J4078-02-04X

4U78 SAS4 JBOD
User's Manual

UM_J4078-02-04X_v1.7_071725

Table of Contents

Document Release History

Release Date	Version	Update Content
December, 2022	1	Release to public.
July, 2024	1.1	Update specification content (AC input).
August, 2024	1.2	Add backplane info. and drive slot map.
October, 2024	1.3	Add 3.5" HDD removal info and correct page37 typo.
January, 2025	1.4	Correct page27/31 pin definition typo.
April, 2025	1.5	Correct sensor numbers on the diagram.
June, 2025	1.6	Update front panel and add 8644 LED indicator.
July, 2025	1.7	Update RQST IDENT_Red LED description.

Preface

Copyright

Trademarks

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 J4078-02-04X.
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 J4078-02-04X. For the latest version of this user's manual, please refer to the AIC® website: https://www.aicipc.com/en/productdetail/51367.

Chapter 1 Product Features

J4078-02-04X 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 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: https://www.aicipc.com/en/index. It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

J4078-02-04X is a high performance JBOD product that includes 78 x 3.5" drive bays and single/dual expander module(s). For more information about our product, please visit our website at https://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 contents of the shipping carton are all there and in good condition.

1.1 Box Content

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

- System chassis

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

PACKAGE CONTENT MAY VARY PER REGION.

1.2 Specifications

General	Number of Expander	Single/Dual
	Expander Chip	Hub: SAS4x48 Edge: SAS35x40 & SAS35x36/SAS4x40 &SAS4x32
	Host/Expansion Interface	4 x Mini SAS HD (SFF-8674) per expander module (backward compatible with SFF-8644 SAS12G)
Drives Supported	Drive Interface	• 24Gb & 12Gb SAS if using dual expanders • 24Gb & 12Gb SAS + 6Gb SAS/SATA if using single expander
	Form Factor	3.5” / 2.5” (with optional kit)
Administration / Management	Admin/Firmware Upgrade	• In-band • IEM port
	LED Indicators, Audible Alarm	Yes
Hot swap and Redundancy	Drive Bays	78
	Cooling	• 8 x 60x56mm hot swap fans • 1 x 40x56mm fan per expander module
	Power Supply	1600W 1+1 hot swap redundant 80+ Platinum/Titanium
	Power Entry	Dual AC Inlet
	Expander Modules	Dual SAS topology (Optional)

Electrical and Environmental	AC Input	Platinum: 200-240Vac , 50/60Hz, 12A(1600W) Titanium: 200-240Vac , 50/60Hz, 10A(1600W)
	Operating Environment	• Temperature : 0ºC to 35º C • Relative humidity : 20% to 80 %
	Non-operating Environment	• Temperature : -20ºC to 60º C • Relative humidity : 10% to 90 %
Physical Specification	Dimensions (W x D x H)	mm : 434 x 810.5 x 176 434 x 974.7 x 176 (with CMA)
		inches : 17 x 31.9 x 7 17 x 38.4 x 7 (with CMA)
	Gross Weight (w/ PSU, Rail and Pallet; w/o Disks)	kgs : 57.67
		lbs : 127.1
	Packaging Dimensions (W x D x H)	mm : 675 x 1120 x 536
		inches : 26.6 x 44.1 x 21.1
Mounting	Standard	31” slide rail
	Option	Cable Management Kit

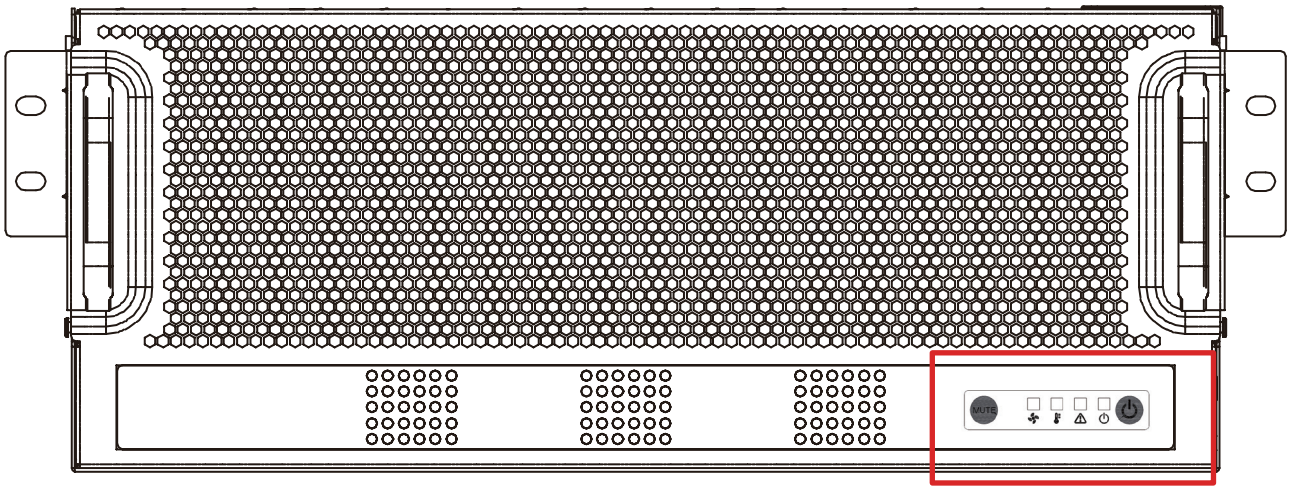
1.3 Feature

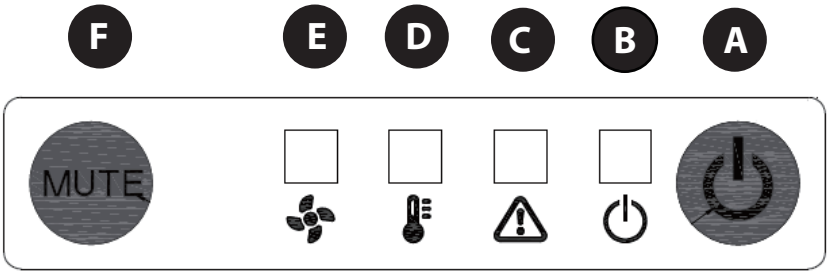
J4078-02-04X is a reliable SAS JBOD with 78 drives bays. This product is designed to accommodate single/dual hub expanders with 4 Mini SAS HD wide ports. Featuring the expander chip, Broadcom SAS4x48, which is underscored for its high scalability and performance of supporting up to 22.5 Gb/s, this product enhances these features by integrating designs, redundant fans, and expansion to offer easy control and high performance for our customers.

- Intelligent Enclosure Management
- Individual drive power management
- Hot swap design for easy maintenance and management
- Enclosure Cable Management Kit
- Tool-less drive trays
- Designed for 1000mm depth rackmount server cabinet

Front Panel

J4078-02-04X 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

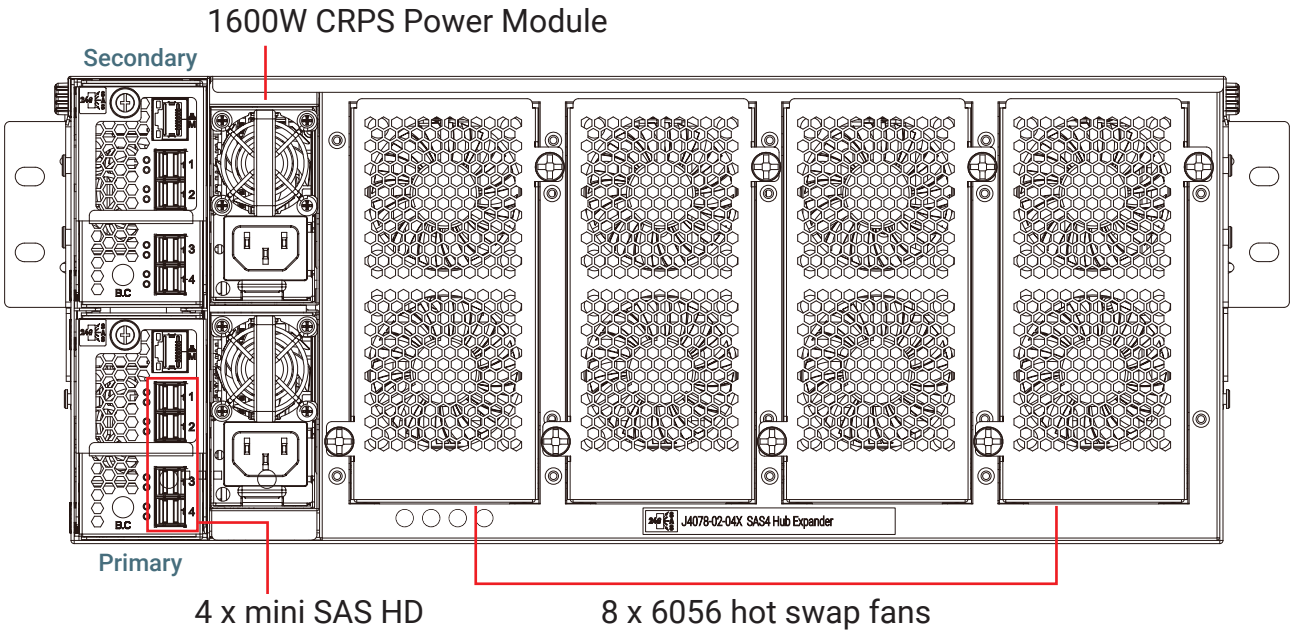
E

Fan Fault LED	
Behavior	Status
Normal	Off
Failed	Red

F

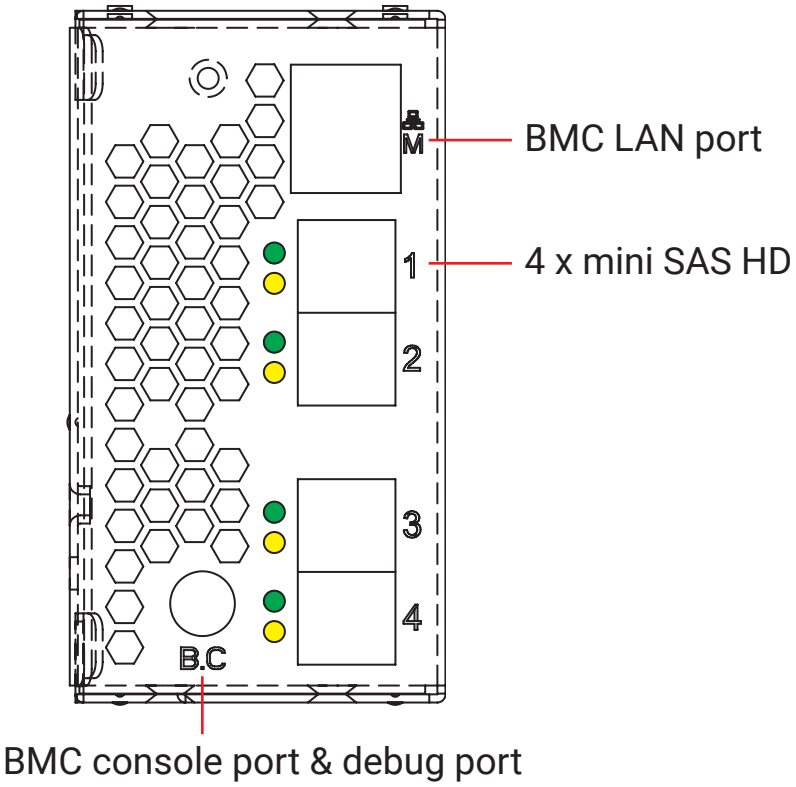
System Alert Mute Switch	
Behavior	Status
Normal	Off
Press	Alert mute

Rear Panel


1600W CRPS Power Module
Secondary
Primary
4 x mini SAS HD
8 x 6056 hot swap fans
J4078-02-04X SAS4 Hub Expander

Rear Expander Panel

J4078-02-04X offers single/dual expander(s) with 1 BMC port and 4 mini SAS HD ports per expander module.



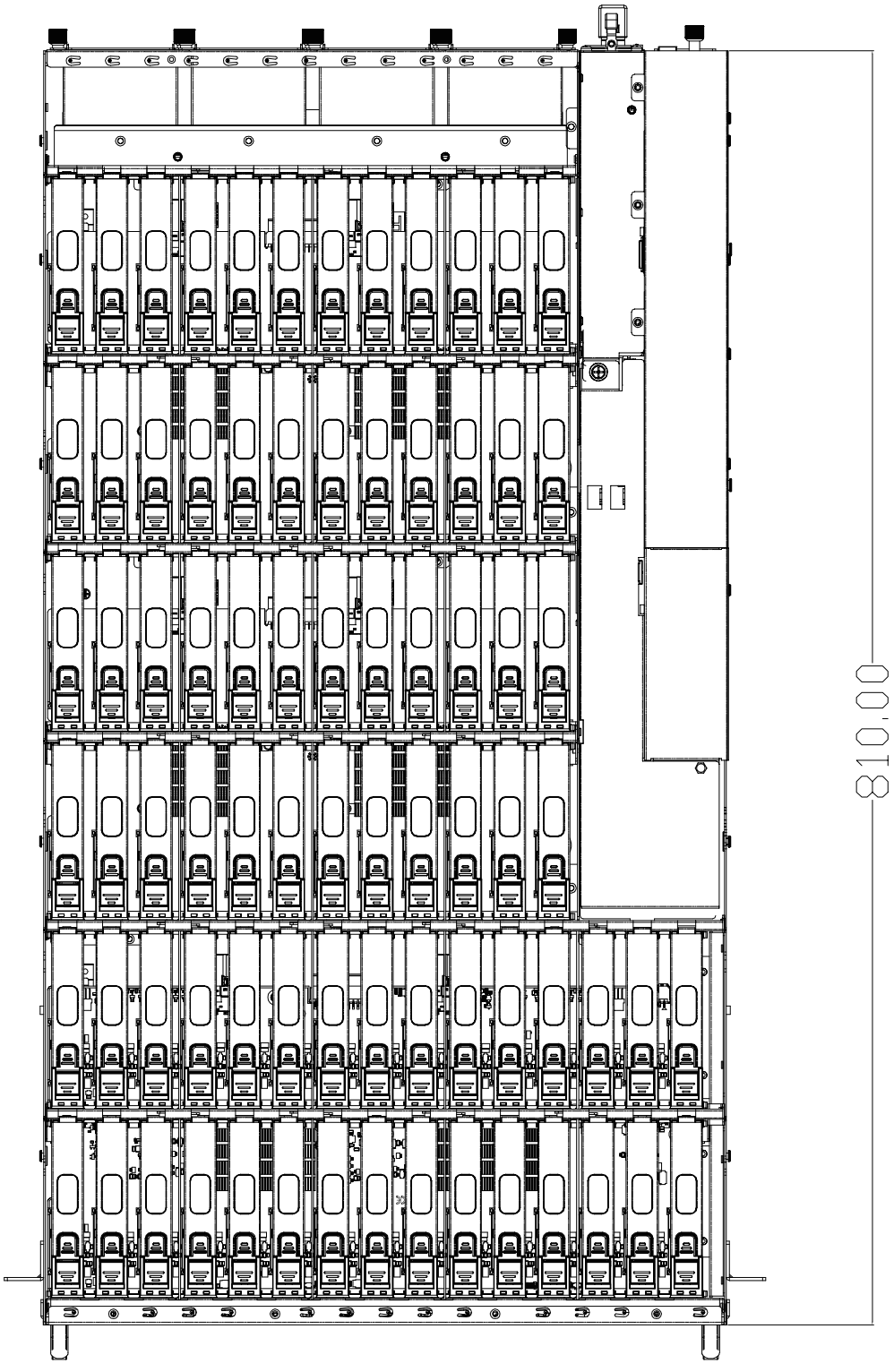
8644-LED Indicator Definition

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

J4078-02-04X offers 3.5" x 78 HDD bays.

- 24Gb & 12Gb SAS if using dual expanders
- 24Gb & 12Gb SAS + 6Gb SAS/SATA if using single expander

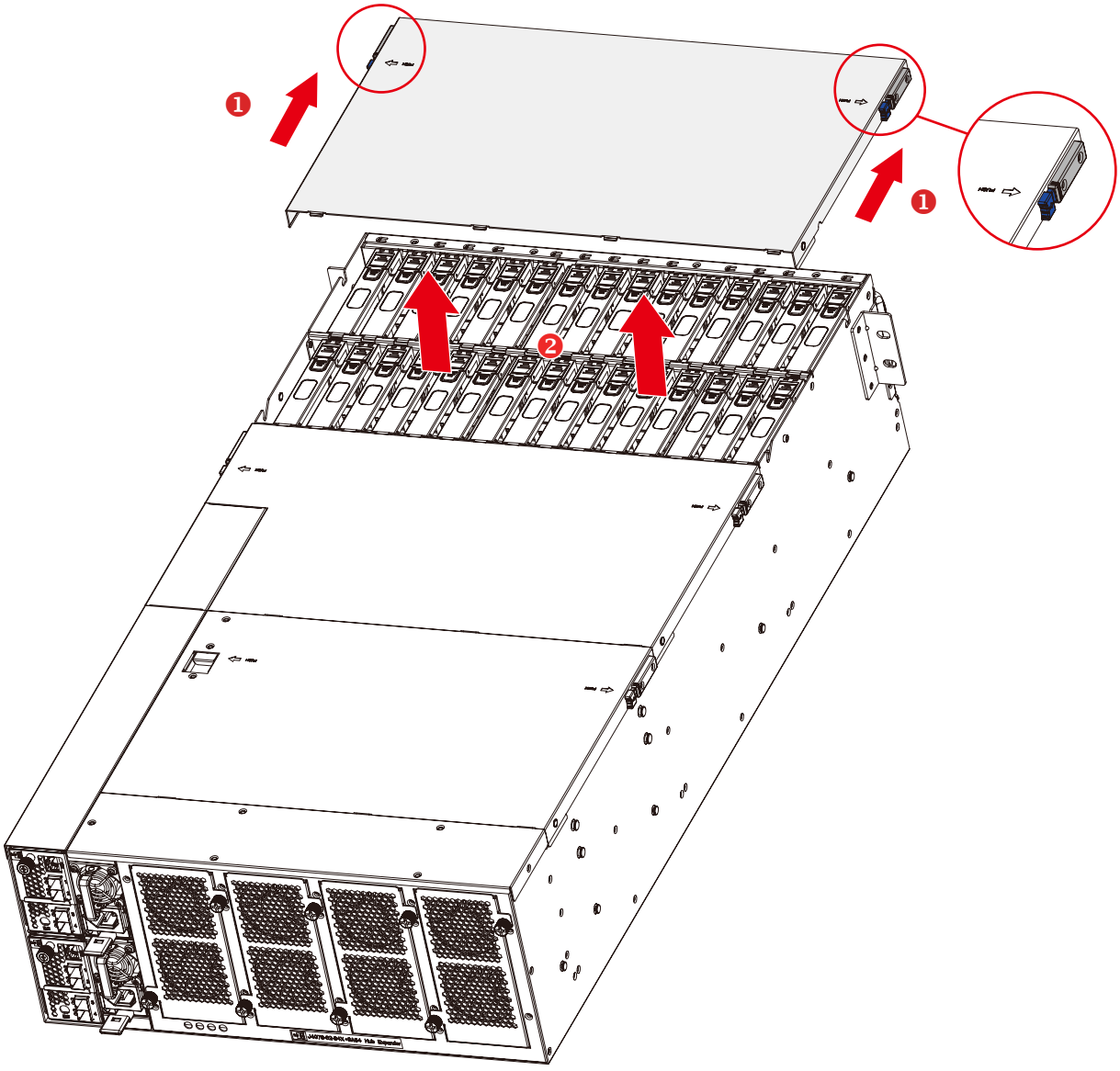


Chapter 2. Hardware Setup

2.1 Top Cover

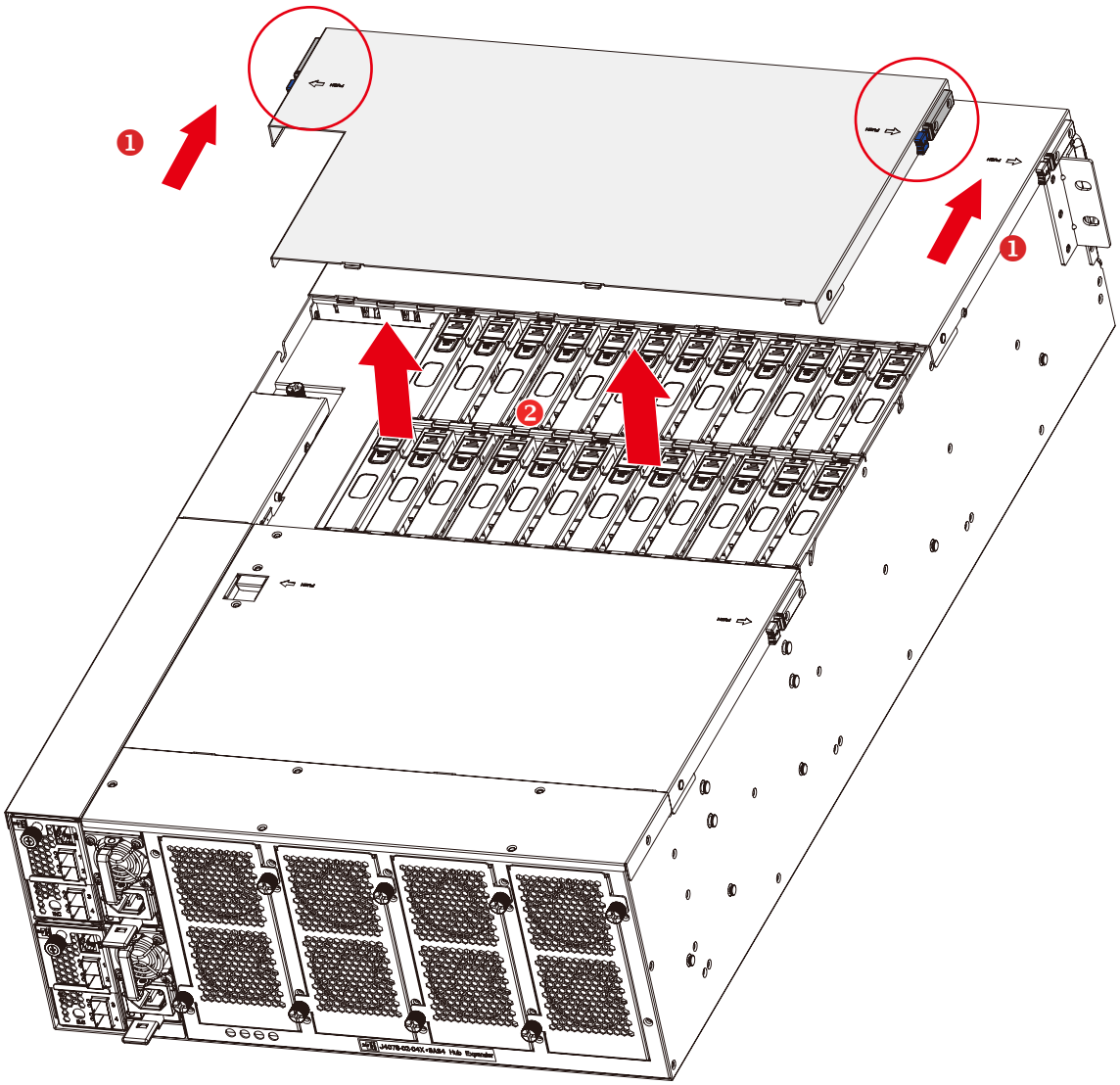
2.1.1 Removing and Installing the Front Top Cover

① Press the release button on both sides of the top cover and simultaneously push the cover towards the front panel.
② Lift upward to remove the cover from the chassis.



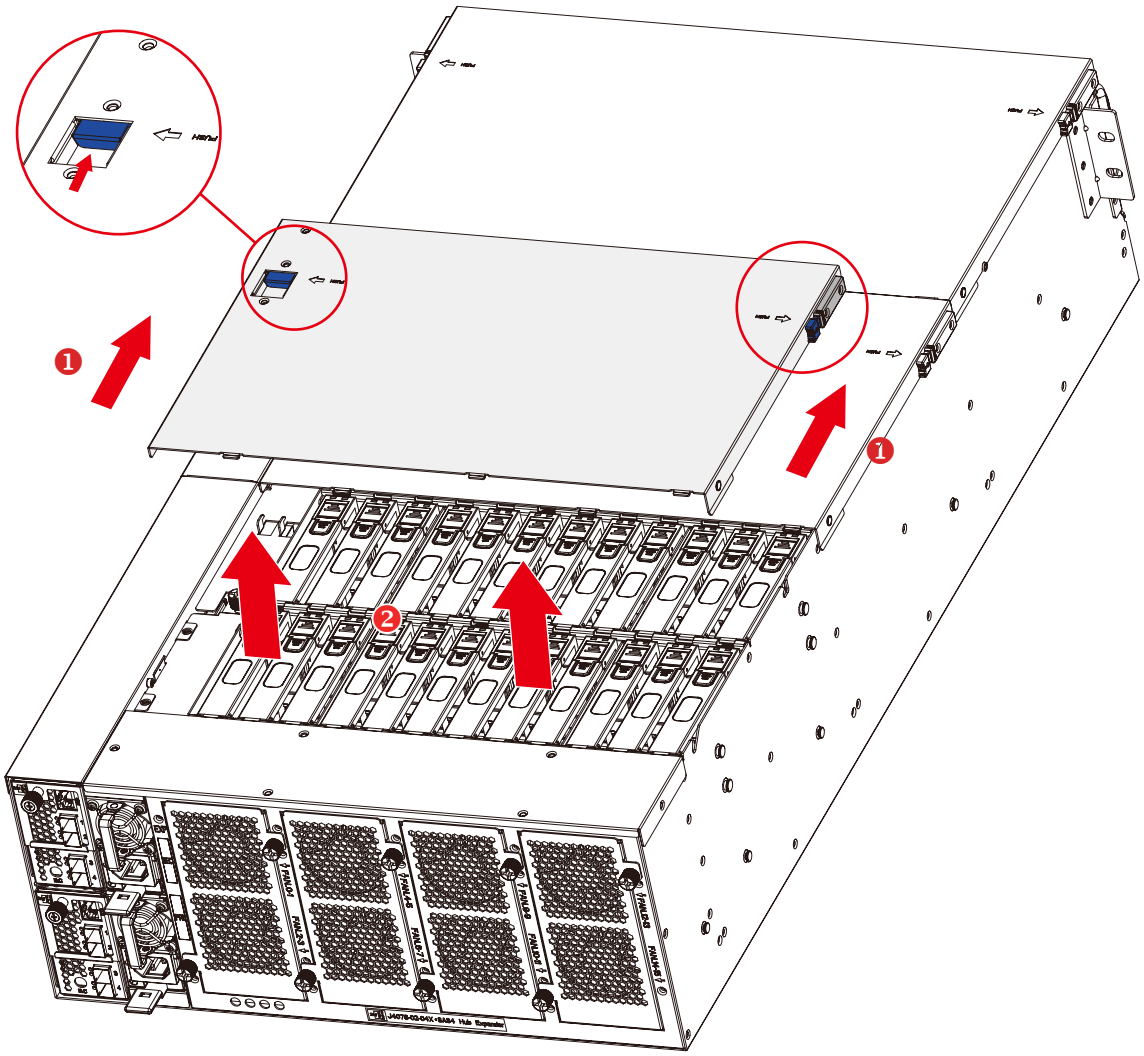
2.1.2 Removing and Installing the Middle Top Cover

① Press the release button on both sides of the top cover and simultaneously push the cover towards the front panel.
② Lift upward to remove the cover from the chassis.



2.1.3 Removing and Installing Rear Top Cover

① Press the release button on both sides of the top cover and simultaneously push the cover towards the front panel.
② Lift upward to remove the cover from the chassis.

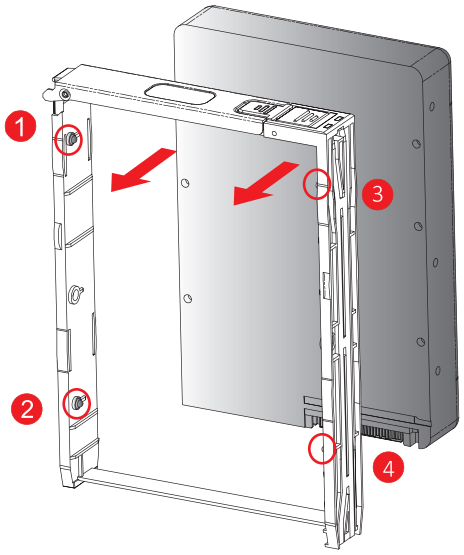


This information is provided for professional technicians only.

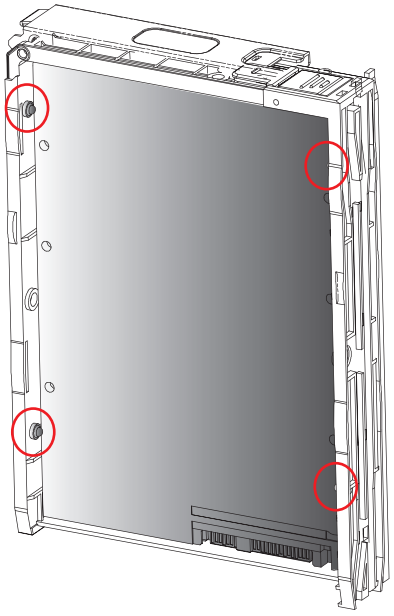
2.2 Disk Drive

2.2.1 Installing the 3.5" Hard Disk Drive

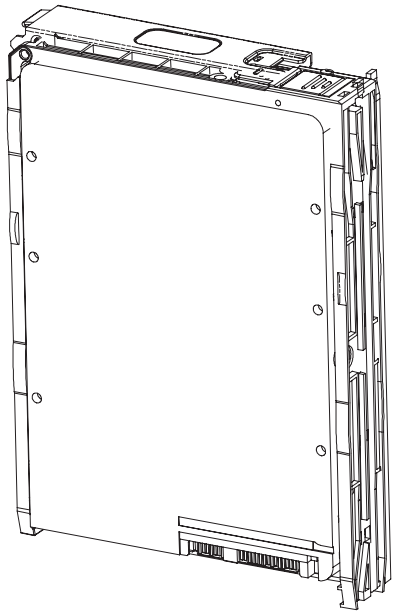
① Match the dimples on the HDD with the tool-less tray.
② Align the HDD with the tray by placing it against each other.



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.

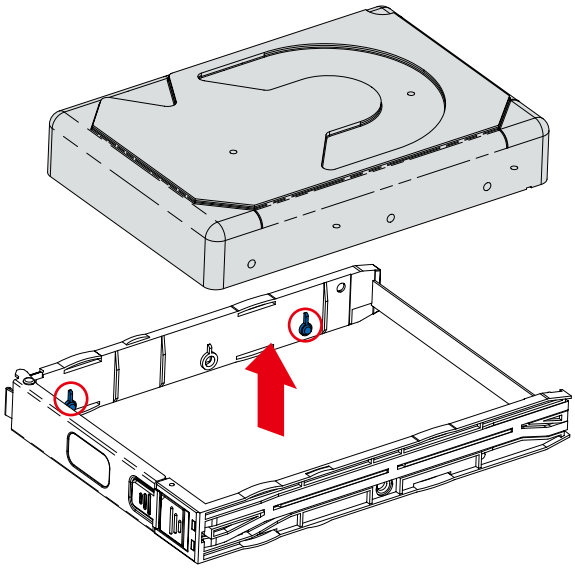


④ Complete the installation.



2.2.2 Removing the 3.5" HDD from the Tray

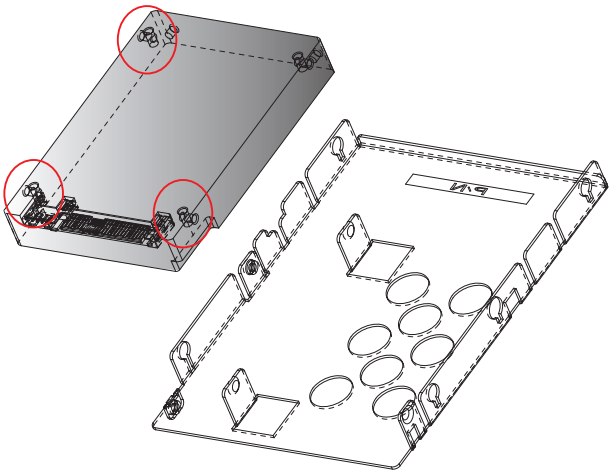
Pull the sides of the tray to remove the HDD. Make certain to pull the tray with smaller dimples first away from the HDD and the larger dimples last for easier removal.



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.

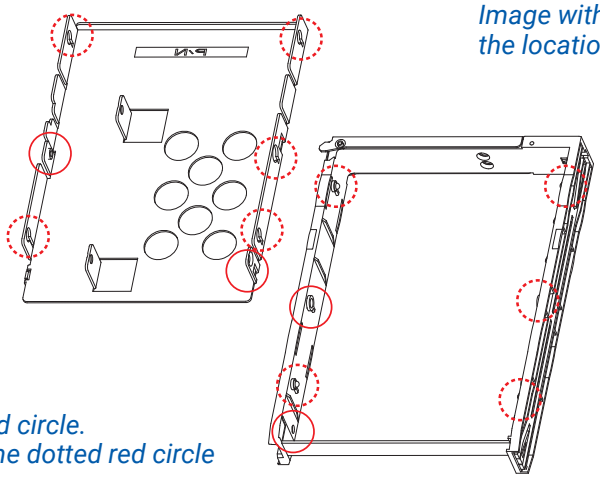
2.2.3 Installing the 2.5" Hard Disk Drive (Optional)

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



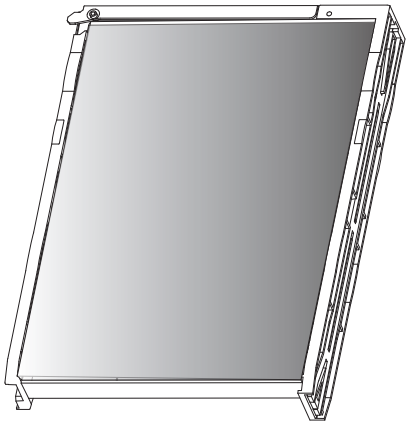
② Match the dimples (in dotted red circle) on the HDD bracket and HDD with the tool-less tray.

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



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

③ Insert the bracket and HDD into the tool-less tray.
④ Secure the screws on the bracket to complete installation.



2.2.4 Removing and Installing the HDD Tray

2.2.4.1 Installing the HDD Tray

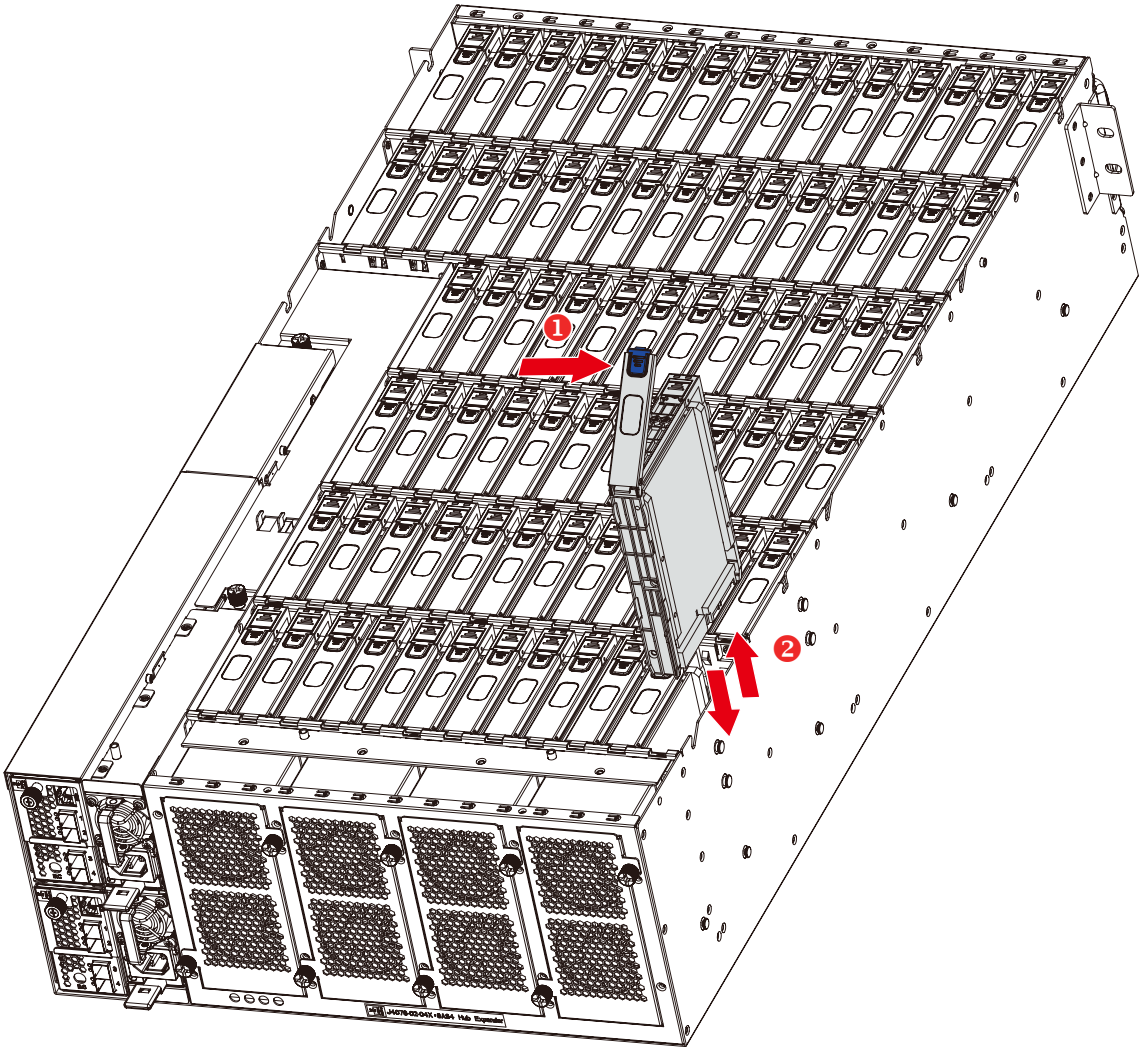
① Insert the drive tray into chassis HDD cage. Make sure the drive tray is correctly secured in place when its front edge aligns with the bay edge.

② Push the tray lever until it reaches the end and clicks.

2.2.4.2 Removing the HDD Tray

① Press the release button on the tray lever.

② Pull upwards to remove the HDD tray from the enclosure.



This information is provided for professional technicians only.

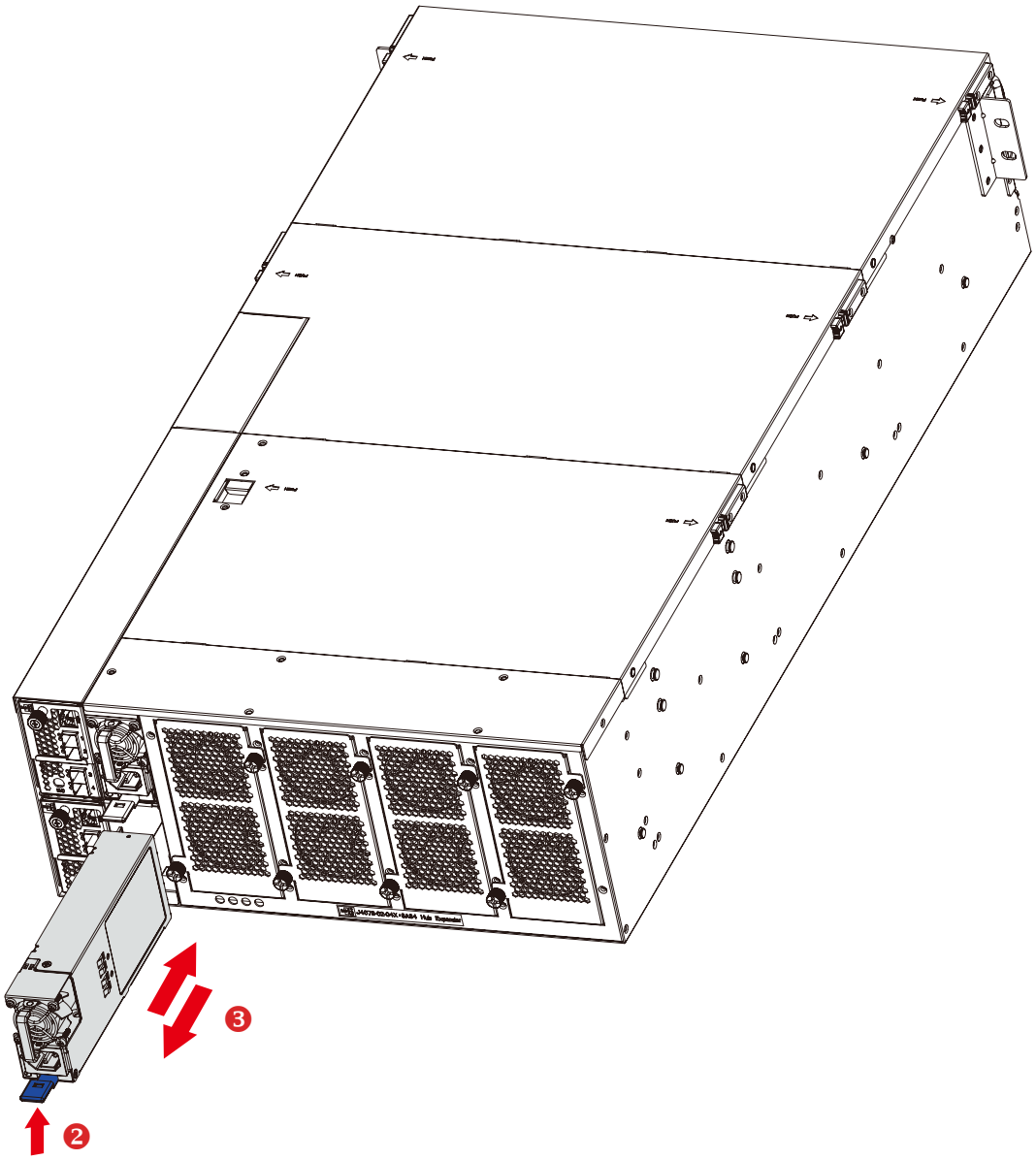
2.3 Power Supply Unit Module

2.3.1 Installing the Power Supply Unit

Push the power supply module into the enclosure. Make sure the latch on the module is fully hooked onto the PSU housing.

2.3.2 Removing the Power Supply Unit

① Remove power cables connected to the power supply module. Allow a minute for fan to spin down.
② Push the latch and hold the tray handle.
③ Pull the power supply module gently until it slides out of the enclosure.



This information is provided for professional technicians only.

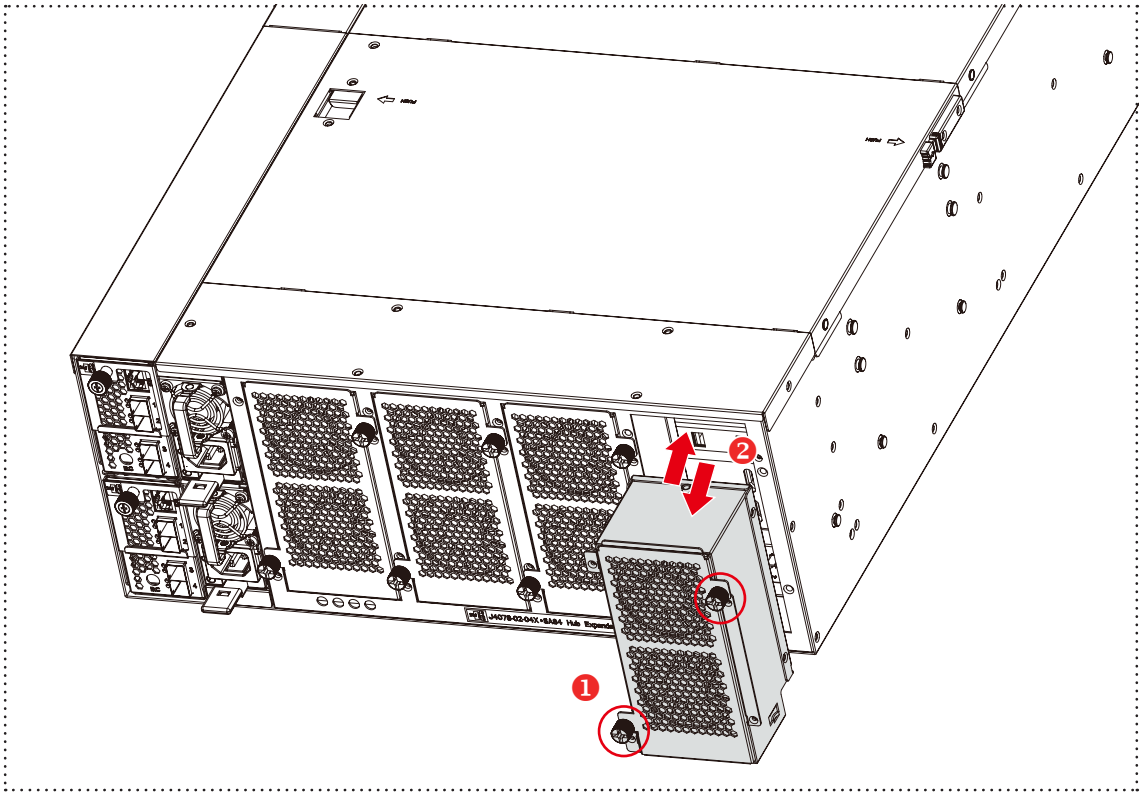
2.4 Fan Module

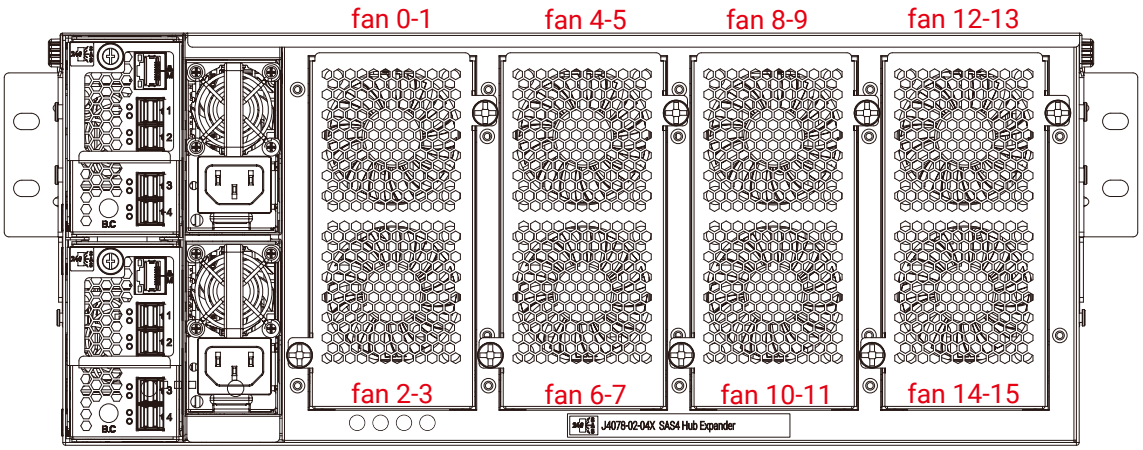
2.4.1 Installing the Fan

Align the fan module with the opening in the enclosure and insert the module into the JBOD.

2.4.2 Removing the Fan

① Loosen the thumb screws x 2 pcs on the fan module.
② Pull the fan module from the enclosure.





This information is provided for professional technicians only.

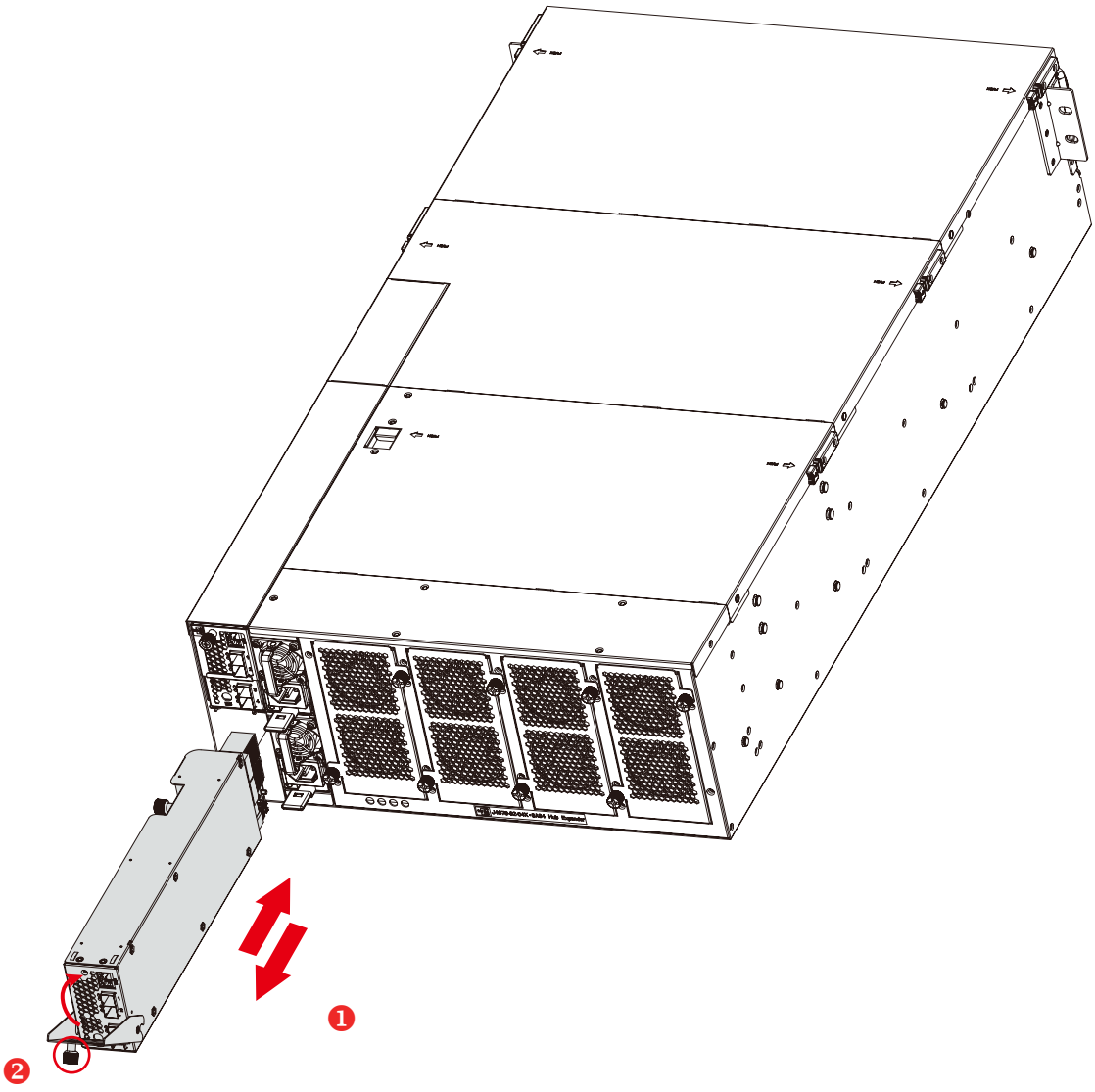
2.5 Expander Module

2.5.1 Installing the Expander

① Align the expander module with the opening in front of the enclosure and insert it into the enclosure.
② Close the lever and secure the retaining screw.

2.5.2 Removing the Expander

Loosen the screw to remove.



This information is provided for professional technicians only.

2.6 Drive Backplane Module

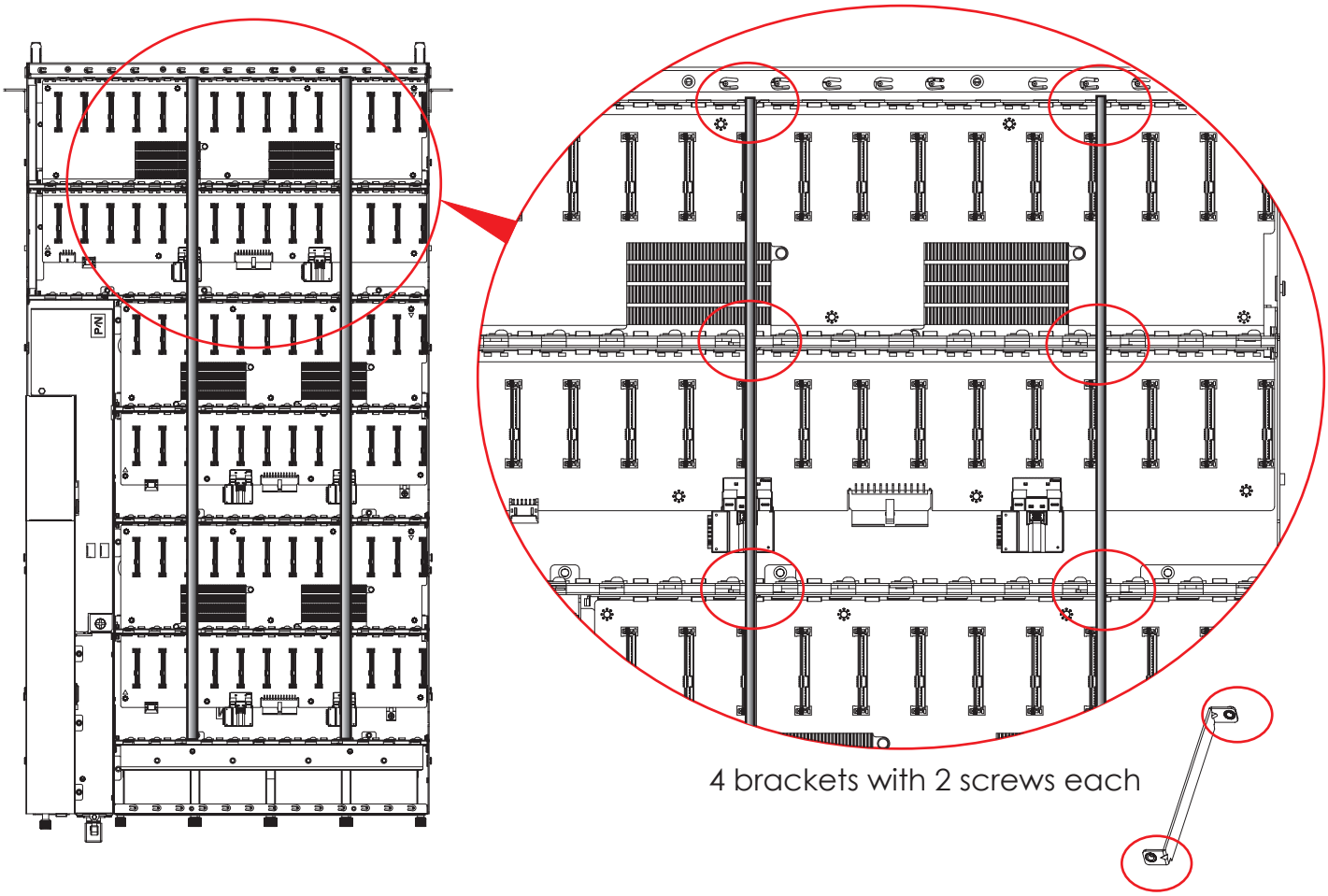
NOTE
Before you pull out the HDD backplane, you must remove all the HDD trays and cables.

2.6.1 Installing the HDD Backplane

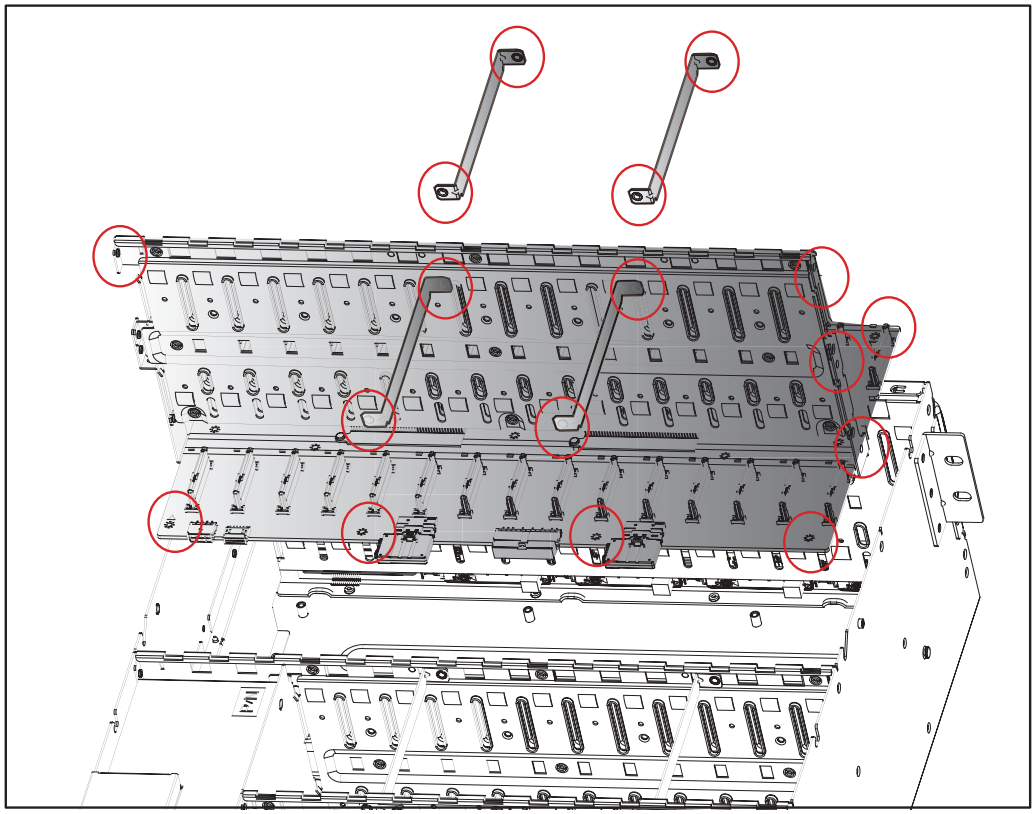
① Position the HDD backplane module into the chassis and secure the screws x 12 pcs onto the enclosure (8 screws on the HDD backplane, 4 screws on the HDD backplane tray).
② Position the brackets x 4 on the top of the HDD backplane module and secure the screws x 8 pcs (1 bracket with 2 screws each).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

2.6.2 Removing the HDD Backplane

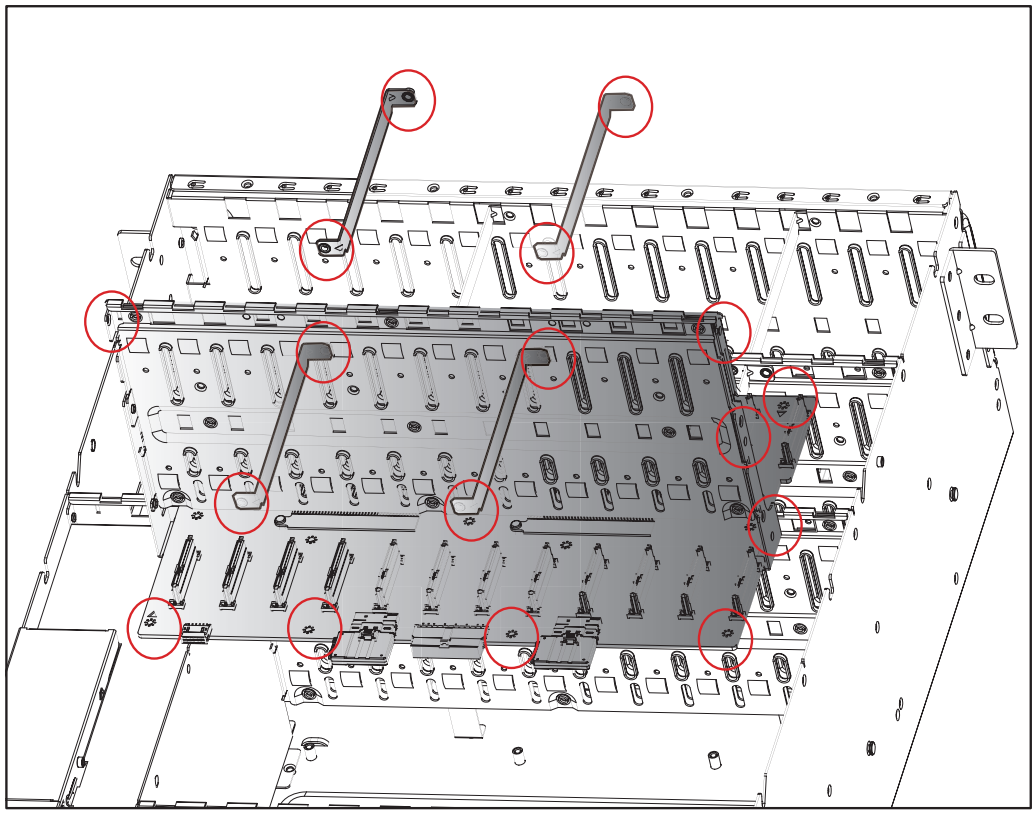
① Remove the HDD disk trays from the enclosure.
② Remove the top brackets x 4 from the chassis by removing the screws x 8 pcs (1 bracket with 2 screws each).
③ Remove the screws x 12 pcs on the HDD backplane module (8 screws on the HDD backplane and 4 screws on the HDD backplane tray).
④ Repeat step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



Bracket and HDD backplane removal

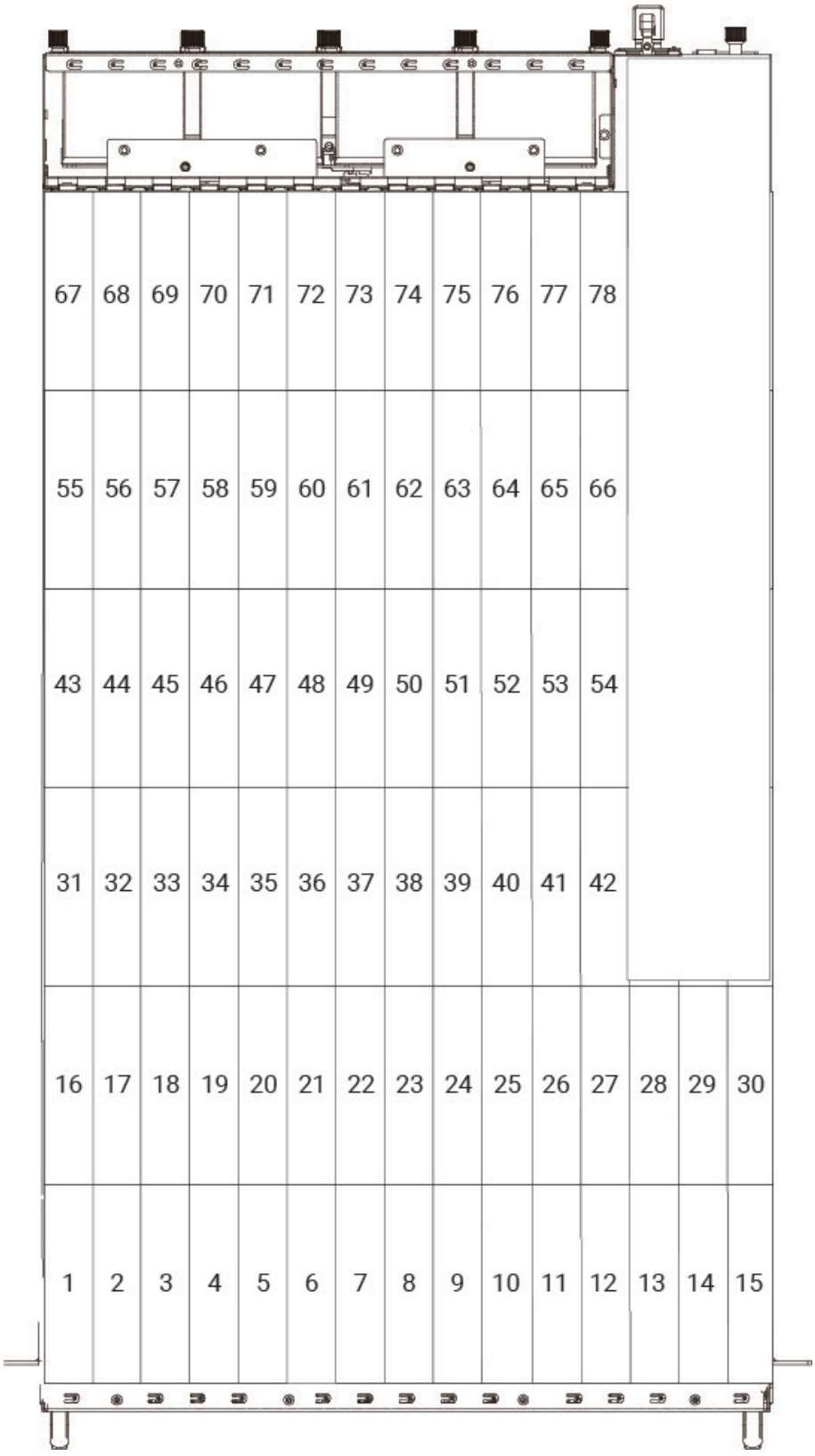


Bracket and second HDD backplane removal



This information is provided for professional technicians only.

2.7 Drive Slot Map



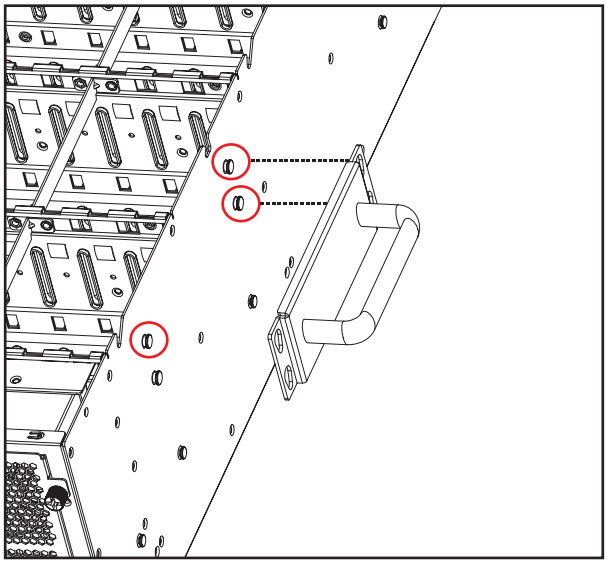
Top view

2.8 Rear Handle

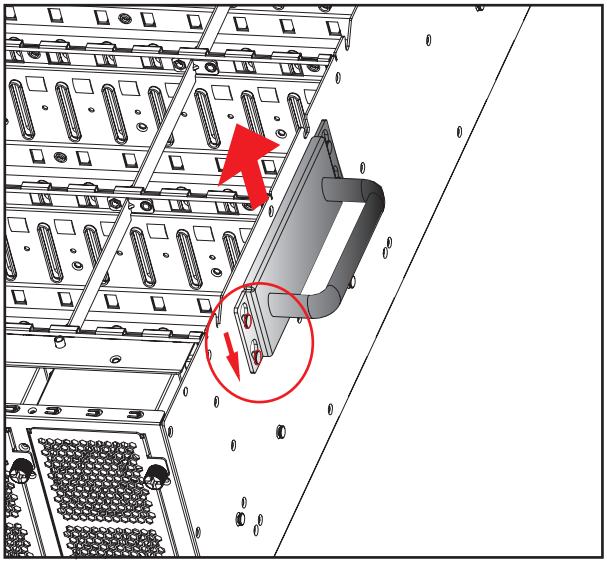
2.8.1 Installing the Rear Handle

① Match the locking plate on the handle with the locks on the chassis.
② Pull the handle upward to lock the handle onto the chassis.

Aligning the handle with the chassis.



Securing the handle.



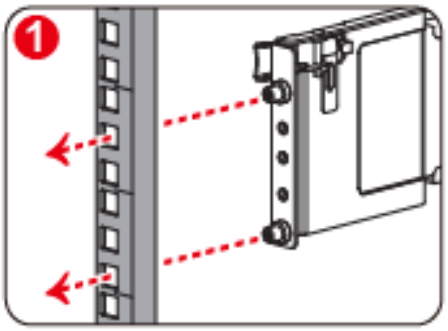
2.8.2 Removing the Rear Handle

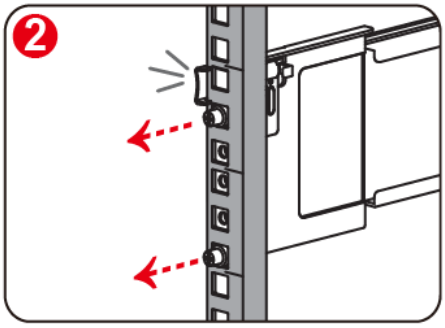
① Push the handle downward to dismantle the lock from the handle.
② Remove the handle from the chassis.

This information is provided for professional technicians only.

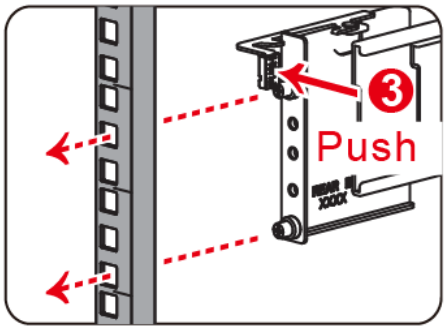
2.9 Slide Rail

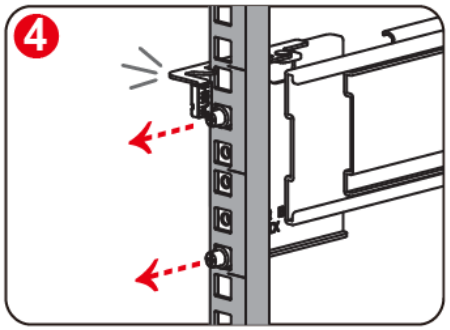
1. Attach the slide rail bracket assembly to the rack frame.
   ① Align and attach the front rail bracket to the rack.
   ② Ensure that the latch on the rail is hooked onto the rack.



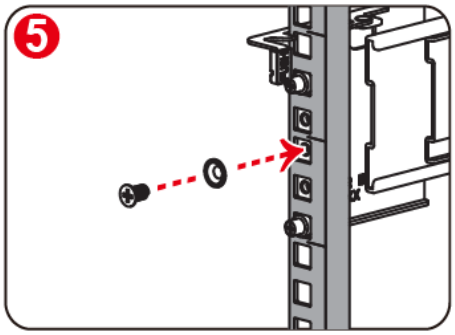


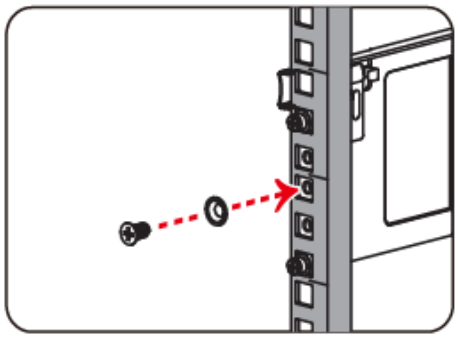
   ③ Align and attach the rear rail bracket to the rack by pushing the latch outward. Ensure the latch is hooked onto the rack.
   ④ Ensure that the latch on the rail is hooked onto the rack.



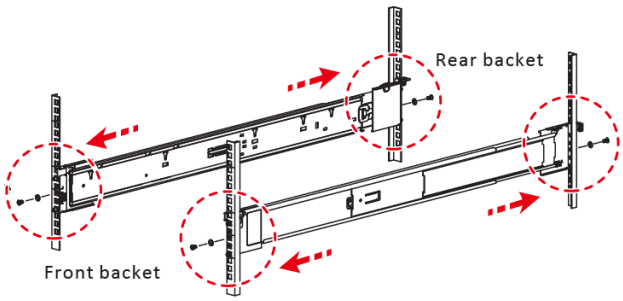


   ⑤ Secure the rail bracket with a washer and screw on both sides of the rail bracket.





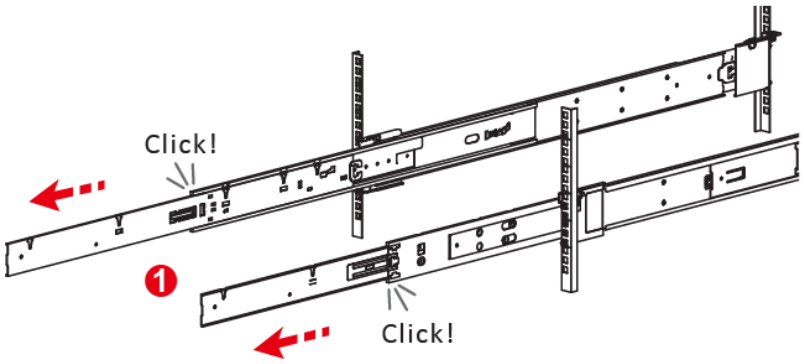
   ⑥ Repeat ① to ⑤ to install the other side of the rack.



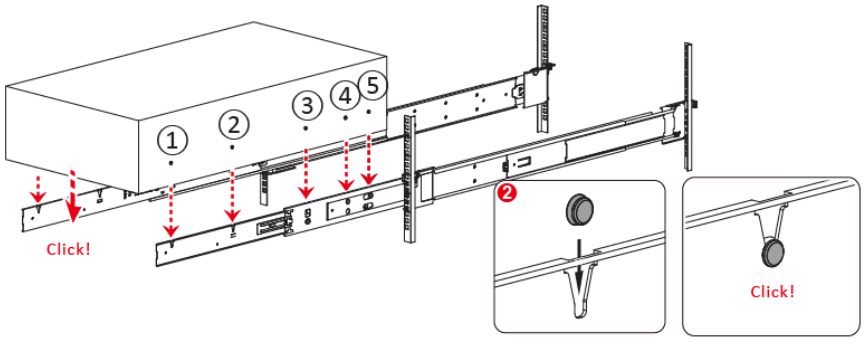
This information is provided for professional technicians only.

2. Attach the chassis onto the rack frame

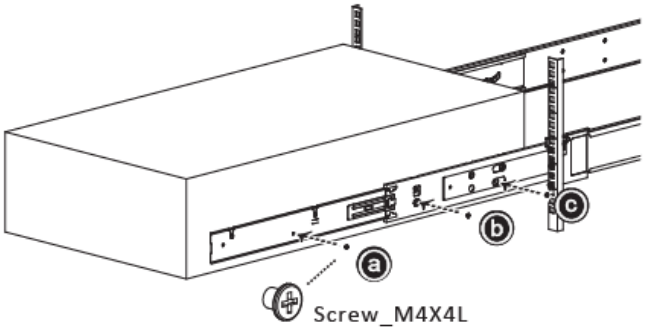
① Pull the inner and middle rail to fully locked position.



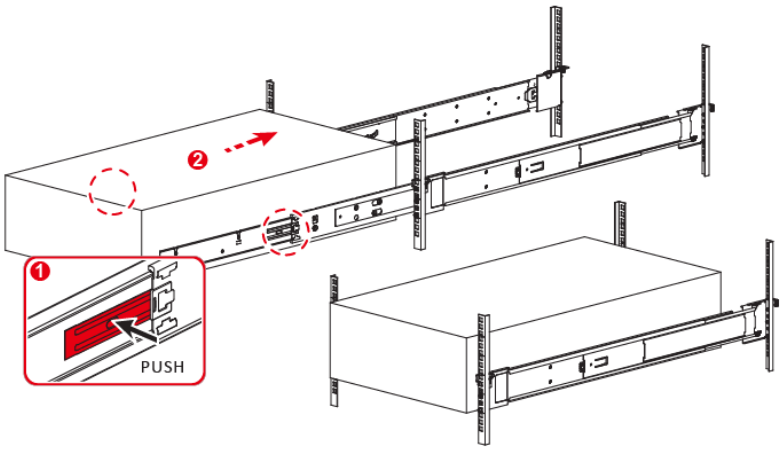
② Position the chassis vertically into the rail. Ensure the standoffs on the chassis slide into the v slots on the rail bracket.



③ Secure the chassis to the rail with screws.

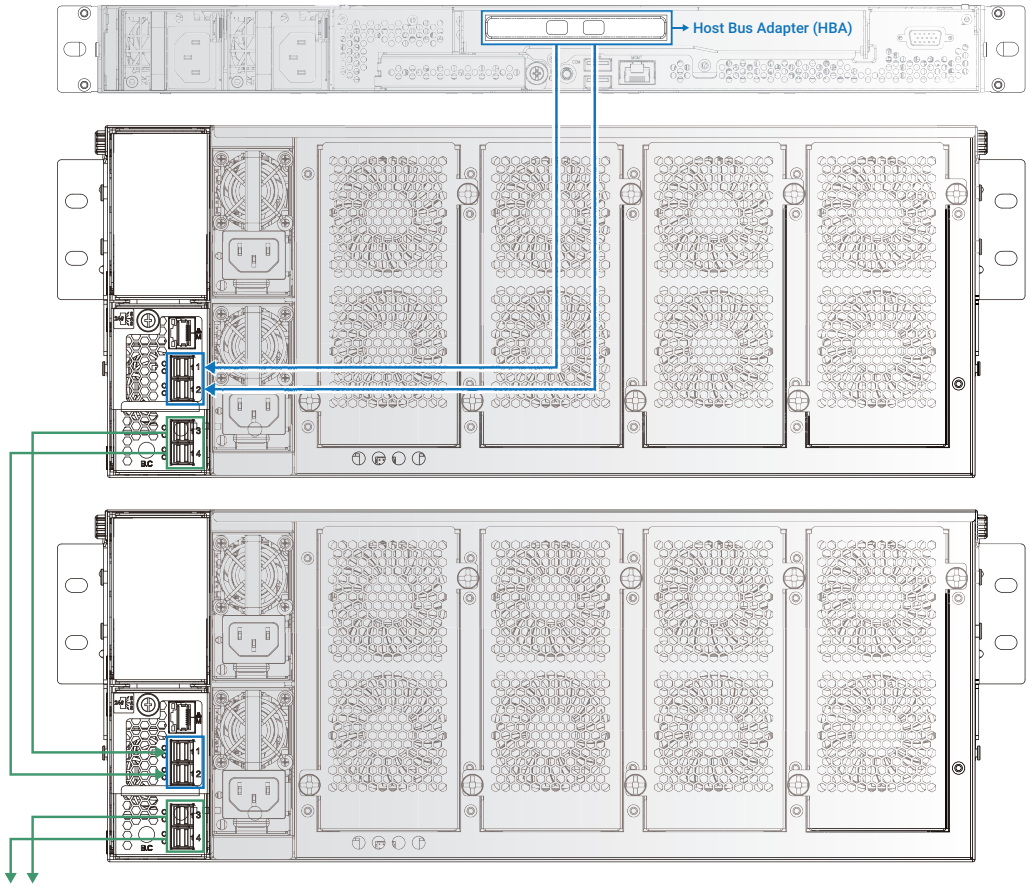


④ Push the release tab on the inner rail and push the chassis into the frame.

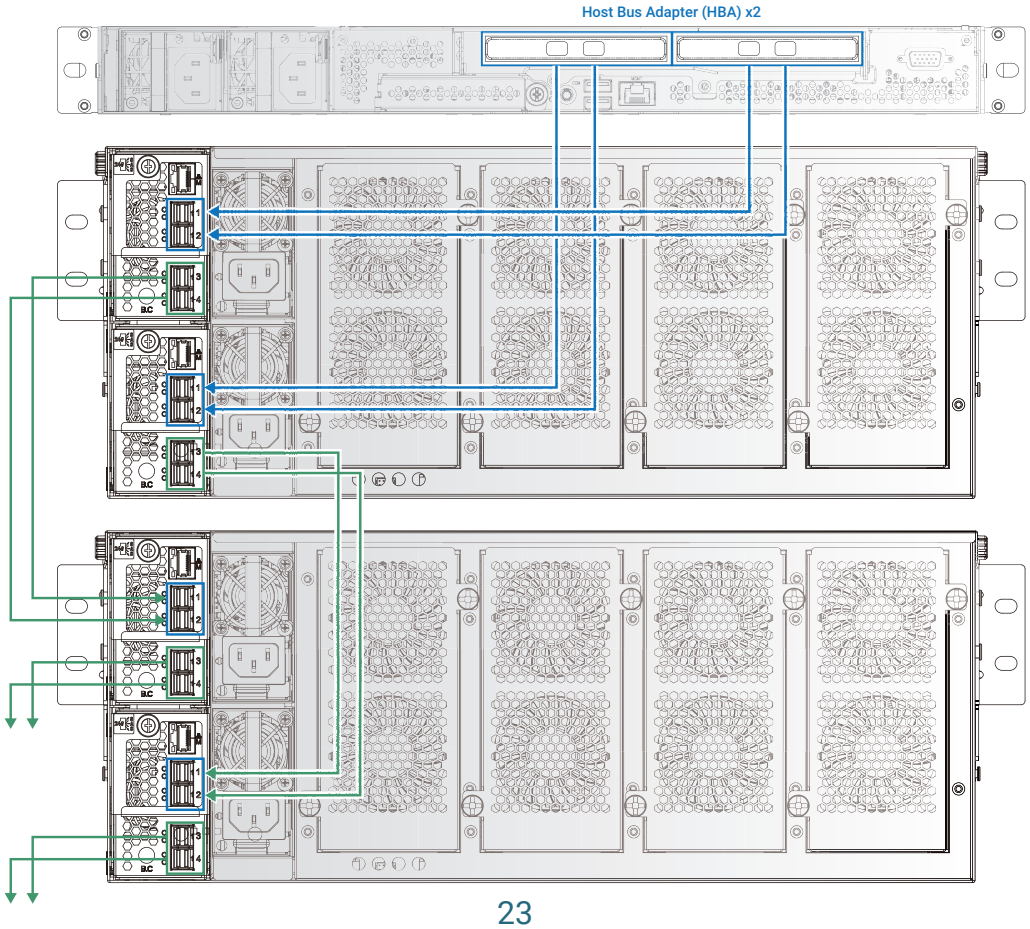


2.10 Standard Cabling

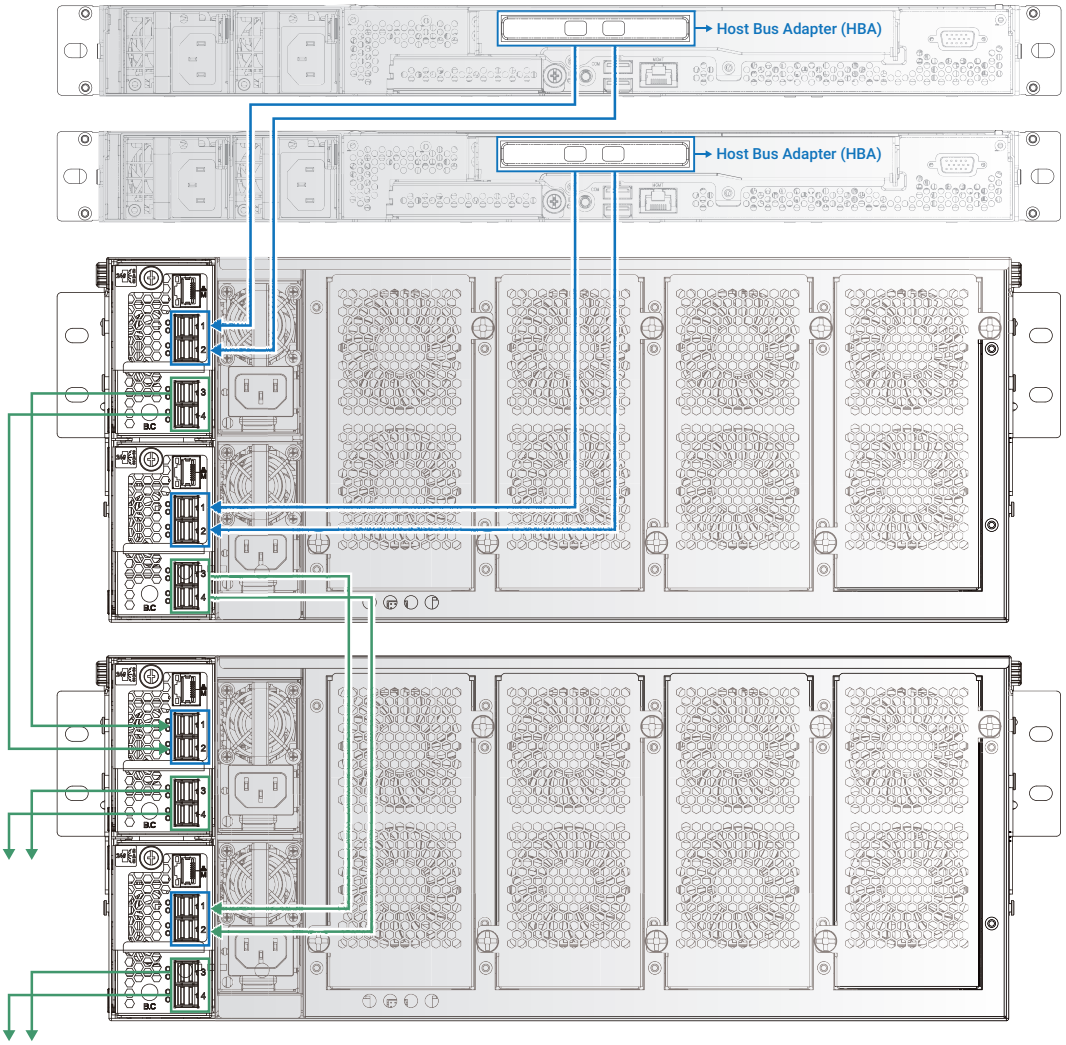
2.10.1 Single expander JBOD and 1 host server with 1 HBA card



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



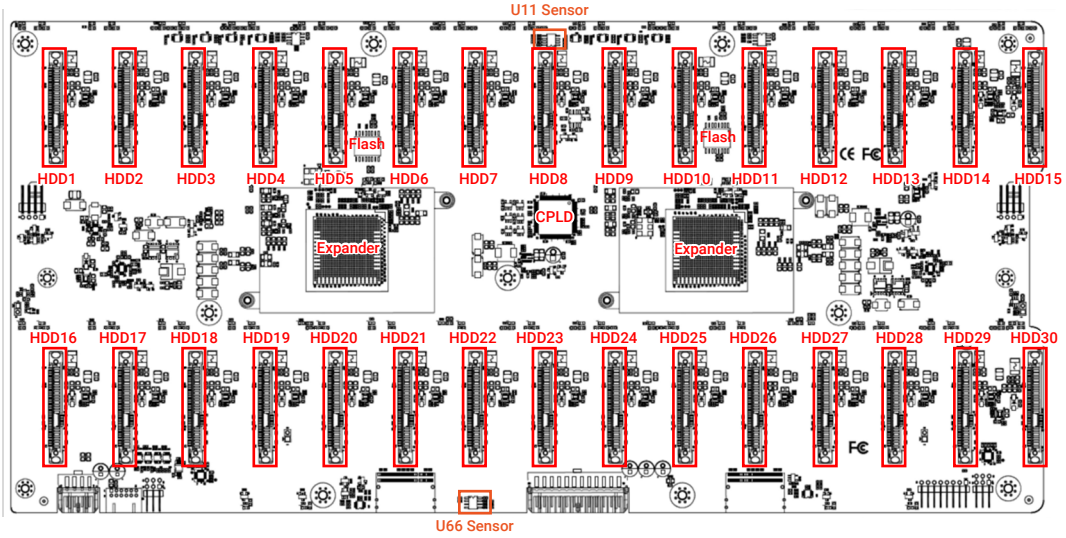
2.10.3 Dual expander JBOD and 2 host servers with 1 HBA card each



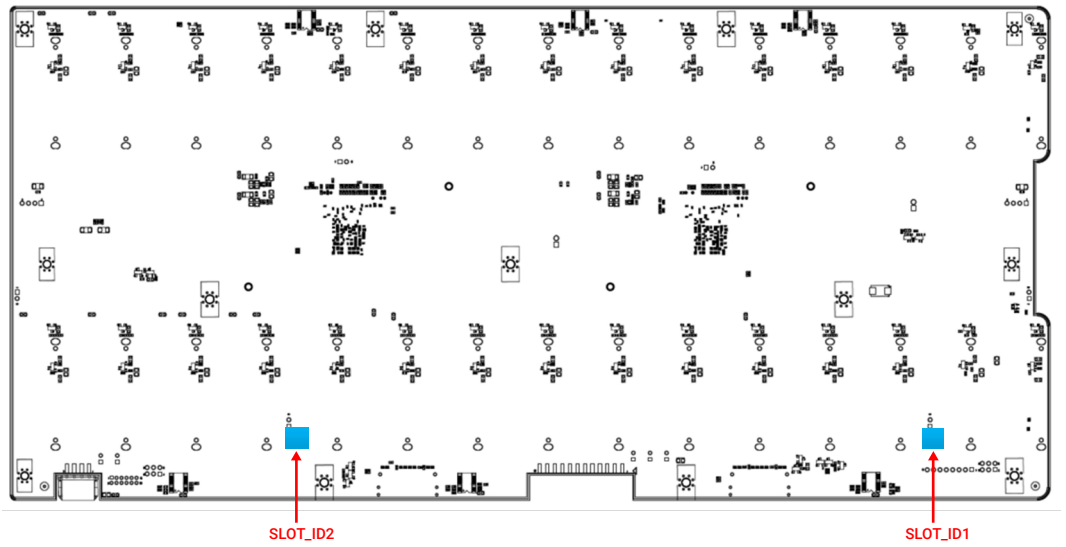
2.11Drive Backplane: 30 Bay

2.11.1 Placement

Top view



Bottom view



SAS PHY Mapping

	HDD1	HDD2	HDD3	HDD4	HDD5	HDD6	HDD7	HDD8	HDD9	HDD10	HDD11	HDD12	HDD13	HDD14	HDD15
Primary	phy-06	phy-05	phy-04	phy-03	phy-02	phy-39	phy-38	phy-37	phy-36	phy-35	phy-34	phy-33	phy-32	phy-31	phy-30
Secondary	phy-10	phy-09	phy-08	phy-07	phy-06	phy-05	phy-04	phy-03	phy-02	phy-39	phy-38	phy-37	phy-36	phy-35	phy-34

Primary U37

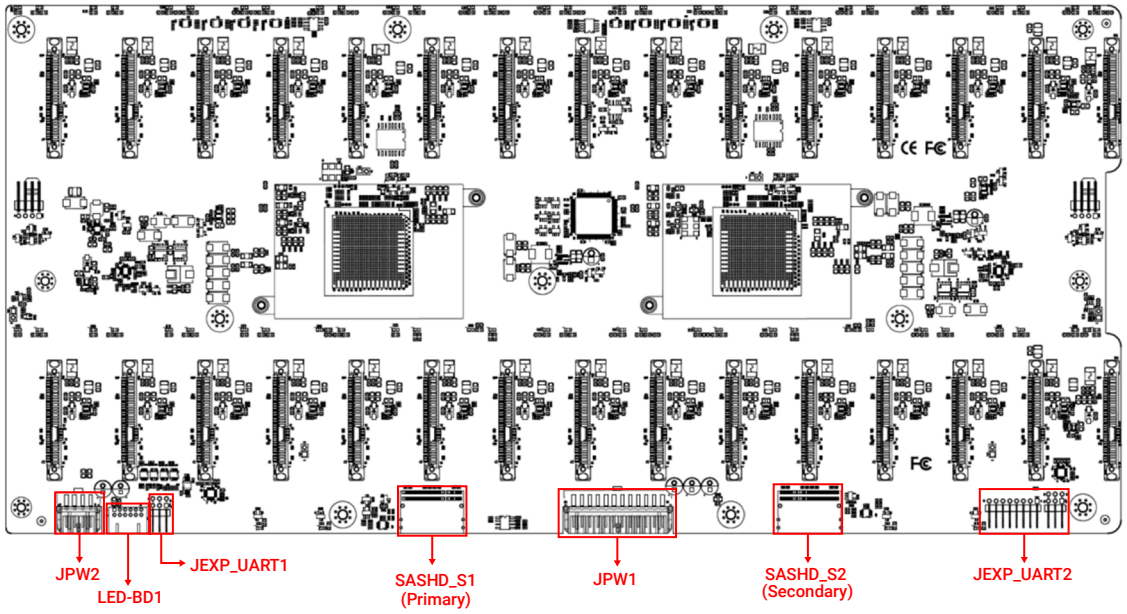
Secondary U36

	HDD16	HDD17	HDD18	HDD19	HDD20	HDD21	HDD22	HDD23	HDD24	HDD25	HDD26	HDD27	HDD28	HDD29	HDD30
Primary	phy-07	phy-08	phy-09	phy-10	phy-11	phy-20	phy-21	phy-22	phy-23	phy-24	phy-25	phy-26	phy-27	phy-28	phy-29
Secondary	phy-11	phy-12	phy-13	phy-14	phy-15	phy-16	phy-17	phy-18	phy-19	phy-20	phy-25	phy-30	phy-31	phy-32	phy-33

About JBOD slot mapping, please refer to 2.7 Drive Slot Map.

2.11.2 Connector

Location



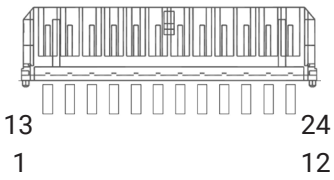
External Connectors

Connector Function	Physical Description	Comments
HDD1~30	SFF-8680 SAS Receptacle(SMT H:14.15mm)	HDD connector

Internal Connectors

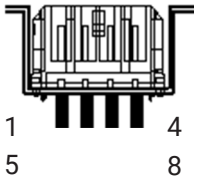
Connector Function	Physical Description	Comments
Power Supply (JPW1)	15 x 2 Pin Power Connector	12V. 4.5 A per pin.
Power Supply (JPW2)	4 x 2 Pin Power Connector	12V. 4.5 A per pin.
SAS SlimLine (SASHD_S1) (SASHD_S2)	74 pin 8i SAS SlimLine	SAS Host connection
UART (JEXP_UART1) (JEXP_UART2)	3 x 2 Pin Header	Expander SMART/DEBUG port.
LED Board (LED-BD1)	6 x 2 Pin Header	Connect to Front LED Board

Power Connector (JPW1)



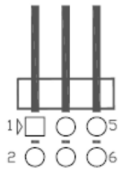
GND	13	1	GND
GND	14	2	GND
GND	15	3	GND
GND	16	4	GND
GND	17	5	GND
GND	18	6	GND
+12V	19	7	+12V
+12V	20	8	+12V
+12V	21	9	+12V
+12V	22	10	+12V
+12V	23	11	+12V
+12V	24	12	+12V

Power Connector (JPW2)



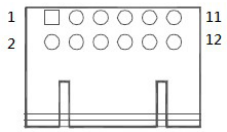
GND	5	1	GND
GND	6	2	GND
+12V	7	3	+12V
+12V	8	4	+12V

Control for Expander (JEXP_UART1/ JEXP_UART2)



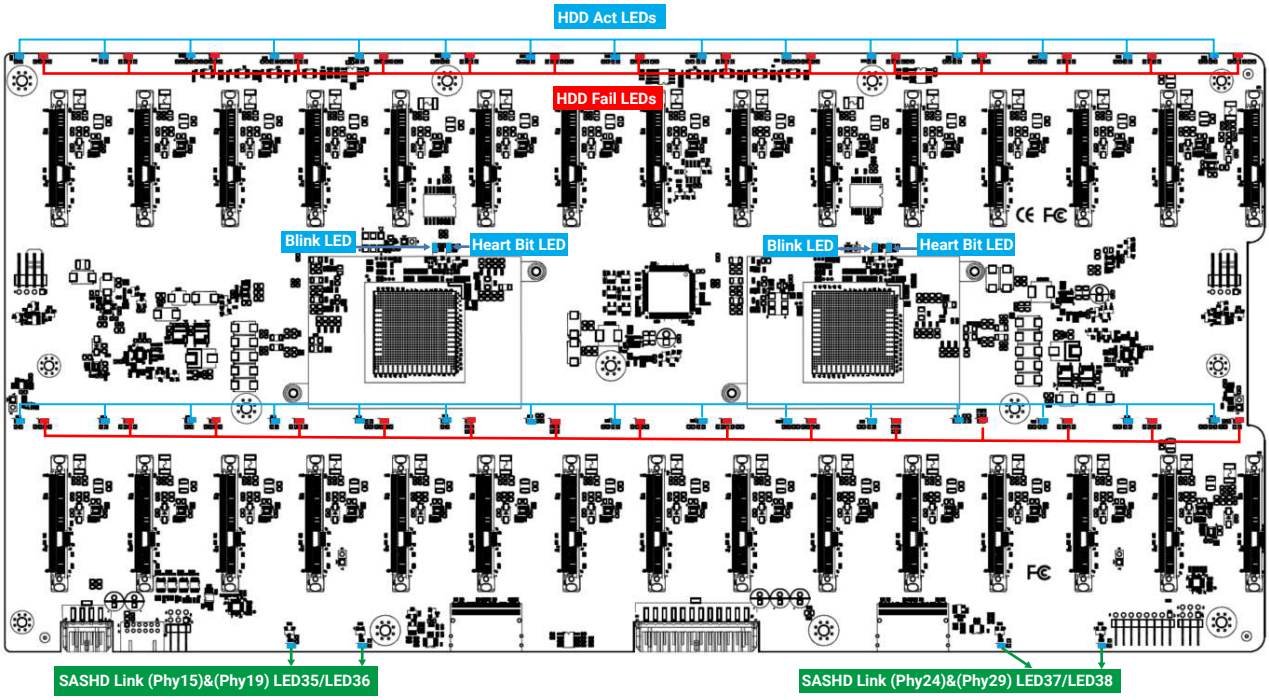
DBG_SIRXD	2	1	SM_SIRXD
GND	4	3	GND
DBG_SITXD	6	5	SM_SITXD

Front LED Board Control for Display HDD LED Status (LED-BD1)



+3V3	1	2	+5V
SLOAD2	3	4	SDATAOUT2
SCLOCK2	5	6	GND
SLOAD1	7	8	SDATAOUT1
SCLOCK1	9	10	CPLD SDA
CPLD SCL	11	12	GND

2.11.3 LED Indicator

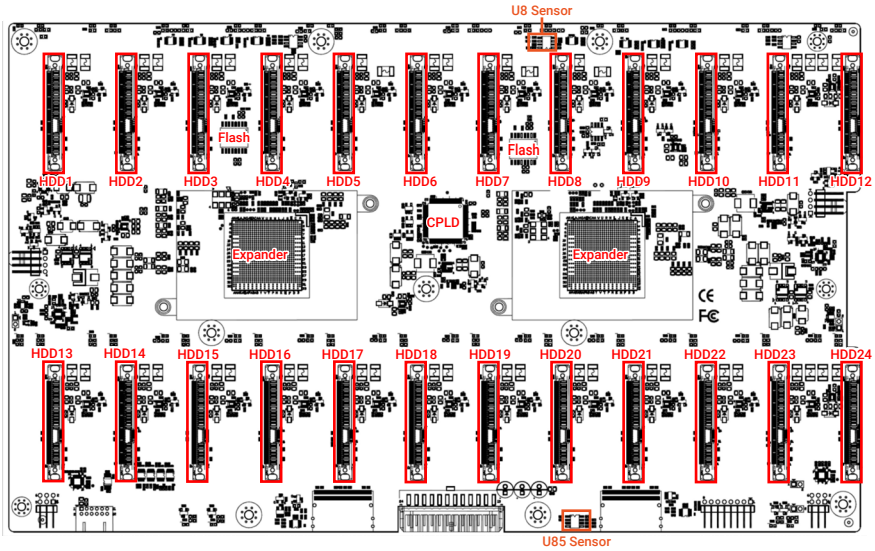


Indicator	Color	Behavior	Description
SAS PHY Link Status (LED35/LED36) (LED37/LED38)	Blue	On	Link up
		Blinking	Activity is detected
		Off	Link down
Expander Blink (LED33) (LED34)	Blue	Blinking	Expander alive, 0.0833Hz (12 seconds per cycle)
Expander HeartBit (LED32) (LED31)	Blue	Blinking	Expander FW running
HDD Activity LEDs	Blue	On	HDD present
		Blinking	HDD Activity detected: 8Hz
		Off	HDD Locate: 0.5Hz
HDD Fault/Status LEDs	Red	On	Set by any of the following bits: 1. RQST MISSING 2. RQST FAULT
		Blinking	Set by any of the following bits: 1. RQST CONS CHECK 2. RQST IN CRIT ARRAY 3. RQST IN FAILED ARRAY 4. RQST REBUILD/REMAP 5. RQST R/R ABORT 6. RQST INSERT 7. RQST REMOVE 8. PRDFAIL
		Off	No control bit is set or set by any of the following bits: 1. RQST OK 2. RQST RSVD DEVICE 3. RQST HOT SPARE 4. RQST ACTIVE 5. DO NOT REMOVE 6. RQST IDENT 7. DEVICE OFF

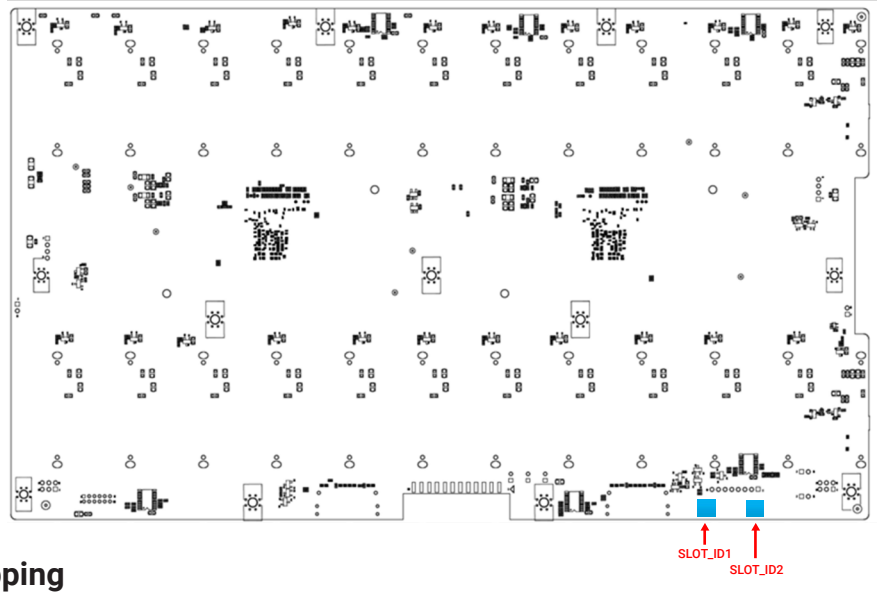
2.12 Drive Backplane: 24 Bay

2.12.1 Placement

Top view



Bottom view



SAS PHY Mapping

	HDD1	HDD2	HDD3	HDD4	HDD5	HDD6	HDD7	HDD8	HDD9	HDD10	HDD11	HDD12
Primary	phy-05	phy-04	phy-03	phy-02	phy-01	phy-00	phy-31	phy-30	phy-29	phy-28	phy-27	phy-26
Secondary	phy-05	phy-04	phy-03	phy-02	phy-01	phy-00	phy-31	phy-30	phy-29	phy-28	phy-27	phy-26

Primary U46

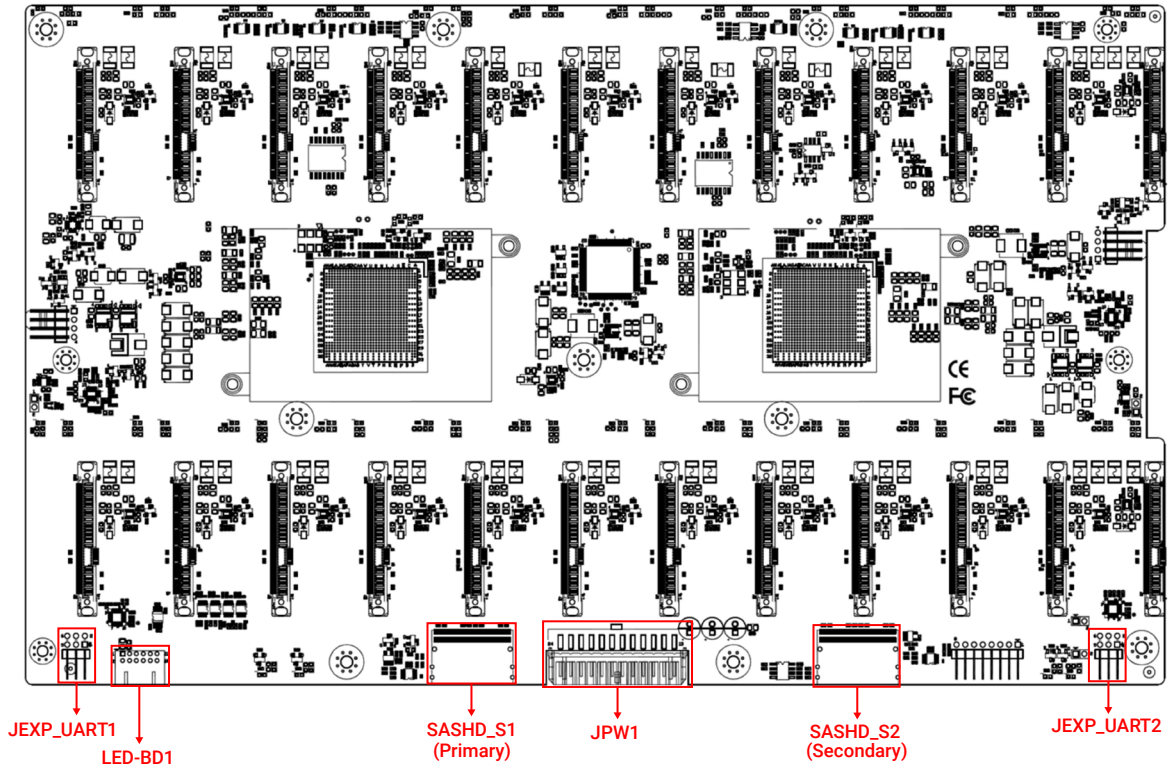
Secondary U47

	HDD13	HDD14	HDD15	HDD16	HDD17	HDD18	HDD19	HDD20	HDD21	HDD22	HDD23	HDD24
Primary	phy-06	phy-07	phy-08	phy-09	phy-18	phy-19	phy-20	phy-21	phy-22	phy-23	phy-24	phy-25
Secondary	phy-06	phy-08	phy-07	phy-10	phy-09	phy-11	phy-12	phy-13	phy-18	phy-23	phy-24	phy-25

About JBOD slot mapping, please refer to 2.7 Drive Slot Map.

2.12.2 Connector

Location



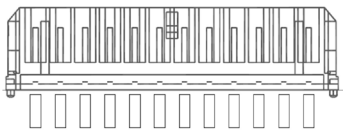
External Connectors

Connector Function	Physical Description	Comments
HDD1~24	SFF-8654 SAS Receptacle(SMT H:14.15mm)	HDD connector

Internal Connectors

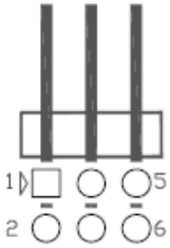
Connector Function	Physical Description	Comments
Power Supply (JPW1)	15 x 2 Pin Power Connector	12V. 4.5 A per pin.
SAS SlimLine (SASHD_S1) (SASHD_S2)	74 pin 8i SAS SlimLine	SAS Host connection
UART (JEXP_UART1) (JEXP_UART2)	3 x 2 Pin Header	Expander SMART/DEBUG port.
LED Board (LED-BD1)	6 x 2 Pin Header	Connect to Front LED Board

Power Connector (JPW1)



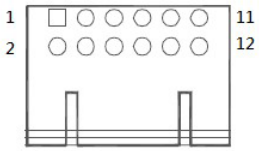
GND	13	1	GND
GND	14	2	GND
GND	15	3	GND
GND	16	4	GND
GND	17	5	GND
GND	18	6	GND
+12V	19	7	+12V
+12V	20	8	+12V
+12V	21	9	+12V
+12V	22	10	+12V
+12V	23	11	+12V
+12V	24	12	+12V

Control for Expander (JEXP_UART1/ JEXP_UART2)



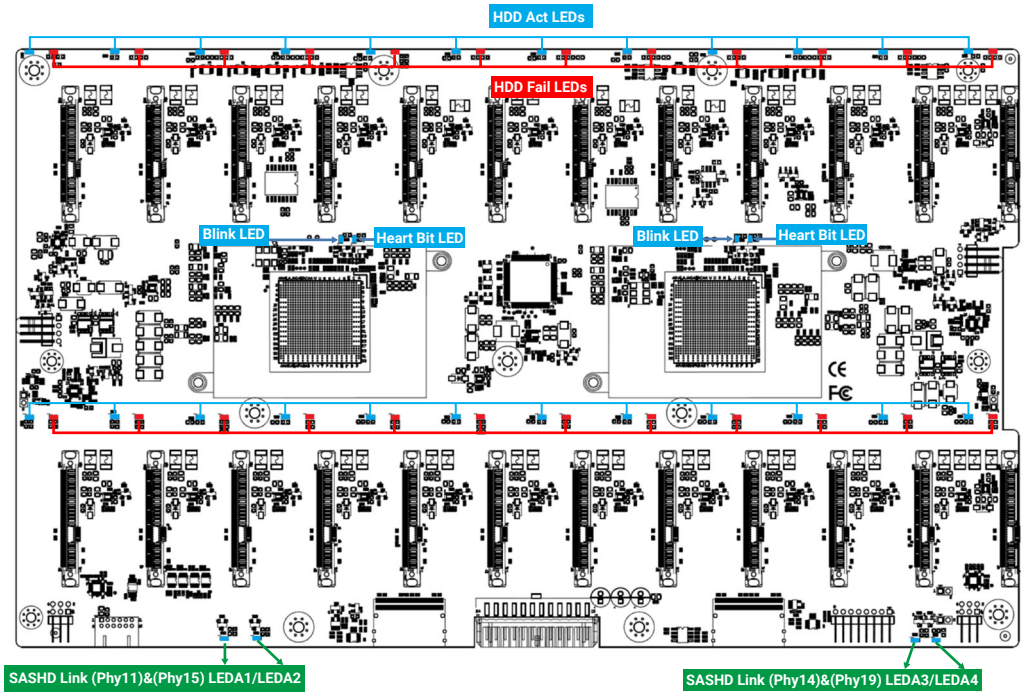
DBG_SIRXD	2	1	SM_SIRXD
GND	4	3	GND
DBG_SITXD	6	5	SM_SITXD

Front LED Board Control for Display HDD LED Status (LED-BD1)



+3V3	1	2	+5V
SLOAD2	3	4	SDATAOUT2
SCLOCK2	5	6	GND
SLOAD1	7	8	SDATAOUT1
SCLOCK1	9	10	CPLD SDA
CPLD SCL	11	12	GND

2.12.3 LED Indicator

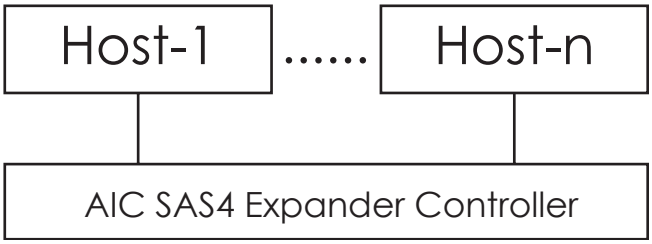


Indicator	Color	Behavior	Description
SAS PHY Link Status (LEDA1/LEDA2) (LEDA3/LEDA4)	Blue	On	Link up
		Blinking	Activity is detected
		Off	Link down
Expander Blink (LED27) (LED25)	Blue	Blinking	Expander alive, 0.0833Hz (12 seconds per cycle)
Expander HeartBit (LED28) (LED26)	Blue	Blinking	Expander FW running
HDD Activity LEDs	Blue	On	HDD present
		Blinking	HDD Activity detected: 8Hz
		Off	HDD Locate: 0.5Hz
HDD Fault/Status LEDs	Red	On	Set by any of the following bits: 1. RQST MISSING 2. RQST FAULT
		Blinking	Set by any of the following bits: 1. RQST CONS CHECK 2. RQST IN CRIT ARRAY 3. RQST IN FAILED ARRAY 4. RQST REBUILD/REMAP 5. RQST R/R ABORT 6. RQST INSERT 7. RQST REMOVE 8. PRDFAIL
		Off	No control bit is set or set by any of the following bits: 1. RQST OK 2. RQST RSVD DEVICE 3. RQST HOT SPARE 4. RQST ACTIVE 5. DO NOT REMOVE 6. RQST IDENT 7. DEVICE OFF

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® SAS4 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 (4U78swapHub) to locate a drive.

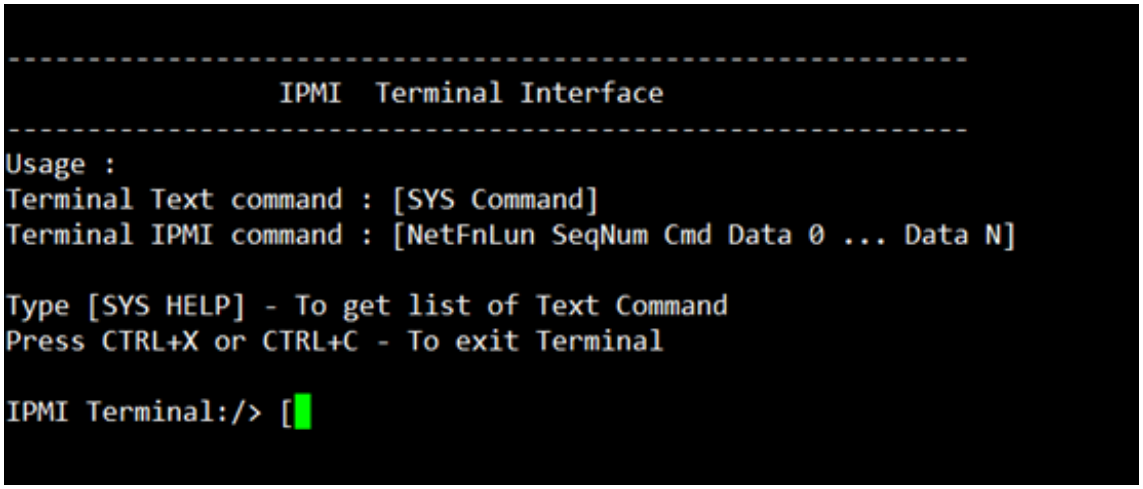
3.1.2 Unsupported Feature

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.

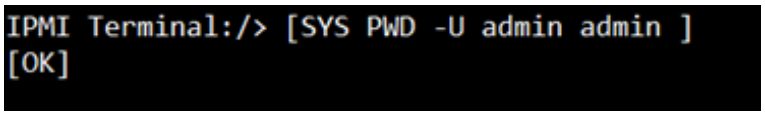
Chapter 4. BMC Configuration Settings

4.1 Login

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



Type command for login the interface.
#[sys pwd –u admin admin]
It will response [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 00 ]
[1C 00 47 00]
```

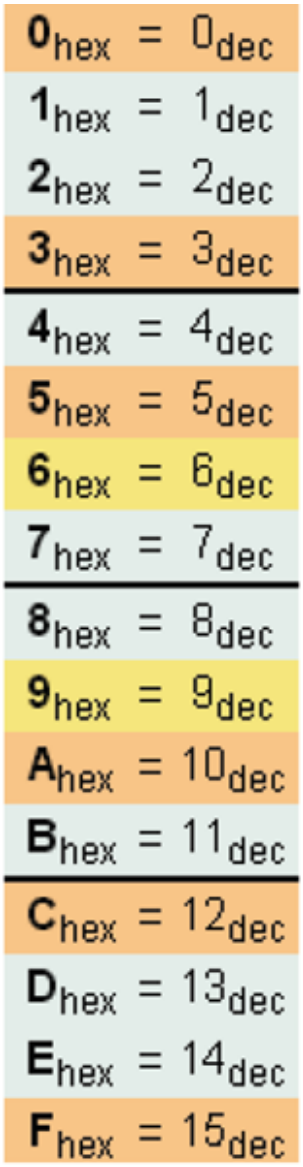
   Retry to login the interface.

   #[sys pwd –u admin 12345678]

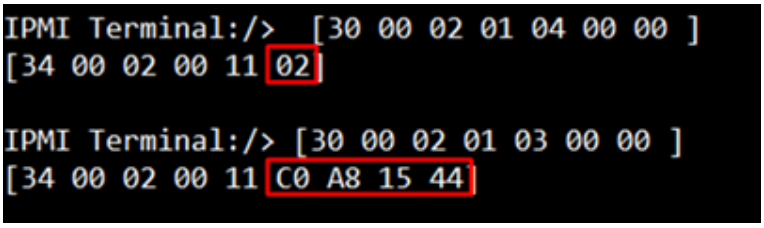
   It will response [OK]

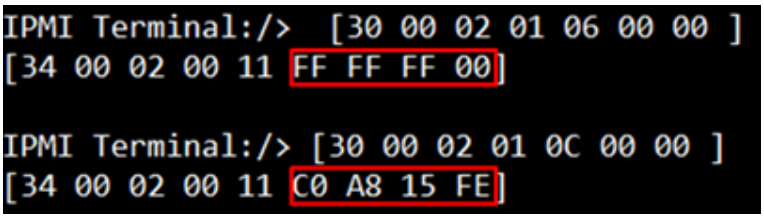
```
IPMI Terminal:/> [SYS PWD -U admin 12345678 ]
[OK]
```

3. Find LAN information.



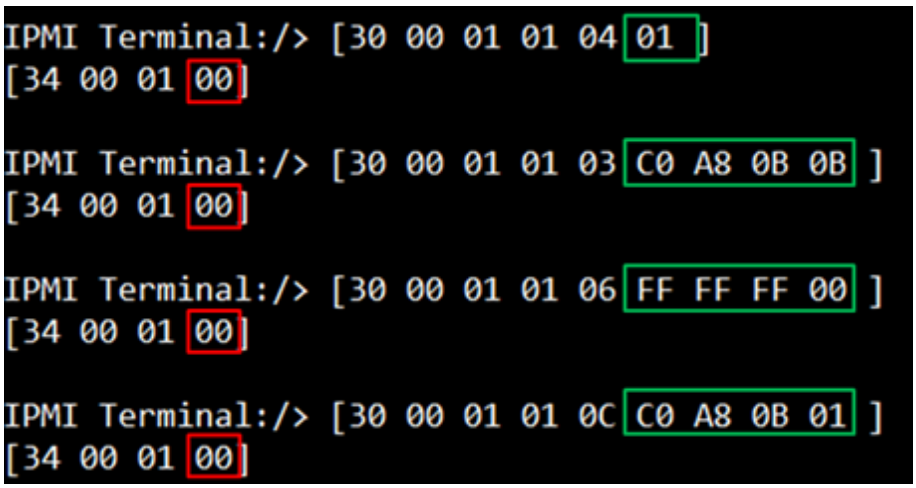
Find LAN static IP /DHCP [30 00 02 01 04 00 00]
LAN static IP /DHCP: 01 is static IP and 02 is DHCP.
Find LAN IP [30 00 02 01 03 00 00]
Find submask [30 00 02 01 06 00 00]
Find gateway [30 00 02 01 0C 00 00]





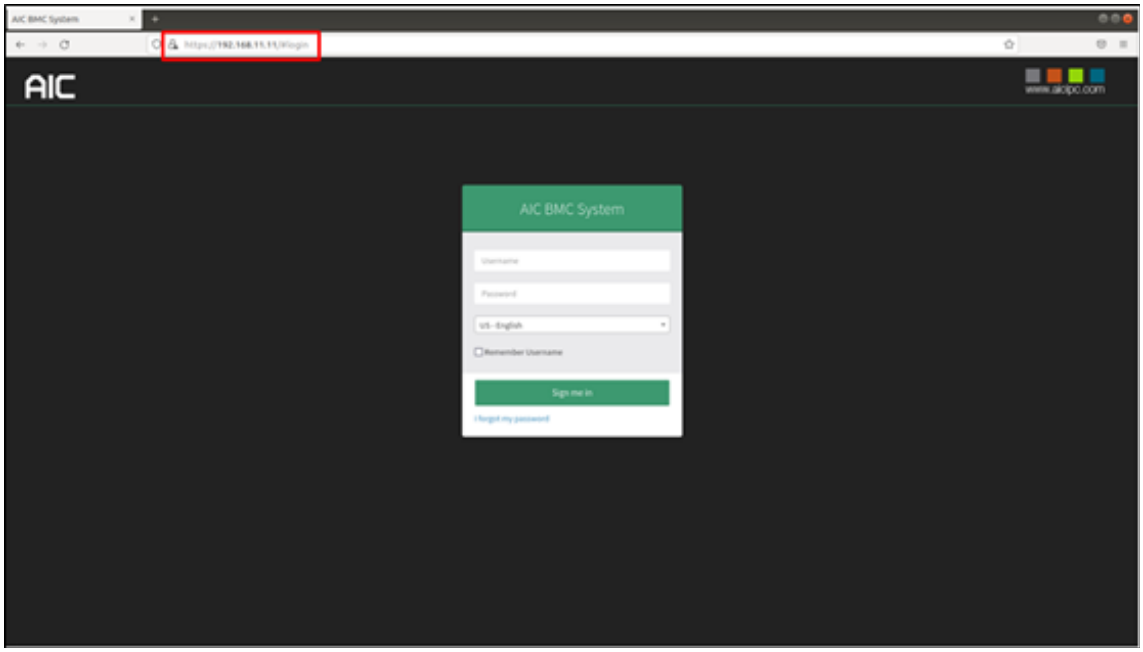
The red box represents hexadecimal digits. According to the left figure, the IP is 16*12 + 0 = 192, 16*10 + 8 = 168, 16*1 + 5 = 21, 16*4 + 4 = 68. Therefore, the IP is 192.168.21.68

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 0B 01]



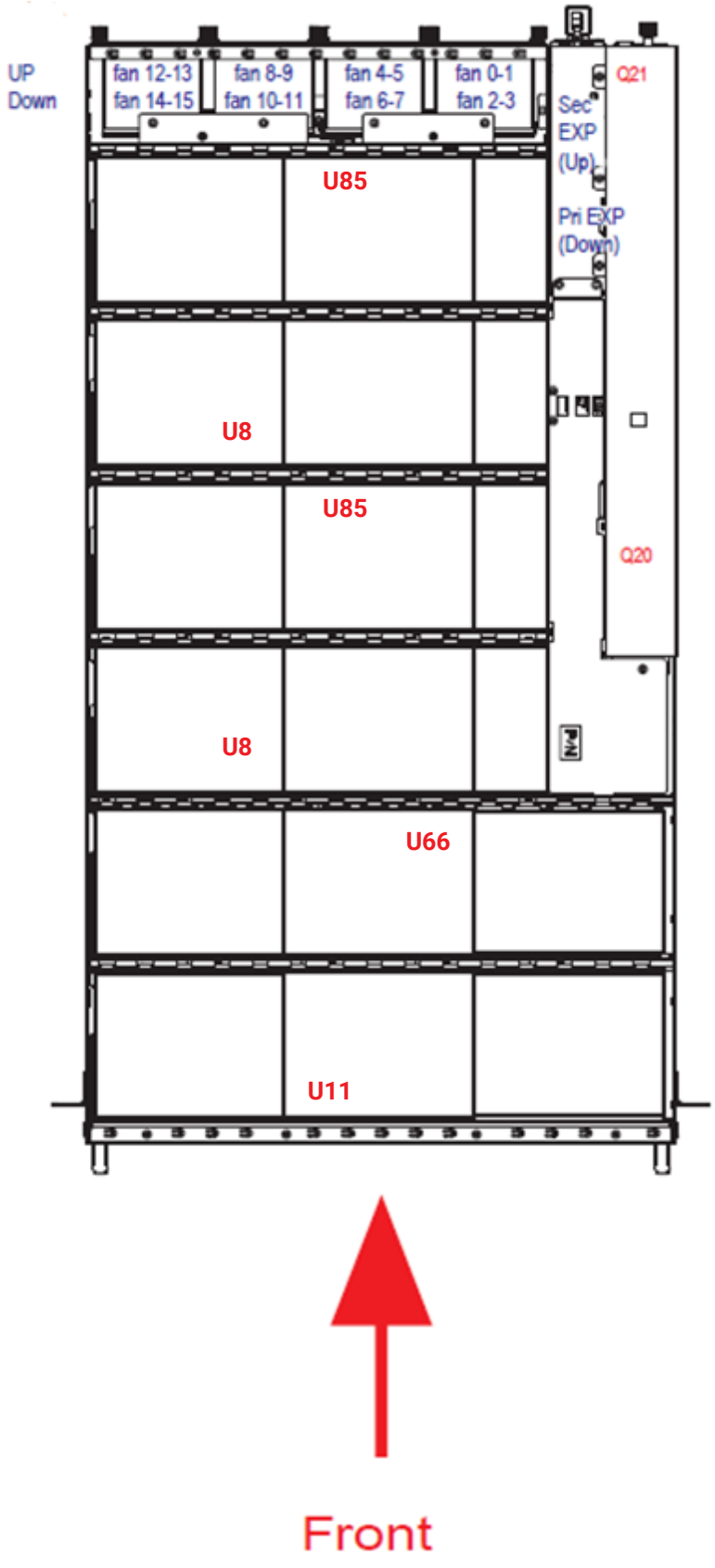
   The digit in the red box is completion code.
   00 represents the confirmed code.
   The digits in the green box are can be configured to any value.
   If you want to change the IP address, you must set the **LAN status to static**.

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

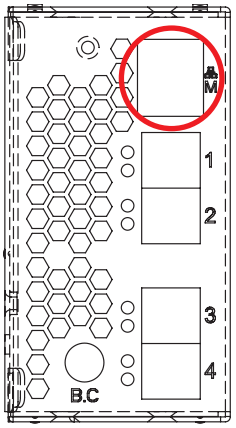
EXP: expander chip



4.3 Expander Setting via 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 Initiate SOL. Use one of the methods below to configure the expander setting.

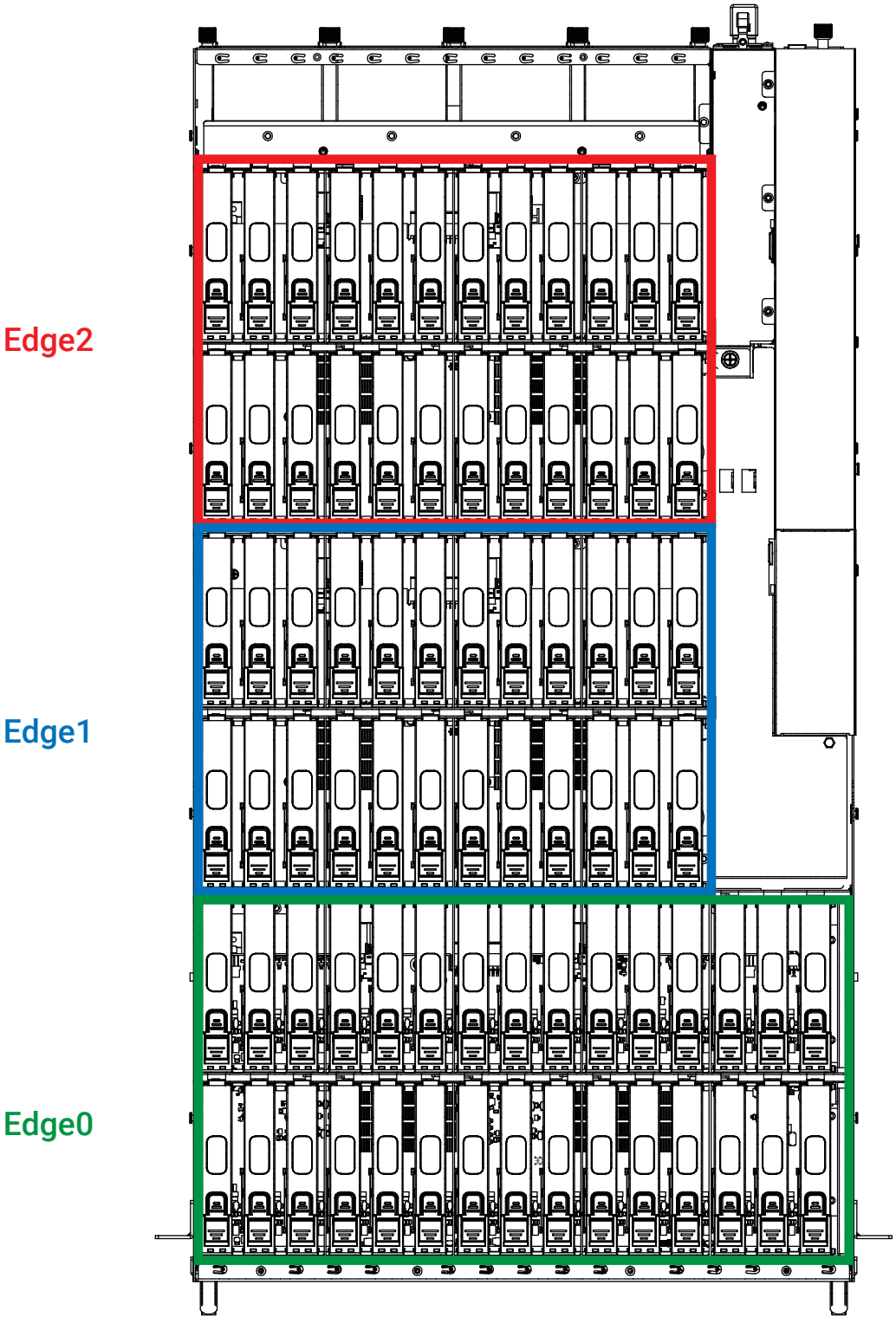
4.3.1 SOL

There are two methods to initiate Sol.

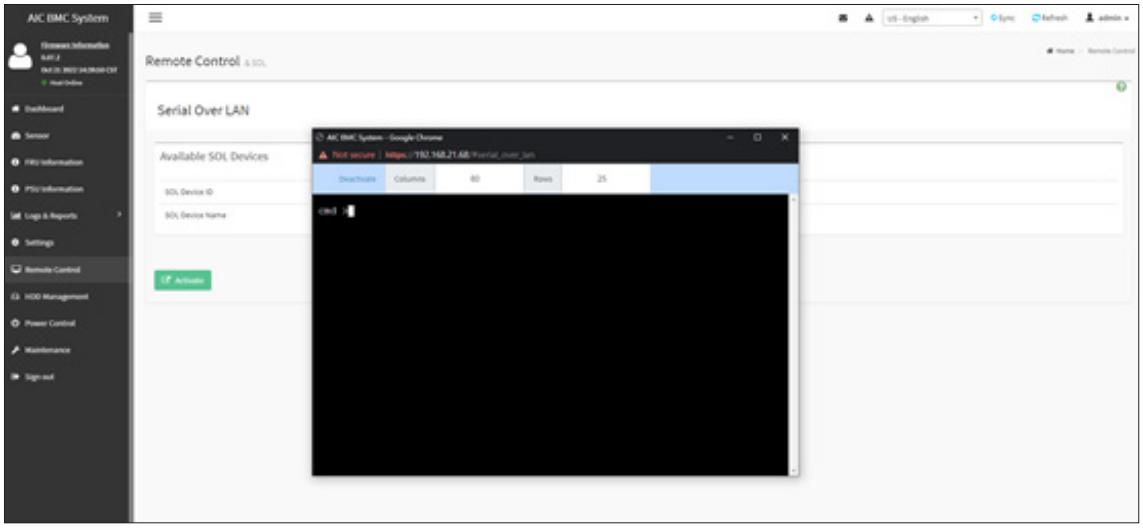
Method 1

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

Edge0, Edge1, Edge2 Top View Location



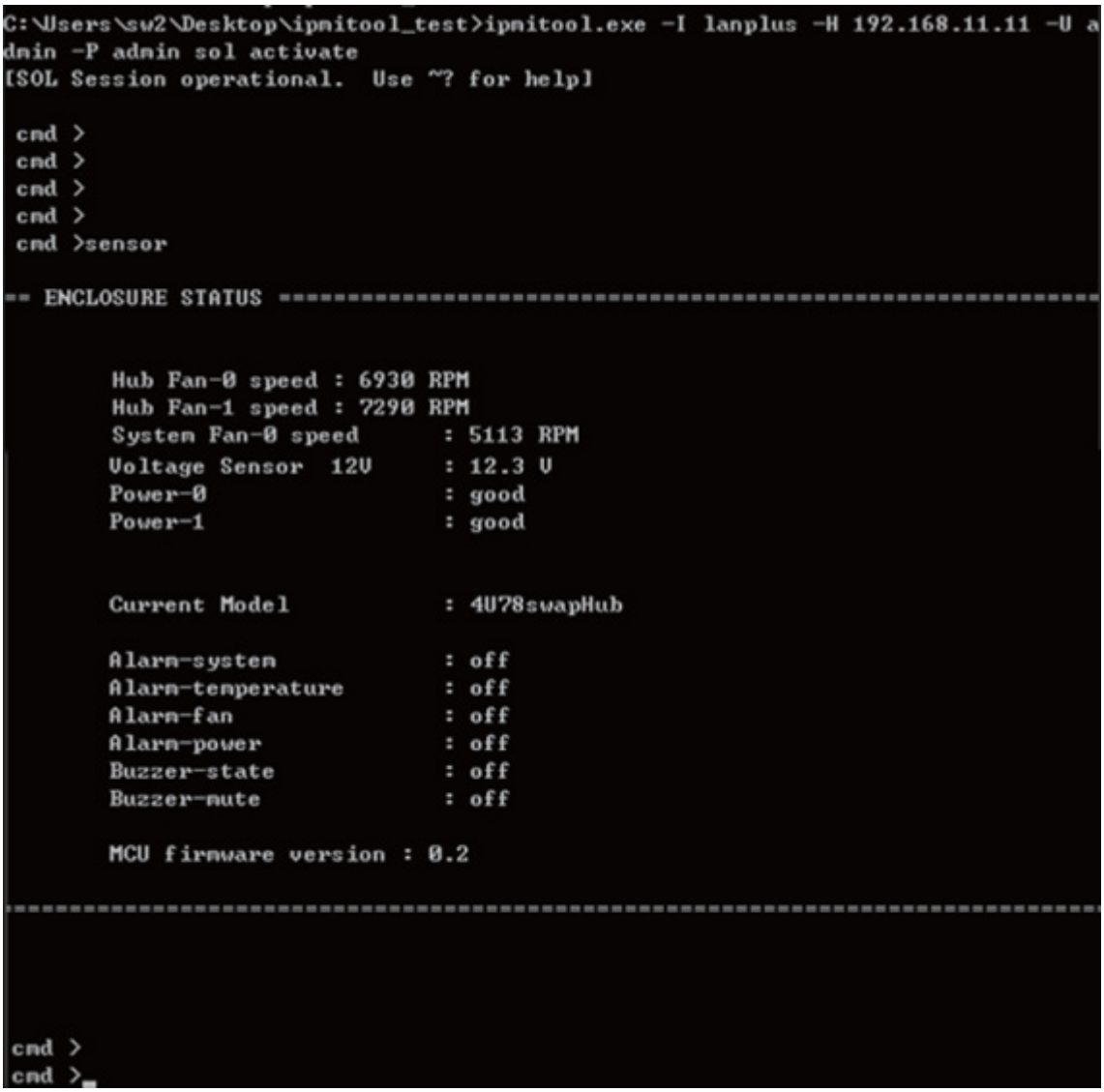
2. Now you can use the expander smart console via BMC SOL.



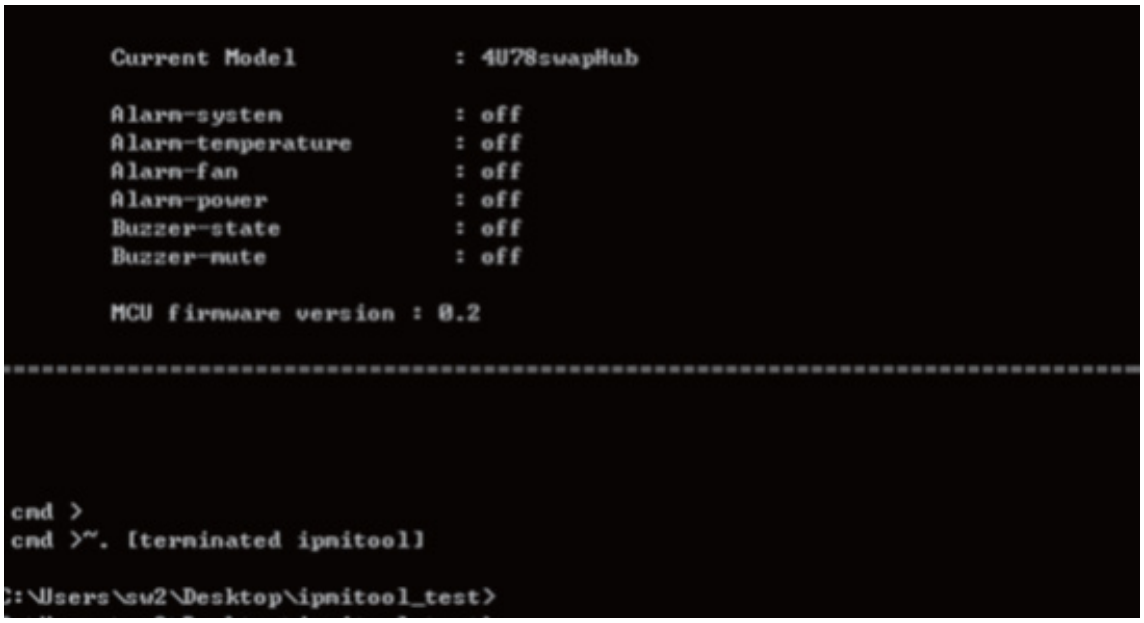
Method 2

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

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



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



3. If you want 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

> **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 **4.4.8.10 Zone Configurations** 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.

4.3.2.1 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 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 <=> 30

```
 cmd >
 cmd >phyinfo
                      SSSSSSS                                                    EE
                  PHY STSMSTMA                          ZONE      CONN CONN MAP DR
PHY  DEV       NLR CNG PPPPPPT                   ROUTE ZONE CTRL CONN ELEM PHY  PHY FR
ID   TYPE      CNT CNT IIITTTA ATTACHED SAS ADDR TYPE  GRP  BUS  TYPE INDX LINK ID  BL

00         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 000 11
01         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 001 11
02         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 002 11
03         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 003 11
04         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 004 11
05         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 005 11
06         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 006 11
07         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 007 11
08         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 008 11
09         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 009 11
10         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 010 11
11         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 011 11
12         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 012 11
13         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 013 11
14         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 014 11
15         0x0 0x03 -------                      T   0x01 0x04 0x00 0x00 0x00 015 11
16   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 016 --
17   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 017 --
18   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 018 --
19   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 019 --
20   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 020 --
21   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 021 --
22   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 022 --
23   EXP 22.5G 0x04 -----1- 50015B21_685A7B3F    T   0x01 0x04 0x00 0x00 0x00 023 --
24   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 024 --
25   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 025 --
26   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 026 --
27   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 027 --
28   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 028 --
29   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 029 --
30   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 030 --
31   EXP 22.5G 0x04 -----1- 50015B21_685A623F    T   0x01 0x04 0x00 0x00 0x00 031 --
32   EXP 22.5G 0x04 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 032 --
33   EXP 22.5G 0x04 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 033 --
34   EXP 22.5G 0x04 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 034 --
35   EXP 22.5G 0x04 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 035 --
36   EXP 22.5G 0x04 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 036 --
37   EXP 22.5G 0x04 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 037 --
38   EXP 22.5G 0x04 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 038 --
39   EXP 22.5G 0x04 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 039 --
40   EXP 22.5G 0x06 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 040 --
41   EXP 22.5G 0x06 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 041 --
42   EXP 22.5G 0x06 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 042 --
43   EXP 22.5G 0x06 -----1- 50015B21_685A8D3F    T   0x01 0x04 0x00 0x00 0x00 043 --
44   EXP 22.5G 0x06 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 044 --
45   EXP 22.5G 0x06 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 045 --
46   EXP 22.5G 0x06 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 046 --
47   EXP 22.5G 0x06 -----1- 50015B21_685A853F    T   0x01 0x04 0x00 0x00 0x00 047 --
SXP0 END 22.5G 0x01 --11--- 50015B23_68E6893D    D   0x01 0x04 0x2F 0x6D 0x00 048
SXP1 END 22.5G 0x01 1----1- 50015B23_68E6893F    D   0x01 0x04 0x00 0x00 0x00 049
SXP2 END 22.5G 0x01 -1----- 50015B23_68E6893E    D   0x01 0x04 0x00 0x00 0x00 050
SXP3       0x0 0x00 -------                      D   0x00 0x04 0x00 0x00 0x00 051

Expander Change Count:  00c7
Zone Configuring:  0
Self Configuring:  0
Configuring:  0
```

Edge0, Edge1, Edge2 Top View Location

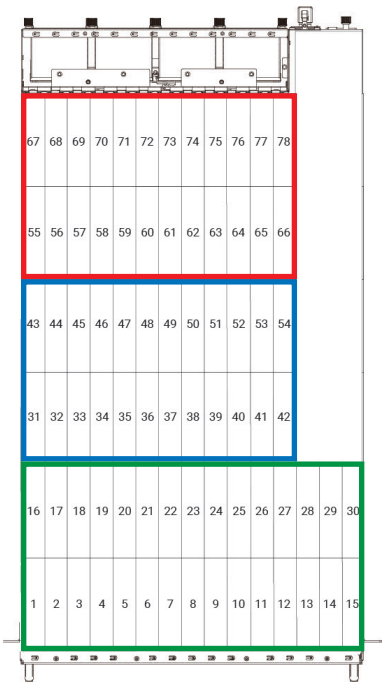


Table 1 **Edge2 PHY ID to JBOD slot number**

slot 67	slot 68	slot 69	slot 70	slot 71	slot 72	slot 73	slot 74	slot 75	slot 76	slot 77	slot 78
PHY 25	PHY 24	PHY 23	PHY 22	PHY 21	PHY 20	PHY 19	PHY 18	PHY 09	PHY 08	PHY 07	PHY 06
slot 55	slot 56	slot 57	slot 58	slot 59	slot 60	slot 61	slot 62	slot 63	slot 64	slot 65	slot 66
PHY 26	PHY 27	PHY 28	PHY 29	PHY 30	PHY 31	PHY 00	PHY 01	PHY 02	PHY 03	PHY 04	PHY 05

Table 2 **Edge1 PHY ID to JBOD slot number**

slot 43	slot 44	slot 45	slot 46	slot 47	slot 48	slot 49	slot 50	slot 51	slot 52	slot 53	slot 54
PHY 25	PHY 24	PHY 23	PHY 22	PHY 21	PHY 20	PHY 19	PHY 18	PHY 09	PHY 08	PHY 07	PHY 06
slot 31	slot 32	slot 33	slot 34	slot 35	slot 36	slot 37	slot 38	slot 39	slot 40	slot 41	slot 42
PHY 26	PHY 27	PHY 28	PHY 29	PHY 30	PHY 31	PHY 00	PHY 01	PHY 02	PHY 03	PHY 04	PHY 05

Table 3 **Edge0 PHY ID to JBOD slot number**

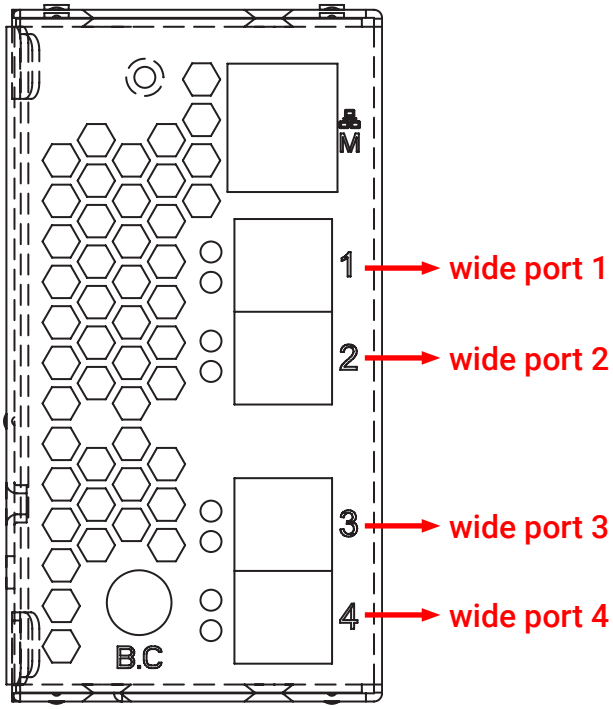
slot 16	slot 17	slot 18	slot 19	slot 20	slot 21	slot 22	slot 23	slot 24	slot 25	slot 26	slot 27	slot 28	slot 29	slot 30
PHY 29	PHY 28	PHY 27	PHY 26	PHY 25	PHY 24	PHY 23	PHY 22	PHY 21	PHY 20	PHY 11	PHY 10	PHY 09	PHY 08	PHY 07
slot 1	slot 2	slot 3	slot 4	slot 5	slot 6	slot 7	slot 8	slot 9	slot 10	slot 11	slot 12	slot 13	slot 14	slot 15
PHY 30	PHY 31	PHY 32	PHY 33	PHY 34	PHY 35	PHY 36	PHY 37	PHY 38	PHY 39	PHY 02	PHY 03	PHY 04	PHY 05	PHY 06

For example, to assign JBOD slot 1-4 (PHY30/PHY31/PHY32/PHY33) for group 8.

cmd> phyzone on
cmd> phyzone 30 08
cmd> phyzone 31 08
cmd> phyzone 32 08
cmd> phyzone 33 08

```
cmd >
cmd >phyzone on

Succeeded to enable zoning


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 32 08

Succeeded to set zone group for the phy


cmd >phyzone 33 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 on
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.

4.3.2.2 How to get all revisions in AIC® SAS 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

4.3.2.3 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

4.3.2.4 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 due to the RAID card limitation.

4.3.2.5 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

4.3.2.6 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

4.3.2.7 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

4.3.2.8 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

4.3.2.9 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 4U78swap before configuring zone count. Power the 4U78swap swap off after configuring zone count. Power on the 4U78swap, and then insert the SAS cable.

Three zone configurations supported are one zone, two 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 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	1~78

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

HUB:

Zone #	1	2
Wideport	1, 2	3, 4

EDGE:

Zone #	1	2
Slot	1~39	40~78

(C-3) 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	1~20	21~40	41~60	61~78

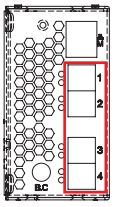
Zone Count

Zone count 1:

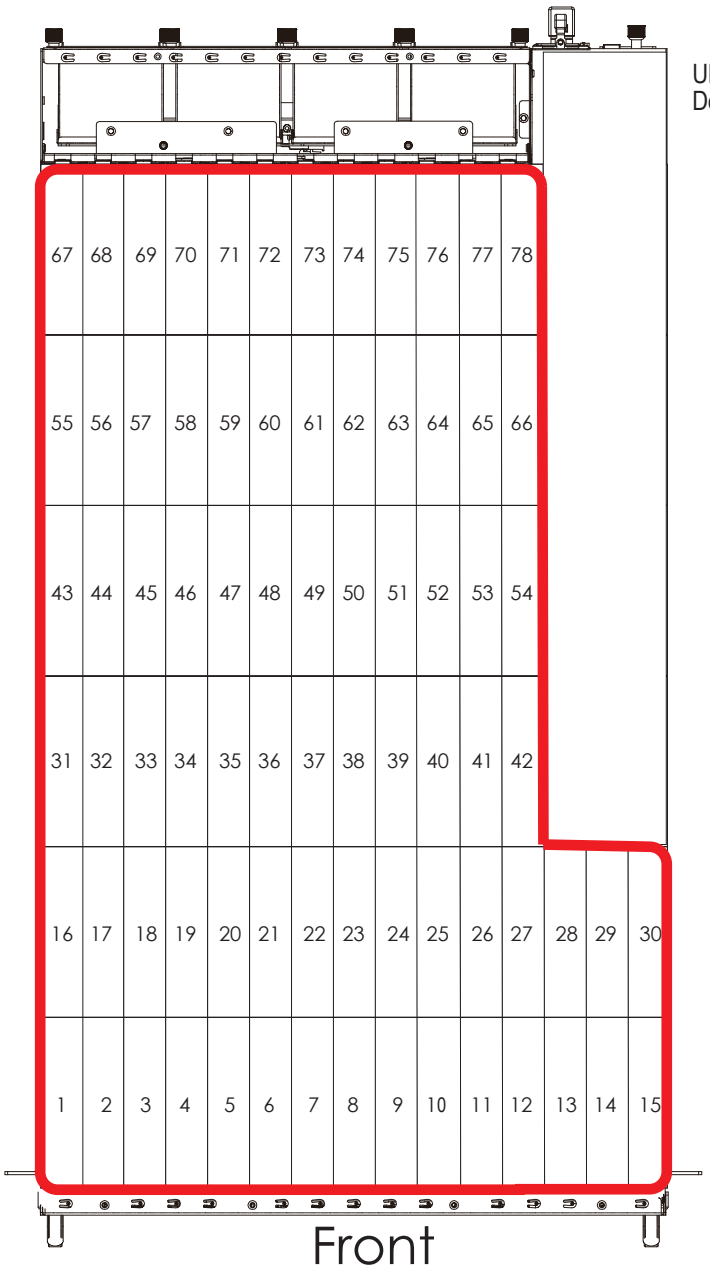
78 drives per zone. All SFF-8644 ports and drives are at the same zone group.

SEE FIGURE BELOW.

Expander rear panel

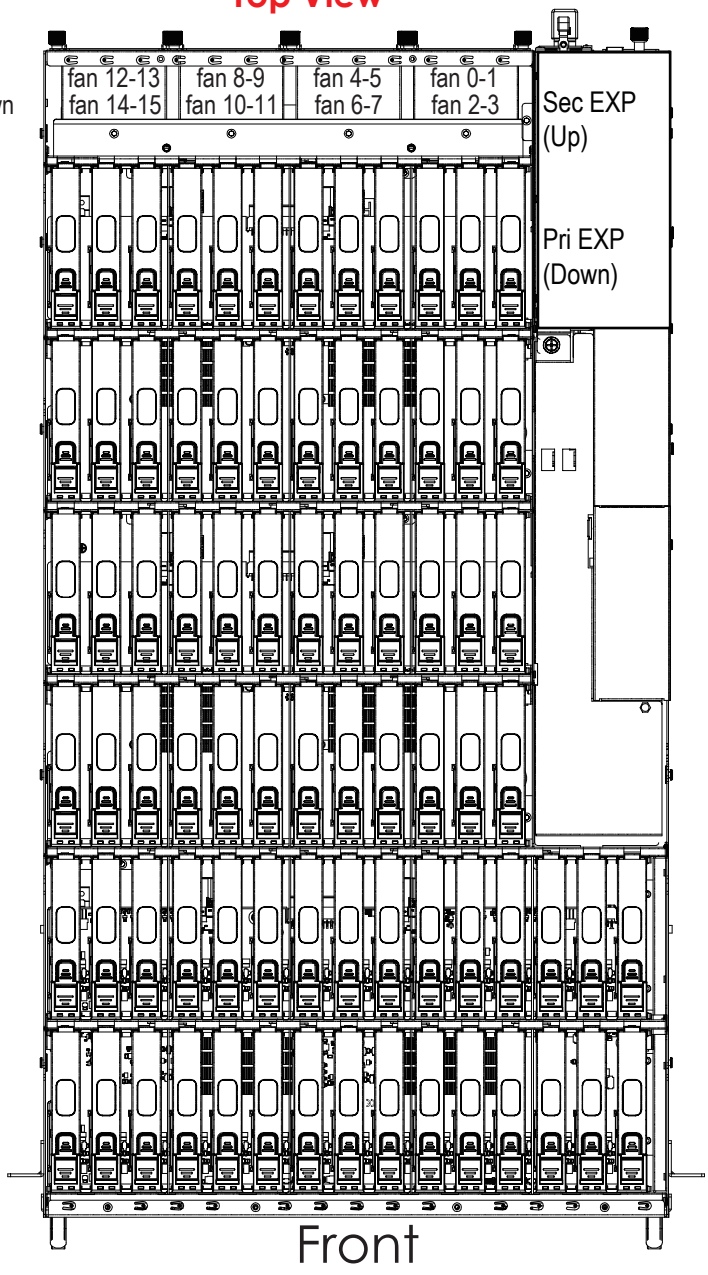


Group 1



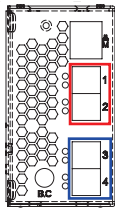
UP
Down

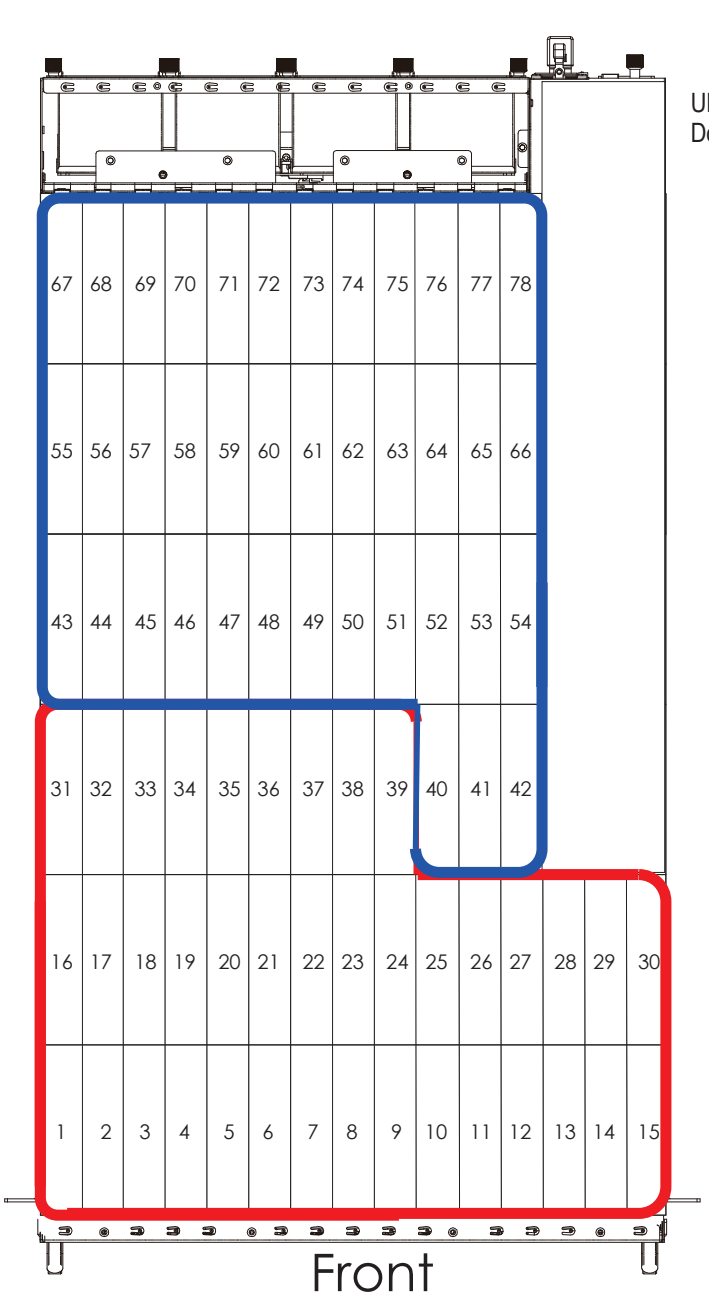
Top View



Zone count 2:
39 drives per zone. Port 1 & 2 is in zone group 1. Port 3 & 4 is in zone group 2.
SEE FIGURE BELOW.

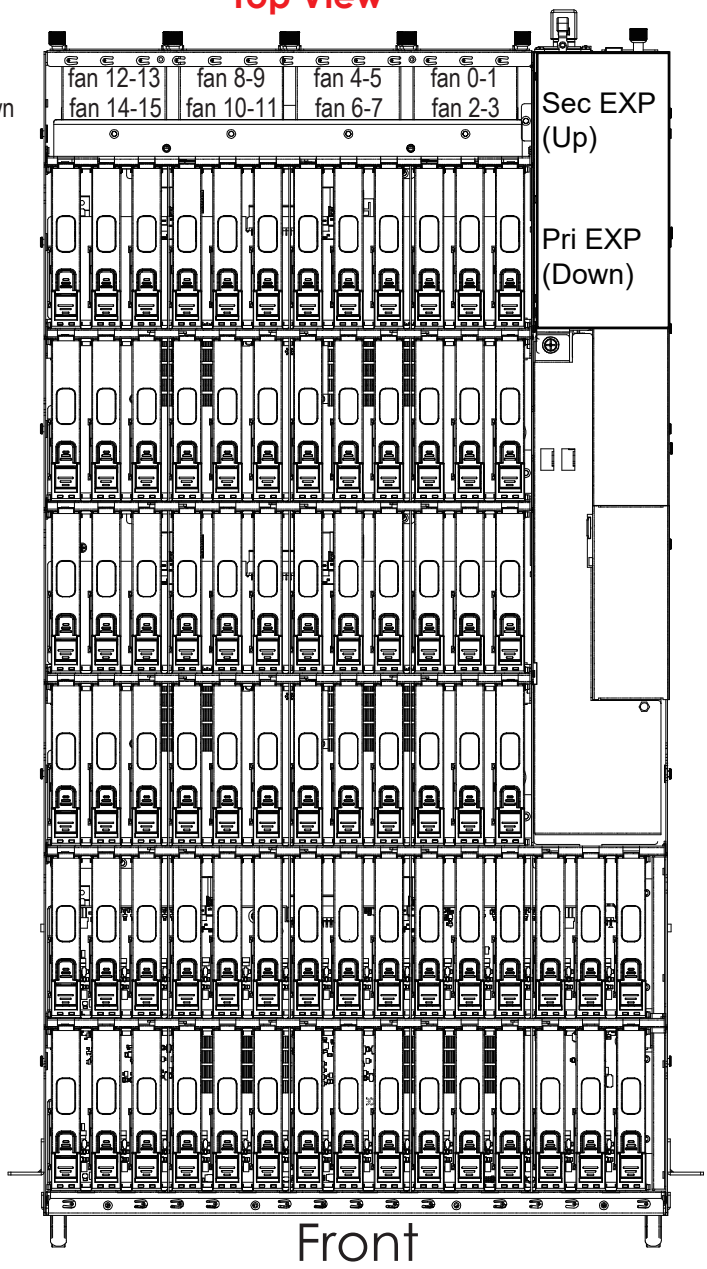
Expander rear panel





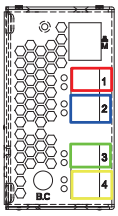
UP
Down

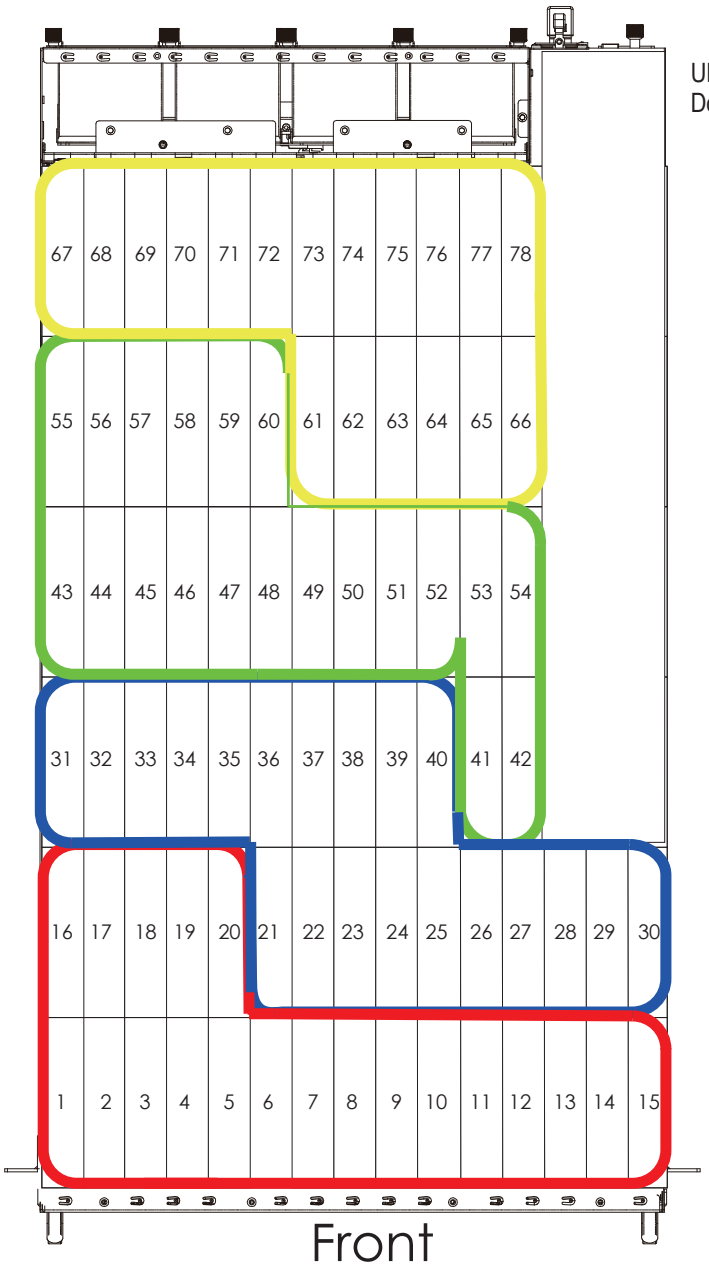
Top View



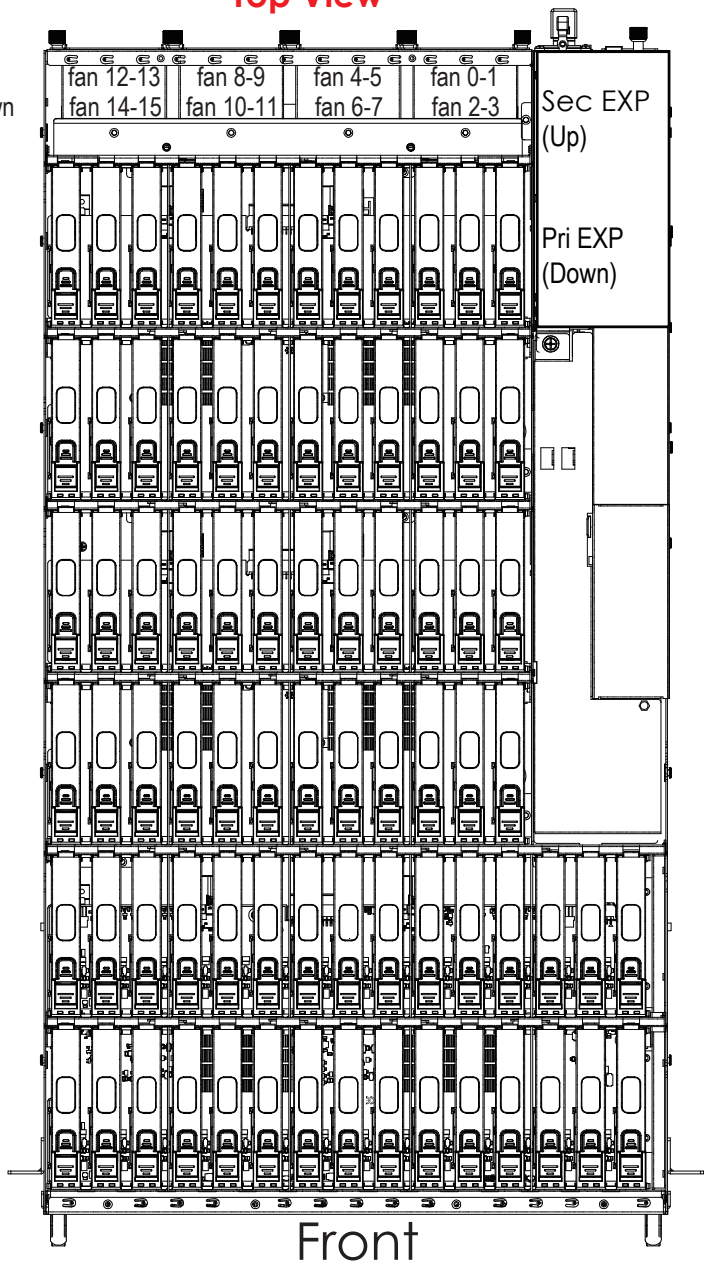
Zone count 4:
20 drives per zone. Port 1 is in at zone group 1. Port 2 is in zone group 2. Port 3 is in zone group 3. Port 4 is at zone group 4.
SEE FIGURE BELOW.

Expander rear panel





Top View



4.3.2.10 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

4.3.2.11 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, J4078-01-35X 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

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							

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								
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	RQST 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.
ACTUAL SPEED CODE	Speed code level bases on current fan RPM.

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 REBULD/ 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 REBULD/ 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 (12G Edge) Slow Blink (24G Edge)
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 REBULD/ 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      4U78swapEdge       0c31
```

(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 due to the 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      24G 4U78swapHub       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

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	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 24G 4U78swapHub 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 24G      4U78swapHub       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 24G 4U78swapHub 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 SysCoolingElement00 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

Enclosure 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 REBULD/ 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 edges 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 all the other edges. 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
```
$ sg_map -i
/dev/sg2    AIC      24G 4U78swapHub       0c30
```

(B) Set "Reserved2" of Disk001 to make the Edge0 visible.
Disk001 for Edge0, Disk031 for Edge1 and Disk055 for Edge2.
```
$ sg_ses --descriptor=Disk001 --set=2:5:1 /dev/sg1
```

(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: Edge0 in Linux
```
$./g3Xflash -i 500605b0000272bf reset exp
```

(E) Show the devices for the Hub and the Edge0
$ sg_map -i

/dev/sg1 AIC 24G 4U78swapHub 0c30
/dev/sg2 AIC 12G 4U78swapEdge0 0c31

(F) Update firmware of the Edge0
$ sg_write_buffer --id=0x0 --in=<firmware filename> --mode=0x2 --offset=0 /dev/sg2

(G) Update MFG of the Edge0
$ sg_write_buffer --id=0x83 --in=<MFG filename> --mode=0x2 --offset=0 /dev/sg2

(H) Get SAS address of Edge0. The SAS address (50015B20:9000EBBF) is used 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/sg1

(L) Reset the Hub to refresh the change of the Edge0 in Linux
$./g3Xflash -i 500605b0000272bf reset exp

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)
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

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       Event1             Event2             Event3             Event4
Id    -----------------  -----------------  -----------------  -------------
          InvWrdCnt          DispErrCnt         LossSyncCnt        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 >
```

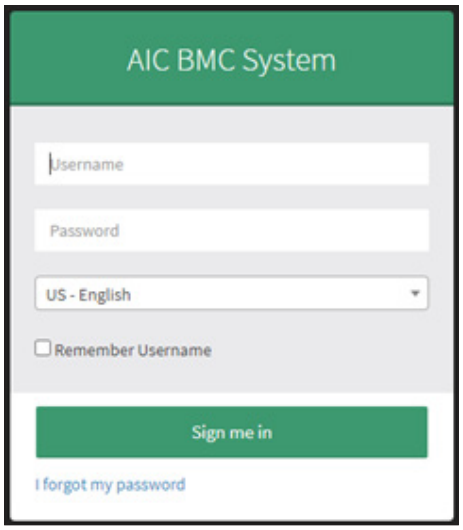
6. Type in “counters” to execute counters command.

```
        Current Model           : 4U78swapEdge1

================================================================================



 cmd >counters

================================================================================

Phy Layer Error Counters
================================================================================

PHY       Event1            Event2            Event3            Event4
Id   ----------------  ----------------  ----------------  ---------------
         InvWrdCnt          DispErrCnt        LossSyncCnt       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
================================================================================



================================================================================

Generic Broadcast Counter
================================================================================

Broadcast Counter Not Configured.

================================================================================



 cmd >
```

4.4 Web UI

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.

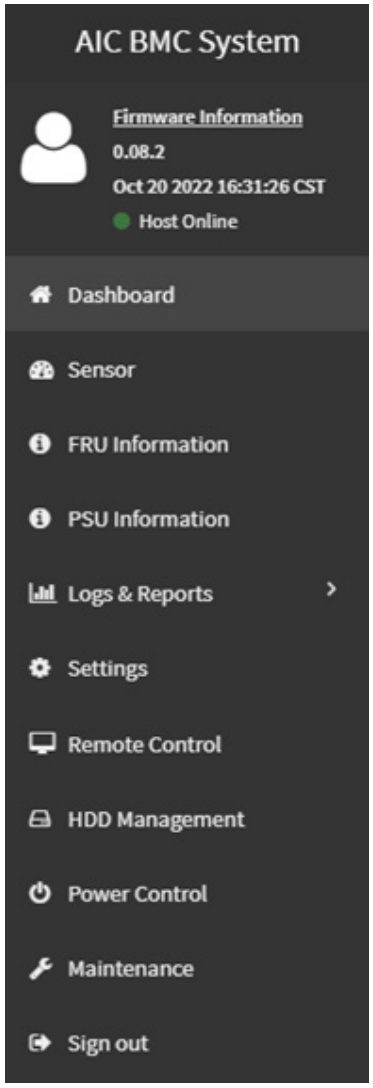
Remember Username: Check this option to remember your login Username. If you select this option, the browser will save your credentials internally in its memory, and when you open that site the next time, it will auto-fill Username for you.

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



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

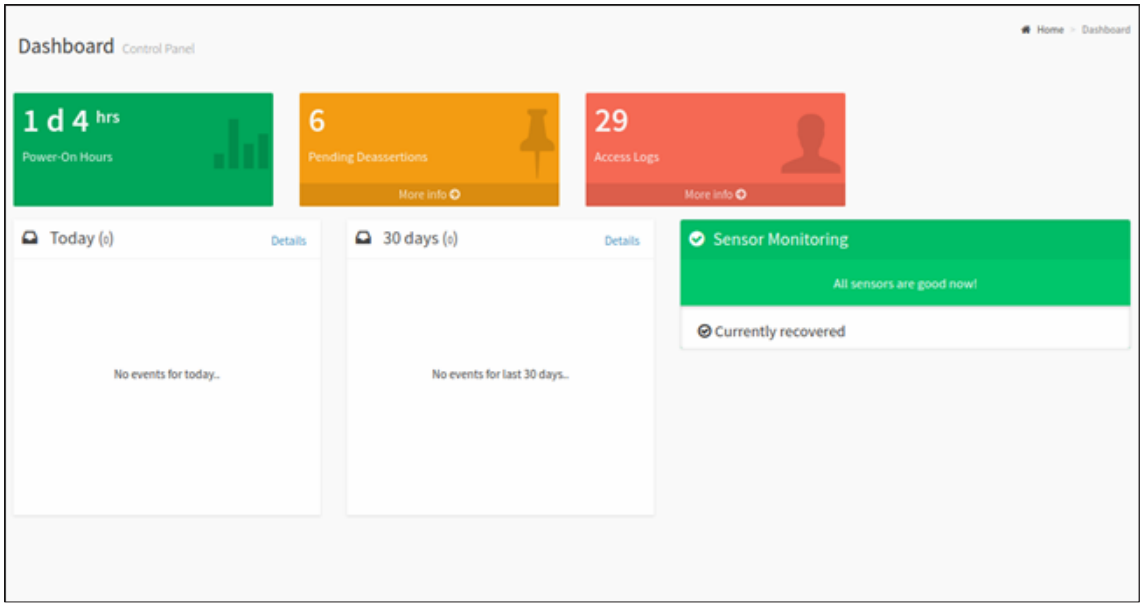
The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions.

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 Sign out 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.

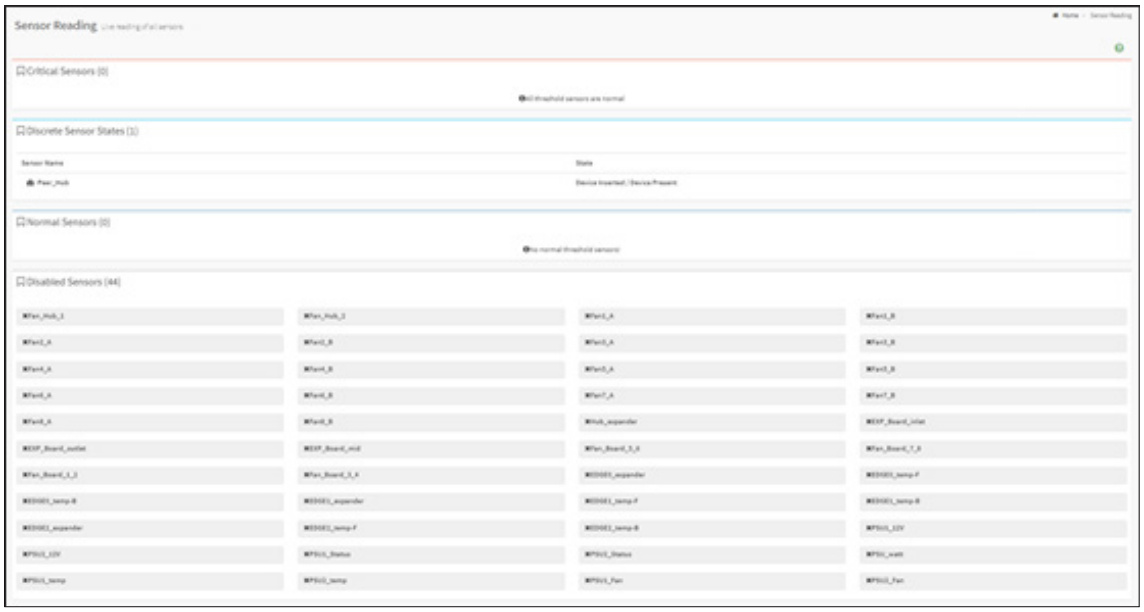
Access Logs
A graphical representation of all events incurred by various sensors and occupied/ available space in logs can be viewed. If you click on the More info link, you can view the Audit Log page.

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.



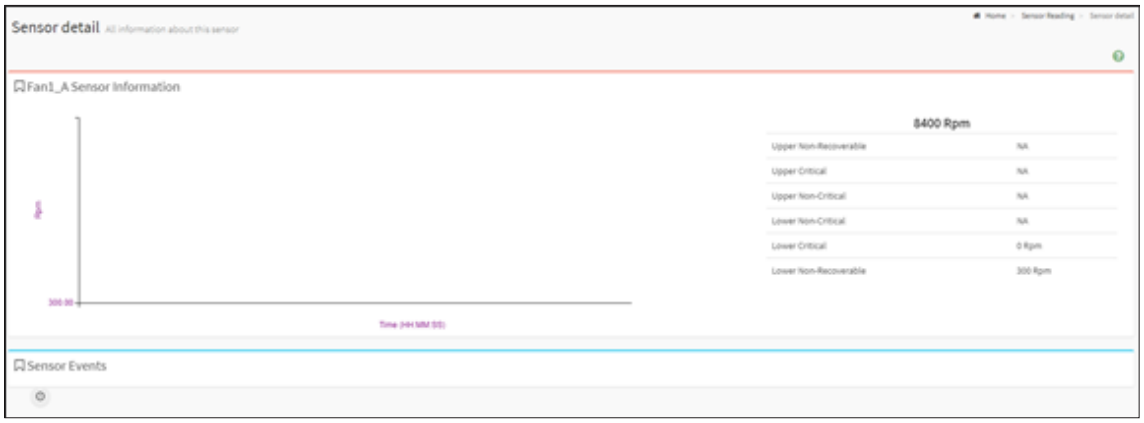
Sensor Readings Page

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.

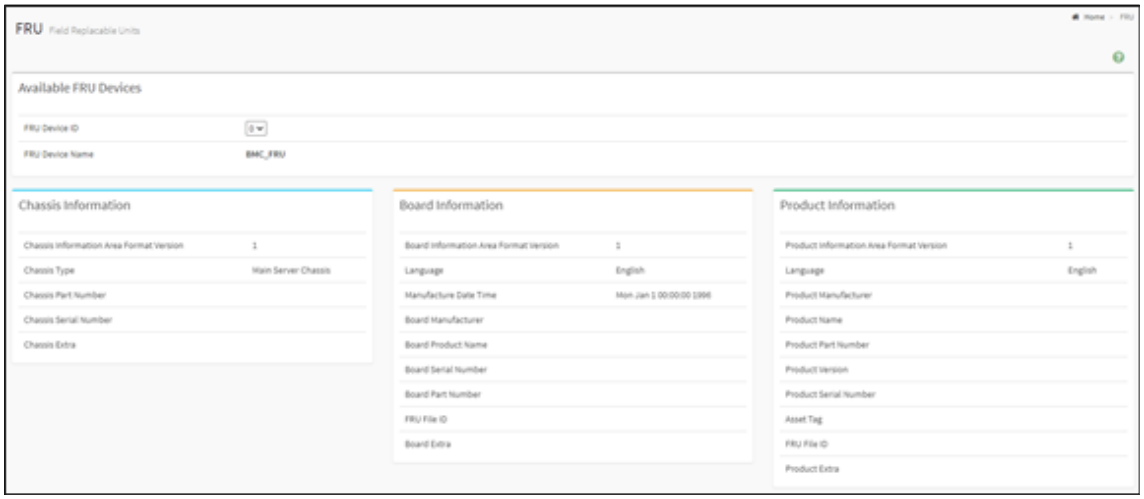
Thresholds are of six types:

- 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.



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

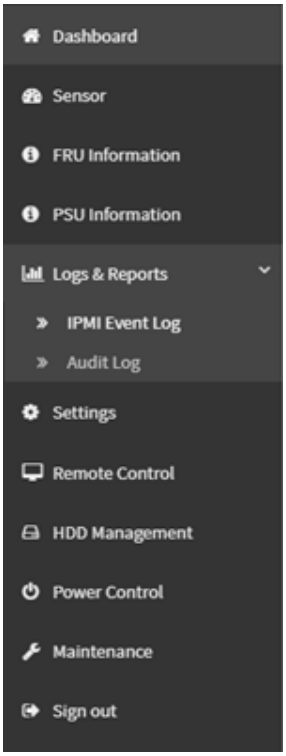
- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

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

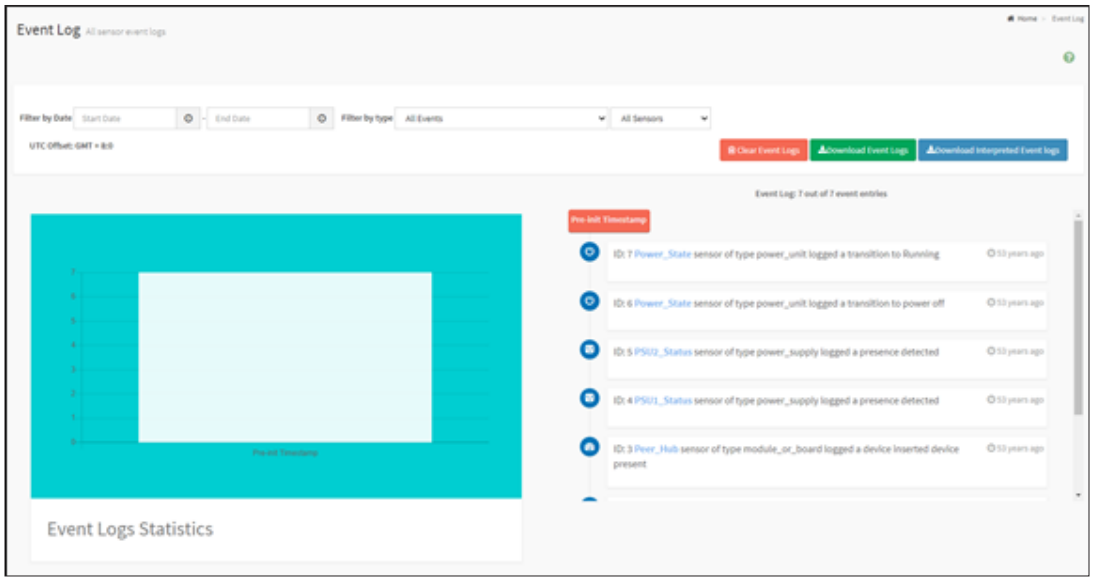


Logs & Reports – Menu

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.

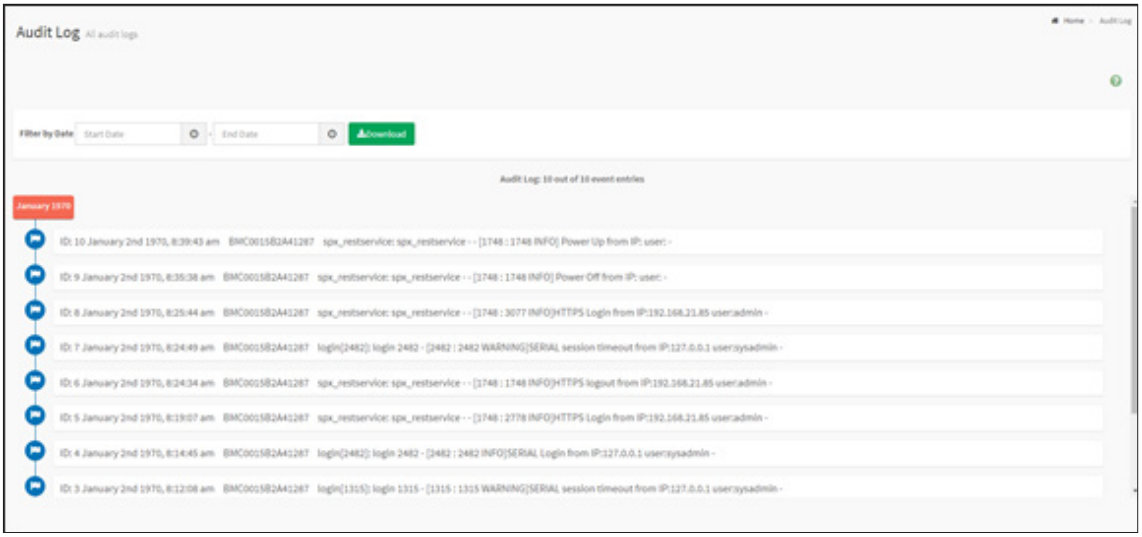
Download Event Logs: To download the event logs.

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.

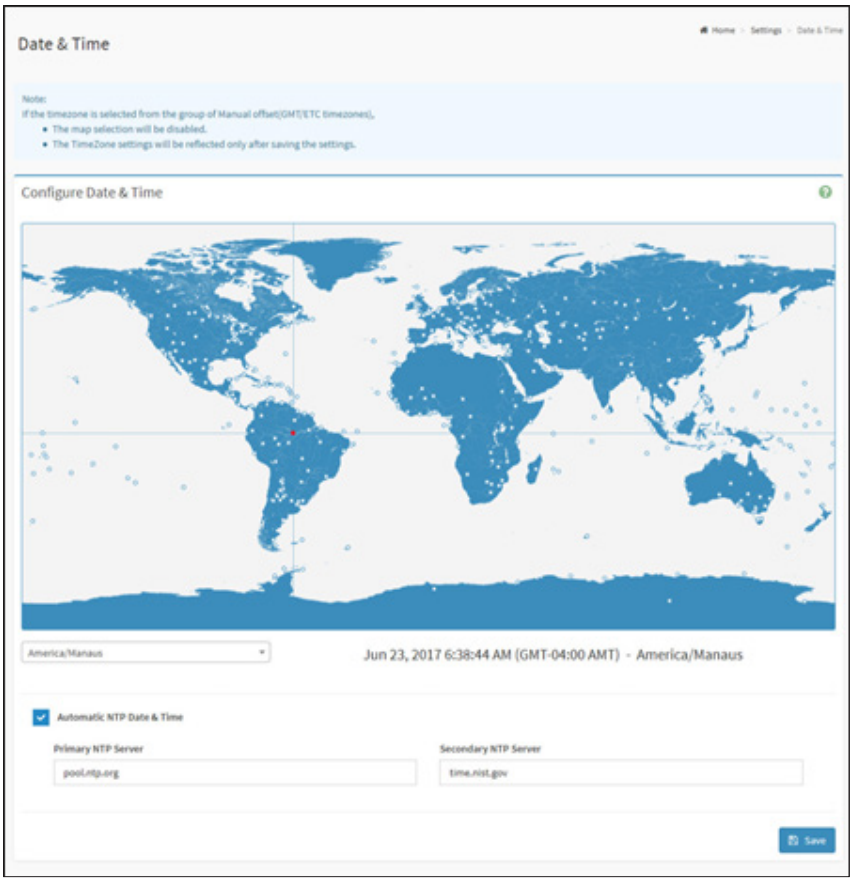
Configuration Group Menu

- 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.



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 set-ting 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

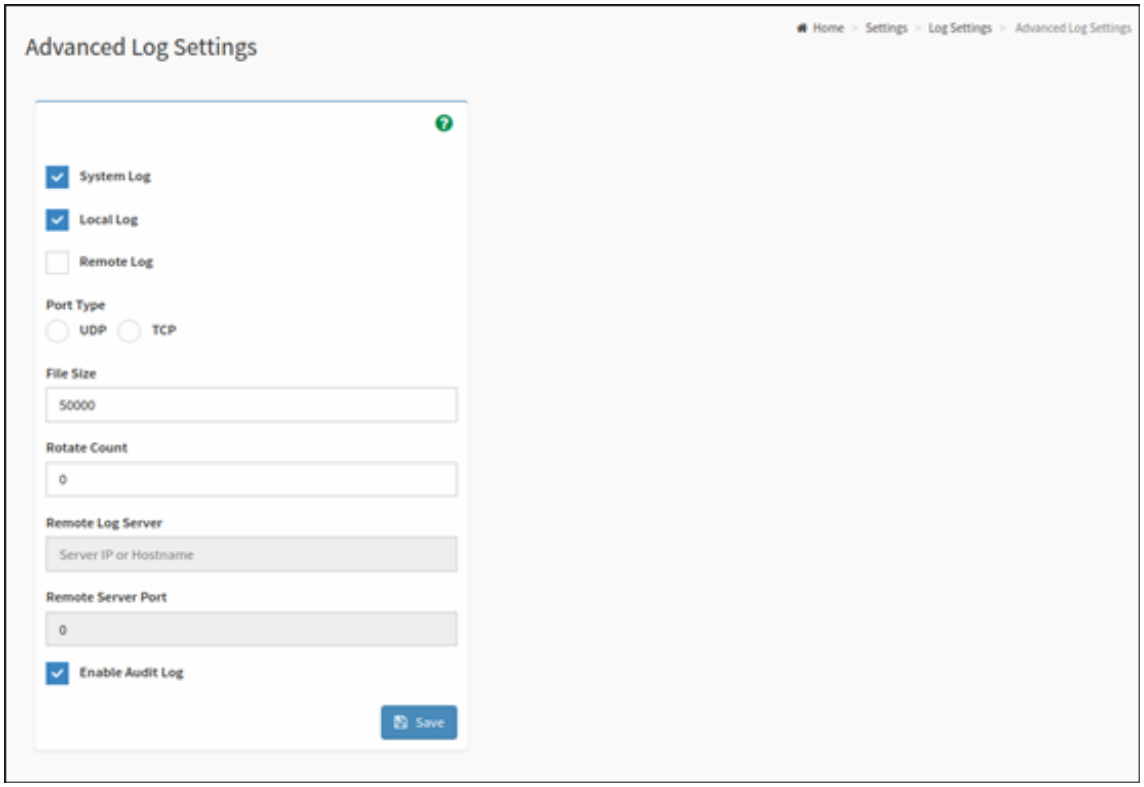
This page is used to configure the log policy for the event log. The fields are as followed

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

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

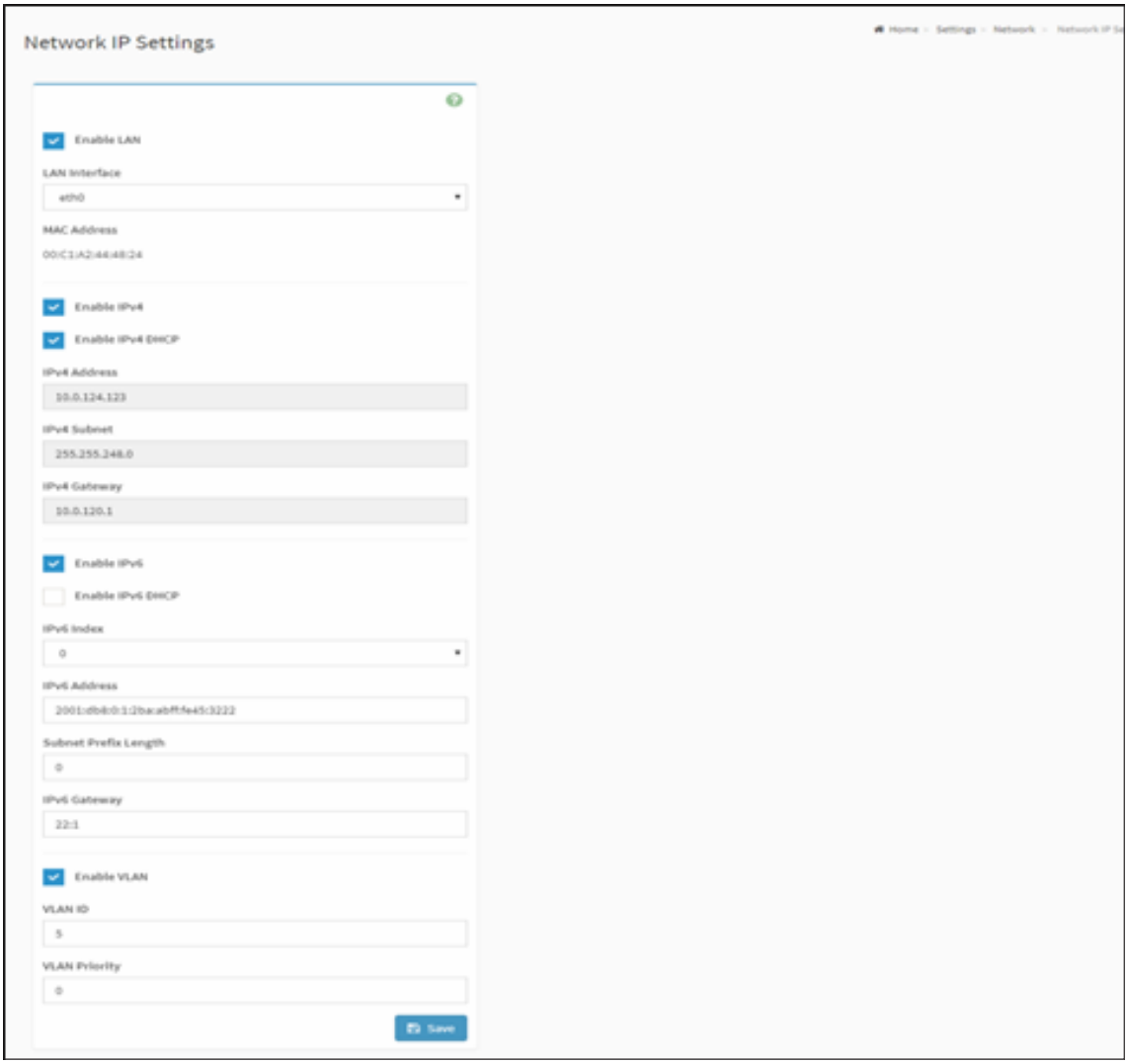
4.4.8.3 Network Settings

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.

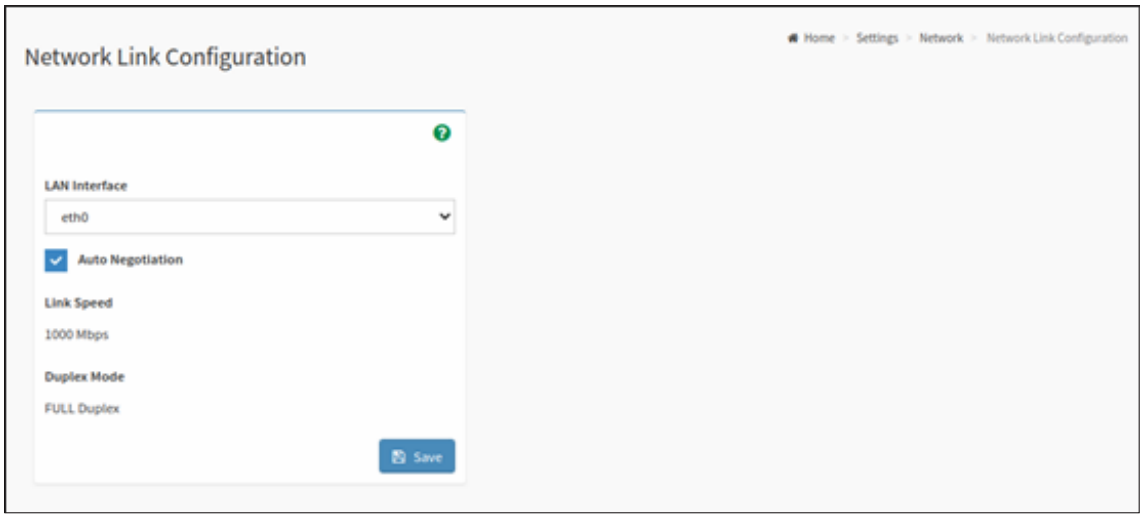
VLAN Priority: The priority for VLAN configuration.

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.

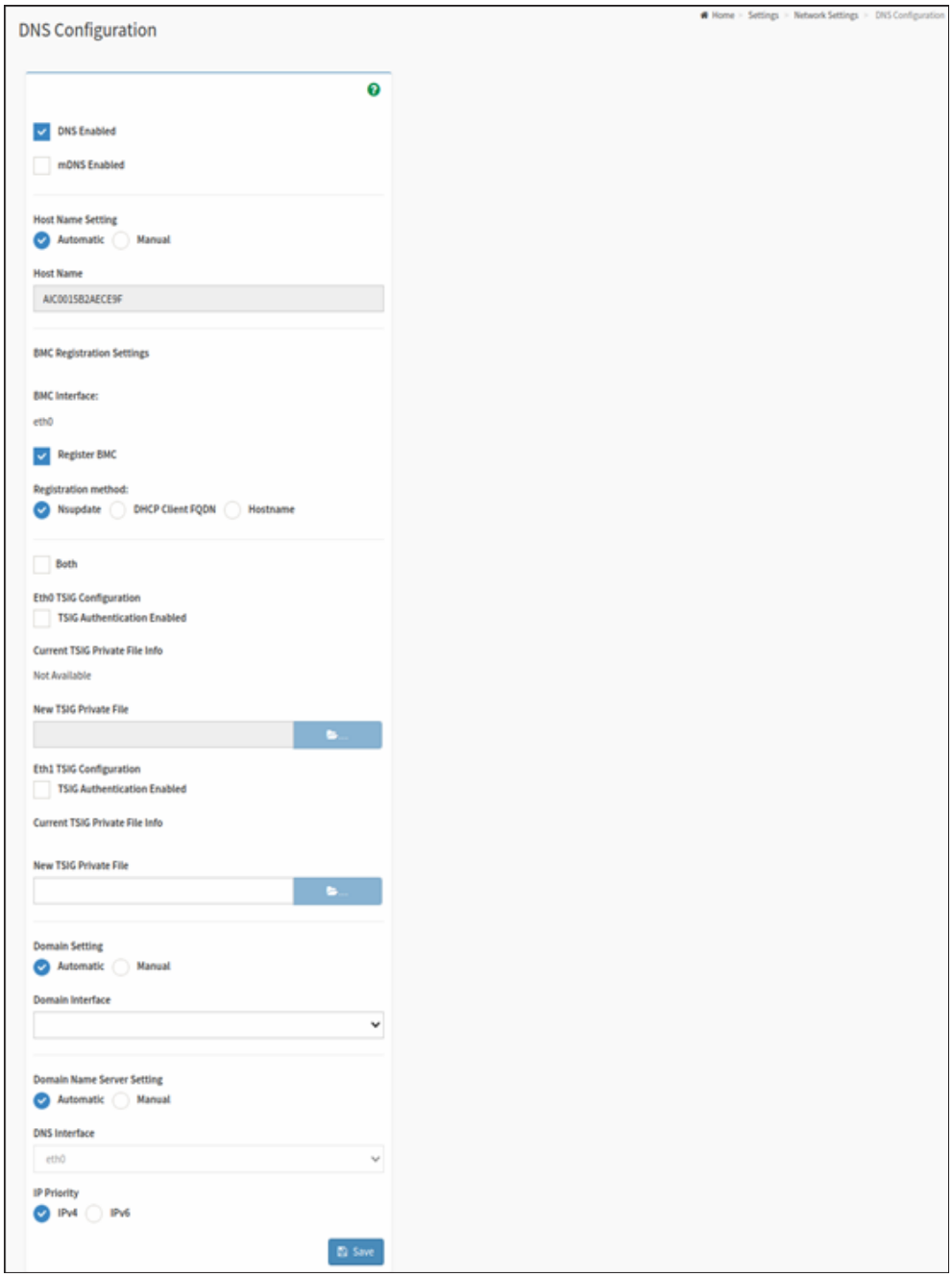
> **NOTE**
> Link speed of 1000 Mbps is not applicable, when Auto Negotiation is OFF.

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 Page

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 (eth0&eth1).

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.

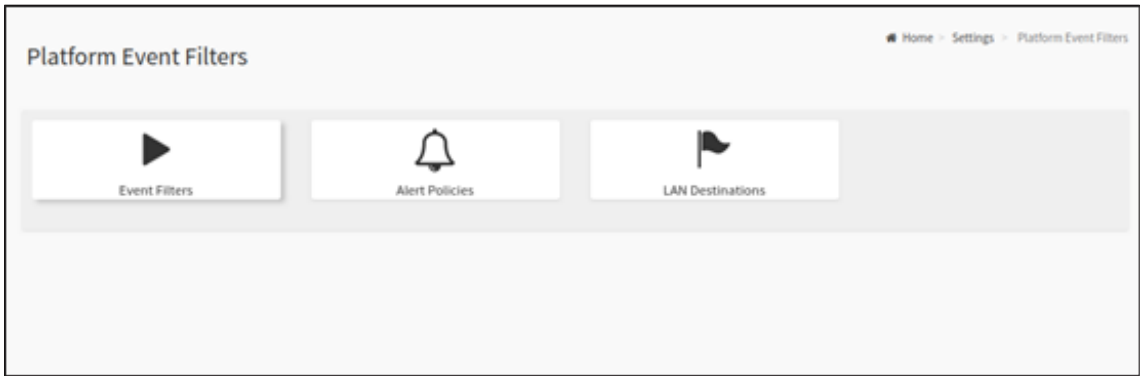
Save: To save the entered changes.

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

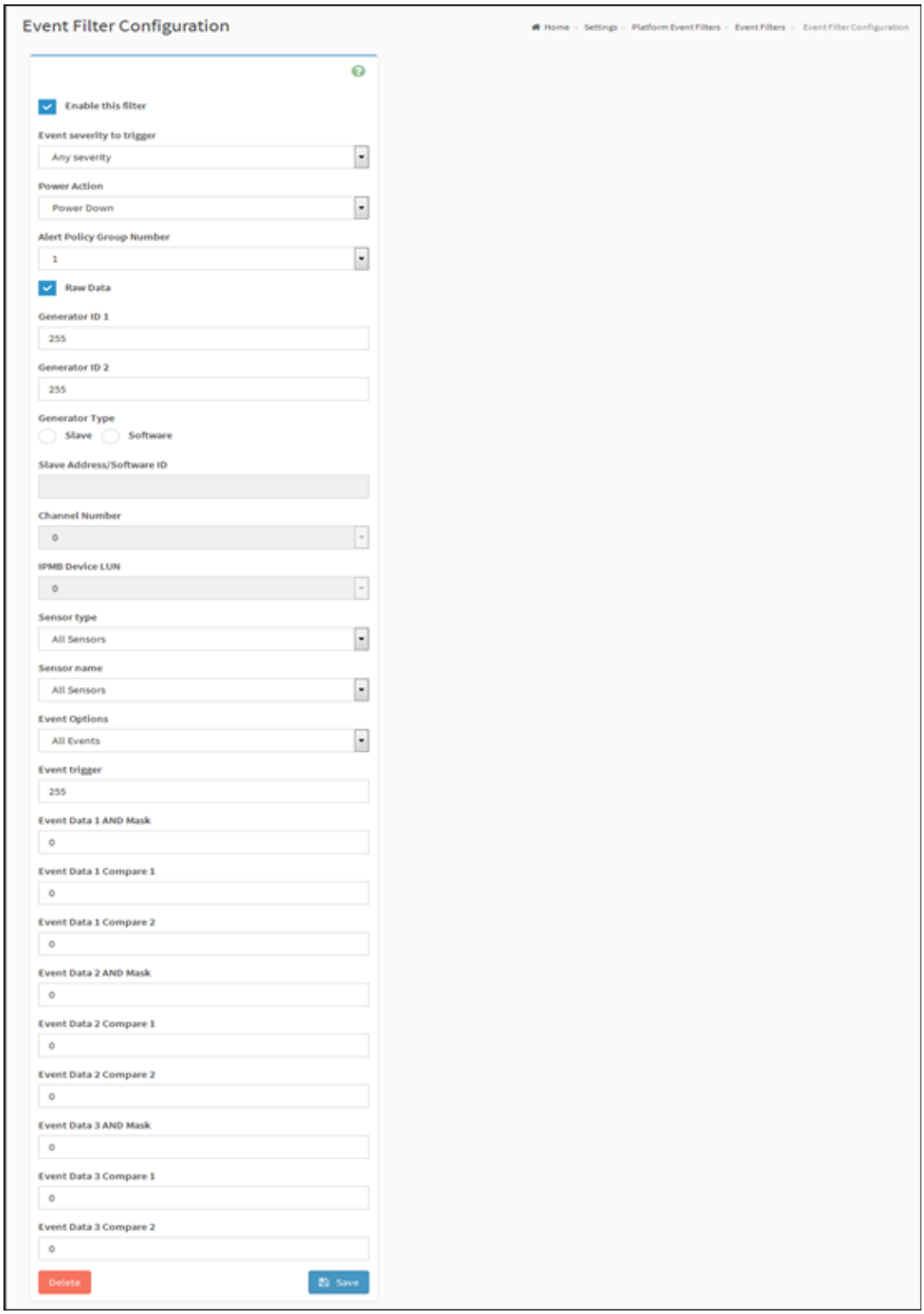
A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM' 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

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.

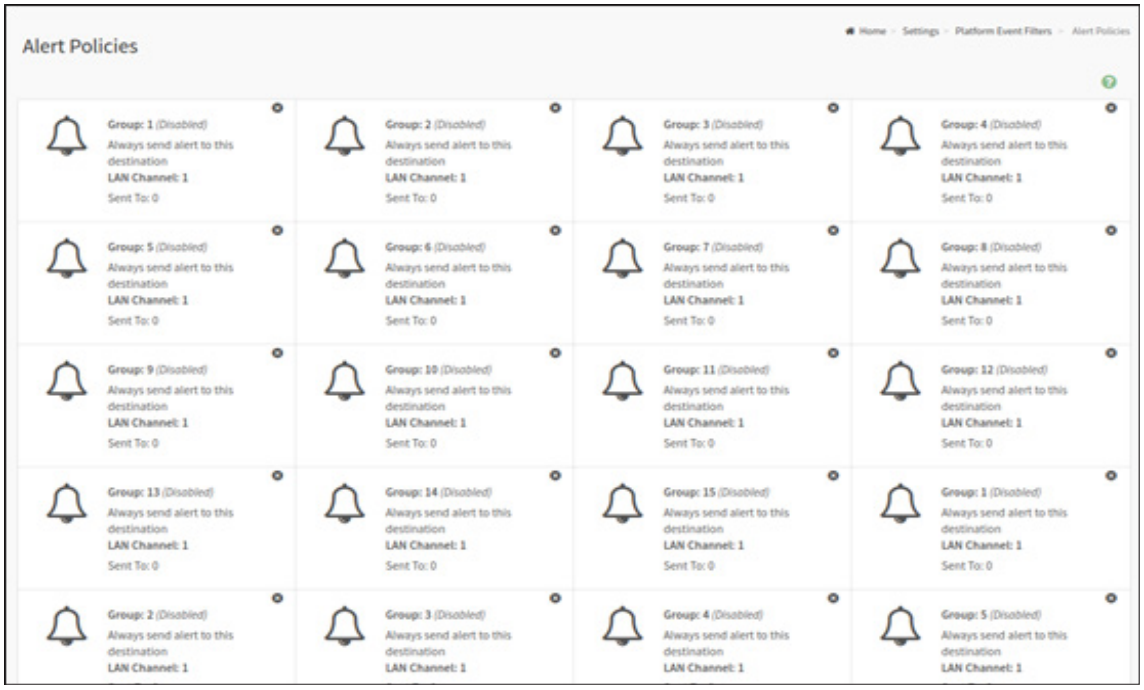
> **NOTE**
> Value ranges from 0 to 255.

- 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.

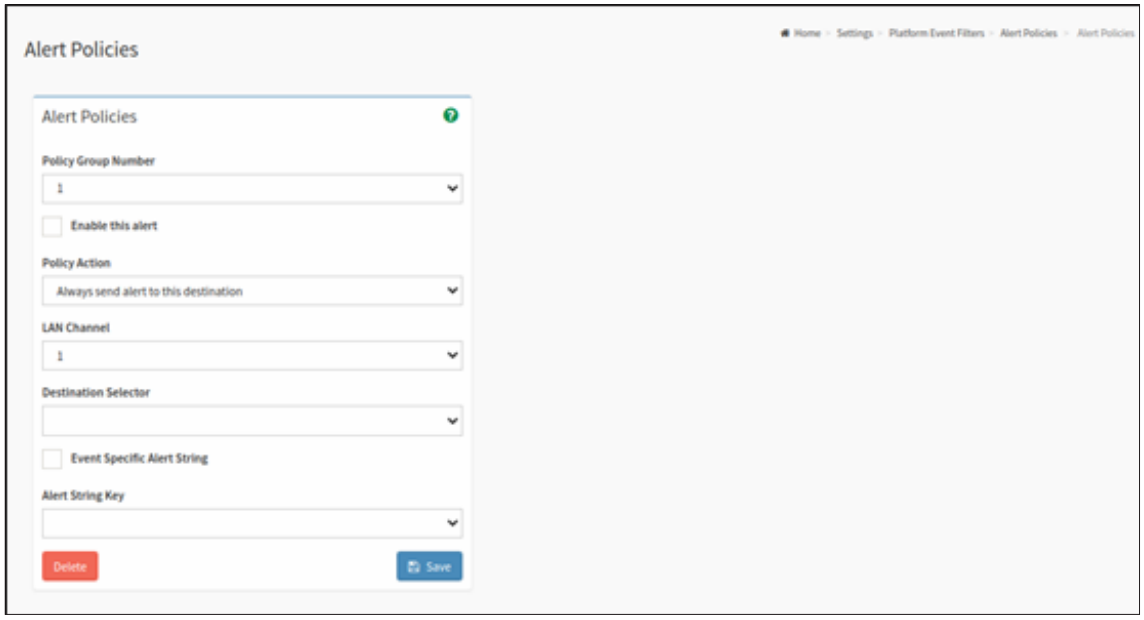
Alert Policies

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.

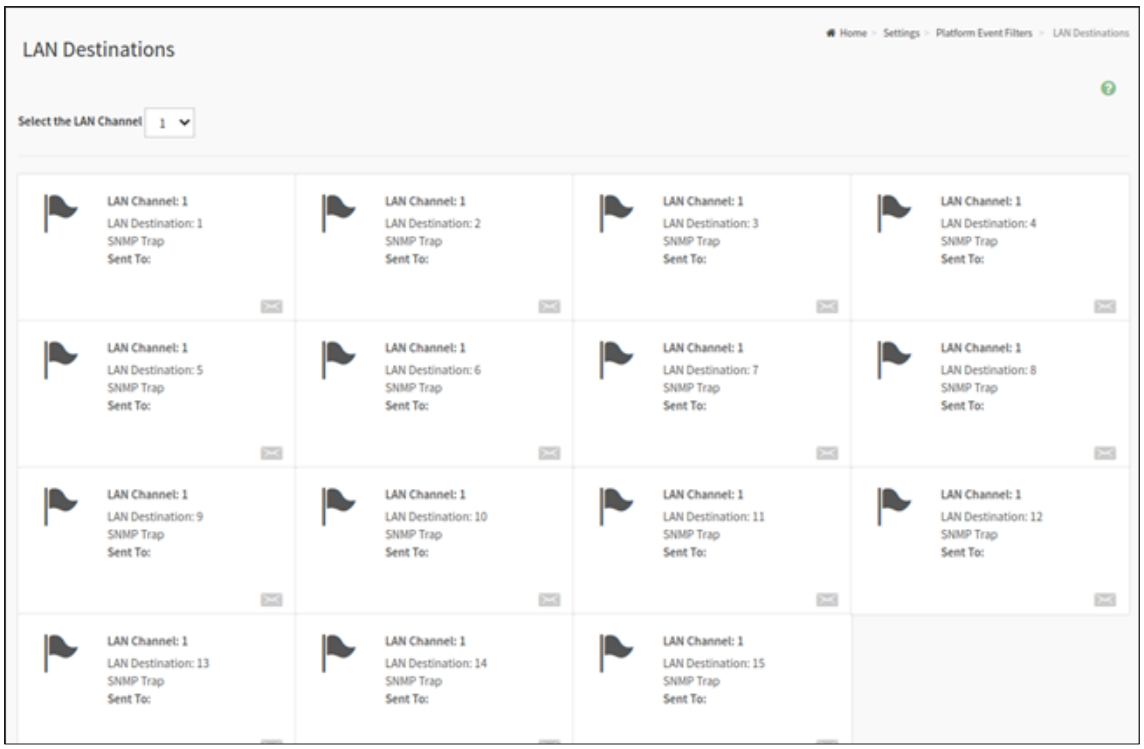
Alert String Key: To specify which string is to be sent for this Alert Policy entry.

Save: To save the Alert Policies entries.

Delete: To delete the selected configured Alert Policy.

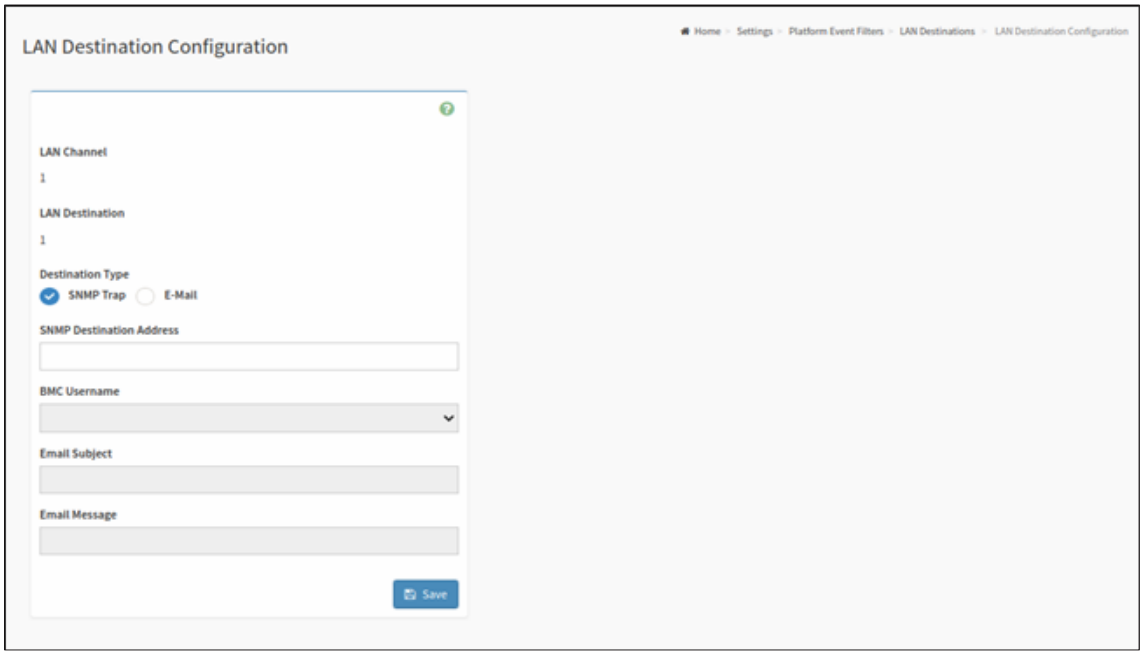
LAN Destinations

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.

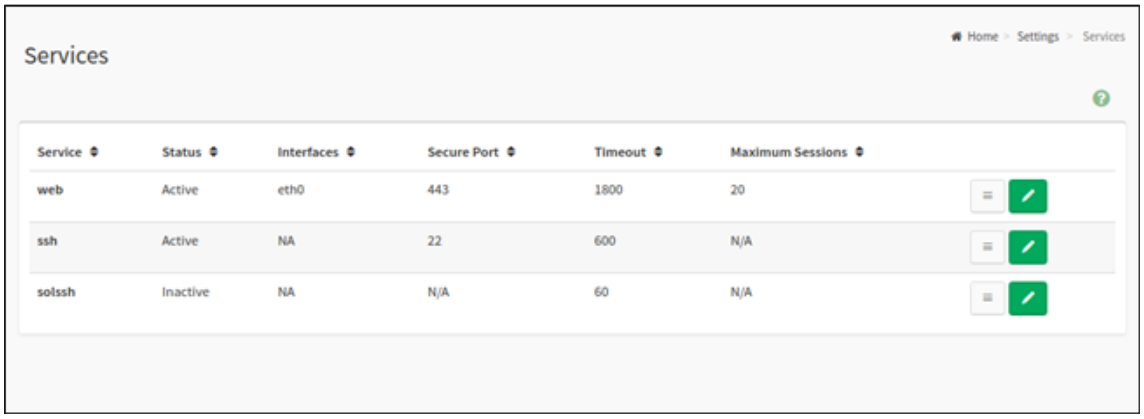
Delete: To delete the selected configured LAN Destination.

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.



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
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.

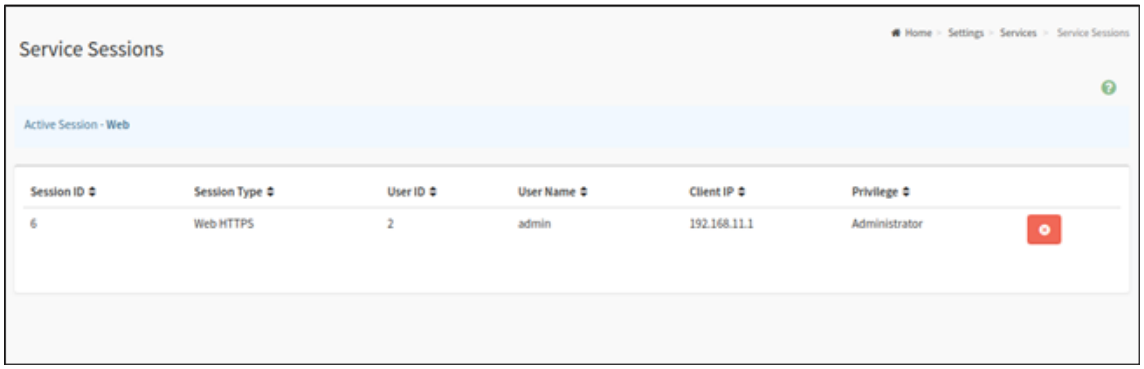
NOTE
- Web timeout value ranges from 300 to 1800 seconds.
- SSH timeout value ranges from 60 to 1800 seconds.

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.



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.

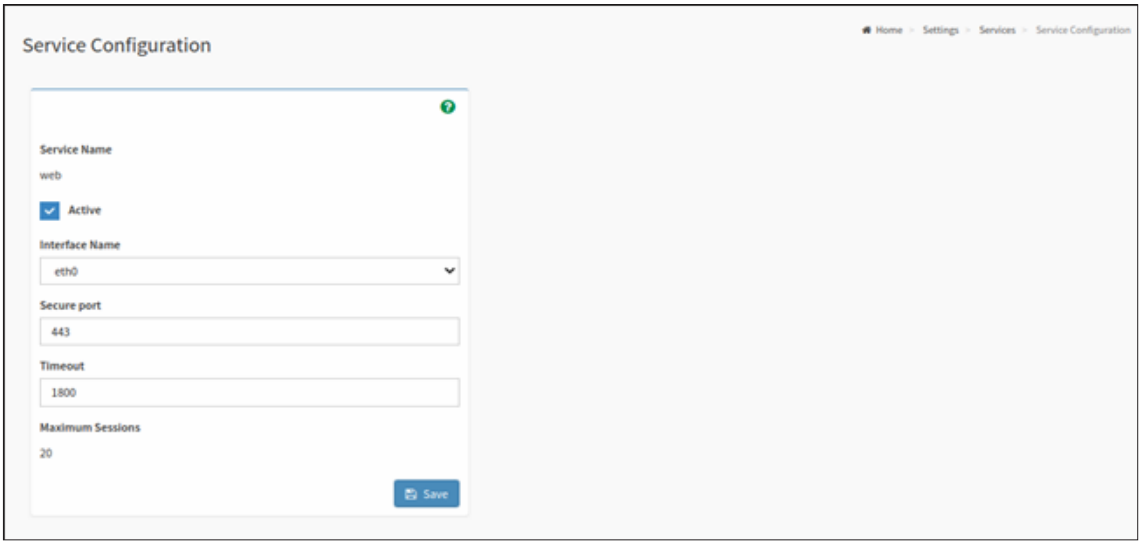
To modify the existing services:

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.

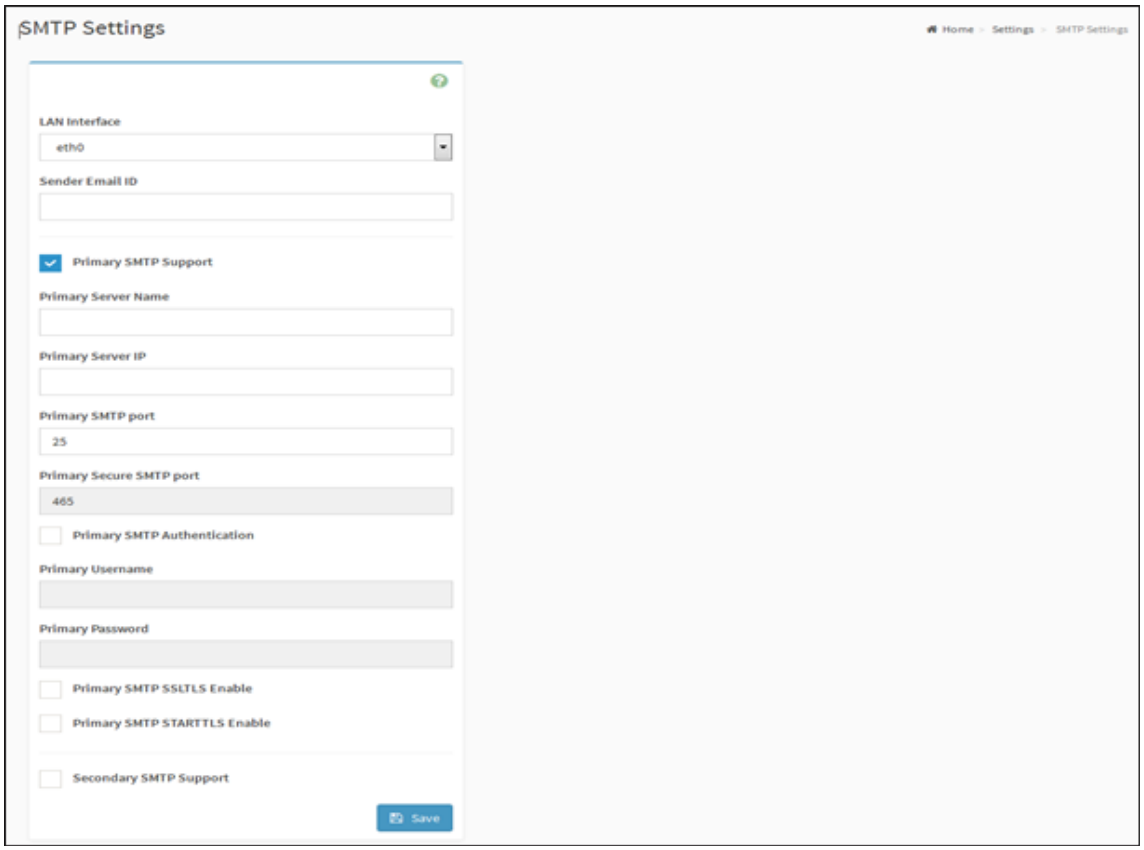
> **NOTE**
> The values in the ***Maximum Sessions*** field cannot be modified.

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.

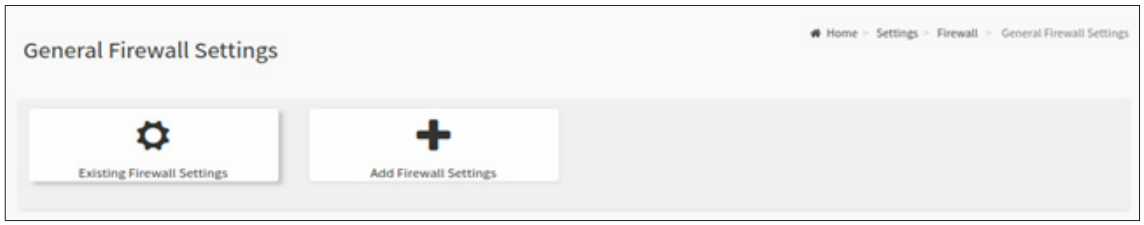
Save: To save the new SMTP server configuration.

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.



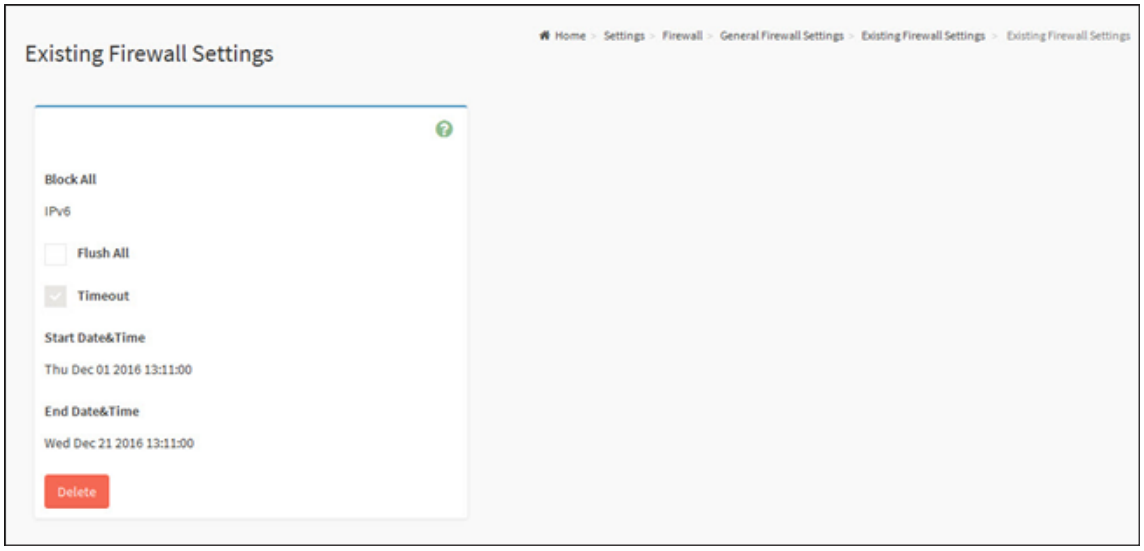
General Firewall Settings

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.

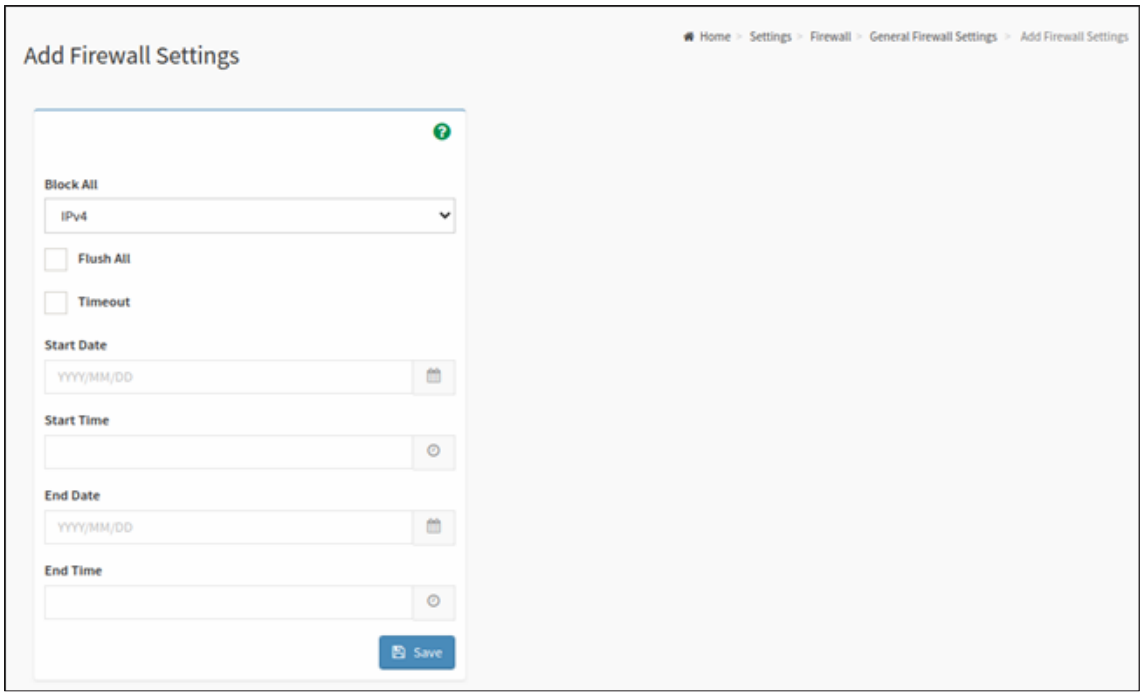


Existing Firewall Settings

- **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.



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.

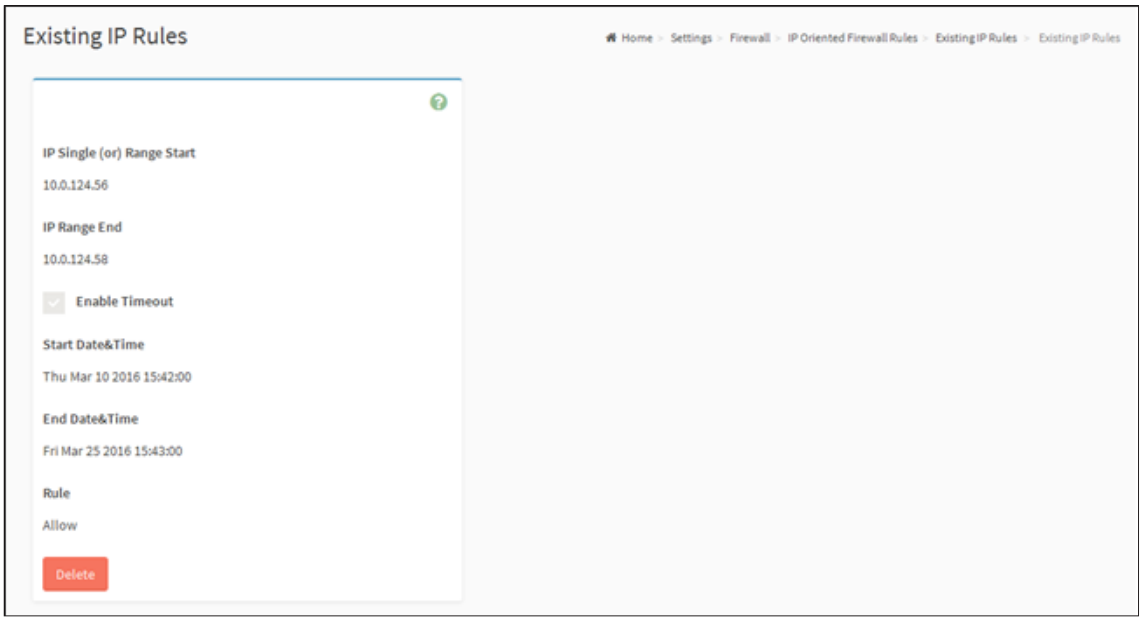
IP Address Firewall Rules

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.

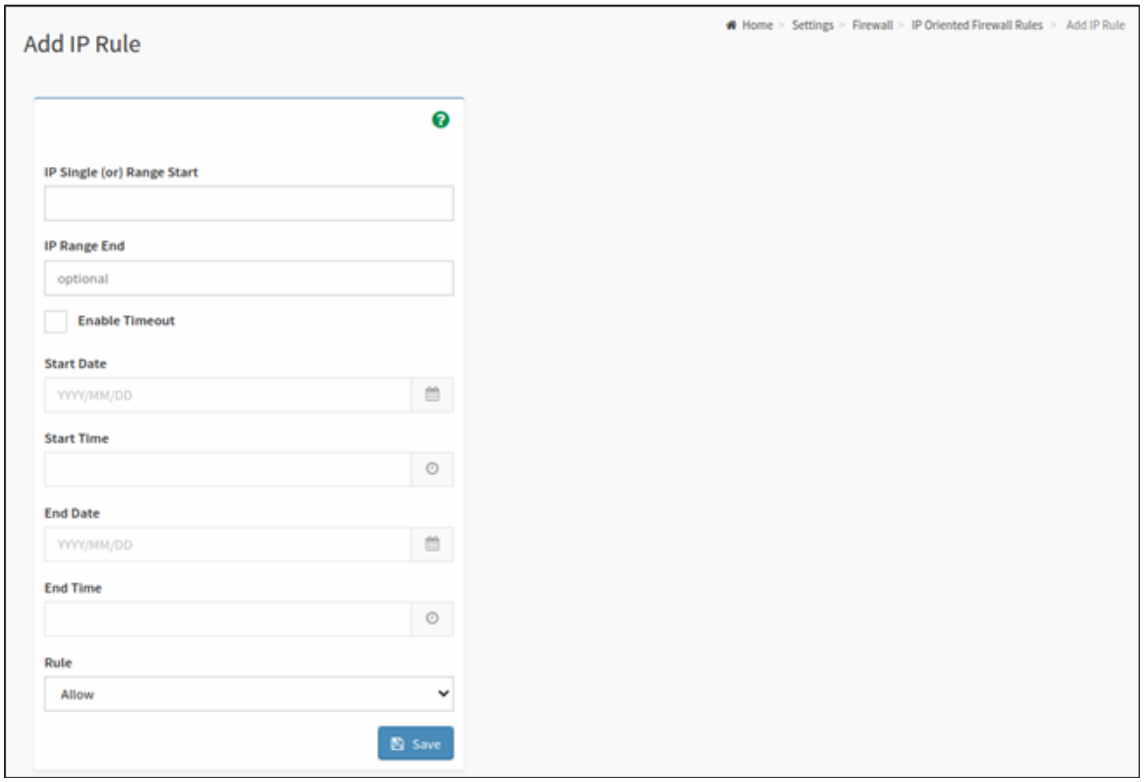


System Firewall - Existing IP Rule

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.



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.

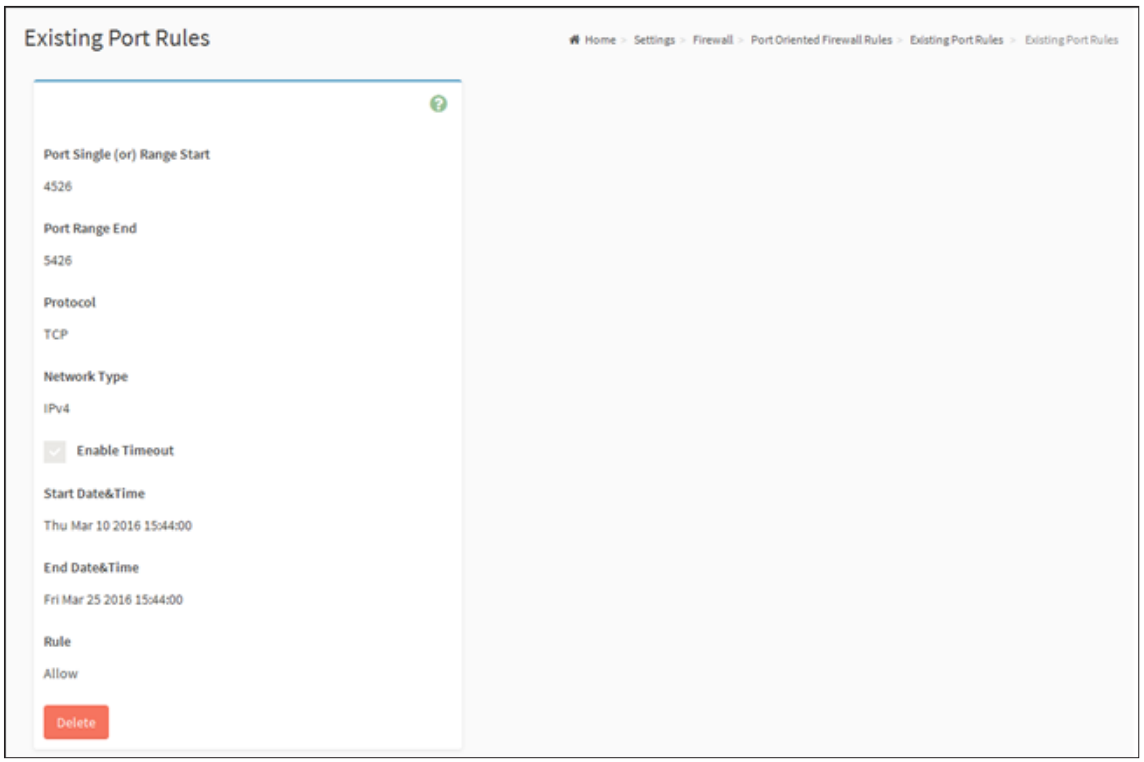
Port Firewall Rules

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.

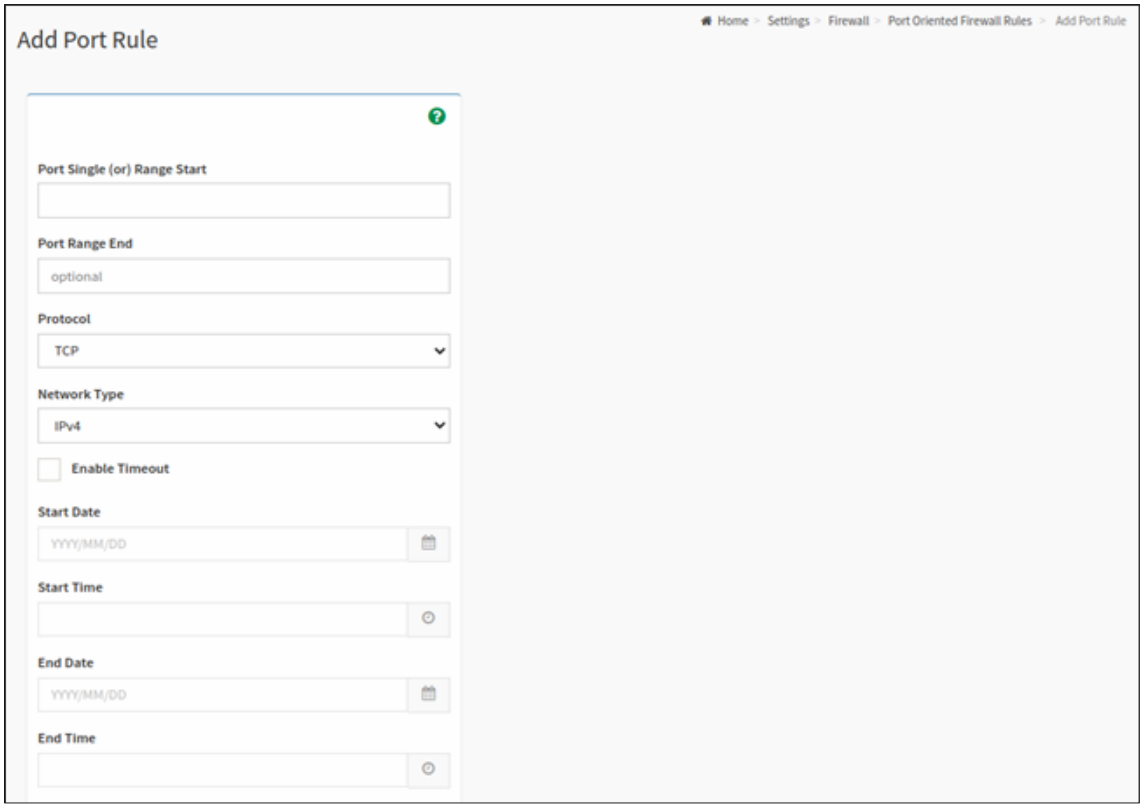


System Firewall - Existing Port Rules

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.



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.

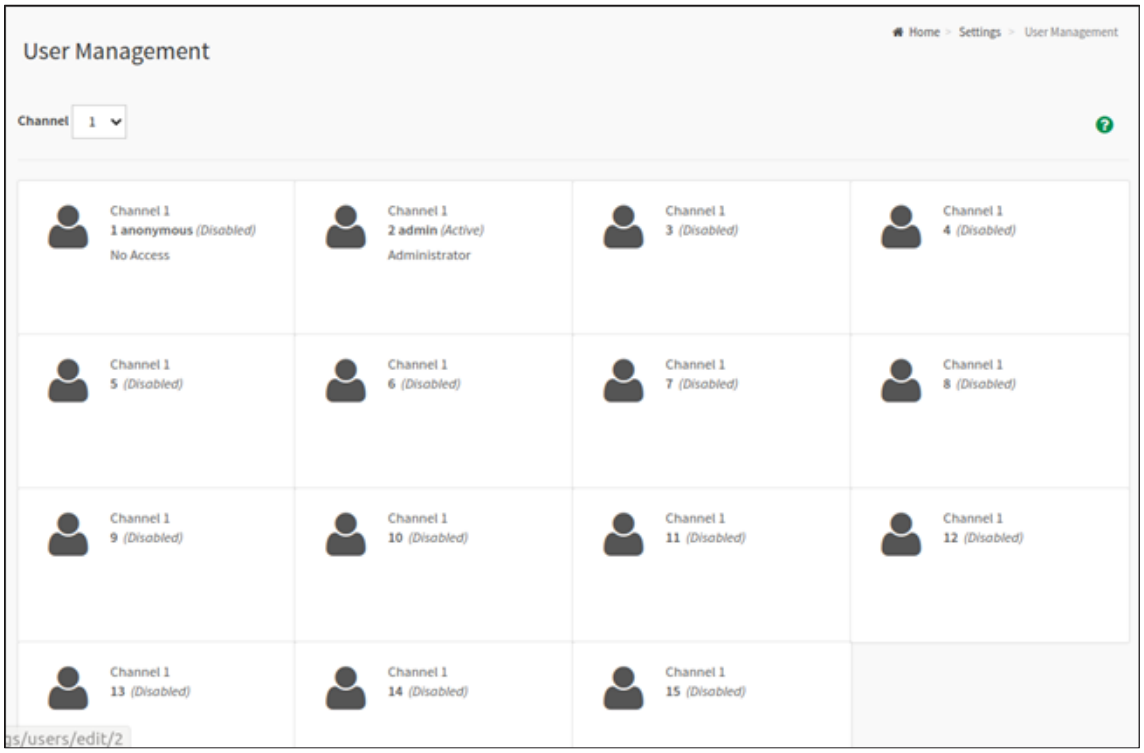
3. Enter the end value in the **Port Range End** field.
4. Select the **Protocol** to be either TCP or UDP or Bot.
5. Select the **Network Type**. It may be IPv4 or IPv6 or Both.
6. Select **Timeout** to enable or disable firewall rules with timeout.
7. Enter **Start Time** to start the respective firewall 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 (**x**) 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.

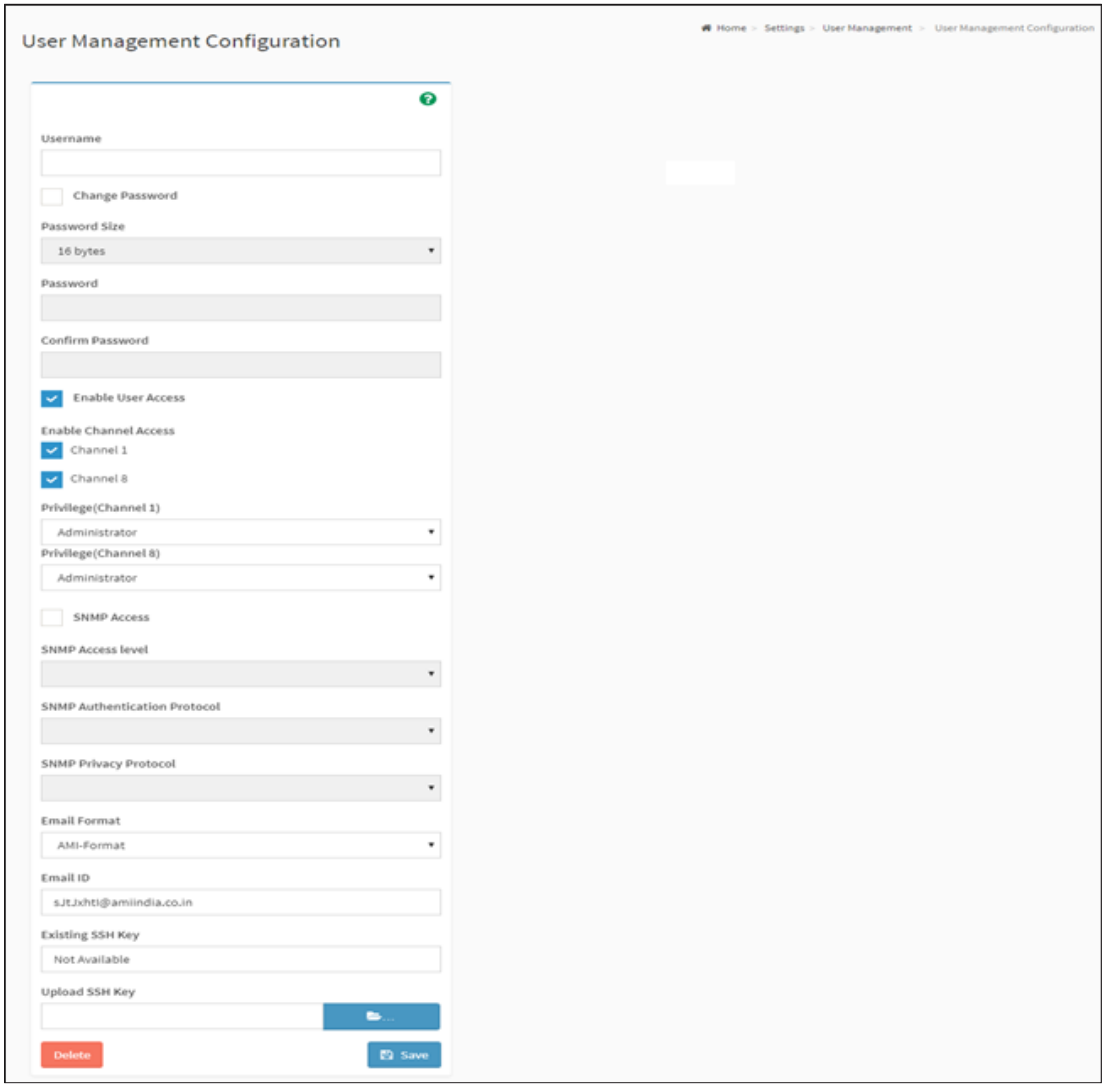
E-mail ID: Displays e-mail address of the user.

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 Page

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.

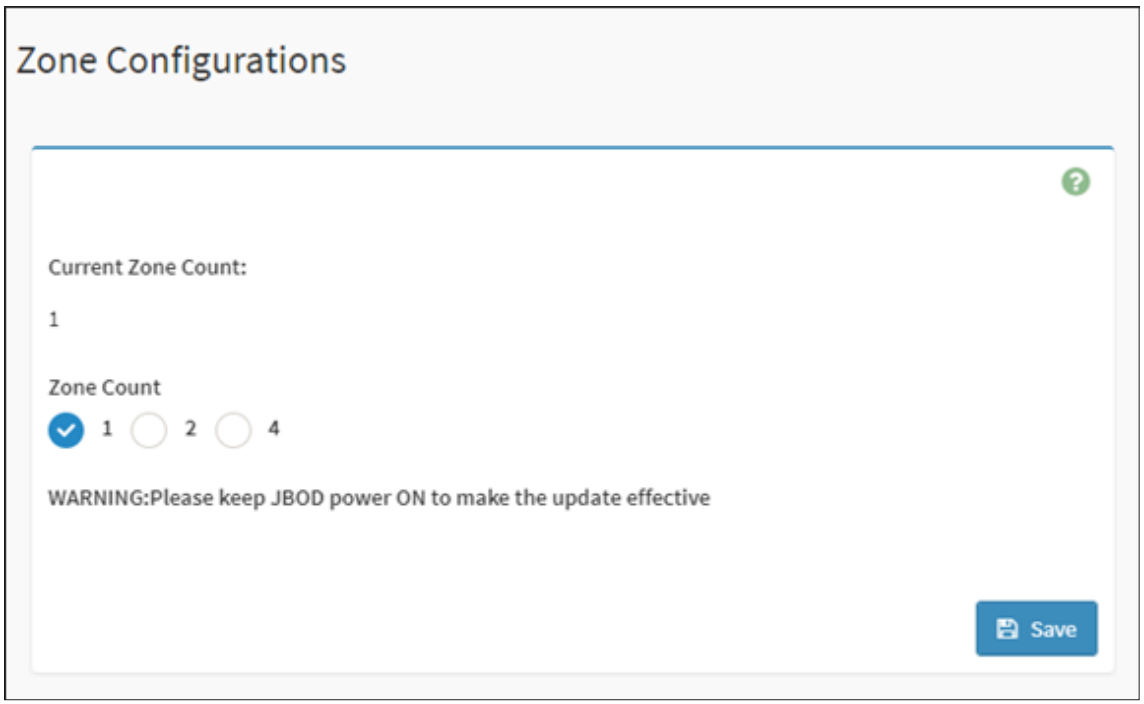
Power Restore Policy

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).

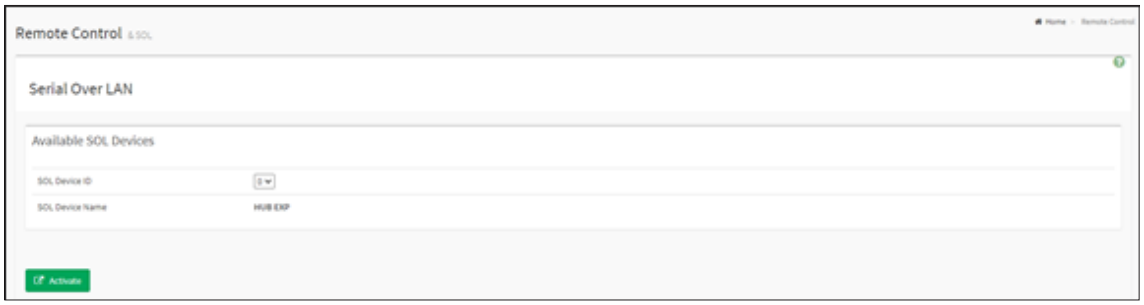
To open Zone Configurations page, click Settings > Zone Configurations from the menu bar. A sample screenshot of Zone Configurations page is shown below.



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

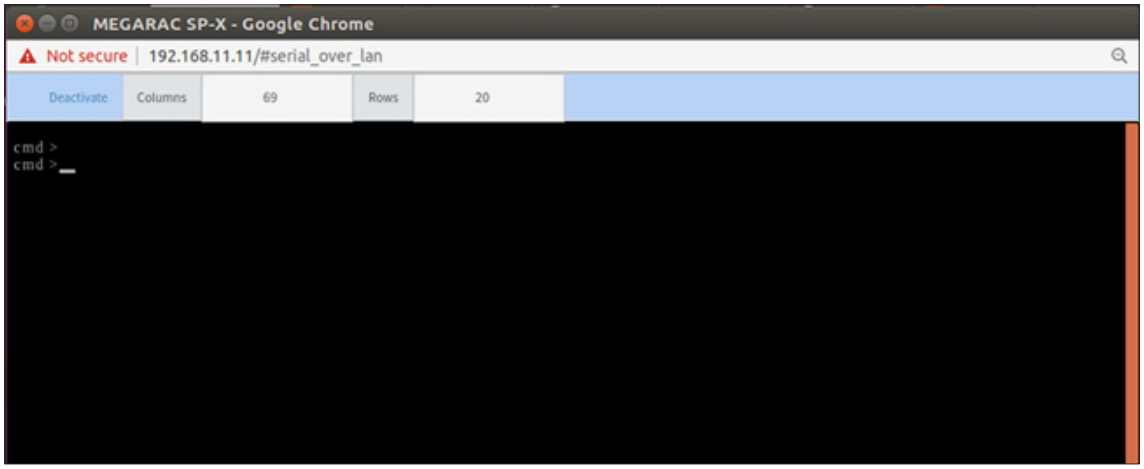
The Remote Control page consists of the following options. A sample screenshot is displayed below.



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.



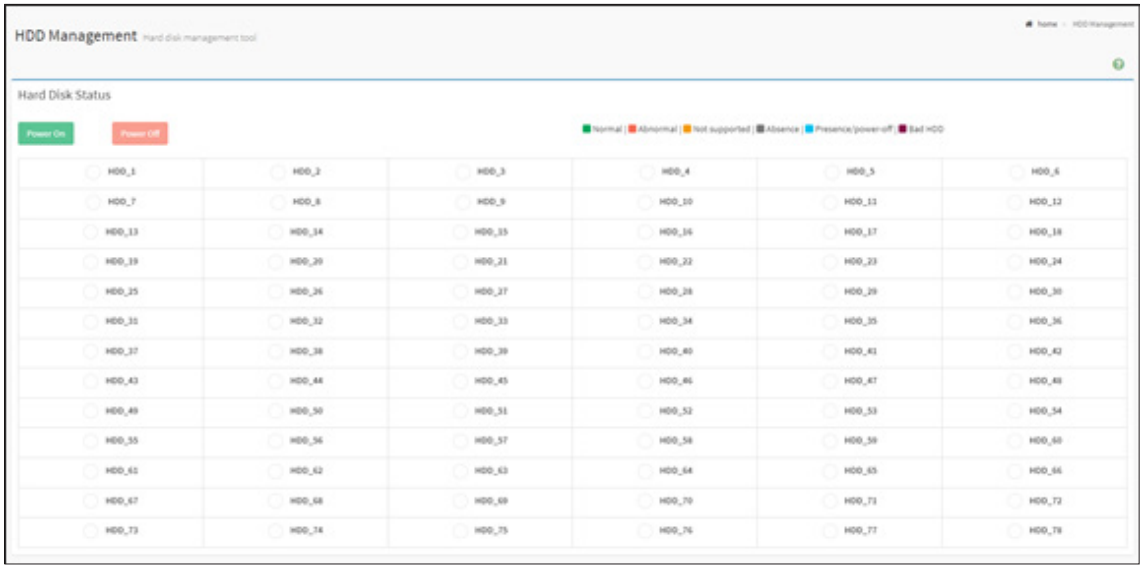
serial over lan

4.4.10 HDD Management

This page allows you to view and control the hard disk drivers.

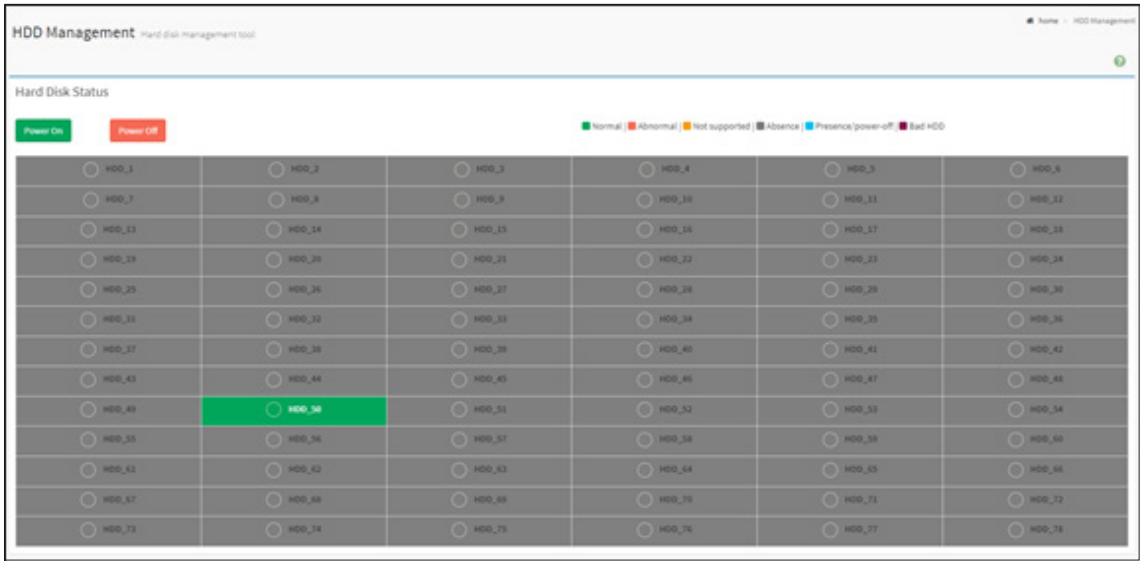
To open HDD Management, click HDD Management from the menu bar. A sample screenshot of HDD Management page is shown below.

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.

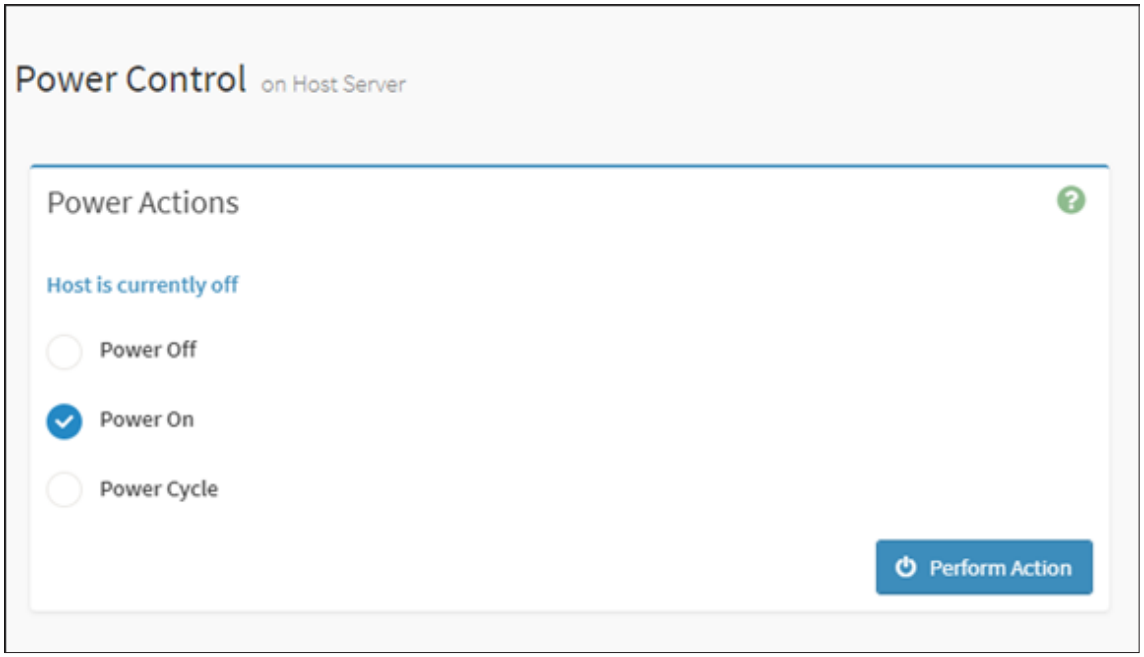
Power on: To power on the hard disk driver.

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

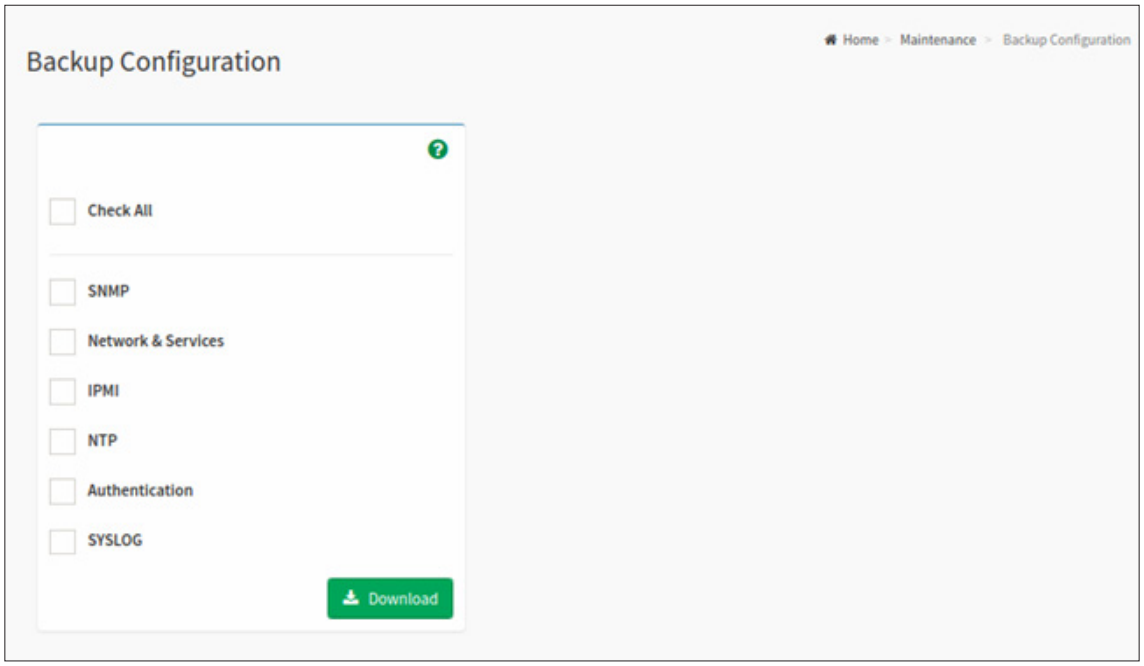
- Backup Configuration
- Firmware Image Location
- BMC Firmware Information
- BMC Firmware Update
- Preserve Configuration
- Restore Configuration
- Expander Update
- BMC Rest

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.

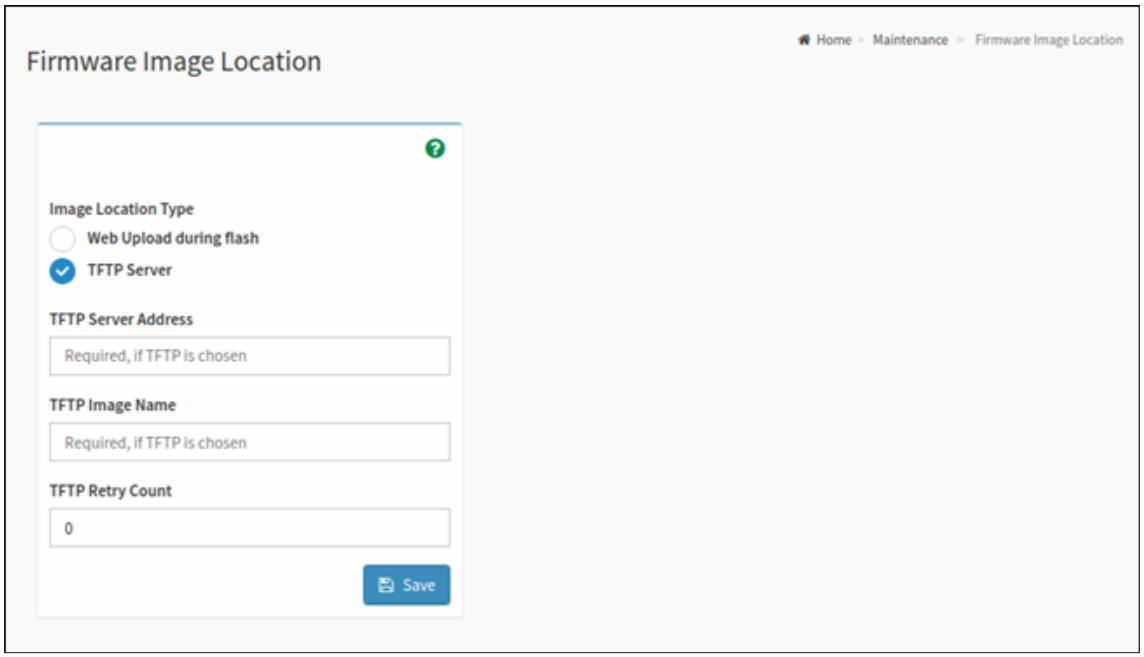
> **NOTE**
>
> Network configurations are inter-related to IPMI, and hence by default IPMI configurations will be selected automatically when you select "Network and Services" to be backed up.

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.

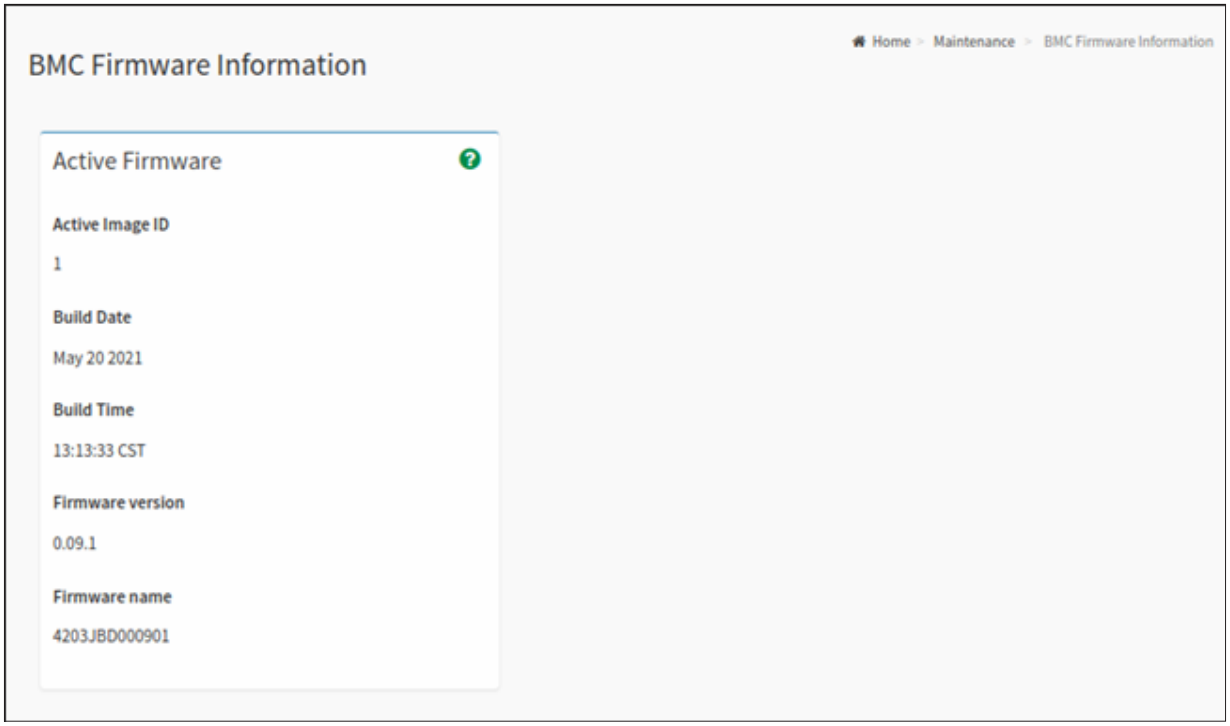
TFTP Retry Count: Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.

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.

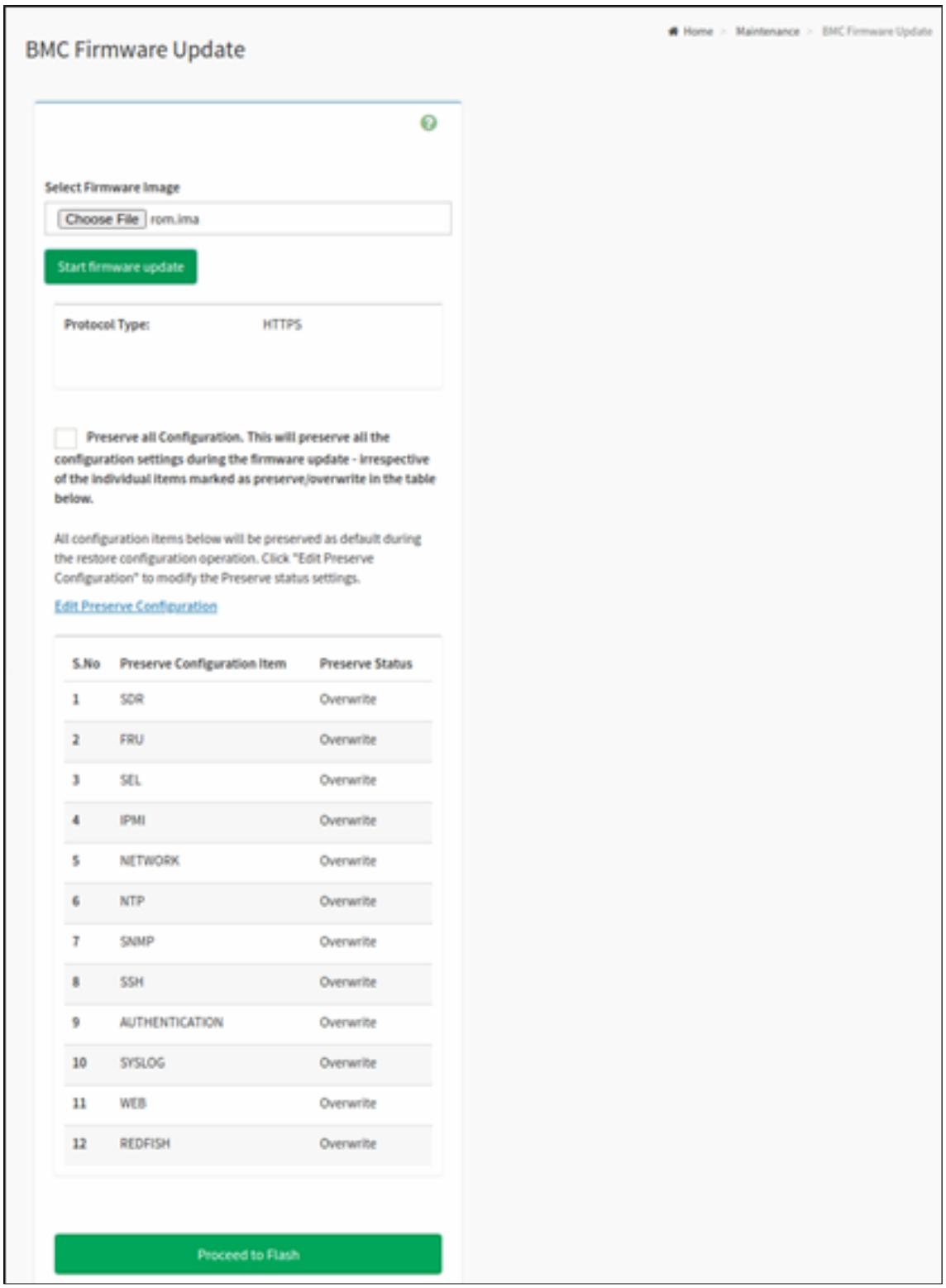
Procedure

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.



BMC Firmware Update Page

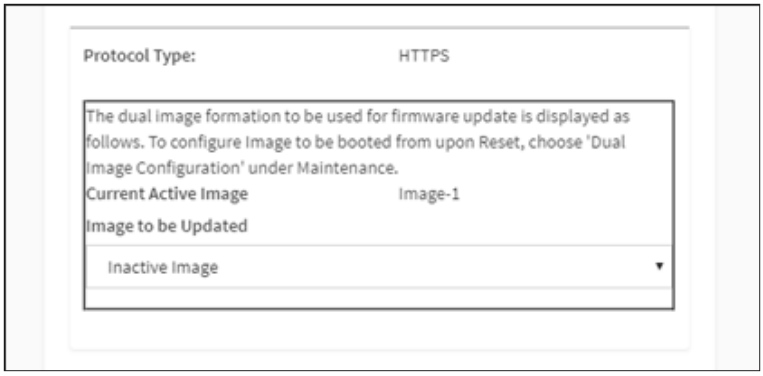
NOTE

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

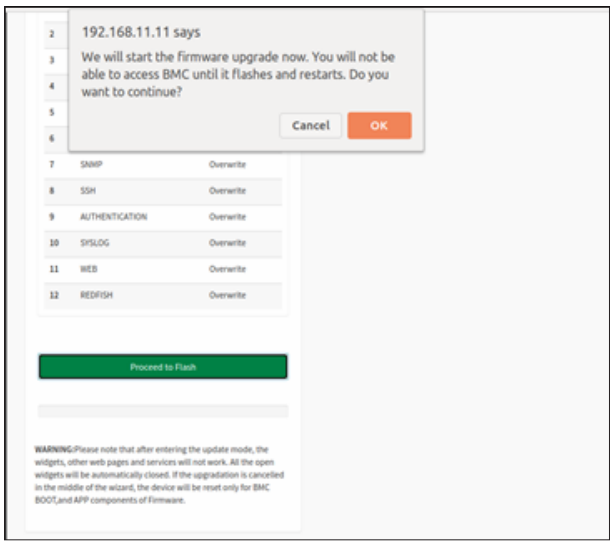
3. Click Preserve all Configuration to preserve all configuration.
   - **Preserve all Configuration:** To preserve all configuration.
   - **Edit Preserve Configuration:** To modify the Preserve status settings.

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.

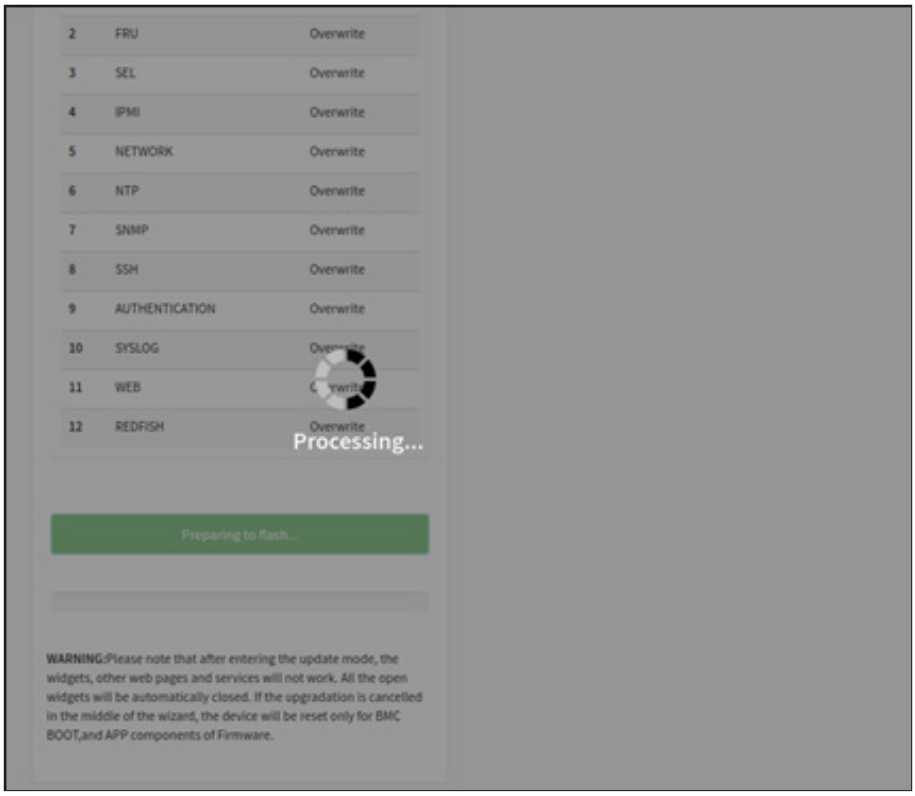
4. Click Proceed to Flash, it will prompt you with the warning message. Click Ok to start the Firmware update.



Firmware Update

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

A sample screenshot is shown as below.



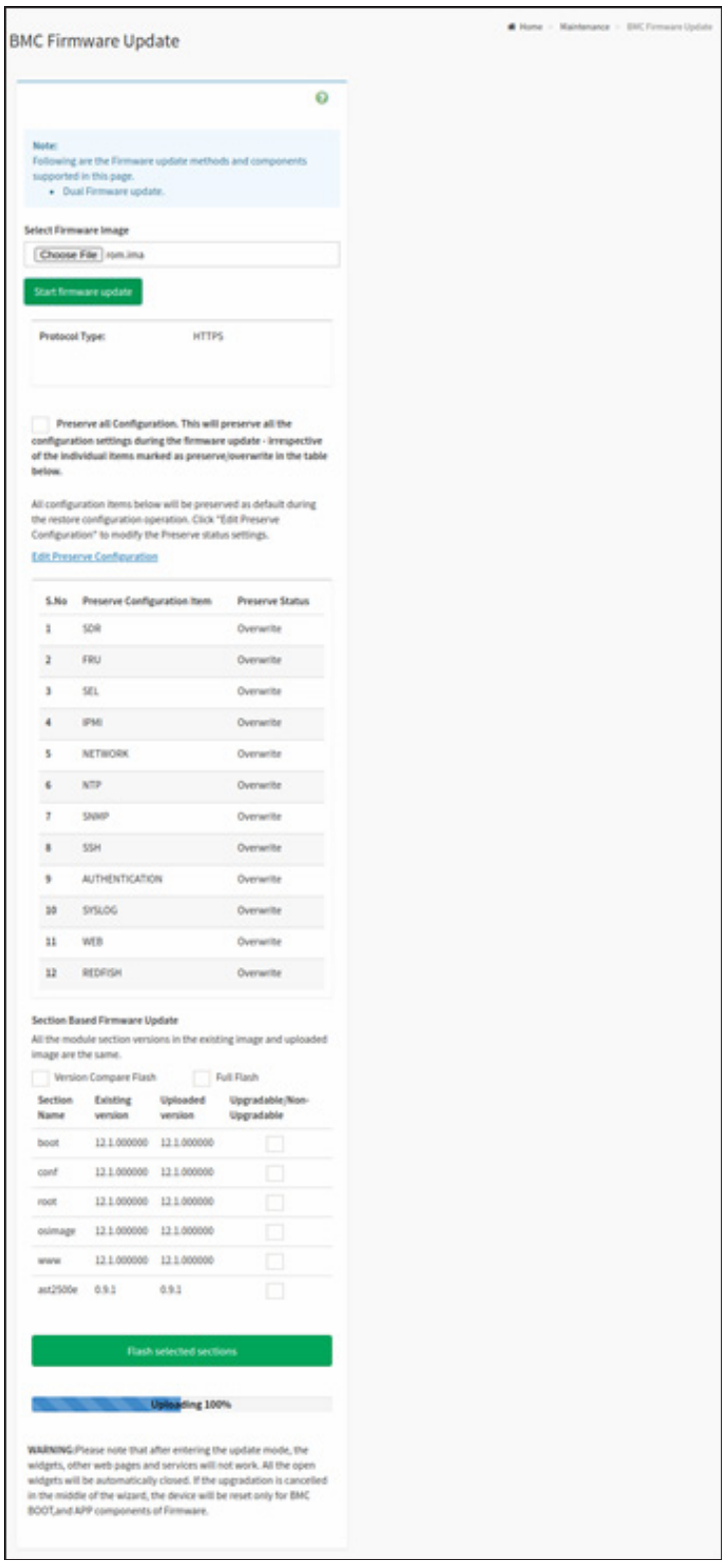
Firmware Update - Image Upload Start

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.

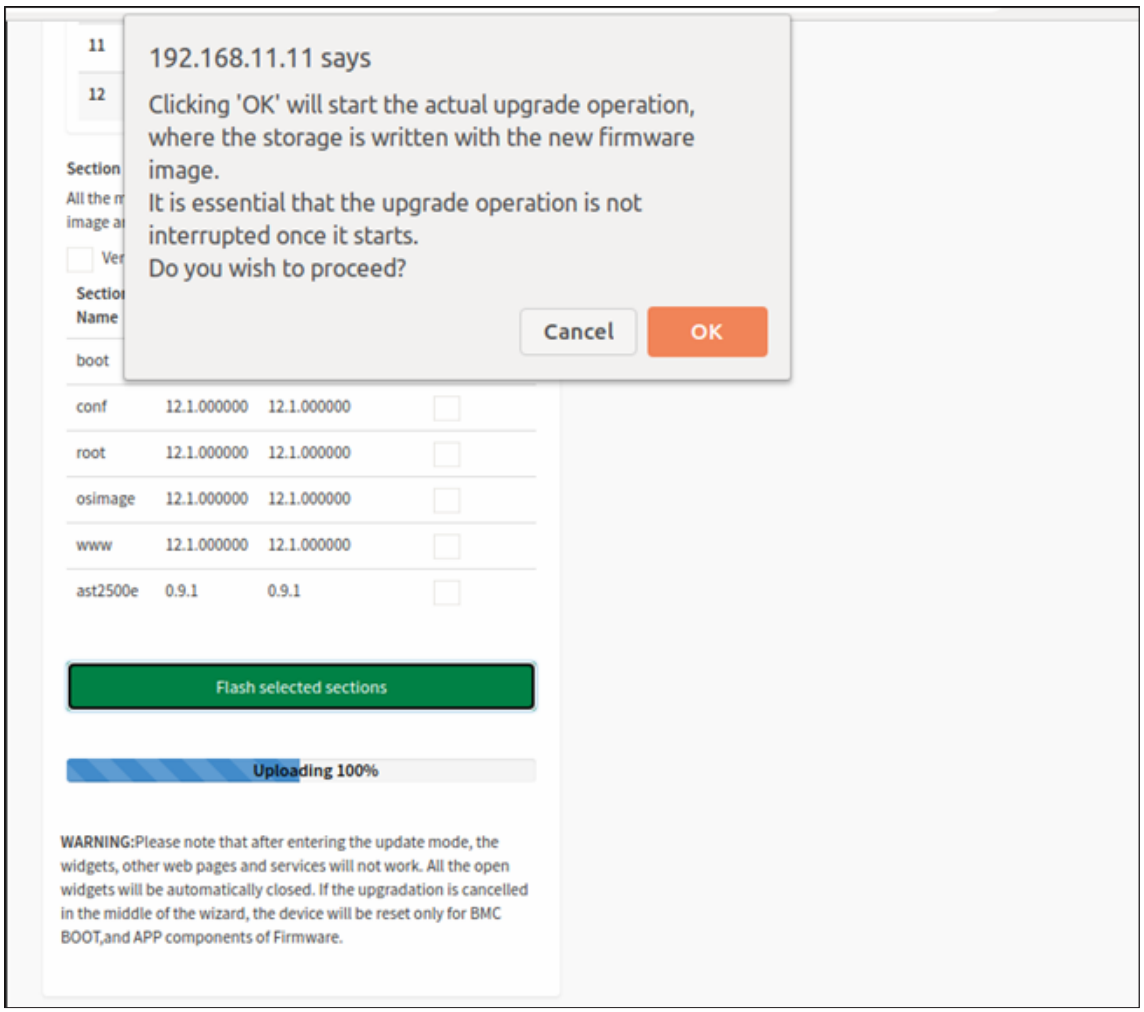
NOTE

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.



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

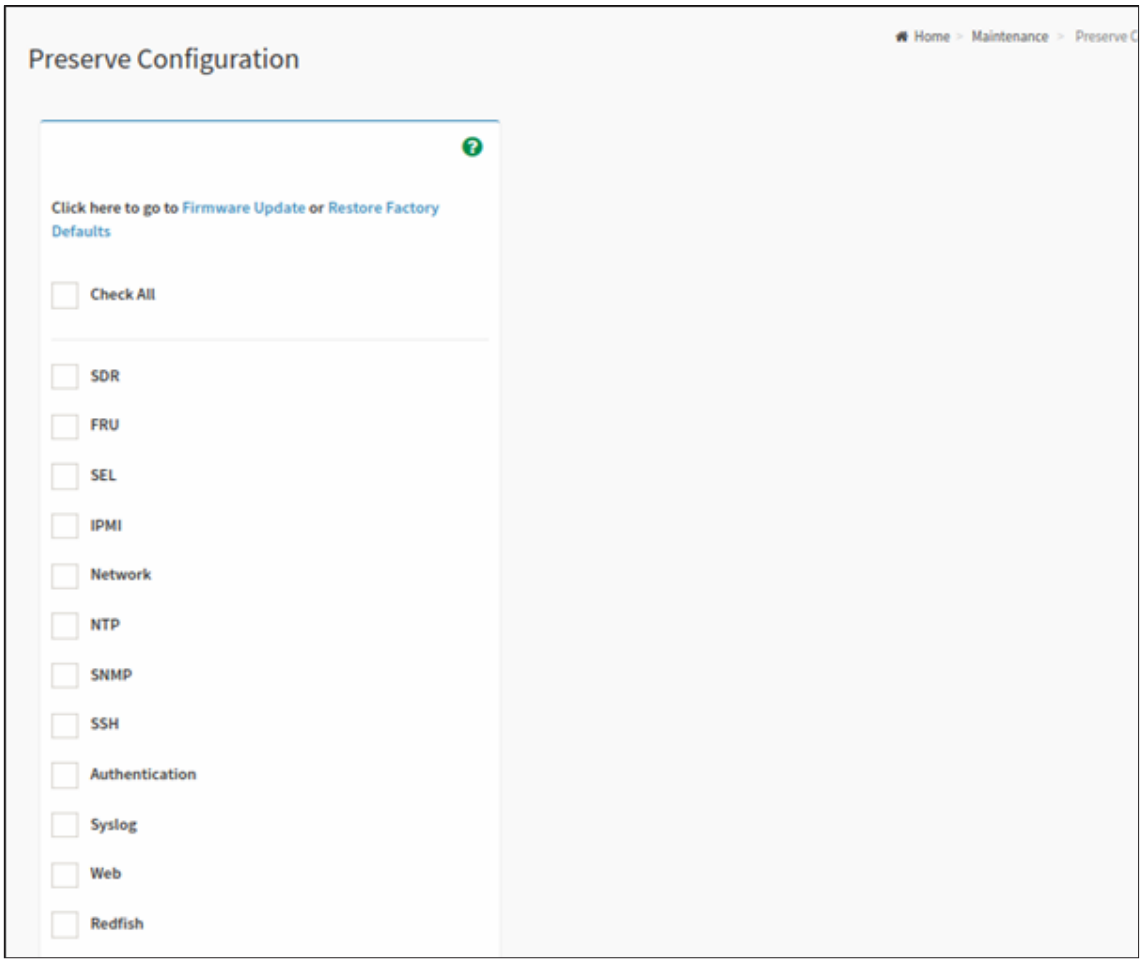
The Firmware Update page will be disabled and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset if update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

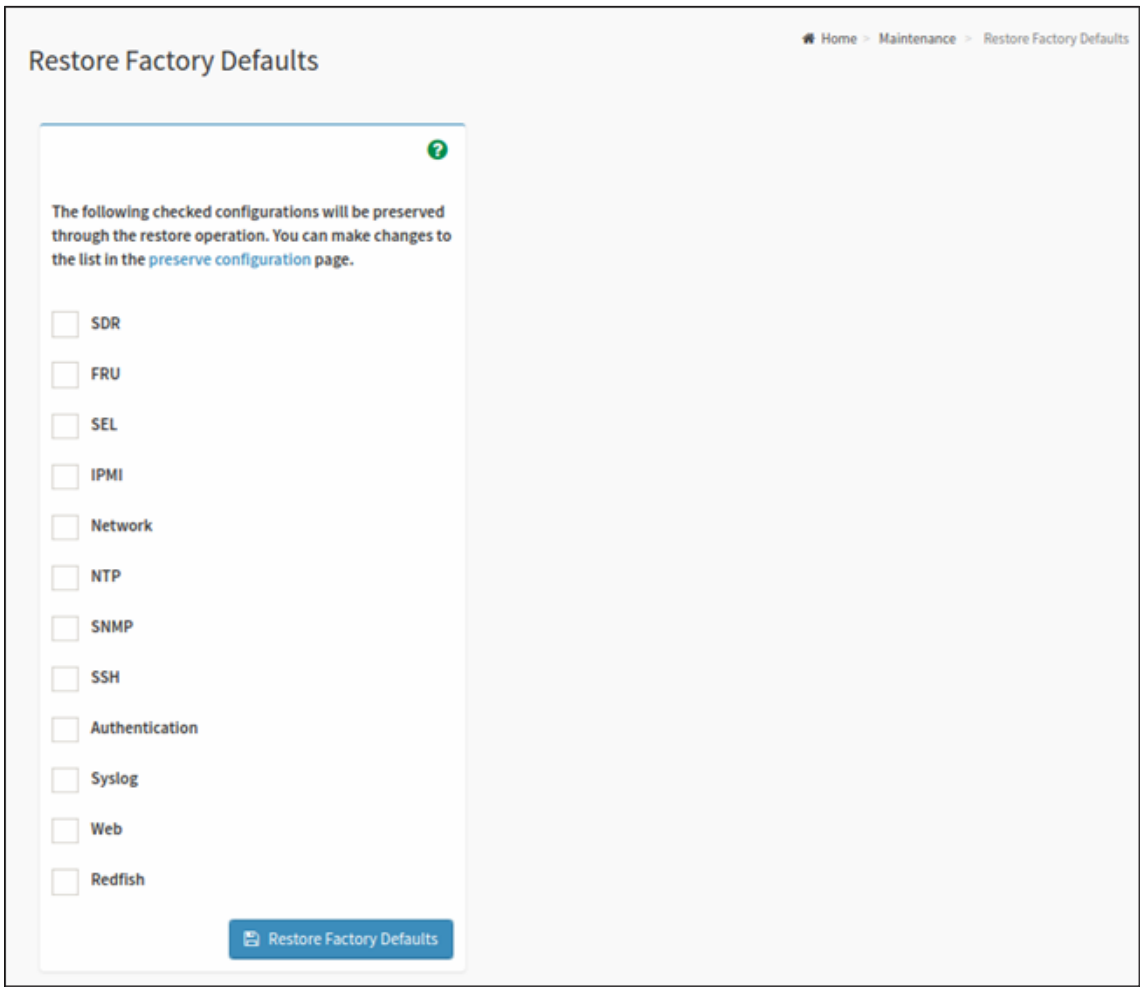
Restore Factory Defaults

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.

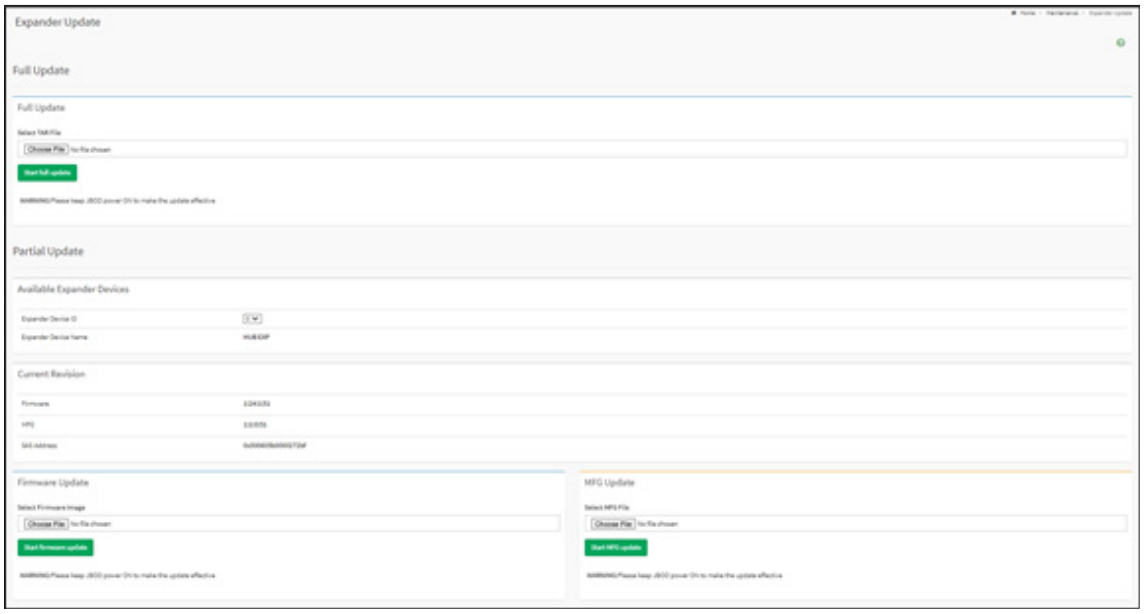
NOTE

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.



Expander Update page

Full Update

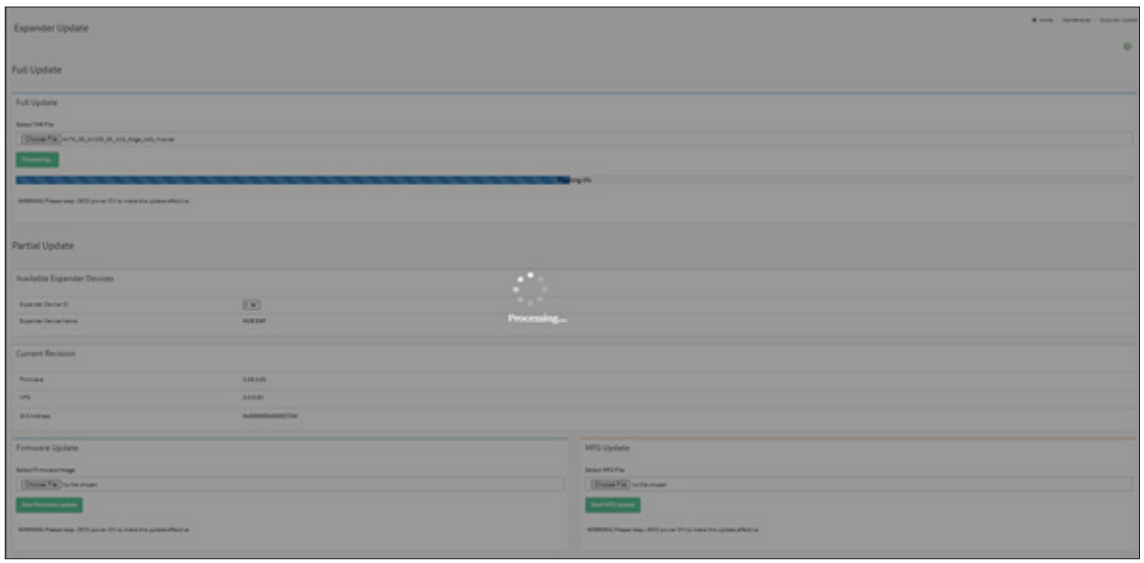
Use TAR archives for full expander updates.

Full Update:

a. Click Choose File to select firmware TAR file.

b. Click Start full update to update all Expander Firmware

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



Partial Update

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

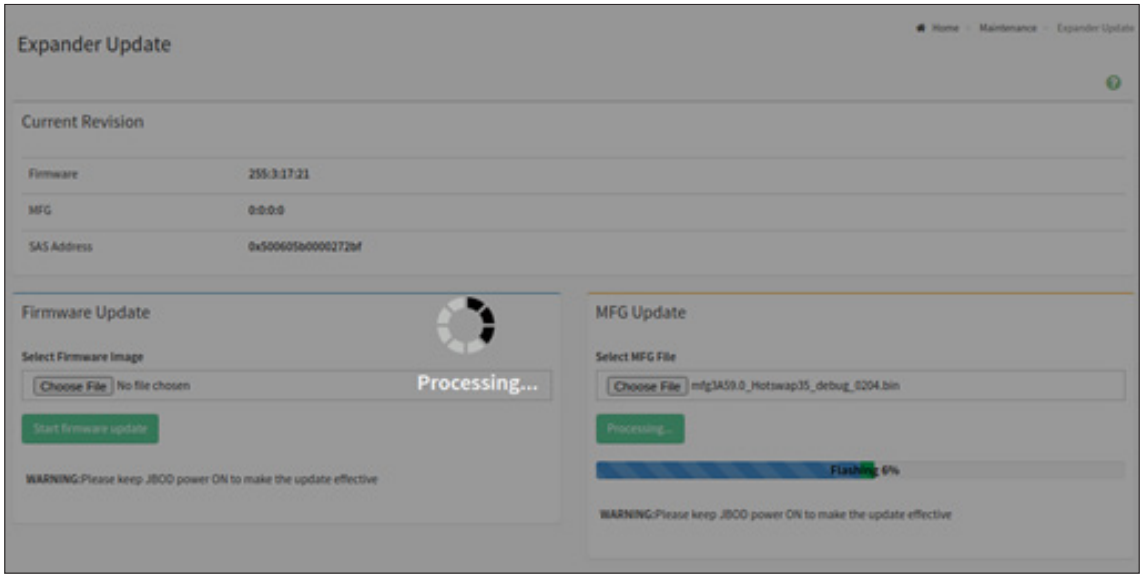
Firmware Update:

a. Click Choose File to select firmware image.
b. Click Start firmware update to update Expander Firmware

MFG Update:

a. Click Choose File to select firmware image.
b. 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.

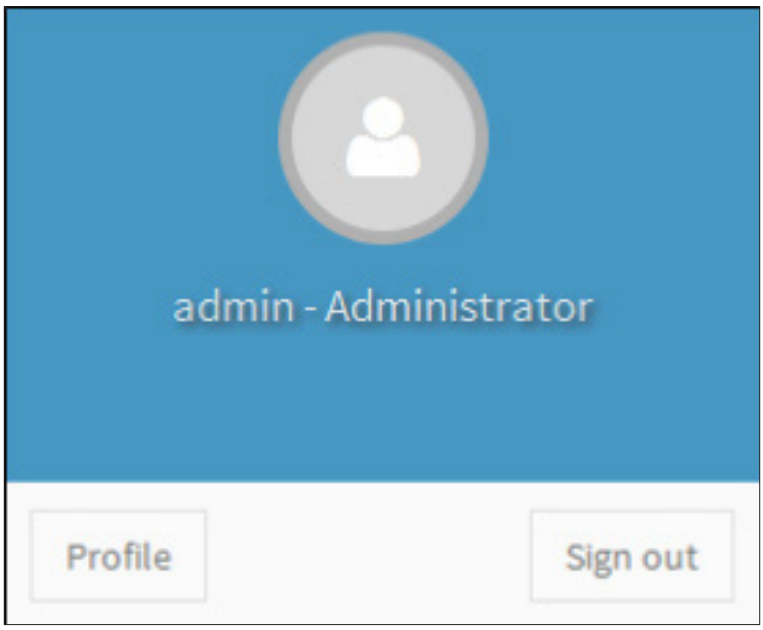
To open BMC Reset page, click Maintenance > BMC Reset from the menu bar. A sample screenshot of BMC Reset page is shown below.

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.

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 Boulvard 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

For additional technical support or questions about trouble shooting, please contact the AIC® representative nearest to you or visit our AIC® website for more information.
AIC® website: https://www.aicipc.com/en/faq.