contact the dealer where the subsystem was purchased for further instructions. Before continuing, first unpack the subsystem and verify that the number of components in the shipping carton is accurate and in good condition.

1.1 Box Contents

This product contains the components listed below.
Please confirm the number and the condition of the components before installation.

- Enclosure
(includes power supply, fan
& hard disk drive tray)
- Power cord (vary per region)
- Rear handle (uninstalled)
- Slide rail x 1 set

PACKAGE CONTENT MAY VARY PER REGION.

1.2 Specifications

General	Number of Expander	Single/Dual	Electrical and Environmental	AC Input	Platinum: 200-240Vac , 50/60Hz, 15A (2000W) Titanium: 200-240Vac , 50/60Hz, 10A (2000W)
	Expander Chip	Broadcom SAS35X48			
	Host/Expansion Interface	4 x Mini SAS HD (SFF-8644) per expander module		Operating Environment	• Temperature : 0°C to 35° C • Relative humidity : 20% to 80 %
Drives Supported	Drive Interface	• 12Gb & 6Gb SAS if using dual expanders • 12Gb & 6Gb SAS/SATA if using single expander		Non-operating Environment	• Temperature : -20°C to 60° C • Relative humidity : 10% to 90 %
	Form Factor	3.5"			
Administration / Management	Admin/Firmware Upgrade	• In-band • IEM port	Physical Specification	Dimensions (W x D x H)	mm : 434 x 1050 x 176 434 x 1273 x 176 (with CMA)
	LED Indicators, Audible Alarm	Yes			inches : 17 x 41 x 7 17 x 50 x 7 (with CMA)
Hot swap and Redundancy	Drive Bays	108		Gross Weight (w/ PSU, Rail and Pallet; w/o Disks)	kgs : 66.97 lbs : 147.6
	Cooling	• 8 x 60x56mm hot swap fans • 1 x 40x56mm fan per expander module		Packaging Dimensions (W x D x H)	mm : 640 x 1380 x 526
	Power Supply	• 2000W 1+1 hot swap redundant 80+ Platinum (with C20 power plug) • 2000W 1+1 hot swap redundant 80+ Titanium (with C14 power plug)			inches : 25.2 x 54.3 x 20.7
	Power Entry	Dual AC Inlet	Mounting	Standard	41" slide rail
	Expander Modules	Dual SAS topology (Optional)		Option	Cable Management Kit

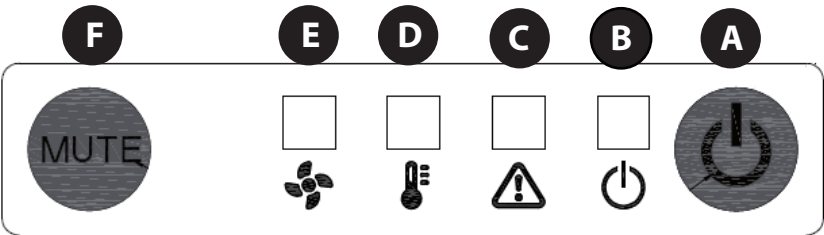
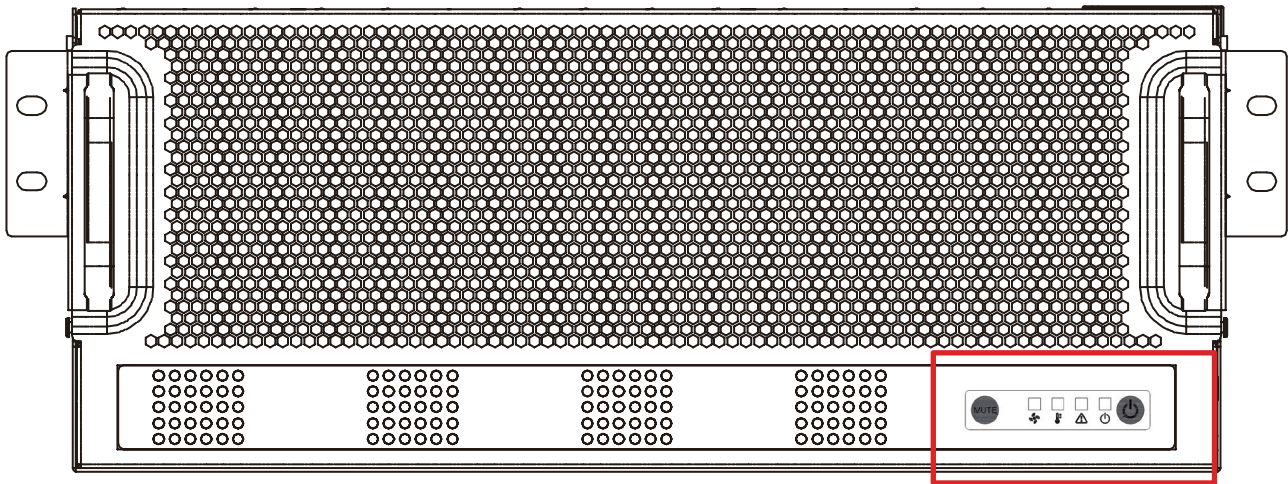
1.3 Feature

J4108-01-35X is a reliable SAS JBOD with 108 hot swap drives bays. This product is designed to accommodate single/dual hub expanders with 4 Mini SAS HD wide ports. Featuring the expander chip, Broadcom SAS35x48, which is underscored for its high scalability and performance of supporting up to 12 Gb/s, this product enhances these features by integrating hot swap designs, redundant fans, and expansion to offer easy control and high performance for our customers.

- Near-line Database Expansion Storage
- High Performance Direct Attached Storage for HPC or Application Server
- Virtual Tape Library
- Multimedia on Demand
- Online E-mail Storage
- Local Storage for Video Post-productions
- Digital Content Source Database Storage
- Private / Public Cloud Expansion

Front Panel

J4108-01-35X offers 2 system buttons (System Power switch & System Alert Mute switch) and 4 LED indicators (Power, Power Fail, Temperature (overheating), and Fan Fault).



A	System Power	
	Behavior	Status
	Normal	Off
	Press	Boot up
	Long Press	System shut down

B	Power LED	
	Behavior	Status
	On	Blue
	Off	No status

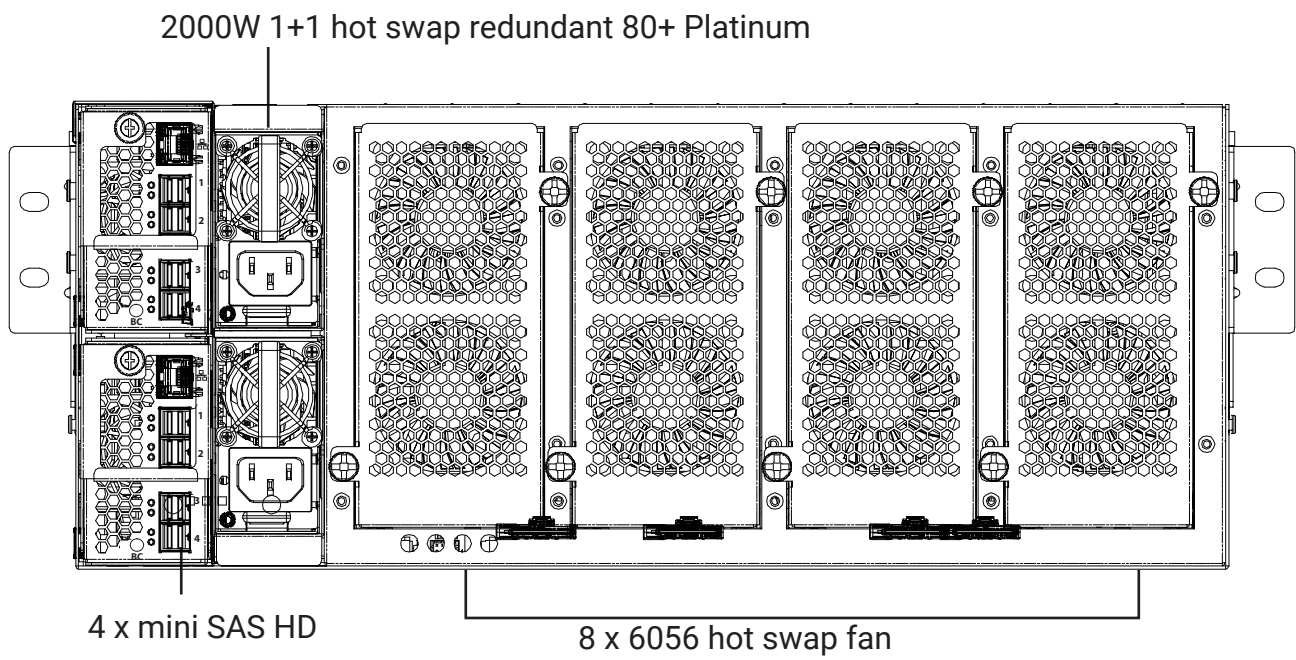
C	Power Fail LED	
	Behavior	Status
	Normal	Off
	Failed	Red

D	Temperature (Overheating) LED	
	Behavior	Status
	Normal	Off
	Failed	Red

E	Fan Fault LED	
	Behavior	Status
	Normal	Off
	Failed	Red

F	System Alert Mute Switch	
	Behavior	Status
	Normal	Off
	Press	Alert mute

Rear Panel

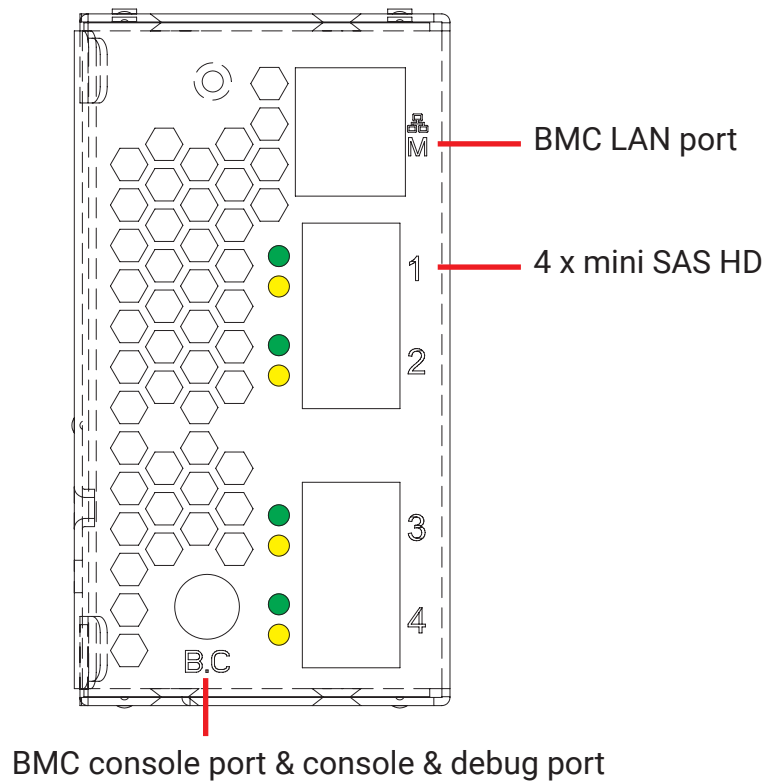


NOTE

The power supply only supports 200V~240V input.

Rear Expander Panel

J4108-01-35X offers single/dual expander(s) with 1 BMC console/debug port and 4 mini SAS HD ports per expander.



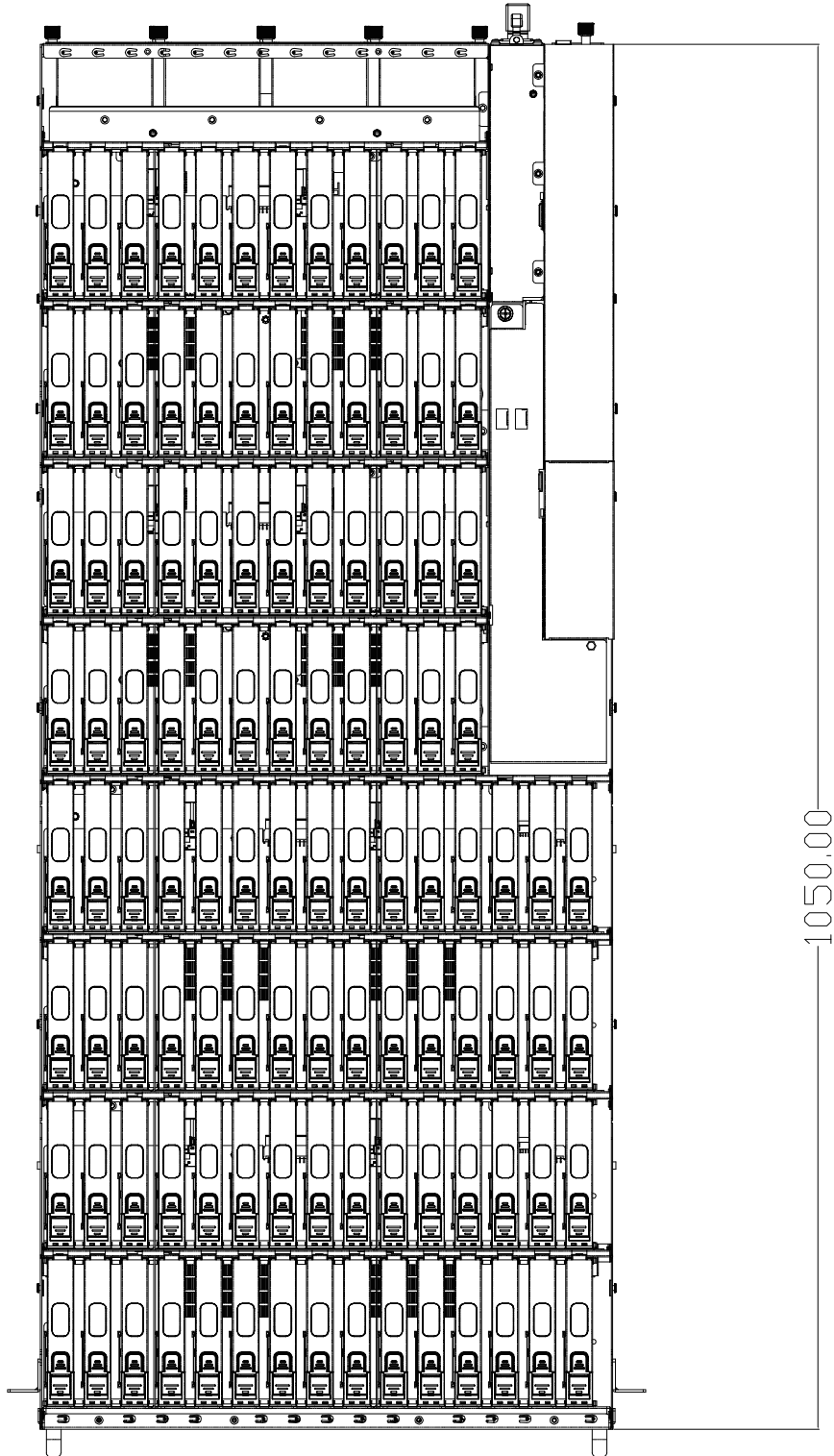
8644-LED Indicator Definition

Color	Description
Green	All 4 PHYs within the port are linked.
Yellow	At least 1 PHY within the port is linked.
Off	No PHYs within the port are linked.

Major Components

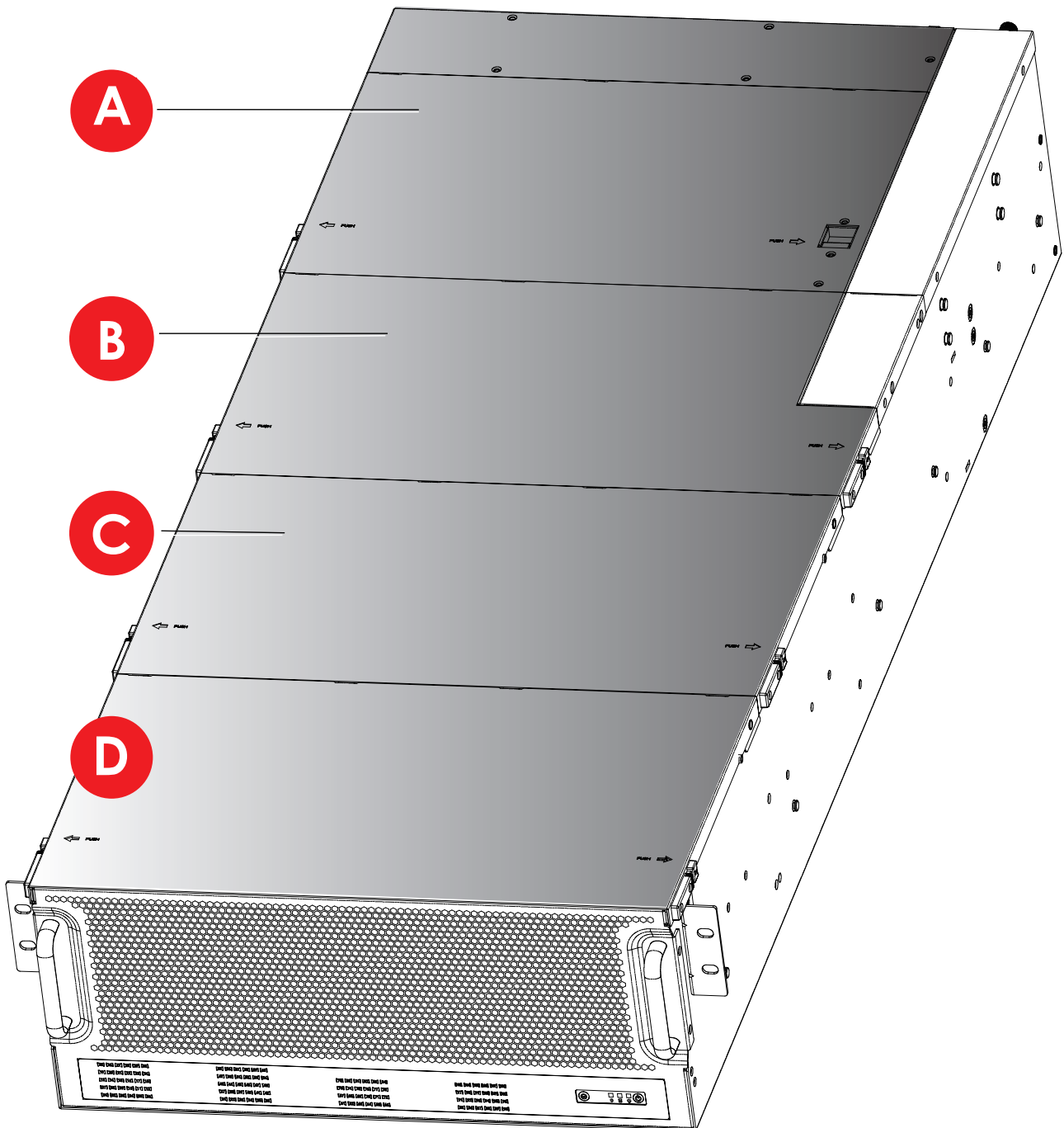
J4108-01-35X offers 3.5" x 108 hot swap bays.

- 12Gb/s & 6Gb/s SAS if using dual expanders
- 12Gb/s SAS and 6Gb/s SATA if using single expander



Chapter 2. Hardware Setup

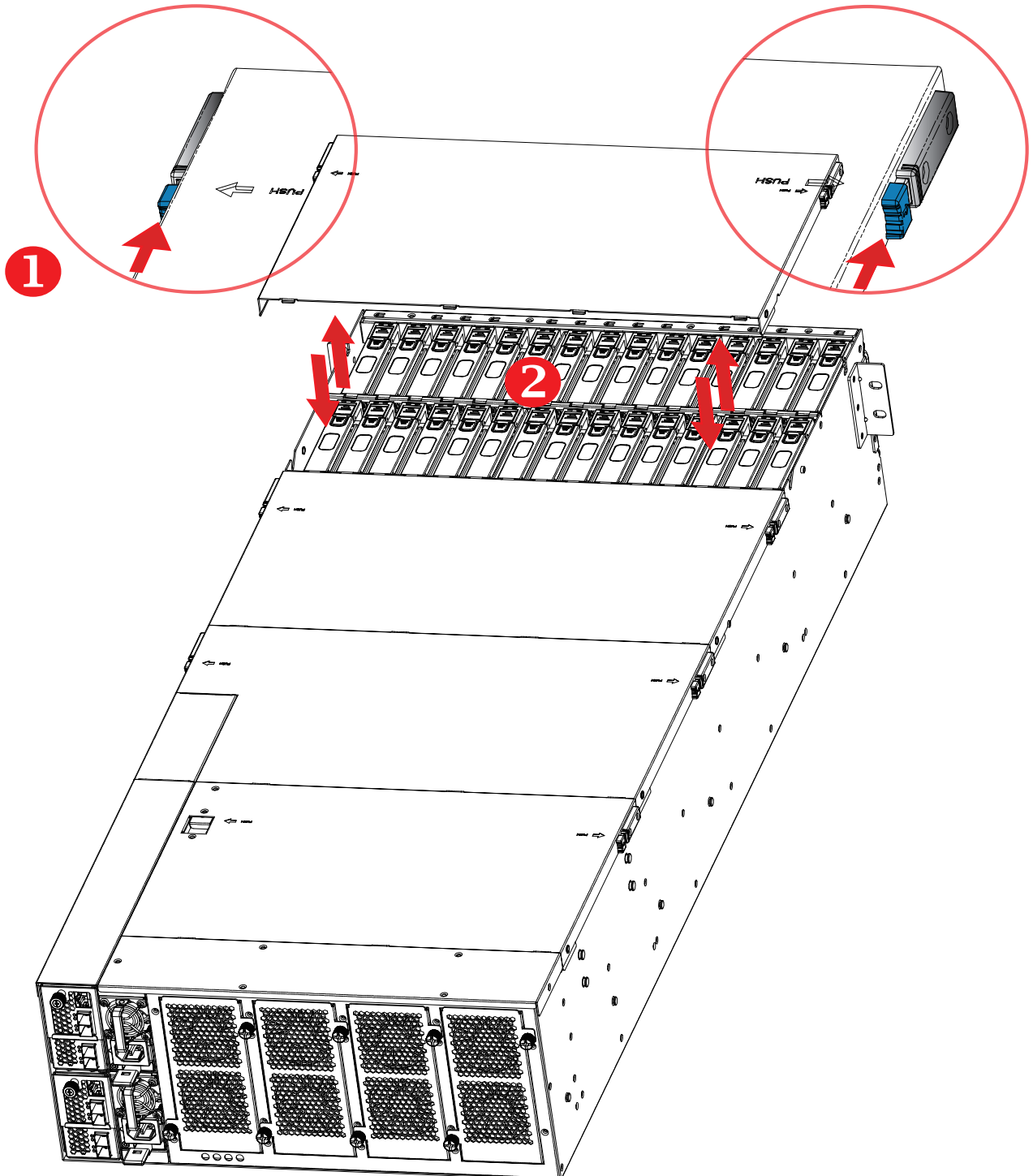
2.1 Top Cover



2.1.1 Installing/Removing the Top Cover A & B

Step 1 Push the release button on both sides of the top cover.

Step 2 Lift upward or downward to remove or install the cover.

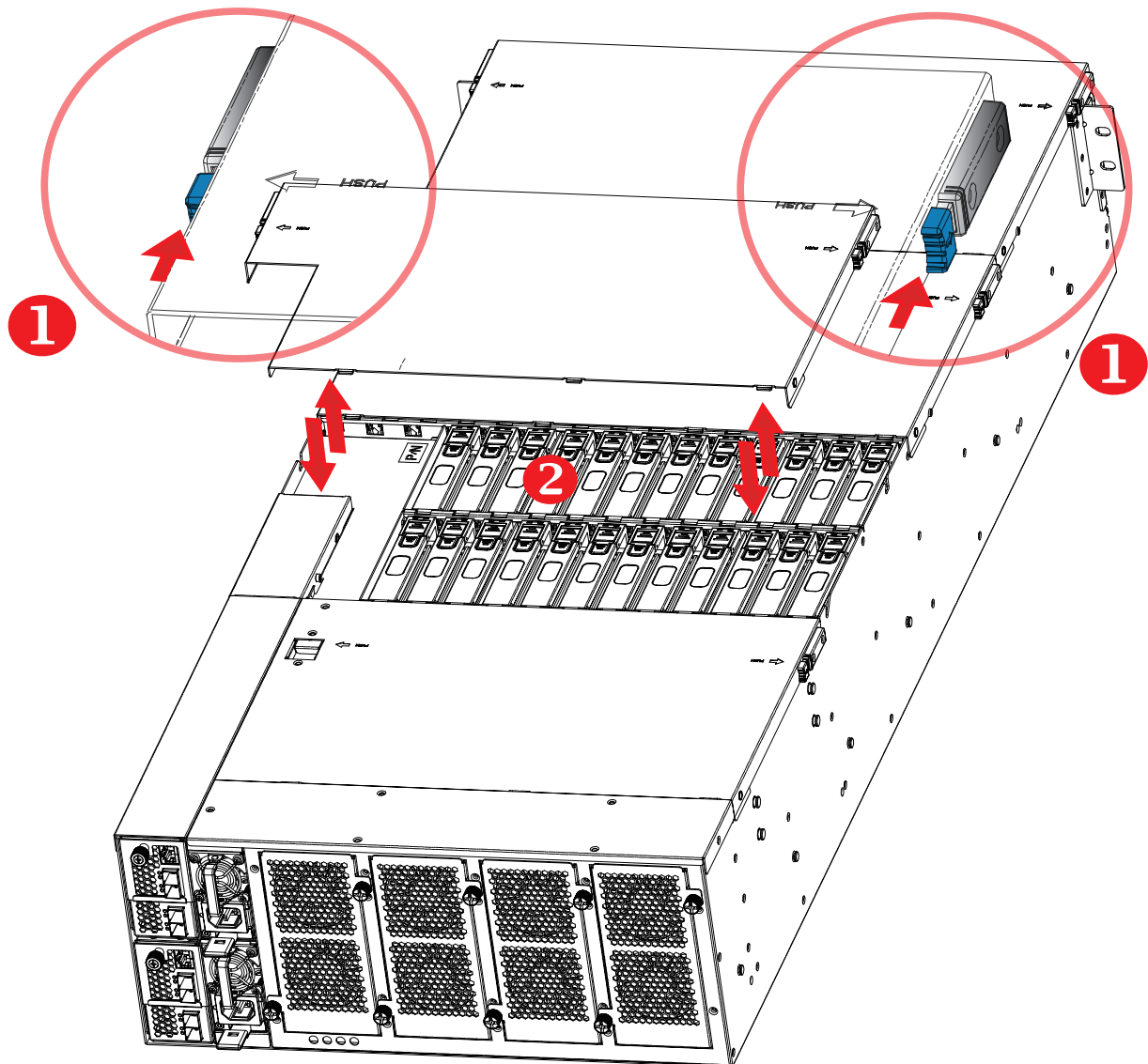


2.1.2 Installing/Removing the Top Cover C & D

Step 1 Push the release button on the top cover.

Check to press the correct release button.

Step 2 Lift upward or downward to install or remove the cover.



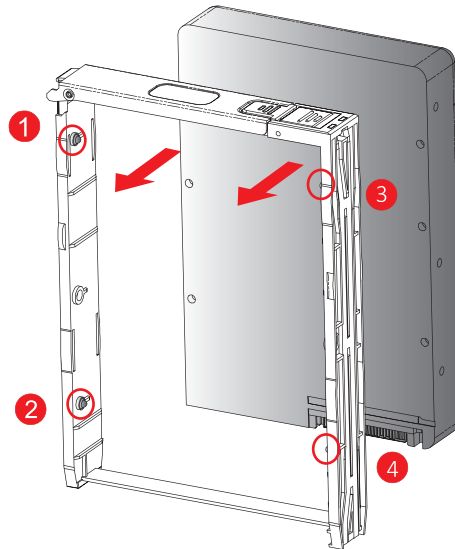
This information is provided for professional technicians only.

2.2 Disk Drive

2.2.1 Installing the Hard Disk Drive

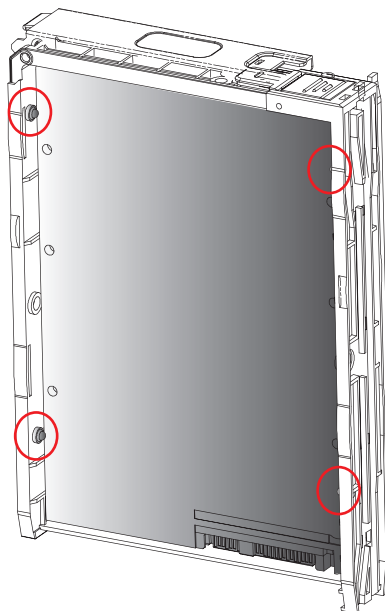
Step 1 Match the dimples on the HDD with the tool-less tray.

Step 2 Align the HDD with the tray by placing it against each other.

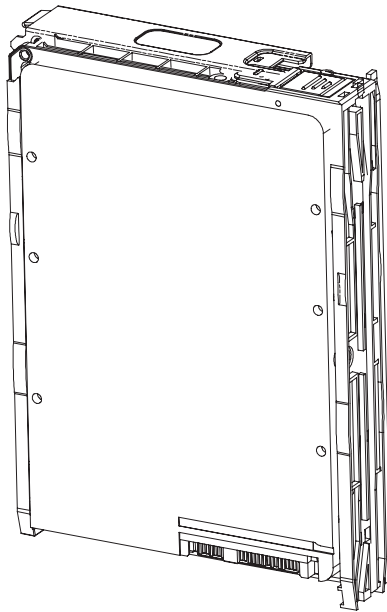


Step 3 Insert the HDD into the tool-less tray in the suggested order above.

Make certain to attach the side of the tray with the larger dimples to the HDD first and the side with the smaller dimples last for easier installation.

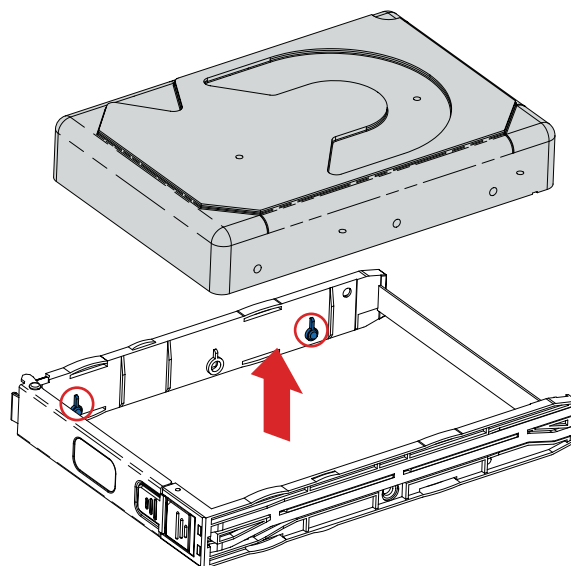


Step 4 Complete the installation.



2.2.2 Removing the HDD from the Tray

Pull the sides of tray to remove the HDD. Make certain to pull one side at a time for easier removal.

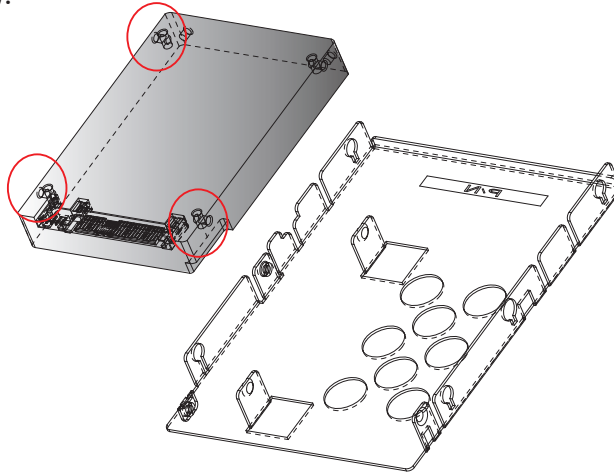


NOTE

When you remove the HDD from the tray, please push out the disk only from one direction to avoid causing damage. According to the image display above, the dimples should be on the bottom of the tray.

2.2.3 Installing the 2.5" Hard Disk Drive (Optional)

Step 1 Attach the HDD onto the HDD bracket and secure the screws (in red circle).



Step 2 Match the dimples (in dotted red circle) on the HDD bracket and HDD with the tool-less tray.

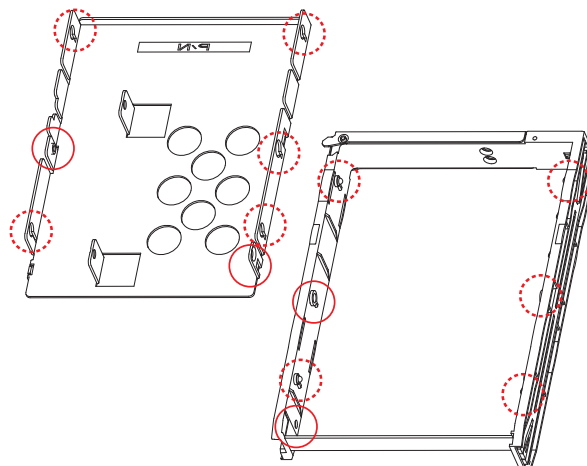
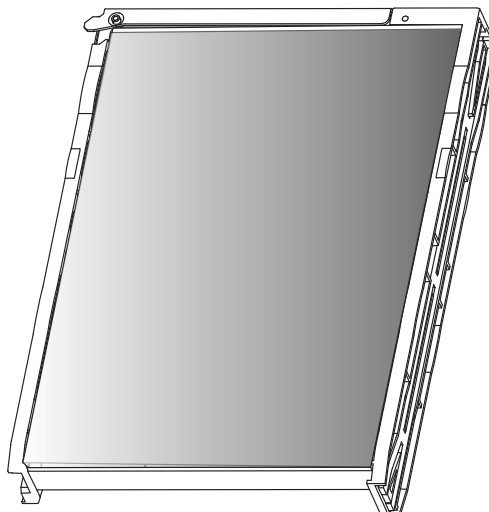


Image without HDD to demonstrate the location of dimple and screw.

- Screw location in red circle.
- Dimple location in the dotted red circle

Step 3 Insert the bracket and HDD into the tool-less tray.

Step 4 Secure the screws on the bracket to complete installation.

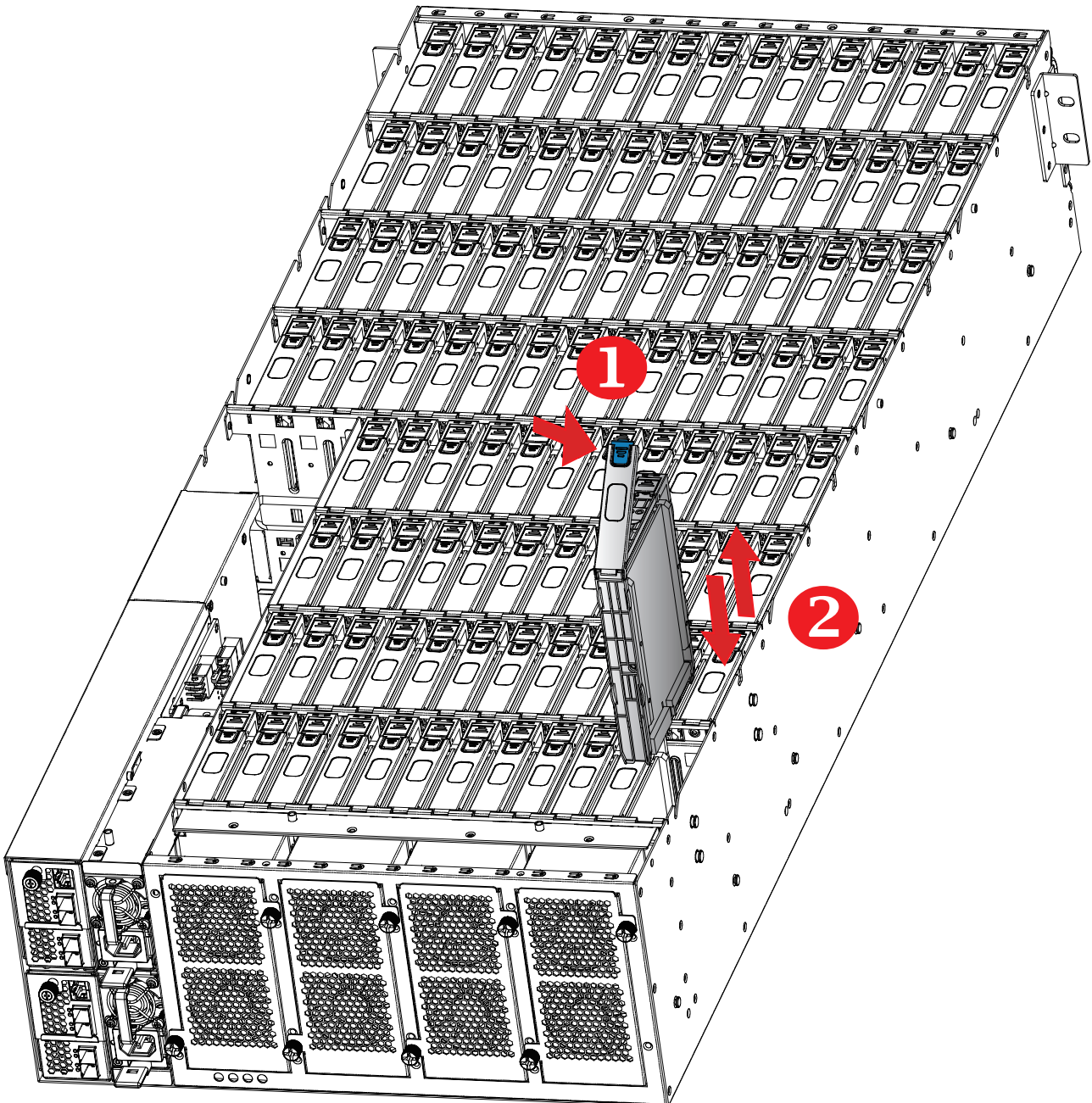


2.2.4 Installing/Removing the HDD Tray

Installing the HDD tray into the chassis

Step 1 Press downward on the tray lever.

Step 2 Insert the HDD into the enclosure until it clicks.



Removing the HDD tray out of the chassis

Step 1 Push the release button upward on the tray lever.

Step 2 Pull upward to remove the 2.5" HDD tray from the enclosure.



This information is provided for professional technicians only.

2.3 Fan Module

2.3.1 Installing the Fan

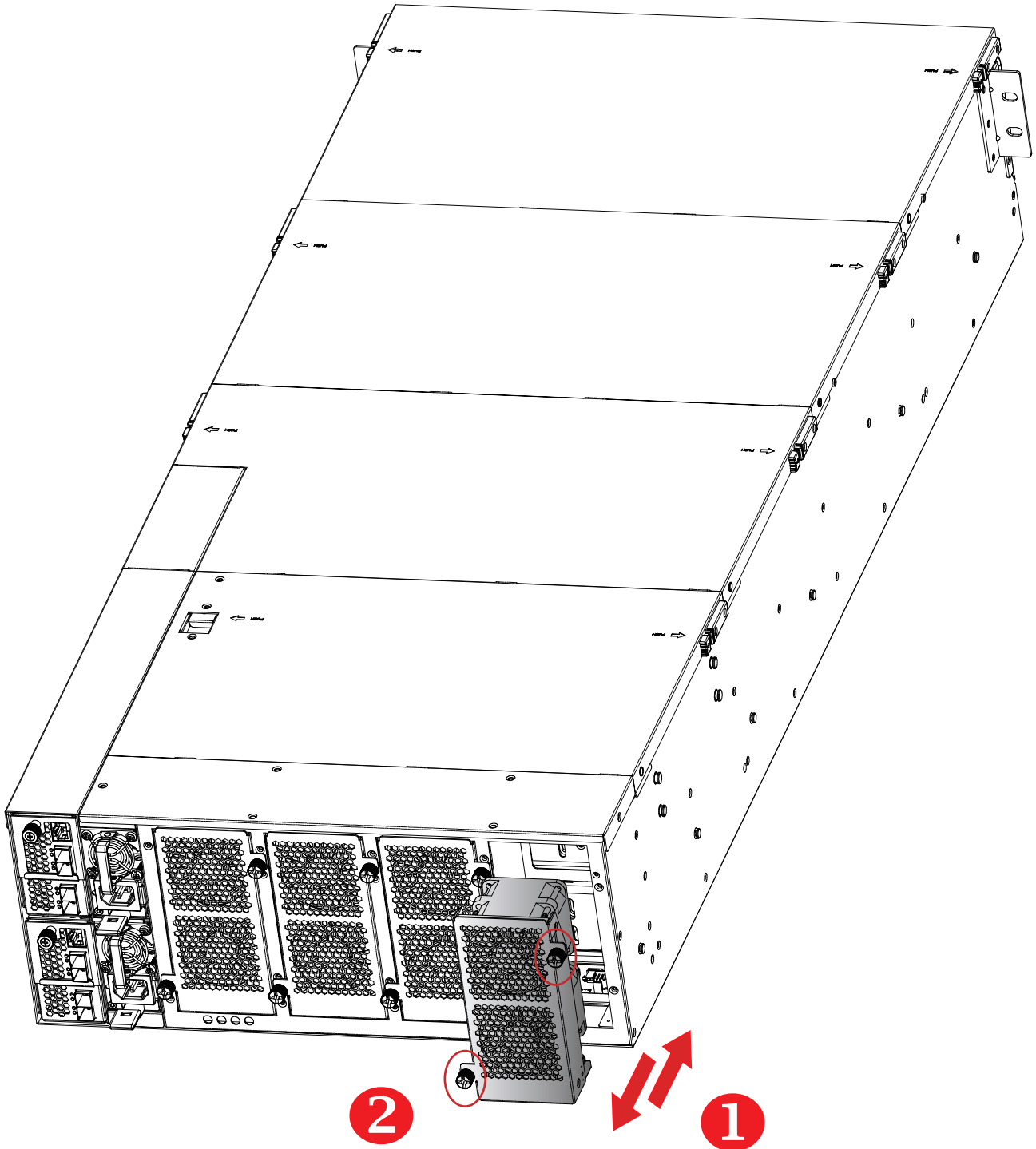
Step 1 Push the fan module into the enclosure.

Step 2 Secure the thumb screws x 2 pcs on the fan module.

2.3.2 Removing the Fan

Step 1 Loosen the thumb screws x 2 pcs on the fan module.

Step 2 Pull the fan module from the enclosure.



This information is provided for professional technicians only.

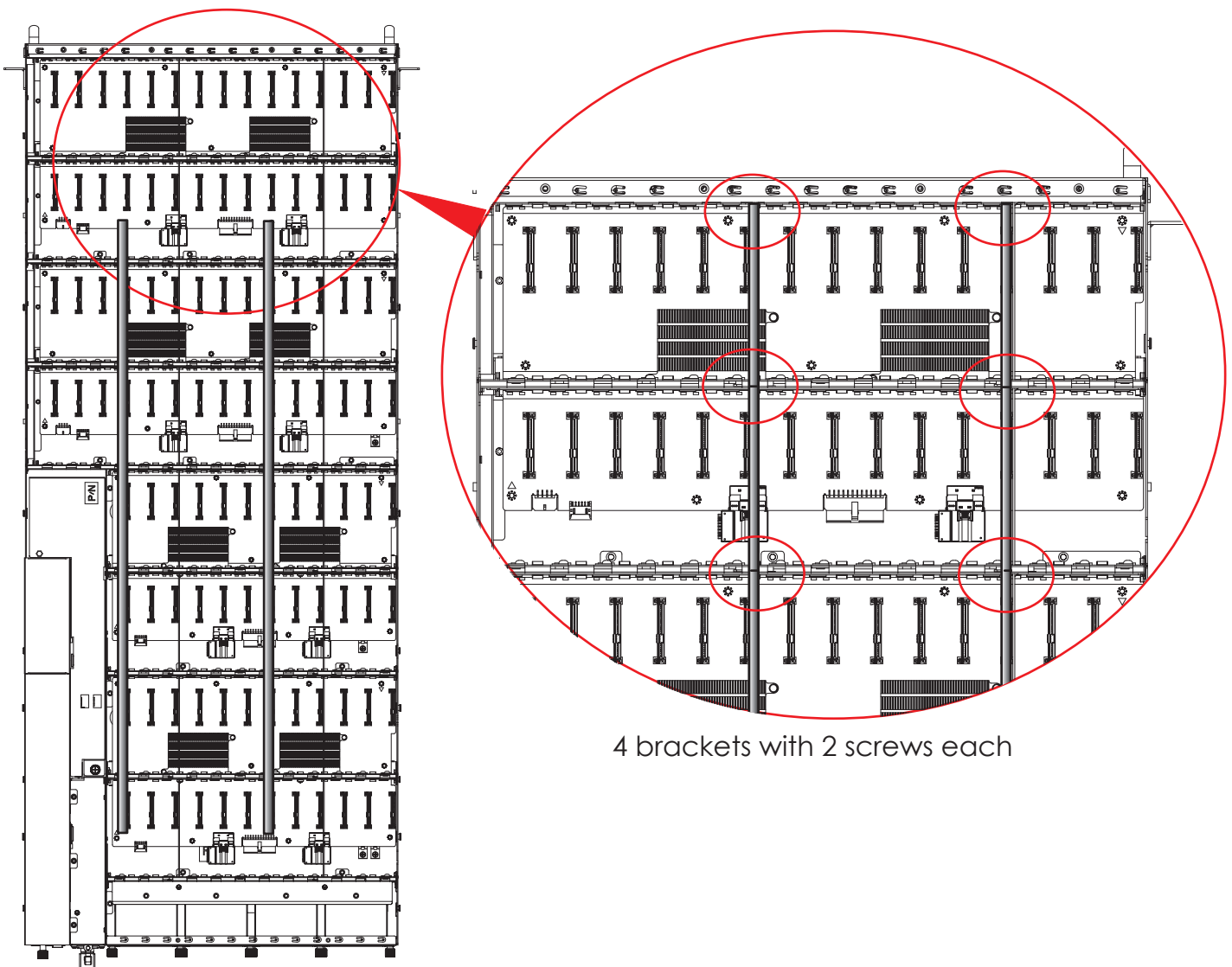
2.4 Drive Backplane Module

2.4.1 Installing the HDD Backplane

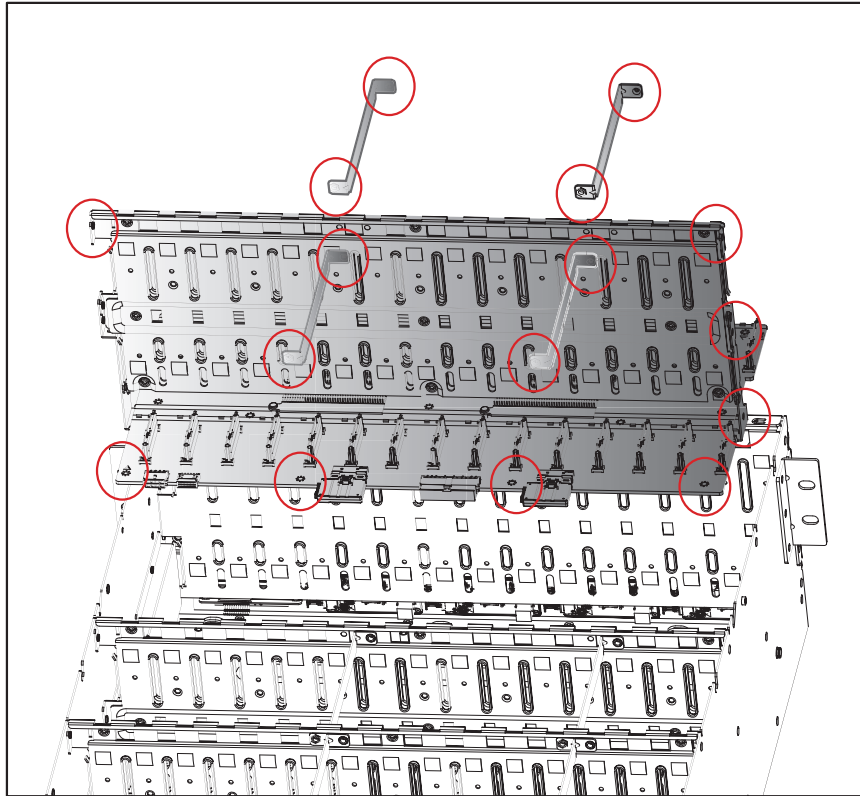
- Step 1** Position the HDD backplane module into the chassis and secure the screws x 12 pcs onto the enclosure (8 screws on the HDD backplane, 4 screws on the HDD backplane tray).
- Step 2** Position the brackets x 4 on the top of the HDD backplane module and secure the screws x 8 pcs (1 bracket with 2 screws each).
- Step 3** Repeat step 1 and step 2 to install the second backplane.

2.4.2 Removing the HDD Backplane

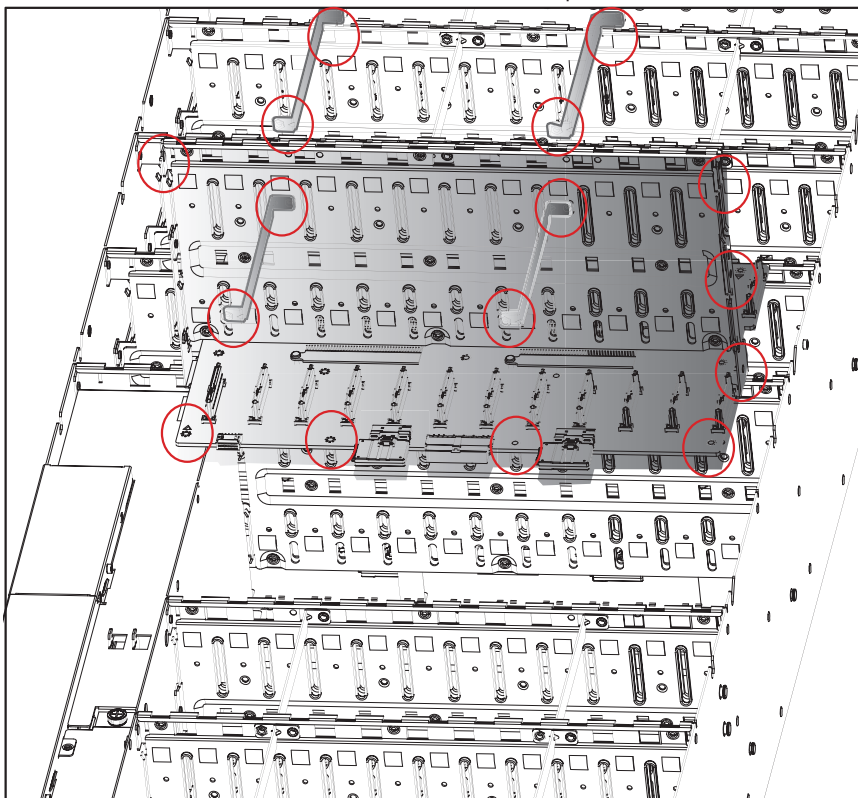
- Step 1** Remove the HDD disk trays from the enclosure.
- Step 2** Remove the top brackets x 4 from the chassis by removing the screws x 8 pcs (1 bracket with 2 screws each).
- Step 3** Remove the screws x 12 pcs on the HDD backplane module (8 screws on the HDD backplane and 4 screws on the HDD backplane tray).
- Step 4** Repeat step 1 to 3 to remove the second HDD backplane module.



Bracket and HDD backplane removal



Bracket and second HDD backplane removal



This information is provided for professional technicians only.

2.5 Power Supply Unit Module

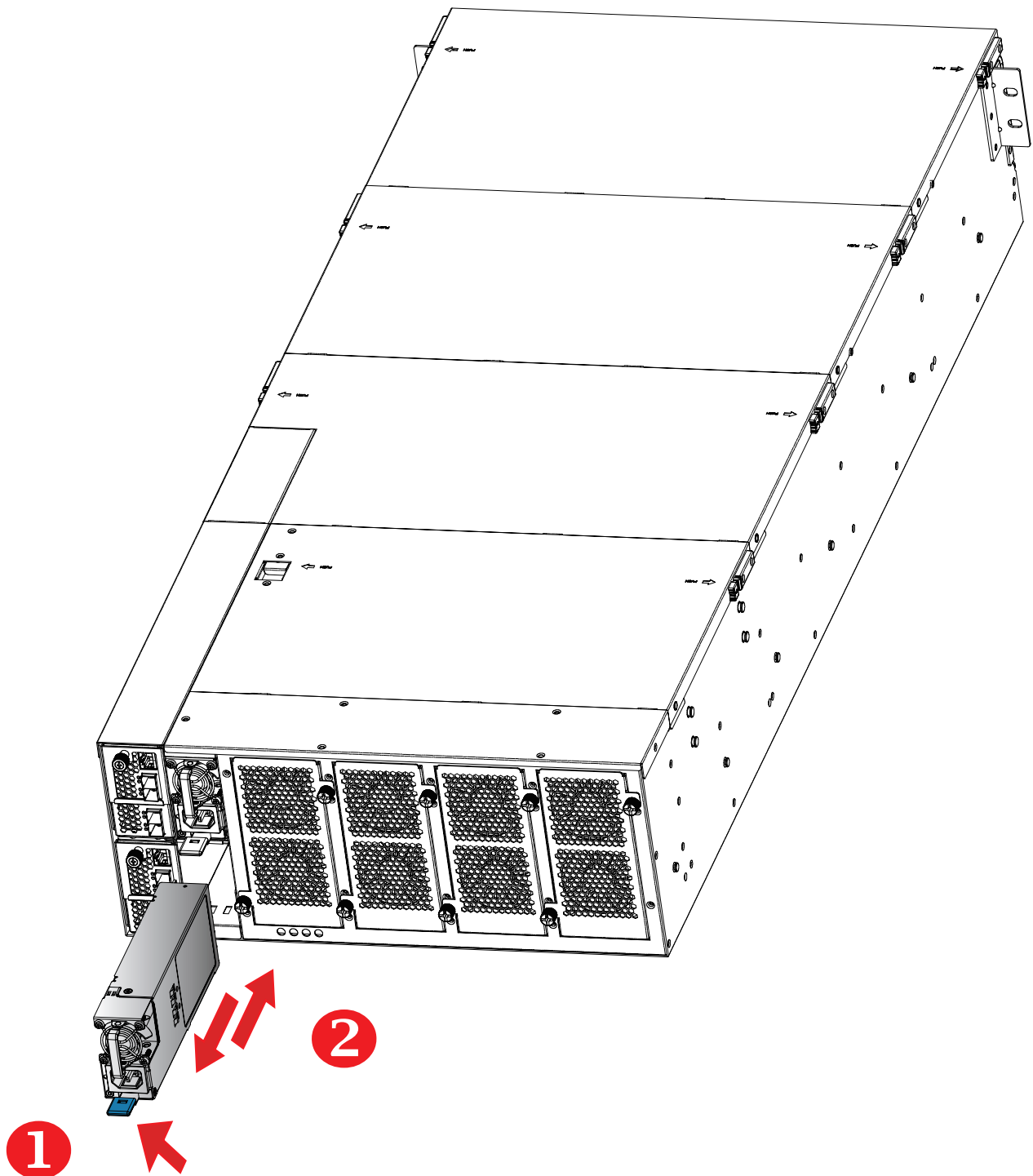
2.5.1 Installing the Power Supply Unit

Push the tray handle on the power supply module to install the device into the enclosure.

2.5.2 Removing the Power Supply Unit

Step 1 Push the latch upward and hold the tray handle.

Step 2 Pull the tray handle on the power supply module.



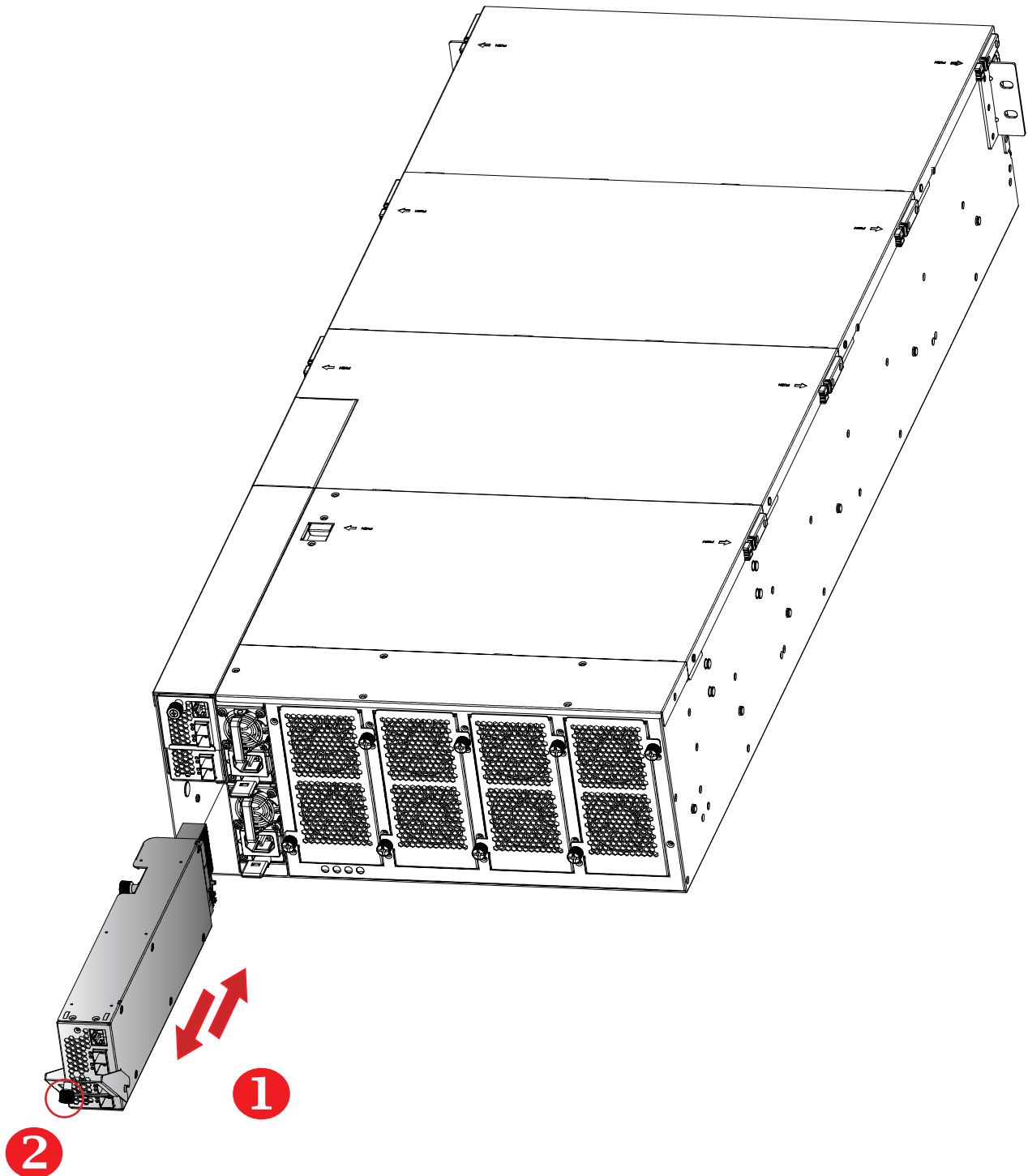
This information is provided for professional technicians only.

2.6 Expander Module

2.6.1 Installing the Expander

Step 1 Push the expander into the enclosure.

Step 2 Secure the thumb screw on the expander tray.



2.6.2 Removing the Expander

Loosen the screw to remove.



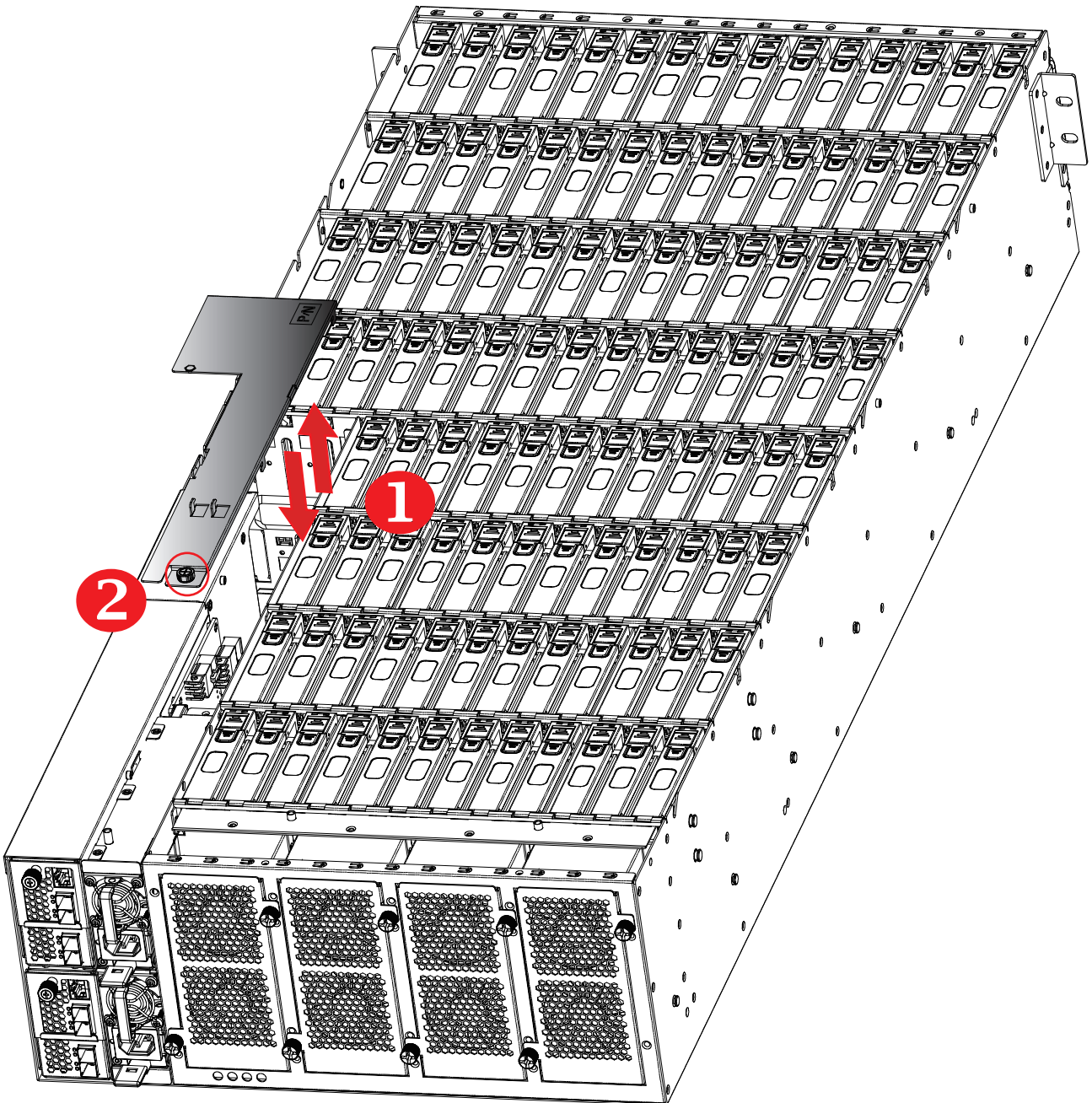
This information is provided for professional technicians only.

2.7 Cable Cover

2.7.1 Installing the Cable Cover

Step 1 Position the cable cover onto the enclosure.

Step 2 Secure the thumb screw x 1 pc on the cable cover.



2.7.2 Removing the Cable Cover

Loosen the thumb screw to remove.



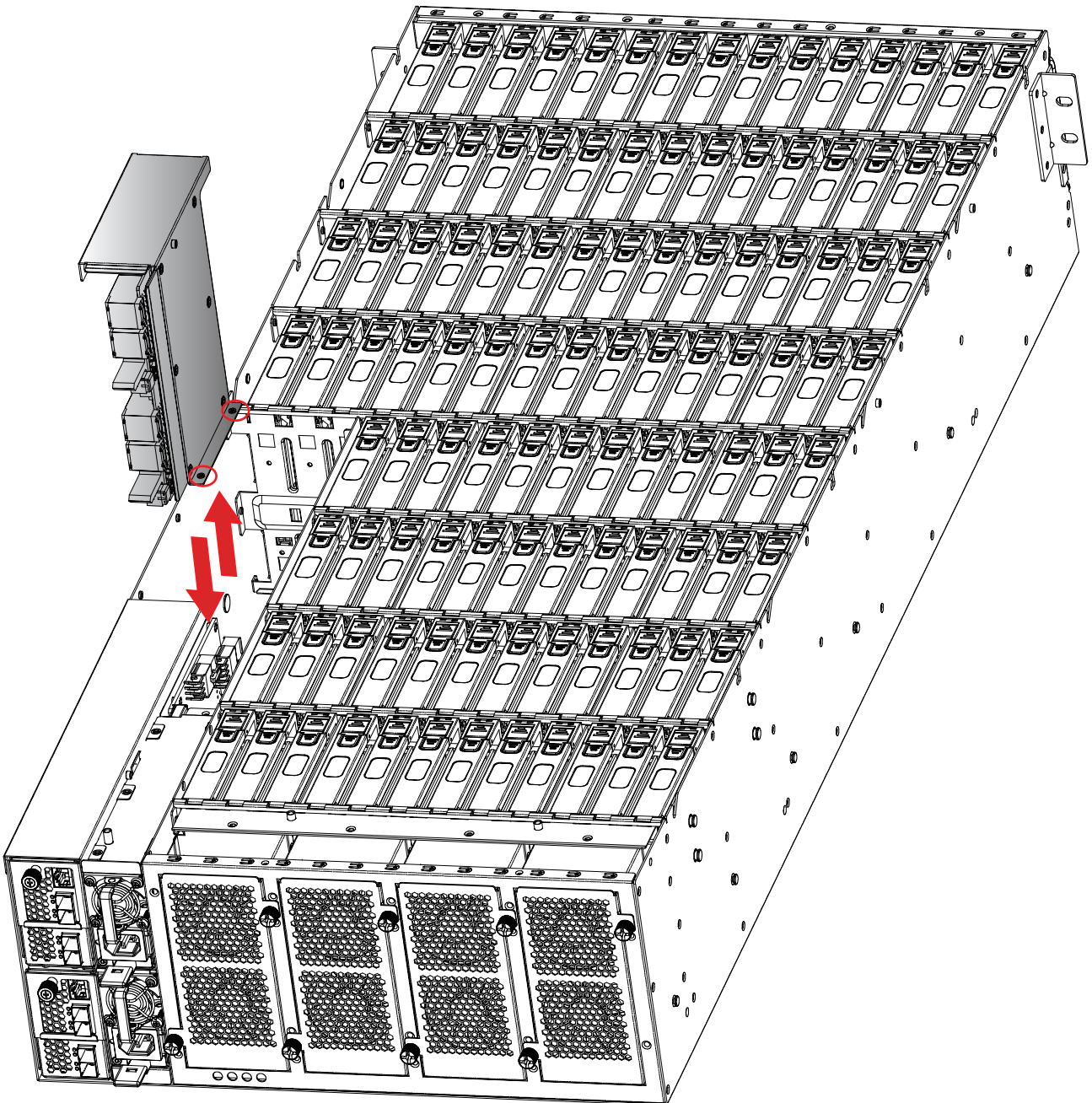
This information is provided for professional technicians only.

2.8 Bridge Board Module

2.8.1 Installing the Bridge Board

Step 1 Secure the screws x 2 pcs on the side of the bridge.

Step 2 Insert the bridge into the enclosure.



2.8.2 Removing the Bridge Board

Loosen the screws to remove.



This information is provided for professional technicians only.

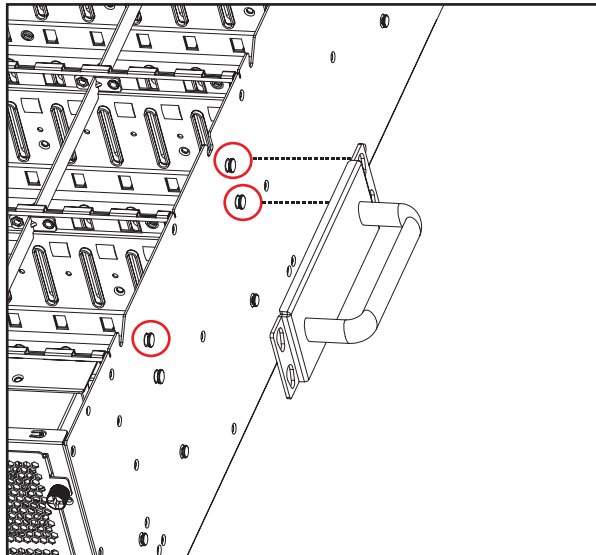
2.9 Rear Handle

2.9.1 Installing the Rear Handle

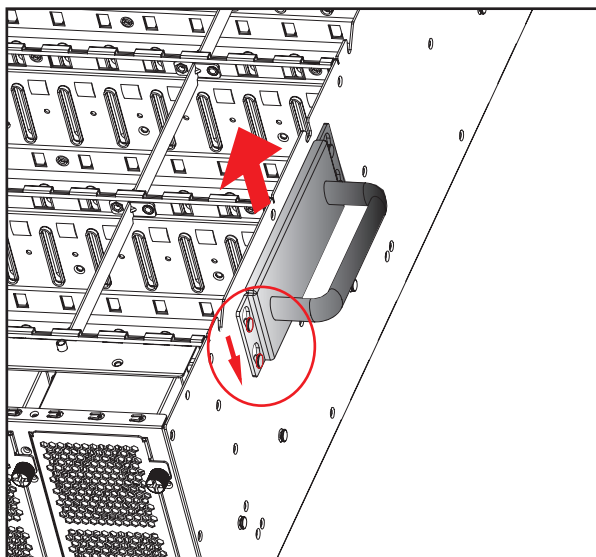
Step 1 Match the locking plate on the handle with the locks on the chassis.

step 2 Pull the handle upward to lock the handle onto the chassis.

Aligning the handle with the chassis.



Securing the handle.



2.9.2 Removing the Rear Handle

Step 1 Push the handle downward to dismantle the lock from the handle.

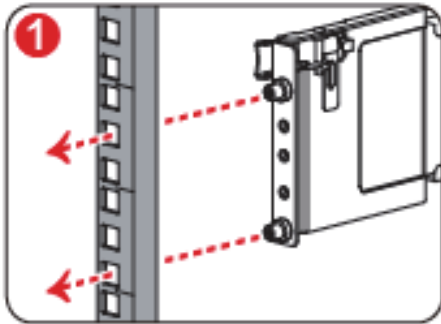
Step 2 Remove the handle from the chassis.



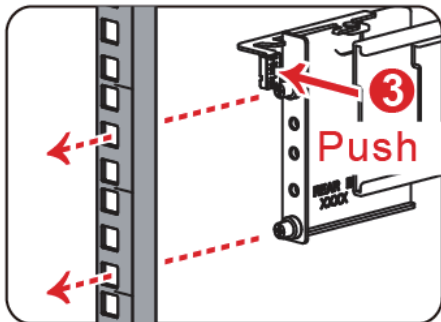
This information is provided for professional technicians only.

2.10 Slide Rail

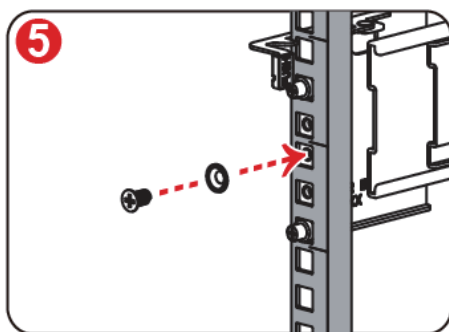
1. Attach the slide rail bracket assembly to the rack frame.
 - ① Align and attach the front rail bracket to the rack.
 - ② Ensure that the latch on the rail is hooked onto the rack.



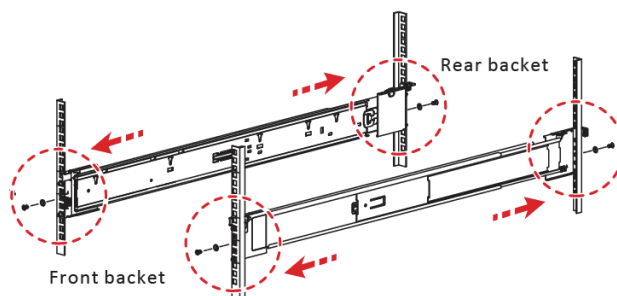
- ③ Align and attach the rear rail bracket to the rack by pushing the latch outward. Ensure the latch is hooked onto the rack.
 - ④ Ensure that the latch on the rail is hooked onto the rack.



- ⑤ Secure the rail bracket with a washer and screw on both sides of the rail bracket.



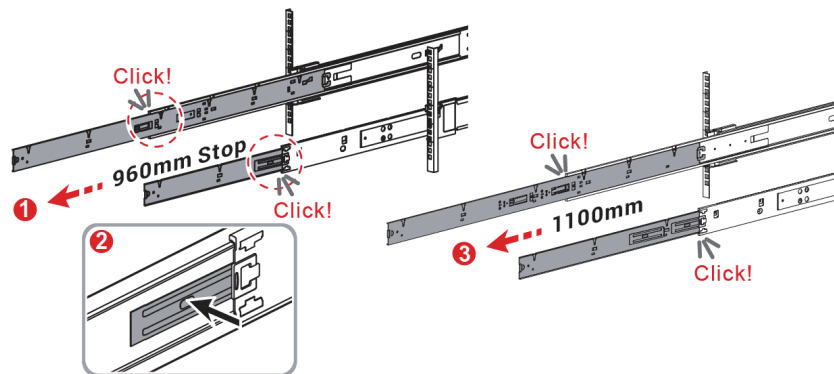
- ⑥ Repeat ① to ⑤ to install the other side of the rack.



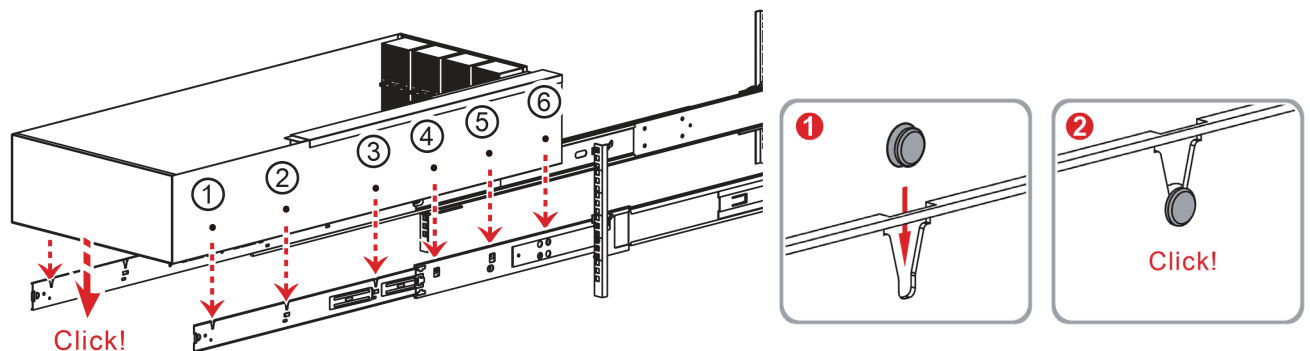
This information is provided for professional technicians only.

2. Attach the chassis onto the rack frame.

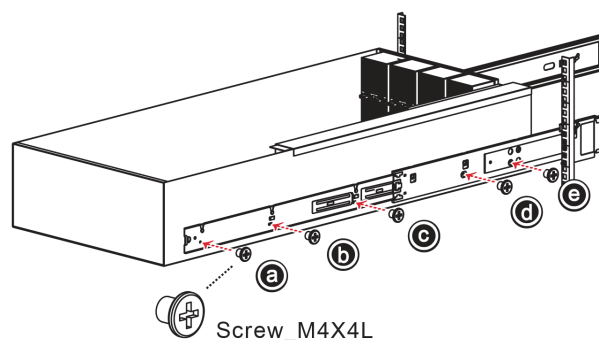
- ① Pull the inner and middle rail to fully locked position. The length of the rail will stop at 960mm. Push the release tab on the side of the rail to release the inner rail to full length (1100mm).



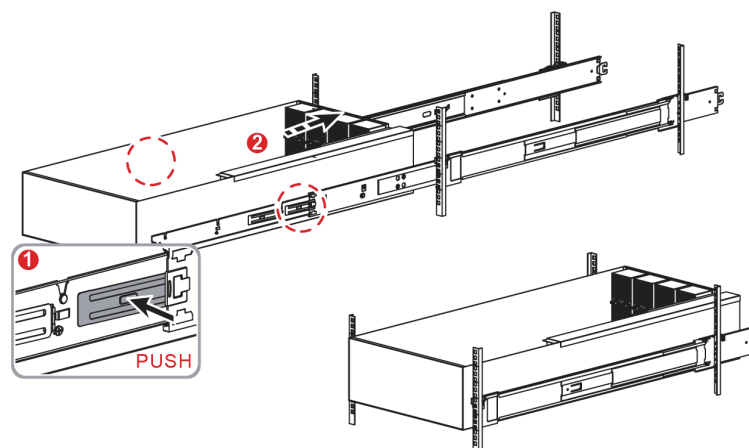
- ② Position the chassis vertically into the rail. Ensure the standoffs on the chassis slide into the v slots on the rail bracket.



- ③ Secure the chassis to the rail with screws.

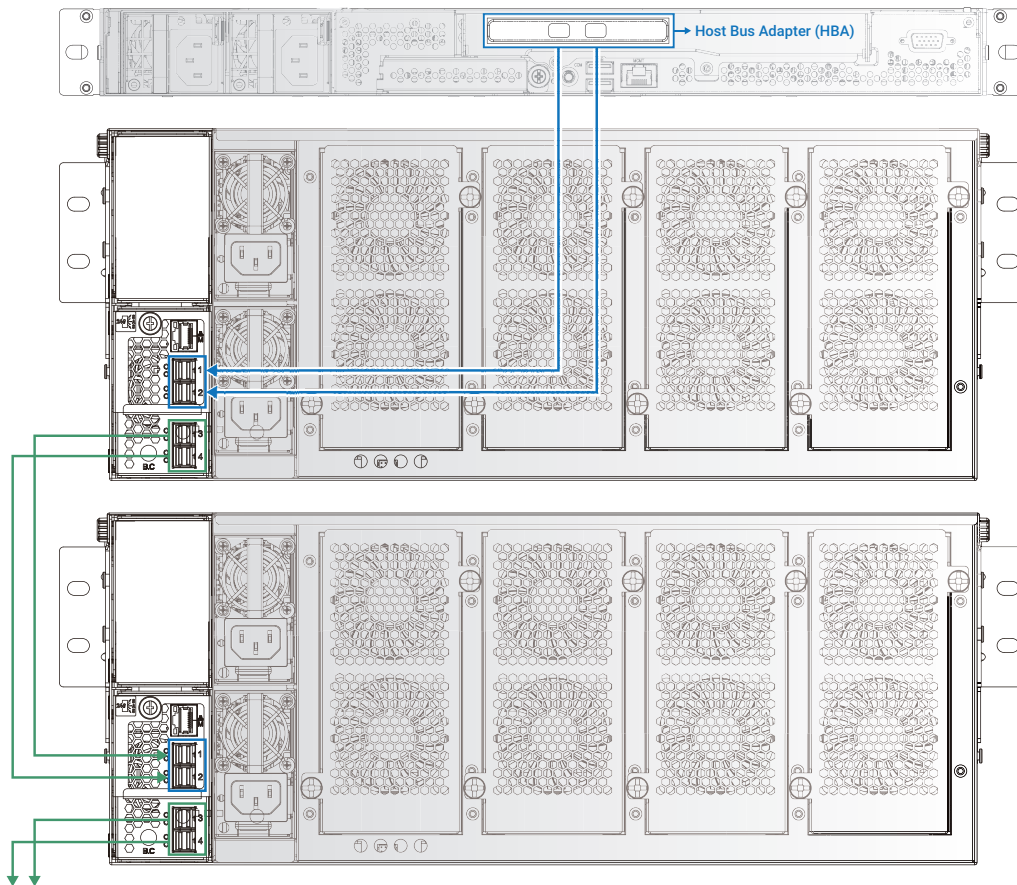


- ④ Push the release tab on the inner rail and push the chassis into the frame.

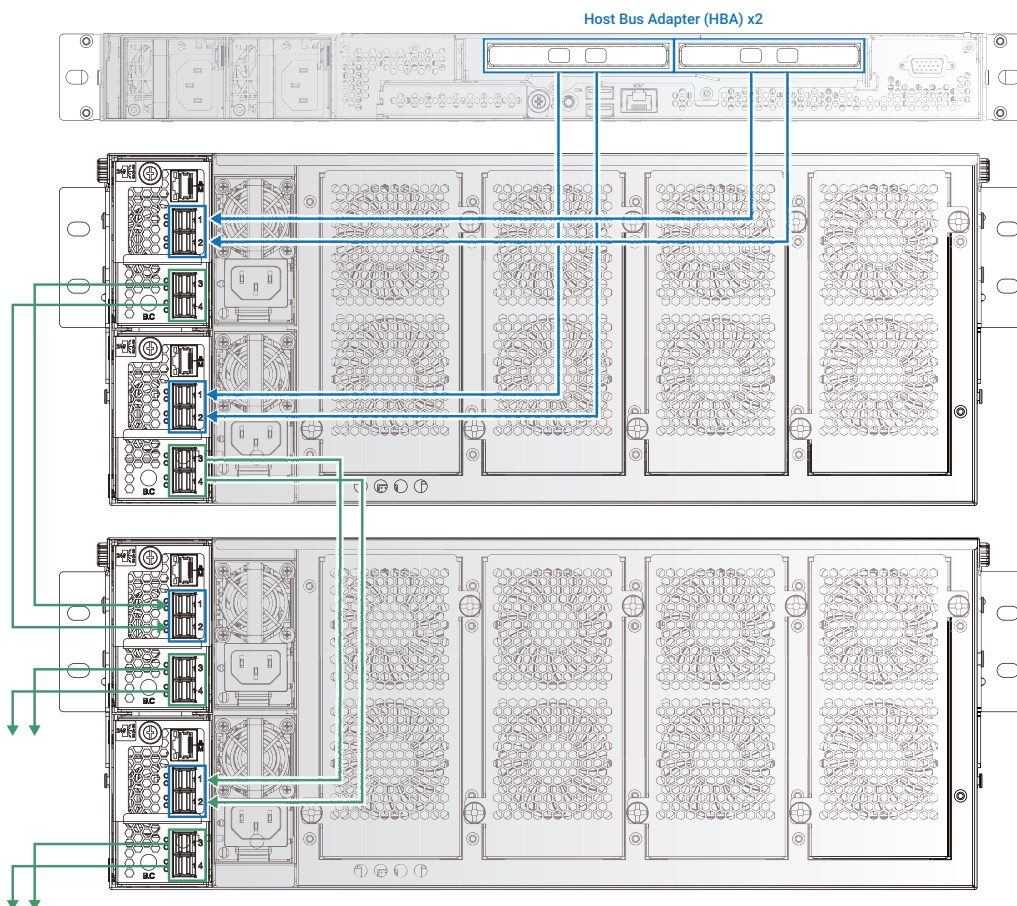


2.11 Standard Cabling

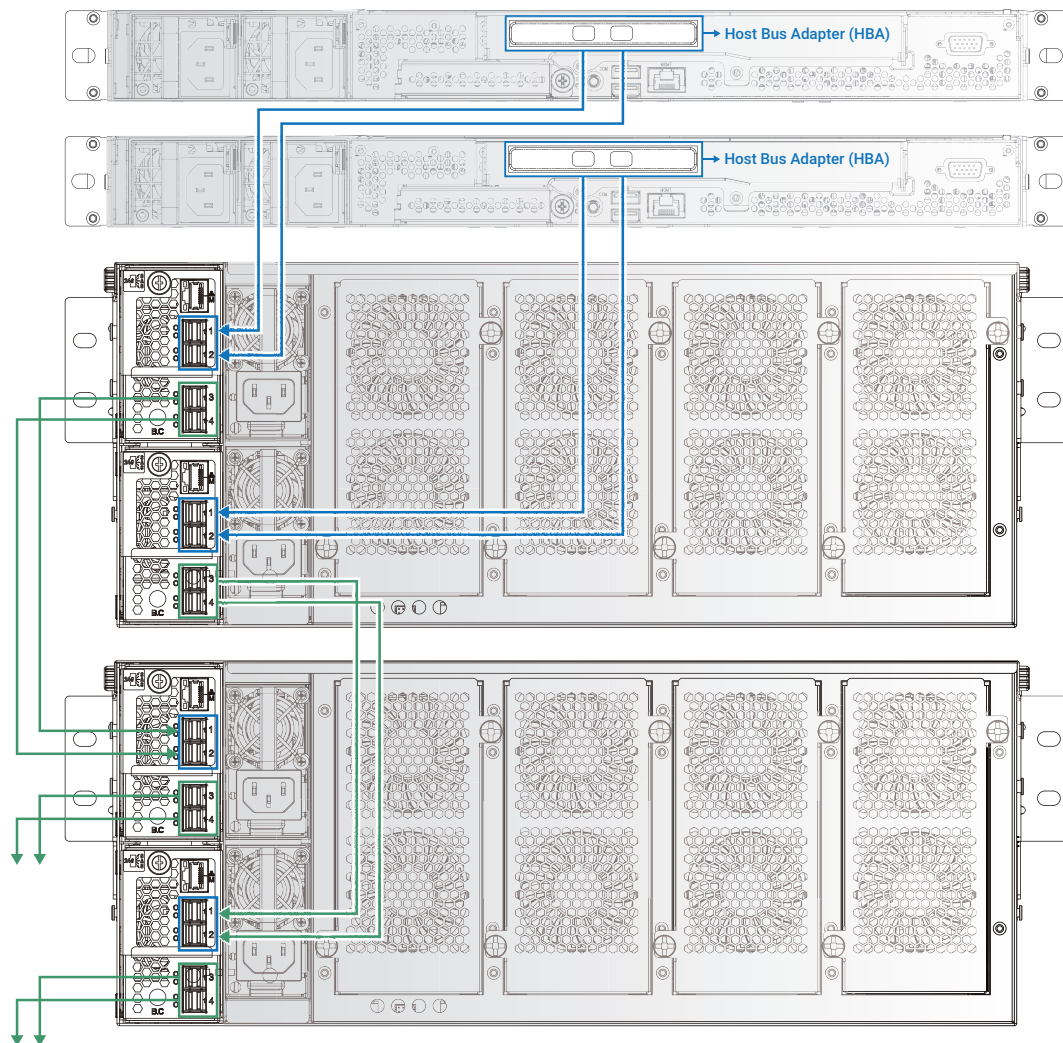
2.11.1 Single expander JBOD and 1 host server with 1 HBA card



2.11.2 Dual expander JBOD and 1 host server with 2 HBA cards



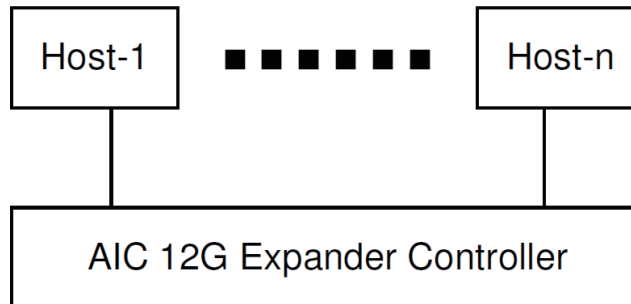
2.11.3 Dual expander JBOD and 2 host servers with 1 HBA card each



Chapter 3 Sub-system Configuration Setup

3.1 Supported Configuration and Unsupported Feature

3.1.1 Supported Configuration



To have multiple host/path access support (the host number can be up to the number of wide ports on each AIC® 12G Expander Controller), only the following drives are supported for shared access:

1. SAS drive / Nearline SAS drive
2. SATA drive with an interposer which provides SATA-to-SAS conversion

Locating a drive via any HBA utility is not supported. Users should send standard SES command to the enclosure (108swapHub) to locate a drive.

3.1.2 Unsupported Feature

1. Enclosure logical identifier can be changed.
2. Locating a drive via any HBA utility. Users should send standard SES command to locate a drive.
3. The management software MegaRAID Storage Manager with LSI 6G RAID Card is not supported.

Chapter 4. BMC Configuration Settings

4.1 Login

1. Push the "[" key, it will show the IPMI serial interface.

```
-----  
IPMI Terminal Interface  
-----  
Usage :  
Terminal Text command : [SYS Command]  
Terminal IPMI command : [NetFnLun SeqNum Cmd Data 0 ... Data N]  
  
Type [SYS HELP] - To get list of Text Command  
Press CTRL+X or CTRL+C - To exit Terminal  
  
IPMI Terminal:/> █
```

Type command for login the interface.

#[sys pwd -u admin admin]

It will response [OK]

```
IPMI Terminal:/> [SYS PWD -U admin admin ]  
[OK]
```

2. Change user password.

Due to security principles, you need to change your password when logging in for the first time. There are 16 Bytes that can be filled with ASCII Hex, at least 8 Bytes with value, and the rest fill in 0.

Change the password to “12345678”:

```
IPMI Terminal:/> [18 00 47 02 02 31 32 33 34 35 36 37 38 00 00 00 00 00 00 00 ]  
[1C 00 47 00]
```

Retry to login the interface.

```
#[sys pwd -u admin 12345678 ]
```

It will response [OK]

```
IPMI Terminal:/> [SYS PWD -U admin 12345678 ]  
[OK]
```

3. Find LAN information.

0 _{hex}	=	0 _{dec}
1 _{hex}	=	1 _{dec}
2 _{hex}	=	2 _{dec}
3 _{hex}	=	3 _{dec}
4 _{hex}	=	4 _{dec}
5 _{hex}	=	5 _{dec}
6 _{hex}	=	6 _{dec}
7 _{hex}	=	7 _{dec}
8 _{hex}	=	8 _{dec}
9 _{hex}	=	9 _{dec}
A _{hex}	=	10 _{dec}
B _{hex}	=	11 _{dec}
C _{hex}	=	12 _{dec}
D _{hex}	=	13 _{dec}
E _{hex}	=	14 _{dec}
F _{hex}	=	15 _{dec}

Find LAN static IP /DHCP [30 00 02 01 04 00 00]

Find LAN IP [30 00 02 01 03 00 00]

Find submask [30 00 02 01 06 00 00]

Find gateway [30 00 02 01 0C 00 00]

```
IPMI Terminal:/> [30 00 02 01 04 00 00 ]
[34 00 02 00 11 02]
```

```
IPMI Terminal:/> [30 00 02 01 03 00 00 ]
[34 00 02 00 11 C0 A8 15 44]
```

```
IPMI Terminal:/> [30 00 02 01 06 00 00 ]
[34 00 02 00 11 FF FF FF 00]
```

```
IPMI Terminal:/> [30 00 02 01 0C 00 00 ]
[34 00 02 00 11 C0 A8 15 FE]
```

Find LAN static IP /DHCP: 01 is static IP and 02 is DHCP.

The red box represents hexadecimal digits. According to the left figure, the IP is $16 \times 12 + 0 = 192$, $16 \times 10 + 8 = 168$, $16 \times 1 + 5 = 21$, $16 \times 4 + 4 = 68$. Therefore, the IP is 192.168.21.68

4. Set LAN information.

Set LAN static IP /DHCP [30 00 01 01 04 01/02]

Set LAN IP [30 00 01 01 03 C0 A8 0B 0B]

Set submask [30 00 01 01 06 FF FF FF 00]

Set gateway [30 00 01 01 0C C0 A8 00 01]

```

IPMI Terminal:/> [30 00 01 01 04 01]
[34 00 01 00]

IPMI Terminal:/> [30 00 01 01 03 C0 A8 0B 0B ]
[34 00 01 00]

IPMI Terminal:/> [30 00 01 01 06 FF FF FF 00 ]
[34 00 01 00]

IPMI Terminal:/> [30 00 01 01 0C C0 A8 00 01 ]
[34 00 01 00]

```

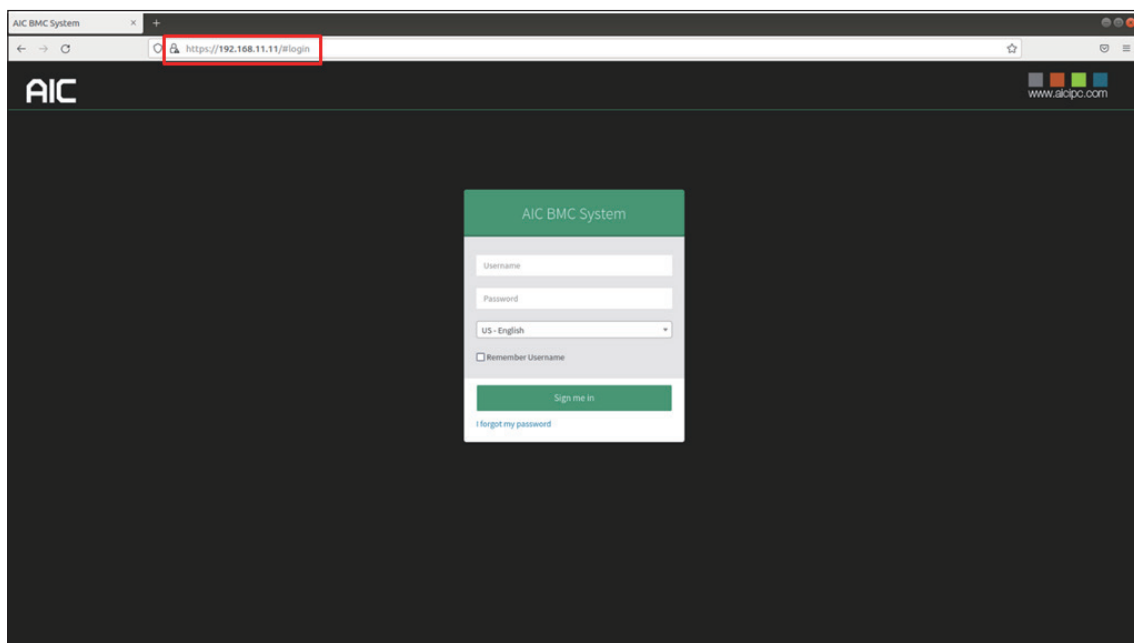
The digit in the red box is completion code.

00 represents the confirmed code.

The digits in the green box are can be configured to any value.

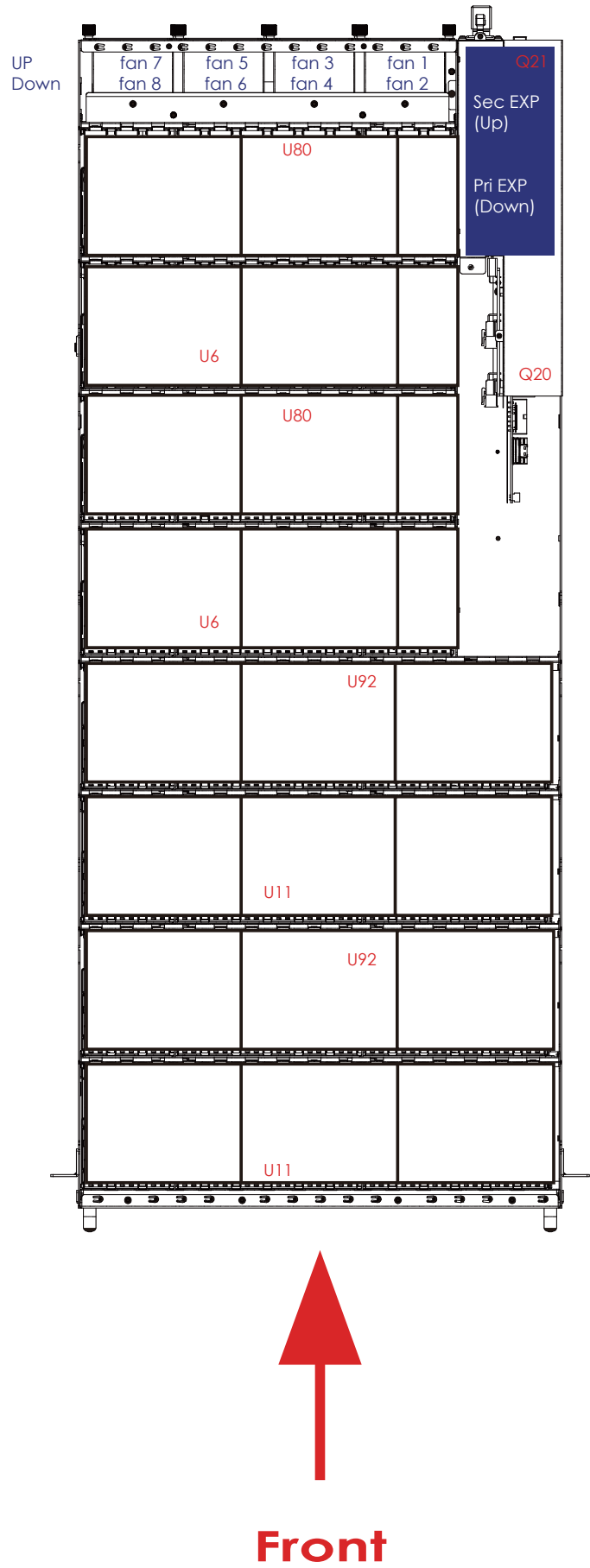
If you want to change the IP address, you must set the **LAN status to static**.

5. Connect to RJ45 port. Set the local host IP to **192.168.11.xx** segment.
6. Open the web browser and enter default IP **http://192.168.11.11**. When the login window appears, set the user name and password from step 2.
7. Click Log In to continue.



4.2 Sensor's Location for Fan and Temperature

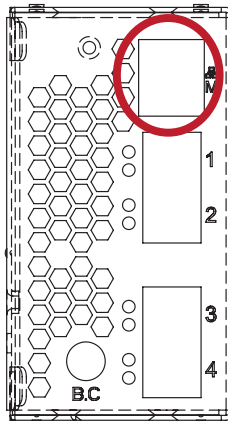
EXP: expander chip



4.3 Expander Setting via Java SOL

Step 1 Plug in the BMC LAN port.

Expander rear panel



Step 2 Log into the BMC interface. Please refer to [4.1 Login](#).

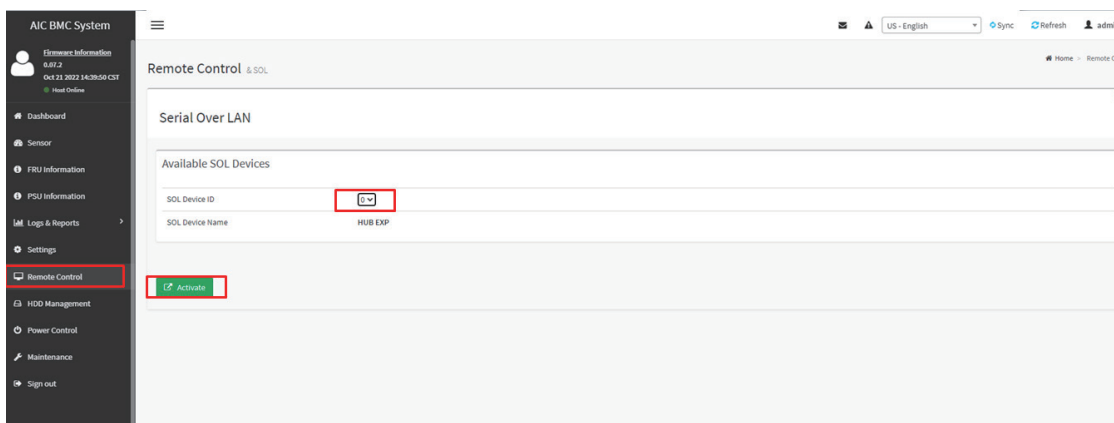
Step 3 Enter Java Sol in BMC to configure the serial command line Interface.

4.3.1 Java SOL

There are two methods to initiate Sol.

Method 1

1. Select an expander under **Select expander** and click Activate.



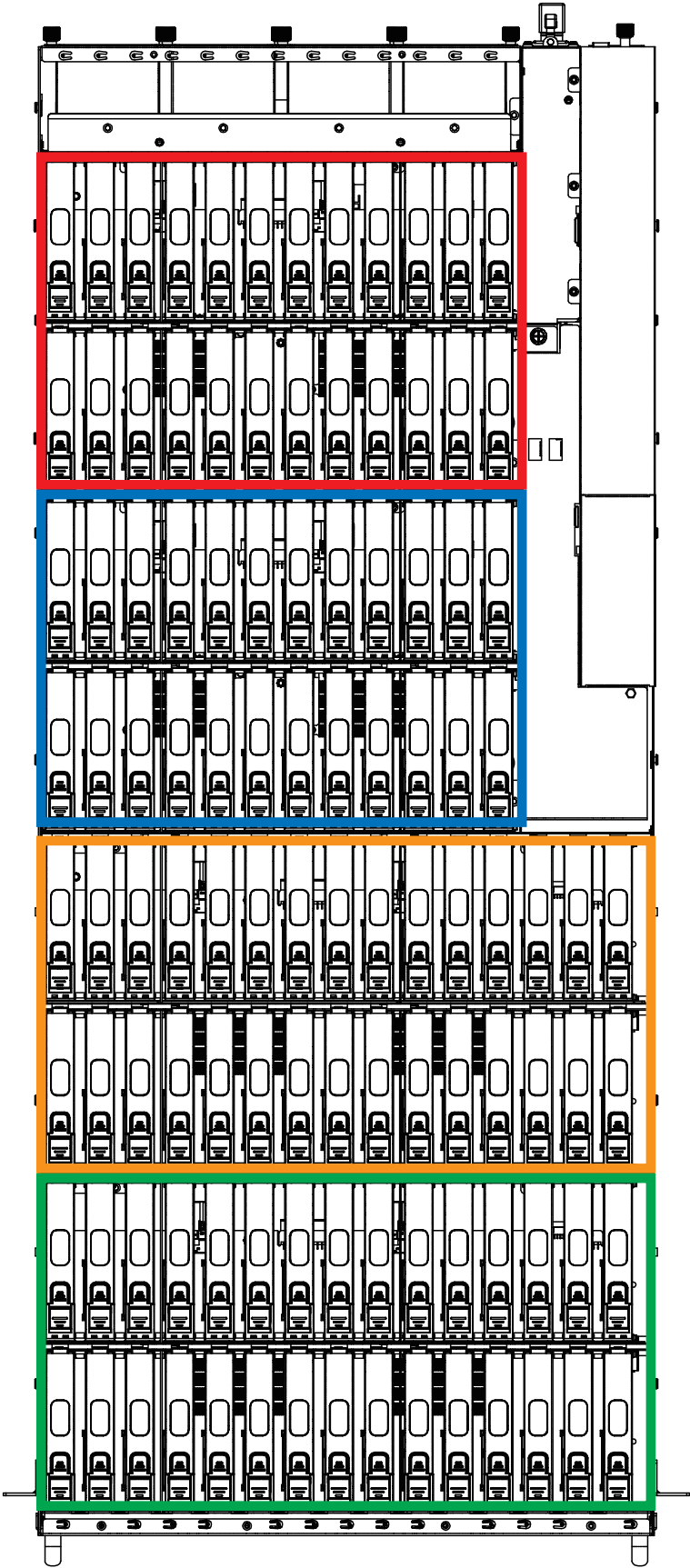
Edge 0, Edge 1, Edge 2, Edge 3 Top View Location

Edge 3

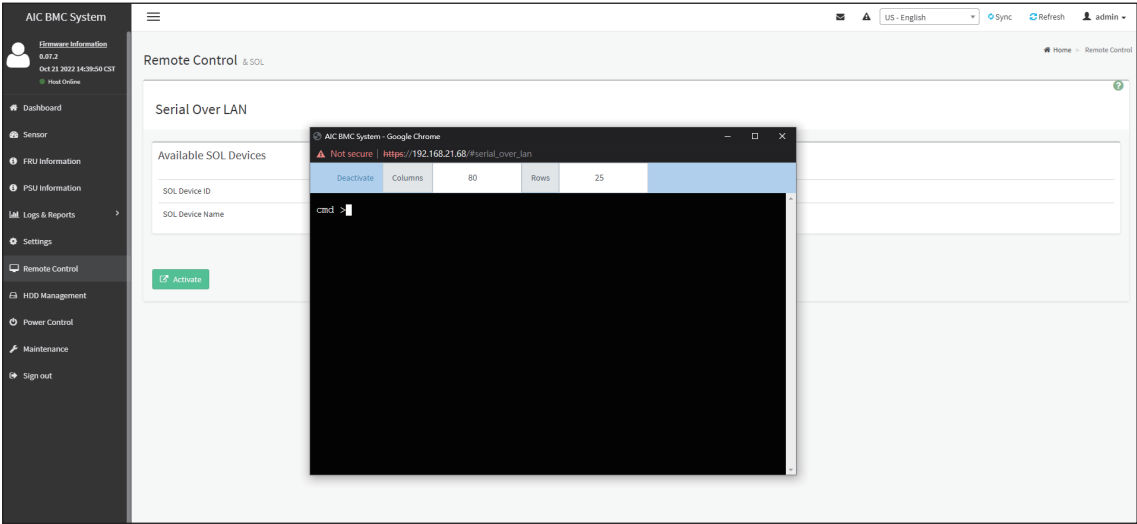
Edge 2

Edge 1

Edge 0



2. Now you can use the expander smart console via BMC SOL.



Method 2

1. In addition, you can use ipmitool to start SOL function.

#ipmitool -I lanplus -H <BMC IP> -U admin -P admin sol activate

```
C:\Users\su2\Desktop\ipmitool_test>ipmitool.exe -I lanplus -H 192.168.11.11 -U admin -P admin sol activate
[SOL Session operational. Use ~? for help]

cmd >
cmd >
cmd >
cmd >
cmd >sensor

== ENCLOSURE STATUS ==

Hub Fan-0 speed : 6930 RPM
Hub Fan-1 speed : 7290 RPM
System Fan-0 speed : 5113 RPM
Voltage Sensor 12V : 12.3 V
Power-0 : good
Power-1 : good

Current Model : 4U78swapHub

Alarm-system : off
Alarm-temperature : off
Alarm-fan : off
Alarm-power : off
Buzzer-state : off
Buzzer-mute : off

MCU firmware version : 0.2

cmd >
cmd >
```

2. When you need to use SOL, type “~.” to exit this function.

```
Current Model      : 4U78swapHub

Alarm-system      : off
Alarm-temperature : off
Alarm-fan         : off
Alarm-power       : off
Buzzer-state      : off
Buzzer-mute       : off

MCU firmware version : 0.2

=====

cmd >
cmd >~. [terminated ipmitool]

C:\Users\suz\Desktop\ipmitool_test>
```

3. If you want to switch to another expander, you do not need to close SOL. Use the command below to switch your expander.

SET EXPANDER

NetFN 3C

Command Code: 40h

Message	Byte	Data Field
Request	1	Expander select 00h: Hub 01h: Edge0 02h: Edge1 03h: Edge2 04h: Edge3 (4U108 only)
Response	1	Select Expander
	2	Expander is being updated FFh: idle
	3	SOL active Expander FFh: idle

#ipmitool -I lanplus -H <BMC IP> -U admin -P admin raw 0x3C 0x40 0x0

4.3.2 Configure Serial Command Line Interface

The RS232 setting - baud rate: 38400 bps, data bits: 8, parity: none, stop bits: 1, flow control: none

4.3.2.1 How to enable/disable T10 zoning

The default T10 zoning configuration is off.

- (A) Check the current zoning state

```
cmd> phyzone state
Zoning is OFF
```

- (B) Enable zoning

```
cmd> phyzone on
```

- (C) Disable zoning

```
cmd> phyzone off
```



NOTE

If you need to configure T10 zoning, we recommend using the "one-click" function for T10 zoning of AIC JBOD BMC. Please refer to [4.4.6.2 Zone Setting](#) for a simple setting. The following section [4.3.2.1 How to configure T10 zoning](#) is for T10 zoning manual settings and can be skipped.

4.3.2.2 How to configure T10 zoning

Remove the SAS cable (SFF-8644) between the HBA/RAID card and the JBOD-4U78 before configuration T10 zoning. After configuring T10 zoning, please power cycle the JBOD-4U78 and then insert the SAS cable back (SFF-8644).

After enabling T10 zoning, five predefined groups are Group1, Group8, Group9, Group10, and Group11. Each PHY should be in one of the five groups, and all PHYs in a wide port should be in the same group. Each PHY in Group1 can access any PHY in other groups, and

vice versa. Each PHY in Group8 cannot access any PHY in Group9, and vice versa.

The command syntax is "phyzone phy_index group." The following example shows how to setup one drive accessed only by the first port and another drive accessed only by the second port. The PHYs for the wide ports and drives in the example are not the PHY map in the 4U108swap.

The configuration for the example is

- (A) PHY8 - PHY11 for the first wide port of HUB
- (B) PHY4 - PHY7 for the second wide port of HUB
- (C) PHY20 - PHY35 for drives on EDGE

Step 1 Read the current group for PHY4 of HUB

```
cmd> phyzone 4  
Phy 4 for Zone Group 1
```

Step 2 Assign the second port (PHY4 - PHY7) for Group9

```
cmd> phyzone 4 9  
cmd> phyzone 5 9  
cmd> phyzone 6 9  
cmd> phyzone 7 9
```

Step 3 Assign the first port (PHY8 - PHY11) of HUB for Group8

```
cmd> phyzone 8 8  
cmd> phyzone 9 8  
cmd> phyzone 10 8  
cmd> phyzone 11 8
```

Step 4 Assign the drive on PHY20 of EDGE to be accessed only by the first port of HUB instead of the second port

```
cmd> phyzone 20 8
```

Step 5 Assign the drive on PHY21 of EDGE to be accessed only by the second port of HUB instead of the first port

```
cmd> phyzone 21 9
```

Step 6 Rest HUB and EDGE for taking effect with the new settings.

```
cmd> reset
```


**NOTE**

The command syntax is “phyzone phy_index group”.

EDGE setting: This command can only set the corresponding group of different PHY ID.

For different kind of models and backplanes, the slot number does not equal to PHY ID number. JBOD slot number equals to CONN ELEM INDEX (CONN TYPE=0x20).

JBOD slot 1(Decimal) <=> CONN ELEM INDEX 0x01(Hexadecimal) <=> PHY ID (Decimal)

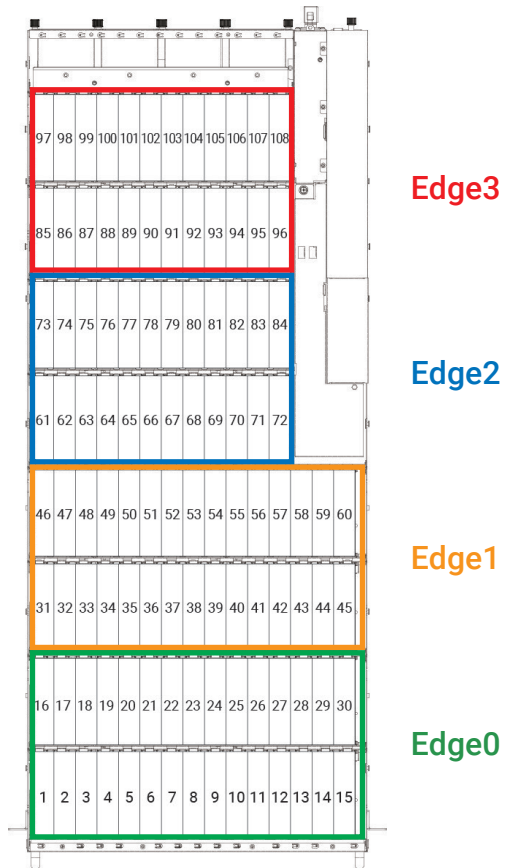
Slot 1 <=> 0x01 <=> 29

```
cmd >phyinfo
```

PHY ID	DEV TYPE	PHY CNL	PHY CNT	SSSSSSS STMSTMA PPPPPPT IIITTTA	ATTACHED	SAS	ADDR	ROUTE TYPE	ZONE GRP	ZONE CTRL BUS	CONN TYPE	CONN ELEM INDEX	CONN PHY LINK	MAP PHY ID	DR FR BL
00		0x0	0x01	-----				D	0x01	0x04	0x20	0x04	0x00	003	11
01		0x0	0x01	-----				D	0x01	0x04	0x20	0x05	0x00	004	11
02		0x0	0x01	-----				D	0x01	0x04	0x20	0x06	0x00	005	11
03		0x0	0x01	-----				D	0x01	0x04	0x20	0x07	0x00	006	11
04		0x0	0x01	-----				D	0x01	0x04	0x20	0x08	0x00	007	11
05		0x0	0x01	-----				D	0x01	0x04	0x20	0x09	0x00	008	11
06		0x0	0x01	-----				D	0x01	0x04	0x20	0x0A	0x00	009	11
07		0x0	0x01	-----				D	0x01	0x04	0x20	0x0B	0x00	010	11
08		0x0	0x01	-----				D	0x01	0x04	0x20	0x0C	0x00	011	11
09		0x0	0x01	-----				D	0x01	0x04	0x20	0x0D	0x00	012	11
10		0x0	0x01	-----				D	0x01	0x04	0x20	0x0E	0x00	013	11
11		0x0	0x01	-----				D	0x01	0x04	0x20	0x0F	0x00	014	11
12		0x0	0x01	-----				D	0x01	0x04	0x20	0x1E	0x00	029	11
13		0x0	0x01	-----				D	0x01	0x04	0x20	0x1D	0x00	028	11
14		0x0	0x01	-----				D	0x01	0x04	0x20	0x1C	0x00	027	11
15		0x0	0x01	-----				D	0x01	0x04	0x20	0x1B	0x00	026	11
16	EXP	12G	0x07	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	030	--
17	EXP	12G	0x07	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	031	--
18	EXP	12G	0x07	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	032	--
19	EXP	12G	0x07	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	033	--
20	EXP	12G	0x07	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	034	--
21	EXP	12G	0x07	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	035	--
22	EXP	12G	0x07	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	036	--
23	EXP	12G	0x06	-----1-	50015823_684A883F			T	0x01	0x04	0x00	0x00	0x00	037	--
24		0x0	0x01	-----				D	0x01	0x04	0x20	0x1A	0x00	025	11
25		0x0	0x01	-----				D	0x01	0x04	0x20	0x19	0x00	024	11
26		0x0	0x01	-----				D	0x01	0x04	0x20	0x18	0x00	023	11
27		0x0	0x01	-----				D	0x01	0x04	0x20	0x17	0x00	022	11
28		0x0	0x01	-----				D	0x01	0x04	0x20	0x00	0x00	038	--
29		0x0	0x01	-----				D	0x01	0x04	0x20	0x01	0x00	000	11
30		0x0	0x01	-----				D	0x01	0x04	0x20	0x02	0x00	001	11
31		0x0	0x01	-----				D	0x01	0x04	0x20	0x03	0x00	002	11
32		0x0	0x01	-----				D	0x01	0x04	0x20	0x16	0x00	021	11
33		0x0	0x01	-----				D	0x01	0x04	0x20	0x15	0x00	020	11
34		0x0	0x01	-----				D	0x01	0x04	0x20	0x14	0x00	019	11
35		0x0	0x01	-----				D	0x01	0x04	0x20	0x13	0x00	018	11
36		0x0	0x01	-----				D	0x01	0x04	0x20	0x12	0x00	017	11
37		0x0	0x01	-----				D	0x01	0x04	0x20	0x11	0x00	016	11
38		0x0	0x01	-----				D	0x01	0x04	0x20	0x10	0x00	015	11
39		0x0	0x01	-----				D	0x01	0x04	0x00	0x00	0x00	039	--
SXP0	END	12G	0x02	--11---	50015821_68453C3D			D	0x01	0x04	0x2F	0x4F	0x00	040	
SXP1	END	12G	0x01	1----1-	50015821_68453C3F			D	0x01	0x04	0x2F	0x50	0x00	041	
SXP2	END	12G	0x01	-1-----	50015821_68453C3E			D	0x01	0x04	0x2F	0x51	0x00	042	

Expander Change Count: 005e
Zone Configuring: 0
Self Configuring: 0
Configuring: 0

Edge0, Edge1, Edge2, Edge3 Top View Location

Table 1 **Edge3** PHY ID to JBOD slot number

slot 97	slot 98	slot 99	slot 100	slot 101	slot 102	slot 103	slot 104	slot 105	slot 106	slot 107	slot 108
PHY 35	PHY 34	PHY 33	PHY 32	PHY 27	PHY 26	PHY 25	PHY 24	PHY 15	PHY 14	PHY 13	PHY 12
slot 85	slot 86	slot 87	slot 88	slot 89	slot 90	slot 91	slot 92	slot 93	slot 94	slot 95	slot 96
PHY 00	PHY 01	PHY 02	PHY 03	PHY 04	PHY 05	PHY 06	PHY 07	PHY 08	PHY 09	PHY 10	PHY 11

Table 2 **Edge2** PHY ID to JBOD slot number

slot 73	slot 74	slot 75	slot 76	slot 77	slot 78	slot 79	slot 80	slot 81	slot 82	slot 83	slot 84
PHY 35	PHY 34	PHY 33	PHY 32	PHY 27	PHY 26	PHY 25	PHY 24	PHY 15	PHY 14	PHY 13	PHY 12
slot 61	slot 62	slot 63	slot 64	slot 65	slot 66	slot 67	slot 68	slot 69	slot 70	slot 71	slot 72
PHY 00	PHY 01	PHY 02	PHY 03	PHY 04	PHY 05	PHY 06	PHY 07	PHY 08	PHY 09	PHY 10	PHY 11

Table 3 Edge1 PHY ID to JBOD slot number

slot 46	slot 47	slot 48	slot 49	slot 50	slot 51	slot 52	slot 53	slot 54	slot 55	slot 56	slot 57	slot 58	slot 59	slot 60
PHY 38	PHY 37	PHY 36	PHY 35	PHY 34	PHY 33	PHY 32	PHY 27	PHY 26	PHY 25	PHY 24	PHY 15	PHY 14	PHY 13	PHY 12
slot 31	slot 32	slot 33	slot 34	slot 35	slot 36	slot 37	slot 38	slot 39	slot 40	slot 41	slot 42	slot 43	slot 44	slot 45
PHY 29	PHY 30	PHY 31	PHY 00	PHY 01	PHY 02	PHY 03	PHY 04	PHY 05	PHY 06	PHY 07	PHY 08	PHY 09	PHY 10	PHY 11

Table 4 Edge0 PHY ID to JBOD slot number

slot 16	slot 17	slot 18	slot 19	slot 20	slot 21	slot 22	slot 23	slot 24	slot 25	slot 26	slot 27	slot 28	slot 29	slot 30
PHY 38	PHY 37	PHY 36	PHY 35	PHY 34	PHY 33	PHY 32	PHY 27	PHY 26	PHY 25	PHY 24	PHY 15	PHY 14	PHY 13	PHY 12
slot 1	slot 2	slot 3	slot 4	slot 5	slot 6	slot 7	slot 8	slot 9	slot 10	slot 11	slot 12	slot 13	slot 14	slot 15
PHY 29	PHY 30	PHY 31	PHY 00	PHY 01	PHY 02	PHY 03	PHY 04	PHY 05	PHY 06	PHY 07	PHY 08	PHY 09	PHY 10	PHY 11

For example, to assign JBOD slot 1-4 (PHY29/PHY30/PHY31/PHY00) for group 8.

```
cmd> phyzone 29 08
```

```
cmd> phyzone 30 08
```

```
cmd> phyzone 31 08
```

```
cmd> phyzone 00 08
```

```
cmd >phyzone on
Succeeded to enable zoning

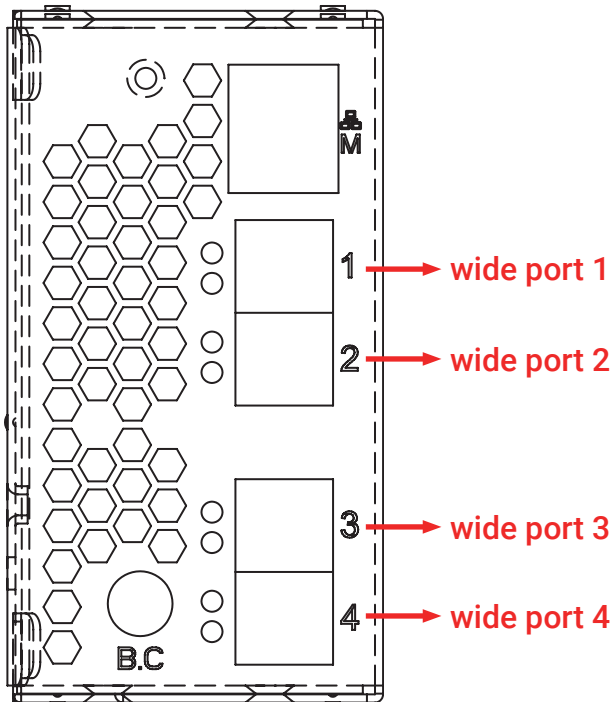
cmd >phyzone 29 08
Succeeded to set zone group for the phy

cmd >phyzone 30 08
Succeeded to set zone group for the phy

cmd >phyzone 31 08
Succeeded to set zone group for the phy

cmd >phyzone 00 08
Succeeded to set zone group for the phy
```

HUB setting: There are four PHY ID number of each wide port. Please refer to the following table of Hub "PHY ID" and JBOD "wide port".



HUB PHY ID to JBOD wide port

wide port 1			
PHY12	PHY13	PHY14	PHY15
wide port 2			
PHY08	PHY09	PHY10	PHY11
wide port 3			
PHY04	PHY05	PHY06	PHY07
wide port 4			
PHY00	PHY01	PHY02	PHY03

For example, to assign wide port 1 (PHY12-PHY15) for group 8.

```
cmd> phyzone 12 08
cmd> phyzone 13 08
cmd> phyzone 14 08
cmd> phyzone 15 08
```



NOTE

Power Cycle

For dual expander JBOD, complete the setting of EDGE and HUB. Meanwhile, PRI EXP and SEC EXP should be applied with the same configuration. After the T10 zoning configuration, you need to power cycle the JBOD to make PRI EXP and SEC EXP simultaneously operate.

4.3.2.3 How to get all revisions in AIC® SAS 12G Expander

- (A) Expander firmware revision
cmd> rev
- (B) Expander configuration revision
cmd> showmfg
- (C) MCU firmware revision or sensor information (MCU firmware revision is reported by Hub only)
cmd> sensor

4.3.2.4 How to configure enclosure address (HUB only)

- (A) Get the current enclosure address
cmd> enclosure_addr
Enclosure Address: 0x500605B0000272BF
- (B) Set the enclosure address with 0x500605B0000272BF. The new setting will take effect after reset.
cmd> enclosure_addr 500605B0000272BF
cmd> reset

4.3.2.5 How to configure standby timer for all disk drives(EDGE only)

This feature is applicable for SAS/SATA drives. Standby timer is in units of minutes. Setting standby timer with 0 minute disables this feature.

- (A) Get current standby timer
cmd> standby_timer
Standby Timer : 0 minutes
- (B) Set the standby timer with 10 minutes. The new setting will take effect after reset.
cmd> standby_timer 10
cmd> reset

**NOTE**

This function is not recommended to use with RAID card since RAID card limitation.

4.3.2.6 How to configure wide port checker

This feature is applicable for SAS drives instead of SATA drives. If there is no connection with any active SAS initiator by checking all wide ports, AIC® Expander Controller stops all attached SAS drives to save power consumption of SAS drives. Otherwise, AIC® Expander Controller starts all attached SAS drives to provide drive access service to any active SAS initiator. The same setting should be applied to HUB and EGDE.

- (A) Get the current state of wide port checker


```
cmd> check_wide_port
Checking wide port is OFF
```
- (B) Enable checking wide port. The new setting will take effect after reset.


```
cmd> check_wide_port on
cmd> reset
```
- (C) Disable checking wide port. The new setting will take effect after reset.


```
cmd> check_wide_port off
cmd> reset
```

4.3.2.7 How to power off/on all disk drives automatically

This feature is applicable for SAS/SATA drives. If there is no connection with any active SAS initiator by checking all wide ports, AIC® Expander Controller powers off all attached SAS/SATA drives to save power consumption. Otherwise, AIC® Expander Controller powers on all attached SAS/SATA drives to provide drive access service to any active SAS initiator. The same setting should be applied to HUB and EDGE.

```
cmd> check_wide_port standby
cmd> reset
```

4.3.2.8 How to configure EDFB (EDGE only)

The default EDFB configuration is off.

- (A) Check the current configuration


```
cmd> edfb
EDFB is OFF
```
- (B) Enable the EDFB


```
cmd>edfb on
```
- (C) Disable the EDFB


```
cmd> edfb off
```

4.3.2.9 How to configure power setting (HUB only)

This feature is for restoring on AC power loss. Three supported options are "keep off," "keep on," and "keep last state." The default setting is "keep off."


NOTE

This feature will be over-written by Hub MFG since Hub firmware 1.12.48.61.

- (A) Get the current power setting
`cmd> power_setting`
 Power setting: keep off
- (B) Set "keep off"
`cmd> power_setting keep_off`
- (C) Set "keep on"
`cmd> power_setting keep_on`
- (D) Set "keep last state"
`cmd> power_setting keep_last_state`

4.3.2.10 How to configure zone count

Before you begin, your JBOD must be equipped with HUB/EDGE setting.

There are 3 kinds of zoning options that can be implemented by Command Line interface operation . By using the zoning option, four of the 8644 ports will have a variety of zone group settings.

Remove the SAS cable between the HBA/RAID card and the 4U108swap before configuring zone count. Power the 4U108swap off after configuring zone count. Power on the 4U108swap, and then insert the SAS cable.

Four zone configurations supported are one zone, two zones, three zones, and four zones. The default configuration is one zone of which T10 zoning configuration is disabled. T10 zoning configuration of the other configurations (two zones, three zones, and four zones) is enabled. All COM ports for Hub and Edge should be applied with the same configuration.

- (A) Get current zone count `cmd> zonecount`
 Zone Count 1
- (B) Set zone count = 2
`cmd> zonecount 2`
 Succeeded to set zone count 2

(C) Predefined zones

(C-1) When Zone Count = 1, T10 zoning is disabled.

HUB:

Zone #	1
Wideport	1, 2, 3, 4

EDGE:

Zone #	1
Slot	1~108

(C-2) When Zone Count = 2, T10 zoning is enabled.

HUB:

Zone #	1	2
Wideport	1, 2	3, 4

EDGE:

Zone #	1	2
Slot	1~54	55~108

(C-3) When Zone Count = 3, T10 zoning is enabled.

HUB:

Zone #	1	2	3	X
Wideport	1	2	3	4

EDGE:

Zone #	1	2	3
Slot	1~36	37~72	73~108

(C-4) When Zone Count = 4, T10 zoning is enabled.

HUB:

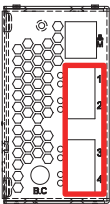
Zone #	1	2	3	4
Wideport	1	2	3	4

EDGE:

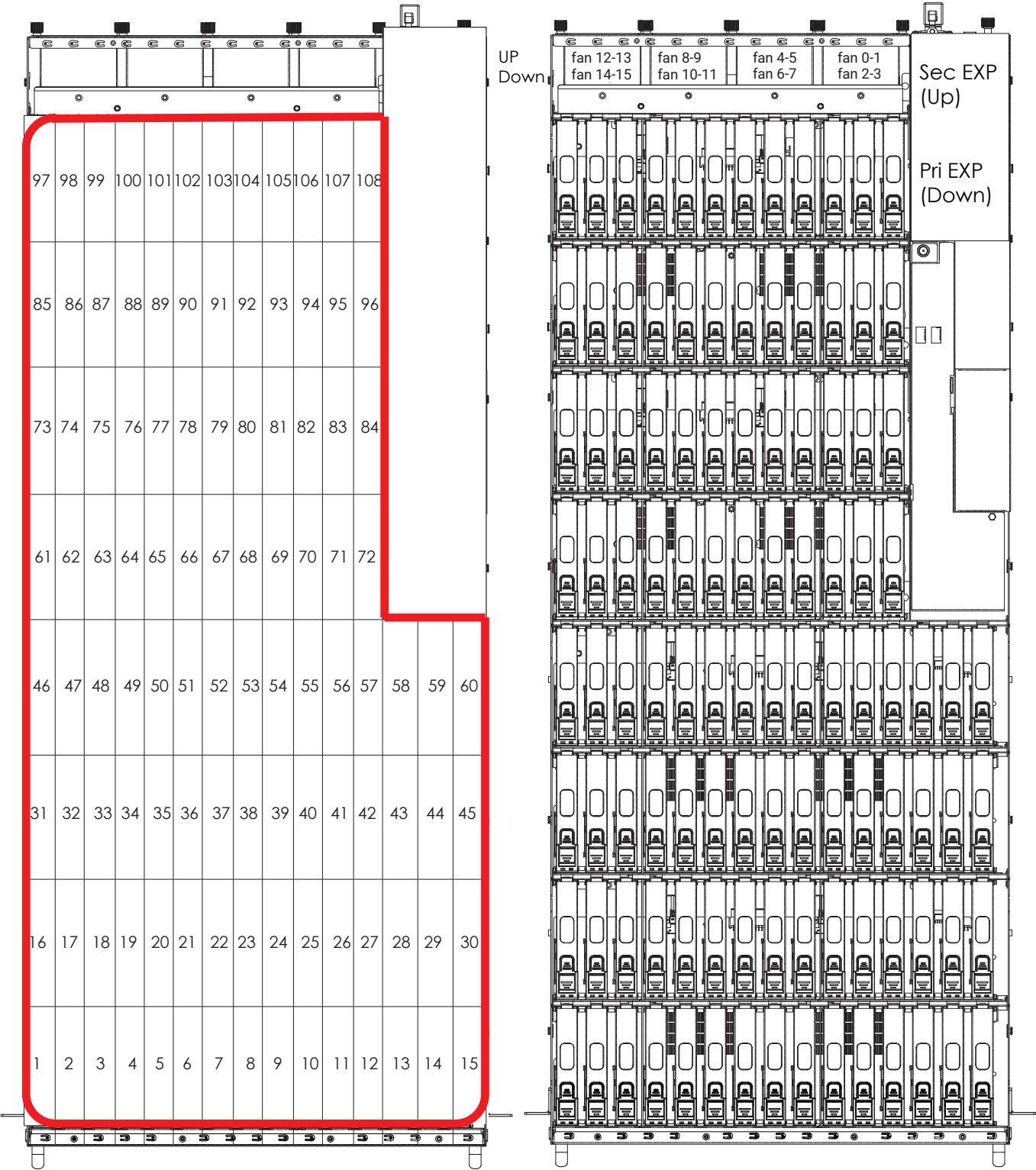
Zone #	1	2	3	4
Slot	1~27	28~54	55~81	82~108

Zone count 1:
108 drives per zone. All SFF-8644
ports and drives are at the same zone
group.
SEE FIGURE BELOW.

Expander rear panel



Group 1

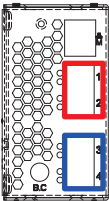


Zone count 2:

54 drives per zone. Port 1 and port 2 are in zone group 1. Port 3 and 4 are in zone group 2.

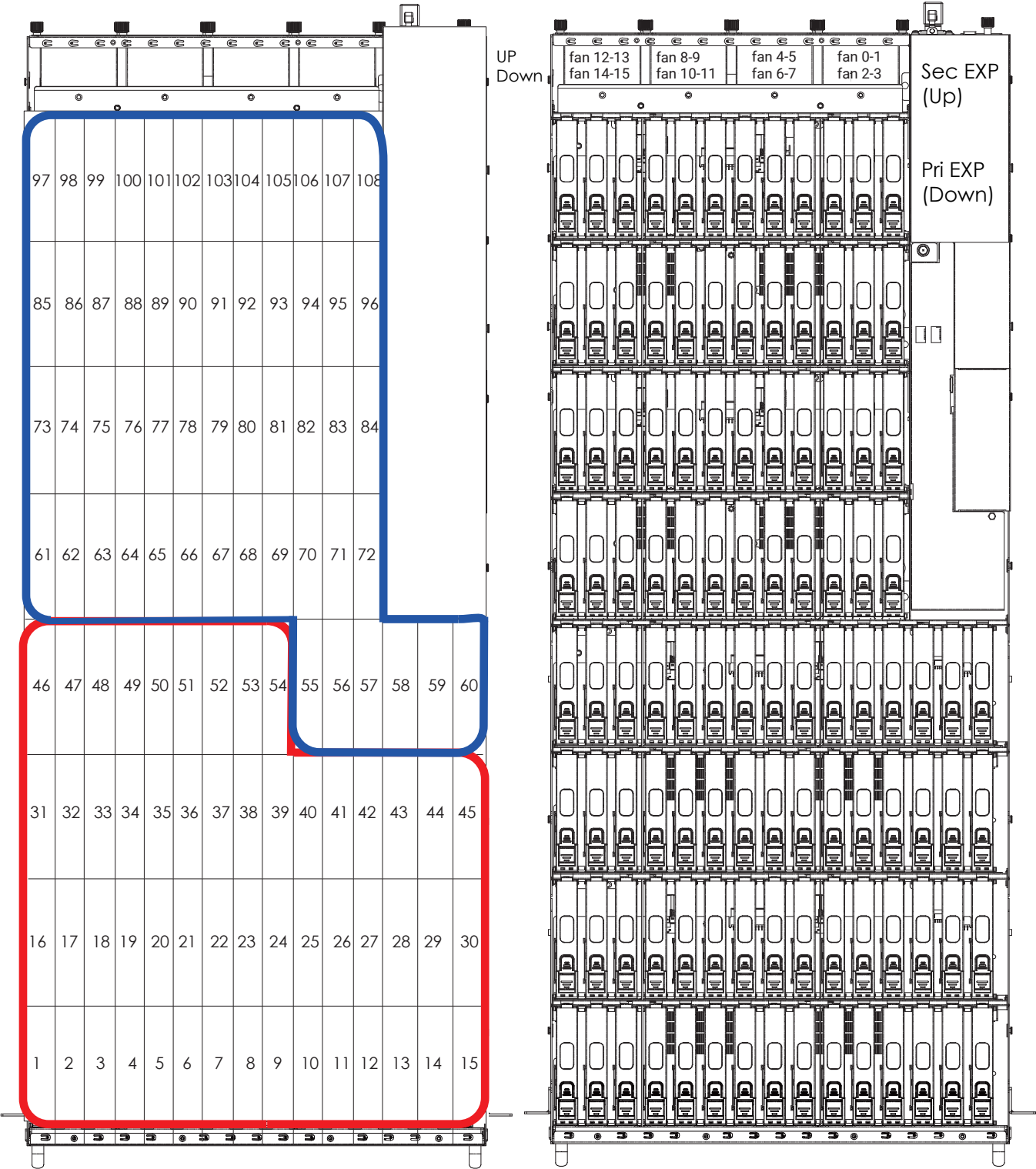
SEE FIGURE BELOW.

Expander rear panel



Group 1

Group 2

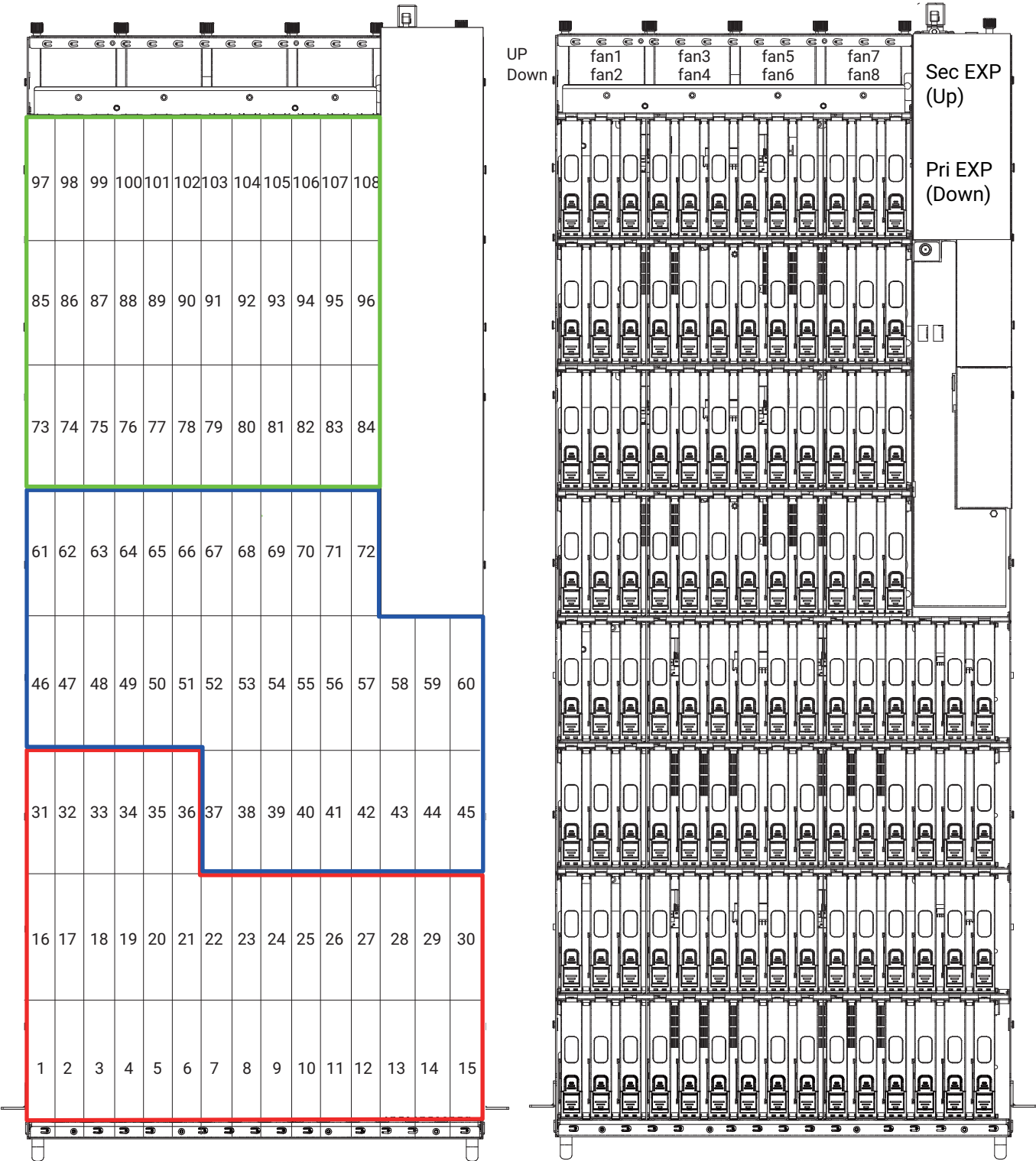
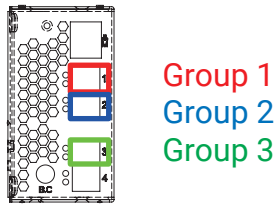


Zone count 3:

36 drives per zone. Port 1 is in zone group1, port 2 is in zone group 2. Port 3 is in zone group 3.

SEE FIGURE BELOW.

Expander rear panel

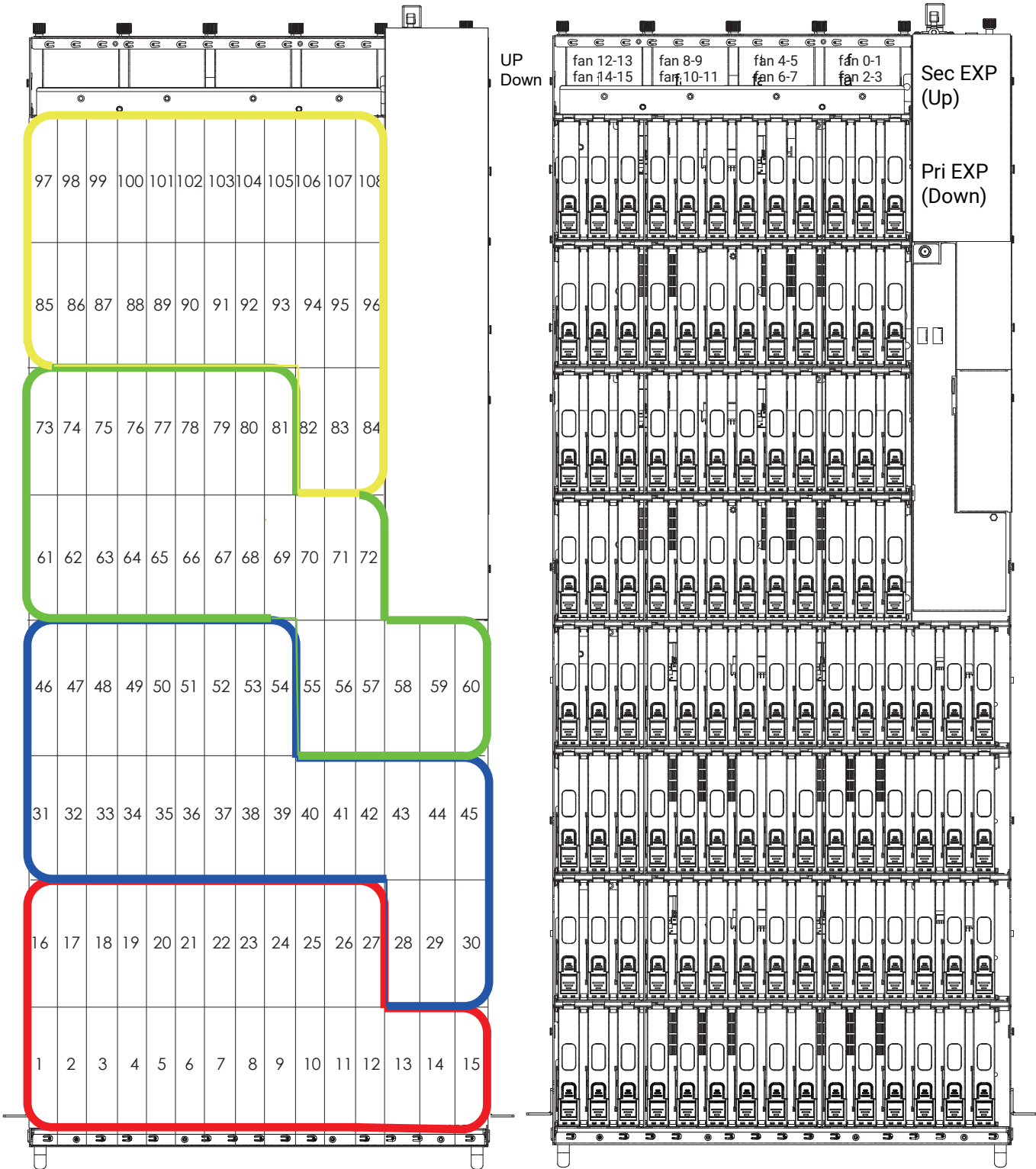
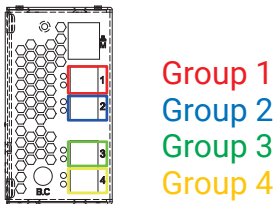


Zone count 4:

27 drives per zone. Port 1 is in zone group1, port 2 is in zone group 2. Port 3 is in zone group3 and port 4 is in zone group 4.

SEE FIGURE BELOW.

Expander rear panel



4.3.2.11 How to configure zoning of the wide port (HUB only)

Remove the SAS cable (SFF-8644) between the HBA/RAID card and the JBOD-4U78 before configuration T10 zoning. After configuring T10 zoning, please power cycle the JBOD-4U78 and then insert the SAS cable back (SFF-8644).

After enabling T10 zoning, five predefined groups are Group1, Group8, Group9, Group10, and Group11.

- (A) Get current zoning of wide port 1

```
cmd> zone_port 1
Wideport 01 for Zone Group 01
```

- (B) Set wideport 1 as Zone Group 8

```
cmd> zone_port 1 8
Succeeded to set zone group for the phy
```

4.3.2.12 How to configure zoning of the disk slot (EDGE only)

Remove the SAS cable (SFF-8644) between the HBA/RAID card and the JBOD-4U78 before configuration T10 zoning. After configuring T10 zoning, please power cycle the JBOD-4U78 and then insert the SAS cable back (SFF-8644).

After enabling T10 zoning, five predefined groups are Group1, Group8, Group9, Group10, and Group11.

- (A) Get current zoning of Disk Slot 10

```
cmd> zone_slot 10
Slot 10 for Zone Group 1.
```

- (B) Set Disk Slot 10 as Zone Group 8

```
cmd> zone_slot 10 8
Succeeded to set zone group for the phy
```

4.3.3 SES Inband Features

To ensure proper function, high performance, and durability, J4108-01-35X has implemented SCSI Enclosure Services to monitor the status of power supply, system cooling fan, and working temperature. It also has indicators to deliver the status of fail devices such as power supply or cooling fan. You can get the information directly from the front indicators to know how your enclosure works.

For detailed information, please visit <http://www.t10.org>

If you are a member of the T10 working group, the Standard which controlled by T10 technical committee, could be found at

<http://www.t10.org/cgi-bin/ac.pl?t=f&f=ses2r19a.pdf>

4.3.3.1 SES Pages

- 00h - List of supported diagnostic pages
- 01h - SES configuration
- 02h - SES enclosure control / enclosure status
- 04h - SES String In
- 05h - SES Threshold Out / In
- 07h - SES element descriptor
- 0Ah - SES additional element
- 0Eh - SES download microcode control / SES download microcode status
- 83h - SES Vendor specific page : Canister Number
- 8Ch - SES Vendor specific page : Firmware Version and MFG Version

4.3.3.2 SES Elements

- 02h - Power Supply
- 03h - Cooling
- 04h - Temperature Sensor
- 0Eh - Enclosure
- 12h - Voltage
- 17h - Array Device

4.3.3.3 Implementation on SES Pages

SES String In Page

Get PMBUS information with String In Page.

String In format

BYTE/BIT	7	6	5	4	3	2	1	0
0	I2C congestion (0: no congestion, 1: congestion or failure)							
1	PSU Module1 STATUS_WORD							
2								
3	PSU Module2 STATUS_WORD							
4								
5-14	Reserved (0xFF)							

SES Threshold Out / In

It includes only Temperature Sensor and Voltage Sensor elements.

Threshold control element format

BYTE/BIT	7	6	5	4	3	2	1	0
0	REQUESTED HIGH CRITICAL THRESHOLD							
1	REQUESTED HIGH WARNING THRESHOLD							
2	REQUESTED LOW WARNING THRESHOLD							
3	REQUESTED LOW CRITICAL THRESHOLD							

Threshold status element format

BYTE/BIT	7	6	5	4	3	2	1	0
0	HIGH CRITICAL THRESHOLD							
1	HIGH WARNING THRESHOLD							
2	LOW WARNING THRESHOLD							
3	LOW CRITICAL THRESHOLD							

SES Vendor specific page: Canister Number (page code 83h) Out / In

The length N of canister number can be 0~30 bytes. If no canister number is entered (N=0), then canister number is restored to default: 0x20 0x20 0x20 0x20 0x20 0x20 0x20 0x20 (8 spaces in ASCII).

Canister Number control format

BYTE/BIT	7	6	5	4	3	2	1	0
0~N	Canister Number							

If no canister number is found, return Status = 1 (failed) only, else return Status=0 (success) followed by canister number.

Canister Number status format

BYTE/BIT	7	6	5	4	3	2	1	0
0	Status (0: success, 1: failed)							
1~N (if success)	Canister Number							

SES Vendor specific page: Firmware Version and MFG Version (page code 8Ch) In

There are one firmware version (4 bytes) and one MFG version (4 bytes) per expander. There are 4 expanders in 4U78 and 5 expanders in 4U108.

Firmware Version and MFG Version status format

BYTE/BIT	7	6	5	4	3	2	1	0
0~3	Hub expander firmware version							
4~7	Hub expander MFG version							
8~11	First Edge firmware version							
12~15	First Edge MFG version							
16~19	Second Edge firmware version							
20~23	Second Edge MFG version							
24~27	Third Edge firmware version							
28~31	Third Edge MFG version							
32~35	Fourth Edge firmware version (only applicable to 4U108)							
36~39	Fourth Edge MFG version (only applicable to 4U108)							

4.3.3.4 Implementation on SES Elements

Only the fields highlighted in green are supported.

Power Supply Element

(A) Power Supply Control Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	Reserved						
2	Reserved							
3	Reserved	RQST FAIL	RQST ON	Reserved				

Field	Value
RQST ON	Please refer to section “SES Element Control Functions” for details.

(B) Power Supply Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLE	SWAP	ELEMENT STATUS CODE			
1	IDENT	Reserved						
2	Reserved				DC OVER VOLTAGE	DC UNDER VOLTAGE	DC OVER CURRENT	Reserved
3	HOT SWAP	FAIL	RQSTED ON	OFF	OVERTMP FAIL	TEMP WARN	AC FAIL	DC FAIL

Field	Value
ELEMENT STATUS CODE	OK: No failure or warning conditions detected CRITICAL: FAIL bit is set due to one or more failure condition
FAIL	A failure condition is detected
RQSTED ON	1: On 0: Off
OFF	1: Off 0: On
AC FAIL	A failure condition is detected
DC FAIL	A failure condition is detected

Cooling Element

(A) Cooling Control Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	Reserved						
2	Reserved							
3	Reserved	RQST FAIL	RQST ON	Reserved		REQUESTED SPEED CODE		

Field	Value
RQST IDENT	Please refer to section “SES Element Control Functions” for details.
REQUESTED SPEED CODE	Please refer to section “SES Element Control Functions” for details.

(B) Cooling Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLE	SWAP	ELEMENT STATUS CODE			
1	IDENT	Reserved				ACTUAL FAN SPEED (MSB)		
2	ACTUAL FAN SPEED (LSB)							
3	HOT SWAP	FAIL	RQSTED ON	OFF	Reserved	ACTUAL SPEED CODE		

Field	Value
ELEMENT STATUS CODE	OK: Actual fan speed > 0 CRITICAL: The fan RPM can't be detected or equal to 0.
IDENT	Applicable only for Cooling element 0 0: Enable the smart fan function 1: Disable the smart fan function
ACTUAL FAN SPEED	Current fan RPM
FAIL	The fan RPM can't be detected or equal to 0.

Temperature Sensor Element

(A) Temperature Sensor Control Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	RQST FAIL	Reserved					
2	Reserved							
3	Reserved							

(B) Temperature Sensor Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLE	SWAP	ELEMENT STATUS CODE			
1	IDENT	FAIL	Reserved					
2	TEMPERATURE							
3	Reserved				OT FAILURE	OT WARNING	UT FAILURE	UT WARNING

Field	Value
ELEMENT STATUS CODE	OK: Everything is Ok NON-CRITICAL: If either warning limit is exceeded CRITICAL: If either failure limit is exceeded
FAIL	A warning or failure condition is detected
TEMPERATURE	Temperature reading
OT FAILURE	Temperature has exceeded the failure high threshold value
OT WARNING	Temperature has exceeded the warning high threshold value
UT FAILURE	Temperature is below the failure low threshold value
UT WARNING	Temperature is below the warning low threshold value

Enclosure Element**(A) Enclosure Control Element**

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	Reserved						
2	POWER CYCLE REQUEST		POWER CYCLE DELAY					
3	POWER OFF DURATION						REQUEST FAILURE	REQUEST WARNING

Field	Value
POWER CYCLE REQUEST	Please refer to section "SES Element Control Functions" for details.
POWER CYCLE DELAY	Please refer to section "SES Element Control Functions" for details.
POWER OFF DURATION	Please refer to section "SES Element Control Functions" for details.
REQUEST FAILURE	Please refer to section "SES Element Control Functions" for details.
REQUEST WARNING	Please refer to section "SES Element Control Functions" for details.

(B) Enclosure Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLE	SWAP	ELEMENT STATUS CODE			
1	IDENT	Reserved						
2	TIME UNTIL POWER CYCLE						FAILURE INDICATION	WARNING INDICATION
3	REQUEST POWER OFF DURATION						FAILURE REQUESTED	WARNING REQUESTED

Field	Value
ELEMENT STATUS CODE	OK
TIME UNTIL POWER CYCLE	The time until the enclosure's power is scheduled to be off. 0: No Power cycle scheduled, 1~60: The enclosure is scheduled to begin a power cycle after the indicated number of minutes. 63: The enclosure is scheduled to begin a power cycle after zero minute.

REQUEST POWER OFF DURATION	The time that power is scheduled to keep off when power is cycled. 0: (i) No power cycle is scheduled or (ii) It is scheduled to be kept off for 10 seconds. 1~60: Power is scheduled to be kept off for the indicated number of minutes. 63: Power is scheduled to be kept off until manually restored.
FAILURE REQUESTED	Set by the REQUEST FAILURE on Enclosure Control Element
WARNING REQUESTED	Set by the REQUEST WARNING on Enclosure Control Element.

Voltage Element

(A) Voltage Control Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	RQST FAIL	Reserved					
2	Reserved							
3	Reserved							

(B) Voltage Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLE	SWAP	ELEMENT STATUS CODE			
1	IDENT	FAIL	Reserved		WARN OVER	WARN UNDER	CRIT OVER	CRIT UNDER
2	VOLTAGE							
3								

Field	Value
ELEMENT STATUS CODE	OK: Everything is Ok NON-CRITICAL: If either warning limit is exceeded CRITICAL: If either failure limit is exceeded
FAIL	A warning or failure condition is detected
WARN OVER	Voltage has exceeded the warning high threshold value
WARN UNDER	Voltage is below the warning low threshold value
CRIT OVER	Voltage has exceeded the failure high threshold value
CRIT UNDER	Voltage is below the failure low threshold value
VOLTAGE	Voltage reading

Array Device Element

(A) Array Device Control Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved0			
1	RQST OK	RQST RSVD DEVICE	RQST HOT SPARE	RQST CONS CHECK	RQST IN CRIT ARRAY	RQST IN FAILED ARRAY	RQST REBUILD/REMAP	RQST R/R ABORT
2	RQST ACTIVE	DO NOT REMOVE	Reserved 2	RQST MISSING	RQST INSERT	RQST REMOVE	RQST IDENT	Reserved 1
3	Reserved 5	Reserved 4	RQST FAULT	DEVICE OFF	ENABLE BYP A	ENABLE BYP B	Reserved3	

Field	Value
PRDFAIL	Please refer to section “SES Element Control Functions” for details.
RQST OK	Please refer to section “SES Element Control Functions” for details.
RQST RSVD DEVICE	Please refer to section “SES Element Control Functions” for details.
RQST HOT SPARE	Please refer to section “SES Element Control Functions” for details.
RQST CONS CHECK	Please refer to section “SES Element Control Functions” for details.
RQST IN CRIT ARRAY	Please refer to section “SES Element Control Functions” for details.
RQST IN FAILED ARRAY	Please refer to section “SES Element Control Functions” for details.
RQST REBUILD/REMAP	Please refer to section “SES Element Control Functions” for details.
RQST R/R ABORT	Please refer to section “SES Element Control Functions” for details.
RQST ACTIVE	Please refer to section “SES Element Control Functions” for details.
DO NOT REMOVE	Please refer to section “SES Element Control Functions” for details.
Reserved2	Please refer to section “SES Element Control Functions” for details.
RQST MISSING	Please refer to section “SES Element Control Functions” for details.
RQST INSERT	Please refer to section “SES Element Control Functions” for details.
RQST REMOVE	Please refer to section “SES Element Control Functions” for details.
RQST IDENT	Please refer to section “SES Element Control Functions” for details.
Reserved5	Please refer to section “SES Element Control Functions” for details.
RQST FAULT	Please refer to section “SES Element Control Functions” for details.
DEVICE OFF	Please refer to section “SES Element Control Functions” for details.

(B) Array Device Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLE	SWAP	ELEMENT STATUS CODE			
1	OK	RSVD DEVICE	HOT SPARE	CONS CHK	IN CRIT ARRAY	IN FAILED ARRAY	REBUILD/REMAP	R/R ABORT
2	APP CLIENT BYPASSED A	DO NOT REMOVE	ENCLOSURE BYPASSED A	ENCLOSURE BYPASSED B	READY TO INSERT	RMV	IDENT	REPORT
3	APP CLIENT BYPASSED B	FAULT SENSED	FAULT REQSTD	DEVICE OFF	BYPASSED A	BYPASSED B	DEVICE BYPASSED A	DEVICE BYPASSED B

Field	Value
PRDFAIL	Set by the PRDFAIL on Array Device Control Element
ELEMENT STATUS CODE	OK: A drive is detected in the slot NOT INSTALLED: No drive is installed in the slot
OK	Set by the RQST OK on Array Device Control Element
RSVD DEVICE	Set by the RQST RSVD DEVICE on Array Device Control Element
HOT SPARE	Set by the RQST HOT SPARE on Array Device Control Element
CONS CHK	Set by the RQST CONS CHECK on Array Device Control Element
IN CRIT ARRAY	Set by the RQST IN CRIT ARRAY on Array Device Control Element
IN FAILED ARRAY	Set by the RQST IN FAILED ARRAY on Array Device Control Element
REBUILD/REMAP	Set by the RQST REBUILD/REMAP on Array Device Control Element
R/R ABORT	Set by the RQST R/R ABORT on Array Device Control Element
DO NOT REMOVE	Set by the DO NOT REMOVE on Array Device Control Element
READY TO INSERT	Set by the RQST INSERT on Array Device Control Element
RMV	Set by the RQST REMOVE on Array Device Control Element
IDENT	Set by the RQST IDENT on Array Device Control Element
FAULT REQSTD	Set by the RQST FAULT on Array Device Control Element
DEVICE OFF	Set by the DEVICE OFF on Array Device Control Element

4.3.3.5 SES Element Control Functions

LED indicators (blue and red) associated with an attached disk drive**Array Device Slot control element**

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved0			
1	RQST OK	RQST RSVD DEVICE	RQST HOT SPARE	RQST CONS CHECK	RQST IN CRIT ARRAY	RQST IN FAILED ARRAY	RQST REBUILD/REMAP	RQST R/R ABORT
2	RQST ACTIVE	DO NOT REMOVE	Reserved 2	RQST MISSING	RQST INSERT	RQST REMOVE	RQST IDENT	Reserved 1
3	Reserved 5	Reserved 4	RQST FAULT	DEVICE OFF	ENABLE BYP A	ENABLE BYP B	Reserved 3	

The default behavior for blue LED is "LED is on when the disk is not busy, and off when the disk is executing a command." When the "RQST IDENT" bit is set, the blue LED overwrites its default behavior with a slow blink while the red LED is off. The blue LED is set "Activity" for not overwriting its default behavior.

The behavior "Fast Blink" is "LED is blinking at 2Hz frequency."

The behavior "Slow Blink" is "LED is blinking at 0.5Hz frequency."

The behavior "ON"/"OFF" is "LED is solid ON/OFF without blinking."

Slot Control Bit	Blue LED	Red LED
RQST OK	Activity	OFF
RQST RSVD DEVICE	Activity	OFF
RQST HOT SPARE	Activity	OFF
RQST CONS CHECK	Activity	Fast Blink
RQST IN CRIT ARRAY	Activity	Slow Blink
RQST IN FAILED ARRAY	Activity	Slow Blink
RQST REBUILD/REMAP	Activity	Fast Blink
RQST R/R ABORT	Activity	Slow Blink
RQST ACTIVE	Activity	OFF
DO NOT REMOVE	Activity	OFF
RQST MISSING	ON	ON
RQST INSERT	Activity	Slow Blink
RQST REMOVE	Activity	Slow Blink
RQST IDENT	Slow Blink	OFF
RQST FAULT	ON	ON
DEVICE OFF	OFF	OFF
PRDFAIL	Activity	Slow Blink

How to turn on/off the power of a drive slot**Array Device Slot control element**

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved0			
1	RQST OK	RQST RSVD DEVICE	RQST HOT SPARE	RQST CONS CHECK	RQST IN CRIT ARRAY	RQST IN FAILED ARRAY	RQST REBUILD/REMAP	RQST R/R ABORT
2	RQST ACTIVE	DO NOT REMOVE	Reserved 2	RQST MISSING	RQST INSERT	RQST REMOVE	RQST IDENT	Reserved 1
3	Reserved 5	Reserved 4	RQST FAULT	DEVICE OFF	ENABLE BYP A	ENABLE BYP B	Reserved3	

The "DEVICE OFF" for a drive slot is defined in the bit4, byte3 of the "Array Device Slot control element" in the SES specification. Set the bit to turn off a slot power, and vice versa. We use the software package "sg3_utils" on Linux for example, and have a SAS HBA and a cable to connect your host with the expander.

(A) Show the device for AIC® Expander Controller (canister)

```
$ sg_map -i
/dev/sg2 AIC 12G 4U108swapEdge 0c30
```

(B) Get the current state of a slot power. The "Device off=0" means the slot power is on.

```
$ sg_ses --page=2 /dev/sg2
```

Element 0 descriptor:

```
App client bypass B=0, Fault sensed=0, Fault reqstd=0, Device off=0
```

(C) Get the descriptor of a slot power

```
$ sg_ses --page=7 /dev/sg2
```

Element 0 descriptor: Disk001

(D) Turn off a slot power

```
$ sg_ses --descriptor=Disk001 --set=3:4:1 /dev/sg2
```

(E) Turn on a slot power

```
$ sg_ses --descriptor=Disk001 --clear=3:4:1 /dev/sg2
```

**NOTE**

This function is not recommended to use with RAID card since RAID card limitation.

How to power off the entire enclosure

Power Supply control element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	Reserved						
2	Reserved							
3	Reserved	RQST FAIL	RQST ON	Reserved				

The "RQST ON" for Power Supply is defined in the bit5, byte3 of the "Power Supply control element" in the SES specification. Clear the bit on Power Supply Element "PowerSupply00" or "PowerSupply01" to power off the entire enclosure. We use the software package "sg3_utils" on Linux for example, and have a SAS HBA and a cable to connect your host with the expander.

(A) Show the device for AIC® Expander Controller (canister)

```
$ sg_map -i
```

```
/dev/sg2  AIC    12G 4U108swapHub    0c30
```

(B) Power off the entire enclosure

```
$ sg_ses --descriptor=PowerSupply00 --clear=3:5:1 /dev/sg2
```

How to enable/disable the enclosure power cycle by your software

Enclosure control element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	Reserved						
2	POWER CYCLE REQUEST		POWER CYCLE DELAY					
3	POWER OFF DURATION						REQUEST FAILURE	REQUEST WARNING

The "POWER CYCLE REQUEST," "POWER CYCLE DELAY" and "POWER OFF DURATION" for Enclosure are defined in the bit7~6, byte2, bit5~0, byte2 and bit7~2, byte3 of the "Enclosure control element" in the SES specification. Set "POWER CYCLE REQUEST" as 01b to begin a power cycle in minutes set by "POWER CYCLE DELAY" (1~60 minutes, 0 for beginning power cycle immediately) and keep off for minutes set by "POWER OFF DURATION" (set 1~60 minutes, 0 for 10 seconds and 63 for keeping off). A request to begin a power cycle while a previous request is still active should override the previous request. Set "POWER CYCLE REQUEST" as 10b to cancel any scheduled power cycle.

(A) Show the device for AIC® Expander Controller (canister)

```
$ sg_map -i
```

```
/dev/sg2  AIC    12G 4U108swapHub    0c30
```

(B) Request to begin a power cycle (POWER CYCLE REQUEST = 01b) after 10 minutes (POWER CYCLE DELAY = 10 = 0Ah) and keep off for 3 minutes (POWER OFF DURATION =3):

```
sg_ses --descriptor=EnclosureElement00 --set=2:7:14=0x1283 /dev/sg2
```

How to enable/disable the enclosure alarm by your software**Enclosure control element**

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	Reserved						
2	POWER CYCLE REQUEST		POWER CYCLE DELAY					
3	POWER OFF DURATION						REQUEST FAILURE	REQUEST WARNING

The system alarm LED is used for the enclosure alarm and power alarm. The "REQUEST FAILURE" and "REQUEST WARNING" for Enclosure are defined in the bit1, byte3 and bit0, byte3 of the "Enclosure control element" in the SES specification. Setting either bit can enable the enclosure alarm. Clearing both bits disables the enclosure alarm. We use the software package "sg3_utils" on Linux for example, and have a SAS HBA and a cable to connect your host with the expander.

(A) Show the device for AIC® Expander Controller (canister)

```
$ sg_map -i
```

```
/dev/sg2  AIC 12G  4U108swapHub  0c30
```

(B) Enable the enclosure alarm

```
$ sg_ses --descriptor=EnclosureElement01 --set=3:1:1 /dev/sg2
```

or

```
$ sg_ses --descriptor=EnclosureElement01 --set=3:0:1 /dev/sg2
```

(C) Disable the enclosure alarm

```
$ sg_ses --descriptor=EnclosureElement01 --clear=3:1:1 /dev/sg2
```

and

```
$ sg_ses --descriptor=EnclosureElement01 --clear=3:0:1 /dev/sg2
```

How to manually change PWM (fan speed) for all Cooling elements**Cooling control element**

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
1	RQST IDENT	Reserved						
2	Reserved							
3	Reserved	RQST FAIL	RQST ON	Reserved		REQUESTED SPEED CODE		

The "RQST IDENT" for Cooling is defined in the bit7, byte1 and the "REQUESTED SPEED CODE" is defined in the bit2 ~ 0, byte3 of the "Cooling control element" in the SES specification. Set "RQST IDENT" bit to disable the smart fan function, and then change PWM or fan speed for all Cooling elements by setting the "REQUESTED SPEED CODE" bits. Clear "RQST IDENT" bit to enable the smart fan function again. Please disable the smart fan function before changing PWM or fan speed. Only the first Cooling element of each type (HUB fans and System fans) supports this feature. We use the software package "sg3_utils" on Linux for example, and have a SAS HBA and a cable to connect your host with the expander.

(A) Show the device for AIC® Expander Controller (canister)

```
$ sg_map -i
```

```
/dev/sg2  AIC 12G   4U108swapHub   0c30
```

(B) Set "RQST IDENT" of the first Cooling element to disable the smart fan function
 "HubCoolingElement00" is the first cooling element for the HUB / motherboard, and
 "SysCoolingElement00" is the first cooling element for the HDDs / backplane. Here we
 take "SysCoolingElement00" as example.

```
$ sg_ses --descriptor= SysCoolingElement00 --set=1:7:1 /dev/sg2
```

(C) Set "REQUESTED SPEED CODE" of SysCoolingElement0 to change PWM or fan speed
 for all Cooling elements. Set "REQUESTED SPEED CODE"=7 (100% PWM) for example.

```
$ sg_ses --descriptor= SysCoolingElement00 --set 3:2:3=7 /dev/sg2
```

REQUESTED SPEED CODE	PWM
7	100%
6	90%
5	80%
4	70%
3	60%
2	50%
1	40%
0	Leave at current speed

How to update firmware / MFG for the Edge expanders**Array Device Slot control element**

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved0			
1	RQST OK	RQST RSVD DEVICE	RQST HOT SPARE	RQST CONS CHECK	RQST IN CRIT ARRAY	RQST IN FAILED ARRAY	RQST REBUILD/REMAP	RQST R/R ABORT
2	RQST ACTIVE	DO NOT REMOVE	Reserved 2	RQST MISSING	RQST INSERT	RQST REMOVE	RQST IDENT	Reserved 1
3	Reserved 5	Reserved 4	RQST FAULT	DEVICE OFF	ENABLE BYP A	ENABLE BYP B	Reserved3	

All Edge expanders are hidden behind the Hub, so please follow the steps below to update firmware and MFG of the Edge0 via inband SAS. The same steps can be applied to the other Edge expanders. We use the software package "sg3_utils" and LSI utility "g3Xflash" on Linux for example, and have a SAS HBA and a cable to connect your host with the expander.

(A) Show the device for AIC® Expander Controller(canister)

```
$ sg_map -i
/dev/sg2  AIC    12G 4U108swapHub    0c30
```

(B) Set "Reserved2" of Disk001 to make the Edge0 visible.

Disk001 for Edge0, Disk031 for Edge1, Disk061 for Edge2 and Disk085 for Edge3.

```
$ sg_ses --descriptor=Disk001 --set=2:5:1 /dev/sg2
```

(C) Get SAS address for the Hub. The SAS address (500605B0:000272BF) is used for the Hub.

```
$ ./g3Xflash -i get avail
```

(D) Reset the Hub to have an additional device for Edge0

```
$ ./g3Xflash -i 500605b0000272bf reset exp
```

(E) Show the devices for the Hub and the Edge0

```
$ sg_map -i
```

```
/dev/sg2  AIC    12G 4U108swapHub    0c30
/dev/sg3  AIC    12G 4U108swapEdge0  0c31
```

(F) Update firmware of the Edge0

```
$ sg_write_buffer --id=0x0 --in=<firmware filename> --mode=0x2 --offset=0 /dev/sg3
```

(G) Update MFG of the Edge0

```
$ sg_write_buffer --id=0x83 --in=<MFG filename> --mode=0x2 --offset=0 /dev/sg3
```

(H) Get SAS address for Edge0. This example uses SAS address (50015B20:9000EBBF) for the Edge0.

```
$ ./g3Xflash -i get avail
```

(I) Reset the Edge0 to activate its new firmware / MFG.

```
$ ./g3Xflash -i 50015b209000ebbf reset exp
```

(J) Get the current firmware version of the Edge0 for confirmation.

```
$ ./g3Xflash -i 50015b209000ebbf get ver
```

(K) Set "Reserved5" of Disk001 to make the Edge0 invisible

```
$ sg_ses --descriptor=Disk001 --set=3:7:1 /dev/sg2
```

(L) Reset the Hub to refresh the change of the Edge0

```
$ ./g3Xflash -i 500605b0000272bf reset exp
```

How to update all firmware/MFG through in-band SES with a tar ball which includes all Edge firmware/MFG and Hub firmware/MFG

Please follow the steps below to update all firmware/MFG through in-band SES with a tar ball which includes all Edge firmware/MFG and Hub firmware/MFG. We use the software package "sg3_utils" on Linux for example, and have a SAS HBA and a cable to connect your host with the expander. The version of the software package "sg3_utils" must be v1.41 or newer.

(A) Show the device for AIC® Expander Controller(canister)

```
$ sg_map -i
/dev/sg2  AIC    12G 4U108swapHub    0c30
```

(B) Set the time-out interval with the option "-t". The update process on 4U78_SE takes about 380 seconds, and the update process on 4U108_SE takes about 500 seconds.

```
$ sg_write_buffer /dev/sg2 --id=0x04 --bpw=4k
--in=4U78_SE_4U108_SE_12G_Edge_12G_Hub.tar --mode=0x2 --offset=0 -t 600
```

4.3.4 Reading Phy Counters via Java Sol

1. Initiate SOL function in BMC.

```
D:\ipmitool_test>ipmitool.exe -I lanplus -H 192.168.11.11 -U admin -P admin sol activate
```

```
#ipmitool -I lanplus -H [BMC_IP] -U admin -P admin sol activate
```

2. Select expander connection

NetFN 3C

Command Code: 40h

Message	Byte	Data Field
Request	1	Expander select 00h: Hub 01h: Edge0 02h: Edge1 03h: Edge2 04h: Edge3 (4U108 only)
	2	Select Expander
Response	2	Expander is being updated FFh: idle
	3	SOL active Expander FFh: idle

```
#ipmitool -I lanplus -H <BMC IP> -U admin -P admin raw 0x3C 0x40 0x0
```

3. Read expander Edge0 counter value

Execute ipmi command to configure BMC SOL to Edge0

```
# ipmitool -I lanplus -H [BMC_IP] -U admin -P admin raw 0x3C 0x40 0x1
```

```
D:\ipmitool_test>ipmitool.exe -I lanplus -H 192.168.11.11 -U admin -P admin123 raw 0x3C 0x40 0x01
01 ff ff

D:\ipmitool_test>ipmitool.exe -I lanplus -H 192.168.11.11 -U admin -P admin123 sol activate
[SOL Session operational. Use ~? for help]

cmd >sensor

== ENCLOSURE STATUS ==

Expander Temperature      : 47 Celsius degree
System Temperature-0      : 27 Celsius degree
System Temperature-1      : 28 Celsius degree

Voltage Sensor 0.9V       : 0.94 V
Voltage Sensor 1.8V       : 1.78 V

Current Model              : 4U78swapEdge0

=====

cmd >
```

4. Type in “counters” to execute counters command.

```
cmd >counters
```

```
=====
```

```
Phy Layer Error Counters
```

```
=====
```

PHY Id	Event1 InvWrdrCnt	Event2 DispErrCnt	Event3 LossSyncCnt	Event4 RstSeqFailCn
00	00000000	00000000	00000000	00000000
01	00000000	00000000	00000000	00000000
02	00000000	00000000	00000000	00000000
03	00000000	00000000	00000000	00000000
04	00000000	00000000	00000000	00000000
05	00000000	00000000	00000000	00000000
06	00000000	00000000	00000000	00000000
07	00000000	00000000	00000000	00000000
08	00000000	00000000	00000000	00000000
09	00000000	00000000	00000000	00000000
10	00000000	00000000	00000000	00000000
11	00000000	00000000	00000000	00000000
12	00000000	00000000	00000000	00000000
13	00000000	00000000	00000000	00000000
14	00000000	00000000	00000000	00000000
15	00000000	00000000	00000000	00000000
16	00000000	00000000	00000000	00000000
17	00000000	00000000	00000000	00000000
18	00000000	00000000	00000000	00000000
19	00000000	00000000	00000000	00000000
20	00000000	00000000	00000000	00000000
21	00000000	00000000	00000000	00000000
22	00000000	00000000	00000000	00000000
23	00000000	00000000	00000000	00000000
24	00000000	00000000	00000000	00000000
25	00000000	00000000	00000000	00000000
26	00000000	00000000	00000000	00000000
27	00000000	00000000	00000000	00000000
28	00000000	00000000	00000000	00000000
29	00000000	00000000	00000000	00000000
30	00000000	00000000	00000000	00000000
31	00000000	00000000	00000000	00000000
32	00000000	00000000	00000000	00000000
33	00000000	00000000	00000000	00000000
34	00000000	00000000	00000000	00000000
35	00000000	00000000	00000000	00000000
36	00000000	00000000	00000000	00000000
37	00000000	00000000	00000000	00000000
38	00000000	00000000	00000000	00000000
39	00000000	00000000	00000000	00000000

```
=====
```

```
Generic Broadcast Counter
```

```
=====
```

```
Broadcast Counter Not Configured.
```

```
=====
```

```
cmd >
```

5. To read the expander Edge1 counter value, 1, execute the ipmi command to configure BMC SOL to Edge1

```
# ipmitool -I lanplus -H [BMC_IP] -U admin -P admin raw 0x3C 0x40 0x2
```

```
D:\ipmitool_test>ipmitool.exe -I lanplus -H 192.168.11.11 -U admin -P admin123 raw
0x3C 0x40 0x02
02 ff ff

D:\ipmitool_test>ipmitool.exe -I lanplus -H 192.168.11.11 -U admin -P admin123 sol
activate
[SOL Session operational. Use ~? for help]

cmd >sensor

== ENCLOSURE STATUS =====

    Expander Temperature      : 45 Celsius degree
    System Temperature-0     : 27 Celsius degree
    System Temperature-1     : 29 Celsius degree

    Voltage Sensor 0.9V      : 0.94 V
    Voltage Sensor 1.8V      : 1.78 V

    Current Model            : 4U78swapEdge1

=====

cmd >
```

6. Type in “counters” to execute counters command.

```

Current Model : 4U78swapEdge1
=====

cmd >counters
=====

Phy Layer Error Counters
=====

PHY      Event1      Event2      Event3      Event4
Id -----
      InvWrdrCnt      DispErrCnt      LossSyncCnt      RstSeqFailCnt
=====

00      00000000      00000000      00000000      00000000
01      00000000      00000000      00000000      00000000
02      00000000      00000000      00000000      00000000
03      00000000      00000000      00000000      00000000
04      00000000      00000000      00000000      00000000
05      00000000      00000000      00000000      00000000
06      00000000      00000000      00000000      00000000
07      00000000      00000000      00000000      00000000
08      00000000      00000000      00000000      00000000
09      00000000      00000000      00000000      00000000
10      00000000      00000000      00000000      00000000
11      00000000      00000000      00000000      00000000
12      00000000      00000000      00000000      00000000
13      00000000      00000000      00000000      00000000
14      00000000      00000000      00000000      00000000
15      00000000      00000000      00000000      00000000
16      00000000      00000000      00000000      00000000
17      00000000      00000000      00000000      00000000
18      00000000      00000000      00000000      00000000
19      00000000      00000000      00000000      00000000
20      00000000      00000000      00000000      00000000
21      00000000      00000000      00000000      00000000
22      00000000      00000000      00000000      00000000
23      00000000      00000000      00000000      00000000
24      00000000      00000000      00000000      00000000
25      00000000      00000000      00000000      00000000
26      00000000      00000000      00000000      00000000
27      00000000      00000000      00000000      00000000
28      00000000      00000000      00000000      00000000
29      00000000      00000000      00000000      00000000
30      00000000      00000000      00000000      00000000
31      00000000      00000000      00000000      00000000
32      00000000      00000000      00000000      00000000
33      00000000      00000000      00000000      00000000
34      00000000      00000000      00000000      00000000
35      00000000      00000000      00000000      00000000
=====

Generic Broadcast Counter
=====

Broadcast Counter Not Configured.
=====

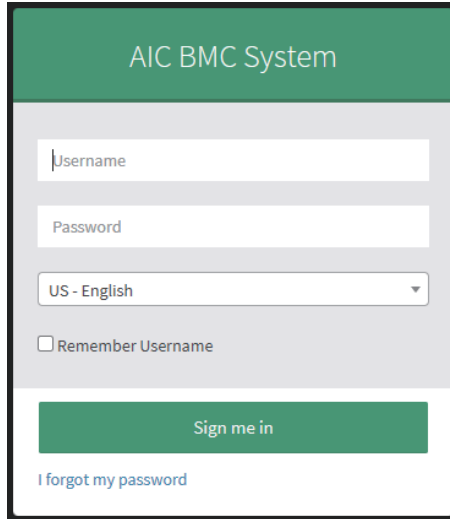
cmd >

```

4.4 Web UI for AST2520

4.4.1 User Name and Password

Initial access of MegaRAC SP-X prompts you to enter the User Name and Password. A sample screenshot of the login screen is given below.



Login page

The fields are explained as follows

Username: Enter your username in this field.

Password: Enter your password in this field.

Language Selection: Language selection drop-down will be populated based on supported languages in Web UI as a part of multi-language support feature. Drop-down option value will be selected based on the browser language. Default language will be selected as US-English if the browser configured language not supported by Web UI. Entire Web UI pages language strings will be displayed based on selected language from drop-down.

Remember Username: Check this option to remember your login Username. If you select this option, the browser will save your credentials internally in its memory, and when you open that site the next time, it will auto-fill Username for you.

Using MegaRAC SP-X

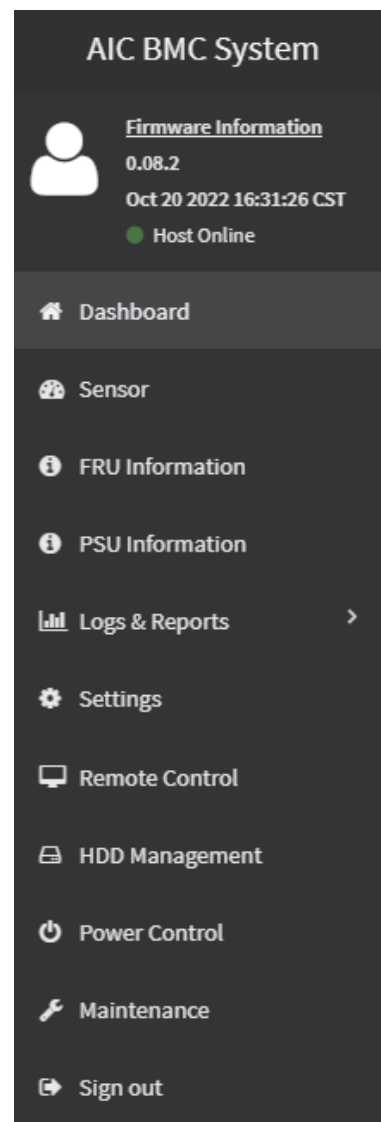
The MegaRAC GUI consists of various menu items.

4.4.2 Menu Bar

Firmware Information will be displayed with the latest version, date and time details. Power Control Status will be displayed as Host Online. To Change the Power Control Status, click [Host Online](#) link.

A screenshot of the menu bar is shown below.

- Dashboard
- Sensor
- FRU Information
- PSU Information
- Logs & Reports
- Settings
- Remote Control
- HDD Management
- Power Control
- Maintenance
- Sign out



Menu Bar

4.4.3 Quick Button and Logged-in User

The user information and quick buttons are located at the top right of the MegaRAC GUI. A screenshot of the logged-in user information is shown below.



User Information

The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions.

Message: Click the  icon to view the event log alert messages. On clicking the messages, it will navigate to the Logs and Reports page.

Language Selection: Change the language to view the language strings in different languages.

Refresh: Click the  Refresh icon or pressing key F5 to reload the current page.

Sync: Click the  Sync icon to synchronize with Latest Sensor and Event Log updates.

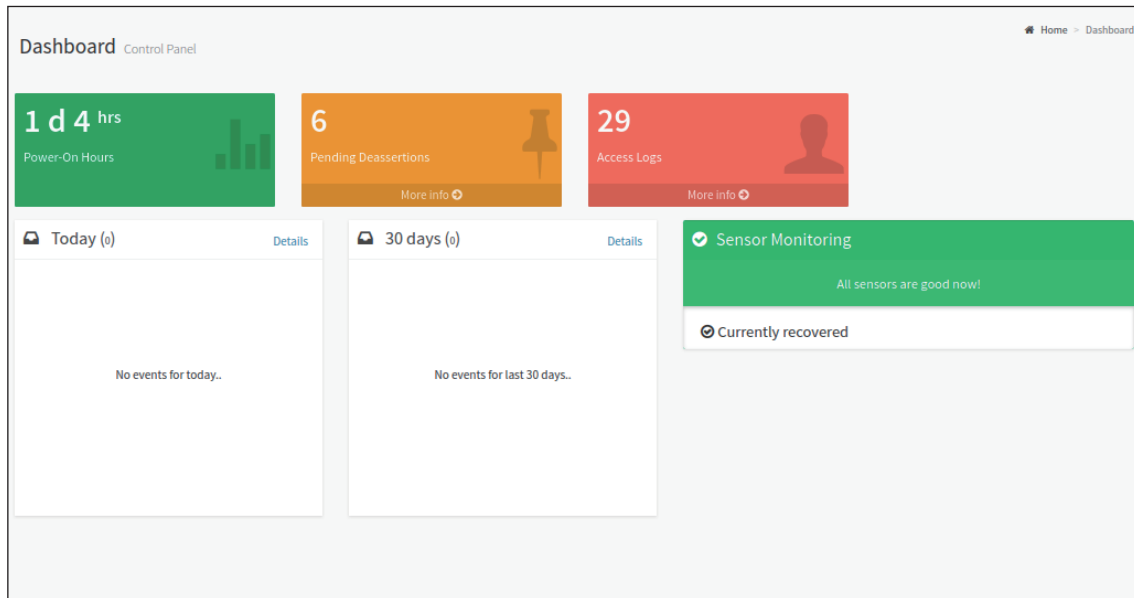
Sign out: Click the  icon to log out of the MegaRAC GUI.

Notification: Click  to view the notification received.

Help: The Help icon () is Located at the top right of each page in MegaRAC GUI. Click this help icon to view more detailed field descriptions

4.4.4 Dashboard

The Dashboard page gives the overall information about the status of a device. To open the Dashboard page, click [Dashboard](#) from the menu bar. A sample screenshot of the Dashboard page is shown below.



BMC Power-On Hours

BMC Power-On Hours will keep on accumulated and will be reset to zero when you flash a new image.

Pending Deassertions

It lists all the asserted events which are waiting for deassert state. To know about the pending events details, click the More info link. This navigates to the Event Log page and display all the asserted events that are waiting for deassertion.

Access Logs

A graphical representation of all events incurred by various sensors and occupied/available space in logs can be viewed. If you click on the More info link, you can view the Audit Log page.

Today & 30 Days (Event Logs)

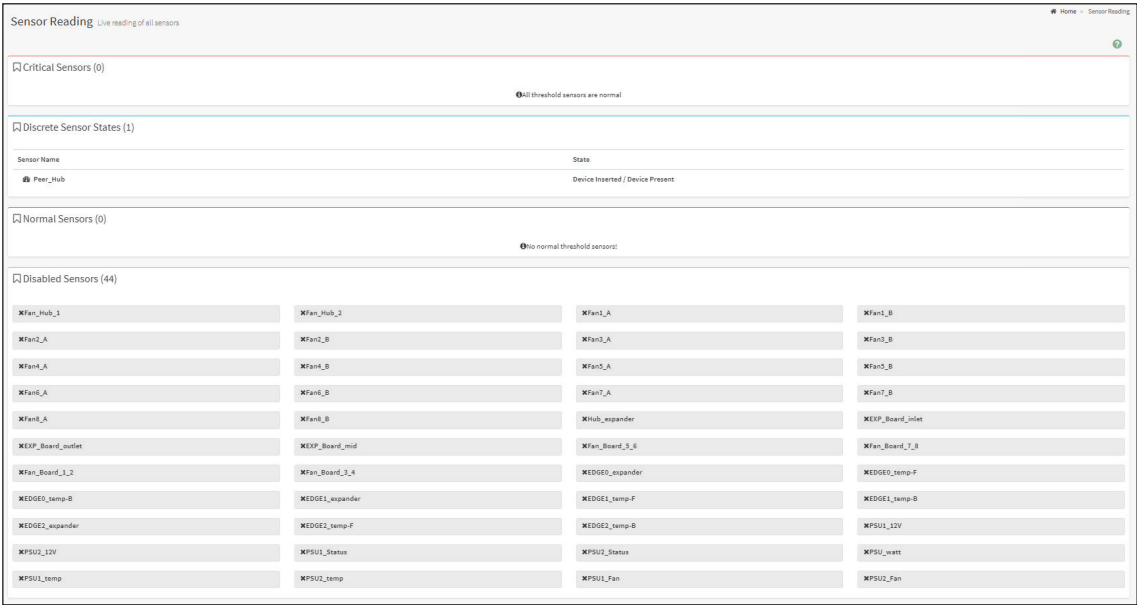
This page displays the list of event logs occurred by the different sensors on this device. Click Details link on Today and 30 days to view the event logs for Today and 30 days respectively.

Sensor Monitoring

It lists all the critical sensors on the device. If you click on any list sensor, you can view the Sensor detail page with the Sensor information and Sensor Events details.

4.4.5 Sensor

The Sensor Readings page displays all the sensor related information. To open the Sensor Readings page, click Sensor from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. A screenshot of Sensor Readings page is given below.



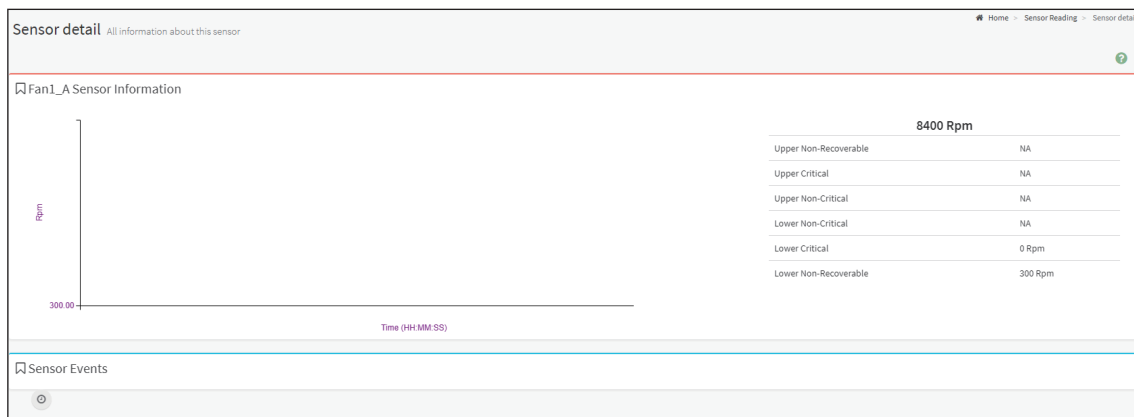
Sensor Readings Page

The Sensor Readings page contains the following information. In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behavior will be appeared, else you can choose the sensor type that you want to display from the list. Some examples for sensors are Temperature Sensors and Fan Sensors etc.

4.4.5.1 Sensor Detail

Select a particular Sensor from the Critical Sensor or Normal Sensor lists. The Sensor Information as Live Widget and Thresholds for the selected sensor will be displayed as shown below.

For Illustrative Purpose, a sample screenshot of Sensor detail page with Change Thresholds option is shown and explained below.



Sensor detail



NOTE

Widgets are little gadgets, which provide real time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget. The session will not expire, until the widgets gets a live data of the last widget that is kept opened.

For the selected sensor, this widget gives a dynamic representation of the readings for the sensor.

Thresholds are of six types:

- Lower Non-Recoverable (LNR)
- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

4.4.6 FRU Information

FRU Information page displays the BMC's FRU device information. FRU page shows information like Basic Information, Chassis Information, Board Information and Product Information of the FRU device.

To open the FRU Information page, click FRU Information from the menu bar. Select a FRU Device ID from the FRU Information section to view the details of the selected device. A screenshot of FRU Information page is given below.

The screenshot shows the 'FRU Field Replaceable Units' page. At the top, there's a header with 'FRU' and a home icon. Below the header, there's a section titled 'Available FRU Devices' with a dropdown menu for 'FRU Device ID' (showing '0') and a text field for 'FRU Device Name' (showing 'BMC_FRU'). Below this, there are three columns of information: 'Chassis Information', 'Board Information', and 'Product Information'. Each column contains a table of fields and their values.

Chassis Information		Board Information		Product Information	
Chassis Information Area Format Version	1	Board Information Area Format Version	1	Product Information Area Format Version	1
Chassis Type	Main Server Chassis	Language	English	Language	English
Chassis Part Number		Manufacture Date Time	Mon Jan 1 00:00:00 1996	Product Manufacturer	
Chassis Serial Number		Board Manufacturer		Product Name	
Chassis Extra		Board Product Name		Product Part Number	
		Board Serial Number		Product Version	
		Board Part Number		Product Serial Number	
		FRU File ID		Asset Tag	
		Board Extra		FRU File ID	
				Product Extra	

FRU Information Page

The following fields are displayed here for the selected device.

Available FRU Devices

- FRU device ID - Select the device ID from the drop down list
- FRU Device Name - The device name of the selected FRU device.

Chassis Information

- Chassis Information Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra

Board Information

- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

Product Information

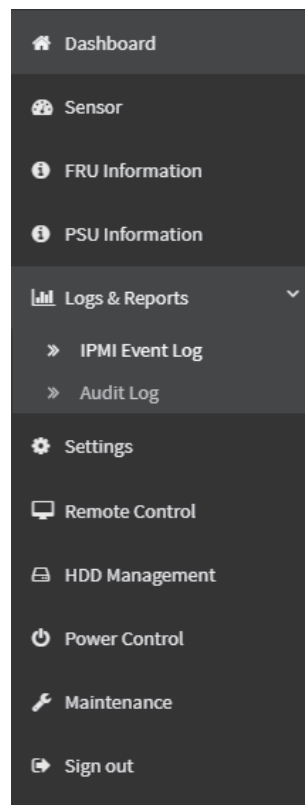
- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

4.4.7 Logs & Reports

The Logs & Reports page displays the following information.

- IPMI Event Log
- Audit Log

A screenshot displaying the menu items under Logs & Reports is shown below

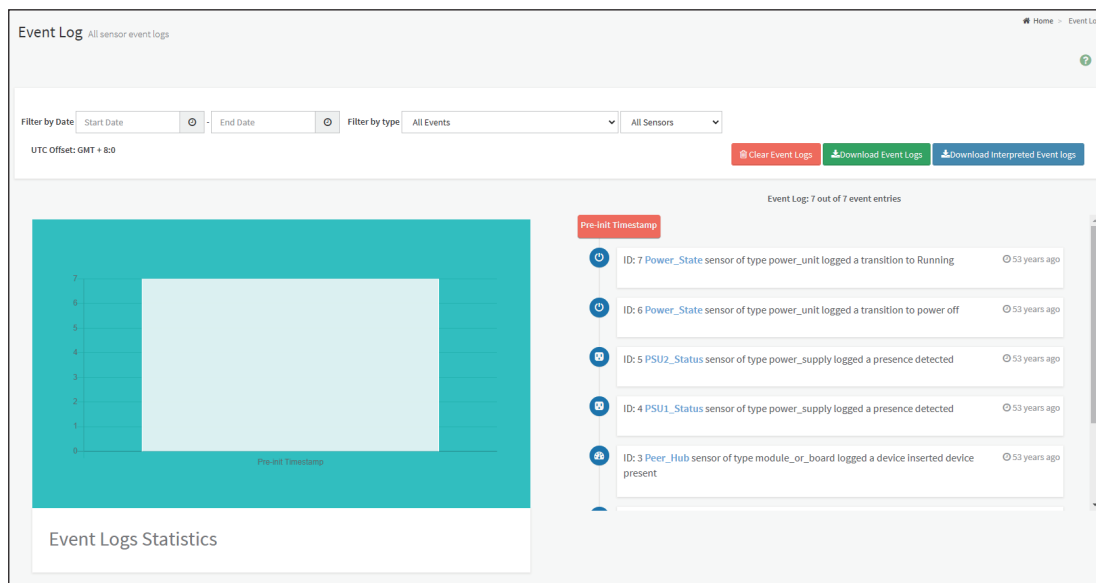


Logs & Reports – Menu

4.4.7.1 IPMI Event Log

This page displays the list of event logs occurred by the different sensors on this device. Double click on a record to see the details of that entry. You can use the sensor type or sensor name filter options to view those specific events or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click [Logs & Reports > Event Log](#) from the menu bar. A sample screenshot of Event Log page is shown below.



Event Log Page

The Event Log page consists of the following Fields.

Filter By Date: Filtering can be done by selecting Start Date and End Date using Calendar.

Filter By Type: The category could be either All Events, System Event Records, OEM Event Records, BIOS Generated Events, SMI Handler Events, System Management Software Events, System Software - OEM Events, Remote Console Software Events, Terminal Mode Remote Console software Events.

UTC Offset: Displays the current UTC Offset value based on which event Time Stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.

Event Log Statistics: Displays the statistical graph for the selected date.

Clear Event Logs: To delete all the event logs.

Download Event Logs: To download the event logs.

4.4.7.2 Audit Log

Audit Log page will display all the system events occurred in this device that has been already configured.



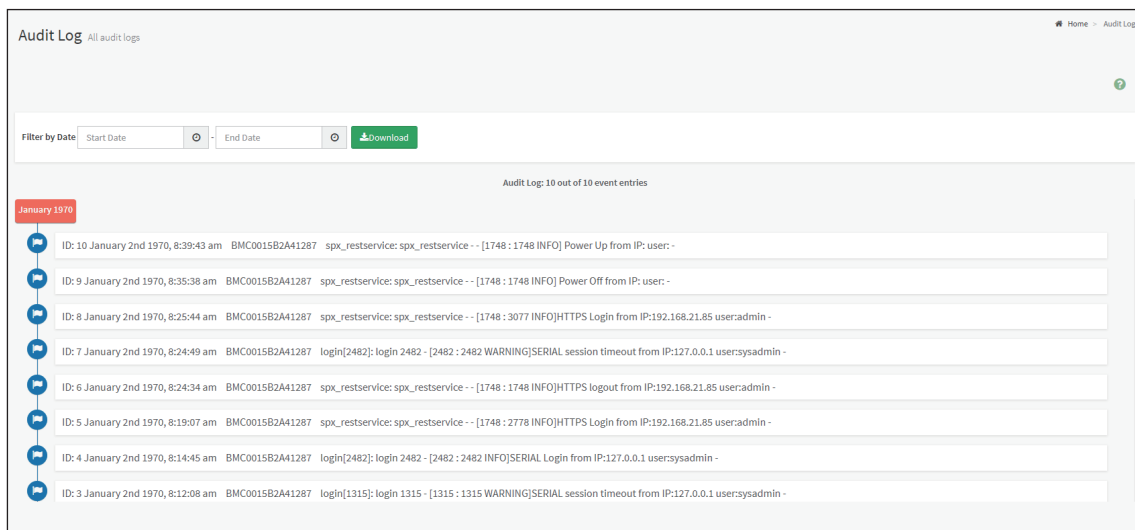
NOTE

Logs have to be configured under Settings -> Log Settings -> Advanced Log Settings in order to display any entries.

To open the Event Log page, click [Logs & Reports > Audit Log](#) from the menu bar.

A sample screenshot of Audit Log page is shown below.

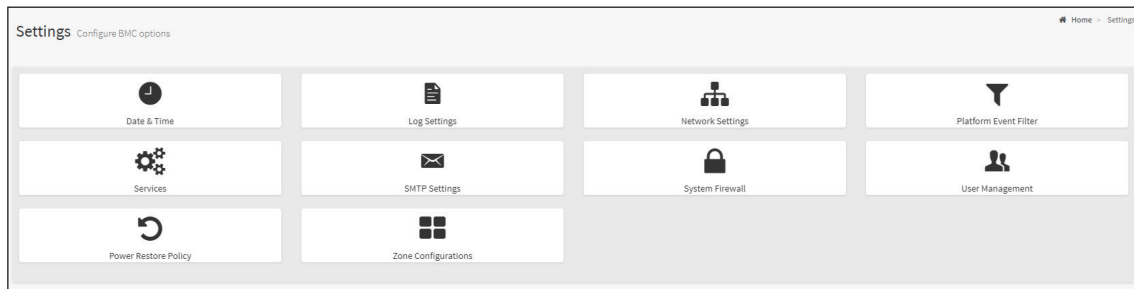
Download: To download the audit logs.



Audit Log

4.4.8 Settings

This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



Configuration Group Menu

- Date & Time
- Log Settings
- Network Settings
- Platform Event Filter
- Services
- SMTP Settings
- System Firewall
- User Management
- Power Restore Policy
- Zone Configurations

A detailed description of the Configuration menu is given below.

4.4.8.1 Date & Time

This field is used to set the date and time on the BMC. A sample screenshot of Date & Time is shown as below.

The screenshot displays the 'Date & Time' configuration interface. At the top, a breadcrumb trail shows 'Home > Settings > Date & Time'. A note states: 'Note: If the timezone is selected from the group of Manual offset(GMT/ETC timezones), • The map selection will be disabled. • The TimeZone settings will be reflected only after saving the settings.' Below this is the 'Configure Date & Time' section. It features a world map with a red dot indicating the selected location, 'America/Manaus'. Below the map, a dropdown menu shows 'America/Manaus' and the current time is displayed as 'Jun 23, 2017 6:38:44 AM (GMT-04:00 AMT) - America/Manaus'. There is a checkbox for 'Automatic NTP Date & Time' which is checked. Below this, there are two input fields: 'Primary NTP Server' with the value 'pool.ntp.org' and 'Secondary NTP Server' with the value 'time.nist.gov'. A 'Save' button is located at the bottom right of the form.

Date & Time - Automatic Date & Time

The Date & Time section consists of the following fields.

Configure Date & Time: Displays Time zone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.

Select Time Zone: This field is used to set the date and time on the BMC.

Automatic Date & Time: To automatically synchronize Date and Time with the NTP Server.

- **Primary NTP Server:** To configure a primary NTP server to use when automatically setting the date and time.
- **Secondary NTP Server:** To configure a secondary NTP server to use when automatically setting the date and time.

Save: To save the settings.



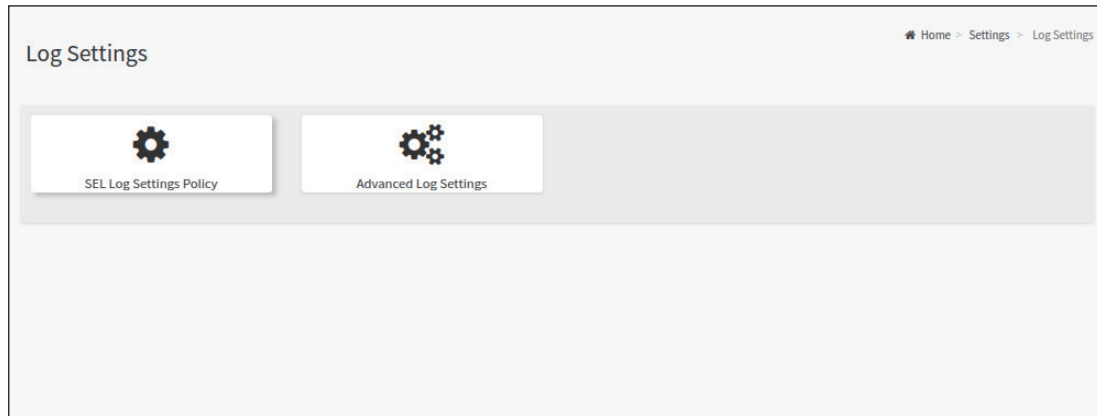
NOTE

If the time zone is selected as Manual Offset, the map selection will be disabled. The Time Zone settings will be reflected only after saving the settings.

4.4.8.2 Log Settings

System and Audit log page displays a list of system logs and audit logs occurred in this device.

To open Log Settings page, click [Settings > Log Settings](#) from the menu bar. A sample screenshot of Log Settings page is shown below.



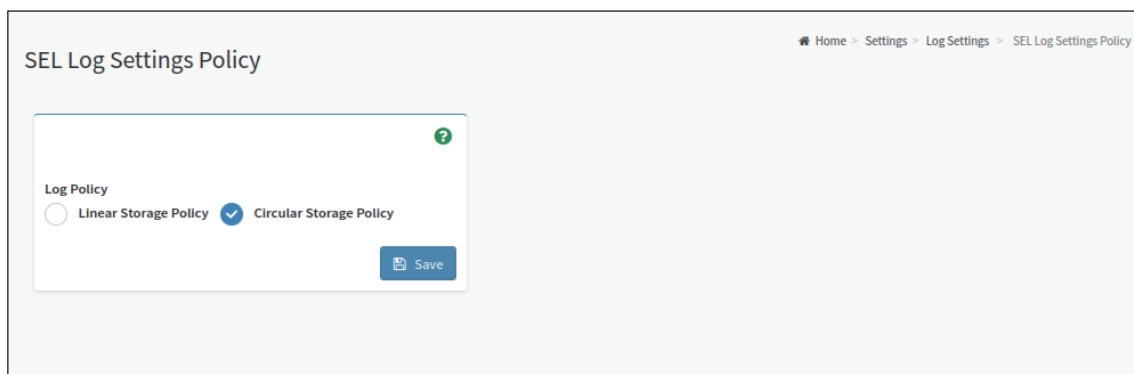
System and Audit Log Settings

The fields of Log Settings page are explained below.

- SEL Log Settings Policy
- Advanced Log Settings

SEL Log Setting Policy

To open Log Settings page, click [Settings > Log Settings > SEL Log Settings Policy](#) from the menu bar. A sample screenshot of SEL Log Settings Policy page is shown below.



SEL Log Settings Policy

This page is used to configure the log policy for the event log. The fields are as followed

Log Policy: This field is to enable or disable the Linear Storage Policy or Circular Storage Policy.

Save: To save the configured settings

Advanced Log Settings

To open Advanced Log Settings page, click [Settings > Log Settings > Advanced Log Settings](#) from the menu bar. A sample screenshot of **Advanced Log Settings Policy** page is shown below.

Advanced Log Settings

Home > Settings > Log Settings > Advanced Log Settings

☒ System Log

☒ Local Log

☐ Remote Log

Port Type

☐ UDP ☐ TCP

File Size

50000

Rotate Count

0

Remote Log Server

Server IP or Hostname

Remote Server Port

0

☒ Enable Audit Log

Save

Advanced Log Settings

This page is used to configure the log policy for the event log. The fields are as followed.

System Log: This field is used to enable or disable the System Log. Select **System Log** to view all system events. Entries can be filtered based on their classification levels. Specifies the Location for system logs, whether it should be preserved in a **Local Log/Remote Log**.

Local Log: Select Local Log to save the logs locally (BMC).

Remote Log: Select Remote Log to save the logs in a remote machine.



NOTE

- You can select either Local Log/Remote Log or both Logs as per the requirement.
- Either one of the Log selection is mandatory.

Port Type: Port Type is supported with the enable of Remote Log. You can select either UDP/TCP as per the requirement.

File Size: This field is to specify the size of the file in bytes if the selected log type is local.



NOTE

Size ranges from 3 to 65535. Log files are rotated when they grow bigger than size bytes mentioned, with regards for the last rotation time interval (1 minute).

Rotate Count: To back up the log information in back up files.

**NOTE**

- Values supported are 0 and 1.
- When log information exceeds the file size, the old log information is automatically moved to back up files based on the rotate count value. If rotate count is zero, then old log information gets cleared permanently.
- File Size and Rotate Count options will be available only when Local Log is enabled.

Remote Log Server: This field is to specify the Remote server address to log the system events.

**NOTE**

Server address will support the following:

- IPv4 address format.
- FQDN (Fully qualified domain name) format.
- Maximum allowed size is 64 bytes.

Remote Server Port: This field is to specify the Remote Server port address to log the system events.

**NOTE**

Remote Log Server and Remote Server Port options will be available only when Remote Log is enabled.

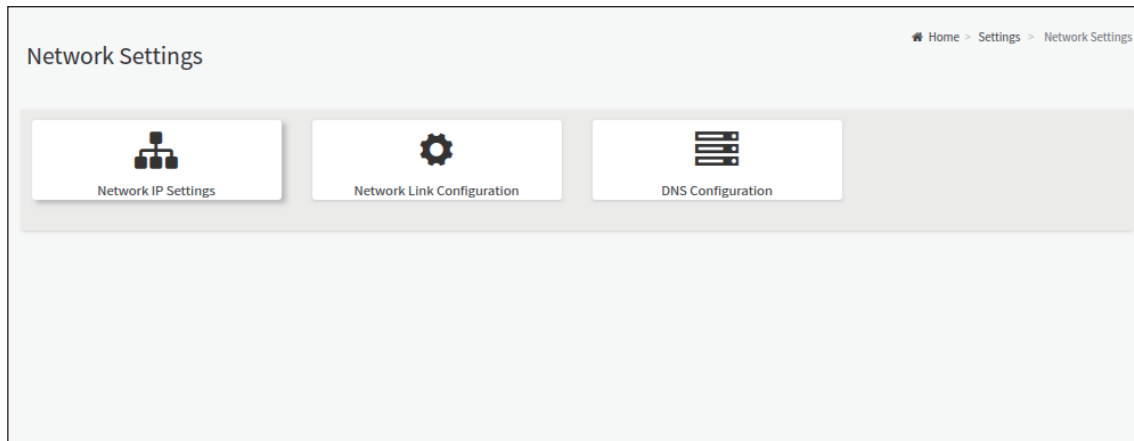
Enable Audit Log: To enable or disable the audit log.

Save: To save the changes

4.4.8.3 Network Settings

The Network Settings Page is used to configure the network settings for the available LAN channels.

A sample screenshot of Network Settings page is shown below.



Network Settings

Network IP Settings

To open Network Settings page, click [Settings](#) -> [Network Settings](#) -> [Network IP Settings](#) from the menu bar. A sample screenshot of Network IP Settings Page is shown below.

The fields of Network IP Settings page are explained below.

Enable LAN: To enable or disable the LAN Settings.

LAN Interface: Lists the LAN interfaces.

MAC Address: This field displays the MAC Address of the device. This is a read only field.

Enable IPv4: This option is to enable/disable the IPv4 settings in the device.

Enable IPv4 DHCP: This option is to enable IPv4 DHCP support for the selected interface.

IPv4 Address, IPv4 Subnet Mask, and IPv4 Default Gateway: These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device.



NOTE

- IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each Number ranges from 0 to 255.
- First Number must not be 0.

Enable IPv6: To Enable/Disable the IPv6 configuration settings.

Enable IPv6 DHCP: To Enable/Disable the IPv6 settings in the device. It dynamically configures IPv6 address using DHCP (Dynamic Host Configuration Protocol).



NOTE

Disable this Enable IPv6 DHCP field to enable and enter the values in following fields such as IPv6 Index, IPv6 Address, Subnet Prefix length and IPv6 Gateway.

IPv6 Index: To specify a static IPv6 Index to be configured to the device. E.g.: 0.

IPv6 Address: To specify a static IPv6 address to be configured to the device. Eg: 2004::2010. User can mention.

Subnet Prefix length: To specify the subnet prefix length for the IPv6 settings.



NOTE

Value ranges from 0 to 128.

IPv6 Gateway: Specify v6 default gateway for the IPv6 settings.



NOTE

If core feature IPV6_COMPLIANCE and SUPPORT_IPMIIPV6_LAN_PARAM_ONLY are enabled, the IPv6 default Gateway field will not be displayed.

Enable VLAN: To enable/disable the VLAN support for selected interface.

VLAN ID: The Identification for VLAN configuration.



NOTE

Value ranges from 2 to 4094.

VLAN Priority: The priority for VLAN configuration.



NOTE

- Value ranges from 0 to 7.
- 7 is the highest priority for VLAN.

Save: To save the entries.

Network Link Configuration

This page is used to configure the network link configuration for available network interfaces.

To open **Network Link** page, click [Settings > Network Settings > Network Link Configuration](#) from the menu bar. A sample screenshot of **Network Link Configuration** page is shown below.

Network Link Configuration Page

The fields of Network Link Configuration page are explained below.

LAN Interface: Select the required network interface from the list to which the Link speed and duplex mode to be configured.

Auto Negotiation: This option is enabled to allow the device to perform automatic configuration to achieve the best possible mode of operation (speed and duplex) over a link.

Link Speed: Link speed will list all the supported capabilities of the network interface. It can be 10/100/1000 Mbps.



NOTE

Link speed of 1000 Mbps is not applicable, when Auto Negotiation is OFF.

Duplex Mode: Duplex Mode could be either Half Duplex or Full Duplex.

Save: To save the settings.

DNC Configuration

The **Domain Name System (DNS)** is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

The DNS Server settings page is used to manage the DNS settings of a device. To open DNS Server Settings page, click [Settings > Network Settings > DNS Configuration](#) from the menu bar. A sample screenshot of DNS Configuration page is shown below.

DNS Configuration

☒ DNS Enabled
☐ mDNS Enabled

Host Name Setting
☒ Automatic ☐ Manual

Host Name
AIC0015B2AECE9F

BMC Registration Settings

BMC Interface:
eth0

☒ Register BMC

Registration method:
☒ Nsupdate ☐ DHCP Client FQDN ☐ Hostname

☐ Both

Eth0 TSIG Configuration
☐ TSIG Authentication Enabled

Current TSIG Private File Info
Not Available

New TSIG Private File

Eth1 TSIG Configuration
☐ TSIG Authentication Enabled

Current TSIG Private File Info
Not Available

New TSIG Private File

Domain Setting
☒ Automatic ☐ Manual

Domain Interface

Domain Name Server Setting
☒ Automatic ☐ Manual

DNS Interface

IP Priority
☒ IPv4 ☐ IPv6

The fields of DNS Configuration page are explained below.

Domain Name Service Configuration

DNS Enabled: To enable/disable all the DNS Service Configurations.

mDNS Enable: To enable/disable the mDNS Support Configurations.

Host Name Settings: Choose either Automatic or Manual settings.

Host Name: It displays host name of the device. If the Host setting is chosen as Manual, then specify the host name of the device.



NOTE

- Value ranges from 1 to 64 alpha-numeric characters.
- Special characters '-'(hyphen) and '_'(underscore) are allowed.
- It must not start or end with a '-'(hyphen). IE browsers won't work correctly if any part of the host name contain underscore (_) character.

BMC Registration Settings

BMC Interface: Options to register the BMC through the Interfaces (eth0ð1).

Register BMC: To register BMC through registration method.

Registration Method

Options to register the BMC are through **NS Update** or **DHCP Client FQDN** or **Hostname**.

TSIG Configuration

Both: Check this option to modify TSIG authentication for both interfaces.

Eth 0&1:

- **TSIG Authentication Enabled:** Check this box to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.
- **Current TSIG Private File:** The information of Current TSIG private file along with its uploaded date/time will be displayed (read-only).
- **New TSIG Private File:** Browse and navigate to the TSIG private file.



NOTE

TSIG file should be of private type.

Domain Setting: Select whether the domain interface will be configured manually or automatically.

- **Automatic** - If you Select **Automatic**, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
- **Manual** - If the Domain setting is chosen as **Manual**, then specify the domain name of the device.



NOTE

If you select "Automatic" it displays the Domain Interface option. If you select "Manual" it displays "Domain name"

- **Domain Name:** It displays the domain name of the device.

Domain Name Server Setting

Automatic - If you select Automatic “DNS Interface” option should be explained.

Manual - Specify the DNS (Domain Name System) server address to be configured for the BMC.

IP Priority:

- If IP Priority is **IPv4**, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server.
- If IP Priority is **IPv6**, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.



NOTE

This is not applicable for Manual configuration.

DNS Server 1, 2 & 3

To specify the DNS (Domain Name System) server address to be configured for the BMC.



NOTE

- IPv4 Addresses should be given in dotted decimal representation.
- IPv6 Addresses are supported and must be global unicast addresses.

DNS Server Address will support the following:

- IPv4 Address format.
- IPv6 Address format.

Save: To save the entered changes.

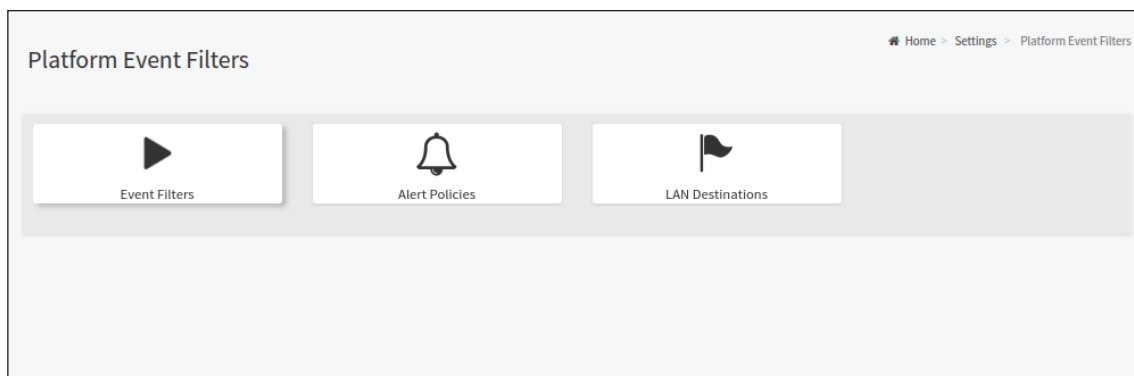
4.4.8.4 Platform Event Filter

Platform Event Filter (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

The PEF Management is used to configure the following

- Event Filters
- Alert Policies
- LAN Destinations

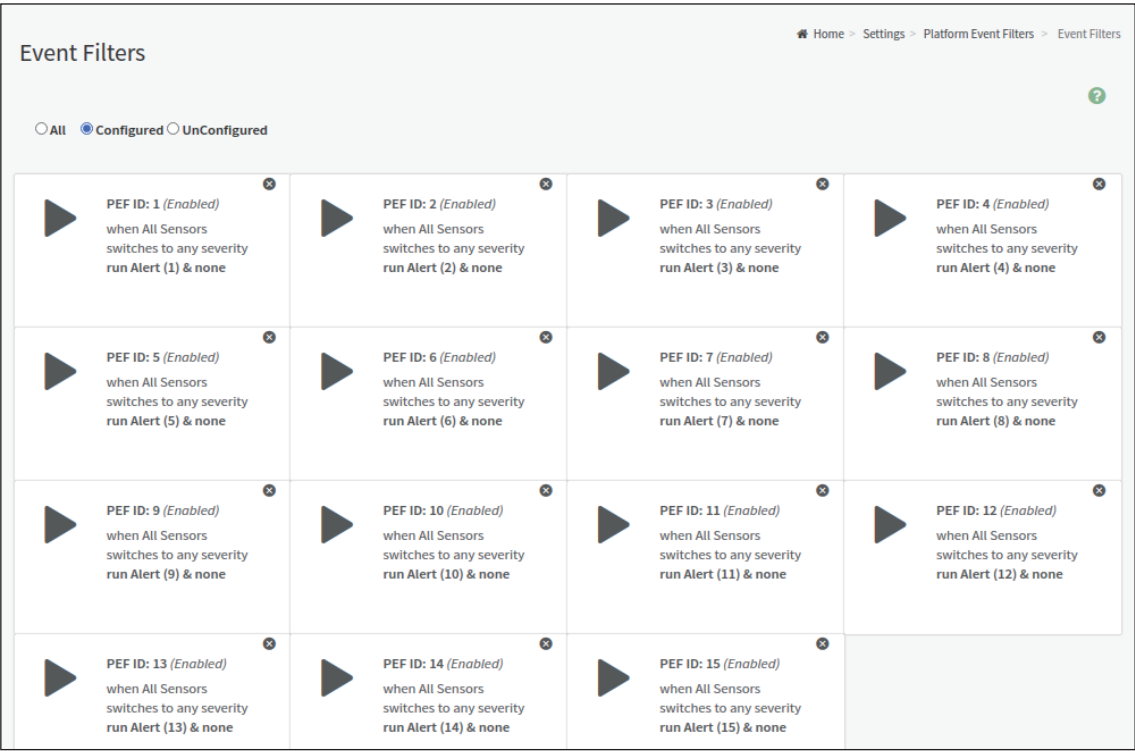
To open PEF Management Settings page, click [Settings > Platform Event Filter](#) from the menu bar. A sample screenshot of Platform Event Filter page is shown below.



Platform Event Filter Page

Event Filters

A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for ‘OEM’ or System Management Software configured events. Note that individual entries can be tagged as being reserved for system use - so this ratio of pre-configured entries to run-time configurable entries can be reallocated if necessary.



Platform Event Filters

The fields of Platform Event Filters Tab are explained below.
This page contains Pre-configured 40 Events with PEF IDs. Click Delete icon (x) on the top right corner to directly delete an item from the list.

Procedure:

- 1. Click the **Event Filters** section to configure the event filters in the available slots.
- 2. To Add an Event Filter entry, select a free section to open the Event Filter entry Page. A sample screenshot of Event Filter Configuration page is shown below.

Event Filter Configuration

Home > Settings > Platform Event Filters > Event Filters > Event Filter Configuration

?

☒ Enable this filter

Event severity to trigger

Any severity

Power Action

Power Down

Alert Policy Group Number

1

☒ Raw Data

Generator ID 1

255

Generator ID 2

255

Generator Type

☐ Slave ☐ Software

Slave Address/Software ID

Channel Number

0

IPMB Device LUN

0

Sensor type

All Sensors

Sensor name

All Sensors

Event Options

All Events

Event trigger

255

Event Data 1 AND Mask

0

Event Data 1 Compare 1

0

Event Data 1 Compare 2

0

Event Data 2 AND Mask

0

Event Data 2 Compare 1

0

Event Data 2 Compare 2

0

Event Data 3 AND Mask

0

Event Data 3 Compare 1

0

Event Data 3 Compare 2

0

Delete

Save

Event Filter Configuration

In the **Event Filter Configuration** section,

- In **Enable this filter**, check this option to enable the PEF settings.
- In **Event Severity to trigger**, select any one of the Event severity from the list.
- **Event Filter Action Alert**: It is checked by default. This action enables PEF Alert action (read-only).
- Select any one of the **Power Action** either Power down, Power reset or Power cycle from the drop down list
- Choose any one of the configured **Alert Policy Group Number** from the drop down list.



NOTE

Alert Policy has to be configured - under Settings->PEF->Alert Policy.

- Check Raw Data option to fill the Generator ID with raw data.
- Generator ID 1 field is used to give raw generator ID1 data value.
- Generator ID 2 field is used to give raw generator ID2 data value.



NOTE

In RAW data field, specify hexadecimal value prefix with '0x'.

- In the Event Generator section, choose the event generator as Slave Address - if event was generated from IPMB. Otherwise as System Software ID - if event was generated from system software.
- In the Slave Address/Software ID field, specify corresponding I2C Slave Address or System Software ID.
- Choose the particular Channel Number that event message was received over. Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
- Choose the corresponding IPMB Device LUN if event generated by IPMB.
- Select the Sensor Type of sensor that will trigger the event filter action.
- In the SensorName field, choose the particular sensor from the sensor list.
- Choose Event Option to be either All Events or Sensor Specific Events.
- Event Trigger field is used to give Event/Reading type value.



NOTE

Value ranges from 1 to 255.

- Event Data 1 AND Mask field is used to indicate wildcarded or compared bits.



NOTE

Value ranges from 0 to 255.

- Event Data 1 Compare 1 & Event Data 1 Compare 2 fields are used to indicate whether each bit position's comparison is an exact comparison or not.



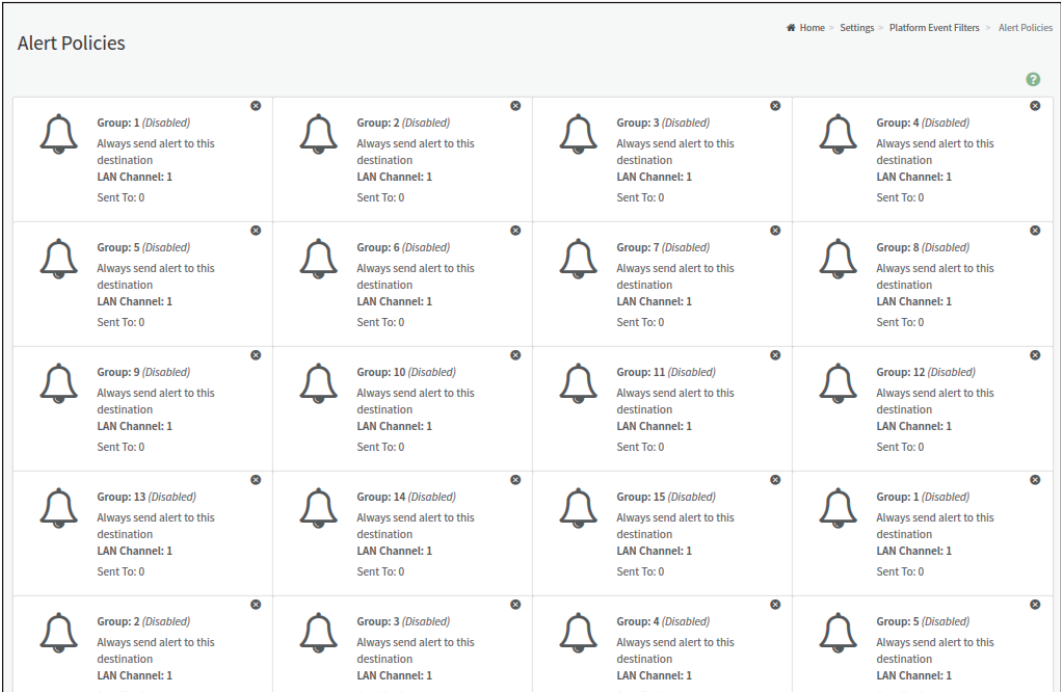
NOTE

Value ranges from 0 to 255.

- Event Data 2 AND Mask field is similar to Event Data 1 AND Mask.
 - Event Data 2 Compare 1 & Event Data 2 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
 - Event Data 3 AND Mask field is similar to Event Data 1 AND Mask.
 - Event Data 3 Compare 1 & Event Data 3 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
3. Click Save to save the changes and return to event filter list.
 4. Click Delete to delete the existing filter.

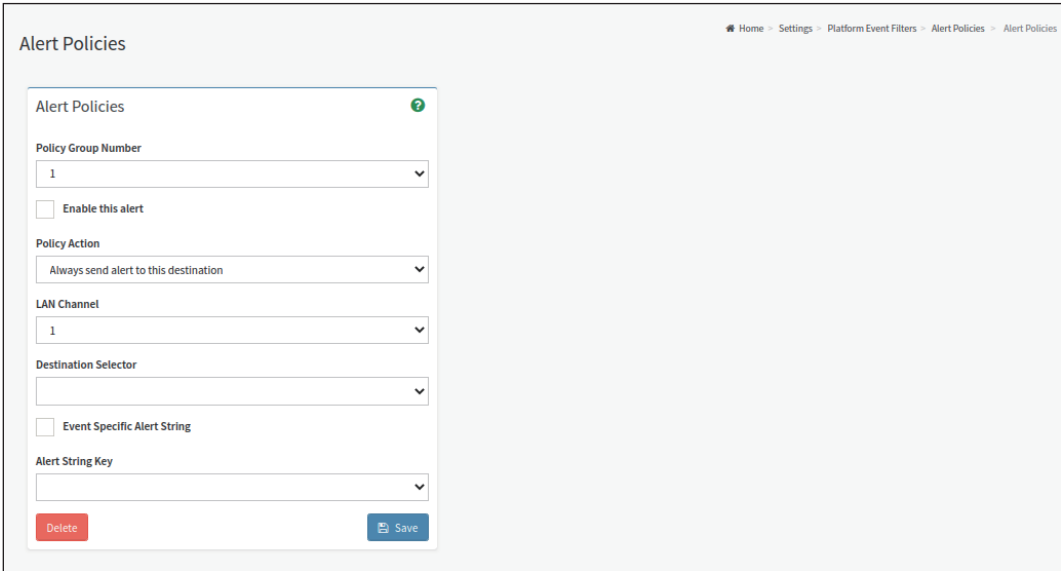
Alert Policies

This page is used to configure the Alert Policy for the PEF configuration. You can add, delete or modify an entry in this page.



Platform Event Filters – Alert Policies

Select the slot and click on the empty slot to open the Alert Policies page as shown in the screenshot below.



Add Alert Policies Page

The fields of Platform Event Filter – Alert Policies section are explained below.

Policy Group Number: Displays the Policy number of the configuration.

Enable this alert: To enable or disable the policy settings.

Policy Action: To choose any one of the Policy set values (0-5) from the list.

0 - Always send alert to this destination.

1 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.

2 - If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.

3 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.

4 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.

LAN Channel: To choose a particular channel from the available channel list.

Destination Selector: To choose a particular destination from the configured destination list.



NOTE

LAN Destination has to be configured - under Settings ->Platform Event Filters -> LAN Destinations.

Event Specific Alert String: To specify an event-specific Alert String.

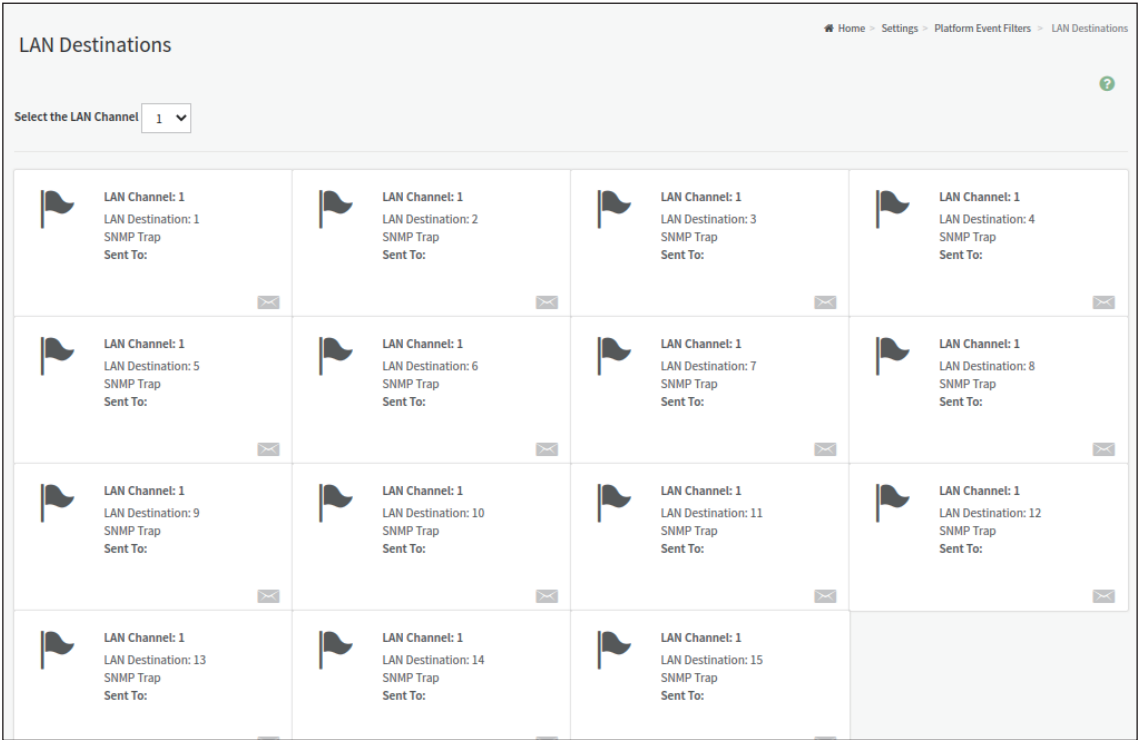
Alert String Key: To specify which string is to be sent for this Alert Policy entry.

Save: To save the Alert Policies entries.

Delete: To delete the selected configured Alert Policy.

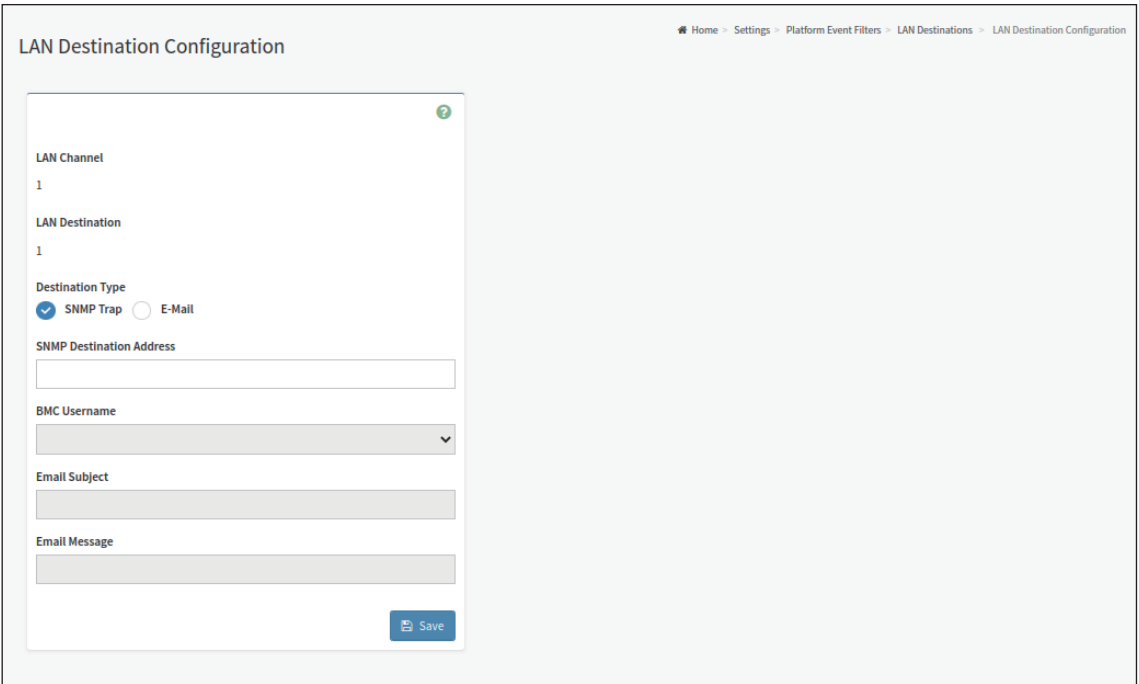
LAN Destinations

This page is used to configure the LAN destinations of PEF configuration. A sample screenshot of LAN Destination Page is given below.



Platform Event Filters LAN Destinations

Select the slot and click on the empty slot to open the LAN Destination Configuration page as shown in the screenshot below.



Add LAN Destination entry Page

The fields of **Platform Event Filter** – LAN Destinations are explained below.

Select the LAN Channel: To select the LAN Channel number.

LAN Channel: Displays LAN Channel Number for the selected slot (read-only).

LAN Destination: Displays ID for setting Destination Selector of Alert Policy (read-only).

Destination Type: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the four fields - SNMP Destination Address, BMC User Name, Email subject and Email message needs to be filled. The SMTP server information also has to be added - under [Settings ->SMTP Settings](#). For SNMP Trap, only the SNMP Destination Address has to be filled.

SNMP Destination Address: If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format.
- IPv6 address format.

BMC User Name: If Destination type is Email Alert, then choose the user to whom the email alert has to be sent. Email address for the user has to be configured under [Settings->Users Management](#).

Email Subject & Email Message: These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address of the user in case of any severity events with a subject specified in subject field and will contain the message field's content as the email body. These fields are not applicable for 'AMI-Format' email users.



NOTE

User should be configured under Settings > Users Management

Save: To add a new entry to the device. Alternatively, double click on a free slot.

Delete: To delete the selected configured LAN Destination.

Click Message icon () to send sample alert to configured destination.



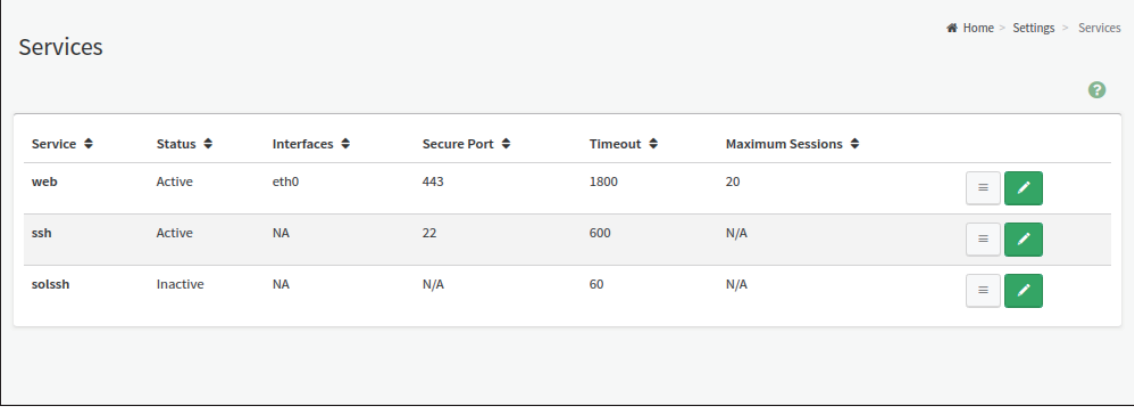
NOTE

Test alert can be sent only with enabled SMTP configuration. SMTP support can be enabled under Settings->SMTP Settings.

4.4.8.5 Services

This page displays the basic information about services running in the BMC. Only Administrator can modify the service.

To open Services page, click [Settings > Services](#) from the menu bar. A sample screenshot of Services Page is shown below.



Service	Status	Interfaces	Secure Port	Timeout	Maximum Sessions
web	Active	eth0	443	1800	20
ssh	Active	NA	22	600	N/A
solssh	Inactive	NA	N/A	60	N/A

Services Page

The fields of Services Page are explained below.

Services: Displays service name of the selected slot (read-only).

Status: Displays the current status of the service, either active or inactive state.

Interfaces: It shows the interface in which service is running.

Secure Port: Used to configure secure port number for the service.

- Web default port is 443
- SSH default port is 22



NOTE

For security reasons, no accounts are allowed to log in via SSH.



NOTE

SOLSSH will not support secure port.

Timeout: Displays the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value.



NOTE

- Web timeout value ranges from 300 to 1800 seconds.
- SSH timeout value ranges from 60 to 1800 seconds.

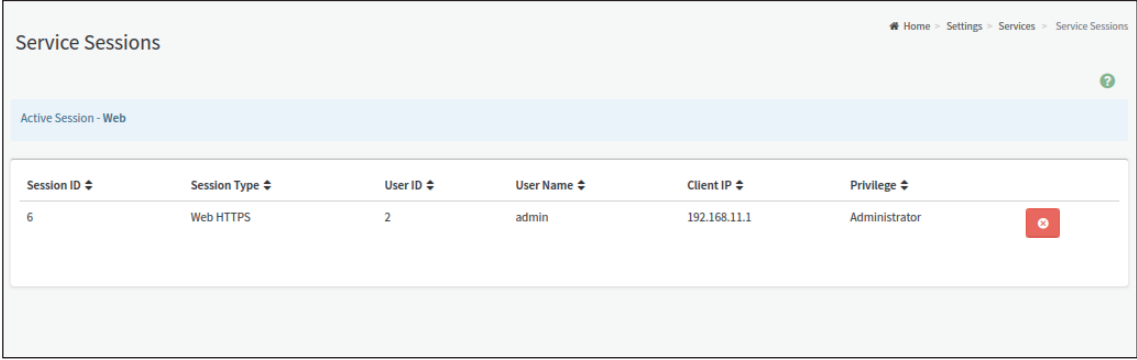
Maximum Sessions: Displays the maximum number of allowed sessions for the service.

Active Sessions: To view the current active sessions for the service.

To view the Active Sessions:

Procedure:

1. Click View Icon () to view the details about the active sessions for the service.
2. This opens the Active Session screen (for example - Service Sessions) as shown in the screenshot below.



Session ID ↕	Session Type ↕	User ID ↕	User Name ↕	Client IP ↕	Privilege ↕
6	Web HTTPS	2	admin	192.168.11.1	Administrator

Service Sessions

3. **Session Type:** Displays the type of the active sessions.
4. **User:** Displays the name of the user.
5. **Client IP:** Displays the IP addresses that are already configured for the active sessions.
6. **Privilege:** Displays the access privilege of the user.
7. Select a slot and click **Terminate** icon () to terminate the particular session of the service.

To modify the existing services:

Procedure:

1. Select a slot and click [Edit](#) icon () to modify the configuration of the service.

**NOTE**

Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

2. This opens the **Service Configuration** screen as shown in the screenshot below.

Service Configuration

3. **Service Name** is a read only field.
4. Activate the Current State by enabling the **Active** check box.

**NOTE**

Interfaces, Nonsecure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

5. Choose any one of the available interfaces from the **Interface Name** drop-down list.
6. Enter the Secure Port Number in the **Secure Port** field.
7. Enter the timeout value in the **Timeout** field.

**NOTE**

The values in the Maximum Sessions field cannot be modified.

8. Click [Save](#) to save the entered changes else click [Cancel](#) to exit.

4.4.8.6 SMTP Settings

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Using MegaRAC GUI, you can configure the SMTP settings of the device.

To open SMTP Settings page, click [Settings > SMTP Settings](#) from the menu bar. A sample screenshot of SMTP Settings Page is shown below.

SMTP Settings Page

The fields of SMTP Settings Page are explained below.

LAN Interface: Displays the list of LAN channels available

Sender Email ID: A valid 'Sender Address' to indicate the BMC, whenever e-mail is sent.

Primary Server Name: The 'Machine Name' of the BMC, from where the e-mail is sent.



NOTE

- Machine Name is a string of maximum 15 alpha-numeric characters.
- Space, special characters are not allowed.

Primary SMTP Support: To enable/disable SMTP support for the BMC.

Primary SMTP Port: To specify the SMTP Normal Port.

Primary Secure SMTP Port: To specify the SMTP Secure Port.



NOTE

- For Primary SMTP Port - Default Port is 25, and the Port value ranges from 1 to 65535.
- For Primary Secure SMTP Port - Default Port is 465, and the Port value ranges from 1 to 65535.

Primary Server IP: The IP address of the SMTP Server. It is a mandatory field.



NOTE

- IP Address made of 4 numbers separated by dots as in "xxx.xxx. xxx.xxx".
- Each Number ranges from 0 to 255.
- First Number must not be 0.
- Supports IPv4 Address format and IPv6 Address format.

Primary SMTP Authentication: To enable/disable SMTP Authentication.



NOTE

- SMTP Server Authentication Types supported are:
- CRAM-MD5
 - LOGIN
 - PLAIN

If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, **Authentication type is not supported by SMTP Server.**

Primary Username: Enter username to access SMTP Accounts.



NOTE

- User Name can be of length 4 to 64 alpha-numeric characters, dot(.), dash(-), and underline(_).
- It must start with an alphabet.
- Other Special Characters are not allowed.

Primary Password: Enter password for the SMTP User Account.



NOTE

- Password must be at least 4 characters long.
- White space is not allowed.
- This field will not allow more than 64 characters.

Primary SMTP STARTTLS Enable: To enable STARTTLS support for the SMTP Client.

- **Upload SMTP CA Certificate File:** File that contains the certificate of the trusted CA certs. CACERT key file should be of pem type,
- **Upload SMTP Certificate File:** Client certificate filename. CERT key file should be of pem type.
- **Upload SMTP Private Key:** Client private key filename. SMTP key file should be of pem type.

**NOTE**

To enable STARTTLS support, the respective SMTP support option should be enabled.

Secondary SMTP Support: It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working fine, then it tries with Secondary SMTP Server configuration.

**NOTE**

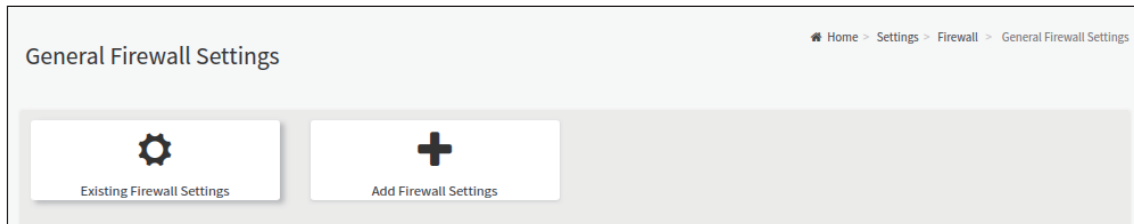
Options of Secondary SMTP Support are same as Primary SMTP Support.

Save: To save the new SMTP server configuration.

4.4.8.7 System Firewall

The System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

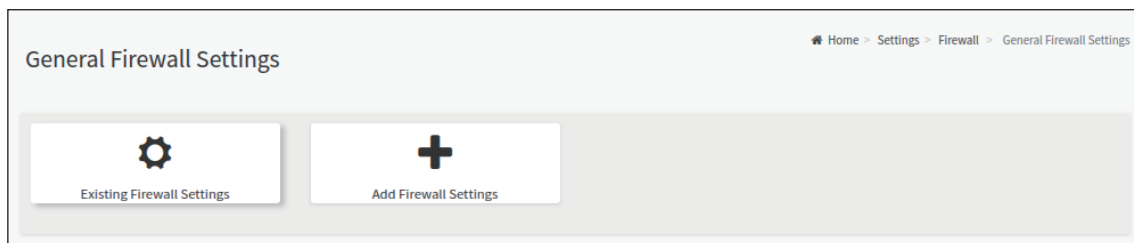
To open System Firewall page, click [Settings > System Firewall](#) from the menu bar.



Firewall Settings

General Firewall Settings

Click [Settings > Firewall > General Firewall Settings](#) from the menu bar. A sample screenshot of General Firewall Settings page is shown below.



General Firewall Settings

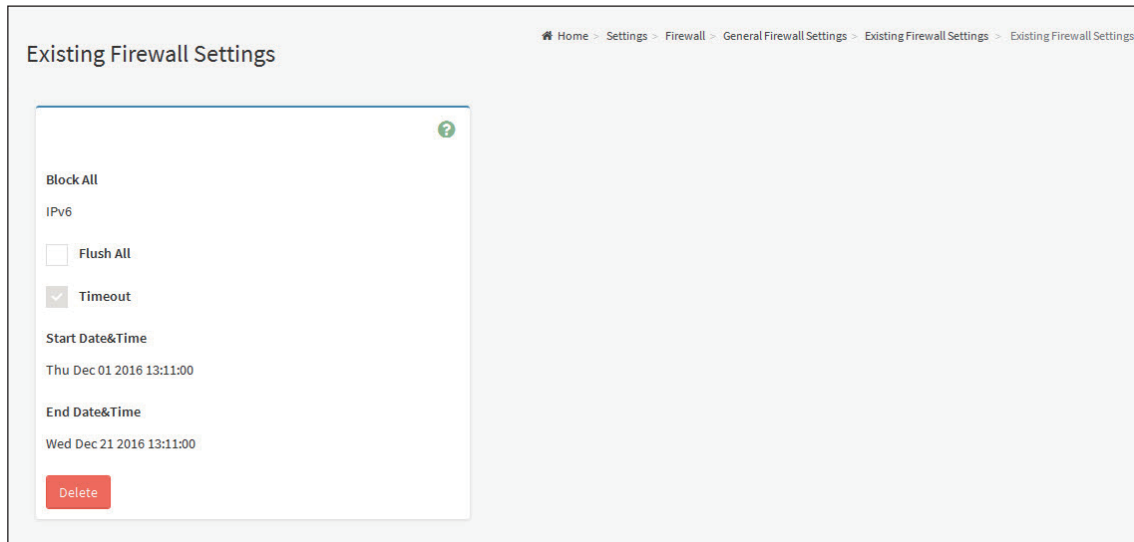
The fields of **Firewall Settings** tab are explained below.

Existing Firewall Settings

A blank page will be opened if you did not add anything in “Add Firewall settings”. If there is no Firewall Settings Exists, add a new Firewall settings by clicking link [Add Firewall Settings](#) page.

Procedure to Add Firewall settings

Click [General Firewall Settings](#) > [Existing Firewall Settings](#) icon. A sample screenshot of Existing Firewall Settings page is shown below.



Existing Firewall Settings

- **Block All:** The blocked incoming IP's and Port's can be viewed.
- **Flush All:** To flush all the system firewall rules (Read-Only).
- Select **Timeout** to enable or disable firewall rules with timeout.
- **Time Out** - The respective firewall rule effect Start Time, End Date, Start Time, End Time will be displayed.
- **Delete:** To Delete the system firewall rules.

Add Firewall Settings

1. Click [General Firewall Settings > Add Firewall Settings](#). This opens the Existing Firewall Settings page as shown below.

The screenshot shows the 'Add Firewall Settings' page. At the top right, there is a breadcrumb trail: Home > Settings > Firewall > General Firewall Settings > Add Firewall Settings. The main form area contains the following elements:

- Block All:** A dropdown menu currently showing 'IPv4'.
- Flush All:** An unchecked checkbox.
- Timeout:** An unchecked checkbox.
- Start Date:** A text input field with the placeholder 'YYYY/MM/DD' and a calendar icon.
- Start Time:** A text input field with a clock icon.
- End Date:** A text input field with the placeholder 'YYYY/MM/DD' and a calendar icon.
- End Time:** A text input field with a clock icon.
- Save:** A blue button with a floppy disk icon and the text 'Save'.

Add Firewall Settings

2. Select [Block All](#) to block all the incoming IP's and Port's.
3. Select [Flush All](#) to flush all the system firewall rules.
4. Select [Timeout](#) to enable or disable firewall rules with timeout.
5. Enter [Start Time](#) to start the respective firewall rule effect from this time.
6. Enter [End Time](#) to end the respective firewall rule effect from this time.



NOTE

The time should be in the dd-mm-yy:hh-mm format.

7. Click [Save](#) to save the changes made else click [Cancel](#) to go back to the previous screen.

IP Address Firewall Rules

Click [Settings > Firewall > IP Address Firewall Rules](#) from the menu bar. A sample screenshot of IP Address Firewall Rules page is shown below.



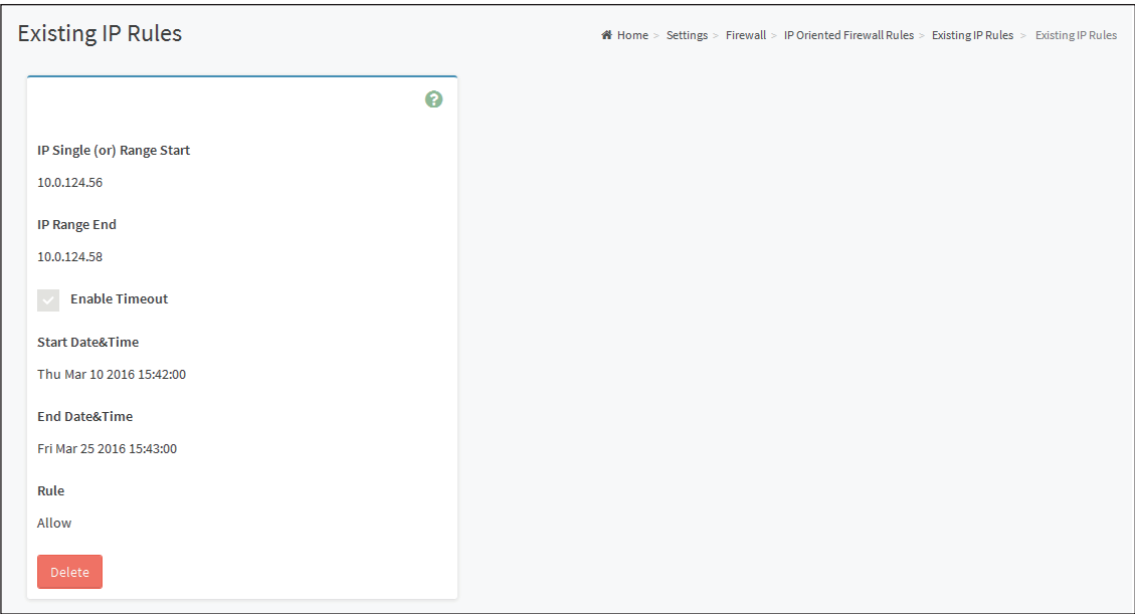
IP Address Firewall Rules

To View Existing IP Rules or a range of IP Addresses

A blank page will be opened if you did not add anything in “Add IP Rule”. If there is no Add IP Rule Exists, add a new IP Rule by clicking link [Add IP Rule](#) page.

Procedure to Add IP Rule

1. Click [Settings > System Firewall > IP Address Firewall Rules > Existing IP Rules](#). A blank page will be opened if you did not add anything in “Add IP Rule”. If any rule is added, then the added rule will be listed in “Existing IP Rules” page.
2. Click the [IP Addresses](#) tab. A sample screenshot of **IP Addresses** tab is shown below.



System Firewall - Existing IP Rule

IP Single (or) Range Start: To show the configured Port Address or Range of Ports.

IP Range End: To show the configured Port Address or Range of Ports.

Enable Timeout: To enable/disable Timeout.

Start Date: The respective firewall rule effect will start from this date.

Start Time: The respective firewall rule effect will start from this time.

End Date: The respective firewall rule effect will end from this date.

End Time: The respective firewall rule effect will end from this time.

Rule: To indicate the current setting of the listed Port or Range of Port rules (Allow or Block) status.

Delete: To delete the selected slot.

Procedure To add an IP address or range of IP addresses

1. Click [Settings > System Firewall > IP Address Firewall Rules > Add New IP Rule](#) to add a new IP or range of IP address.

The screenshot shows the 'Add IP Rule' form within a web interface. The breadcrumb trail at the top right reads: Home > Settings > Firewall > IP Oriented Firewall Rules > Add IP Rule. The form itself is titled 'Add IP Rule' and contains the following fields:

- IP Single (or) Range Start:** A text input field.
- IP Range End:** A text input field with the placeholder text 'optional'.
- Enable Timeout:** A checkbox.
- Start Date:** A date picker showing 'YYYY/MM/DD'.
- Start Time:** A time picker.
- End Date:** A date picker showing 'YYYY/MM/DD'.
- End Time:** A time picker.
- Rule:** A dropdown menu currently set to 'Allow'.
- Save:** A blue button at the bottom right of the form.

Add IP rule

2. In the **Add new rule for IP** page, Enter the IP address and a range of IP addresses in the **IP Single or IP Range Start** field.



NOTE

IP Address will support IPv4 Address format only:

- IPv4 Address made of 4 numbers separated by dots as in xxx.xxx.xxx.xxx.
- Each number ranges from 0 to 255.
- First number must not be 0.
- IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by colon as in xxx x:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

3. Enter IP range end value in the **IP Range End** field.
4. Enable **Timeout** to enable firewall rules with timeout.
5. Enter **Start Date** to start the respective firewall rule effect from this date.
6. Enter **End Date** to end the respective firewall rule effect from this date.
7. Enter **Start Time** to start the respective firewall rule effect from this time.
8. Enter **End Time** to end the respective firewall rule effect from this time.

**NOTE**

The date and time should be in the YYYY/MM/DD and hh-mm format respectively.

9. Determine the rule to block or accept.
10. Click [Save](#) to save the changes made.

Port Firewall Rules

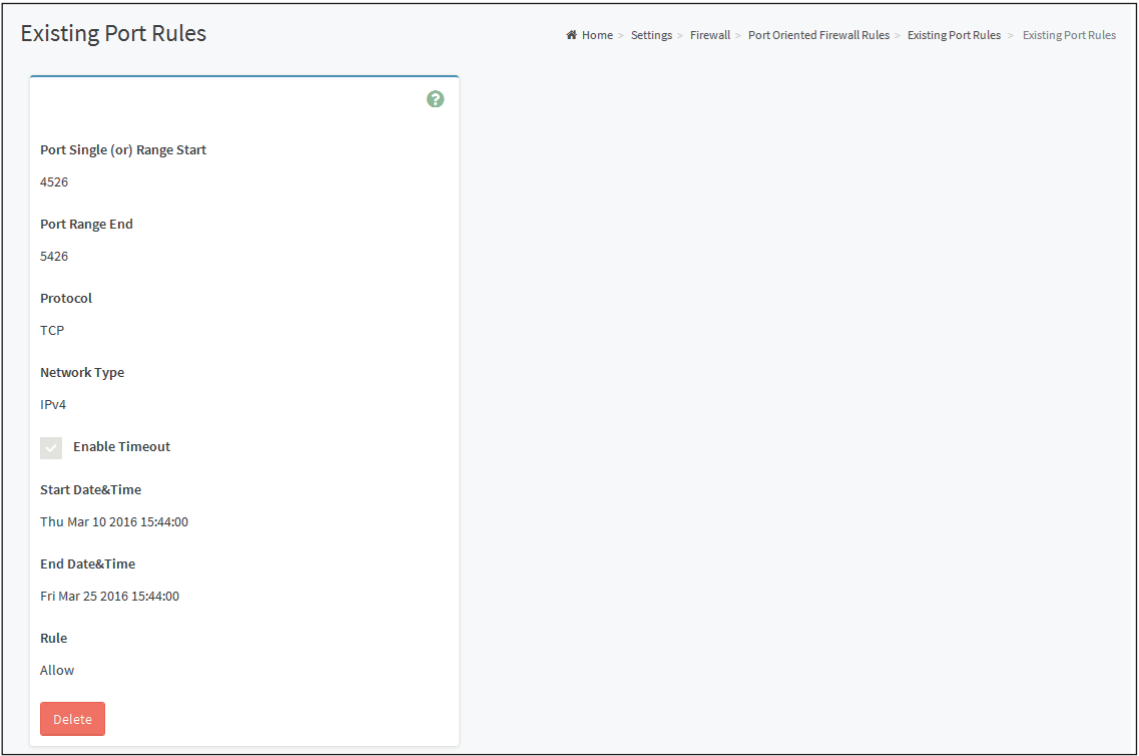
Click [Settings > Firewall > Port Firewall Rules](#) from the menu bar. A sample screenshot of Port Firewall Rules page is shown below.



Port Firewall Rules

To view Existing Port Rules

1. Click [Settings > System Firewall > Port Firewall Rules > Existing Port Rules](#). A blank page will be opened if you did not add anything in “Add New port Rule”. If any rule is added, then the added rule will be listed in “Existing Port Rules” page
2. Click the [Existing Port Rules](#). A sample screenshot of Port tab is shown below.



System Firewall - Existing Port Rules

The fields of System Firewall: **Existing Port Rules** page are explained below.

Port Single (or) Range Start : To configure the Port or Range of Port Addresses.

Port Range End : To configure the Port or Range of Port Addresses.

Protocol : This field specifies the protocols for the configured Port or Port Ranges.

Network Type : This field specifies the affected network type for the particular Port or Port Ranges.

Enable Timeout : To enable or disable firewall rules with timeout.

Start Date : The respective firewall rule effect will start from this time.

Start Time : The respective firewall rule will start from this time.

End Date : The respective firewall rule effect will end on this date.

End Time : The respective firewall rule will end at this time.

Rule : To indicate **Allow** or **Block** status.

Delete : To delete the entry to the firewall rules list.

To Add Port/Range of ports

1. To add a new rage of Port address, click the [Add](#) button.

The screenshot displays the 'Add Port Rule' configuration page. The breadcrumb trail at the top indicates the navigation path: Home > Settings > Firewall > Port Oriented Firewall Rules > Add Port Rule. The form contains the following fields:

- Port Single (or) Range Start**: A text input field.
- Port Range End**: A text input field with the placeholder text 'optional'.
- Protocol**: A dropdown menu currently set to 'TCP'.
- Network Type**: A dropdown menu currently set to 'IPv4'.
- Enable Timeout**: A checkbox that is currently unchecked.
- Start Date**: A date picker field showing 'YYYY/MM/DD'.
- Start Time**: A time picker field.
- End Date**: A date picker field showing 'YYYY/MM/DD'.
- End Time**: A time picker field.

Add Port rule

2. In the **Add new rule for Port** window, Enter the port number or a range of port numbers in the **Port Single (or) Range Start** field.

**NOTE**

Port value ranges from 1 to 65535.

3. Enter the end value in the **Port Range End** field.
4. Select the **Protocol** to be either TCP or UDP or Bot.
5. Select the **Network Type**. It may be IPv4 or IPv6 or Both.
6. Select **Timeout** to enable or disable firewall rules with timeout.
7. Enter **Start Time** to start the respective firewall rule effect from this time.
8. Enter **Start Date** to start the respective firewall rule effect from this date.
9. Enter **End Date** to end the respective firewall rule effect on this date.
10. Enter **End Time** to end the respective firewall rule effect at this time.

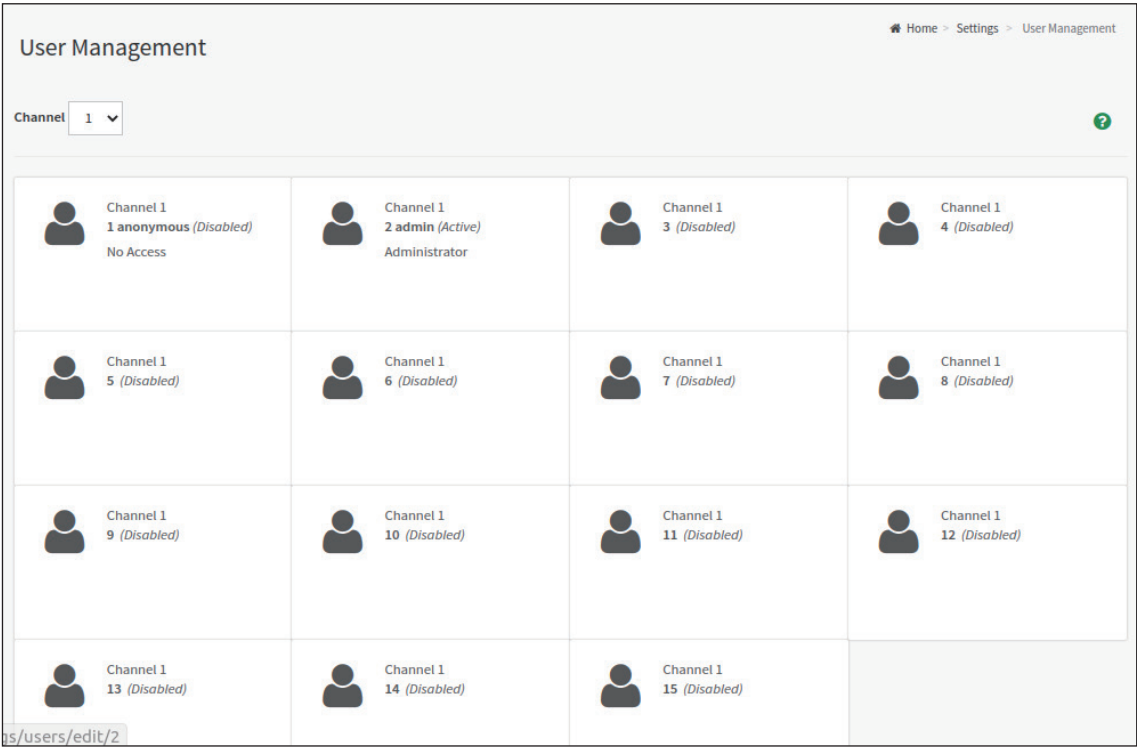
**NOTE**

The time should be in the YYYY/MM/DD:hh-mm format.

11. Select the **Rule** to determine the rule to **Block** or **Allow**.
1. 12. Click [Save](#) to save the changes made.

4.4.8.8 User Management

The User Management page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users. To open User Management page, click [Settings > User Management](#) from the menu bar. A sample screenshot of User Management page is shown below.



User Management

Click user icon () and select any free slot to add a new user from the User Management main page.
Click Delete icon () on the top right corner to directly delete an item from the list.



NOTE

The Free slots are shown as “Disabled” in all columns for the slot.

The fields of User Management Page are explained below.

Channel: To choose a particular channel from the available channel list.

User ID: Displays the ID number of the user.



NOTE

The list contains a maximum of fifteen users only.

User Name: Displays the name of the user.

User Access: To enable or disable the access privilege of the user.

Network Privilege: Displays the network access privilege of the user.

SNMP Status: Displays if the SNMP status for the user is enabled or Disabled.

E-mail ID: Displays e-mail address of the user.

Add User: To add a new user.

Delete User: To delete an existing user.

Procedure to add a new User

1. To add a new user, select a free section and click on the empty section. This opens the Add User screen as shown in the screenshot below.

User Management Configuration

Home > Settings > User Management > User Management Configuration

Username

☐ Change Password

Password Size

16 bytes

Password

Confirm Password

☒ Enable User Access

Enable Channel Access

☒ Channel 1

☒ Channel 8

Privilege(Channel 1)

Administrator

Privilege(Channel 8)

Administrator

☐ SNMP Access

SNMP Access level

SNMP Authentication Protocol

SNMP Privacy Protocol

Email Format

AMI-Format

Email ID

sJtJxhtl@amilindia.co.in

Existing SSH Key

Not Available

Upload SSH Key

2. Enter the name of the user in the **User Name** field.



NOTE

- User Name is a string of 1 to 16 alpha-numeric characters.
- It must start with an alphabetical character.
- It is case-sensitive.
- Special characters '-'(hyphen), '_'(underscore), '@'(at sign) are allowed.
- For 20 Bytes password, LAN session will not be established.

3. Set **Password Size** for the new password.

4. In the **Password** and **Confirm Password** fields, enter and confirm your new password.

NOTE

- Password should be the combination of alphabets, numbers, symbol and upper case characters.
- White space is not allowed.
- This field will not allow more than 16/20 characters based on Password size field value.
- This field will not allow the below mentioned characters.
- The password should be a string, if you try to set password using "ipmitool user set password".

Hex	Char
00	NUL '\0'
01	SOH (start of heading)
02	STX (start of text)
03	ETX (end of text)
04	EOT (end of transmission)
05	ENQ (enquiry)
06	ACK (acknowledge)
07	BEL '\a' (bell)
08	BS '\b' (backspace)
09	HT '\t' (horizontal tab)
0A	LF '\n' (new line)
0B	VT '\v' (vertical tab)
0C	FF '\f' (form feed)
0D	CR '\r' (carriage ret)
0E	SO (shift out)
0F	SI (shift in)
10	DLE (data link escape)
11	DC1 (device control 1)
12	DC2 (device control 2)
13	DC3 (device control 3)
14	DC4 (device control 4)
15	NAK (negative ack.)

Hex	Char
16	SYN (synchronous idle)
17	ETB (end of trans. blk)
18	CAN (cancel)
19	EM (end of medium)
1A	SUB (substitute)
1B	ESC (escape)
1C	FS (file separator)
1D	GS (group separator)
1E	RS (record separator)
1F	US (unit separator)
20	SPACE
7F	DEL

5. In **Enable User Access**, select this option to enable the network access for the appropriate user.

**NOTE**

- Enabling Channel User Access will intern assign the IPMI messaging privilege to the specific Channel user.
- It is recommended that the IPMI messaging option should be enabled for the user to enable the User Access option, while creating User through IPMI.

6. In **Enable Channel Access** field, select the channel/channels to enable the network access for the appropriate channels.

7. In the **Privilege** field, select the privilege assigned to the user which could be Administrator, Operator, User, OEM or None. By default, the channel privileges will be displayed based on the channel availability.

8. Check the **SNMP Access** check box to enable SNMP access for the user.

**NOTE**

Password field is mandatory, if SNMP Status is enabled.

9. Choose the SNMP Access level option for user from the **SNMP Access level** (SHA or MD5) drop-down list. Either it can be Read Only or Read Write.

10. Choose the **SNMP Authentication Protocol** (SHA or MD5) to use for SNMP settings from the drop down list.

**NOTE**

Password field is mandatory, if Authentication protocol is changed.

11. Choose the Encryption algorithm to use for SNMP settings from the **SNMP Privacy protocol** (AES or DES) drop-down list.

12. In the **Email ID** field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

**NOTE**

SMTP Server must be configured to send emails.

Email Format: Two types of formats are available:

AMI-Format: The subject of this mail format is 'Alert from (your Host name)'. The mail content shows sensor information, ex: Sensor type and Description.

Fixed-Subject Format: This format displays the message according to user's setting. You must set the subject and message for email alert.

13. In the Upload SSH Key field, click Browse and select the SSH key file.

**NOTE**

SSH key file should be of pub type.

14. Click [Save](#) to save the new user and return to the users list.

To Modify User

1. To modify the existing user, click on the active user tab.
2. Check **Change Password**, if you wish to change the existing Password.
3. Follow the steps (3 to 15) of Procedure to add a new User.
4. Click [Save](#) to save the changes and return to the users list.
5. Click [Save](#) to save the changes and return to the users list.

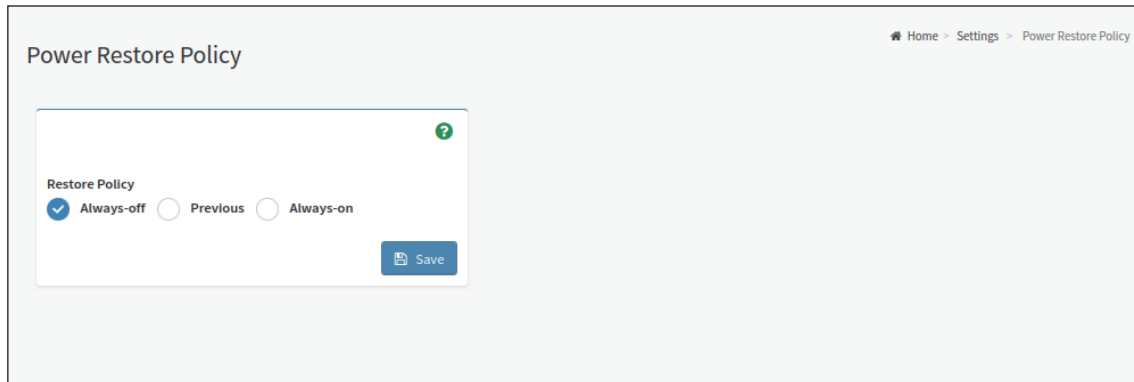
Important:

Reserved Users: There are certain reserved users which cannot be added as BMC Users. The list of reserved users are given below,

- sysadmin
- daemon
- sshd
- ntp
- root

4.4.8.9 Power Restore Policy

To open Power Restore Policy page, click [Settings > Power Restore Policy](#) from the menu bar. A sample screenshot of Power Restore Policy page is shown below.



Power Restore Policy

After an unexpected power failure, the state of the system power supply when the power supply is restored.

Always-off: Keep power off

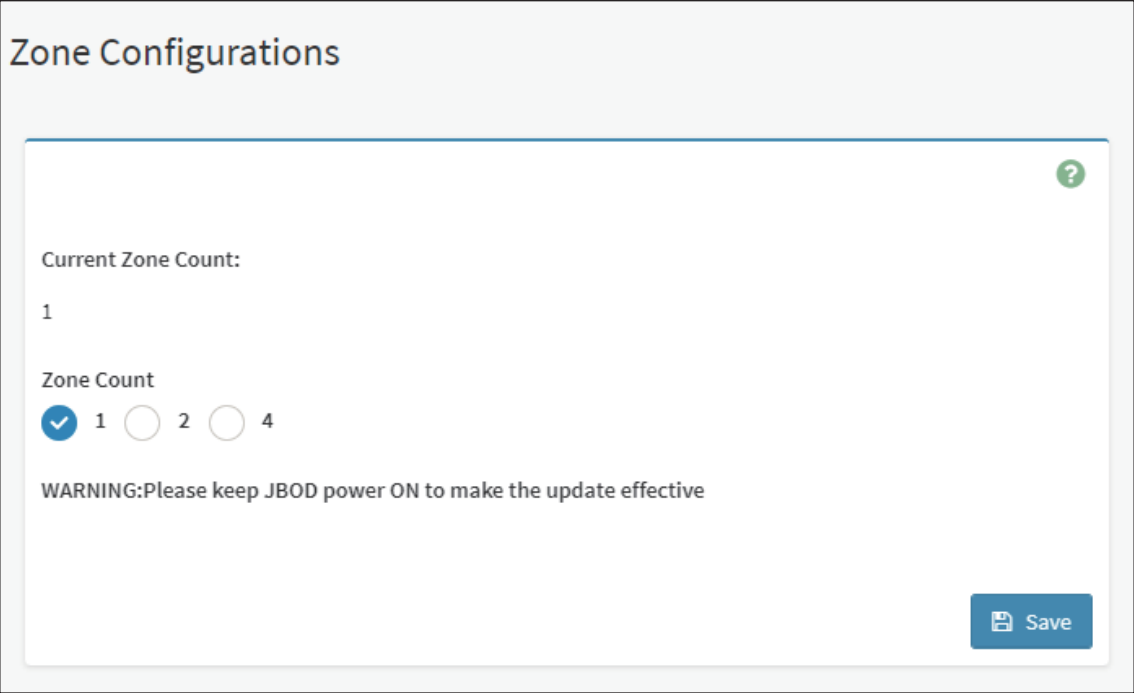
Previous: Restore to the previous state

Always-on: Keep power on

4.4.8.10 Zone Configurations

Remove the SAS cable (SFF-8644) between the HBA/RAID card and the JBOD-4U78 before configuration T10 zoning. After configuring T10 zoning, please power cycle the JBOD-4U78 and then insert the SAS cable back (SFF-8644).

To open Zone Configurations page, click [Settings > Zone Configurations](#) from the menu bar. A sample screenshot of Zone Configurations page is shown below.



The screenshot shows the 'Zone Configurations' page. At the top, the title 'Zone Configurations' is displayed. Below it, a green question mark icon is visible. The main content area shows 'Current Zone Count:' followed by the value '1'. Underneath, the 'Zone Count' section has three radio button options: '1' (which is selected with a blue checkmark), '2', and '4'. A warning message states: 'WARNING: Please keep JBOD power ON to make the update effective'. In the bottom right corner, there is a blue 'Save' button with a floppy disk icon.

In the BMC Web UI, we only provide three default settings (1, 2, 4),
The chassis is set to three states (1, 2, 4) through EXP console command "zonecount".

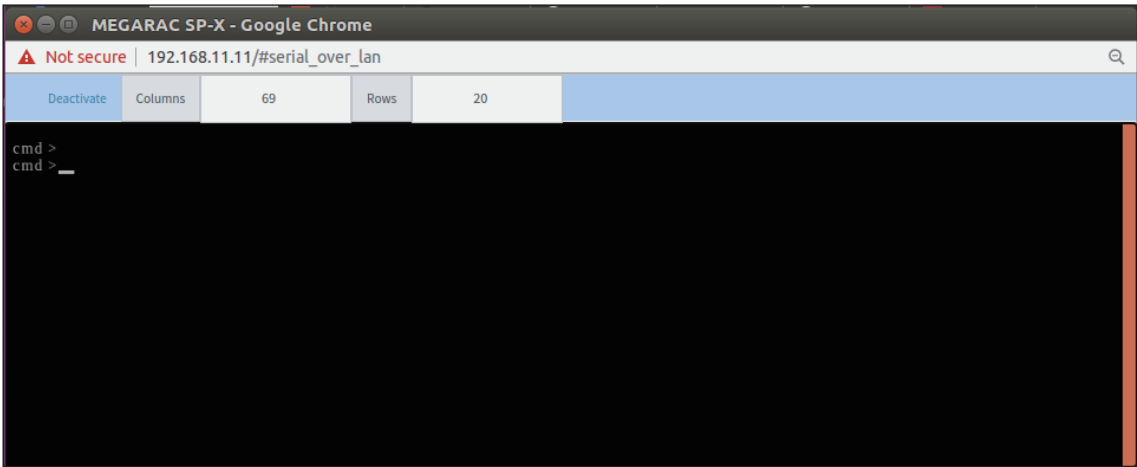
4.4.9 Remote Control

The Remote Control page consists of the following options. A sample screenshot is displayed below.



Remote Control page

To open Remote Control page, click [Remote Control](#) from the menu bar. Open the Remote Control page, click [Activate](#). A sample screenshot of the Remote **serial over lan** page is shown below.

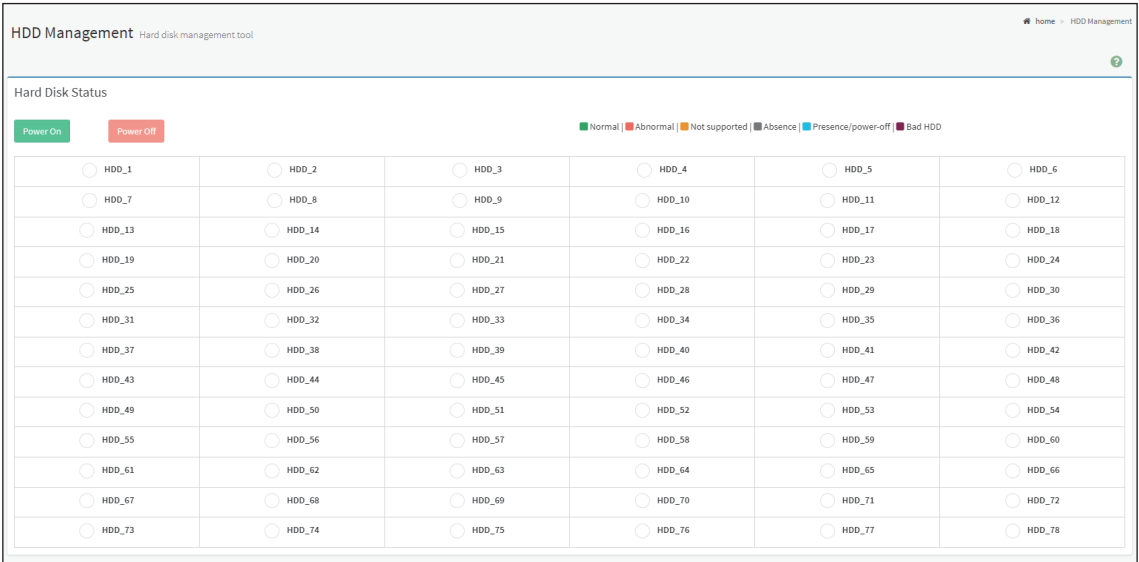


serial over lan

4.4.10 HDD Management

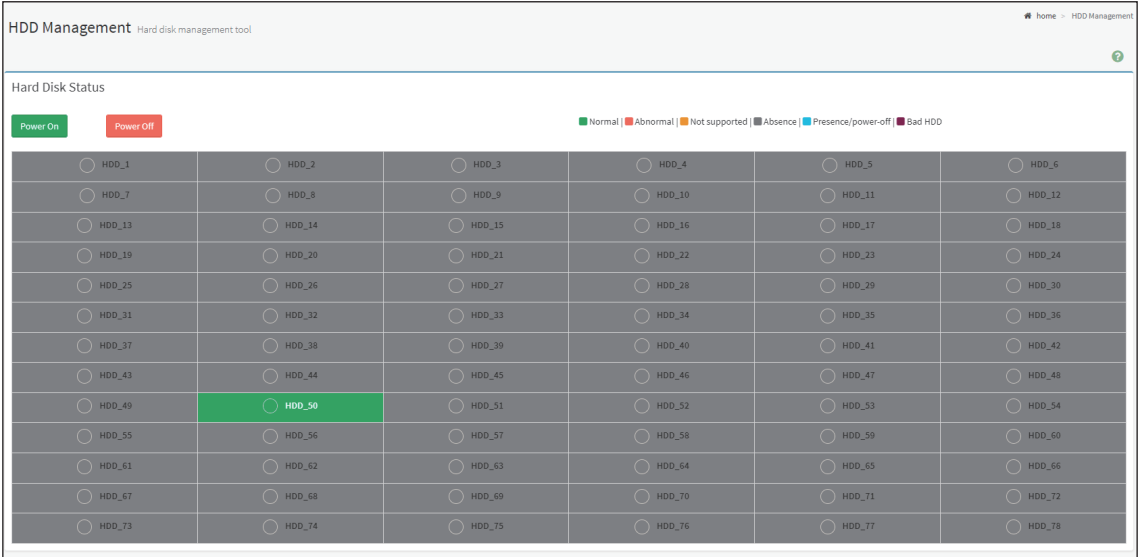
This page allows you to view and control the hard disk drivers.
To open HDD Management, click [HDD Management](#) from the menu bar. A sample screenshot of HDD Management page is shown below.

When host is currently off



HDD Management page

When host is currently on



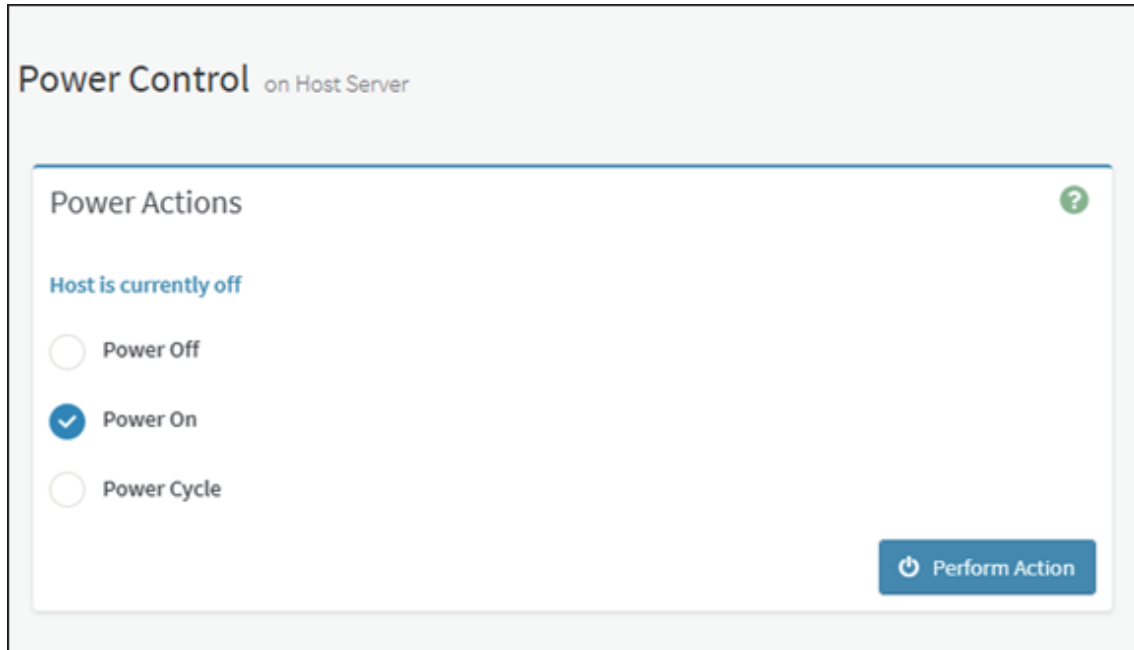
HDD Management page

Each hard disk driver will display a different color, each color represents a different state including normal, abnormal and absence, etc.
Power on: To power on the hard disk driver.
Power off: To power off the hard disk driver.

4.4.11 Power Control

This page allows you to view and control the power of your server.

To open Power Control, click [Power Control](#) from the menu bar. A sample screenshot of Power Control is shown below.



Power Control

The various options of Power Control are given below.

Power Off: To immediately power off the server.

Power On: To power on the server.

Power Cycle: This option will first power off, and then reboot the system (cold boot).

4.4.12 Maintenance Group

To open Power Control, click [Maintenance](#) from the menu bar. A sample screenshot of Maintenance page is displayed below.



Maintenance

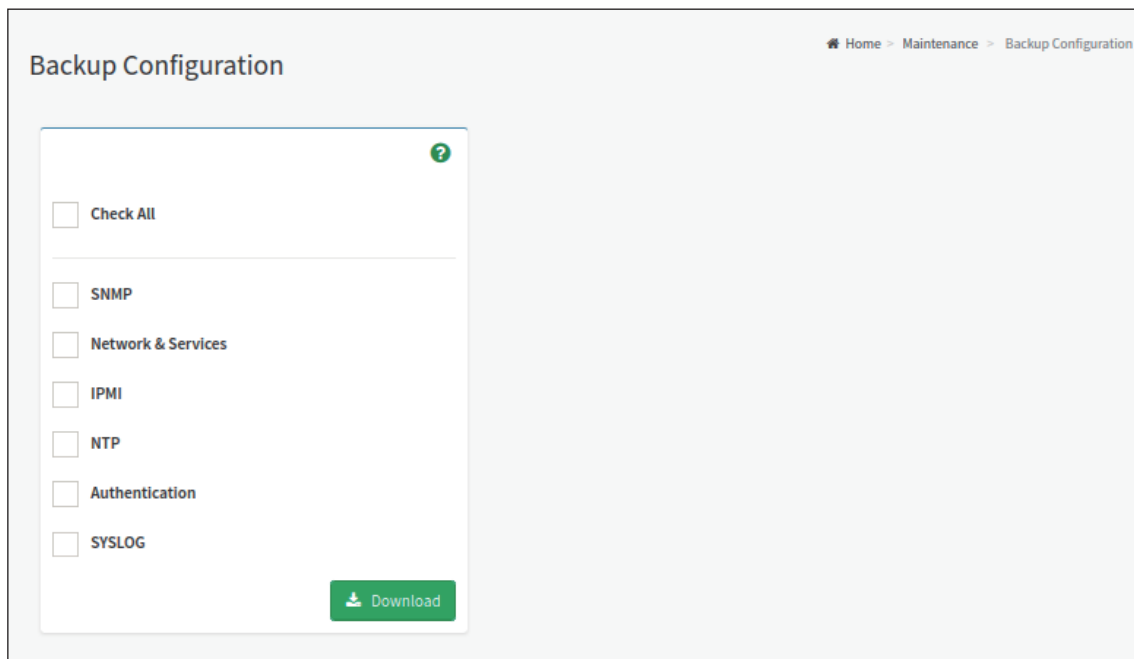
- Backup Configuration
- Firmware Image Location
- BMC Firmware Information
- BMC Firmware Update
- Preserve Configuration
- Restore Configuration
- Expander Update
- BMC Rest

A detailed description is given below.

4.4.12.1 Backup Configuration

This page allows you to select the specific configuration items to be backup in case of “Backup Configuration”.

To open Backup Configuration page, click [Maintenance > Backup Configuration](#) from the menu bar. A sample screenshot of Backup Configuration page is shown below.



Backup Configuration

Check All: To select all the configuration list.

Download: To download and save the configuration files backup from BMC to client system.



NOTE

During backup, because of security concern, the mechanism parses sensitive data to filter it out and not backup sensitive files. User has to set password again after restoring configuration by using default user in case of login failure.

Procedure for Backup Configuration:

1. Click [Check All](#) to back up all the configuration items or check the configuration that needs to be back up. The Backup Configuration page will appear as shown in the above screenshot.



NOTE

Network configurations are inter-related to IPMI, and hence by default IPMI configurations will be selected automatically when you select “Network and Services” to be backed up.

2. Click [Download Config](#) to save the backup file to the client system.

4.4.12.2 Firmware Image Location

This page is used to configure firmware image into the BMC.

To open **Firmware Image Location**, click [Maintenance > Firmware Image Location](#) from the menu bar. A sample screenshot of **Firmware Image Location** page is shown below.

Firmware Image Location

The various options of Image Transfer Protocol are given below.

Image Location Type : Type of location to transfer the firmware image into the BMC either Web Upload during Flash or TFTP Server.

TFTP Server Address: Address of the server where the firmware image is stored.



NOTE

The Server supports both IPv4 and IPv6 addresses

- IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each number ranges from 0 to 255.
- First number must not be 0.
- IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by colon as in "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx".
- Hexadecimal digits are expressed as lower-case letters.

TFTP Image Name: Full Source path with filename of the firmware image is stored on TFTP Server.

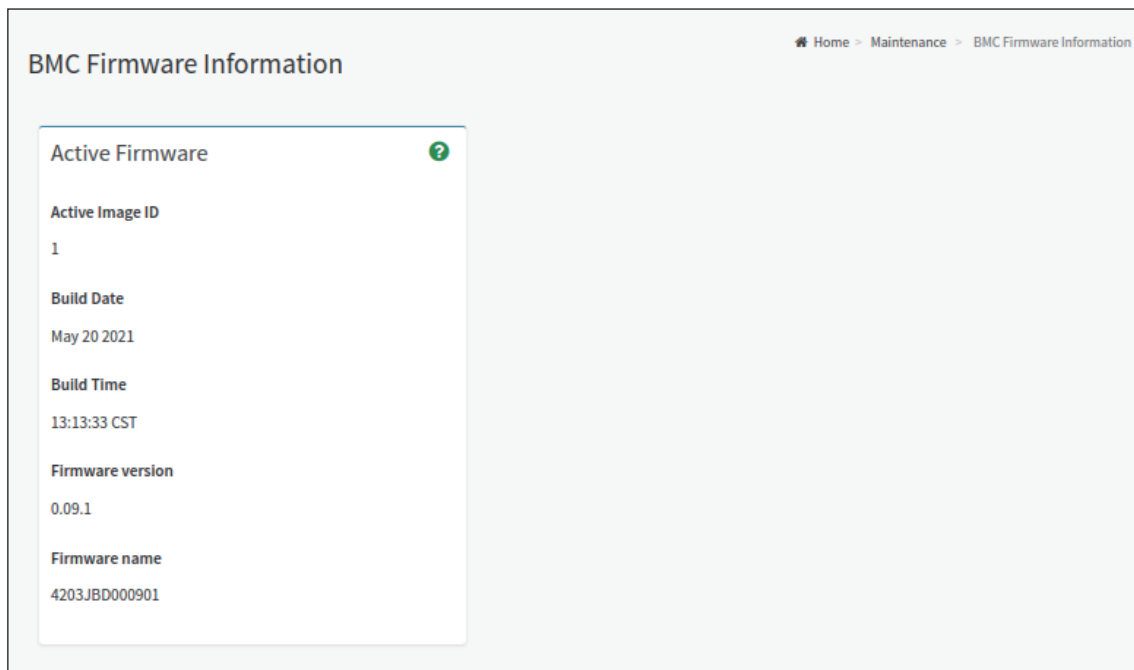
TFTP Retry Count: Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.

Save: To save the configured settings.

4.4.12.3 BMC Firmware Information

This page shows the BMC Firmware Information.

To open BMC Firmware Information page, click [Maintenance > BMC Firmware Information](#) from the menu bar. A sample screenshot of BMC Firmware Information page is shown below.



Backup Firmware Information

The various fields of BMC Firmware Information page are given below.

Active Image ID: Describes the Active Image ID of the active BMC image.

Build Date: Describes the Build Date of the active BMC image.

Build Time: Describes the Build Time of the active BMC image.

Firmware version: Describes the Firmware version of the active BMC image.

Firmware name: Describes the Firmware name of the active BMC image.

4.4.12.4 BMC Firmware Update

This wizard takes you through the process of firmware upgradation. A reset of the box will automatically follow if the upgrade is completed or cancelled. An option to Preserve All Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade.

**Warning**

Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will be reset.

**NOTE**

The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.

Once you enter into Update Mode and choose to cancel the firmware flash operation, the BMC must be reset. This means that you must close the Internet browser and log back onto the BMC before you can perform any other types of operations.

Once Firmware upgrade using web is started, the regular IPMI command will not be allowed for safety concern if Enable IPMI Command handling during flashing support is disabled in project configuration.

This feature enables the user to perform all Firmware Update operations such as Firmware Update.

To configure, choose 'Firmware Image Location' under **Maintenance**. To open BMC Firmware Update page, click [Maintenance > BMC Firmware Update](#) from the menu bar. A sample screenshot of BMC Firmware Update Page is shown below.

Procedure

1. Click Choose File to select firmware image.

**NOTE**

A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of upload.

2. Click [Start firmware update](#) to load the Firmware Update information. A sample screenshot is displayed below.

Home > Maintenance > BMC Firmware Update

BMC Firmware Update

?

Select Firmware Image

Choose File

rom.ima

Start firmware update

Protocol Type:

HTTPS

☐

Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.

All configuration items below will be preserved as default during the restore configuration operation. Click "Edit Preserve Configuration" to modify the Preserve status settings.

[Edit Preserve Configuration](#)

S.No	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	NETWORK	Overwrite
6	NTP	Overwrite
7	SNMP	Overwrite
8	SSH	Overwrite
9	AUTHENTICATION	Overwrite
10	SYSLOG	Overwrite
11	WEB	Overwrite
12	REDFISH	Overwrite

Proceed to Flash

BMC Firmware Update Page



NOTE

SignImage Public Key is feature based option. If encrypted Signimage feature is enabled, then support to **Upload** a public.pem key info option will be available.

**NOTE**

Dual Firmware Update:

Select an Image (Inactive Image, Image 1, Image 2 or Both Image) from **Image to be Updated** drop-down list. The selected image will be getting flashed.

- **Image to be Updated:** To update an Image (Inactive, Image 1, Image 2 or Both) to be flashed. If You select an Inactive image, the Inactive image will be flashed. If you select both images, then Both Image 1 and Image 2 will be flashed with uploaded image file.
- **reboot the device after update:** This option is used to reboot the device after the firmware update.

Dual Image Selected

3. Click [Preserve all Configuration](#) to preserve all configuration.

- **Preserve all Configuration:** To preserve all configuration.
- **Edit Preserve Configuration:** To modify the Preserve status settings.

The protocol information to be used for firmware image transfer during this update is as follows.

**NOTE**

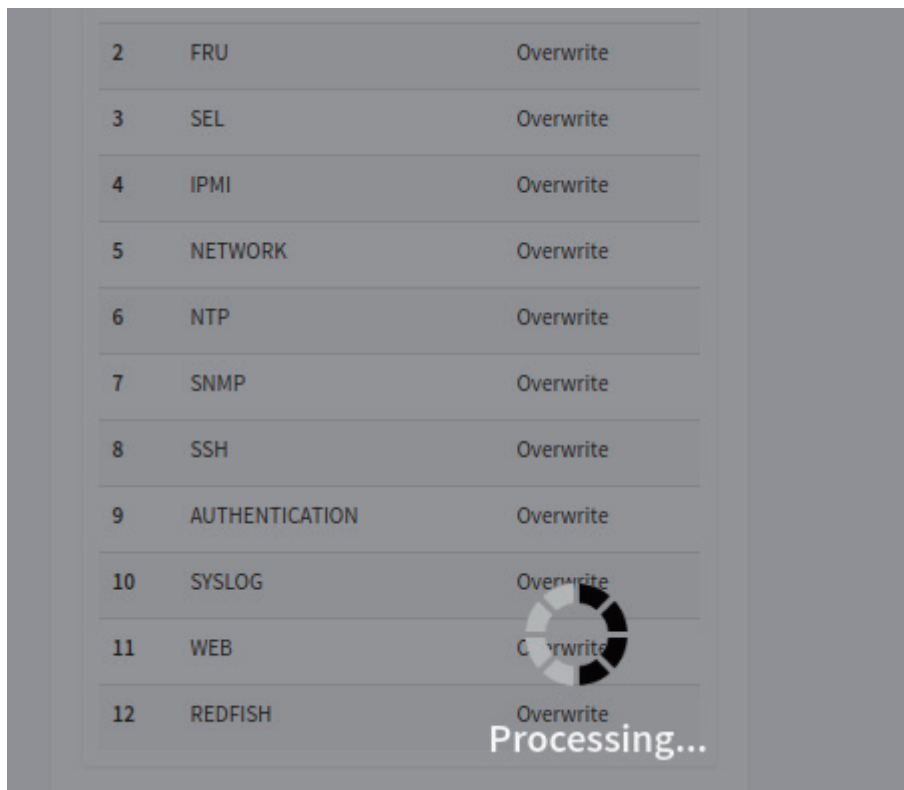
All configuration items will be preserved/overwrite as default during the restore configuration operation.

4. Click [Proceed to Flash](#), it will prompt you with the warning message. Click [Ok](#) to start the Firmware update.

Firmware Update

5. The Firmware update undergoes the following steps:
- Closing all active client requests
 - Preparing Device for Firmware Upgrade
 - Uploading Firmware Image.

A sample screenshot is shown as below.



Firmware Update - Image Upload Start

d. Verifying Firmware Image

In Section Based Firmware Update, you can configure the firmware image for section based flashing. Check the required sections and click [Proceed](#) to update the firmware.

If flashing is required for all images, select the option Full Flash .

If you select **Version Compare Flash** option from web, the current and uploaded module versions, FMHlocation, size will be compared.

If the modules differ in size and location, proceed with force firmware upgrade.

If all the module versions are same, restart BMC by saying all the module versions are similar.

If only few module versions are differing, those modules will be flashed.



NOTE

Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.

BMC Firmware Update

Home > Maintenance > BMC Firmware Update

?

Note:

Following are the Firmware update methods and components supported in this page.

Dual Firmware update.

Select Firmware Image

Choose File

rom.ima

Start firmware update

Protocol Type:

HTTPS

☐

Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.

All configuration items below will be preserved as default during the restore configuration operation. Click "Edit Preserve Configuration" to modify the Preserve status settings.

[Edit Preserve Configuration](#)

S.No	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	NETWORK	Overwrite
6	NTP	Overwrite
7	SNMP	Overwrite
8	SSH	Overwrite
9	AUTHENTICATION	Overwrite
10	SYSLOG	Overwrite
11	WEB	Overwrite
12	REDFISH	Overwrite

Section Based Firmware Update

All the module section versions in the existing image and uploaded image are the same.

☐Version Compare Flash

☐Full Flash

Section Name	Existing version	Uploaded version	Upgradable/Non-Upgradable
boot	12.1.000000	12.1.000000	☐
conf	12.1.000000	12.1.000000	☐
root	12.1.000000	12.1.000000	☐
osimage	12.1.000000	12.1.000000	☐
www	12.1.000000	12.1.000000	☐
ast2500e	0.9.1	0.9.1	☐

Flash selected sections

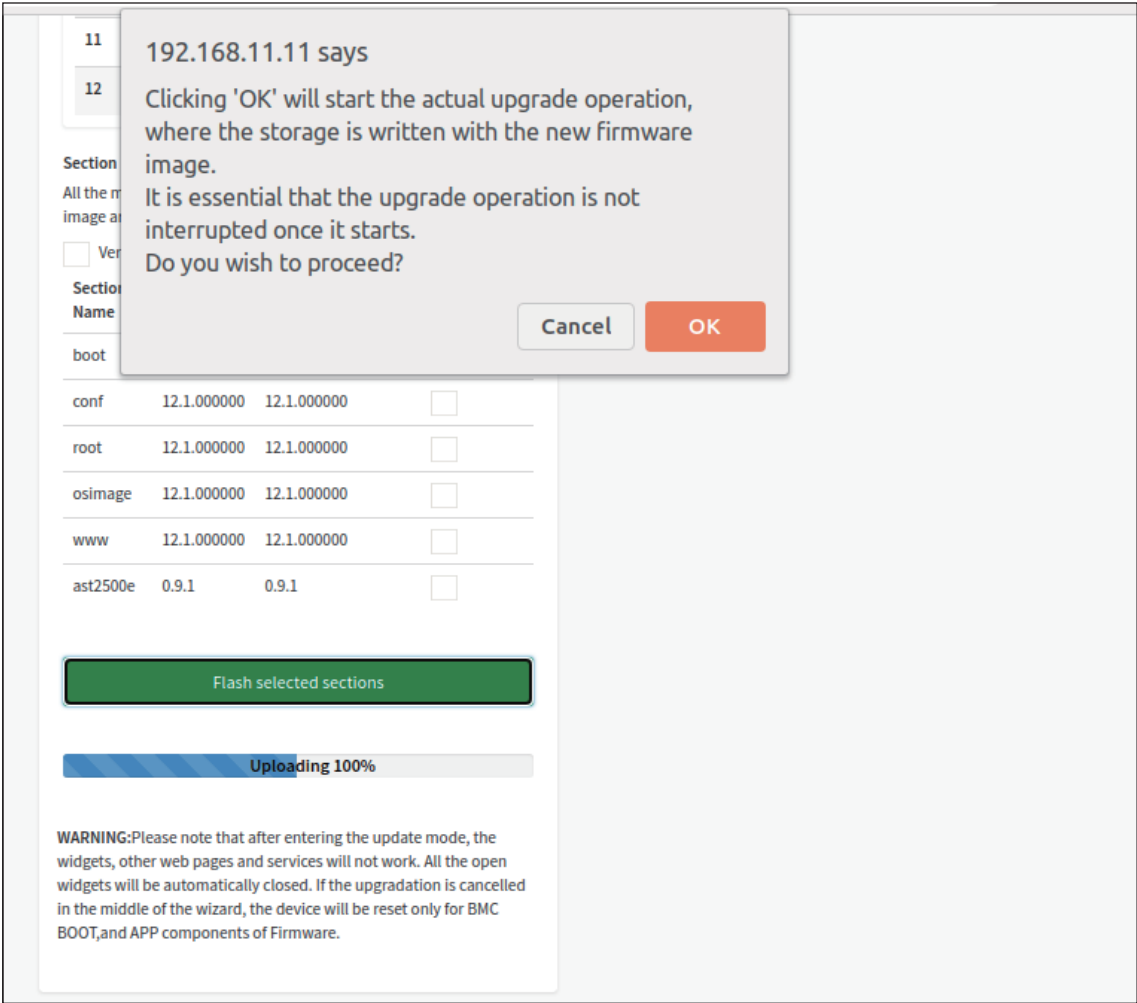
Uploading 100%

WARNING:

Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

Section Based Firmware Flashing

- e. Flashing Firmware Image
- f. Resetting the image. The sample screenshot of Firmware update is as shown below.



Firmware Update



NOTE

The Firmware Update page will be disabled and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.

4.4.12.5 Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without overwriting with defaults/ Firmware Upgrade configuration.

To open Preserve Configuration page, click [Maintenance > Preserve Configuration](#) from the menu bar. A sample screenshot of Preserve Configuration page is shown below.



NOTE

You can navigate to the Firmware Update Page and Restore Factory Defaults by clicking the respective links.

Preserve Configuration

The various fields of Preserve Configuration are as follows.

Click here to go to Firmware Update or Restore Factory Defaults: This link will redirect to the Firmware Update or Restore Factory Defaults page which needs to be preserved.

Check All: To check the entire configuration list.

Save: To save any changes made.



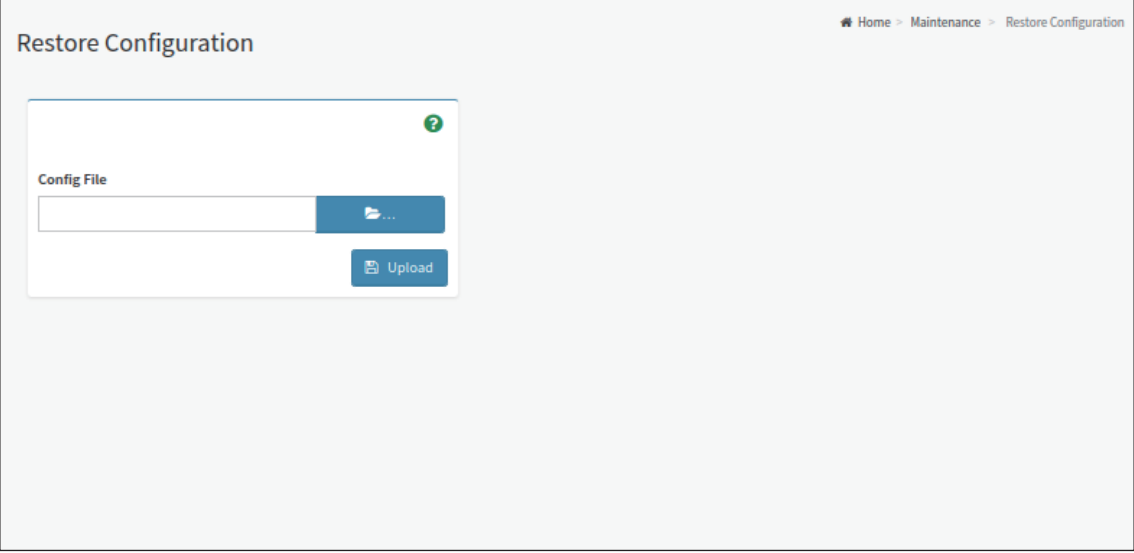
NOTE

This configuration is used by Restore Factory Defaults process.

- **SDR** : the sensor data record information will be preserved.
- **FRU** : the fru data will be preserved.
- **SEL** : the system event logs that are being logged by the IPMI will be preserved.
- **IPMI** : preserve the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.
- **Network** : To save network settings related with IPMI (LAN IP or DHCP configuration), selecting "IPMI" will automatically select another option "Network" and it's vice versa. After restore configuration, the Network Configuration will be preserved successfully.
- **NTP** : automatic or manual network type protocol and time settings will be preserved.
- **SNMP** : the SNMP user configurations and the SNMP user's privilege levels will be preserved.
- **SSH** : ssh configuration will be preserved.
- **Authentication** : Authentication related documents and settings will be preserved.
- **Syslog** : the system log configuration details will be preserved.
- **Web** : the firmware image location details will be preserved.
- **Redfish** : Redfish's files and settings will be preserved.

4.4.12.6 Restore Configuration

This page allows you to restore the configuration files from the client system to the BMC. To open Restore Configuration page, click [Maintenance > Restore Configuration](#) from the menu bar. A sample screenshot of Restore Configuration page is shown below.



Restore Configuration

The various fields Restore Configuration page are given below.

Config File : This option is used to select the file which was back up earlier.

Upload : To upload the backup file to restore the backup files.

Restore Factory Defaults

This option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during restore factory default configuration.



Warning

Please note that after entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

To open Restore Factory Defaults page, click [Maintenance > Restore Factory Defaults](#) from the menu bar. A sample screenshot of Restore Factory Defaults Page is shown below.

Restore Factory Defaults

Procedure

1. Click [Preserve Configuration](#) to redirect to **Preserve Configuration** page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click [Restore Factory Defaults](#) to restore the factory defaults of the device firmware.



NOTE

When Restore Factory Defaults action is performed, there might be some log events present after performing restore operation. Those events might be newly generated which can be verified using its timestamp.

4.4.12.7 Expander Update

This page is used to update expander.

To open Expander Update page, click [Maintenance > Expander Update](#) from the menu bar. A sample screenshot of Expander Update page is shown below.

The screenshot shows the 'Expander Update' page with a breadcrumb trail: Home > Maintenance > Expander Update. The page is divided into two main sections: 'Full Update' and 'Partial Update'.

Full Update Section:

- Section title: Full Update
- Form: Select TAR File. A file selection button 'Choose File' is followed by 'No file chosen'.
- Action: A green 'Start full update' button.
- Warning: 'WARNING! Please keep JBOD power ON to make the update effective'.

Partial Update Section:

- Section title: Partial Update
- Form: Available Expander Devices. It includes a dropdown for 'Expander Device ID' and a text field for 'Expander Device Name' containing 'HUB EXP'.
- Table: Current Revision.

Firmware	124E1351
MPG	1330351
SAS Address	0x500000000000272F

Bottom Section:

- Firmware Update:** Select Firmware Image. A file selection button 'Choose File' is followed by 'No file chosen'. A green 'Start firmware update' button is present. A warning message is at the bottom: 'WARNING! Please keep JBOD power ON to make the update effective'.
- MFG Update:** Select MFG File. A file selection button 'Choose File' is followed by 'No file chosen'. A green 'Start MFG update' button is present. A warning message is at the bottom: 'WARNING! Please keep JBOD power ON to make the update effective'.

Expander Update page

Full Update

Use TAR archives for full expander updates.

Full Update:

- Click [Choose File](#) to select firmware TAR file.
- Click [Start full update](#) to update all Expander Firmware

Resetting the image. The sample screenshot of Firmware update is as shown below.

This screenshot shows the 'Expander Update' page during a full update. The 'Full Update' section is active, showing a progress bar at 100% completion. The file selected for the update is 'A7FL3R_4110L_RL_133_146_146.tar'.

Full Update Section:

- Section title: Full Update
- Form: Select TAR File. The file 'A7FL3R_4110L_RL_133_146_146.tar' is selected.
- Progress: A blue progress bar is at 100%.
- Action: A green 'Start full update' button.
- Warning: 'WARNING! Please keep JBOD power ON to make the update effective'.

Partial Update Section:

- Section title: Partial Update
- Form: Available Expander Devices. It includes a dropdown for 'Expander Device ID' and a text field for 'Expander Device Name' containing 'HUB EXP'.
- Table: Current Revision.

Firmware	134E1351
MPG	1330351
SAS Address	0x500000000000272F

Bottom Section:

- Firmware Update:** Select Firmware Image. A file selection button 'Choose File' is followed by 'No file chosen'. A green 'Start firmware update' button is present. A warning message is at the bottom: 'WARNING! Please keep JBOD power ON to make the update effective'.
- MFG Update:** Select MFG File. A file selection button 'Choose File' is followed by 'No file chosen'. A green 'Start MFG update' button is present. A warning message is at the bottom: 'WARNING! Please keep JBOD power ON to make the update effective'.

Partial Update

Current Revision: current expander information includes expander firmware version, MFG version and SAS Address.

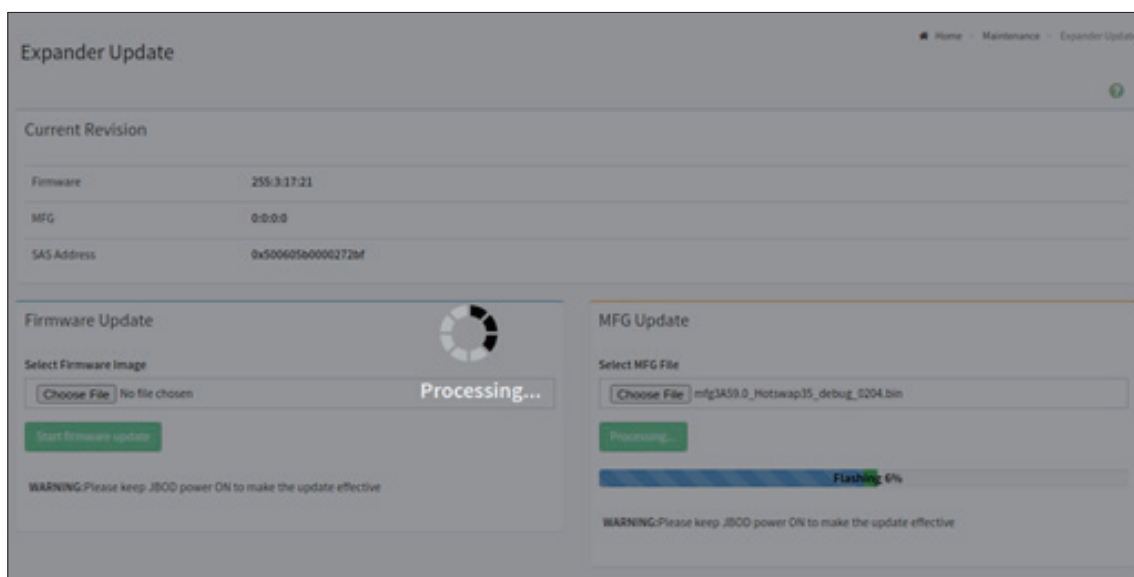
Firmware Update:

- Click [Choose File](#) to select firmware image.
- Click [Start firmware update](#) to update Expander Firmware

MFG Update:

- Click [Choose File](#) to select firmware image.
- Click [Start firmware update](#) to update MFG Firmware.

Resetting the image. The sample screenshot of Firmware update is as shown below.

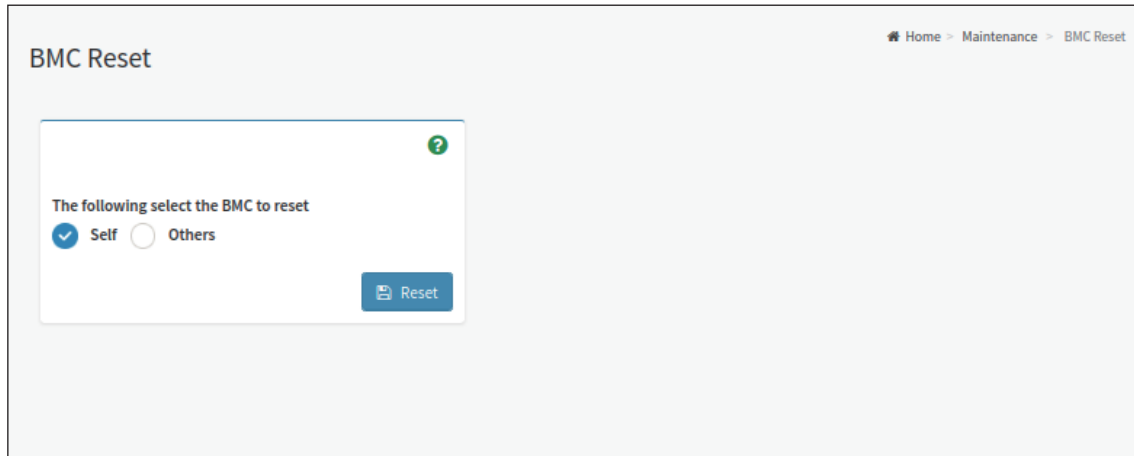


Firmware Update

4.4.12.8 BMC Reset

This page is used to reset BMC.

To open BMC Reset page, click [Maintenance > BMC Reset](#) from the menu bar. A sample screenshot of BMC Reset page is shown below.



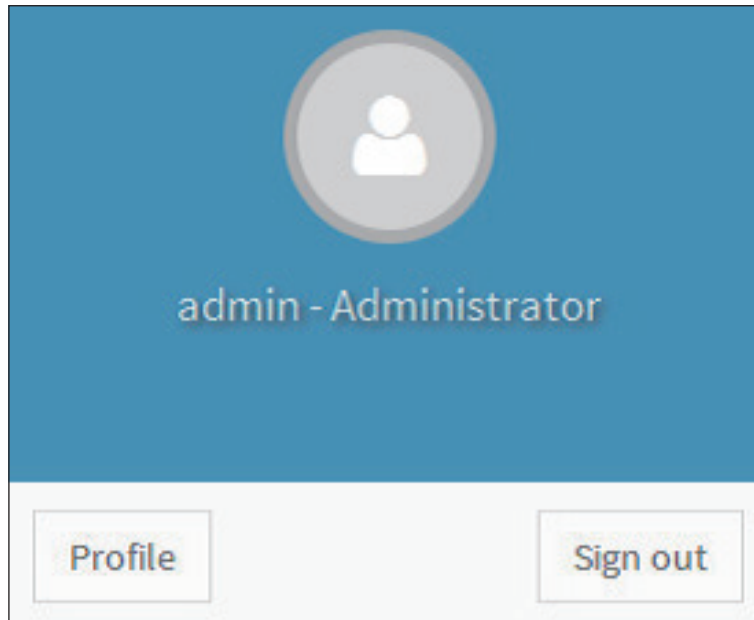
BMC Reset page

Self: activate BMC

Others: other BMC

4.4.13 Sign Out

To log out from the MegaRAC GUI, click the icon (👤) on the top right corner of the screen. A sample screenshot is shown below.

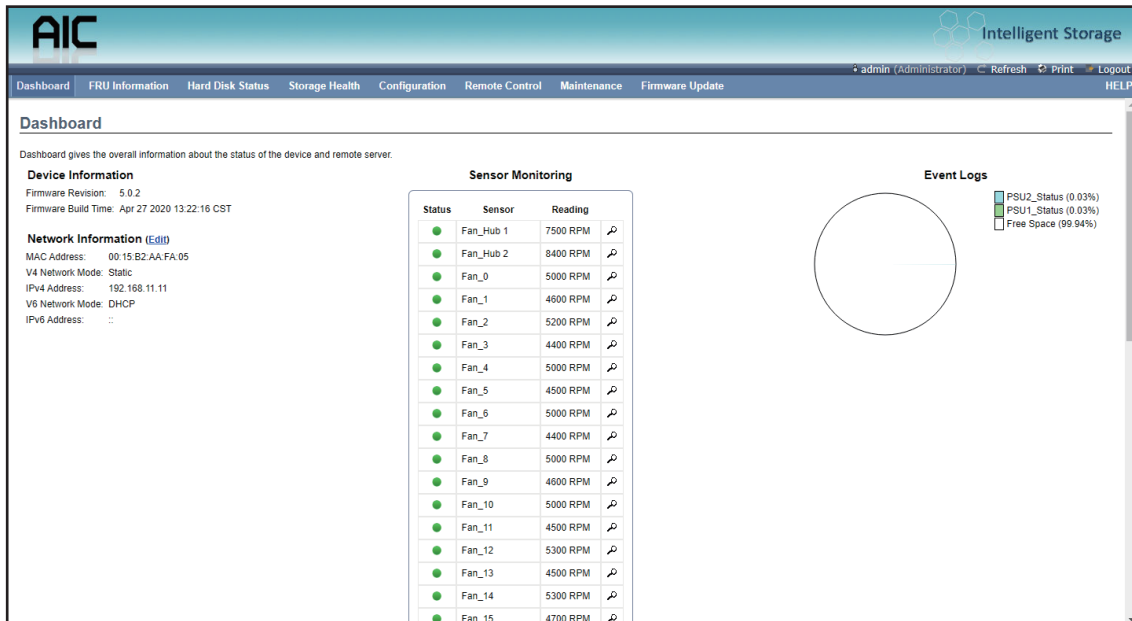


Sign out

Click [Sign Out](#) to perform log out from the MegaRAC GUI. A Warning message will be prompted you to proceed further, click [OK](#) to log out else [Cancel](#) to retain the MegaRAC GUI.

4.5 Web UI for AST1250

4.5.1 Dashboard



Device Information

Displays the Firmware Revision and Firmware Build Time (Date and Time).

Network Information

Shows network settings for the device. Click on the link Edit to view the Network Settings Page.

Sensor Monitoring

It lists all available sensors on the device, with information such as status, name, reading, and status icon, as well as a link to that sensor's page.

There are 3 possible states for a Sensor:

- Green dot denotes a Normal state.
- Yellow exclamation mark denotes a Warning state.
- Red x denotes a Critical state.

The magnifying glass allows access to the Sensor details page for that sensor.

Event Logs

A graphical representation of all events incurred by the various sensors and occupied/available space in logs. If you click on the color-coded rectangle in the Legend for the chart, you can view a list of those specific events only.

4.5.2 FRU information

AIC Intelligent Storage

admin (Administrator) Refresh Print Logout HELP

Field Replaceable Unit(FRU)

This page gives detailed information for the various FRU devices present in this system.

Basic Information:

FRU Device ID: 0

FRU Device Name: BMC_FRU

Chassis Information:

Chassis Information Area Format Version: 1

Chassis Type: Main Server Chassis

Chassis Part Number:

Chassis Serial Number:

Chassis Extra:

Board Information:

Board Information Area Format Version: 1

Language: 0

Manufacture Date Time: Wed Nov 20 17:49:00 2013

Board Manufacturer: ABC

This page displays the BMC FRU file information. On selecting a particular FRU Device ID its corresponding FRU information will be displayed.

Basic Information

It displays the FRU device ID and device name for the selected FRU device ID.

Chassis Information

It displays the following Chassis information fields.

- Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra

Board Information

It displays the following Board information fields.

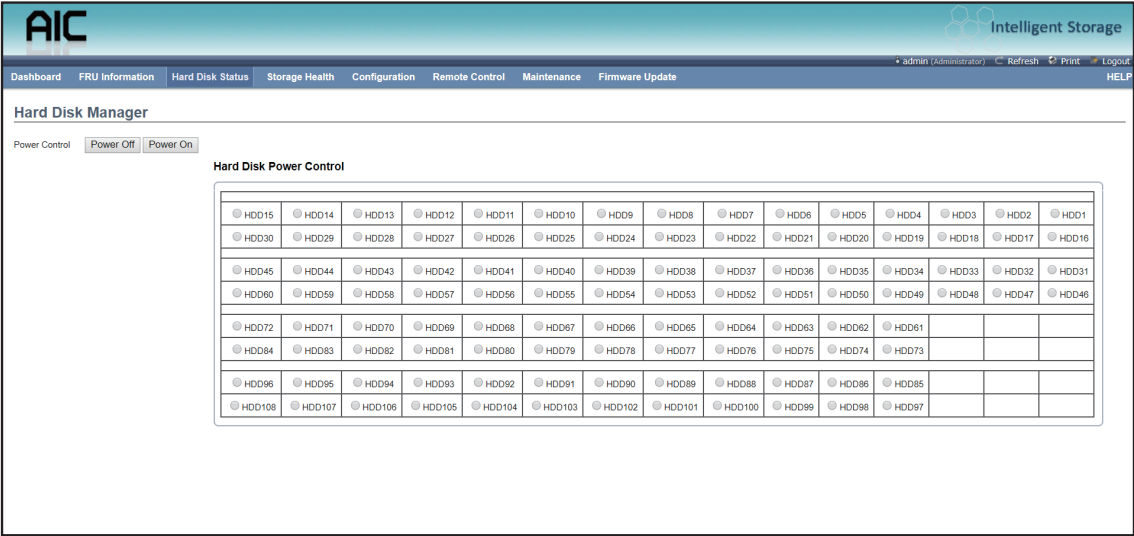
- Area Format Version
- Language
- Manufacture Date Time
- Board Manufacture
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

Product Information

It displays the following Product information fields.

- Area Format Version
- Language
- Manufacturer Name
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

4.5.3 Hard Disk Status



Displays all the HDD power on/off status, user the "Power On" and "Power Off" button to control HDD power.

ACTIONS

Power On

Select a HDD to turn it power on.

Power off

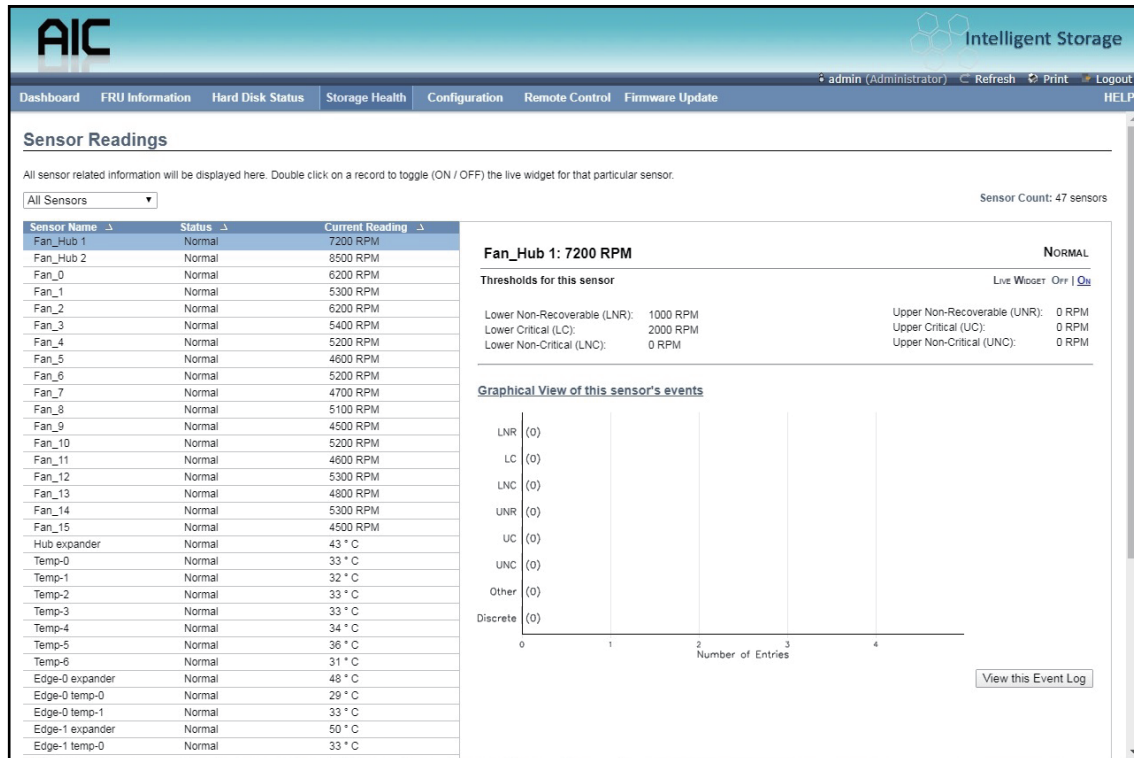
Select a HDD to turn it power off.

Icon status

- Green: This slot inserted HDD and host linked.
- Blue: This slot inserted HDD and host did not link.
- Red: This slot inserted HDD and got fail.
- Gray: This slot not inserted HDD.

4.5.4 Storage Health

4.5.4.1 Sensor Readings



A list of sensor readings will be displayed here. Click on a record to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. Double click on a record to toggle (ON / OFF) the live widget for that particular sensor. You can filter the list to view particular sensors only using the drop-down listbox.

NOTE: N/A represents Not Applicable.

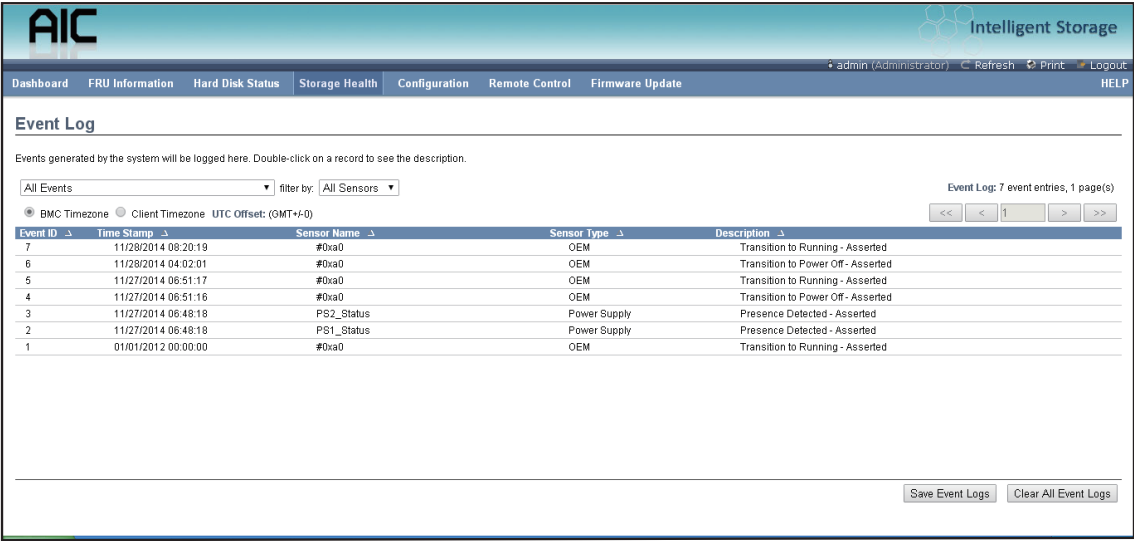
Live Widget

Turn On or Off the live widget for this sensor. This widget gives a dynamic representation of the readings for the sensor.

View this Event Log

Click this button to go the event log page for the viewed sensor.

4.5.4.2 Event Log



AIC Intelligent Storage

admin (Administrator) Refresh Print Logout

Dashboard FRU Information Hard Disk Status **Storage Health** Configuration Remote Control Firmware Update

Event Log

Events generated by the system will be logged here. Double-click on a record to see the description.

All Events filter by: All Sensors Event Log: 7 event entries, 1 page(s)

☒ BMC Timezone ☐ Client Timezone UTC Offset: (GMT+/-0)

Event ID	Time Stamp	Sensor Name	Sensor Type	Description
7	11/28/2014 08:20:19	#0xa0	OEM	Transition to Running - Asserted
6	11/28/2014 04:02:01	#0xa0	OEM	Transition to Power Off - Asserted
5	11/27/2014 08:51:17	#0xa0	OEM	Transition to Running - Asserted
4	11/27/2014 08:51:16	#0xa0	OEM	Transition to Power Off - Asserted
3	11/27/2014 08:48:18	PS2_Status	Power Supply	Presence Detected - Asserted
2	11/27/2014 08:48:18	PS1_Status	Power Supply	Presence Detected - Asserted
1	01/01/2012 00:00:00	#0xa0	OEM	Transition to Running - Asserted

Save Event Logs Clear All Event Logs

This page displays the list of events incurred by different sensors on this device. Double click on a record to see the details of that entry. You can also sort the list of entries by clicking on any of the column headers. You can use the sensor type or sensor name filter options to view those specific events logged in the device.

BMC Timezone

Check this option to display the event log entries logged with the BMC Timezone value.

Client Timezone

Check this option to display the event log entries logged with the Client (user's) Timezone value.

UTC Offset

Displays the current UTC Offset value based on which event Time Stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.

Clear All Event Logs

Clear All Event Logs option will delete all existing records for all sensors.

Save All Event Logs

Save All Event Logs option will save all existing records for all sensors.

4.5.5 Configuration

4.5.5.1 DNS

The screenshot shows the AIC Intelligent Storage web interface. The top navigation bar includes links for Dashboard, FRU Information, Hard Disk Status, Storage Health, Configuration, Remote Control, and Firmware Update. The Configuration tab is active. The main content area is titled 'DNS Server Settings' and contains the following sections:

- Host Configuration:**
 - Host Settings:** A dropdown menu set to 'Automatic'.
 - Host Name:** A text field containing 'AM0015B2A624AA'.
- Register BMC:**
 - eth0:** A checkbox labeled 'Register BMC' is checked. Below it, a radio button labeled 'Direct Dynamic DNS' is selected.
- Domain Name Configuration:**
 - Domain Settings:** A dropdown menu set to 'eth0_v4'.
 - Domain Name:** A text field containing 'iamyourfather'.
- Domain Name Server Configuration:**
 - DNS Server Settings:** A dropdown menu set to 'eth0'.
 - IP Priority:** Two radio buttons, 'IPv4' (selected) and 'IPv6'.
 - DNS Server 1:** A text field containing '192.168.88.1'.
 - DNS Server 2:** An empty text field.
 - DNS Server 3:** An empty text field.

This page is used to configure the Host name and Domain Name Server configuration of the device.

Host configuration

Host Settings

Choose either Automatic or Manual settings.

Host Name

It displays the hostname of the device if Auto is selected. If the Host setting is chosen as Manual, then specify the hostname of the device.

Register BMC

Choose the BMC's network port to register with the DNS settings. Check the option 'Register BMC' to register with the DNS settings. Choose the option 'Direct Dynamic DNS' to register with direct dynamic DNS or choose 'DHCP Client FQDN' to register through a DHCP server.

Domain Name Configuration

Domain Settings

It lists the options for the domain interface as Manual, v4 or v6 for multi LAN channels.

Domain Name

It displays the domain name of the device if Auto is selected. If the Domain setting is chosen as Manual, then specify the domain name of the device.

Domain Name Server Configuration**DNS Server Settings**

It lists the options for the DNS interface, Manual and available LAN interfaces.

IP Priority

If the IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server. If the IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.

NOTE: This is not applicable for Manual configuration.

DNS Server 1, 2 & 3

Specify the DNS (Domain Name System) server address to be configured for the BMC.

- An IPv4 Address is made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each number ranges from 0 to 255.
- The first number must not be 0.

DNS Server Address will support the following:

- IPv4 Address format.
- IPv6 Address format.

Save

Click 'Save' to save any changes made. You will be logged out of current UI session and will need to log back in.

Reset

Reset the modified changes.

4.5.5.2 Network Settings

AIC Intelligent Storage

admin (Administrator) Refresh Print Logout HELP

Dashboard FRU Information Hard Disk Status Storage Health **Configuration** Remote Control Firmware Update

Network Settings

Manage network settings of the device.

LAN Interface eth0

LAN Settings ☒ Enable

MAC Address 00:15:B2:A6:24:AA

IPv4 Configuration

Obtain an IP address automatically ☒ Use DHCP

IPv4 Address 192.168.88.130

Subnet Mask 255.255.255.0

Default Gateway 192.168.88.1

IPv6 Configuration

IPv6 Settings ☐ Enable

Obtain an IP address automatically ☐ Use DHCP

IPv6 Address ::

Subnet Prefix length 0

Default Gateway ::

This page is used to configure the network settings for available LAN channels.

LAN Interface

Select the LAN interface to be configured.

LAN Settings

Check this option to enable LAN support for the selected interface.

MAC Address

This field displays the MAC address of the selected interface (read only).

IPv4 Configuration

It lists the IPv4 configuration settings.

Obtain an IP address automatically.

Enable 'Use DHCP' to dynamically configure the IPv4 address using Dynamic Host Configuration Protocol (DHCP).

IPv4 Address, Subnet Mask, Default Gateway

If DHCP is disabled, specify a static IPv4 address, Subnet Mask and Default Gateway to be configured for the selected interface.

- An IP Address consists of 4 sets of numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each set ranges from 0 to 255.
- The first Number must not be 0.

IPv6 Configuration

It lists the IPv6 configuration settings.

IPv6 Settings

Check this option to enable IPv6 support for the selected interface.

Obtain an IP address automatically

Enable 'Use DHCP' to dynamically configure the IPv4 address using Dynamic Host Configuration Protocol (DHCP).

IPv6 Address

Specify a static IPv6 address to be configured for the selected interface.

Subnet Prefix length

Specify the subnet prefix length for the IPv6 settings.

- Value ranges from 0 to 128.

Default Gateway

Specify the v6 default gateway for IPv6 settings.

Save

Click 'Save' to save any changes made. You will be prompted to log out of the current UI session and log back in at the new IP address.

Reset

Click 'Reset' to reset the modified changes.

4.5.5.3 Network Link

This page is used to configure the network link option for the available network interfaces.

LAN Interface

Select the network interface from the list for which the Link speed and duplex mode are to be configured.

Auto Negotiation

This option is enabled to allow the device to perform automatic configuration to achieve the best possible mode of operation (speed and duplex) over a link.

Link Speed

Link speed will list all the supported capabilities of the network interface. It can be 10/100/1000 Mbps.

Duplex Mode

Select any one of the following Duplex Modes.

- Half Duplex
- Full Duplex

Save

Click 'Save' to save the settings.

Reset

Click 'Reset' to reset the modified changes.

4.5.5.4 NTP

This page displays the device's current Date & Time Settings. It can be used to configure either Date & Time or NTP (Network Time Protocol) server settings for the device.

Date

Specify the current Date for the device.

Time

Specify the current Time for the device.

NOTE: As a year 2038 problem exists, the acceptable date range is from 01-01-2005 to 01-18-2038.

NTP Server

Specify the NTP Server for the device. Check the 'Automatically synchronize' option to configure the NTP Server. The NTP Server will support the following:

- IP Address (Both IPv4 and IPv6 format).
- FQDN (Fully qualified domain name) format.

UTC Offset

UTC Offset list contains the UTC offset values for the NTP server, which can be used to display the exact local time.

NOTE: Use the correct UTC offset after adjusting for DST.

Automatically synchronize

Check this option to automatically synchronize Date and Time with the NTP Server.

Refresh

Click 'Refresh' to reload the current date & time settings.

Save

Click 'Save' to save any changes made.

Reset

Click 'Reset' to reset the modified changes.

4.5.5.5 PEF

AIC Intelligent Storage

admin (Administrator) Refresh Print Logout HELP

PEF Management

Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify an entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add".

Event Filter | Alert Policy | LAN Destination

Configured Event Filter count: 15

PEF ID	Filter Configuration	Event Filter Action	Event Severity	Sensor Name
1	Enabled	[Alert]	Unspecified	Any
2	Enabled	[Alert]	Unspecified	Any
3	Enabled	[Alert]	Unspecified	Any
4	Enabled	[Alert]	Unspecified	Any
5	Enabled	[Alert]	Unspecified	Any
6	Enabled	[Alert]	Unspecified	Any
7	Enabled	[Alert]	Unspecified	Any
8	Enabled	[Alert]	Unspecified	Any
9	Enabled	[Alert]	Unspecified	Any
10	Enabled	[Alert]	Unspecified	Any
11	Enabled	[Alert]	Unspecified	Any
12	Enabled	[Alert]	Unspecified	Any
13	Enabled	[Alert]	Unspecified	Any

Add Modify Delete

This page is used to configure the Event Filter, Alert Policy and LAN Destination. To view the page, the user must at least be an Operator. To modify or add a PEF, the user must be an Administrator.

NOTE: Free slots are denoted by '~' in all columns for the slot. For more information, refer the Platform Event Filtering (PEF) section in IPMI Specification.

Event Filter

Click the Event Filter tab to show configured Event filters and available slots. You can modify or add new event filter entries here. A maximum of 40 slots are available and include the default of 15 event filter configurations.

Alert Policy

Click the Alert policy tab to show configured Alert policies and available slots. You can modify or add new alert policy entries here. A maximum of 60 slots are available.

LAN Destination

Click the LAN Destination tab to show configured LAN destinations and available slots. You can modify or add new LAN destination entries here. A maximum of 15 slots are available

Send Test Alert

Select a configured slot in the LAN Destination tab and click 'Send Test Alert' to send a sample alert to the configured destination.

NOTE: Test alerts can be sent only with SMTP configurations set to enabled. SMTP support can be enabled under Configuration->SMTP.

Add

Select a free slot and click 'Add' to add a new entry to the device. Alternatively, double click on a free slot.

Modify

Select a configured slot and click 'Modify' to modify that entry. Alternatively, double click on the configured slot.

Delete

Select the desired configured slot to be deleted and click 'Delete.'

4.5.5.6 SMTP

This page is used to configure the SMTP settings.

LAN Channel Number

Select the LAN channel to which the SMTP information needs to be configured.

Sender Address

Enter the 'Sender Address' valid on the SMTP Server.

Machine Name

Enter the 'Machine Name' of the SMTP Server.

- Machine Name is a string of maximum 15 alpha-numeric characters.
- Space, special characters are not allowed.

Primary SMTP Server

It lists the Primary SMTP Server configuration.

SMTP Support

Check this option to enable SMTP support for the BMC.

Server Address

Enter the 'IP address' of the SMTP Server. It is a mandatory field.

- An IP Address is made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each Number ranges from 0 to 255.
- The first Number must not be 0.

The server address will support the following:

- IPv4 Address format.
- IPv6 Address format.

SMTP Server requires Authentication

Check the option 'Enable' to enable SMTP Authentication.

Note: SMTP Server Authentication Types supported are:

- CRAM-MD5
- LOGIN
- PLAIN

If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, "Authentication type is not supported by SMTP Server"

Username

Enter the username to access SMTP Accounts.

- The User Name can be 4 to 64 alpha-numeric characters.
- It must start with an alphabet.
- Special characters ';' (comma), ':' (colon), ';' (semicolon), ' ' (space) and '\' (backslash) are not allowed.

Password

Enter the password for the SMTP User Account.

- Passwords must be at least 4 characters long.
- Space is not allowed.

NOTE: This field will not allow more than 64 characters.

Secondary SMTP Server

It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working, then it tries the Secondary SMTP Server configuration.

Save

Click 'Save' to save the new SMTP server configuration.

Reset

Click 'Reset' to reset the modified changes.

4.5.5.7 Schedule Power ON/OFF

The screenshot shows the 'Schedule Power ON/OFF' configuration page in the AIC Intelligent Storage web interface. The page has a navigation bar with links: Dashboard, FRU Information, Hard Disk Status, Storage Health, Configuration, Remote Control, and Firmware Update. The 'Configuration' link is active. The page title is 'Schedule Power ON/OFF'.

Below the title, there is a section for 'Manage the date & time to do power on/off of the device.' with the following fields:

- Date:** January 1 2012
- Time:** 01:25:58
- Timezone:** (dropdown menu)

There are two main sections for scheduling:

Weekly schedule

- ☒ **Enable schedule**
- Action:** ☐ Power on ☒ Power off
- Set days for action:** ☐ Sun ☐ Mon ☒ Tue ☐ Wed ☐ Thu ☒ Fri ☒ Sat
- Time:** 10:51

Specific days schedule

- ☐ **Enable schedule**
- Action:** ☐ Power on ☒ Power off
- Date:** January 16
- Time:** 8:50
- ☐ **Enable schedule**
- Action:** ☐ Power on ☒ Power off
- Date:** August 13
- Time:** 4:30

At the bottom right, there are 'Save' and 'Reset' buttons.

This page displays the device's current date & time. It can be used to configure dates within a week or specific a date to power on/off the device.

If you want to change the device date & time, please go to the NTP page.

ACTIONS

Enable schedule

Check this option for enable/disable the schedule.

Action

Check a action to do power on/off for the device.

Set days for action

Setting dates within a week to do power on/off for the device.

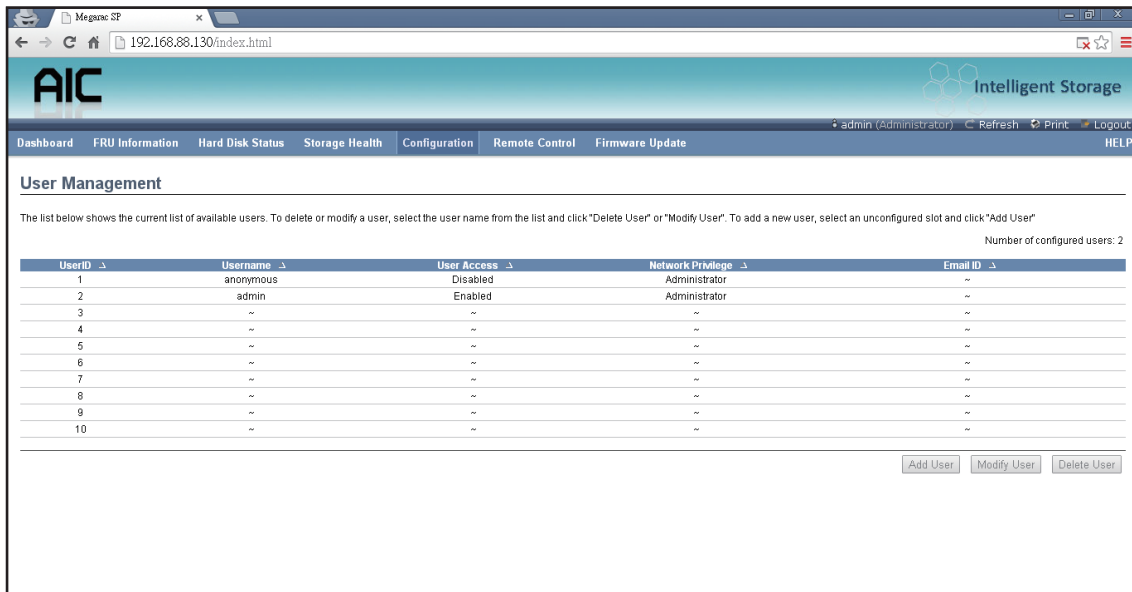
Date

Specify a date for the device.

Time

Specify a time for the device.

4.5.5.8 User



The displayed table shows any configured Users and available slots. You can modify or add new users from here. A maximum of 10 slots are available, including the default admin and anonymous. It is advised that the anonymous user's privilege and password should be modified as a security measure. To view the page, you must have Operator privileges. To modify or add a user, You must have Administrator privileges.

NOTE: Free slots are denoted by "~" in all columns for the slot.

Add User

Select a free slot and click 'Add User' to add a new user to the device. Alternatively, double click on a free slot to add a user.

Modify User

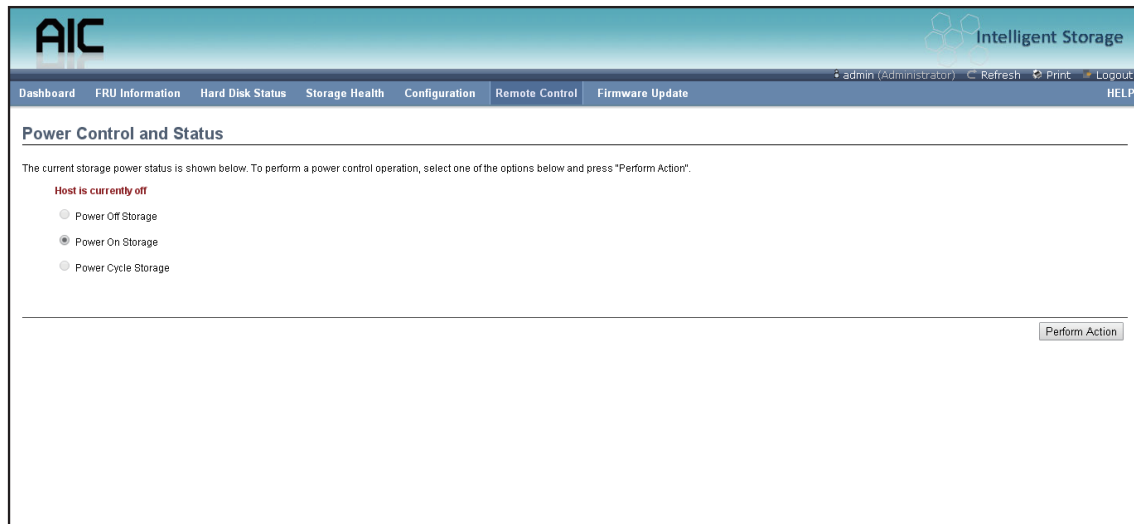
Select a configured slot and click 'Modify User' to modify that user. Alternatively, double click on the configured slot.

Delete User

Select the desired user to be deleted and click 'Delete User'

4.5.6 Remote Control

4.5.6.1 Storage power control



This page helps you to view or perform any host power cycle operations.

Power Off Storage

Select this option to immediately power off the storage.

Power On Storage

Select this option to power on the storage.

Power Cycle Storage

Select this option to first power off, and then reboot the system (cold boot).

Perform Action

Click 'Perform Action' to perform the selected option.

4.5.6.2 Zone Setting

AIC Intelligent Storage

admin (Administrator) Refresh Print Logout HELP

Dashboard FRU Information Hard Disk Status Storage Health Configuration Remote Control Maintenance Firmware Update

ZONE Settings

Here you can configure the zone setting.

Set zone value 1 Set

Expander Zone Check expander_Hub Refresh status

Zone Count 1

You can setup and check zone count setting in the page.

Set zone value

You can set a zone count value and press the SET button. BMC will setup all the hub and edge expander.

Refresh status

Select an expander location and press refresh for the zone count status to display.

Zone Count

This shows the current zone count value.

NOTE

Follow the steps below to configure your zone count:



1. Set the zone count via BMC Web GUI.
2. Re-read and confirm the zone count on each expander after the zone count is set.
3. Power cycle the JBOD in order for the zone count to take effect.

Below command is for ipmitool use.

GET ZONE COUNT*NetFN 36**Command Code: 52h*

Message	Byte	Data Field
Request	1	Expander select 01h: Hub 02h: Edge_0 03h: Edge_1 04h: Edge_2 05h: Edge_3
Response	1	Completion Code 00h Success
	2	zone count value

```
#ipmitool -I lanplus -H <BMC IP> -U admin -P admin raw 0x36 0x52 0x1
```

SET ZONE COUNT*NetFN 36**Command Code: 53h*

Message	Byte	Data Field
Request	1	Expander select 00h: Set all expander 01h: Hub 02h: Edge_0 03h: Edge_1 04h: Edge_2 05h: Edge_3
	2	zone count value
Response	1	Completion Code 00h Success CCh Invalid value data

```
#ipmitool -I lanplus -H <BMC IP> -U admin -P admin raw 0x36 0x53 0x0 0x1
```

4.5.7 Maintenance Control

4.5.7.1 Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without overwriting with defaults/ Firmware Upgrade configuration.

To open Preserve Configuration page, click Maintenance Group > Preserve Configuration from the menu bar. A sample screenshot of Preserve Configuration page is shown below.



NOTE

You can navigate to the Firmware Update Page and Restore Factory Defaults by clicking the respective links.

#	Preserve Configuration Item	Preserve Status
1	Authentication	☐
2	KVM	☐
3	SNMP	☐
4	SEL	☐
5	FRU	☐
6	Network	☐
7	NTP	☐
8	IPMI	☐
9	SSH	☐
10	SDR	☐

Number of Preserved Items: 0

Check All Uncheck All Save Reset

Preserve Status

To check/uncheck a check box to preserve/overwrite the configuration for your system.

Check All

To check the entire configuration list.

Uncheck All

To uncheck the entire configuration list.

Save

To save any changes made.



NOTE

This configuration is used by Restore Factory Defaults process.

Reset

To reset the modified changes.

The preserved files for dependency configurations are listed below as follows.



NOTE

Dependency configuration designates that the option you choose to select may have a subordinate option for you to configure in order for the system to function.

For example, when you select "**SEL**," you must also select "**IPMI**" for the system to operate.

SDR

The sensor data record information that is used in IPMI.

No Dependency

FRU

The logical field replaceable unit data that are used by IPMI.

Dependency Configurations: SDR

SEL

The system event logs that are being logged by the IPMI. Following files will be preserved when Delete SEL reclaim space is enabled.

Dependency Configurations: IPMI

IPMI

The keys that are used to decrypt the passwords. When the user password option is enabled in the MDS project configuration, this file will be preserved.

No Dependency

Network

Configure the channel ID, package ID for the NCSI interface.

Configure the link speed, duplex and MTU value for the specified interface.

Store the pre IPv4 address.

Dependency Configurations: IPMI

NTP

The correct time zone in the system time zone directly.

Dependency Configurations: IPMI

SNMP

The SNMP users privilege levels such as ro user and rw user.

No Dependency

SSH

The public parts of the host keys.

No Dependency

KVM & VMedia

The image name and the remote machine information like IP address, user name, password, domain name and share type.

No Dependency

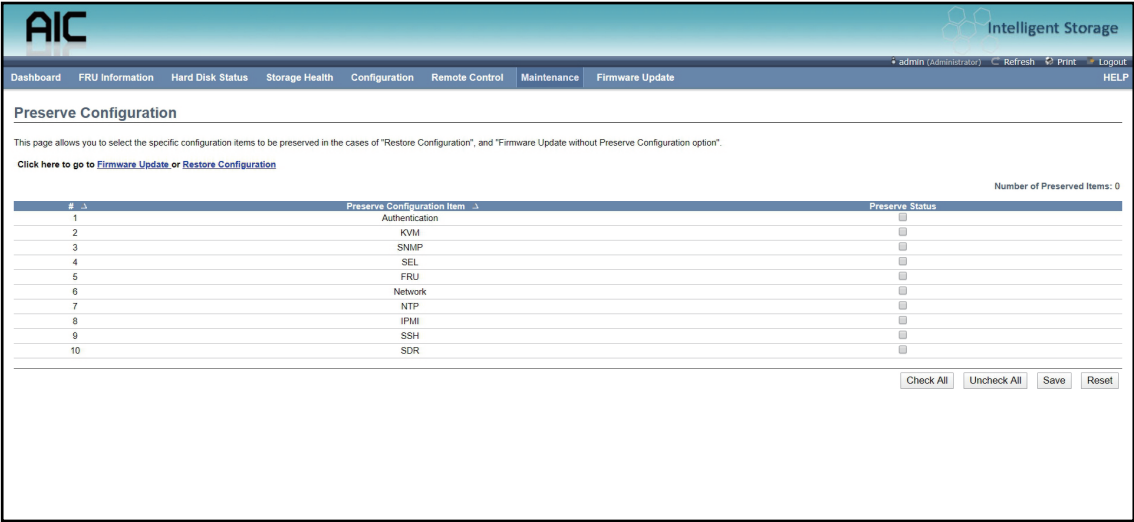
Authentication

The radius server IP address, port number, secret, timeout, privilege etc.

No Dependency

To Preserve your changes:

- 1. Select the required Preserve Configuration items by either selecting the items individually by ticking the check boxes or by selecting all or none using **Check All** or **Uncheck All** buttons respectively.



2. Click **Save** to save the changes.

AIC Intelligent Storage

admin (Administrator) Refresh Print Logout HELP

Dashboard FRU Information Hard Disk Status Storage Health Configuration Remote Control Maintenance Firmware Update

Preserve Configuration

This page allows you to select the specific configuration items to be preserved in the cases of "Restore Configuration", and "Firmware Update without Preserve Configuration option".

Click here to go to [Firmware Update or Restore Configuration](#)

Number of Preserved Items: 0

#	Preserve Configuration Item	Preserve Status
1	Authentication	☐
2	KVM	☐
3	SNMP	☐
4	SEL	☐
5	FRU	☐
6	Network	☐
7	NTP	☐
8	IPMI	☐
9	SSH	☐
10	SDR	☐

Check All Uncheck All **Save** Reset

3. The pop up screen "Preserve configuration settings have been saved successfully" appears. Click **OK** to complete.

AIC Intelligent Storage

admin (Administrator) Refresh Print Logout HELP

Dashboard FRU Information Hard Disk Status Storage Health Configuration

Preserve Configuration

192.168.22.65 顯示
Preserve configuration settings have been saved successfully.

REQUESTING

Number of Preserved Items: 0

#	Preserve Configuration Item	Preserve Status
1	Authentication	☒
2	KVM	☒
3	SNMP	☒
4	SEL	☒
5	FRU	☒
6	Network	☒
7	NTP	☒
8	IPMI	☒
9	SSH	☒
10	SDR	☒

Check All Uncheck All **Save** Reset

4.5.7.2 Restore Configuration

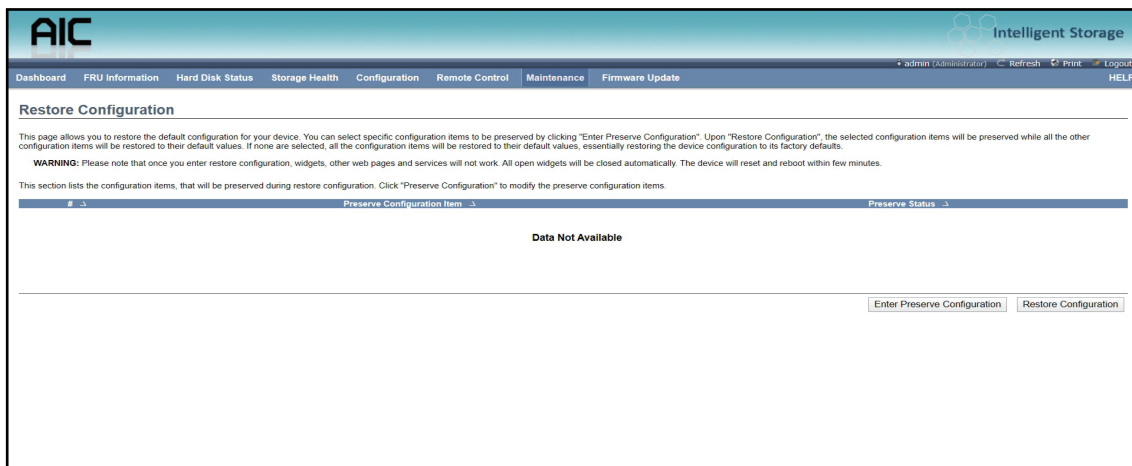
This option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during restore factory default configuration.

NOTE



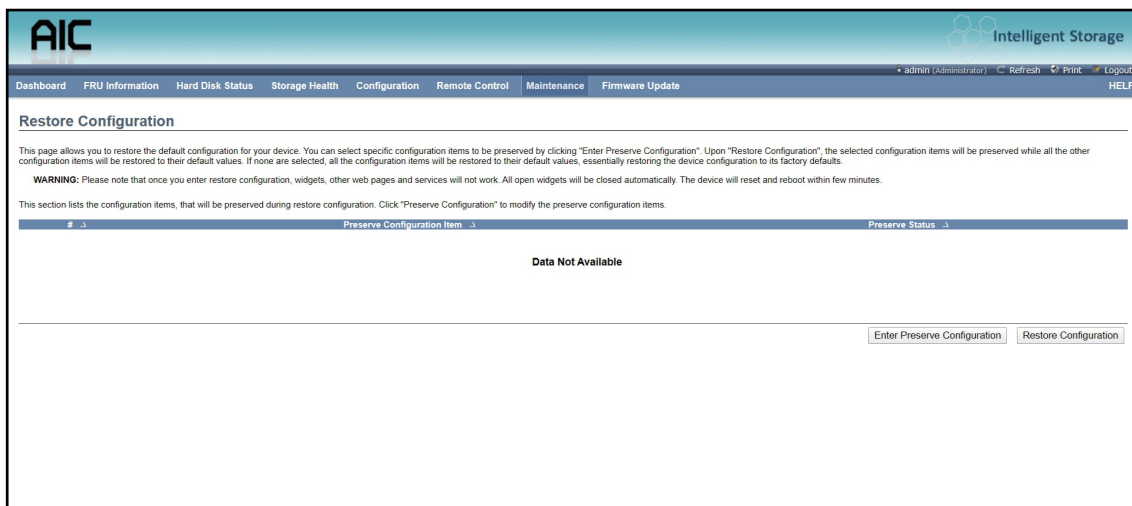
Please note that after entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

To open Restore Factory Defaults page, click Maintenance > Restore Factory Defaults from the menu bar. A sample screenshot of Restore Factory Defaults Page is shown below.

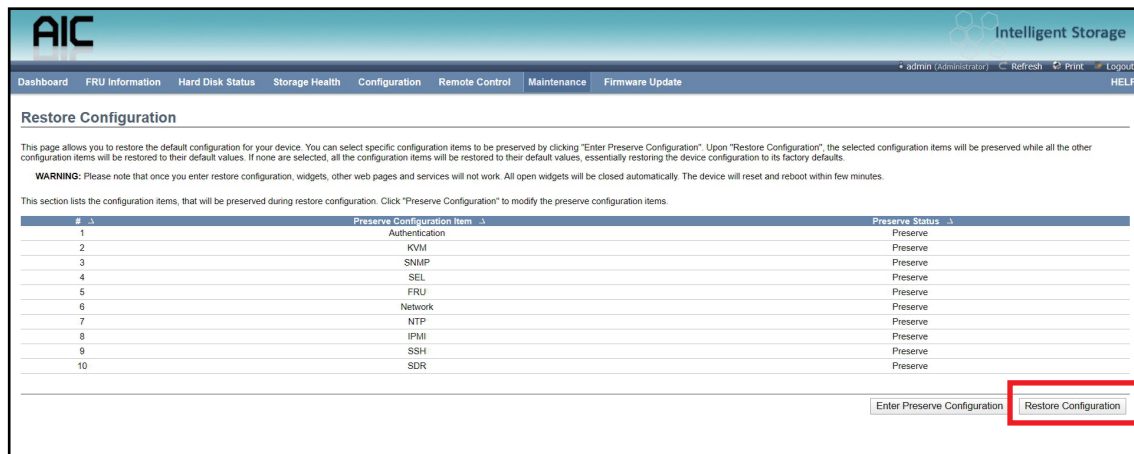


To restore your configuration:

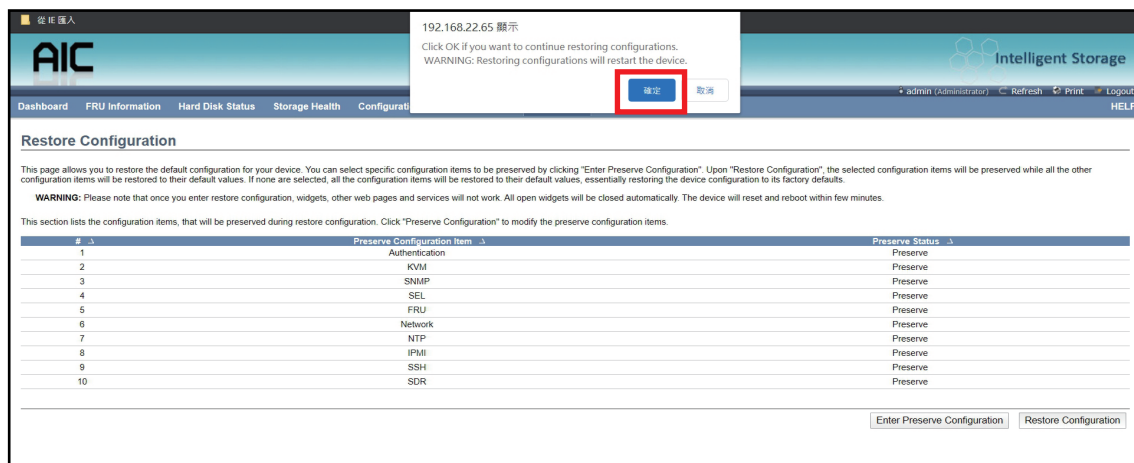
1. Click **Enter Preserve Configuration** to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.



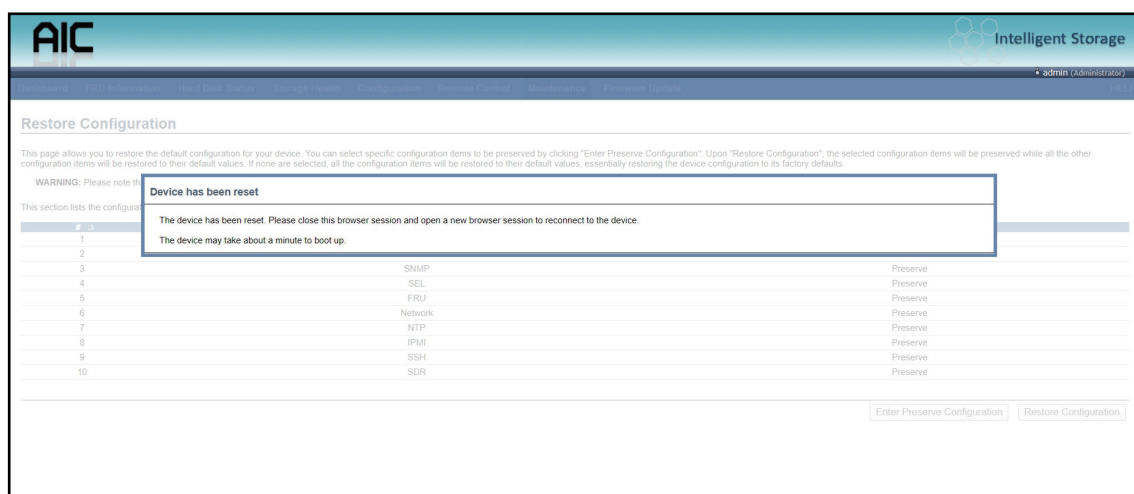
2. Click **Restore Configuration** to restore the factory defaults of the device firmware.



3. Click **OK** to confirm.



4. The factory defaults of the device has been reset.



4.5.8 BMC Firmware Update

4.5.8.1 Requirement

Browsers: FireFox 24.0 or later version

Chrome 35.0 or later version

I.E. 7.0 or later version

Linux: Redhat 6.4

If you want to update a new version firmware for BMC, when finished all the update process, please clear the web browser cookies.

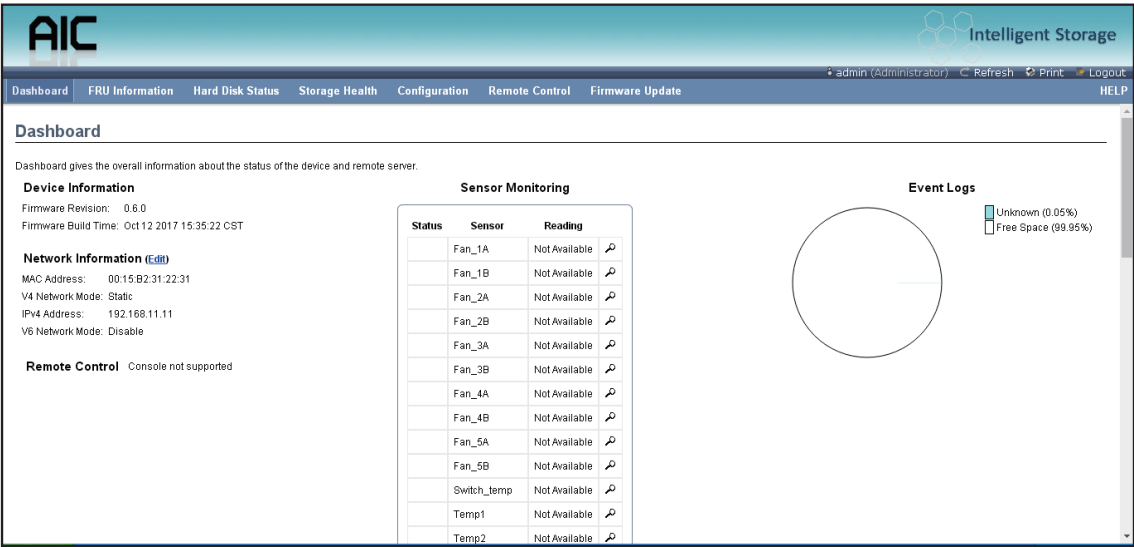
4.5.8.2 Web update

1. Check if the BMC IP is valid.
2. Open a browser and type in the BMC IP. It will show the BMC web UI. Type in the default account or use the administrator privileged account.

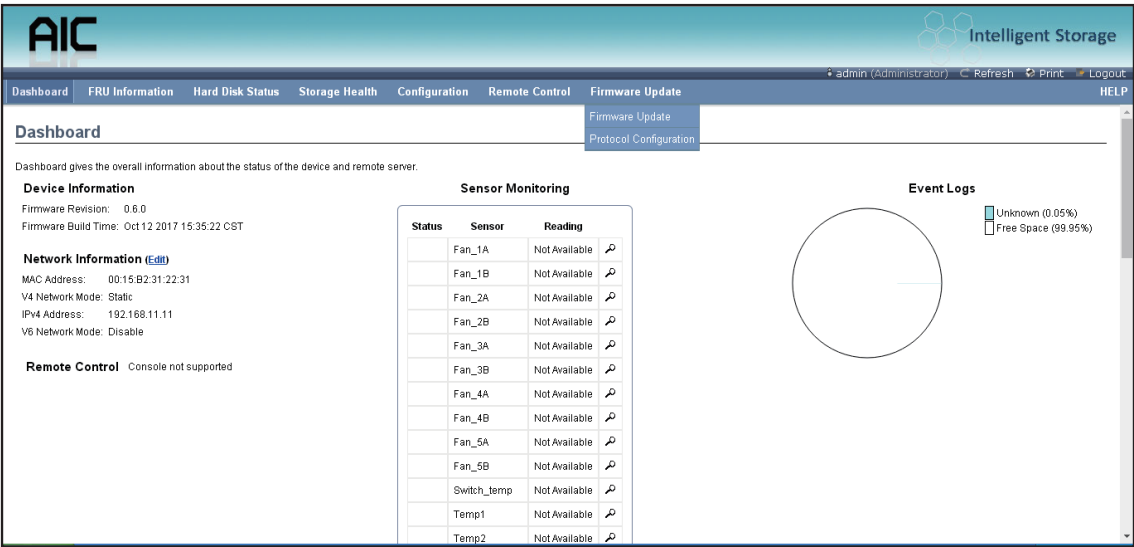
Username: admin

Password: admin

3. This is login main page.



4. Click the “Firmware Update” and it will pop a drop-down menu. Click the “Firmware Update.”



- If you need to preserve all the configurations settings during the expander update process including during the IP address, user account password and ect, click "Preserve all Configuration" and then click "Enter Update Mode." If you do not need to preserve all configurations, click "Enter Update Mode" to proceed to the next step.

Firmware Update

Upgrade firmware of the device. Press "Enter Update Mode" to put the device in update mode.

The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose "Protocol Configuration" under Firmware Update menu.
Protocol Type : HTTP/HTTPS

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.

☒ **Preserve all Configuration** This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.
 All configuration items below will be preserved as default during the restore configuration operation. Click "Enter Preserve Configuration" to modify the Preserve status settings.

#	Preserve Configuration Item	Preserve Status
1	Authentication	Overwrite
2	KVM	Overwrite
3	SNMP	Overwrite
4	SEL	Overwrite
5	FRU	Overwrite
6	Network	Overwrite
7	NTP	Overwrite
8	IPMI	Overwrite
9	SSH	Overwrite
10	SDR	Overwrite

Enter Preserve Configuration Enter Update Mode

- Click "Ok" to continue update.

Firmware Update

Upgrade firmware of the device. Press "Enter Update Mode" to put the device in update mode.

The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose "Protocol Configuration" under Firmware Update menu.
Protocol Type : HTTP/HTTPS

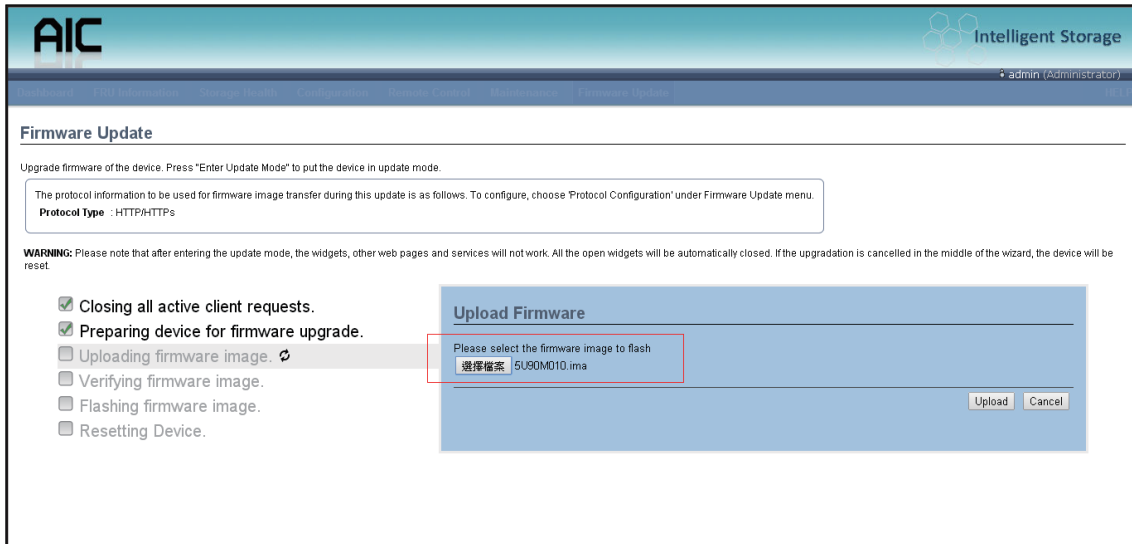
WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.

☒ **Preserve all Configuration** This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.
 All configuration items below will be preserved as default during the restore configuration operation. Click "Enter Preserve Configuration" to modify the Preserve status settings.

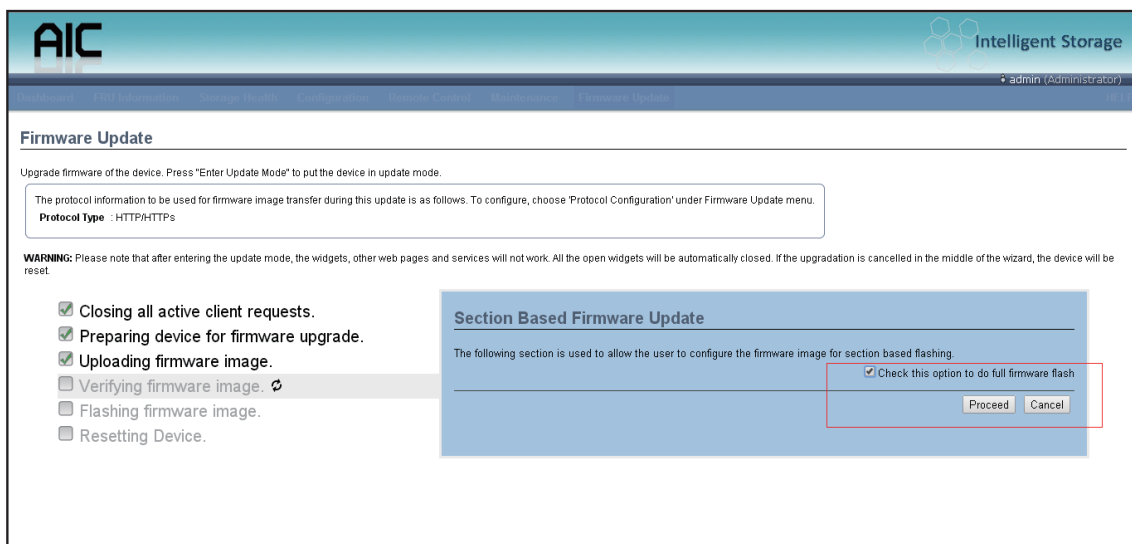
#	Preserve Configuration Item	Preserve Status
1	Authentication	Overwrite
2	KVM	Overwrite
3	SNMP	Overwrite
4	SEL	Overwrite
5	FRU	Overwrite
6	Network	Overwrite
7	NTP	Overwrite
8	IPMI	Overwrite
9	SSH	Overwrite
10	SDR	Overwrite

Enter Preserve Configuration Enter Update Mode

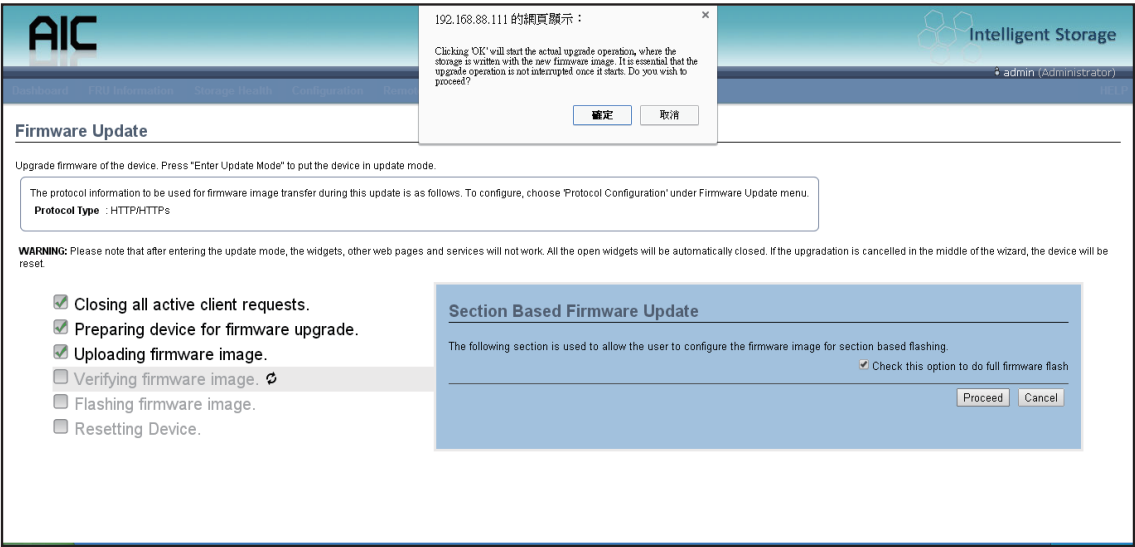
- Wait few minutes and it will pop a window. Click the “Select file” to upload firmware file that you want update.



- Wait a minutes and it will pop a window for check update section. Check the “Check this option to do all full firmware flash” option.



9. Click “OK” and the firmware will start the update process.

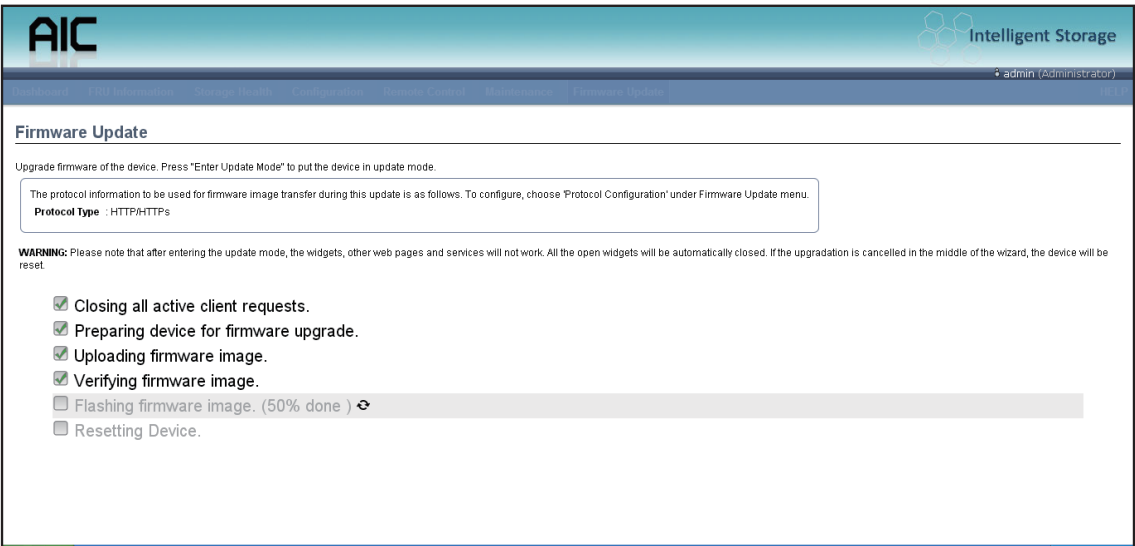


10. In the update process, it will take 3~5 minutes.

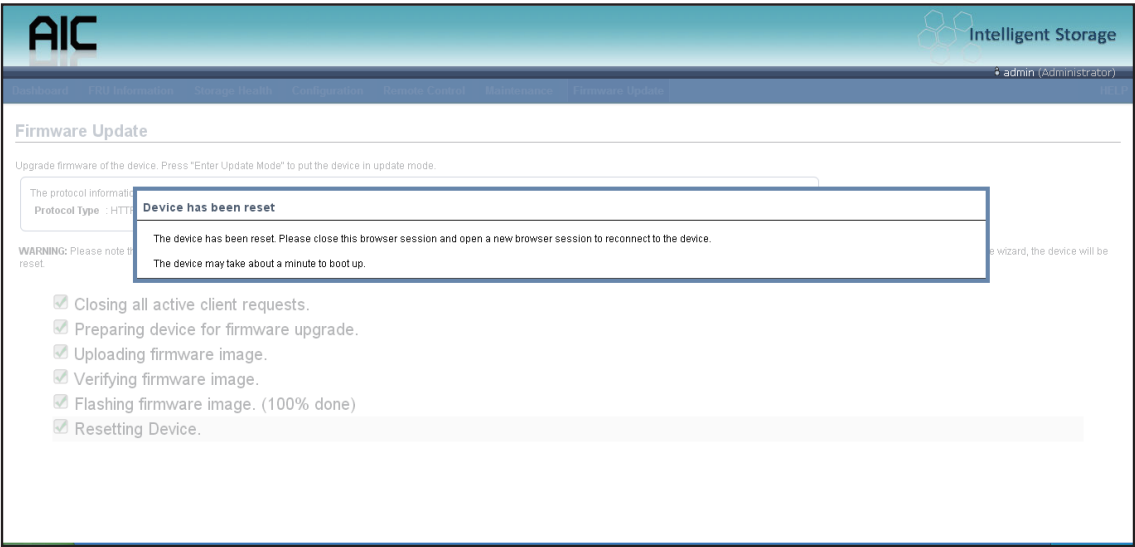


NOTE

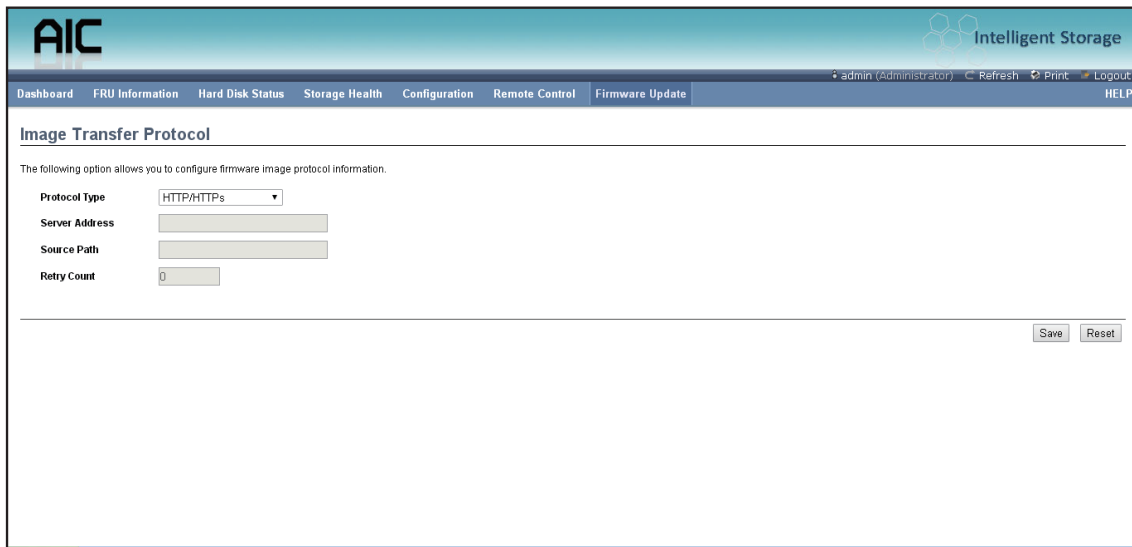
Please do not close this web page! Closing the web page may cause firmware to crash.



11. When “Device has been reset” window appears, it means the firmware update is successful. Wait 90 seconds for the BMC to restart.



4.5.8.3 Image Transfer Protocol



The screenshot shows the AIC Intelligent Storage web interface. The top navigation bar includes links for Dashboard, FRU Information, Hard Disk Status, Storage Health, Configuration, Remote Control, Firmware Update, and a user menu for 'admin (Administrator)' with options for Refresh, Print, and Logout. The main content area is titled 'Image Transfer Protocol' and contains a sub-header 'The following option allows you to configure firmware image protocol information.' Below this, there are four configuration fields: 'Protocol Type' (a dropdown menu currently showing 'HTTP/HTTPS'), 'Server Address' (a text input field), 'Source Path' (a text input field), and 'Retry Count' (a text input field currently showing '0'). At the bottom right of the form are 'Save' and 'Reset' buttons.

This page is used to configure the firmware image protocol information.

ACTIONS

Protocol Type

Protocol to be used to transfer the firmware image into the BMC.

Server Address

Address of the server where the firmware image is stored.

IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".

Each number ranges from 0 to 255.

First number must not be 0.

Source Path

Full Source path (including image filename) to its location on server.

Retry Count

Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.

Save

Click 'Save' to save the configured settings.

Reset

Click 'Reset' to reset the modified changes.

4.5.9 Expander Firmware/MFG Update

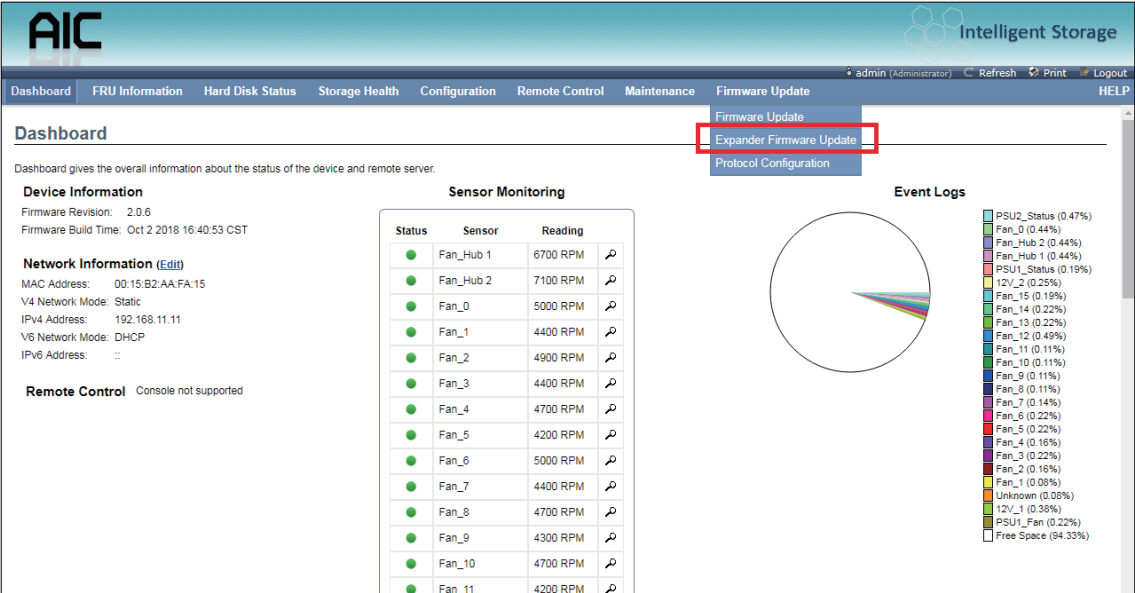


For systems with dual expander modules, please repeat the following steps below to successfully operate both primary and secondary expander.

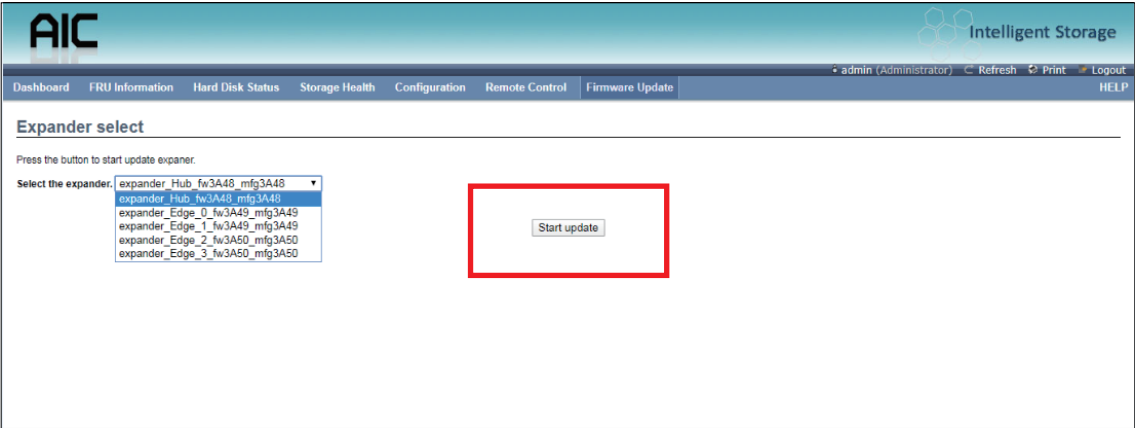


NOTE
Support browser:
Chrome with incognito mode.

1. Click **Firmware Update > Expander Firmware Update** in your BMC menu bar.



2. Under "Select the expander," choose an expander and click **Start update**.



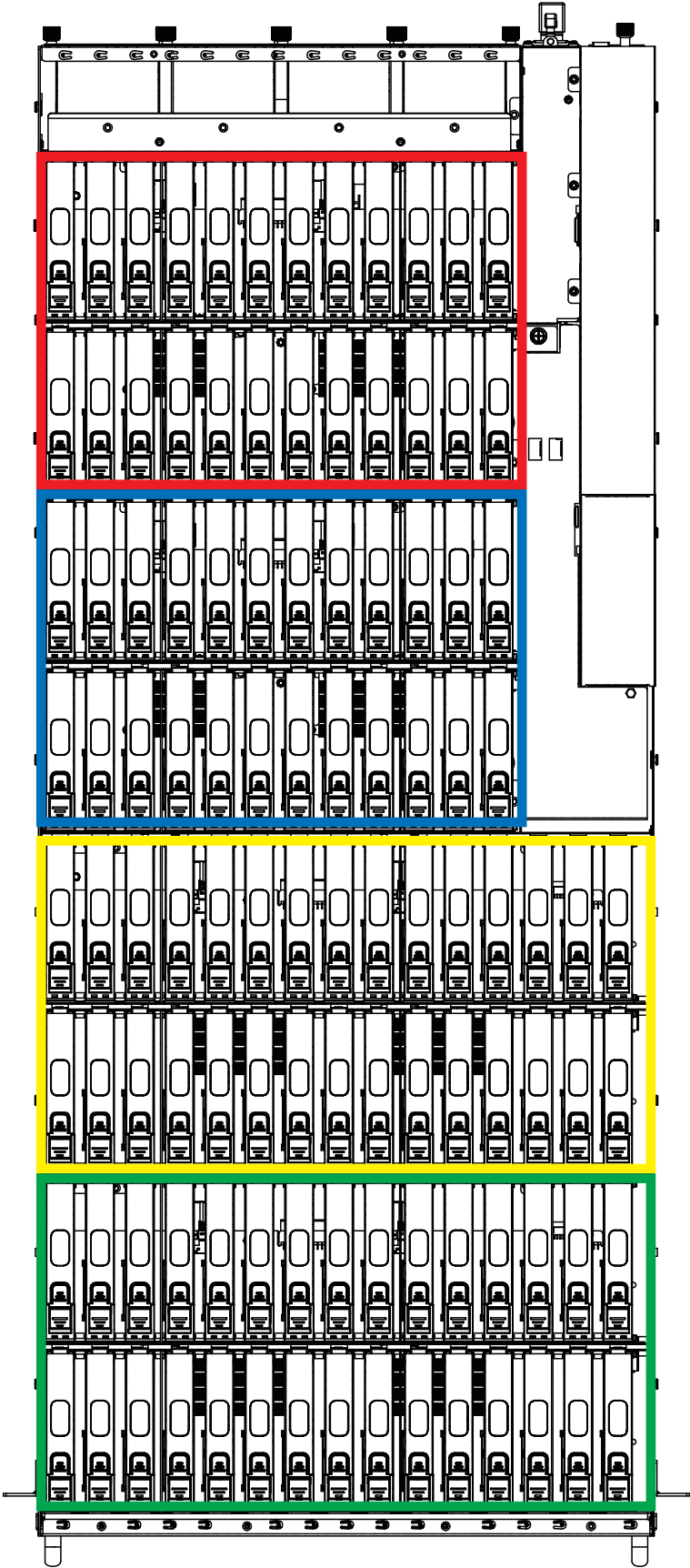
Edge 0, Edge 1, Edge 2, Edge 3 Top View Location

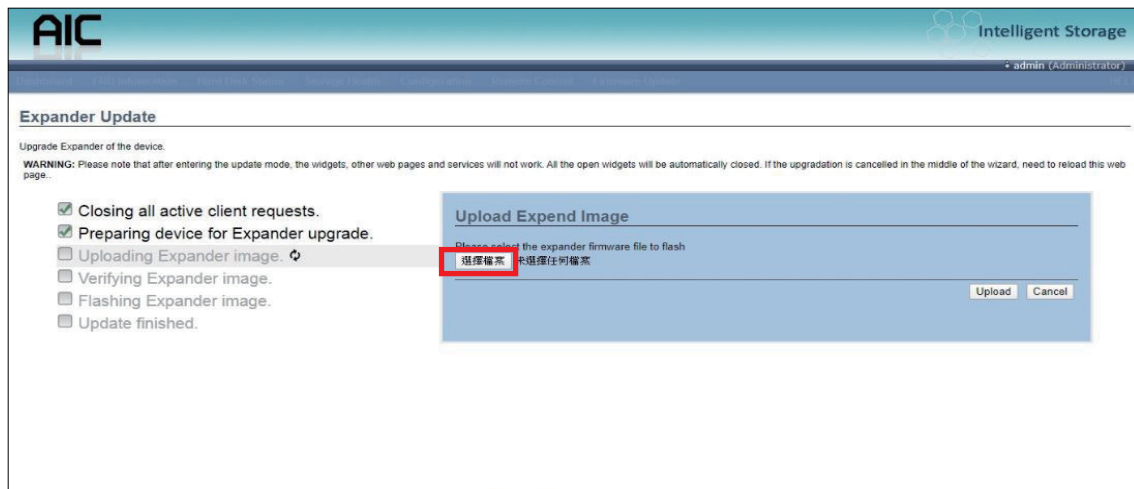
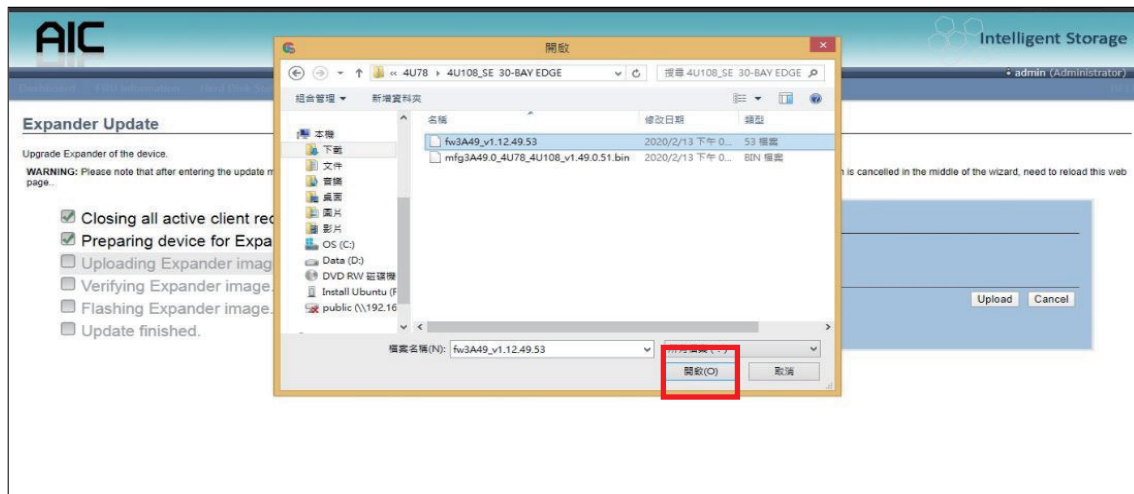
Edge 3

Edge 2

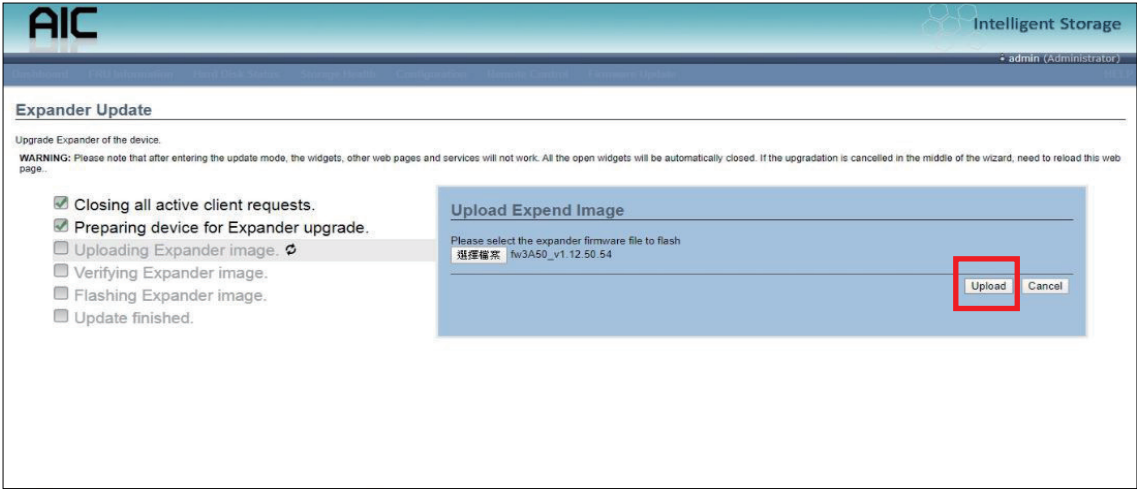
Edge 1

Edge 0



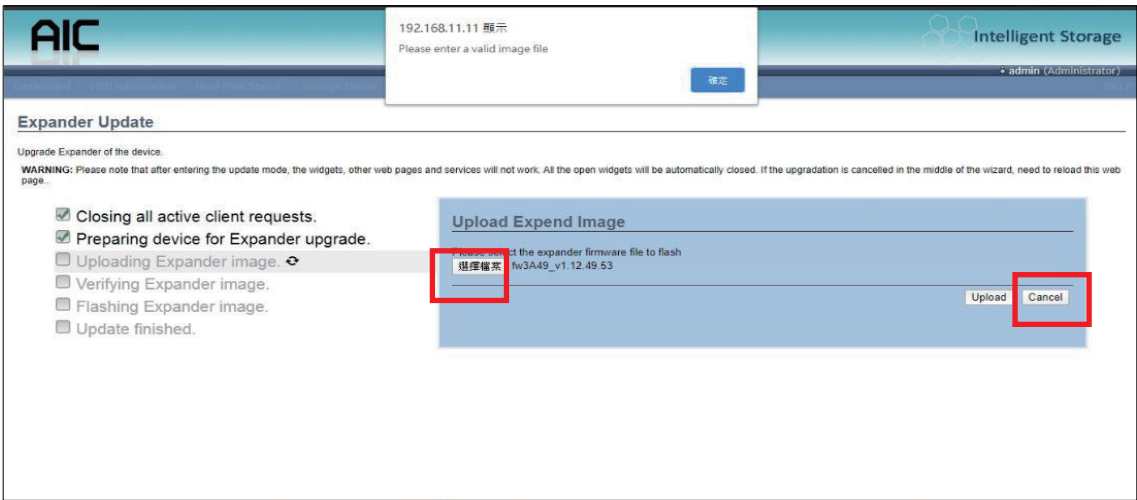
3. Click **Choose File**.4. Select your expander image and click **Open**.

4. Click **Upload**.

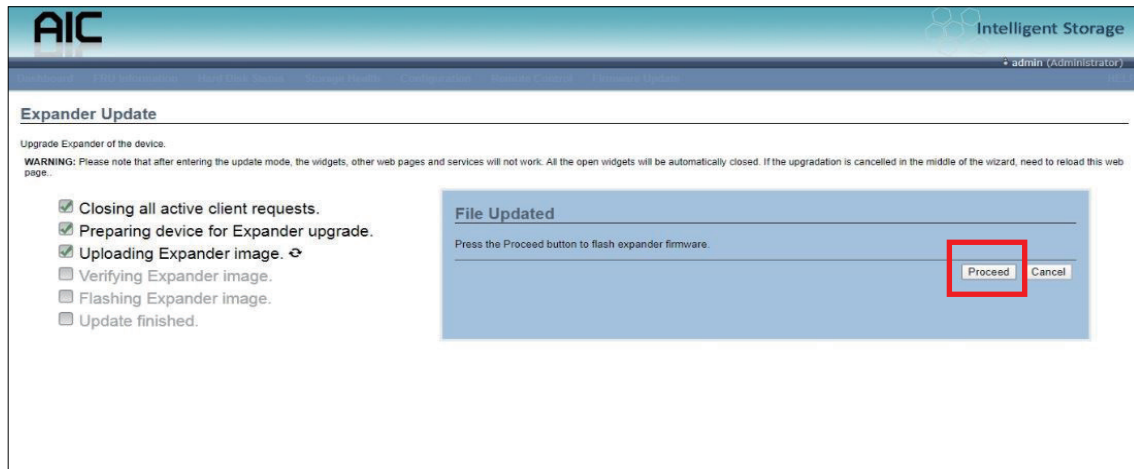


NOTE

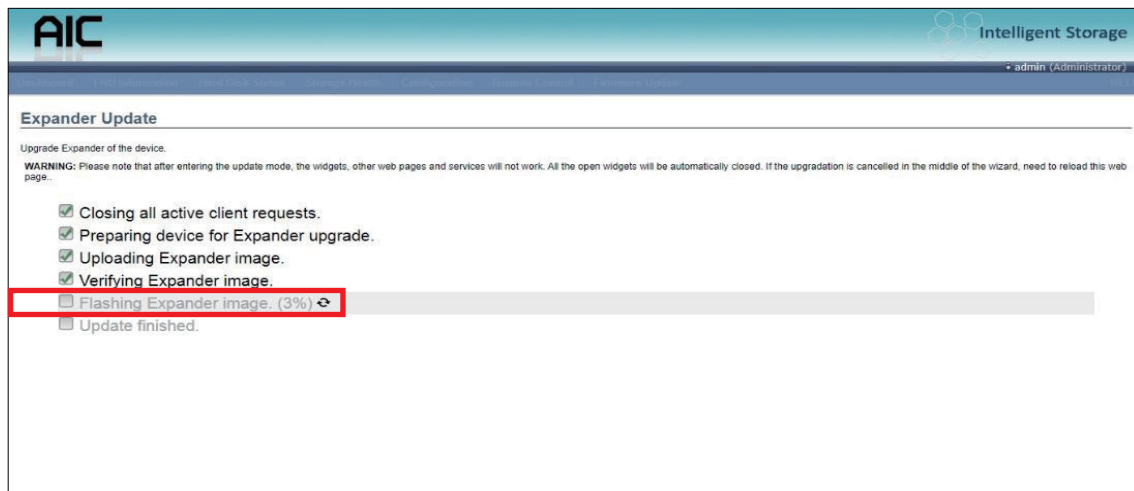
If an error message appears after you clicked upload, please reselect an expander image or press **Cancel**.



5. Under "File Updated," click **Proceed**.



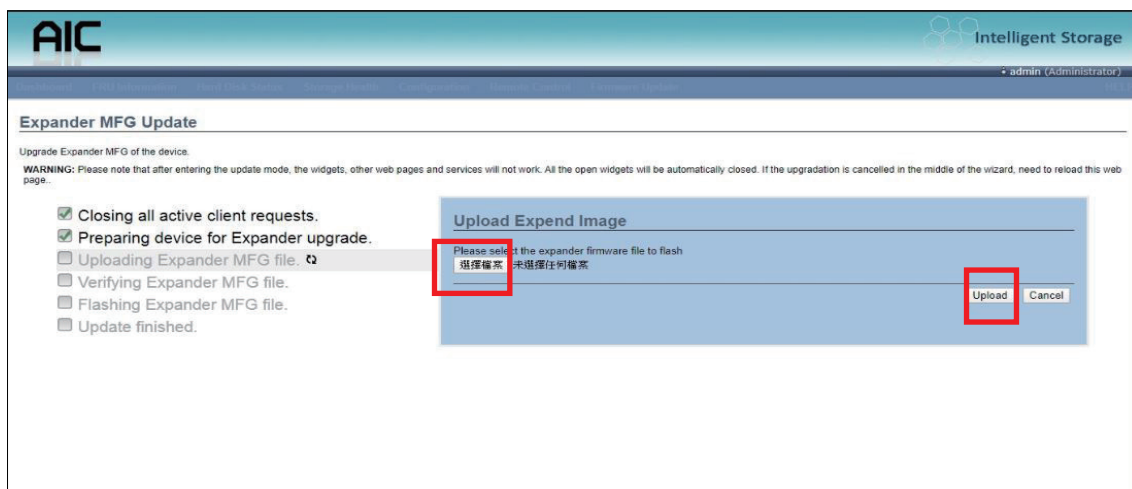
6. Wait a few seconds for the system to confirm that expander image upload is complete.



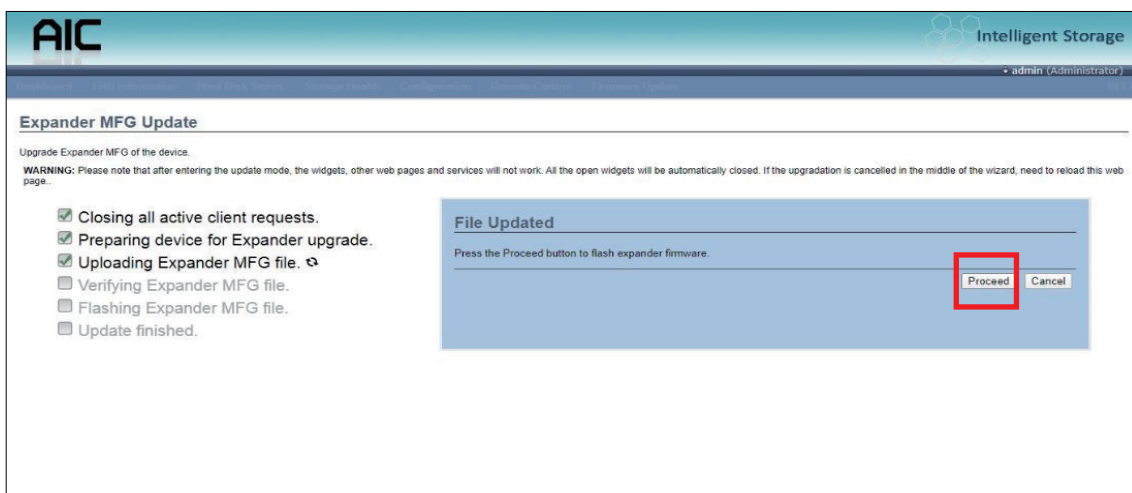
**NOTE**

For steps 7 and 8, do not wait for more than 5 minutes to process. After 5 minutes, the system will fail to update the expander.

- The screen automatically jumps to Expander MFG Update page after FW expander image has been updated. Under "Upload Expander image," select a MFG image and click **Upload**.



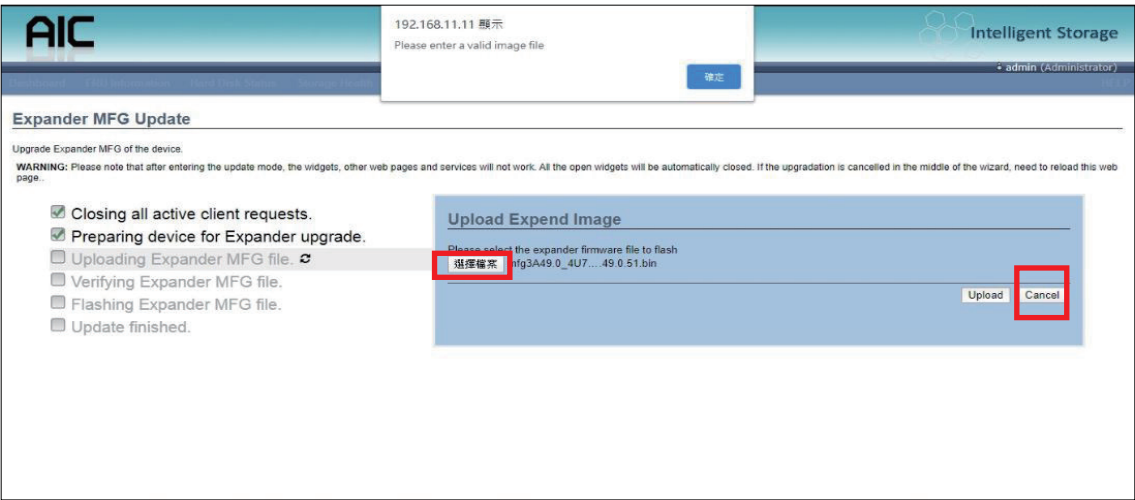
- Under "File Updated," click **Proceed** to continue.



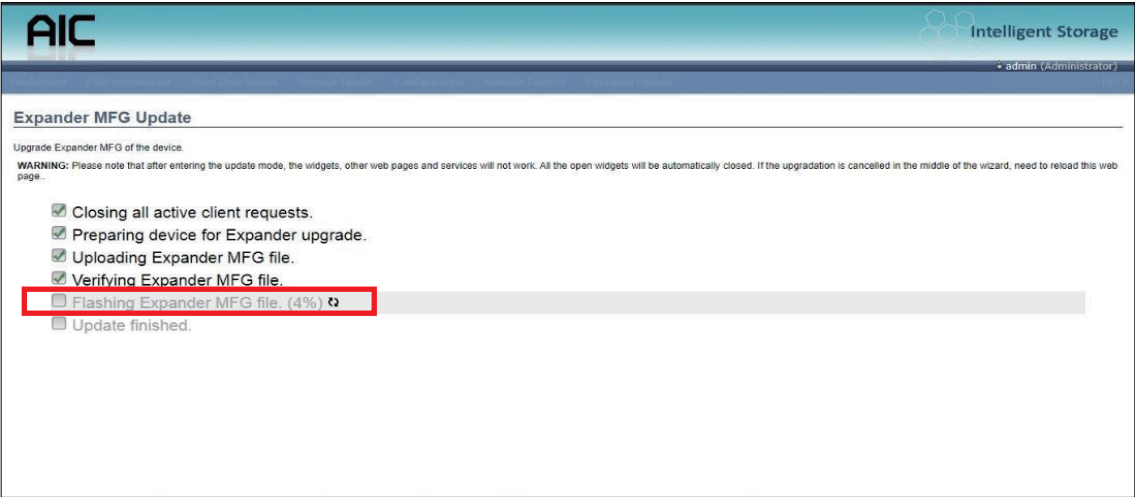


NOTE

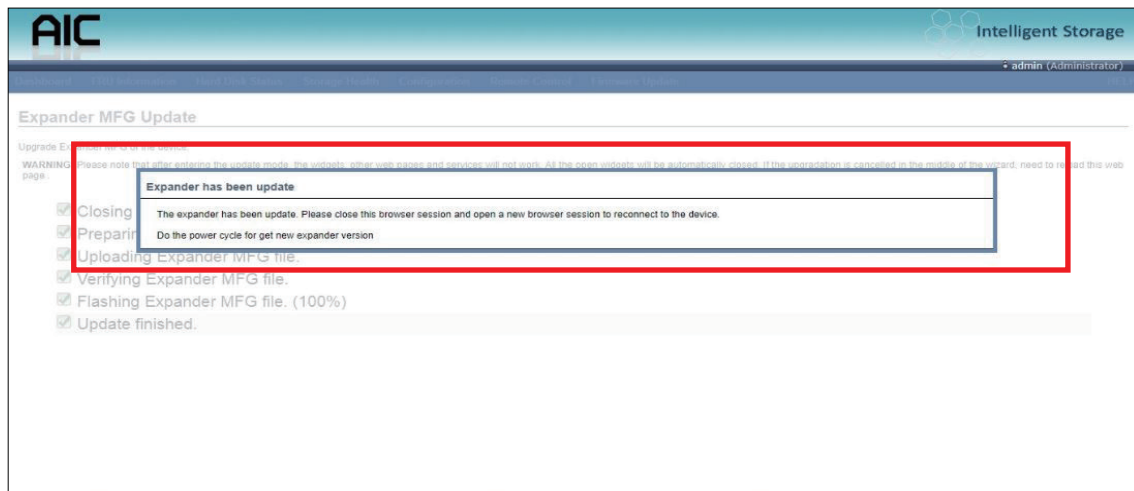
If an error message appears after you clicked upload, please reselect an expander image or press **Cancel**.



9. Wait a few seconds for the system to confirm that **Flashing MGF Image** is complete.



10. The message "Expander has been updated" appears.



11. Close the browser page and power cycle the system to complete update.

Chapter 5. Technical Support



www.aicipc.com

Taiwan, Global Headquarters

Address: No. 152, Section 4,
Linghang N. Rd, Dayuan District,
Taoyuan City 337, Taiwan
Tel: +886-3-433-9188
Fax: +886-3-287-1818
Sales Email: sales@aicipc.com.tw
Support Email: support@aicipc.com

Shanghai, China

Address: Room 215, Building 4, No.471
Guiping Road, Xuhui District, Shanghai City,
200233 China
Tel: +86-21-54961421
Sales Email: sales@aicipc.com.cn
Support Email: support@aicipc.com

Moscow, Russia

Address: No.500, 5th Floor, 5th Entrance,
32A, Khoroshevskoye Shosse, Moscow,
123007
Tel: +7-4997019998
Sales Email: support-ru@aicipc.com.tw
Support Email: rma.russia@aicipc.com.tw

North California, United States

Address: 48531 Warm Springs
Boulevard Suite 404 Fremont, CA
94539, United States
Tel: +1-510-573-6730
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

South California, United States

Address: 21808 Garcia Lane
City of Industry, CA 91789,
United States
Toll free: + 1-866-800-0056
Tel: +1-909-895-8989
Fax: +1-909-895-8999
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

New Jersey, United States

Address: 322 Route 46 West Suite 100
Parsippany, NJ 07054 United States
Tel: +1-973-884-8886
Fax: +1-973-884-4794
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

Houten, The Netherlands

Address: Peppelkade 58, 3992AK, Houten,
The Netherlands
Tel: +31-30-6386789
Fax: +31-30-6360638
Sales Email: sales@aicipc.nl
Support Email: support@aicipc.com