J2024-08-04X

2U24 04X SAS4 HS JBOD
User's Manual

UM_J2024-08-04X_v1.1_061125

Table of Contents

Document Release History

Release Date	Version	Update Content
March, 2025	1	Release to public.
June, 2025	1.1	Update spec content(dimensions).

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 you commence, please attentively read the following important discretions below. All cautions and warnings on the equipment or in the manuals should be circumspectly noted and reviewed.

Always ground yourself to prevent static electricity.
請全程接地，以防止靜電。
请全程接地，以防止静电。
Всегда заземляйте себя, чтобы избежать статического электричества.
Aard jezelf altijd om statische elektriciteit te voorkomen.

- Firmly ground yourself at all times when installing or assembling the internal components of the server. Most of electronic components in the server are highly sensitive to electrical static discharge.
- Use a solid grounding wrist strap and distinctively place all electronic components in static-shielded devices to prevent static. Grounding wrist straps can be purchased in any electronic supply store.
- Confirm that the power source is turned off and then disconnect the power cords from your system before performing any type of installation or manual servicing. A sudden surge of power could severely damage the sensitive electronic components.
- Do not precipitously open the system's top cover. If you must open the cover for maintenance purposes, only a trained technician should be allowed to proceed this action. Integrated circuits on computer boards are highly sensitive to static electricity. Before operating a board or integrated circuit, touch an unpainted portion of the system unit chassis for a couple of seconds to discharge any static electricity on your body.

Place the server in a stable environment.
請將伺服器放置在穩定的環境中。
请将伺服器放置在稳定的环境中。
Поместите сервер в стабильную среду.
Plaats de server in een stabiele omgeving.

- Place this equipment on a stable surface when installing. A small mild drop or fall could cause fatal injury to both the equipment and the person handling the equipment.
- Please keep this equipment away from humidity to prevent vast rust and disintergration.
- Carefully and accurately mount the equipment into the rack. Uneven mechanical loading may lead to hazardous consequences.
- This equipment is to be installed for operation in an environment with maximum ambient temperature below 35°C.
- Review the environment before performing any installation or servicing. Keep the equipment away from hazardous and uneven grounds.
- This server must be installed only in Restricted Access Locations.

Handle equipment with care.
請謹慎操作設備。
请谨慎操作设备。
Обращайтесь с оборудованием осторожно.
Behandel de apparatuur voorzichtig.

- Do not cover the openings of the system. The openings on the system are for air convection, which intentionally protect the equipment from overheating.
- Never pour any liquid into ventilation openings of the system. This could cause catastrophic fire or electrical shock.

- Ensure that 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 must be within the specification.
- This equipment must be firmly connected to reliable grounding before usage. 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.

Pay attention to hardware maintenance.
注意硬體維護。
注意硬体维护。
Обратите внимание на обслуживание оборудования.
Besteed aandacht aan hardware-onderhoud.

- If the equipment is not used for a long time, disconnect the equipment from mains to avoid being damaged by transient over-voltage.
- Module and drive bays must not be empty. They must have a dummy cover.
- Never open the equipment without professional assistance. For safety reasons, only qualified service personnel should open the equipment.
- If one of the following situations arise, the equipment should be checked and tested 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.

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

CAUTION
There will be a risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. After performing any installation or servicing, make sure the enclosure is correct in position before turning on the power.

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 J2024-08-04X.
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 J2024-08-04X. For the latest version of this user's manual, please refer to the AIC® website: https://www.aicipc.com/en/productdetail/51573.

Chapter 1 Product Features

J2024-08-04X 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 Hardware Settings

This chapter provides details about backplane and expander board. These descriptions assist users to configure different settings and functions of the backplane, as well as to confirm the placement of each connector and jumper.

Chapter 4 Sub-system Configuration Setup

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

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

J2024-08-04X is a high performance JBOD product that includes 24 x 2.5" hot swap 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.

Pre-installed into the system		Number
✓	2.5-inch external hot swap disk drive tray	24
✓	easy swap 60*56mm fan	4
✓	36-inch tool-less slide rail assembly	1
Accessory Item		**Number**
✓	EPE foam for front board: 563*420*105H	1
✓	EPE foam for rear board: 563*420*105H	1
✓	EPE foam for front tray: 563*300*145H	1
✓	EPE foam for rear tray: 563*300*145H	1
✓	EPE pad for rail: 130*100*40T	2
✓	800W redundant power supply 80+ Platinum/ Titanium	1+1
BTO	Power cord	vary per region

Product features are subject to change without notice.

1.2 Specifications

General	Number of Expander	Dual
	Expander Chip	LSI SAS4X40
	Host/Expansion Interface	4 x Mini-SAS HD (SFF-8674) per expander module
Drives Supported	Drive Interface	12Gb & 6Gb SAS/SATA
	Form Factor	3.5”
Administration / Management	Admin/Firmware Upgrade	• In-band & Serial port interface • IEM port
	LED Indicators, Audible Alarm	Yes
Hot swap and Redundancy	Disk Drive	24 hot swap
	Cooling	4 x 60x56mm easy swap fans
	Power Supply	800W 1+1 hot swap redundant 80+ Platinum/Titanium
Hot swap and Redundancy	Power Entry	Dual AC Inlet
	Expander Modules	Dual expanders (Optional)

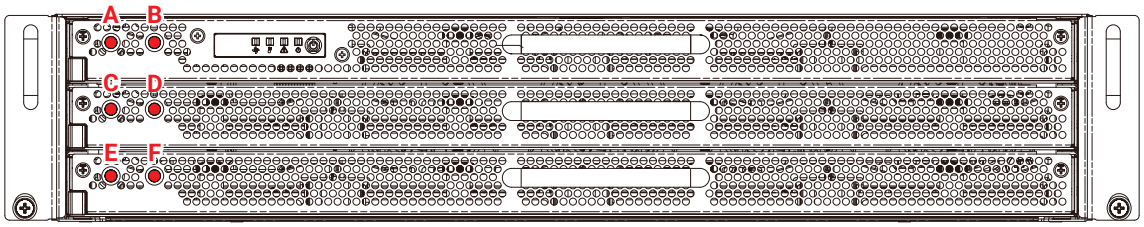
Electrical and Environmental	Universal A/C Input	• 100-127V~, 50/60Hz, 10A • 200-240V~, 50/60Hz, 5A
	Operating Environment	• Temperature : 0ºC to 35º C • Relative humidity : 20% to 80 %
	Non-operating Environment	• Operating altitude condition : 0 ~ 10K ft • Storage temperature : -20° ~ 60° C • System relative humidity : 10% - 90%
Physical Specification	Dimensions (W x D x H)	mm : 438 x 838 x 8 8
		inches : 17.24 x 33 x 3. 5
	Gross Weight (w/ PSU, Rail; w/o Pallet, Disks)	kgs : 34.35
		lbs : 75.7
	Packaging Dimensions (W x D x H)	mm : 605 x 1140 x 308
		inches : 23.8 x 44.9 x 12.1
Mounting	Standard	36” slide rail

J2024-08-04X is a reliable SAS JBOD with 24 hot swap drives bays. This product is designed to accommodate single expanders with 4 Mini SAS HD. Featuring the expander chip, LSI SAS4x40, 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.

- 2U with 24-bay hot-swap LFF 3.5” drive bays
- 4 x SAS-4 24G Mini-SAS host port per expander module
- Built-in RTC module for reliable timekeeping
- Less than 33” without Cable Management Arm (CMA)
- Redundant 80+ Platinum and Titanium level hot-plug power supplies

1.3 Feature

Front Panel

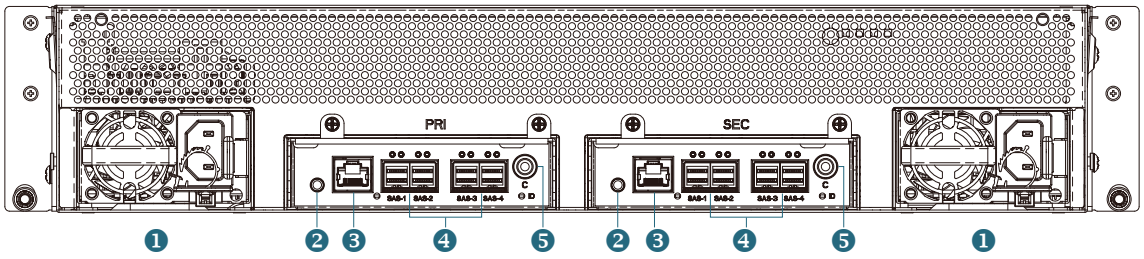


Item	Description		
	Power Button	Normal	Off
		Press	Boot off
		Long Press	System shutdown
	Power Status LED	On	Blue
		Off	Off
		ID	Blue (blinking)
	Power Failure LED	Normal	Off
		Failed	Red
	Temperature Failure LED	Normal	Off
		Failed	Red
	Fan Fault Status LED	Normal	Off
		Failed	Red

Item	Description
A	1~4 HDD Fail LED
B	5~8 HDD Fail LED
C	9~12 HDD Fail LED
D	13~16 HDD Fail LED
E	17~20 HDD Fail LED
F	21~24 HDD Fail LED

Item	Color	Description
HDD Fail LED	Off	Normal
	Red	When any HDD is detected to have failed in each row.

Rear Panel

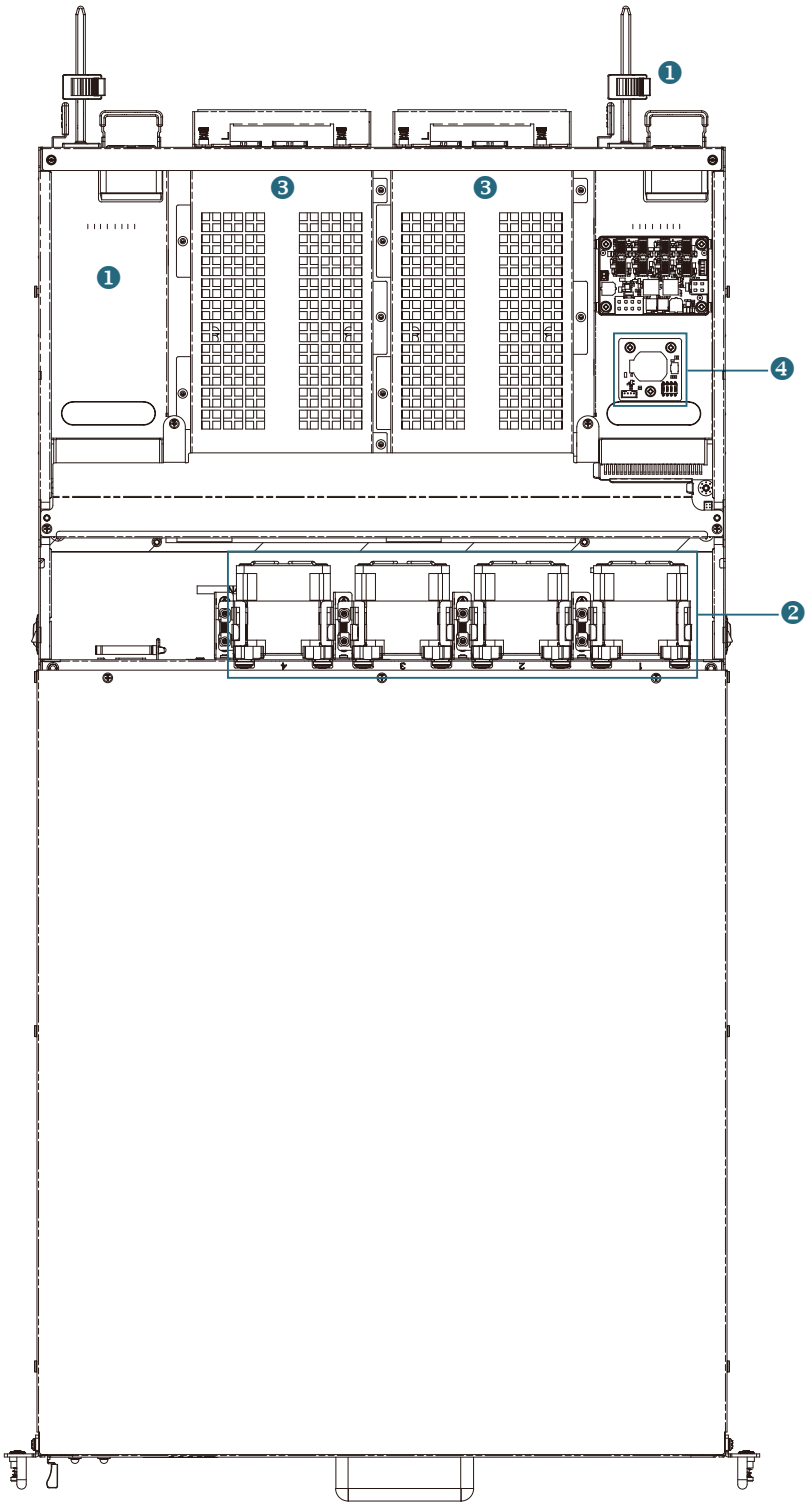


Item	Description
1	800W 1+1 redundant power supply 80+ Platinum/Titanium
2	2 * BMC console port (1 per expander)
3	2 * BMC LAN port (1 per expander)
4	8 * SFF-8644 wide port (per expander moudule)
5	2 * Expander console port (1 per expander)

LED Indicator

Item	Color	Description
PSU LED	Green	OK
	Green (blinking)	Ready
	Amber	Failed
	Amber (blinking)	Warning
Fan LED	Green	Normal
	Red	Failed
Expander SAS ports LED	Off	No connection
	Blue	Normal
	Red	Failed
Expander BMC LED	Blue (blinking)	Normal
	Red	Get sensor failed
Expander ID LED	Off	Normal
	Blue (blinking)	Identity

Top View

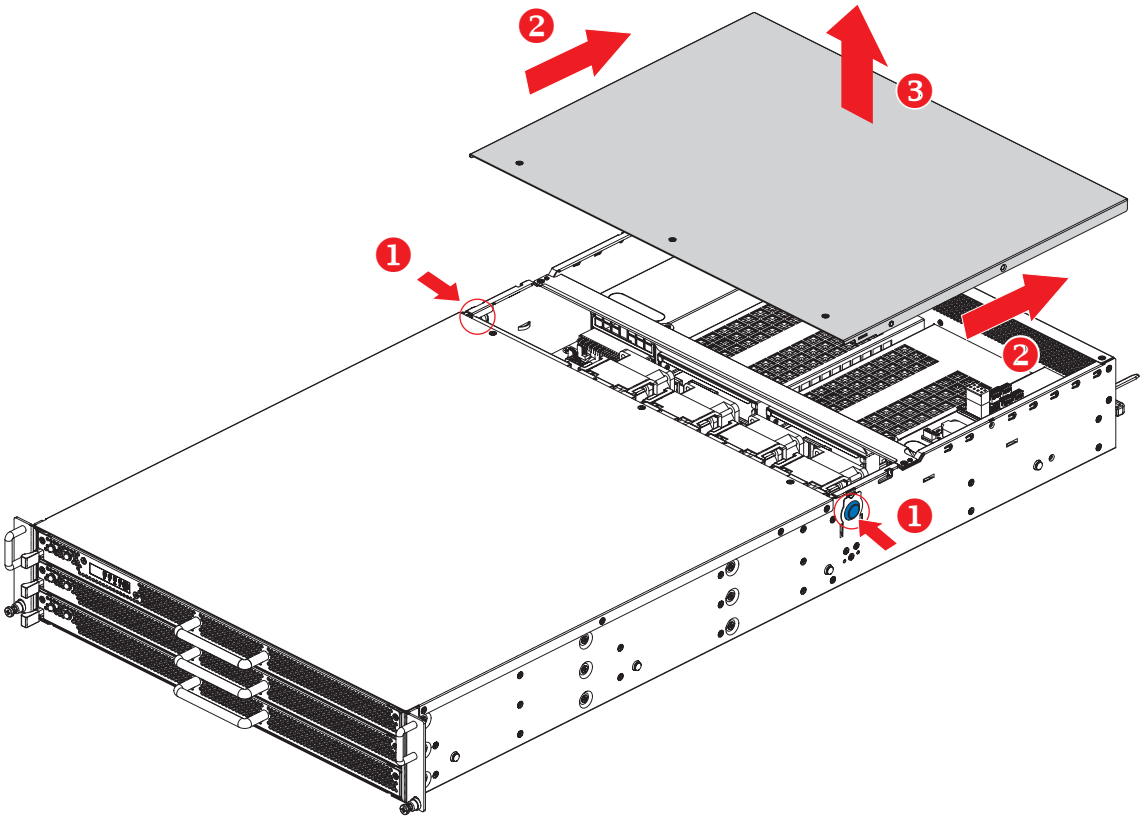


Item	Description
1	800W 1+1 redundant power supply 80+ Platinum/Titanium
2	4 x 60x56 easy swap fans
3	Dual Expanders (optional)
4	RTC board

Chapter 2. Hardware Setup

2.1 Top Cover

① Press the release button on the both side of the chassis.
② Push the top cover towards the rear panel.
③ Lift the top cover upward to remove.

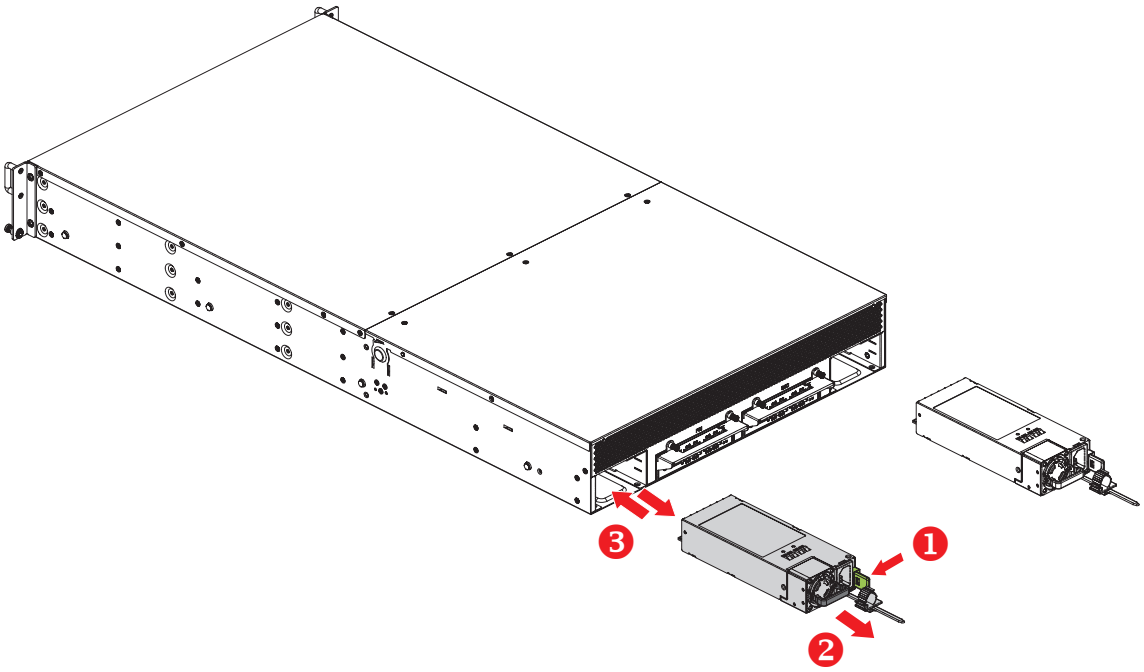


This information is provided for professional technicians only.

2.2 Power Supply Unit

2.2.1 Installation

① Press the ejector to release the module.
② Pull the handle to remove the module out of the chassis.
③ Push the replaced power supply unit into the chassis. Ensure that the module is hooked into the cage.



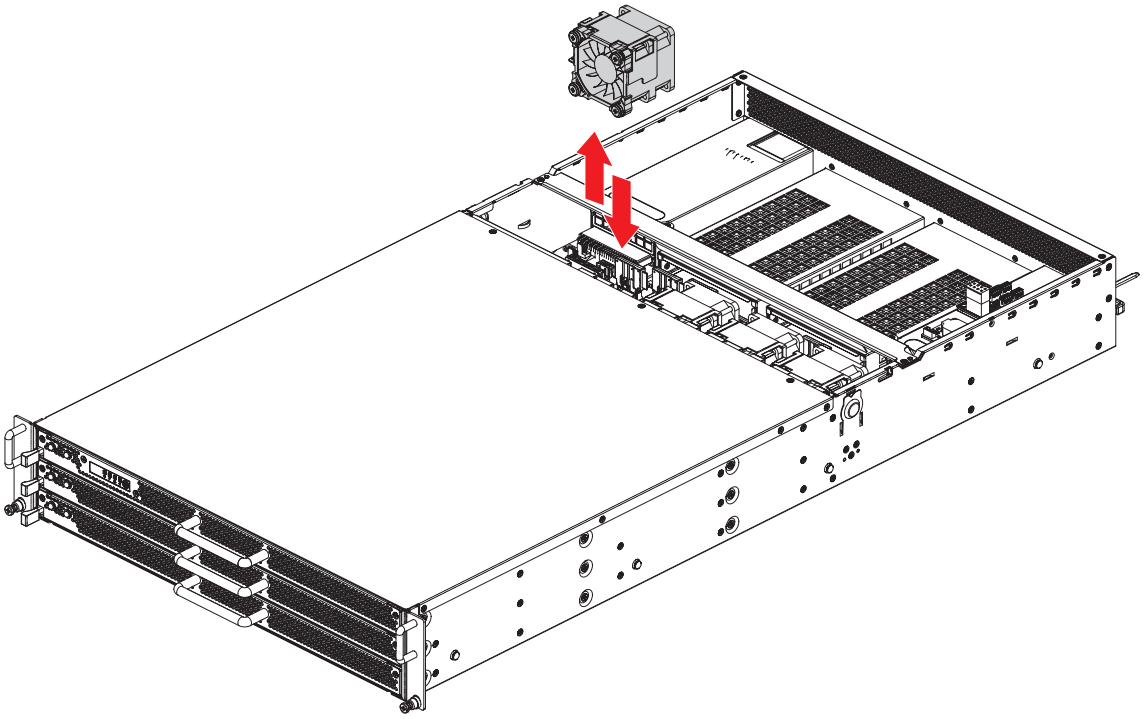
2.2.2 LED Indicator

Indicator Color	Behavior
Green (solid)	Power is on.
Green (blinking)	Only 12Vsb (PS off) or PSU is in cold redundant state
Red (solid)	Power has failed.

This information is provided for professional technicians only.

2.3 Fan

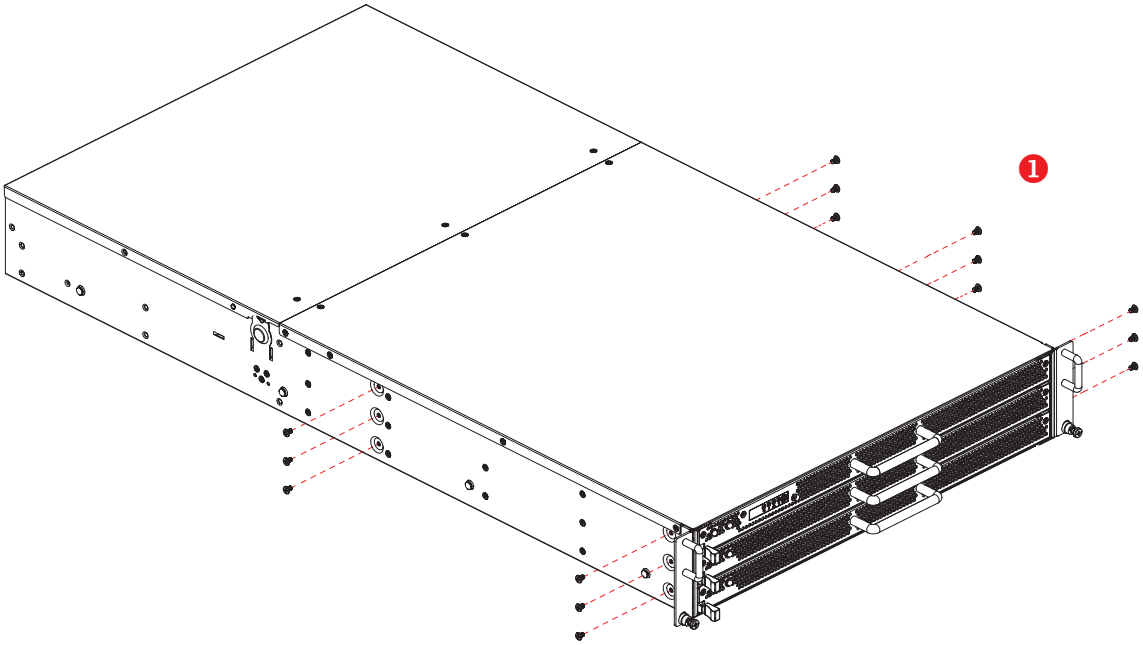
① Remove the top cover. Please refer to Section 2.1 Top Cover.
② Unplug the fan cables and connectors from the server board.
③ Pull the fan out of the chassis.

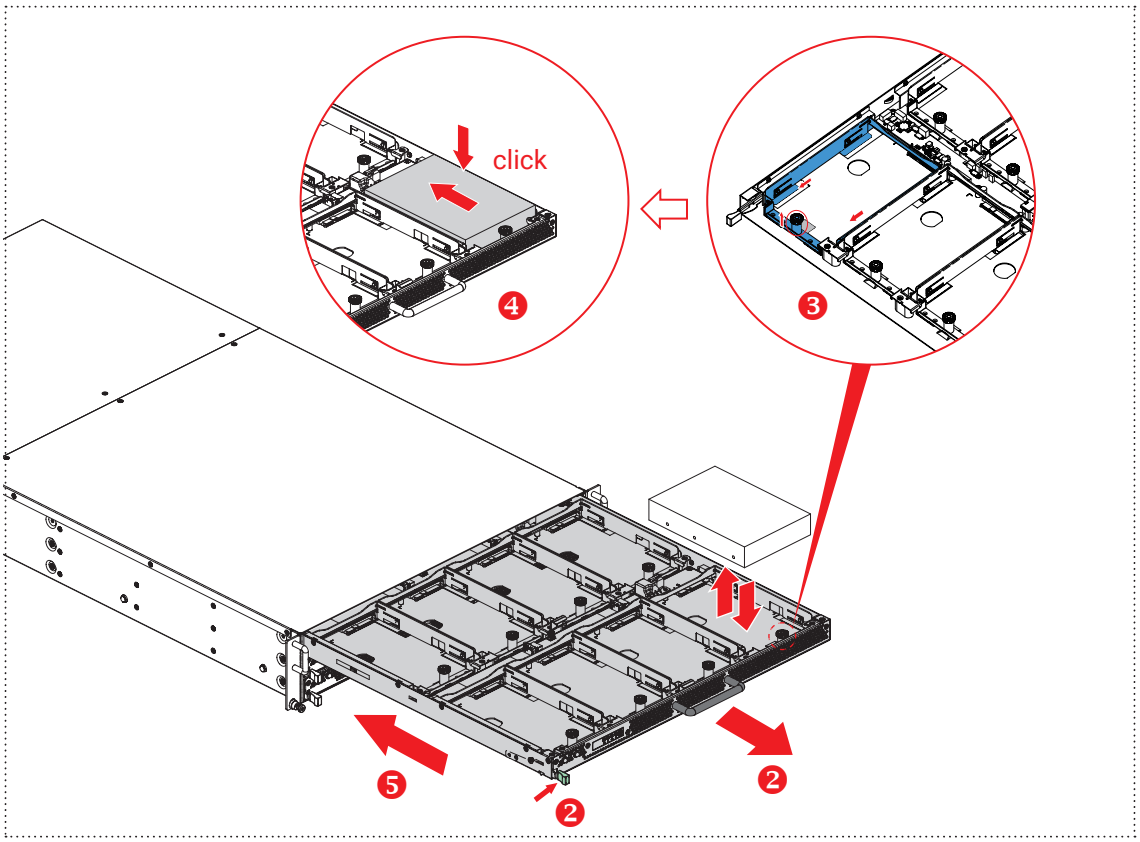


This information is provided for professional technicians only.

2.4 Hard Disk Drive

① Dislodge the screws on the both side of chassis.
② Press the ejector and pull the HDD plate outward.
③ Pull the plunger upward, and the HDD tray will pop forward, then lift the HDD upward to remove.
④ Insert the replaced HDD into the chassis. Ensure that the HDD is aligned and locked into the tray.
⑤ Push the HDD plate into the chassis to complete installation.

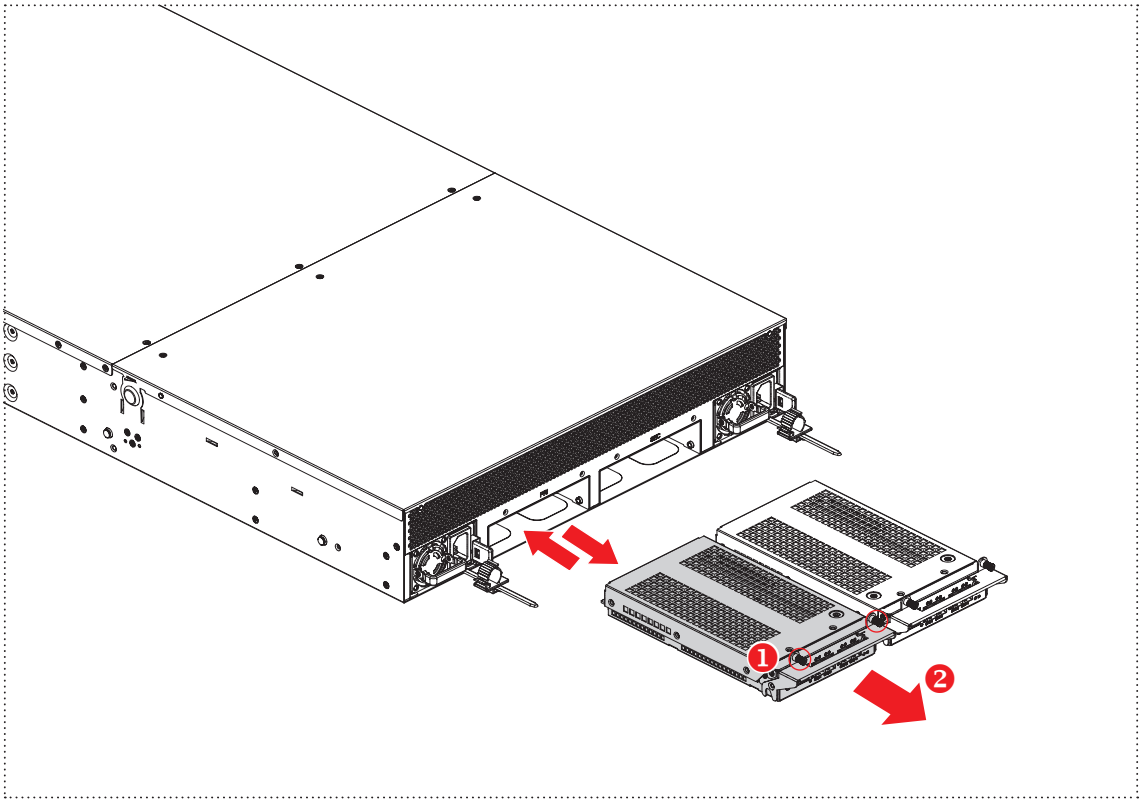




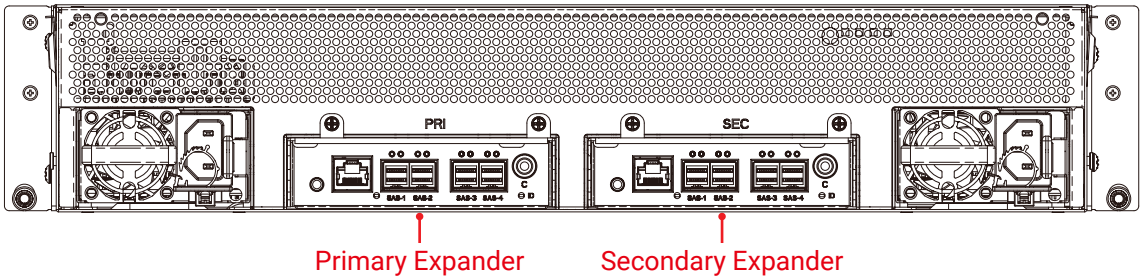
This information is provided for professional technicians only.

2.5 Expander

① Loosen the captive screw on the module.
② Pull the tray handle to remove the expander.



Rear panel



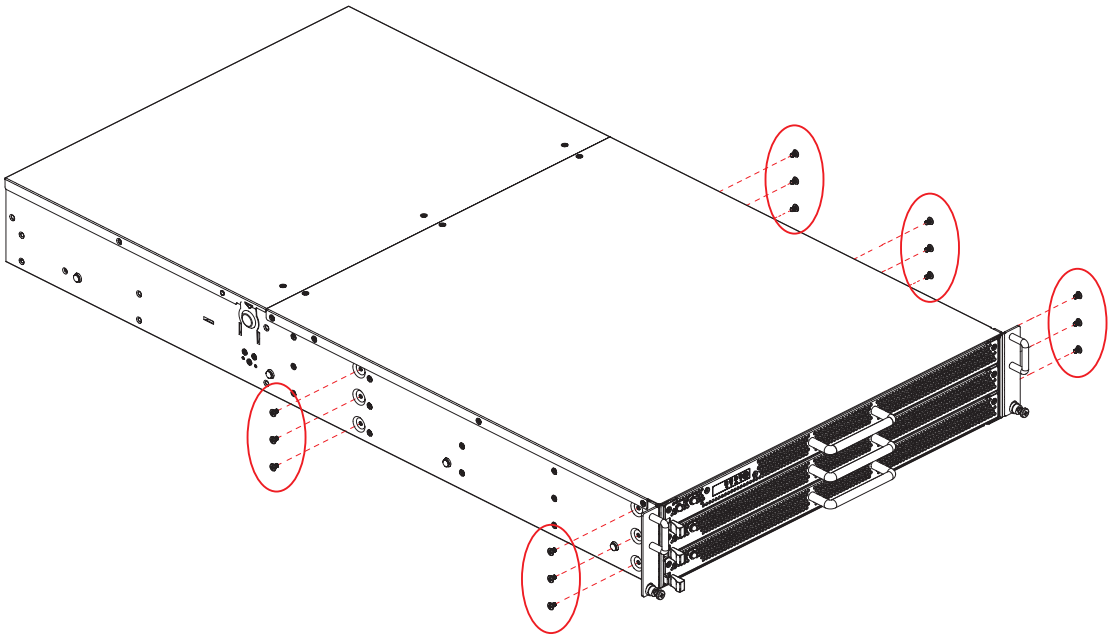
This information is provided for professional technicians only.

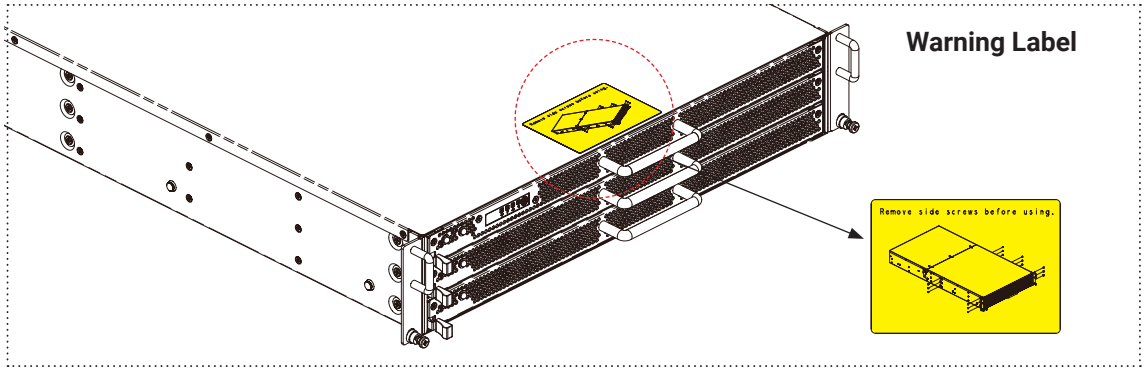
2.6 Slide Rail

NOTE
This section provides a basic instruction for mounting the slide rail onto the system. Tool-less rails vary per order. The rail in this manual may not exactly match the rail for your system. Please refer to the specifications or quick installation guide that came with your purchased product.

CAUTION
They rack may tilt and fall due to incorrect installation or placed on uneven grounds. The rack must be placed in a flat surface before you begin to slide the system barebone in for servicing.

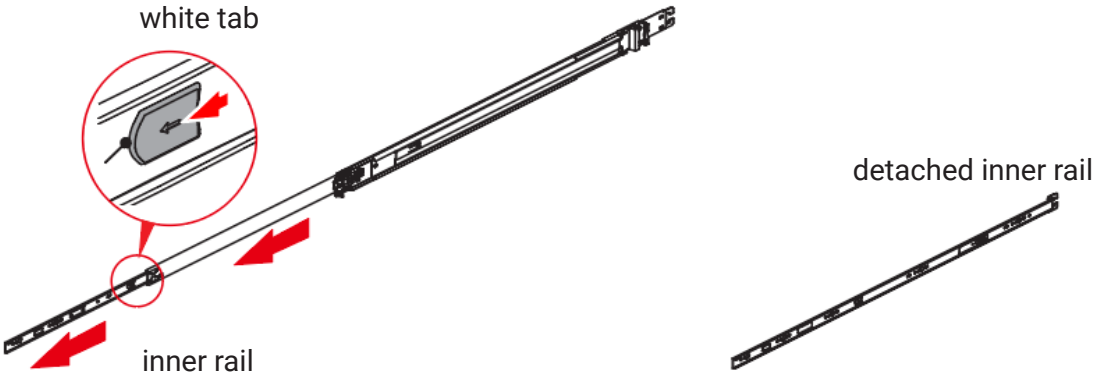
NOTE
The screws*15 in the red circle below are for transportation safety. Please ensure that all the screws have been removed before installing the chassis onto the slide rail. (Also, there is no necessary to fasten the screws back to the chassis.)



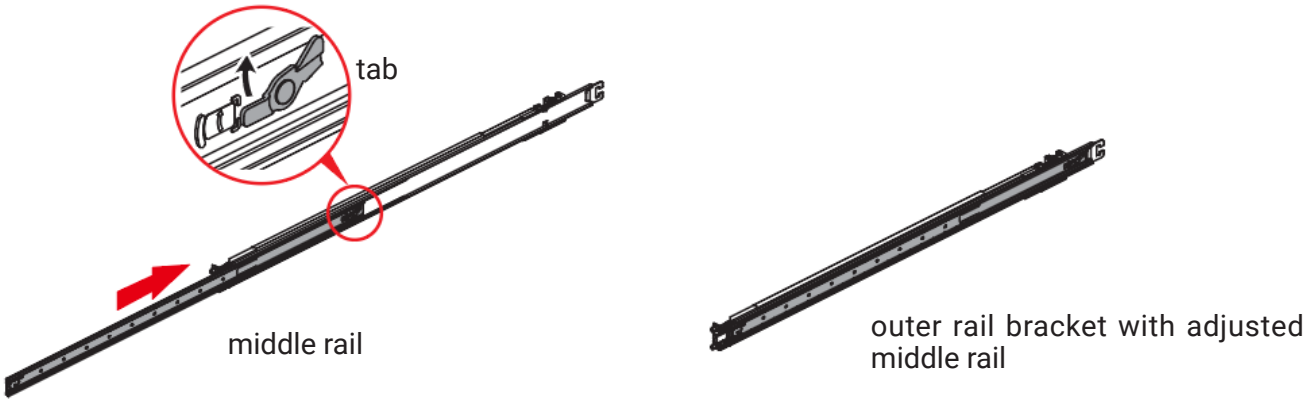


Length	Elongation length	Available cabinet rack (without CMA)
932.8 mm	611.8 mm	1000mm

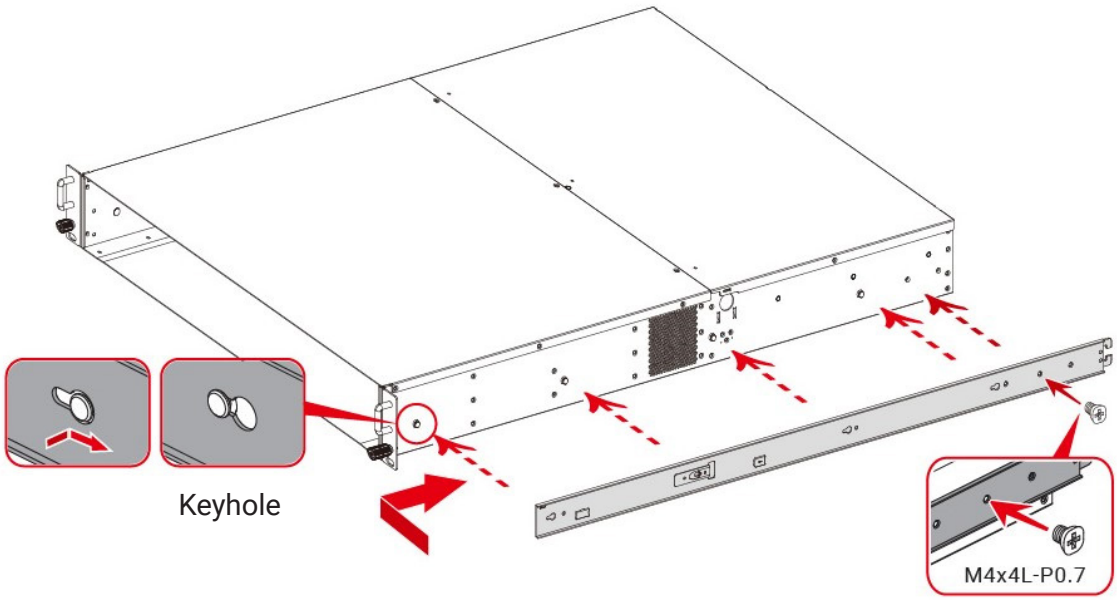
1. Pull the inner rail out of the slide rail until it clicks.
2. Detach the inner rail completely from the slide rail by pulling the white tab forward.



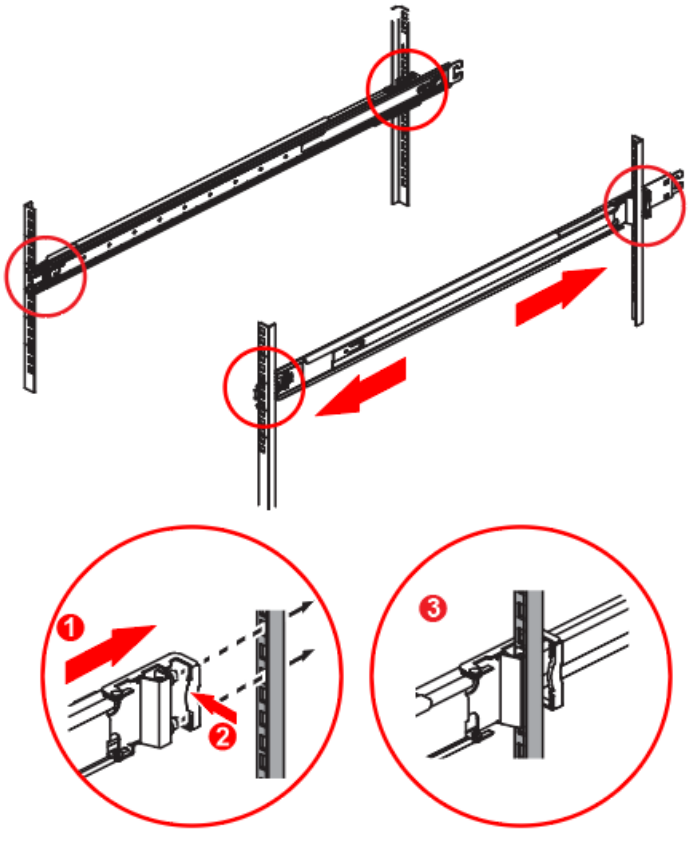
3. After the inner rail is dislodged, adjust the middle rail back to its original position by pushing the tab on the middle rail.



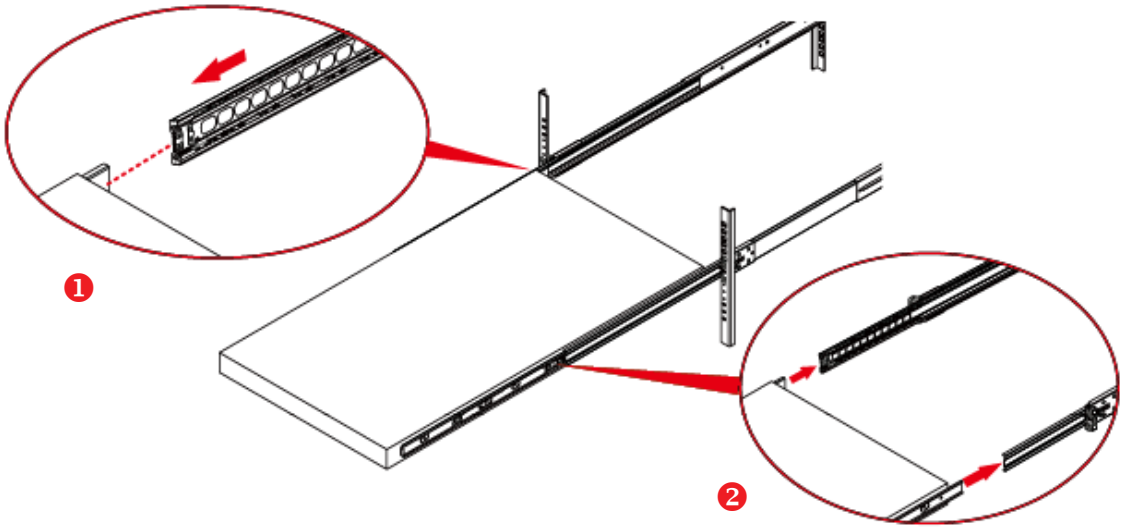
4. Install the inner rail onto the system barebone. Lock the keyholes and secure the screws on sides of the system.



5. Continue installing the outer rail bracket to the mounting frame. Attach the outer rail assembling to the frame and press the bracket to form a rack on both ends. Repeat to fully mount the bracket assembly on the other side.

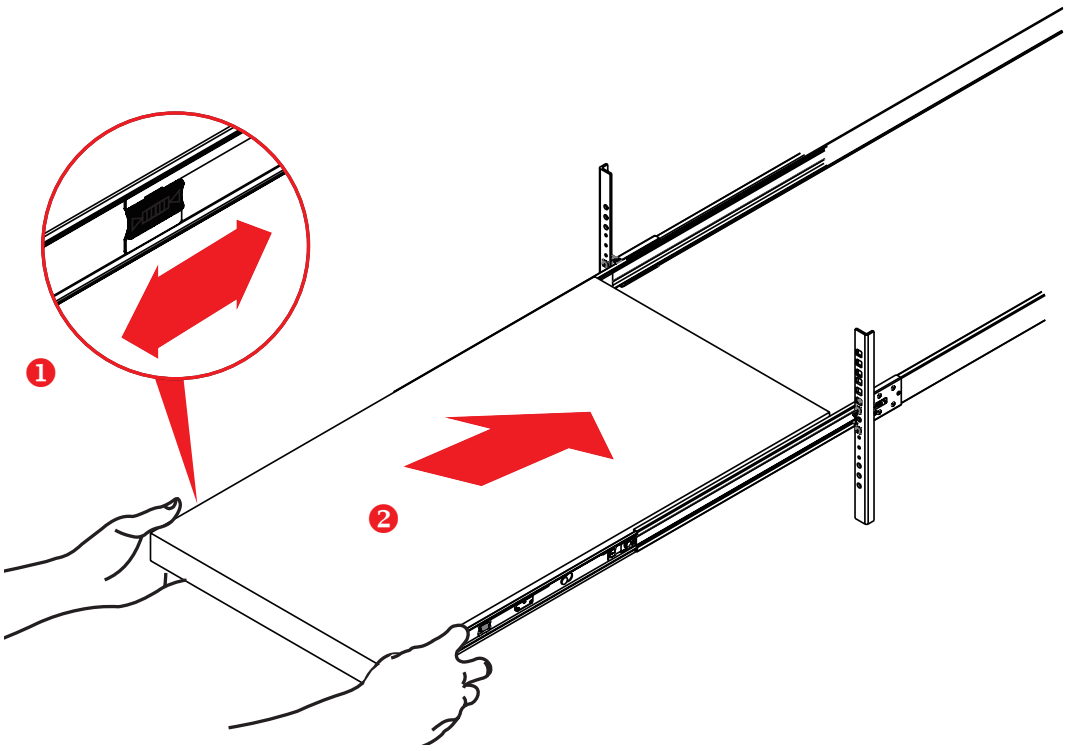


6. Pull out the middle channel until the ball bearing retainer is locked forward.



NOTE
Verify ball bearing retainer is locked forward.

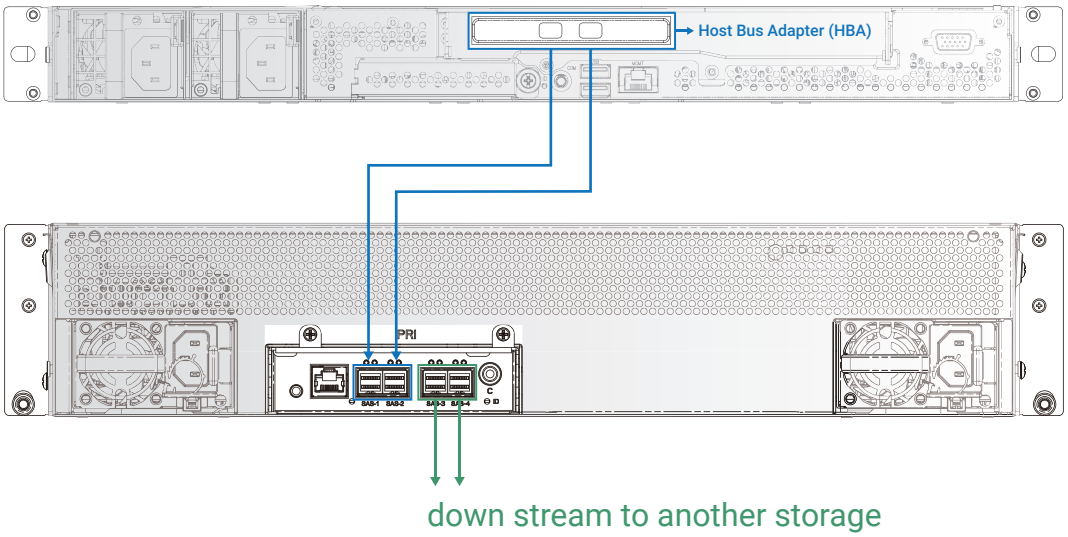
7. Slide the release tab and push barebone into rack. Make sure the barebone is completely installed onto the rack.



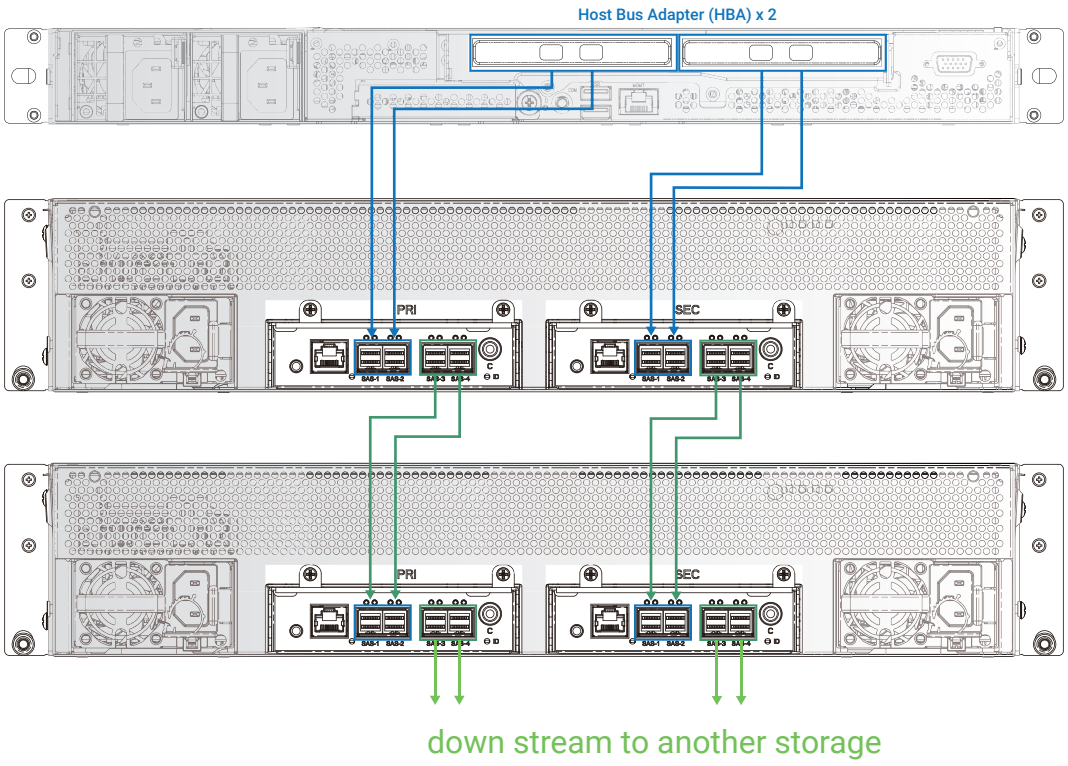
This information is provided for professional technicians only.

2.7 Standard Cabling

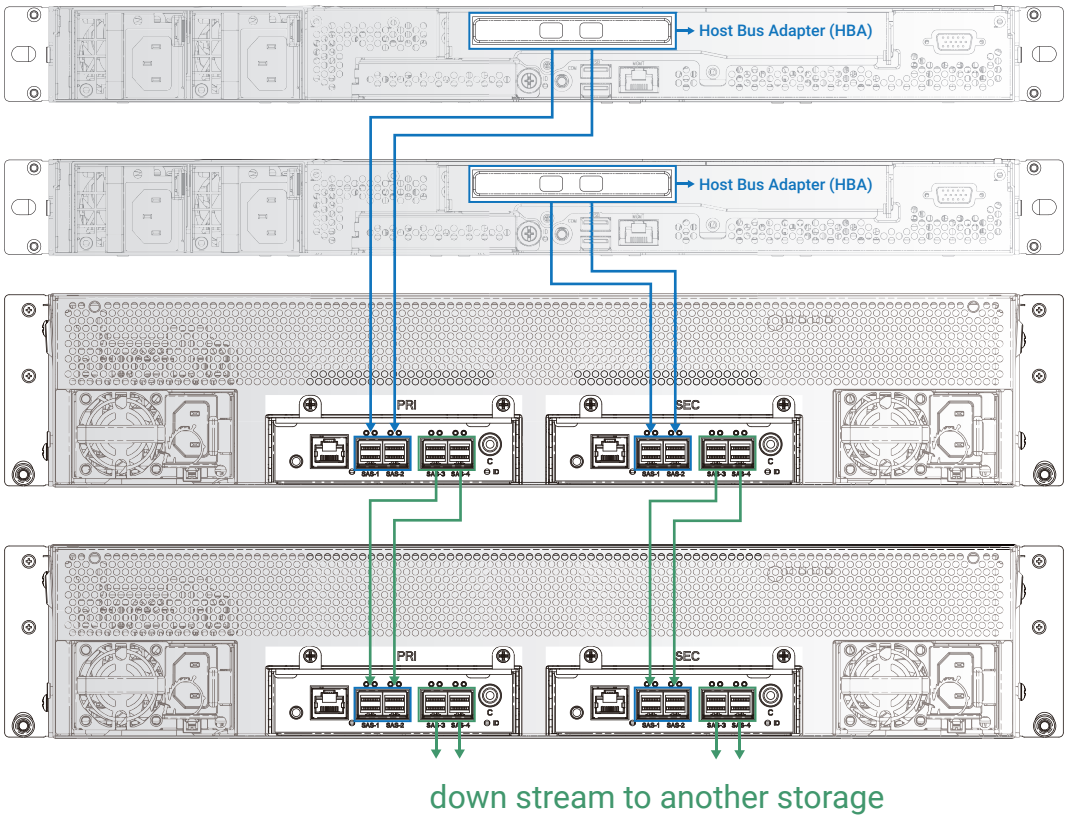
2.7.1 Single expander JBOD and 1 host server with 1 HBA card



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



2.7.3 Dual expander JBOD and 2 host servers with 1 HBA card

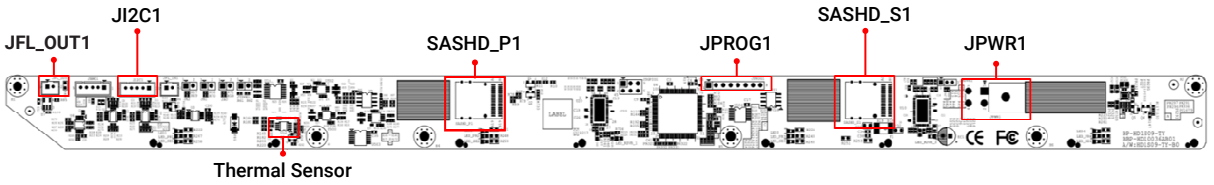


Chapter 3. Hardware Settings

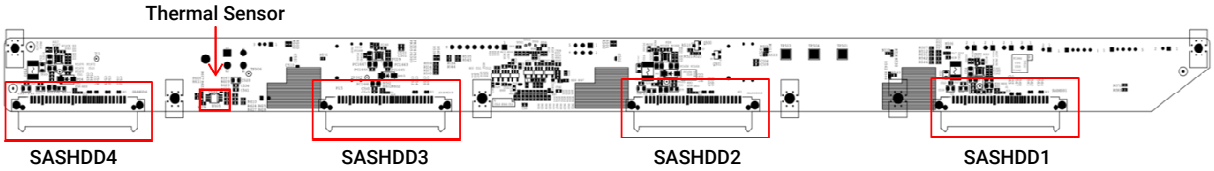
3.1 Drive Backplane: 4 Bay

3.1.1 Placement

Top view



Bottom view

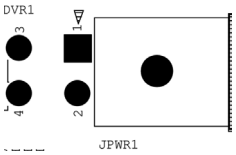


3.1.2 Connector

Connectors Summary

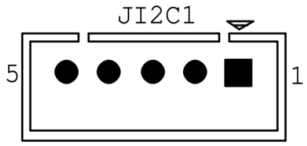
Connector	Description	Function
Dual SAS3.0	SFF-8680	SASHDD1, SASHDD2, SASHDD3, SASHDD4
Slimline	SFF-8654	SASHD_P1, SASHD_S1
Power	2 x 2 Pin 4.2mm ATX Power Connector	JPWR1
I2C (HDD fault LED control)	Box Header, 1x5p	JI2C1
LED (BP fault Indicator)	Box Header, 1x2p	JFL_OUT1
CPLD programming	Pin Header, 1x8p	JPROG1

Power Connector (JPWR1)



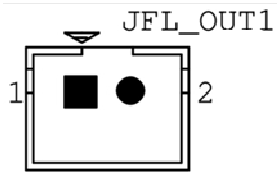
1	GND
2	GND
3	+12V
4	+12V

I2C Connector (JI2C1)



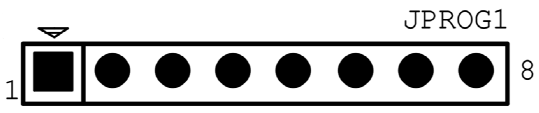
1	GND
2	PR_I2C_SCL
3	PR_I2C_SDA
4	SE_I2C_SCL
5	SE_I2C_SDA

LED Connector (JFL_OUT1)



1	LED_FAULT
2	+3V3

CPLD programming Pin Header (JPROG1)

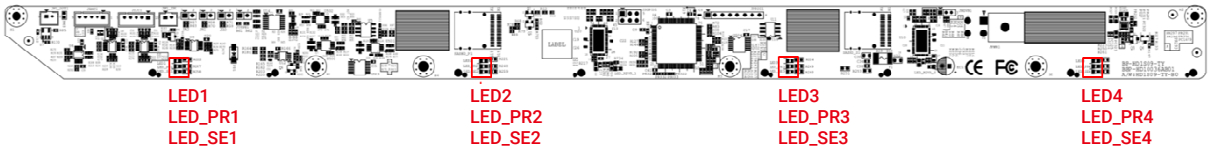


1	+3V3
2	TDO
3	TDI
4	PROGRAM_L
5	INTI_L
6	TMS
7	GND
8	TCK

3.1.3 LED Indicator

Indicator	Color	Description
LED1	Blue (Blinking)	SASHDD1 SSD Activity
	Off	SASHDD1 SSD not activity detected
LED_PR1 / LED_SE1	Red	SASHDD1 SSD Fault
	Off	SASHDD1 SSD Normal
LED2	Blue (Blinking)	SASHDD2 SSD Activity
	Off	SASHDD2 SSD not activity detected
LED_PR2 / LED_SE2	Red	SASHDD2 SSD Fault
	Off	SASHDD2 SSD Normal
LED3	Blue (Blinking)	SASHDD3 SSD Activity
	Off	SASHDD3 SSD not activity detected
LED_PR3 / LED_SE3	Red	SASHDD3 SSD Fault
	Off	SASHDD3 SSD Normal
LED4	Blue (Blinking)	SASHDD4 SSD Activity
	Off	SASHDD4 SSD not activity detected
LED_PR4 / LED_SE4	Red	SASHDD4 SSD Fault
	Off	SASHDD4 SSD Normal

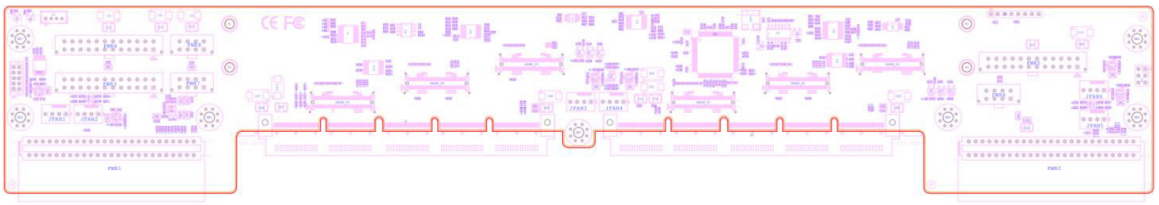
Placement



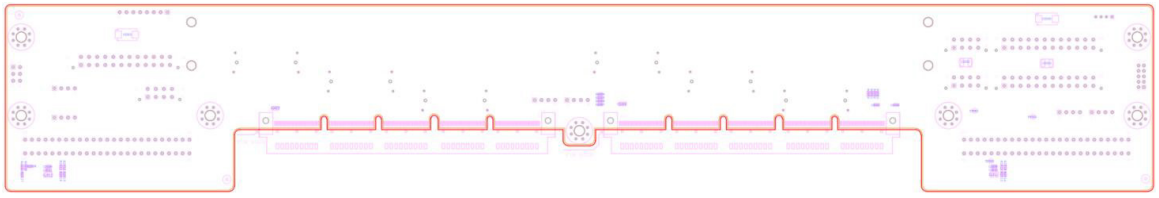
3.2 Bridge Board

3.2.1 Placement

Top view



Bottom view



External Connectors

Connector	Description	Function
PSU1-2 (PWR1,2)	CRPS	12V PWR, 12V_STBY PWR
EXPANDER BOARD (J5,J6)	GenZ_280P	GenZ_8C_STRADDLE(PCIE GEN5)

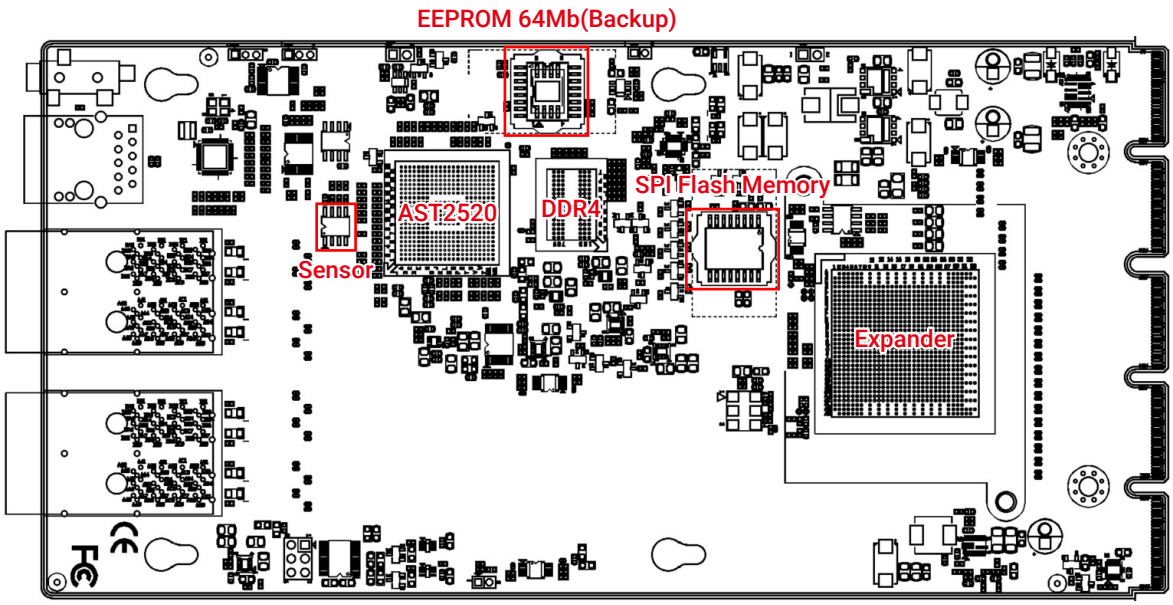
Internal Connectors

Connector	Description	Function
SASHD_P1-3	SLIMLINE 74P	SLIMLINE_VERTICAL_SMD(PCIe GEN5)
SASHD_S1-3	SLIMLINE 74P	SLIMLINE_VERTICAL_SMD(PCIe GEN5)
PWR3,4,5	ATX_12X2P	12V PWR
PWR6,7,8	ATX_4X2P	12V PWR
FRONT PANEL(J1)	Header_2X5P	LED
FAN1-6(JFAN1-6)	Header_1X4P	FAN

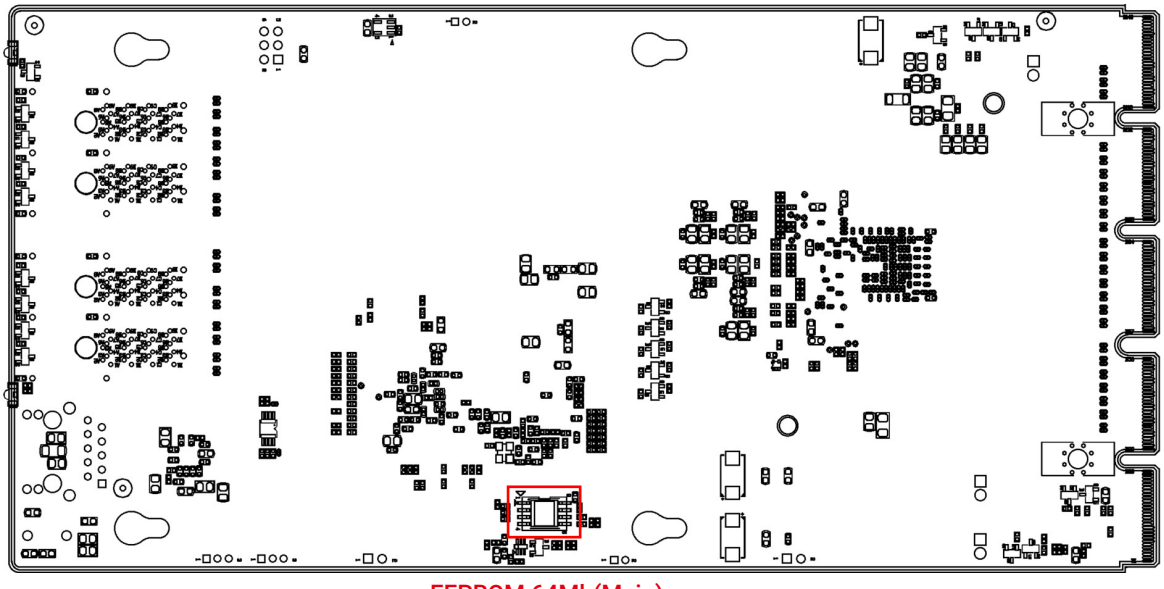
3.3 Expander Board

3.3.1 Placement

Top view



Bottom view



3.3.2 Connector

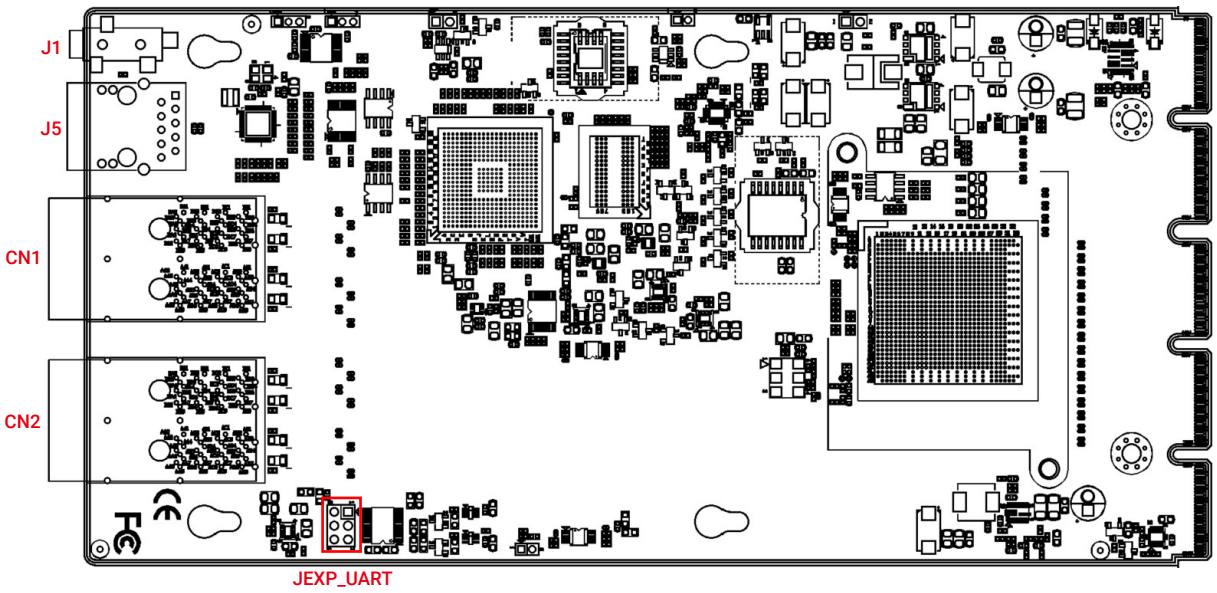
External Connectors

Connector	Description	Function
MiniSAS-HD (CN1,CN2)	72 pin MiniSAS-HD 8x	SAS Host/Up/Down connection
BMC UART(J1)	Phone Jack(3.5mm)	Debug/Smart port
10/100/1000 LAN(J5)	RJ45 connector	SOL Link

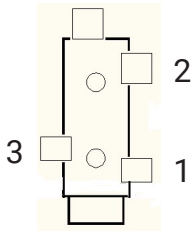
Internal Connectors

Connector	Description	Function
UART (JEXP_UART)	3 x 2 Pin Header	Expander SMART/DEBUG port.

Location

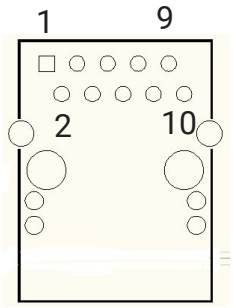


BMC UART (J1)



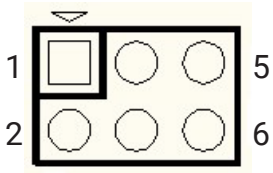
1	GND
2	RX
3	TX

10/100/1000 LAN (J5)



1	MDI0_PHY_P
2	MDI0_PHY_N
3	MDI1_PHY_P
4	MDI1_PHY_N
5	GND
6	GND
7	MDI2_PHY_P
8	MDI2_PHY_N
9	MDI3_PHY_P
10	MDI3_PHY_N

Console for Expander (JEXP_UART)



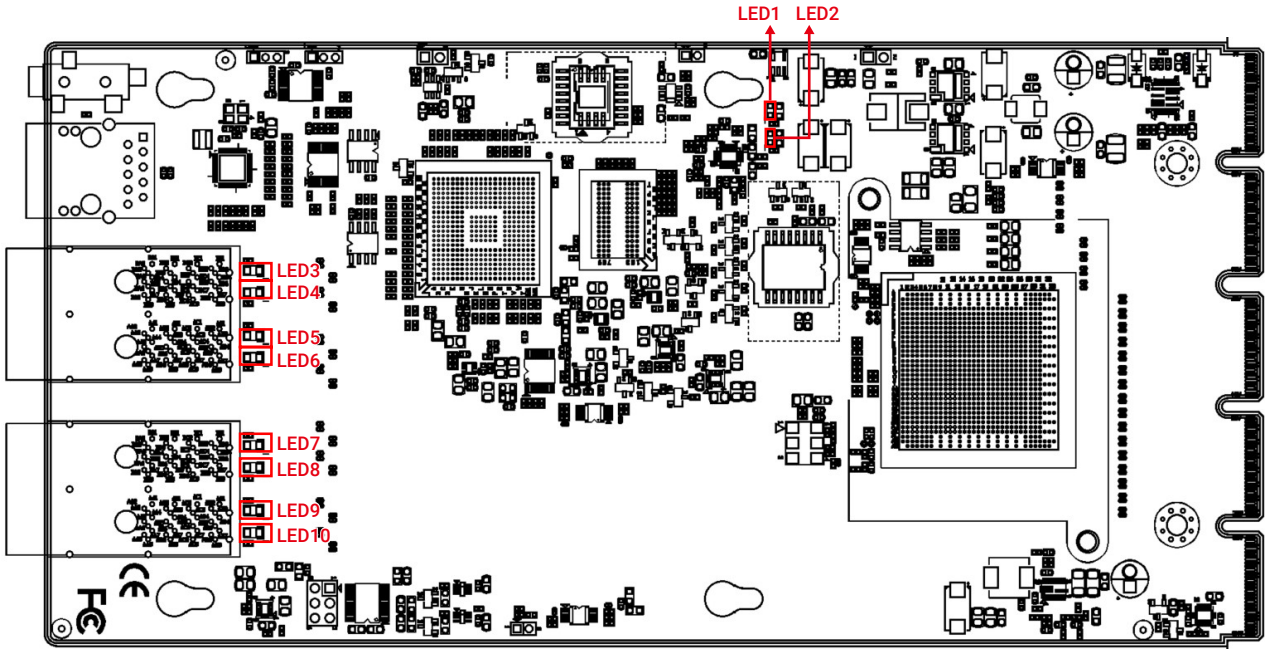
DBG_SIRXD	2	1	SM_SIRXD
GND	4	3	GND
DBG_SITXD	6	5	SM_SITXD

3.3.3 LED Indicator

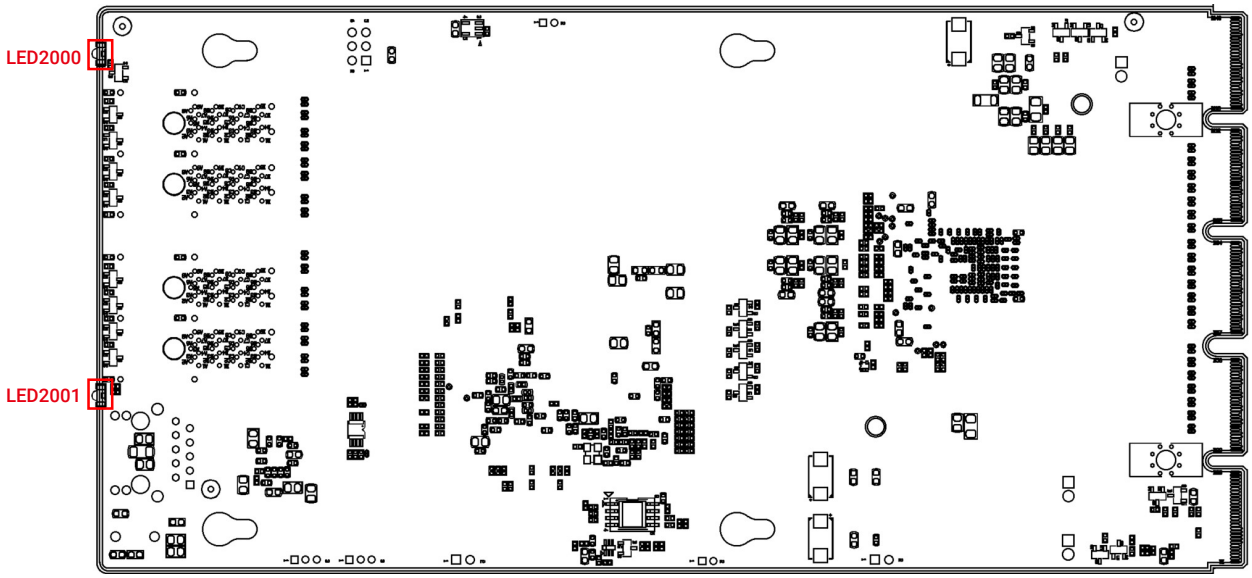
Indicator	Color	Description
UP/ DOWN Link Status LEDs (LED3,LED5,LED7,LED9)	Blue (On)	Link up
	Off	NO Link down
UP/ DOWN Link Status LEDs (LED4,LED6,LED8,LED10)	Red (On)	Phy Loss
	Off	Phy Normal
Expander Blink (LED2)	Blue (Blinking)	Expander alive, 0.833Hz (12 seconds per cycle)
Expander Heart Bit (LED1)	Blue (Blinking)	Expander FW running
BMC ID LED (LED2000)	Blue (On)	ID LED indicator
BMC Heart beat LED/Status LED (LED2001)	Blue (On)	• 10Hz : ARM Running on Flash. (instruction fetch from flash). • 2Hz : ARM Running on DRAM without interrupt enabled. (instruction fetch from DRAM) • 0.5Hz : ARM Running on DRAM with interrupt monitor enabled. The (normal operation mode). • 0.1Hz : Abnormal mode, some interrupts are not serviced for over 2 seconds. • 0Hz : Always dark indicates firmware is not running or dead.
	Red (On)	System Fail

Location

Top view

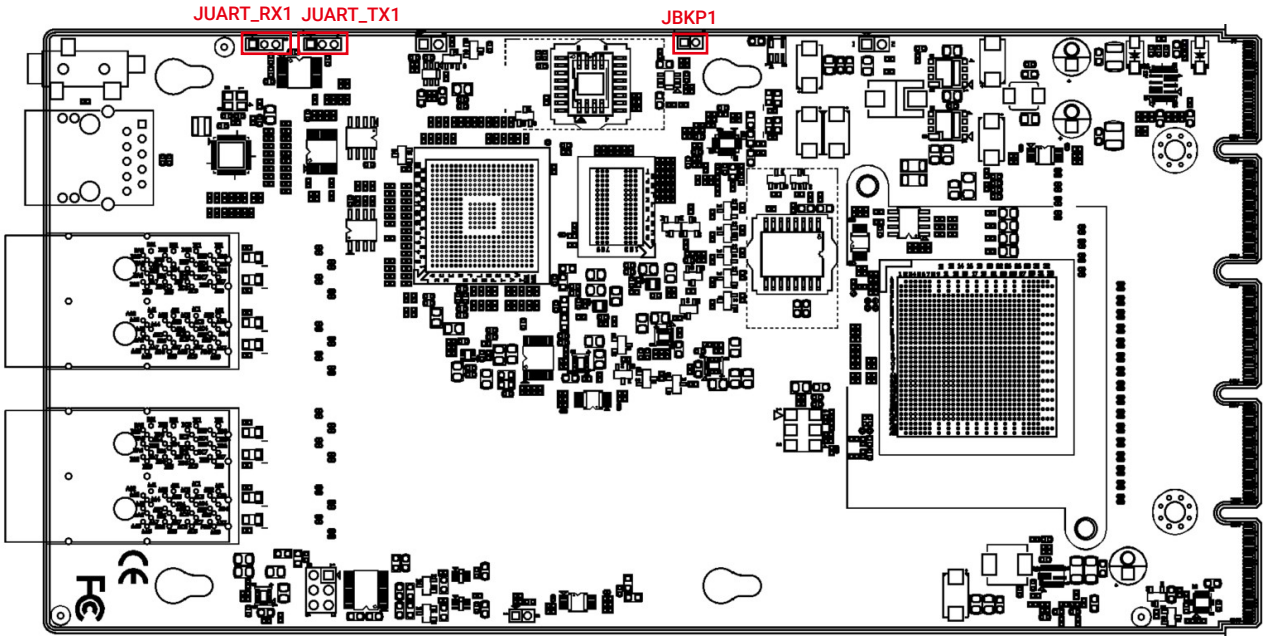


Bottom view



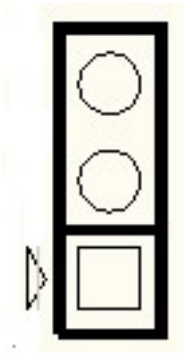
3.3.4 Jumper

Top view



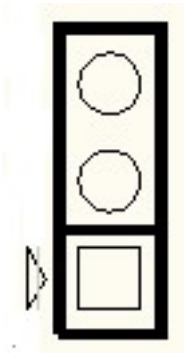
BMC UART Mode Option Description(JUART_TX1, JUART_RX1):

JUART_TX1



Pin 1,2 short	Smart Port Enable
Pin 2,3 short	Debug Port Enable

JUART_RX1



Pin 1,2 short	Smart Port Enable
Pin 2,3 short	Debug Port Enable

SPI CS0 select(JBKP1) Description:

SPI CS0 select (JBKP1)	FW_SPI_CS_N	**SPI CS0 Enable**	Pin 1,2 Short
	+3V3 level	SPI CS0 Disable	Pin 1,2 open
	GPIOK4	GPIOK4 High CS0 to Main ROM , CS1 to Backup ROM GPIOK4 Low CS1 to Main ROM , CS0 leave	

3.3.5 Backplane Phy Mapping

J2024-08-04X Phy Mapping:

SAS Phy Mapping (Primary Expander)

HDD1	HDD2	HDD3	HDD4	HDD5	HDD6	HDD7	HDD8	HDD9	HDD10	HDD11	HDD12
PHY39	PHY38	PHY37	PHY36	PHY35	PHY34	PHY33	PHY32	PHY31	PHY30	PHY29	PHY28
HDD13	HDD14	HDD15	HDD16	HDD17	HDD18	HDD19	HDD20	HDD21	HDD22	HDD23	HDD24
PHY27	PHY26	PHY25	PHY24	PHY23	PHY22	PHY21	PHY20	PHY19	PHY18	PHY17	PHY16

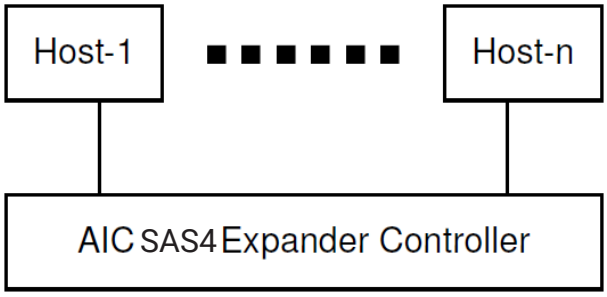
SAS Phy Mapping (Secondary Expander)

HDD1	HDD2	HDD3	HDD4	HDD5	HDD6	HDD7	HDD8	HDD9	HDD10	HDD11	HDD12
PHY39	PHY38	PHY37	PHY36	PHY35	PHY34	PHY33	PHY32	PHY31	PHY30	PHY29	PHY28
HDD13	HDD14	HDD15	HDD16	HDD17	HDD18	HDD19	HDD20	HDD21	HDD22	HDD23	HDD24
PHY27	PHY26	PHY25	PHY24	PHY23	PHY22	PHY21	PHY20	PHY19	PHY18	PHY17	PHY16

Chapter 4 Sub-system Configuration Setup

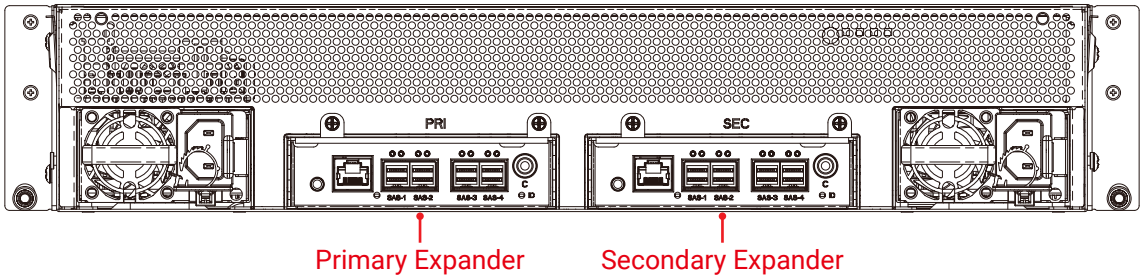
4.1 Supported Configuration and Unsupported Feature

4.1.1 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:
(A) SAS drive / Nearline SAS drive
(B) SATA drive with an interposer which provides SATA-to-SAS conversion

Rear Panel



4.2 SES Inband Features

4.2.1 SES Pages

00h - List of supported diagnostic pages
01h - SES configuration
02h - SES enclosure control / enclosure status
05h – SES Threshold Out / In
07h - SES element descriptor
0Ah - SES additional element
0Eh - SES download microcode control / SES download microcode status
82h – SES vendor specific page: Chassis Number
83h – SES vendor specific page: Canister Number
8Bh – SES vendor specific page: Drive Bay Blue LED
8Dh – SES vendor specific page: BMC Firmware Version

4.2.2 SES Elements

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

4.2.3 Implementation on SES Pages

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: Chassis Number (page code 82h) Out / In
The length N of chassis number can be 0 ~ 247 bytes. If no chassis number is input (N=0), then chassis number is cleared.

Chassis Number control format

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

If no chassis number is found, report Status = 1 (failed). Otherwise report Status = 0 (success) followed by chassis number.

Chassis Number status format

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

SES vendor specific page: Canister Number (page code 83h) Out / In
The length N of canister number can be 0 ~ 247 bytes. If no canister number is input (N=0), then canister number is restored to its SAS address.

Canister Number control format

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

If no canister number is found, report Status = 1 (failed). Otherwise report Status = 0 (success) followed by canister number.

Canister Number status format

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

SES vendor specific page: Drive Bay Blue LED (page code 8Bh) Out / In
The drive bay blue LED can be enabled/disabled through the control format:

Drive Bay Blue LED control format

BYTE/BIT	7	6	5	4	3	2	1	0
0	Drive Bay ID in hexadecimal							
1	0x00 to disable the blue LED, and 0x1 to enable the blue LED							

The reported length of the drive bay blue LED status format depends on the number of the drive bays. The report represents the statuses of all drive bays. The status of the drive bay is either 0x00 or 0x01. The status “0x00” means that the drive bay blue LED is disabled, and the status “0x01” means the drive bay blue LED is enabled.

SES vendor specific page: BMC Firmware Version (page code 8Dh) In
There are 3 bytes for BMC firmware version.

BMC Firmware Version status format

BYTE/BIT	7	6	5	4	3	2	1	0
0~2	BMC Firmware Version							

4.2.4 Implementation on SES Elements

Only the fields highlighted in blue 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	DO NOT REMOVE	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	DISABLED	SWAP	ELEMENT STATUS CODE			
1	IDENT	DO NOT REMOVE	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 UNKNOWN: The power supply can’t be read
DC OVER CURRENT	An output overcurrent fault has occurred
FAIL	A failure condition is detected
RQSTED ON	1: On 0: Off for Disk Power Supply
OFF	1: Off for Disk Power Supply 0: On
OVERTMP FAIL	Over temperature fault has occurred
TEMP WARN	Over temperature warning has occurred
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	DO NOT REMOVE	Reserved					
2	Reserved							
3	Reserved	RQST FAIL	RQST ON	Reserved		REQUESTED SPEED CODE		

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

(B) Cooling Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLED	SWAP	ELEMENT STATUS CODE			
1	IDENT	DO NOT REMOVE	Reserved			ACTUAL FAN SPEED (MSB)		
2	ACTUAL FAN SPEED (LSB)							
3	HOT SWAP	FAIL	RQSTED ON	OFF	Reserved	ACTUAL SPEED CODE		

Field	Value
ELEMENT STATUS CODE	OK: Everything is Ok. NON-CRITICAL: Either warning limit is exceeded. CRITICAL: The fan RPM can’t be detected, or either failure limit is exceeded.
IDENT	Applicable only for Cooling element 0 0: Enable the auto fan function 1: Disable the auto fan function
ACTUAL FAN SPEED	Current fan RPM
FAIL	The fan RPM can’t be detected, or either failure limit is exceeded.
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	OFFSET FOR REFERENCE TEMPERATURE					
2	REQUESTED TEMPERATURE							
3	RQST OVERRIDE	Reserved						

(B) Temperature Sensor Status Element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON STATUS							
	Reserved	PRDFAIL	DISABLED	SWAP	ELEMENT STATUS CODE			
1	IDENT	FAIL	OFFSET FOR REFERENCE TEMPERATURE					
2	TEMPERATURE							
3	RQSTED OVERRIDE	Reserved			OT FAILURE	OT WARNING	UT FAILURE	UT WARNING

Field	Value
ELEMENT STATUS CODE	OK: Everything is Ok NON-CRITICAL: Either warning limit is exceeded CRITICAL: Either failure limit is exceeded
FAIL	A warning or failure condition is detected
TEMPERATURE	Temperature reading
OT FAILURE	Temperature exceeds the failure high threshold value
OT WARNING	Temperature exceeds 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
RQST IDENT	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	DISABLED	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
IDENT	Set by the RQST IDENT on Enclosure Control Element
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	DISABLED	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: Either warning limit is exceeded CRITICAL: Either failure limit is exceeded
FAIL	A warning or failure condition is detected
WARN OVER	Voltage exceeds the warning high threshold value
WARN UNDER	Voltage is below the warning low threshold value
CRIT OVER	Voltage exceeds 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	Reserved			
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	RQST MISSING	RQST INSERT	RQST REMOVE	RQST IDENT	Reserved
3	Reserved		RQST FAULT	DEVICE OFF	ENABLE BYP A	ENABLE BYP B	Reserved	

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.
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.
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	DISABLED	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 drive bay NOT INSTALLED: No drive is installed in the drive bay
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

4.2.5 SES Element Control Functions

LED indicators (blue and red) associated with an attached disk drive

(A) Array Device Slot control element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
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	RQST MISSING	RQST INSERT	RQST REMOVE	RQST IDENT	Reserved
3	Reserved		RQST FAULT	DEVICE OFF	ENABLE BYP A	ENABLE BYP B	Reserved	

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 8Hz frequency”.
The behavior “Slow Blink” is “LED is blinking at 1Hz 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	Slow Blink
RQST FAULT	ON	ON
DEVICE OFF	OFF	OFF
PRDFAIL	Activity	Slow Blink

How to turn on/off the power of a drive bay

Array Device Slot control element

BYTE/BIT	7	6	5	4	3	2	1	0
0	COMMON CONTROL							
	SELECT	PRDFAIL	DISABLE	RST SWAP	Reserved			
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	RQST MISSING	RQST INSERT	RQST REMOVE	RQST IDENT	Reserved
3	Reserved		RQST FAULT	DEVICE OFF	ENABLE BYP A	ENABLE BYP B	Reserved	

The "DEVICE OFF" for a drive bay is defined in the bit4, byte3 of the "Array Device Slot control element" in the SES specification. Set the bit to turn off a drive bay 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 24G Hotswap Expander 1801

(B) Get the current power state of a drive bay. The "Device off=0" means the drive bay 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 drive bay
$ sg_ses --page=7 /dev/sg2
Element 0 descriptor: Disk001

(D) Turn off a drive bay power
$ sg_ses --descriptor=Disk001 --set=3:4:1 /dev/sg2

(E) Turn on a drive bay power
$ sg_ses --descriptor=Disk001 --clear=3:4:1 /dev/sg2

How to power off/on all drive bays manually

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	DO NOT REMOVE	Reserved					
2	Reserved							
3	Reserved	RQST FAULT	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 “DiskPowerSupply” to power off all drive bays. Set the bit on Power Supply Element “DiskPowerSupply” to power on all drive bays. 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 Hotswap Expander 1801
(B) Power off all drive bays
    $ sg_ses --descriptor=DiskPowerSupply --clear=3:5:1 /dev/sg2
(C) Power on all drive bays
    $ sg_ses --descriptor=DiskPowerSupply --set=3:5:1 /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 Hotswap Expander 1801
(B) Enable the enclosure alarm
    $ sg_ses --descriptor=EnclosureElement --set=3:1:1 /dev/sg2
    or
    $ sg_ses --descriptor=EnclosureElement --set=3:0:1 /dev/sg2
(C) Disable the enclosure alarm
    $ sg_ses --descriptor=EnclosureElement --clear=3:1:2 /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 FAULT	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 auto 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 auto fan function again. Please disable the auto fan function before changing PWM or fan speed. Only Cooling element 0 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 Hotswap Expander 1801
(B) Set "RQST IDENT" of Cooling element 0 to disable the auto fan function
    $ sg_ses --descriptor=CoolingElement00 --set=1:7:1 /dev/sg2
(C) Set "REQUESTED SPEED CODE" of Cooling element 0 to change PWM or fan speed for all Cooling elements. Set "REQUESTED SPEED CODE"=7 (100% PWM) for example.
    $ sg_ses --descriptor=CoolingElement00 --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 enable/disable the enclosure identification

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 blue and red LEDs of all the drives are used for the enclosure identification with slow blink. The "RQST IDENT" for Enclosure is defined in the bit7, byte1 of the "Enclosure control element" in the SES specification. Setting the bit can enable the enclosure identification. Clearing the bit disables the enclosure identification. 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 Hotswap Expander 1801
(B) Enable the enclosure identification
    $ sg_ses --descriptor=EnclosureElement --set=1:7:1 /dev/sg2
(C) Disable the enclosure identification
    $ sg_ses --descriptor=EnclosureElement --clear=1:7:1 /dev/sg2

4.3 Serial Command Line Interface Functions

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

4.3.1 How to enable/disable T10 zoning

The default T10 zoning configuration is off.

(A) Check the current zoning state
    cmd> phyzone state
    Zoning is OFF
(B) Enable zoning
    cmd> phyzone on
(C) Disable zoning
    cmd> phyzone off

4.3.2 How to configure T10 zoning

Remove the SAS cable between the HBA/RAID card and the JBOD-2U24 before configuration T10 zoning. After configuring T10 zoning, please power cycle the JBOD-2U24 and then insert the SAS cable back.

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 bay accessed only by the first wide port and another drive bay accessed only by the second wide port.The PHYs for the wide ports and drives in the example are not the PHY map in the Hotswap4.

The configuration for the example is

(A) PHY0 ~ PHY3 for the first wide port

(B) PHY4 ~ PHY7 for the second wide port

(C) PHY12 ~ PHY35 for drive bays

Step 1: Read the current group for PHY4
cmd> phyzone 4
Phy 4 for Zone Group 1

Step 2: Assign the second wide 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 wide port (PHY0 ~ PHY3) for Group8
cmd> phyzone 0 8
cmd> phyzone 1 8
cmd> phyzone 2 8
cmd> phyzone 3 8

Step 4: Assign the drive bay on PHY12 to be accessed only by the first wide port instead of the second wide port
cmd> phyzone 12 8

Step 5: Assign the drive bay on PHY13 to be accessed only by the second wide port instead of the first wide port
cmd> phyzone 13 9

Step 6: Reset for taking effect with the new settings
cmd> reset

4.3.3 How to get all revisions in AIC SAS4 Expander

(A) Expander firmware revision
cmd> rev
(B) Expander configuration revision
cmd> showmfg
(C) Model and sensor information
cmd> sensor

4.3.4 How to configure temperature sensor

There are 5 temperature sensors. Four temperature settings in Celsius per sensor are T1, T2, warning threshold, and alarm (critical) threshold. The T1 and T2 are applied to the auto fan function.

(A) Get the current settings of Temperature Sensor 1
cmd> temperature 1
Temperature in Celsius (t1=20 C, t2=60 C, warning=57 C, alarm=60 C)
(B) Set with new T1=18 C, T2=52 C, warning threshold=48 C, and alarm threshold=54 C.
The new setting will take effect after reset.
cmd> temperature 1 18 52 48 54
cmd> reset

4.3.5 How to configure enclosure address

(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

4.3.6 How to configure standby timer for all disk drives

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

4.3.7 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.

(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

4.3.8 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.

cmd> check_wide_port standby
cmd> reset

The function will not work properly when the drive bay power is turned off with SES command of clearing “RQST_ON” of the Power Supply Element “DiskPowerSupply”.

The drive bay power will be turned on/off when SAS cable is connected/disconnected, even if the drive bay power is turned off/on by BMC or SES command of array device before SAS cable connected/disconnected.

4.3.9 How to configure EDFB

The default EDFB configuration is on.

(A) Check the current configuration
cmd> edfb
EDFB is OFF

(B) Enable EDFB
cmd> edfb on

(C) Disable EDFB
cmd> edfb off

4.4 Vendor Specific Vital Product Data (VPD) Page

The Vendor Specific VPD pages provide MFR_ID, MFR_MODEL, MFR_REVISION, MFR_SERIAL, and MFR_FW_ REVISION of the power module 0 (page code 0xC1) and power module 1 (page code 0xC2).

Vendor Specific VPD Page Format

BYTE/BIT	7	6	5	4	3	2	1	0
1	MFR_ID							
m								
m+1	0x20 (ASCII code space)							
m+2	MFR_MODEL							
n								
n+1	0x20 (ASCII code space)							
n+2	MFR_REVISION							
o								
o+1	0x20 (ASCII code space)							
o+2	MFR_SERIAL							
p								
p+1	0x20 (ASCII code space)							
p+2	MFR_FW_REVISION							
q								
q+1	0x20 (ASCII code space)							

Chapter 5. BMC Configuration Settings

5.1 Introduction

5.1 Intoduction to the BMC Platform

The BMC (Baseboard Management Controller) permits remote networking access to multiple users situated in different locations. In addition to this, it facilitates remote system health monitoring and computer event management for system administrators.

5.2 Overview of the ASPEED AST2520 BMC

The ASPEED AST2520 is a powerful stand alone BMC chip with internal 800MHz ARM11 CPU and the mainstream double data rate memory migrating from DDR3 to DDR4.
The BMC facilitates remote monitoring and management of systems.

5.3 AIC BMC Features

The BMC functions supported by AIC are as follows.

- Hardware monitoring
- Overall health status display on the main page
- Remote system power control
- Remote serial over LAN (text console)
- Event Log support
- Automatic notifications and alerts (SNMP and email)
- Out-of-band management via shared or dedicated LAN
- Change LAN interface options at runtime
- VLAN
- Factory default settings from web support
- OS independent
- System Lockdown
- Backup and restore the configuration file
- Update firmware via browser and OS
- Redfish

5.4 Applicable or Supported Platforms

This BMC firmware applies to J2024-08-04X series platforms.

5.2 Log In to the Remote Console

5.2.1 Required Browser Settings

Use a computer and configure its web browsers.

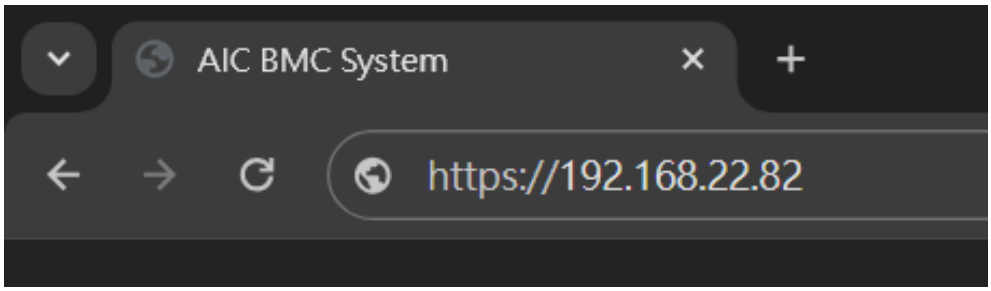
- Accept the file download when prompted in all browsers
- Javascript and cookie settings should be enabled in order to access the web site

> **NOTE**
> Cookies must be enabled in order to access the website.

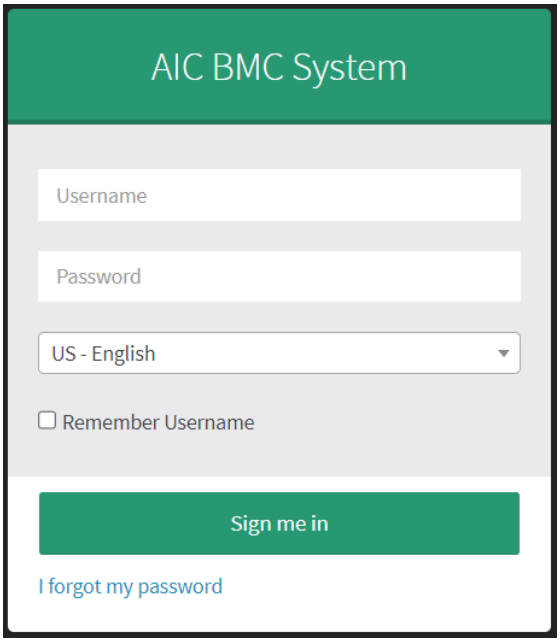
5.2.2 Username and Password

The computer and BMC need to be on the same subnet. After setting the static IP, they should be able to communicate. To establish a connection, follow the steps below.

1. Use the computer's terminal to ping the BMC IP address and ensure that it can be pinged.
2. If the BMC IP address is pingable, open a web browser on your computer, enter the BMC IP address in the URL bar.



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



The fields are explained as follows:

Fields Name	Description
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. For example, if browser language is configured with Simplified Chinese language (ZH-CN), then option value will be auto selected as China. 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.
Sign me in	After entering the required credentials, click the **Sign me in** to login.
I forgot my password	If you forget your password, you can generate a new password using this link.

5.2.3 Default User Name and Password

Default Username: **admin**

Default Password: **admin**

NOTE

The default user name and password are in lower-case characters. When you log in using the user name and password, you get full administrative rights. It is advised to change your password once you login.

Duplicate user names shouldn't exist across various authentication methods like AD, LDAP, RADIUS or IPMI since the privilege of one Authentication method is overwritten by another authentication method when login and hence the correct privilege can not be returned properly. Duplicate user names shouldn't be existed across different channels in IPMI.

Warning:

Once you login to the application, it is recommended not to use the following options.

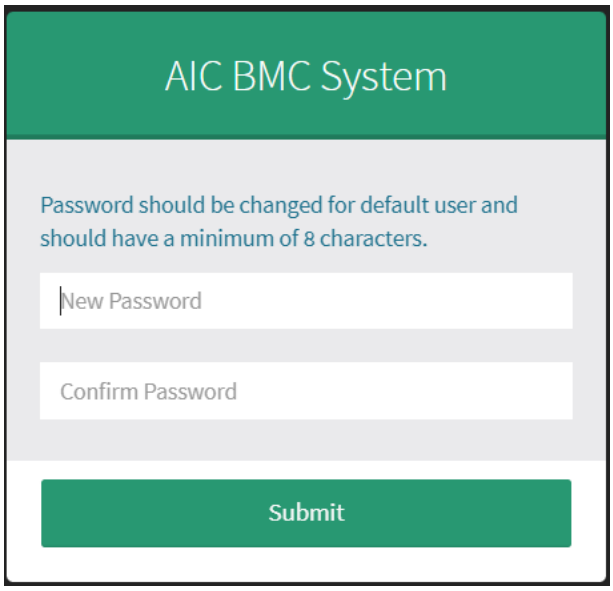
- Refresh button of the browser
- Refresh menu of the browser
- Back and Forward options of the browser
- F5 on the keyboard
- Backspace on the keyboard

The changes done in user account properties through IPMI/Redfish interfaces will not be reflected in current active web sessions.

5.2.4 Need to change password

It is mandatory to change the password for the default user at first successful login due to California Law SB-327 security fix. If the authentication is successful, then Web UI will prompt a new page which will ask to change the user password. Once the password is changed, login page will be reloaded. Enter the username and modified password to Login.

A sample screenshot is given below.



Default User's password can be changed using any of the following method.

- Web UI
- IPMI Tool
- Redfish (If Redfish Support is enabled)

> **NOTE**
> The last password used cannot be used to reset the password.

Password Change Required Case

1. When the BMC boots with factory firmware, user needs to change the default password on first boot.
2. When the user upgrades the BMC firmware without preserving the configuration, default pass word needs to be changed on the first boot.
3. When the user restores factory settings and restarts the BMC, the default password needs to be changed during the restart.
4. Whenever the user detects BMC configuration corruption and restores the configuration to factory settings, the default password needs to be changed on the next boot.

Limitations

If the current Firmware in BMC is without CA law enabled and the default password is modified and user tries to preserve configuration and upgrade firmware with CA law enabled firmware image, BMC will still prompt to change the user password.

Reason

In BMC firmware default password is not preserved or stored anywhere, so it is not possible to check if the default password is modified or not. Default password can also be modified during Build time in PMCP file as required by OEM.

NOTE

Since Password Change at first login is made as PRJ configurable and if this feature is disabled then it is not mandatory to change the default password at first login.

5.3 Menu Bar and Quick Button

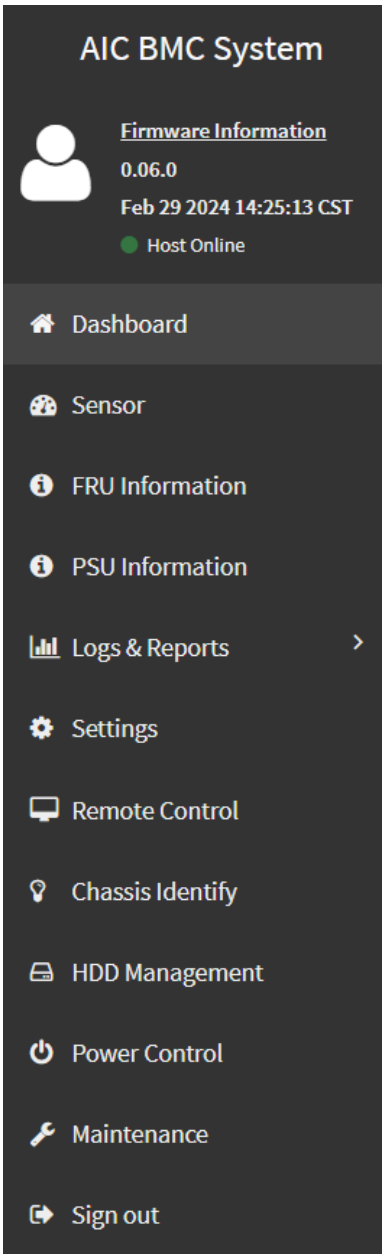
5.3.1 Menu Bar

The menu bar displays the following.

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.

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



5.3.2 Quick Button and Logged-in User

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

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.

Logged-in user and its privilege level

This option shows the logged-in user name and privilege. There are five kinds of privileges.

1. **User**: Only valid commands are allowed.
2. **Operator**: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.
3. **Administrator**: All BMC commands are allowed.
4. **No Access**: Login access denied.
5. **OEM**: All OEM commands are allowed.

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

Notification: Click to view the notification received.

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.

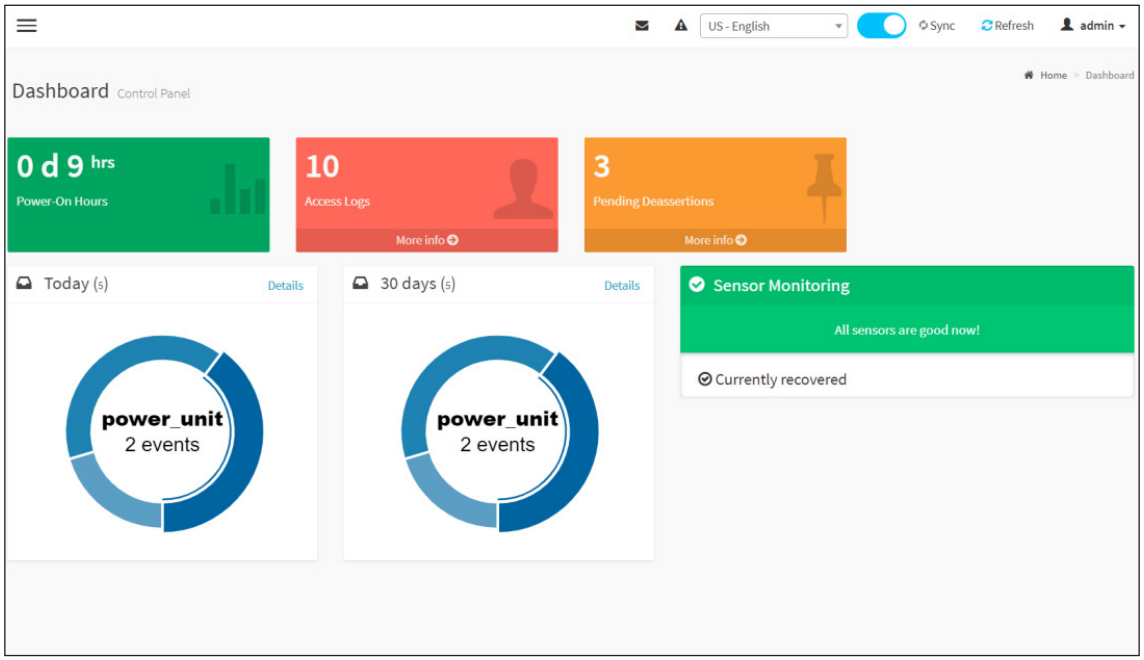
Quick Search: Quick Search is a short-cut for the available menu and sub-menu pages. It displays available search queries. Click US - English (Quick Search) field, and type search terms of the lists in the menu bar. As you type, the suggestions will be displayed in a drop-down list below the Quick Search field as a navigational links of the menu and sub- menu. On selecting your search term from the drop-down list, it will directly go to the specific page which you have searched.

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

5.4 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.



A brief description of the Dashboard page is given below.

BMC Power-On Hours

BMC Power-On Hours will keep on accumulated.

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

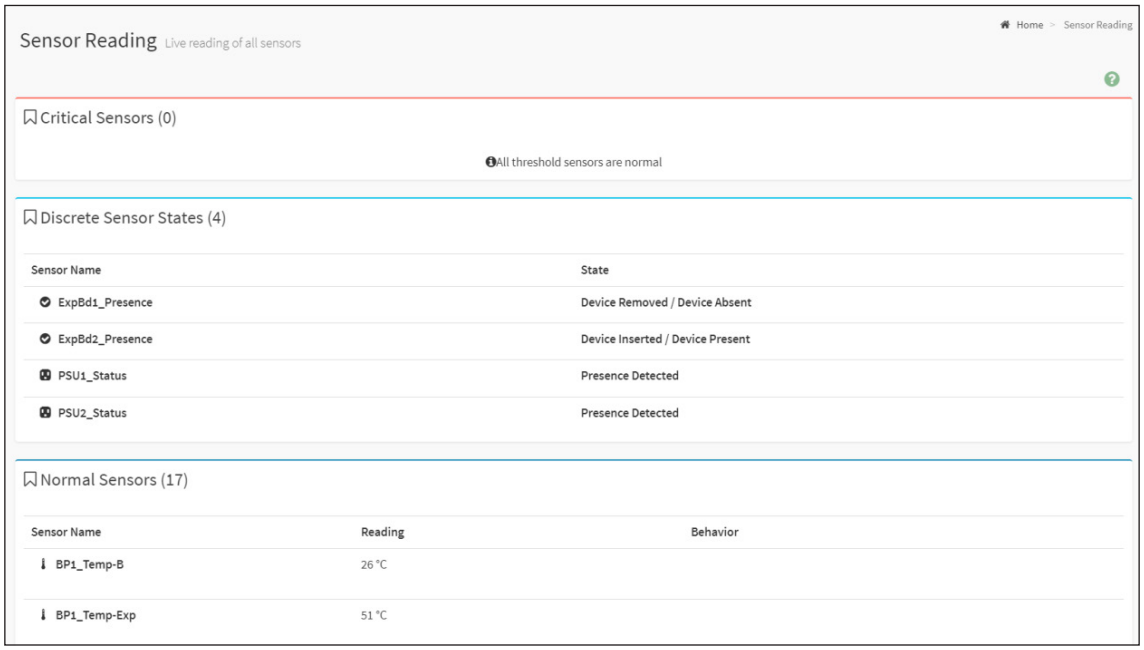
It lists all the critical sensors on the device. If you click on any list sensor, you can view the Sensor detail page with the Sensor information and Sensor Events details.

5.5 Sensor

The Sensor Reading page displays all the sensor related information.

To open the Sensor Reading 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 Reading page is given below.



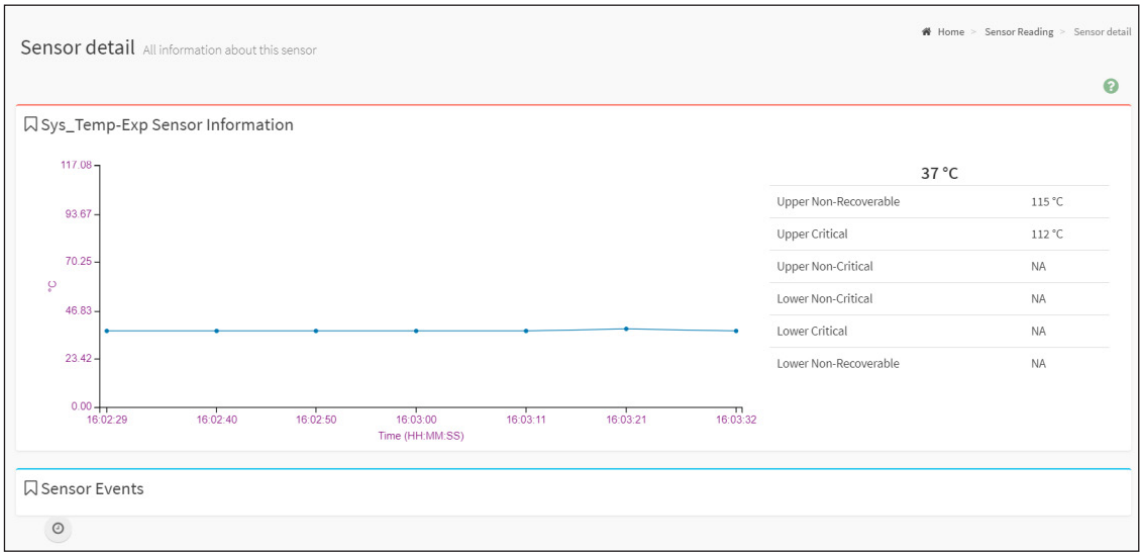
Sensor Readings Page

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.

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.



Sensor detail

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)

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.

The threshold states could be

- Lower Non-critical - going low
- Lower Non-critical - going high
- Lower Critical - going low
- Lower Critical - going high
- Lower Non-recoverable - going low
- Lower Non-recoverable - going high
- Upper Non-critical - going low
- Upper Non-critical- going high
- Upper Critical - going low
- Upper Critical - going high
- Upper Non-recoverable - going low
- Upper Non-recoverable - going high

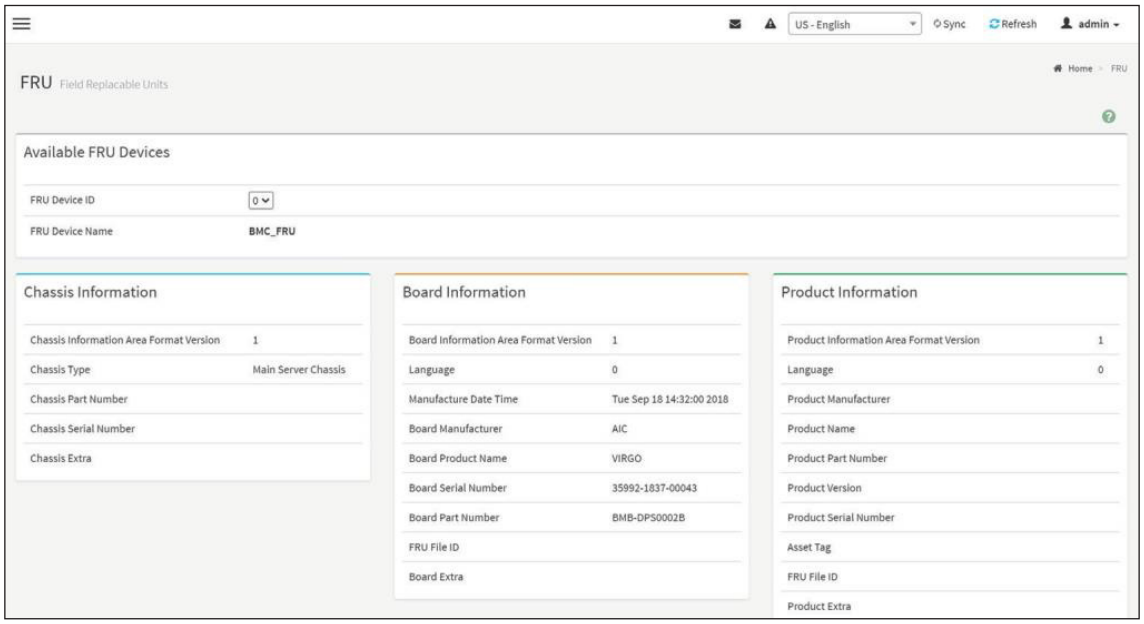
View this Event Log

You can click here to view the Logs & Reports for the selected sensor.

5.6 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

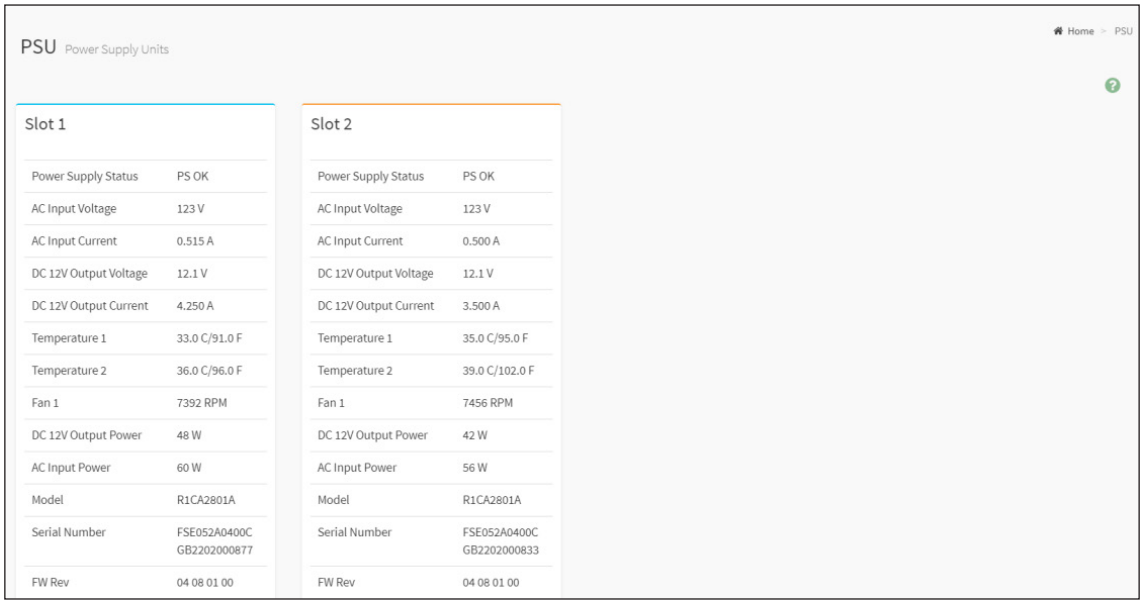
Product Information

- 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

5.7 PSU Information

PSU Information page displays the BMC's Power Supply Unit information. This page shows information like Status, Sensor Reading and Model Details of the PSU.

To open the PSU Information page, click PSU Information from the menu bar. A screenshot of PSU Information page is given below.



PSU Information Page

NOTE

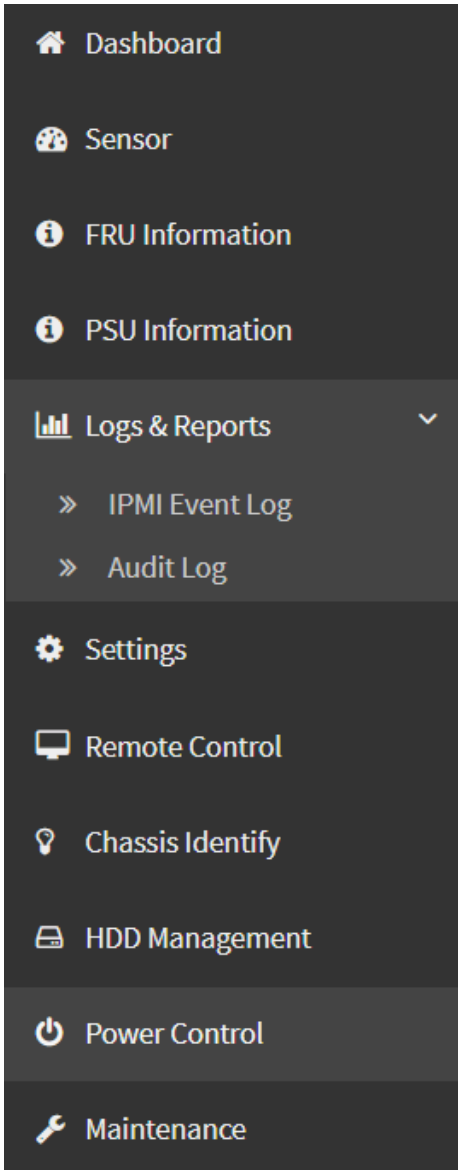
If the device is not detected successfully, please turn on the power or reinstall the device.

5.8 Logs & Reports

To open the Logs & Reports page, click Logs & Reports from the menu bar. The Logs & Reports page displays the following information.

- IPMI Event Log
- System Log

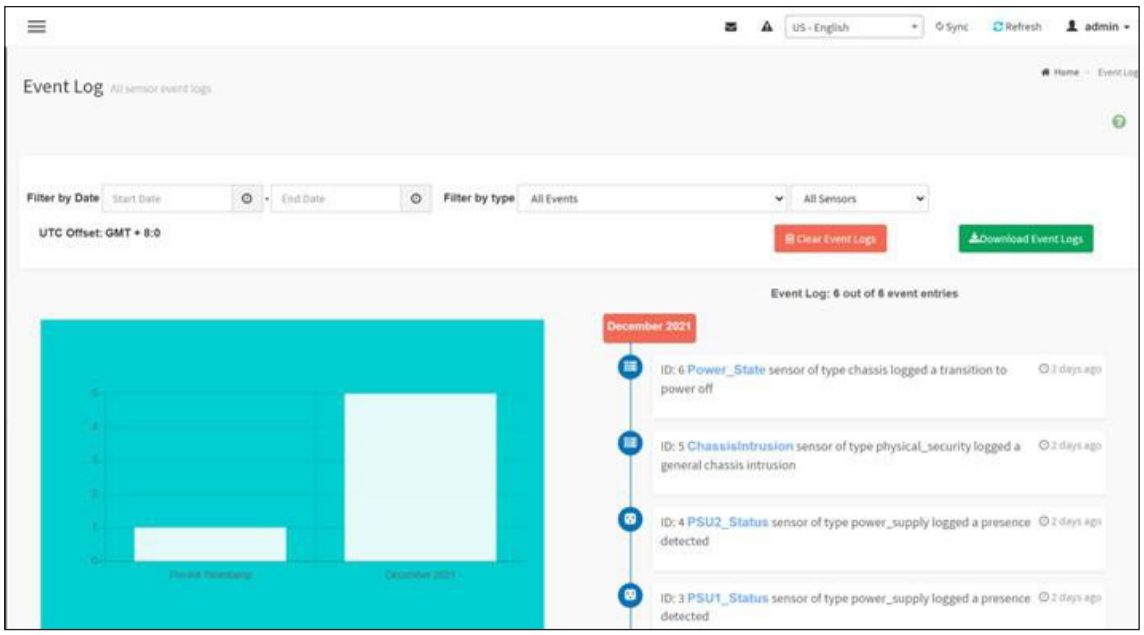
A screenshot displaying the menu items under Logs & Reports is shown below



5.8.1 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.

> **NOTE**
> Date should be in MM/DD/YYYY format. By default, all log time will be displayed in BMC time zone.

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.

> **NOTE**
> Once the Filter By Date and Filter type are selected, the list of events will be displayed with the Event ID, Time Stamp, Sensor Type, Sensor Name and Description.

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.

Procedure

1. From the Filter By Date field, select the time period by Start Date and End Date using Calendar for the event categories. The events will be displayed according to the selected date.
2. From the Filter By Type field, select the Type of the event and Sensor name to view the events for the date. The events will be displayed based on the selected time period.
3. To clear all events from the list, click Clear All Event Logs.
4. To download the event logs, click Download Event Logs.

NOTE

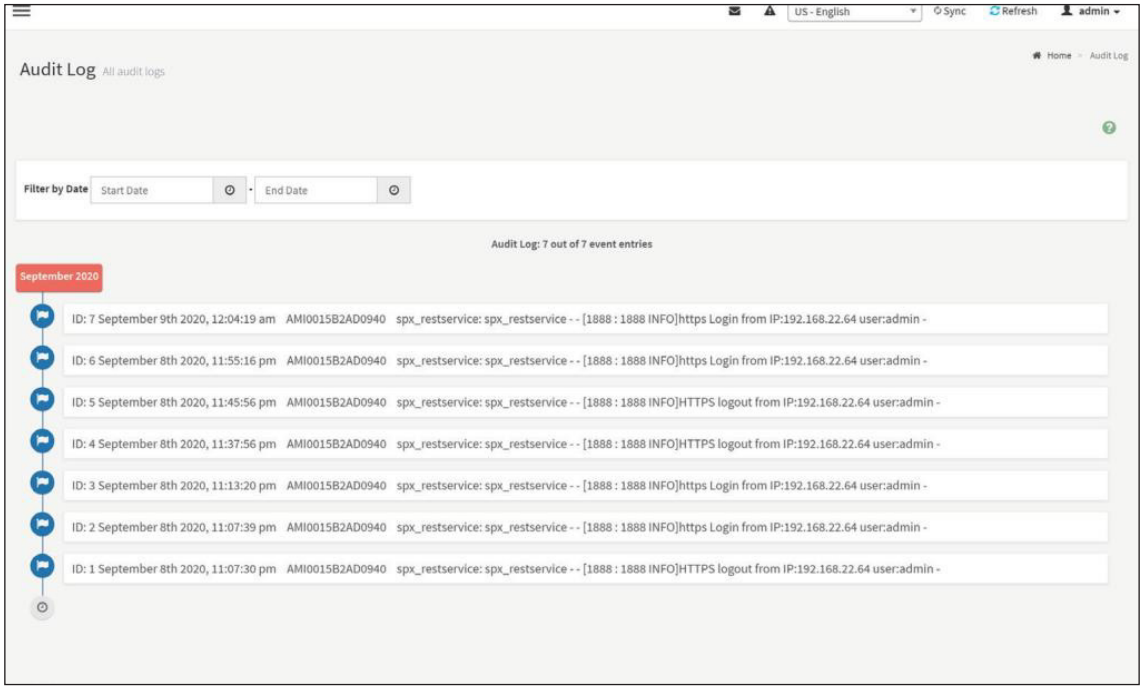
When Clear All Event Logs action is performed, there might be some events present even after clearing those events are generated after performing clear operation which can be verified using its time stamp.

5.8.2 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.

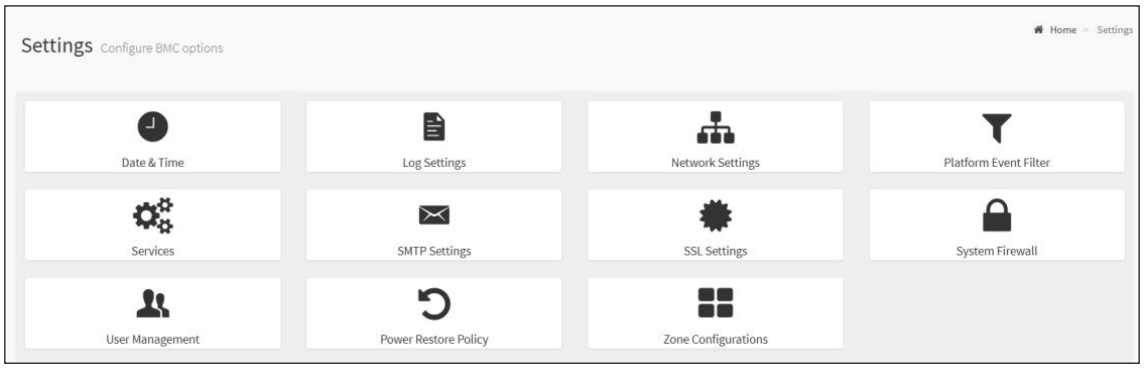


Procedure

To view Audit Log, click the Audit Log tab to view all audit events for this device.

5.9 Settings

To open the Settings page, click Settings from the menu bar. This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



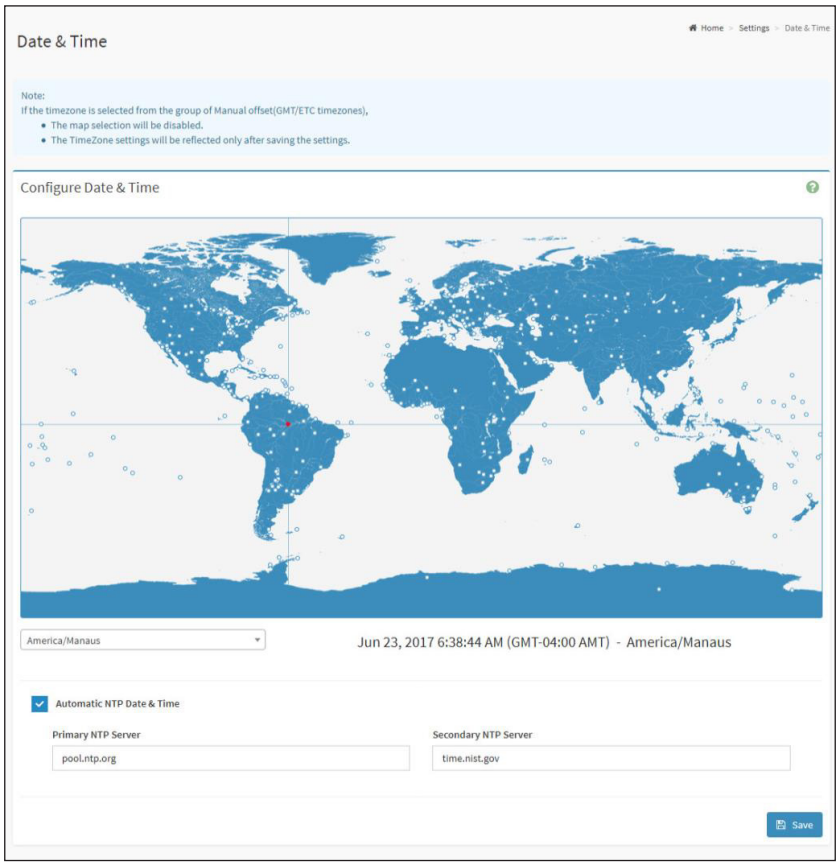
Configuration Group Menu

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

A detailed description of the Configuration menu is given below.

5.9.1 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.

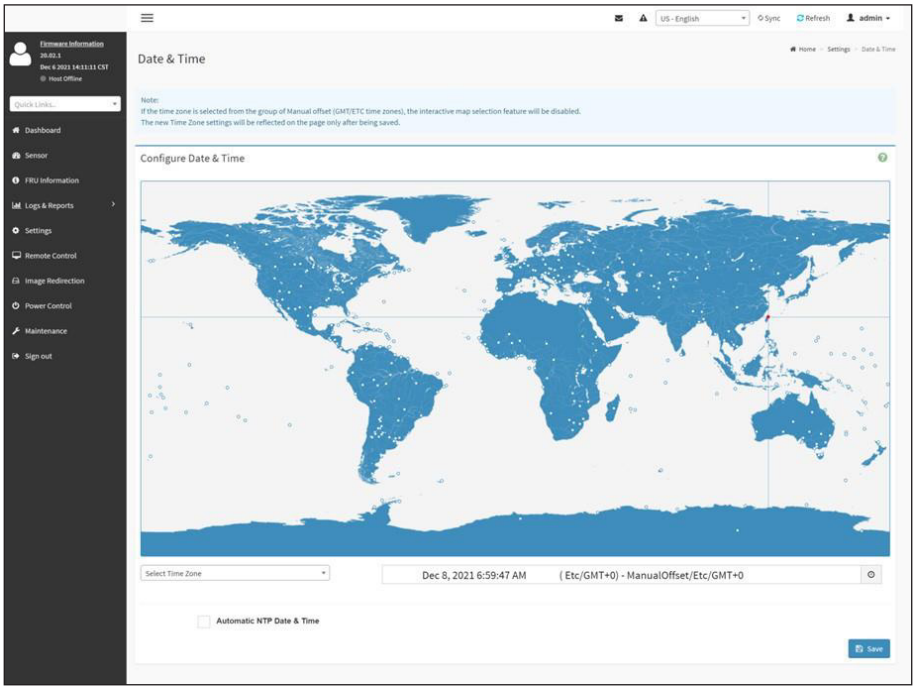
Disable Automatic Date & Time Option

User can modify the Date and Time manually by disabling the Automatic Date and Time option.

This will provide option to choose time, time zone and date manually.

This Web GUI provides two options to modify the Date and Time.

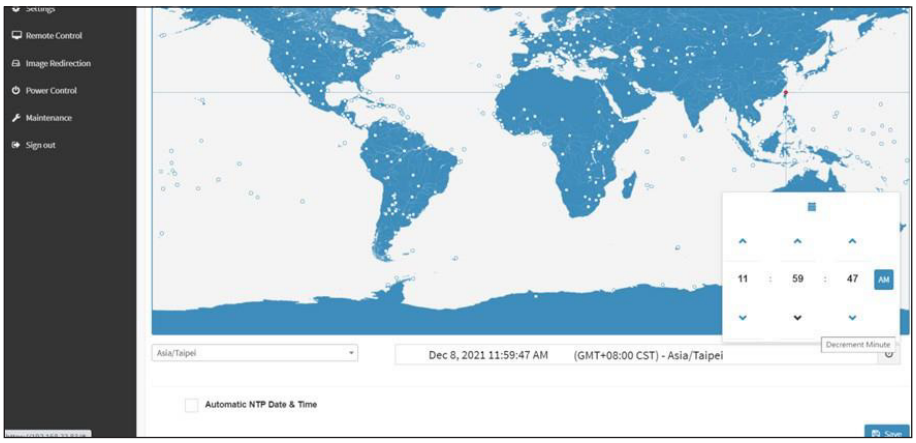
1. We can choose Interactive map section to update the time and time zone. If we choose the time zone from interactive map section, the time will update accordingly with the time zone.



Date&Time - Automatic Date & Time Disabled

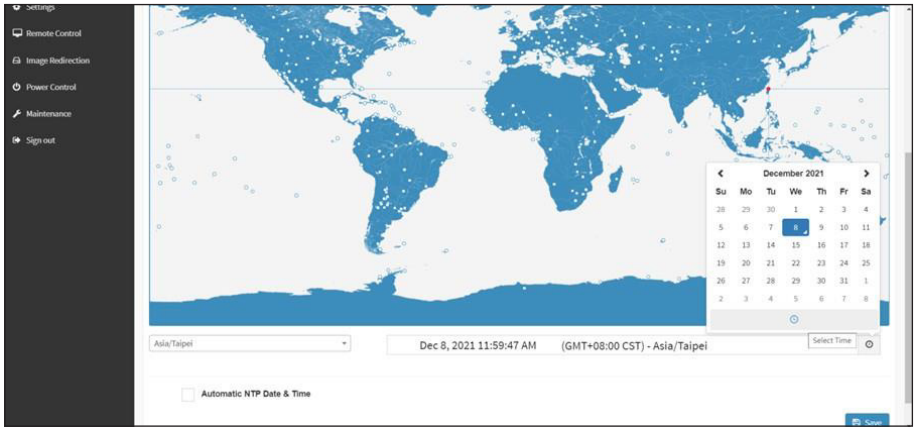
If we change the time zone, the time will be modified by their time zone reference. Still if the user want to modify the date and time, the user can click the clock icon on Web UI to modify the date and time.

2. We can choose the time zone from the group of Manual Offset. If the time zone is selected from the group of Manual offset (GMT/ETC time zones), then interactive map selection feature will be disabled. The user has to manually modify the Date and Time from the user web GUI. To manually modify Date and Time, click on clock icon.



Configure Date & Time Manually

The User can modify the Date and Time using this option. If we click on the calendar icon option to change, Date will be visible to the user.



Option to Change Date

Procedure

1. Select the Timezone location either using drop down or Map.
2. Enable Automatic Date & Time option to enable/disable the use of NTP servers to automatically set the date and time.
   a. In the Primary NTP Server and Secondary NTP Server fields, specify the NTP servers of the device respectively.

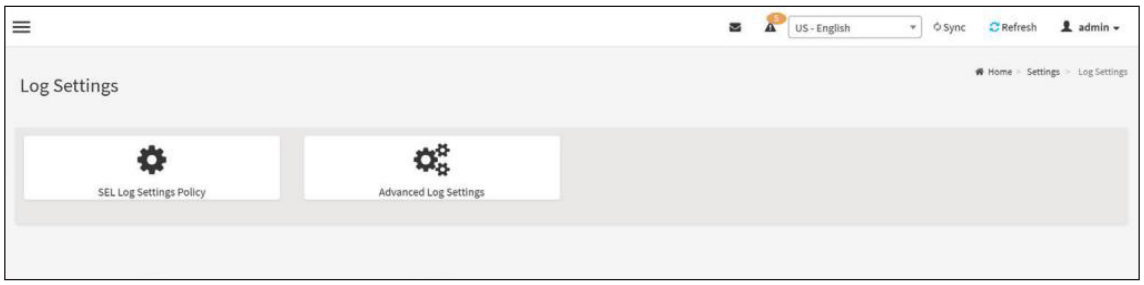
> **NOTE**
> Secondary NTP server is optional field.
> If the Primary NTP server is not working fine, then the Secondary NTP Server will be tried.

3. Click Save button to save the settings.

5.9.2 Log Settings

Logs and Reports page displays a list of IPMI Event 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.



The fields of Log Settings page are explained below.

- SEL Log Settings Policy
- Advanced Log Settings

5.9.2.1 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.

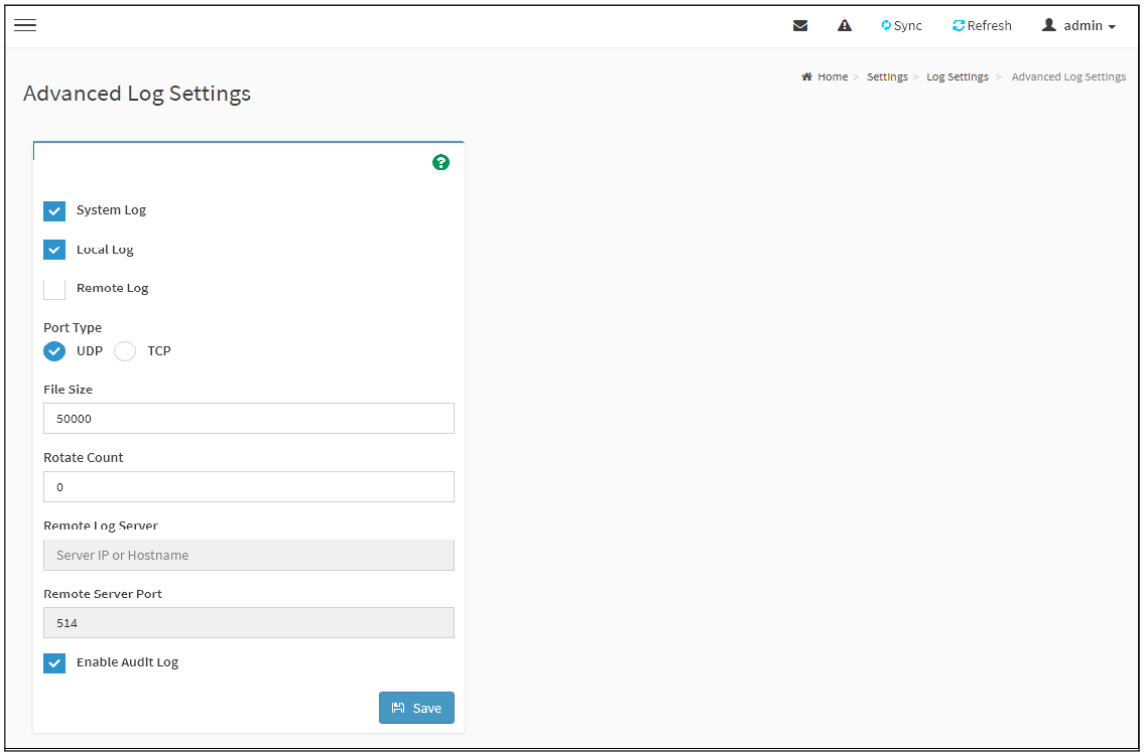
This page is used to configure the log policy for the event log. The fields are as followed

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

Save: To save the configured settings

5.9.2.2 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.



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).

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

> **NOTE**
> Values supported are 0 and 1.

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.
> - Local file resides at /var/log/

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.

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).

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

Procedure

1. In the System Log field, enable or disable the option.
2. Select the Log type: Local Log or Remote Log.
3. If Local log is selected, enter the file size in the File Size field and rotate count in the Rotate Count field.

> **NOTE**
> If Remote log is selected, the fields file size and rotate count need not be mentioned.

4. If remote log is selected, specify the Server Address of the remote server where the system events are logged.
5. In the Audit Log field, check or uncheck the Enable option as desired.
6. Click Save to save the changes.

Steps to configure the remote server to enable syslogging

> **NOTE**
> This example uses FC13 as the remote machine to log syslog. On FC machine, disable the following lines for UDP in /etc/rsyslog.conf.

1. MODLOAD imudp

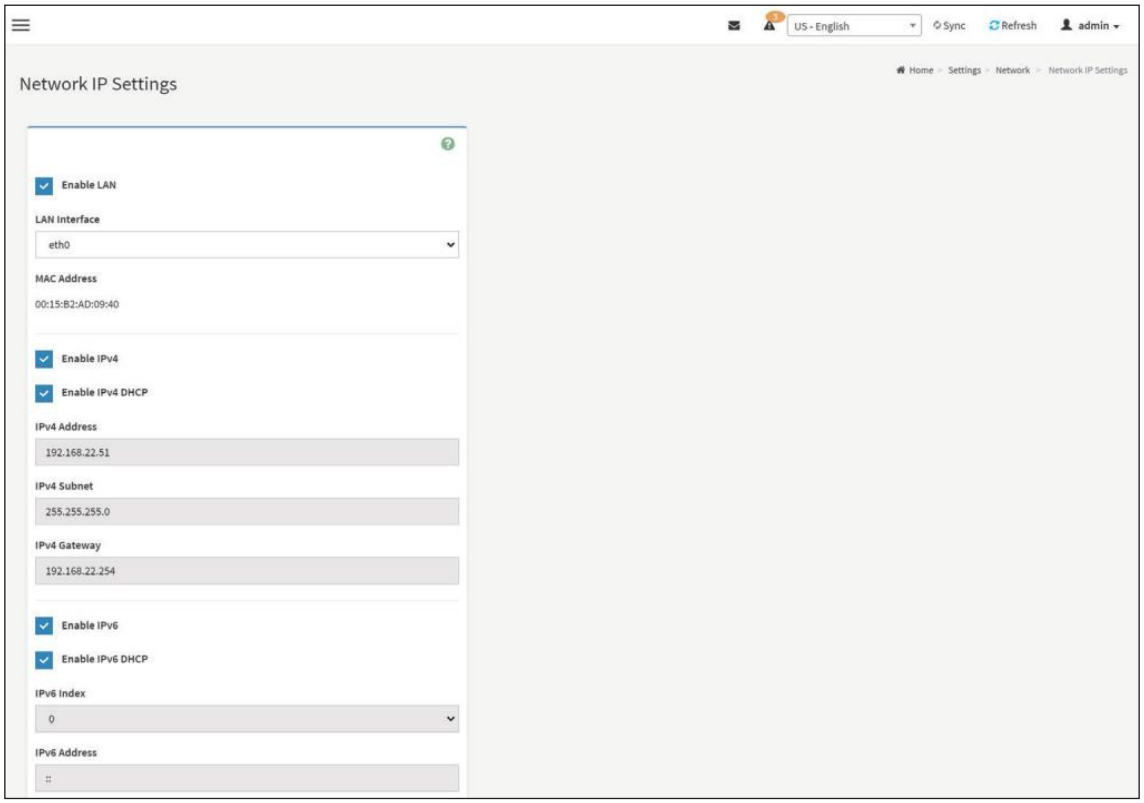
2. UDPSERVER 514

5.9.3 Network Settings

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

5.9.3.1 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).

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.

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

> **NOTE**
> Value ranges from 0 to 128.

Default 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.

Clear IPv6 Address: This field will be displayed to clear the IPv6 address only if the IPv6 address and Subnetwork Prefix Length is available for the selected index value.

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.

Procedure

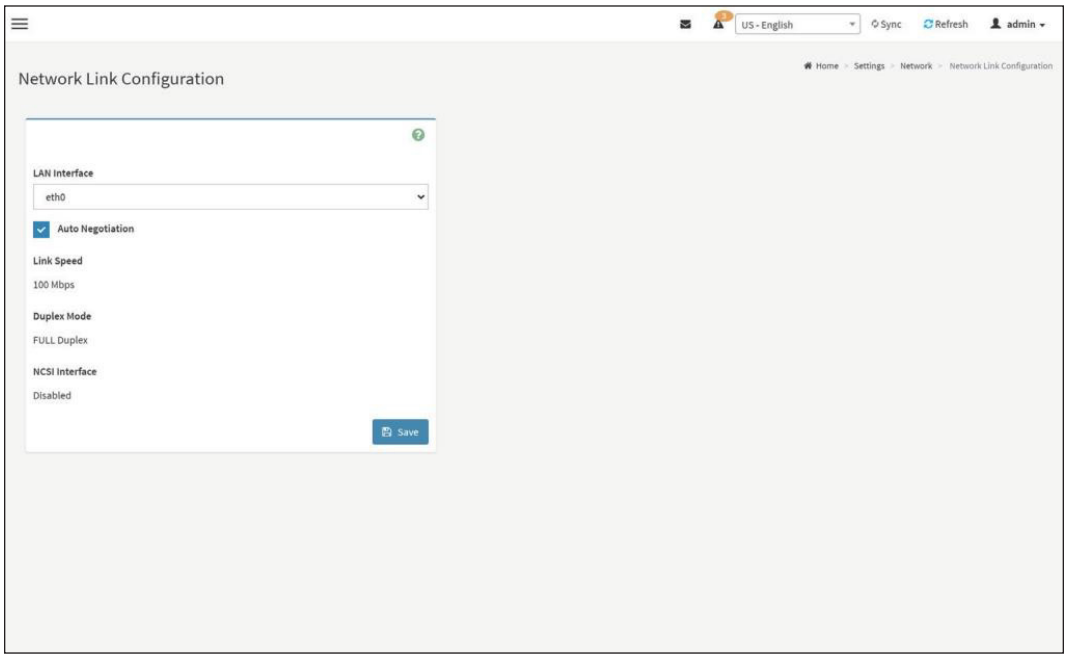
1. Check **Enable LAN** to enable LAN support for the selected interface..
2. Select the LAN Interface to be configured.
3. Check **Enable IPv4** to enable IPv4 support for the selected interface.
4. Check **Enable IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled, enter the IPv4 Address , IPv4 Subnet Mask and IPv4 Default Gateway in the respective fields.
6. In IPv6 Configuration, if you wish to enable the IPv6 settings, check **Enable IPv6**.
7. If the IPv6 setting is enabled, enable or disable the option **Enable IPv6 DHCP**.
8. If the field is disabled, enter the IPv6 Address, Subnet Prefix length and IPv6 Index in the given field.
9. In VLAN Configuration, if you wish to enable the VLAN settings, check **Enable LAN**.

10. Enter the VLAN ID in the specified field.
11. Enter the VLAN Priority in the specified field.
12. Click **Save** to save the entries.

5.9.3.2 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 from the menu bar. A sample screenshot of **Network Link Configuration** page is shown below.



The fields of Network Link Configuration page are explained below.

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

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

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

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

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

Save: To save the settings.

Procedure

1. Select the LAN Interface from the drop down list.
2. Select either Enable or Disable for Auto Negotiation.

NOTE
The Link Speed and Duplex Mode will be active only when Auto Negotiation is OFF.

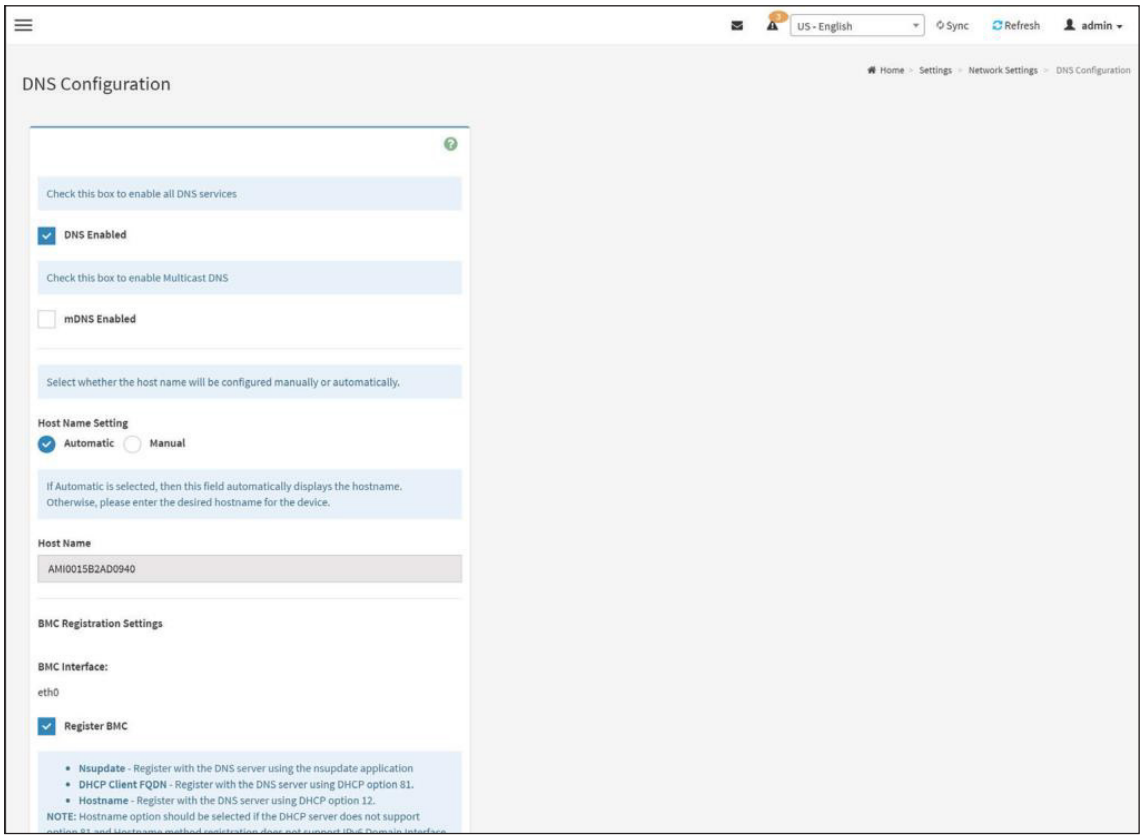
3. Select the **Link Speed** from the drop-down list.
4. Select the Duplex Mode either **Full duplex** or **Half duplex**.
5. Click **Save** to save the configuration.

5.9.3.3 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.



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.

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.

Procedure

1. In Domain Name Service Configuration, Enable DNS Service.
   - Check the option DNS Enabled to enable all the DNS Service Configurations.
2. Choose the Host Name Setting either Automatic or Manual.

> **NOTE**
> If you choose Automatic, you need not enter the Host Name and if you choose Manual, you need to enter the Host Name.

3. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
4. Under Register BMC, choose the BMC’s network port to register with DNS settings.
   Check **Register BMC** option to register with DNS settings.
   - **Nsupdate** - Choose **Nsupdate** option to register with DNS server using nsupdate application.
   - **DHCP Client FQDN** - Choose **DHCP Client FQDN** option to register with DNS Server using DHCP option.
   - **Hostname** - Choose **Hostname** option to register with DNS server using DHCP option.

> **NOTE**
> Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.
> Hostname option is not support at DHCPv6, hence IPv6 will not register to DNS server at option hostname.

5. Check **Both** option to modify TSIG authentication for both interfaces (eth0&1).
6. In **Eth 0&1 TSIG Configuration**, Check **TSIG Authentication Enabled** option to enable/disable TSIG authentication while registering DNS via nsupdate.
   - The current file name will be displayed in **Current TSIG Private file info** field.
   - To view a new one, click **New TSIG private file** to browse and navigate to the TSIG private file.
7. In the Domain Settings
   - Select the domain settings (Automatic or Manual).
   - Enter the **Domain Name** in the given field if the option "**Manual**" is being selected in domain settings field.
8. In Domain Name Server Setting
   - Select the **DNS Name Server Setting**.
   - Choose the IP Priority, either IPv4 or IPv6.
   - Enter the DNS Server address.
9. In DNS Server1, DNS Server2 and DNS Server3, enter the server addresses to be configured for the BMC.
10. Click **Save** to save the entries

5.9.4 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

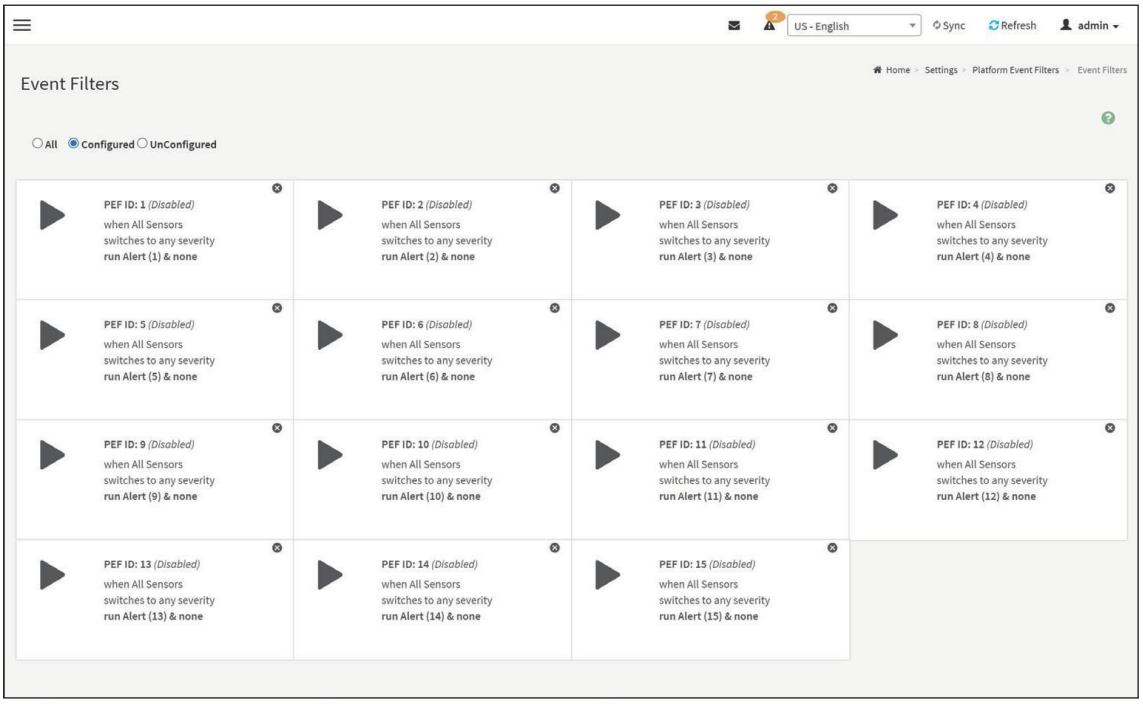
- Event Filters
- Alert Policies
- LAN Destinations

To open PEF Management Settings page, click Settings → Platform Event Filter from the menu bar. Each tab is explained below.

5.9.4.1 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.



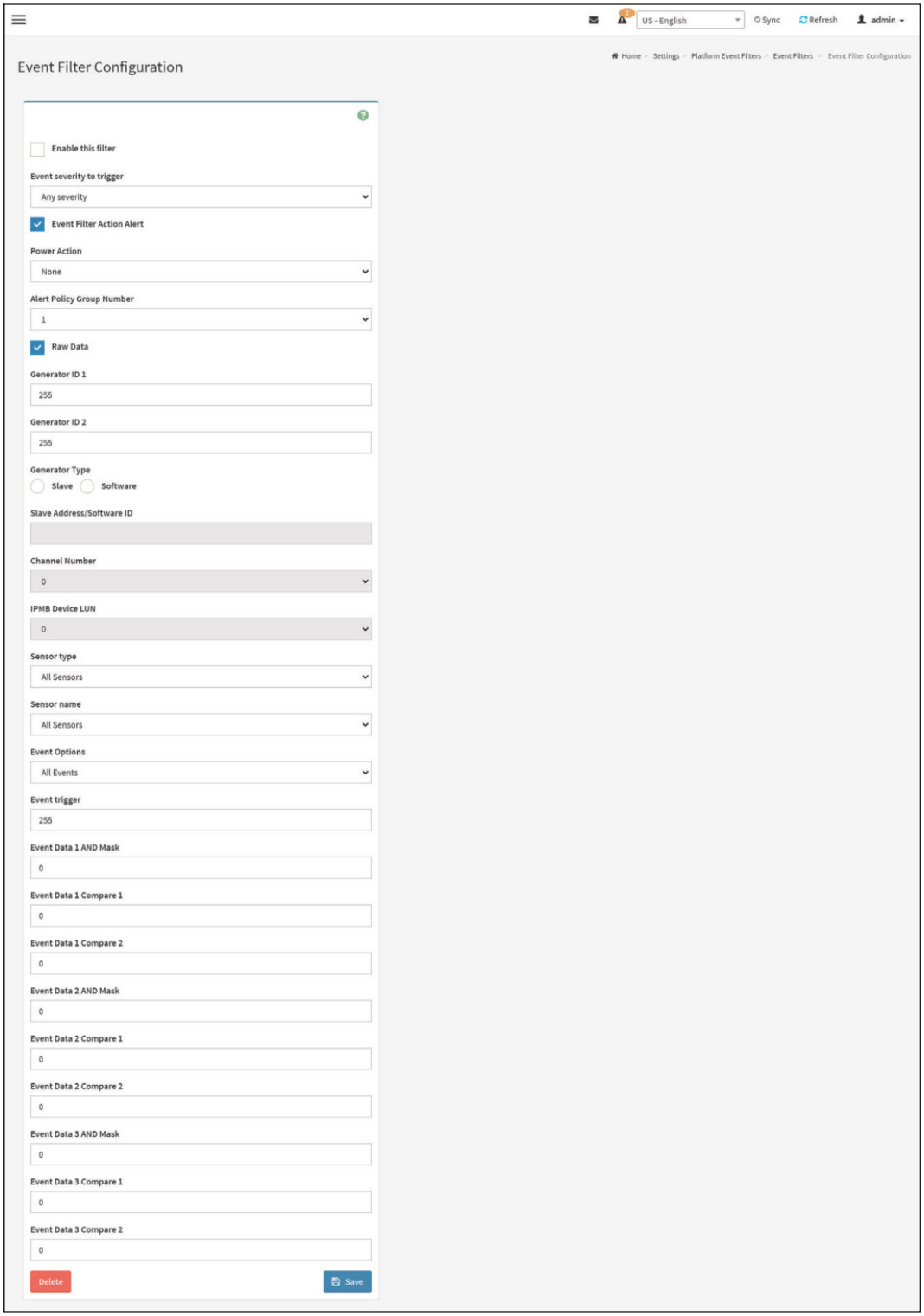
Platform Event Filters - Event Filter

The fields of Platform Event Filters Tab are explained below.

This page contains Pre-configured 40 Events with PEF IDs. Click Delete icon (⊗) 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.

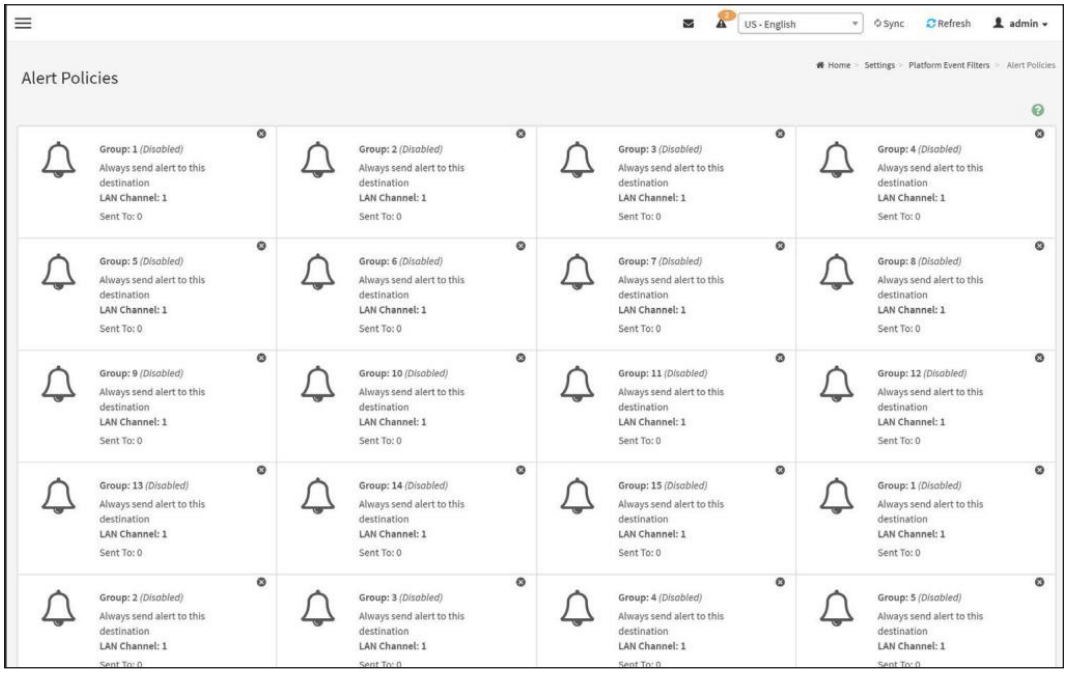
> **NOTE**
> Value ranges from 0 to 255.

- **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.

5.9.4.2 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

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.

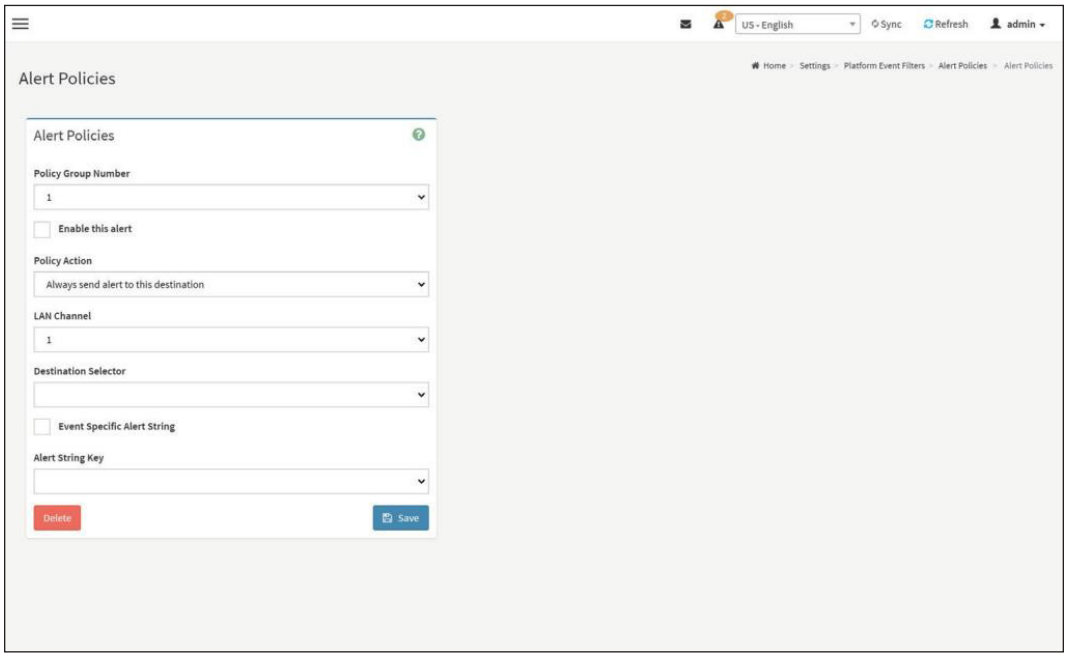
Alert String Key: To specify which string is to be sent for this Alert Policy entry.

Save: To save the Alert Policies entries.

Delete: To delete the selected configured Alert Policy.

Procedure

1. In the Alert Policies Section, select the slot for which you have to configure the Alert policy. That is, In the Alert Policies page, if you have chosen Alert Policy Group Number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click on the empty slot to open the Alert Policies page as shown in the screenshot below.



3. Select **Policy Group Number** from the drop-down list.
4. Check **Enable this alert** to enable the policy settings.
5. Choose any of the **Policy Action** from the list.
6. Choose particular **LAN Channel** from the available channel list.
7. In the **Destination Selector**, choose particular destination from the configured destination list.

> **NOTE**
> LAN Destination has to be configured under Settings → Platform Event Filters → LAN Destinations. That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destinations tab.

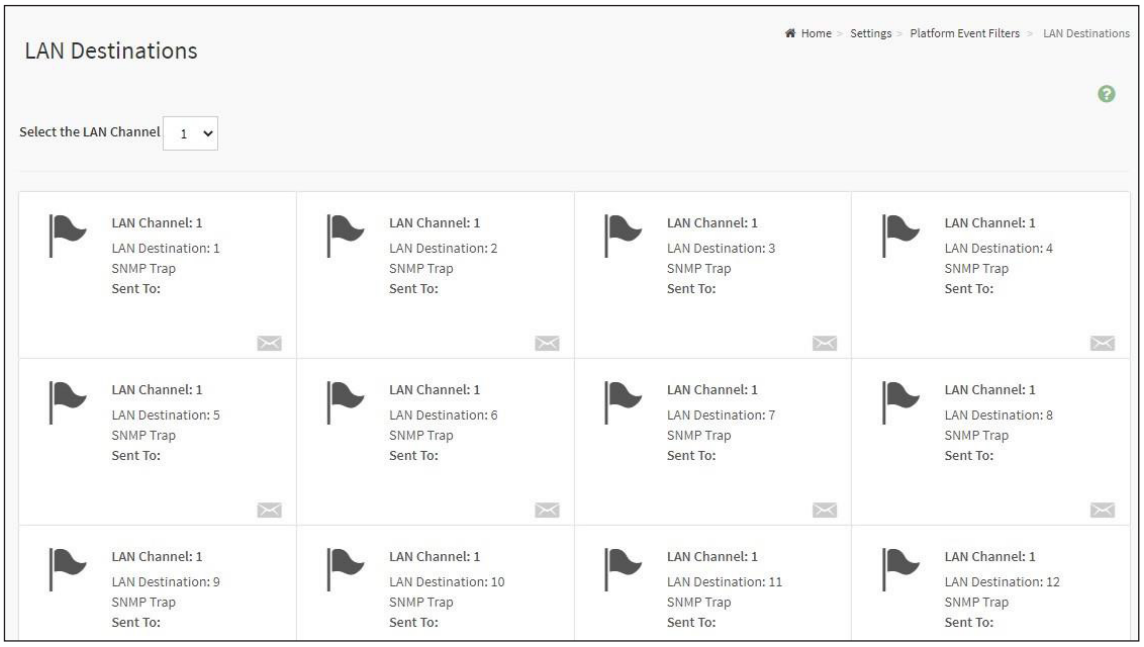
8. Enable **Event Specific Alert String**, if the Alert policy entry is Event Specific .
9. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.

> **NOTE**
> Using Web UI, Alert strings cannot be configured but option for Event Specific alert strings can be enabled/disabled. There is an option to select only the alert string keys, but alert strings has to be configured using IPMI Command (Set PEF Config Parameter “Alert String”). # and ; symbols are not supported for PEF Alert string.

10. Click **Save** to save the new alert policy and return to Alert Policy list.
11. Click **Delete** to delete a configuration.

5.9.4.3 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

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

Select any empty slot to configure LAN Destinations.

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.

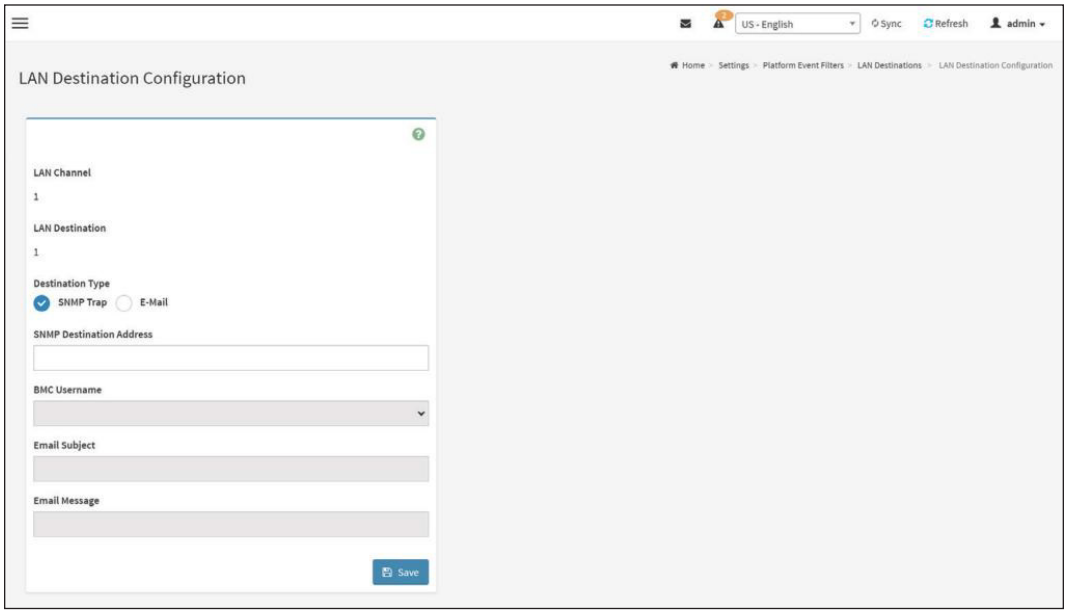
NOTE
User should be configured under ***Settings*** → ***Users Management***

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

Delete: To delete the selected configured LAN Destination.

Procedure

1. In the **LAN Destinations** section, choose the number of slots to be configured. This should be the same number of slot that you have selected in the Alert Policies - Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policies page of Alert Policies tab, then you have to configure the 4th slot of LAN Destination page.
2. Select the slot and click on the empty slot. This opens the **LAN Destination entry**.



Add LAN Destination entry Page

3. In the **LAN Channel Number** field, the LAN Channel Number for the selected slot is displayed and this is a read only field.
4. In the LAN Destination field, the destination for the newly configured entry is displayed and this is a read only field.
5. In the **Destination Type** field, select the one of the types.
6. In the **SNMP Destination Address** field, enter the destination address.

> **NOTE**
> If Destination type is E-mail Alert, then give the e-mail address that will receive the e-mail.

7. If the destination type is Email alert, select the **BMC User Name** from the list of users.

> **NOTE**
> E-mail address should be configured under Settings → User Management.

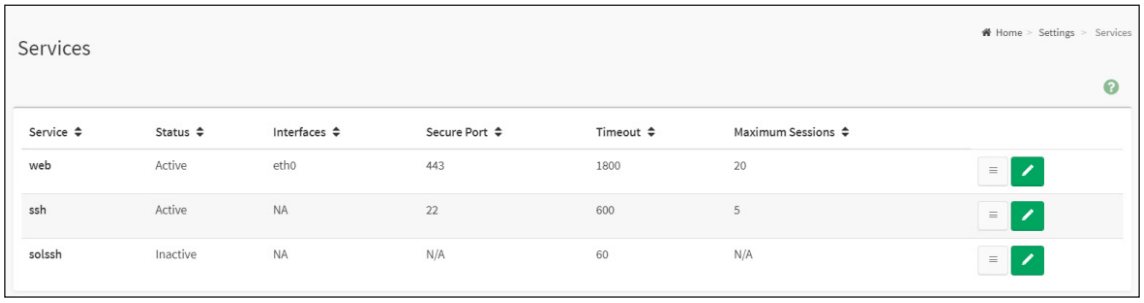
8. In the **Email Subject** field, enter the subject.
9. In the **Email Message** field, enter the message.
10. Click **Save** to save the new LAN destination and return to LAN destination list.
11. Click **Delete** to delete a configuration.
12. Click Message icon ( ) to send sample alert to configured destination.

> **NOTE**
> Test alert can sent only with enabled SMTP configuration. SMTP support can be enabled under Settings → SMTP Settings.

5.9.5 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.



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**
> Telnet service and SOLSSH will not support secure port. Port value ranges from 1 to 65535.

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 and Telnet timeout value ranges from 60 to 1800 seconds.
> - SSH and Telnet timeout value ranges from 60 to 1800 seconds.
> - SSH and telnet service will be using the same timeout value. If you configure SSH timeout value, it will be applied to telnet service also and vice versa.

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:

> **NOTE**
> All active sessions in the BMC will be terminated if the BMC is rebooted.

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.

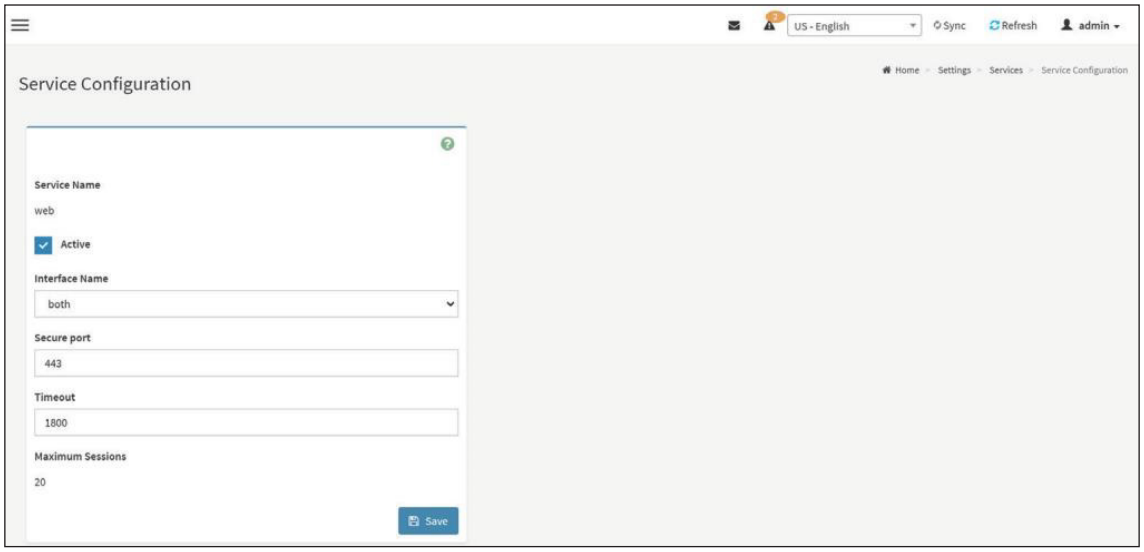
To modify the existing services:

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.



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.

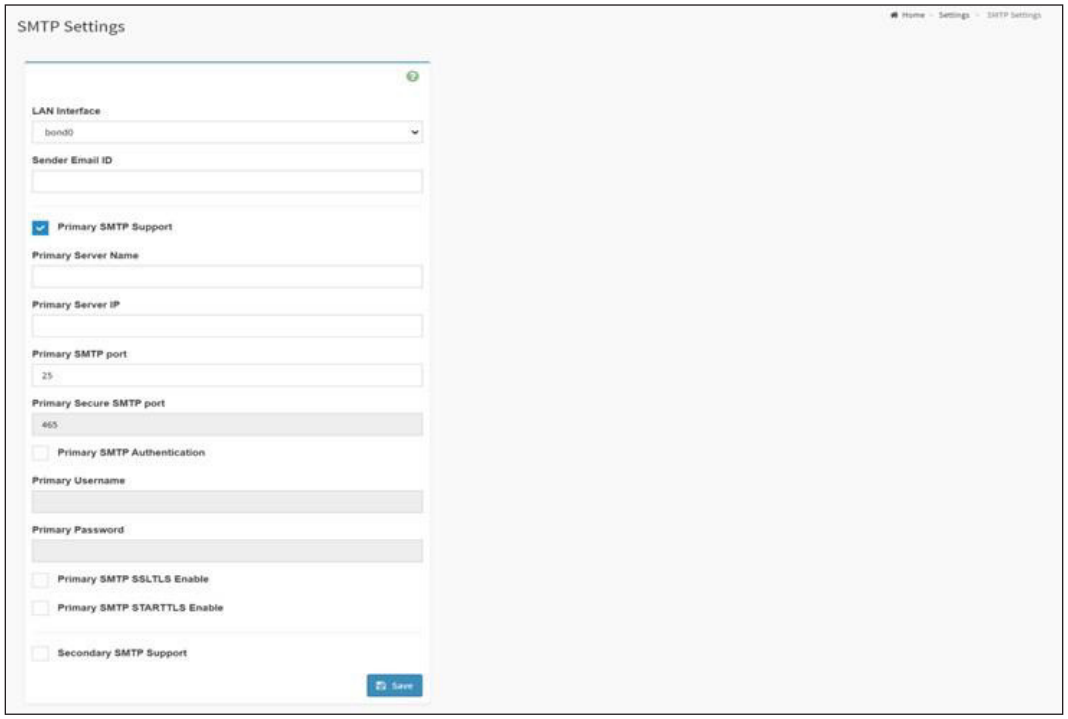
8. Click Save to save the entered changes else click Cancel to exit.

> **NOTE**
> Make sure that the SOLSSH service idle timeout should not be greater than the SSH idle timeout.

5.9.6 SMTP Settings

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

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.

- **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.

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

Upload SMTP CA Certificate File: File that contains the certificate of the trusted CA certs.

- **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 SSL 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.

Secondary 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.

Save: To save the new SMTP server configuration.

Secondary SMTP SSL Enable: To enable SSL 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 SSL support, the respective SMTP support option should be enabled.

Procedure

1. Select the **LAN Interface** from the drop-down list.
2. Enter the **Sender Email ID** in the specified field.
3. Check **Primary SMTP Support** option to enable SMTP support for the BMC.
4. Enter the Machine Name of the SMTP Server in the **Primary Server Name**.

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

5. Enter IP address of the SMTP Server in the **Primary Server IP** field. It is a mandatory field.
6. Enter the **Primary SMTP Port** in the specified field.
7. Enter the **Primary Secure SMTP Port** in the specified field.
8. Enable the check box **Primary SMTP Authentication** if you want to authenticate SMTP Server.
9. Enter your **Primary User name** and **Primary Password** in the respective fields.
10. Enable the check box P**rimary SMTP SSLTLS Enable** to send data through secure Port.

NOTE
If this option is selected, STARTTLS option and Normal Port will be hidden.

11. Check the **Secondary SMTP Support** option to enable Secondary SMTP support for the BMC.
12. Enter the **Secondary Server Name**, **Secondary Server IP**, **Secondary SMTP Port** and **Secure Port** values in the respective fields.
13. Enable the check box **SMTP Server Authentication** if you want to authenticate SMTP Server.

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

14. Enter your **Secondary User name** and **Password** in the respective fields.
15. Enable the check box **Secondary SMTP SSLTLS** to send data through secure Port.

NOTE
If this option is selected, STARTTLS option and Normal Port will be hidden.

16. Click **Save** to save the entered details.

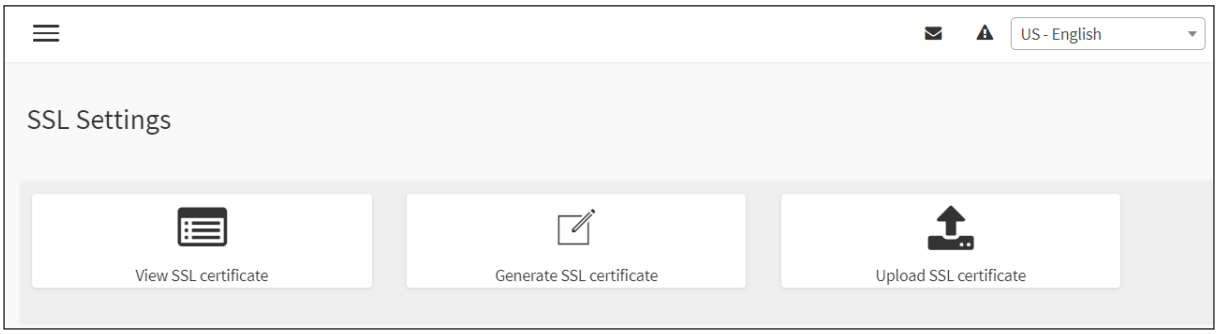
5.9.7 SSL Settings

The **Secure Socket Layer** protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a **Certificate Authority (CA)**, to identify one end or both end of the transactions.

Configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open SSL Certificate Configuration page, click Settings → SSL Settings from the menu bar. There are three tabs in this page.

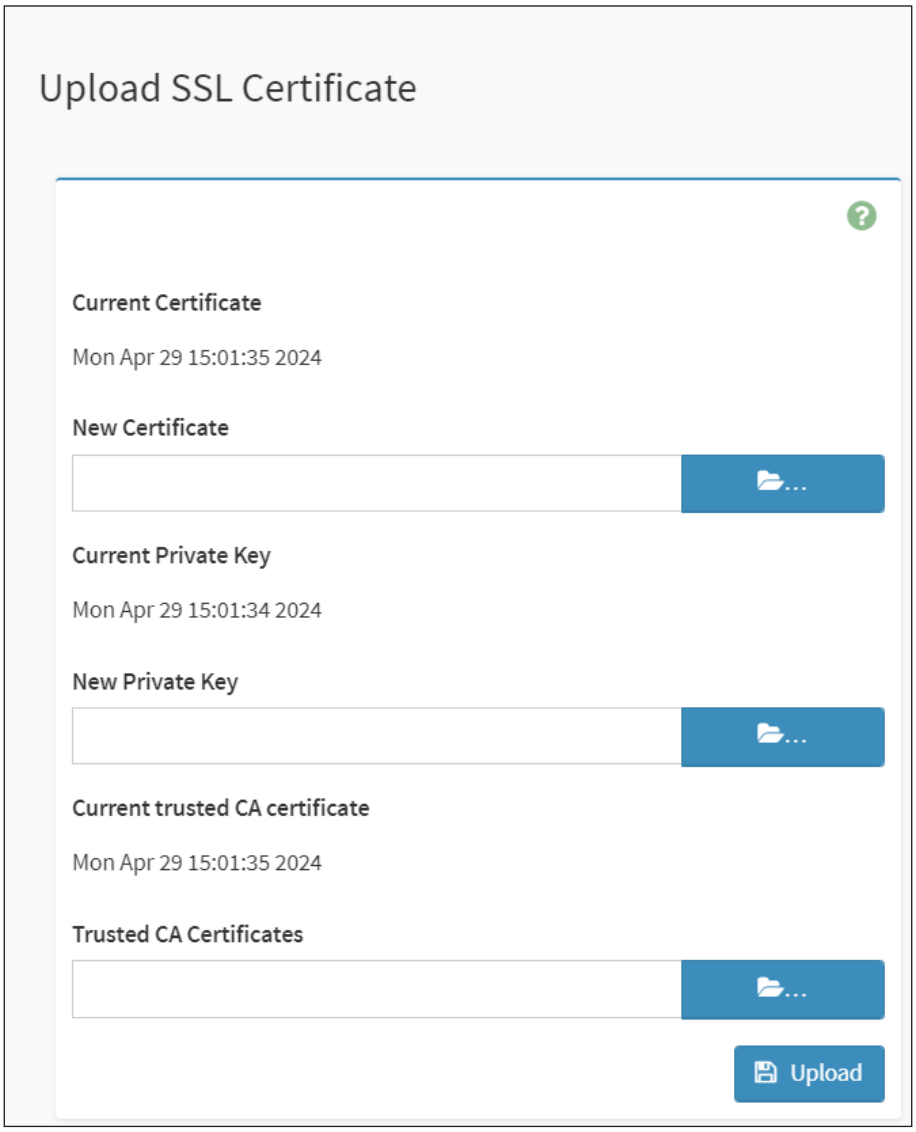
- **Upload SSL Certificate** option is used to upload the certificate and private key file into the BMC.
- **Generate SSL Certificate** option is used to generate the SSL certificate based on configuration details.
- **View SSL Certificate** option is used to view the uploaded SSL certificate in readable format.



SSL Settings

5.9.7.1 Upload SSL Certificate

A sample screenshot of Upload SSL Certificate page is shown below.



SSL Settings – Upload SSL Certificate

The fields of SSL Settings – Upload SSL Settings tab are explained below.

Current Certificate: Current certificate and uploaded date/time will be displayed (read-only).

New Certificate: Certificate file should be of pem type

Current Private Key: Current Private key information will be displayed (read-only).

New Private Key: Private key file should be of pem type

Trusted CA Support: If the Trusted CA Support checkbox is enabled then user can able to upload the Trusted CA Certificates in BMC, otherwise user can able to upload New Certificate & New Private key only.

NOTE

If Redfish feature is disabled, Trusted CA Support checkbox will be displayed, and Trusted CA Support checkbox and Trusted CA Certificates fields are optional.

If Redfish feature is enabled, Trusted CA Support checkbox will be hidden, and Trusted CA Certificates field is mandatory to upload.

Current trusted CA Certificate: Current trusted CA certificate and uploaded date/time will be displayed (read-only).

Trusted CA Certificates: Certificate chain (or Chain of Trust) is made up of a list of certificates that start from a server's certificate and terminate with the root certificate. If your server's certificate is to be trusted, its signature has to be traceable back to its root CA.

If the user uploaded New Certificate, New Private key & Intermediate key means in bmc concatenate all three files together and serve as server.pem

Based on the interlink between cacert & intermediate key shows the certificate chain.

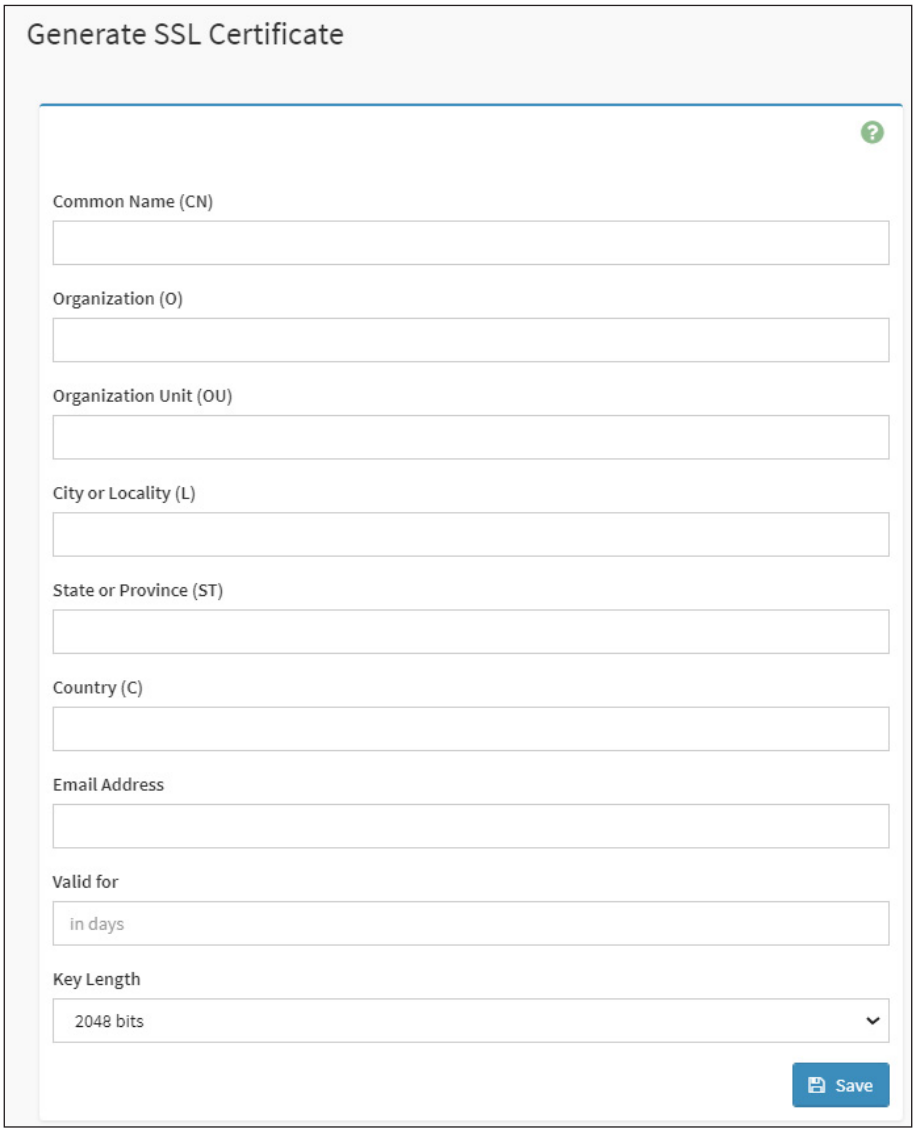
Upload: To upload the SSL certificate and privacy key into the BMC.

NOTE

- Maximum New certificate size is 10240.
- Maximum New private key size is 10240.
- Uploading New Certificate and Private key should have 2048 bit.
- New Private key should not be encrypted.
- New Certificate should not expire.
- After successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.
- If the user give Factory Restore Defaults, SSL certificate at the run-time will get vanish and it moves to the SSL certificate provided at the built-time.

5.9.7.2 Generate SSL Certificate

A sample screenshot of Generate SSL Certificate page is shown below.



SSL Settings – Generate SSL Certificate

The fields of SSL Settings – Generate SSL Certificate are explained below.
Common Name(CN): Common name for which certificate is to be generated.
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization(O): Organization name for which the certificate is to be generated.
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization Unit(OU): Over all organization section unit name for which certificate is to be generated.
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

City or Locality(L): City or Locality of the organization (mandatory).
- Maximum length of 128 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

State or Province(ST): State or Province of the organization (mandatory).
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

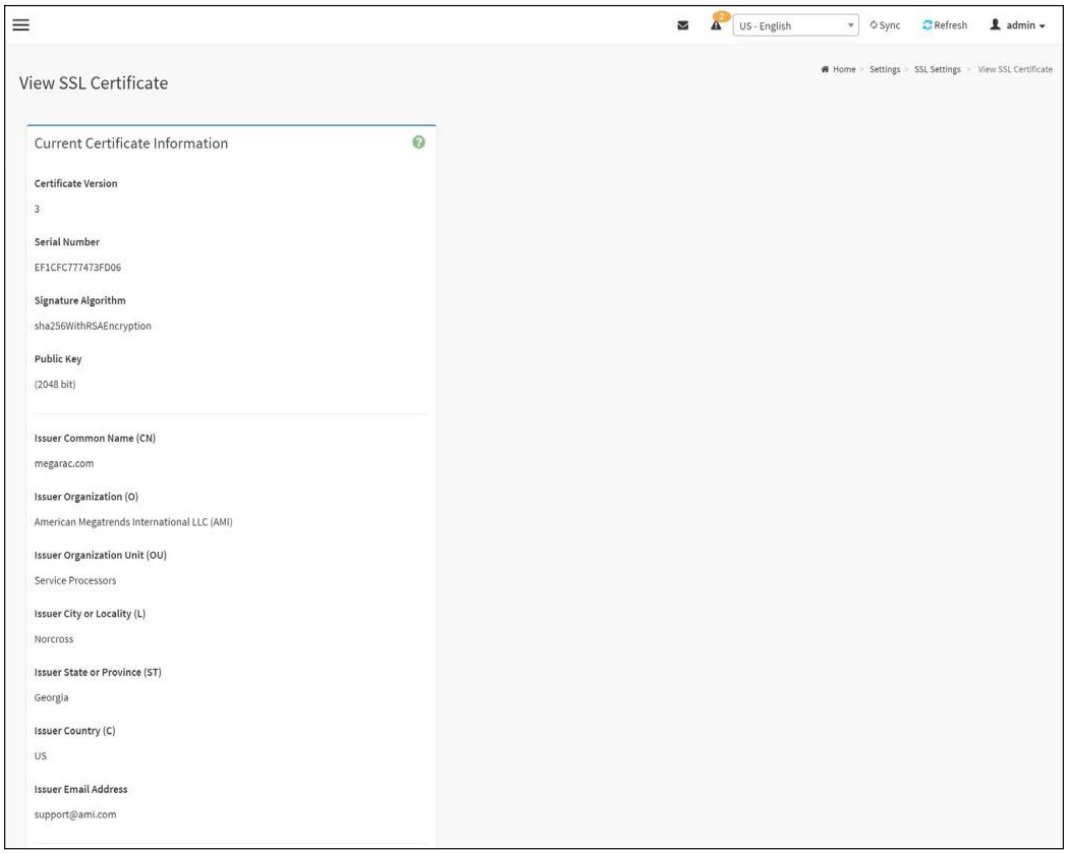
Country(C): Country code of the organization (mandatory).
- Only two characters are allowed.
- Special characters are not allowed.

Email Address: E-mail Address of the organization (mandatory).
Valid for: Validity of the certificate.
- Value ranges from 1 to 3650 days.

Key Length: The key length bit value of the certificate.
Save: To generate the new SSL certificate.

NOTE
HTTPs service will get restarted, to use the newly generated SSL certificate.

5.9.7.3 View SSL Certificate



SSL Settings – View SSL Certificate

The fields of SSL Settings – View SSL Certificate are explained below.

Basic Information: This section displays the basic information about the uploaded SSL certificate. It displays the following fields.

- Version Serial Number
- Signature Algorithm
- Public Key
- Issuer Common Name(CN)
- Issuer Organization(O)
- Issuer Organization Unit(OU)
- Issuer City or Locality(L)
- Issuer State or Province(ST)
- Issuer Country(C)
- Issuer E-mail Address
- Valid From
- Valid Till

Procedure

1. Click the Upload SSL Certificate tab, Browse the New Certificate and New Private key.
2. Click Upload to upload the new certificate and private key.
3. In Generate SSL Certificate, enter the following details in the respective fields.
   - The Common Name for which the certificate is to be generated.
   - The Organization for which the certificate is to be generated.
   - The Organization Unit name for which certificate to be generated.
   - The City or Locality of the organization
   - The State or Province of the organization
   - The Country of the organization
   - The Email address of the organization.
   - The number of days the certificate will be valid in the Valid For field.
4. Choose the Key Length bit value of the certificate.
5. Click Save to generate the certificate.
6. Click View SSL Certificate tab to view the uploaded SSL certificate in user readable format.

NOTE

- Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- You can now access your BMC securely using the following format in your IP Address field from your Internet browser: https://<your BMC address here>
- For example, if your BMC's IP address is 192.168.22.30, enter the following: https://192.168.22.30
- Please note the <s> after <http>. You must accept the certificate before you are able to access your BMC.

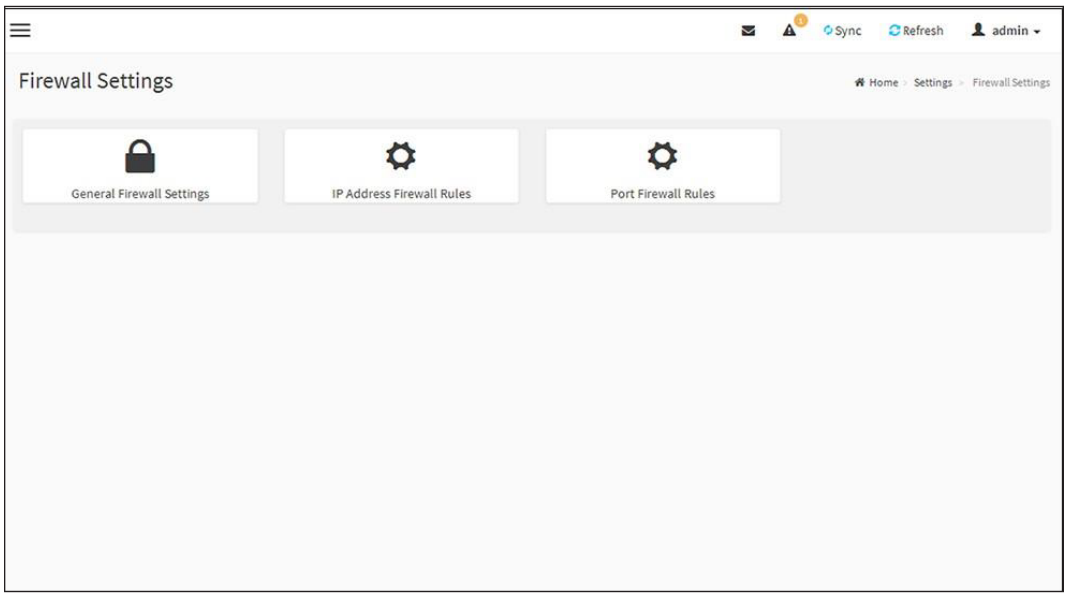
5.9.8 System Firewall

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.

5.9.8.1 General Firewall Settings

Click **General Firewall Settings** page. A sample screenshot of General Firewall Settings page is shown below.



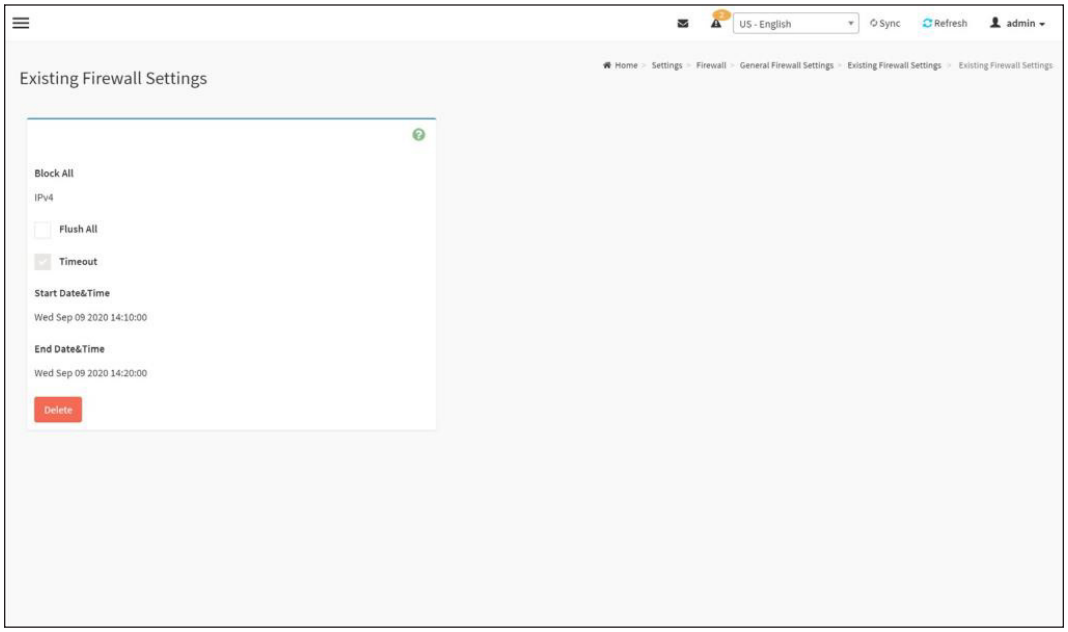
Firewall Settings

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 setting by clicking link Add Firewall Settings page.

Click General Firewall Settings → Existing Firewall Settings icon. A sample screenshot of Existing Firewall Settings page is shown below.

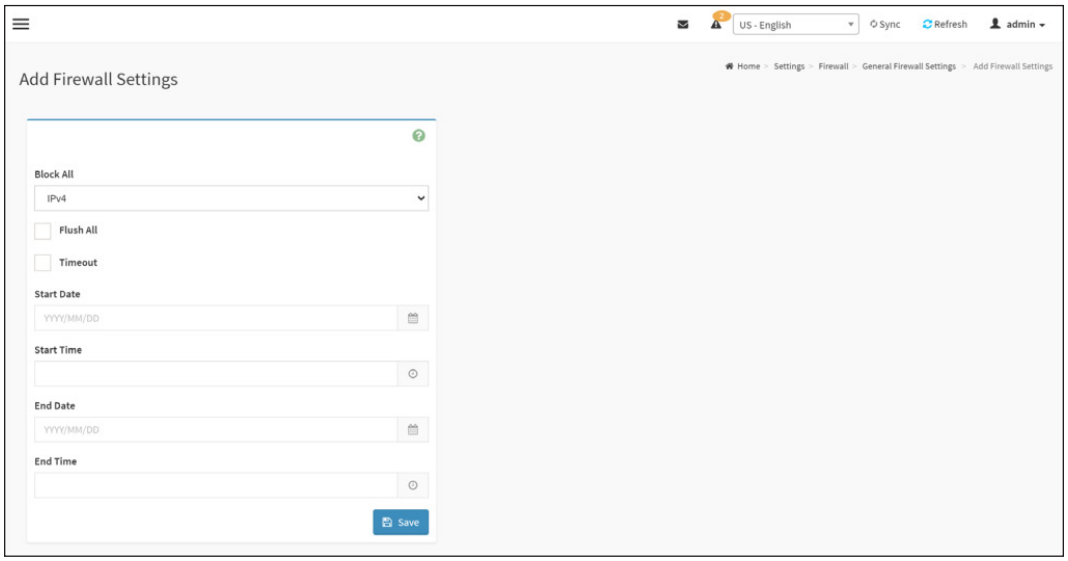


Existing Firewall Settings

- **Block All:** The blocked all the incoming IP's and Port's.
- **Flush All:** to flush all the system firewall rules.
- 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.

Procedure to add an IP address or range of IP addresses

1. Click General Firewall Settings → Add Firewall Settings. This opens the Add 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 formart.

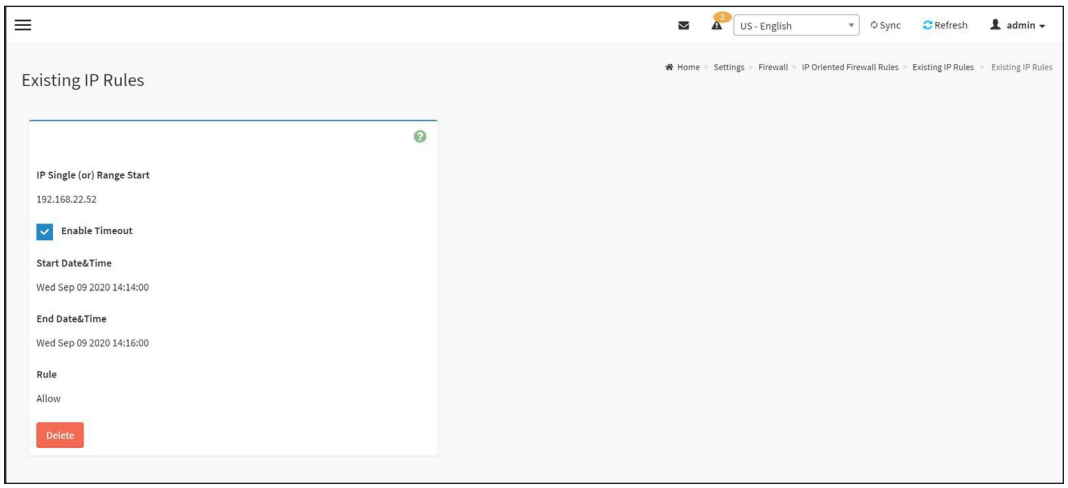
7. Click **Save** to save the changes made else click **Cancel** to go back to the previous screen.

5.9.8.2 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. lick the **IP Addresses** tab. A sample screenshot of **IP Addresses** tab is shown below.

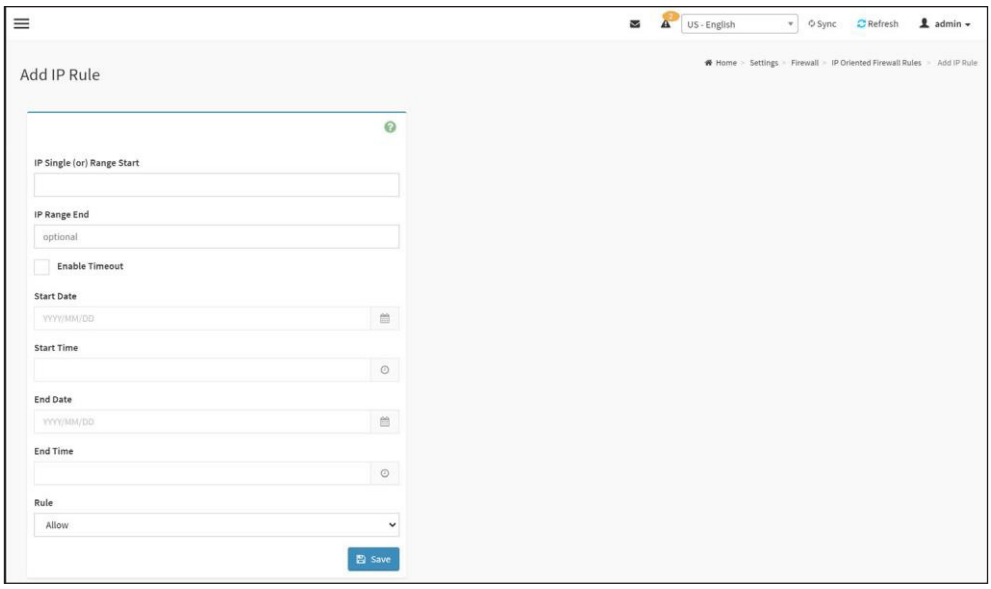


System Firewall - Existing IP Rule

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

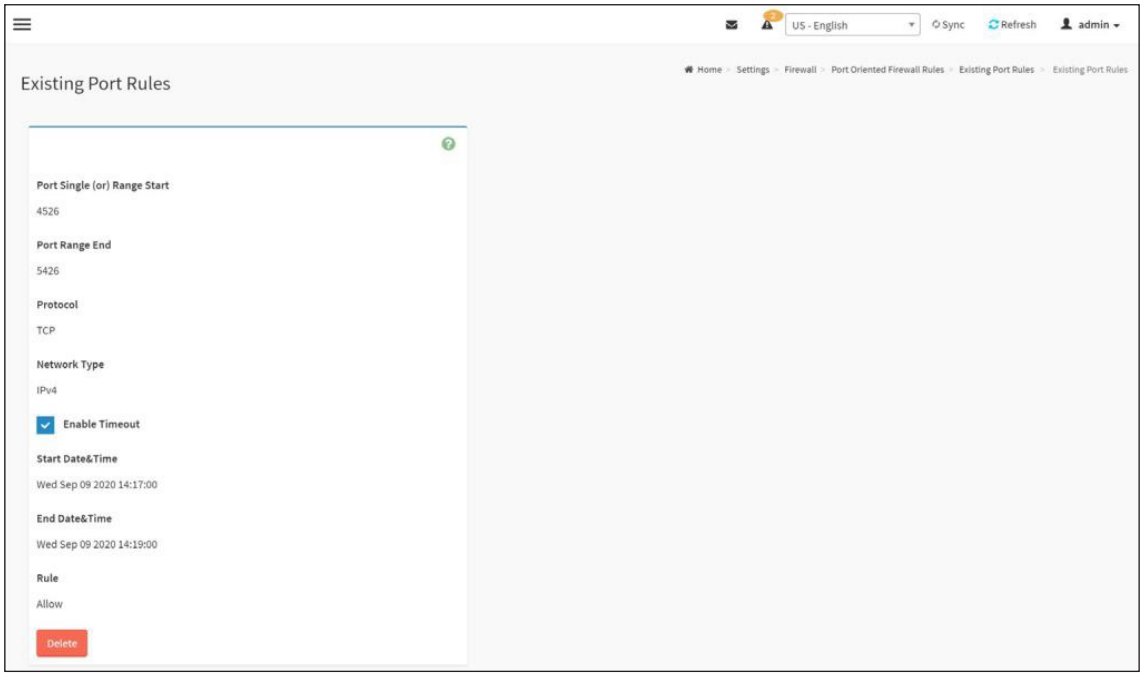
The date and time should be in the YYYY/MM/DD and hh-mm formart respectively.

9. Determine the rule to block or accept.
10. Click **Save** to save the changes made.

5.9.8.3 Port Firewall Rules

To view Existing Port Rules

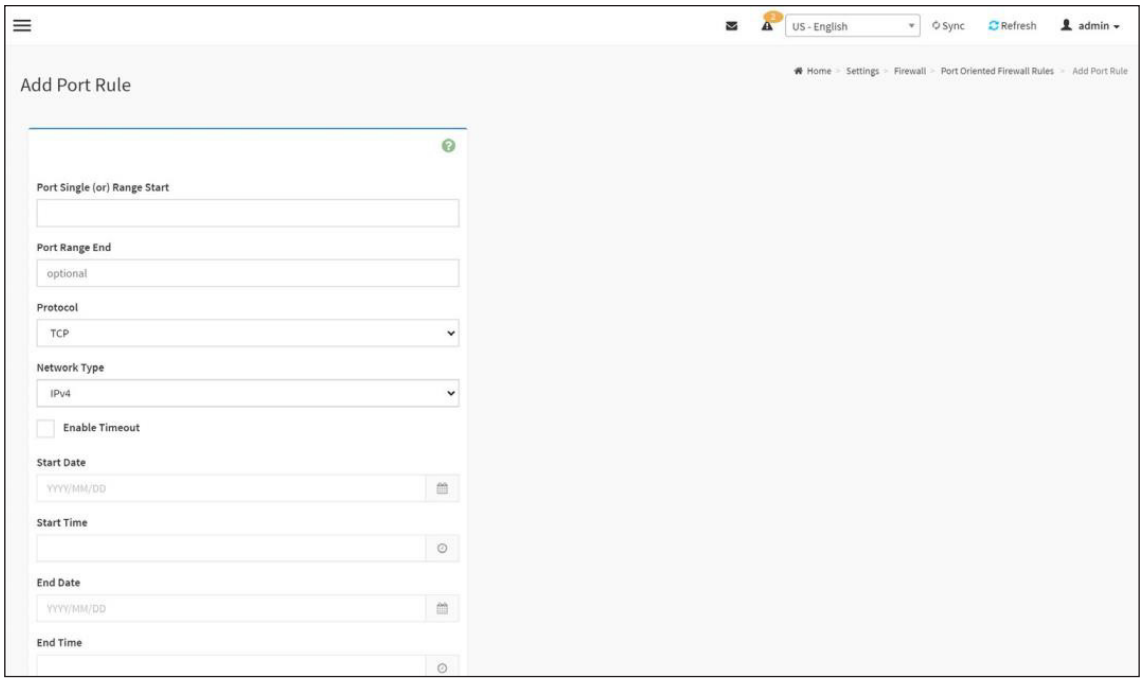
1. Click Settings → System Firewall → Port Firewall Rules → Existing Port Rules. A blank page will be opened if you did not add anything in “Add New port Rule”. If any rule is added, then the added rule will be listed in “Existing Port Rules” page
2. Click the Existing Port Rules. A sample screenshot 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.

Procedure
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.

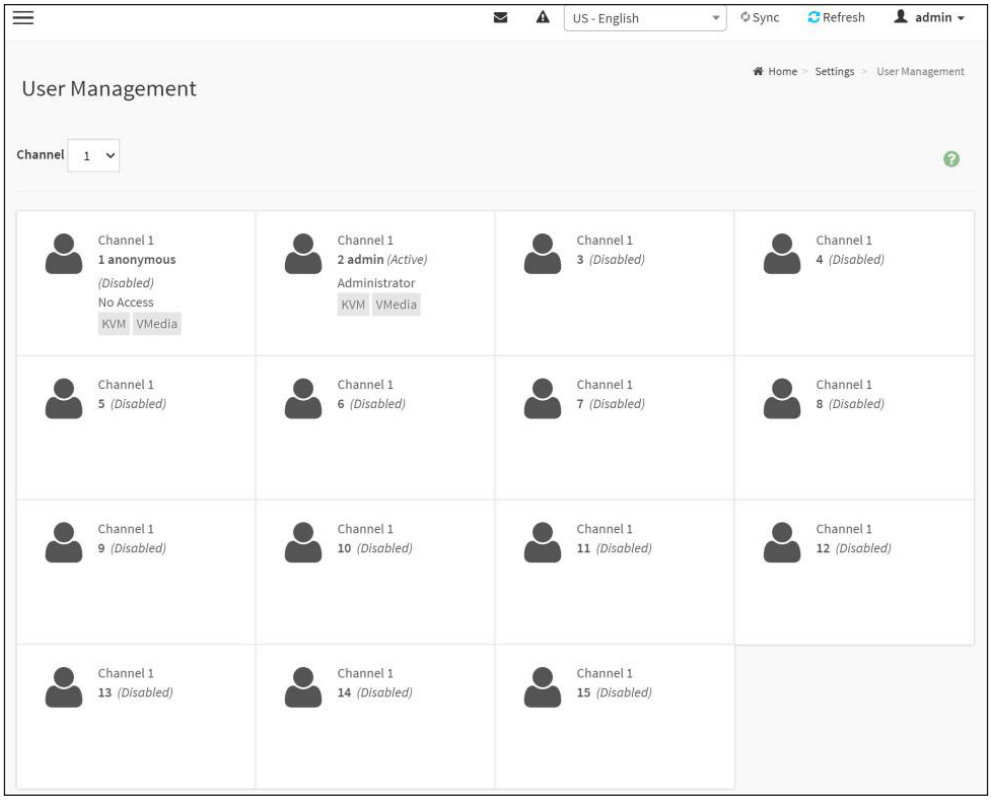
> **NOTE**
> The time should be in the YYYY/MM/DD:hh-mm format.

11. Select the **Rule** to determine the rule to **Block** or **Allow**.
1. 12. Click Save to save the changes made.

5.9.9 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.



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.

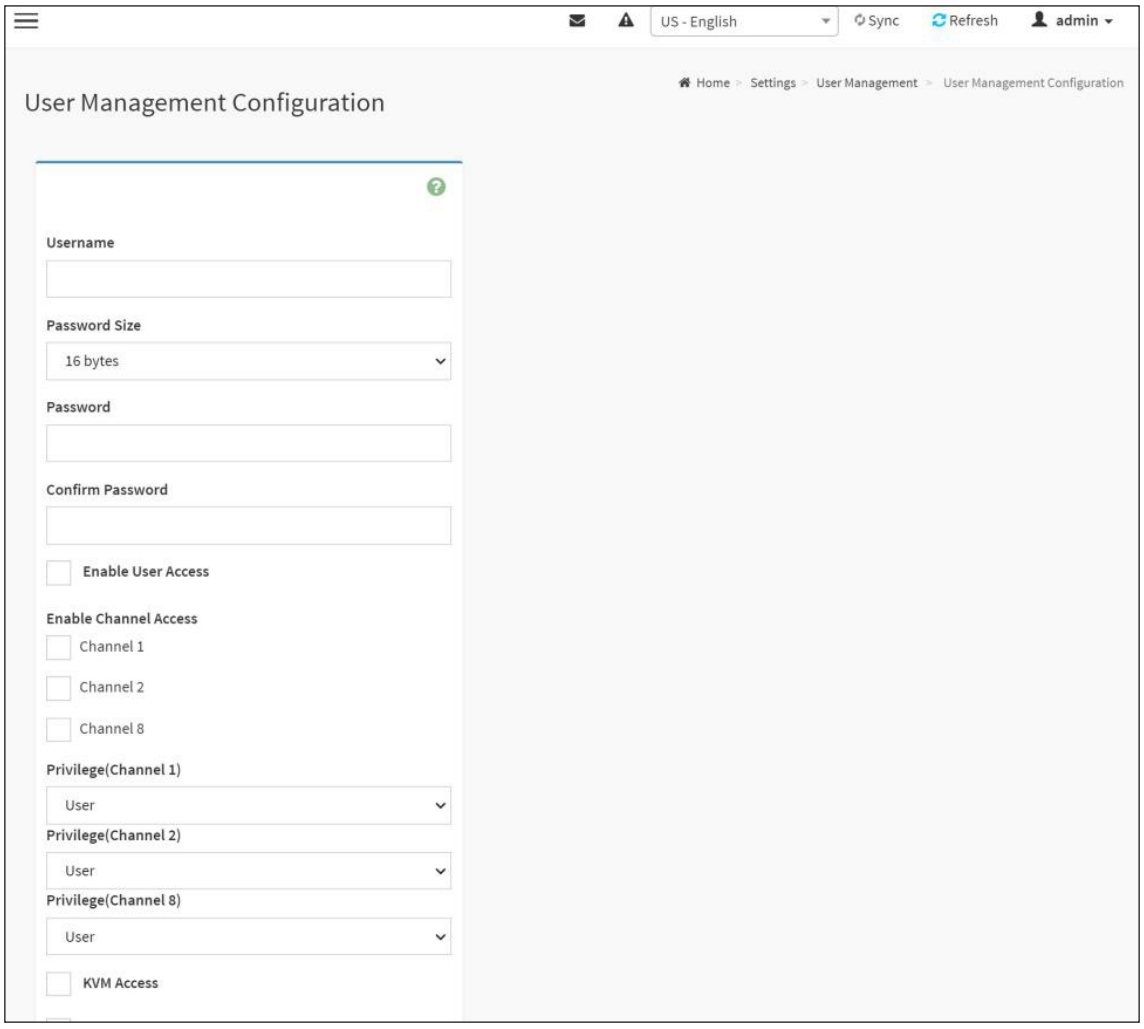
E-mail ID: Displays e-mail address of the user.

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

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	Hex	Char
00	NUL '\0'	11	DC1 (device control 1)
01	SOH (start of heading)	12	DC2 (device control 2)
02	STX (start of text)	13	DC3 (device control 3)
03	ETX (end of text)	14	DC4 (device control 4)
04	EOT (end of transmission)	15	NAK (negative ack.)
05	ENQ (enquiry)	16	SYN (synchronous idle)
06	ACK (acknowledge)	17	ETB (end of trans. blk)
07	BEL '\a' (bell)	18	CAN (cancel)
08	BS '\b' (backspace)	19	EM (end of medium)
09	HT '\t' (horizontal tab)	1A	SUB (substitute)
0A	LF '\n' (new line)	1B	ESC (escape)
0B	VT '\v' (vertical tab)	1C	FS (file separator)
0C	FF '\f' (form feed)	1D	GS (group separator)
0D	CR '\r' (carriage ret)	1E	RS (record separator)
0E	SO (shift out)	1F	US (unit separator)
0F	SI (shift in)	20	SPACE
10	DLE (data link escape)	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** (SHA256, SHA384 and SHA512) to use for SNMP settings from the drop down list.

> **NOTE**
>
> Password field is mandatory, if Authentication protocol is changed. Currently only SHA256, SHA384 and SHA512 is supported. SHA and MD5 protocols are deprecated and can be used only if previously configured and preserved user has this protocol enabled.

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.

- **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.

> **NOTE**
>
> SMTP Server must be configured to send emails.

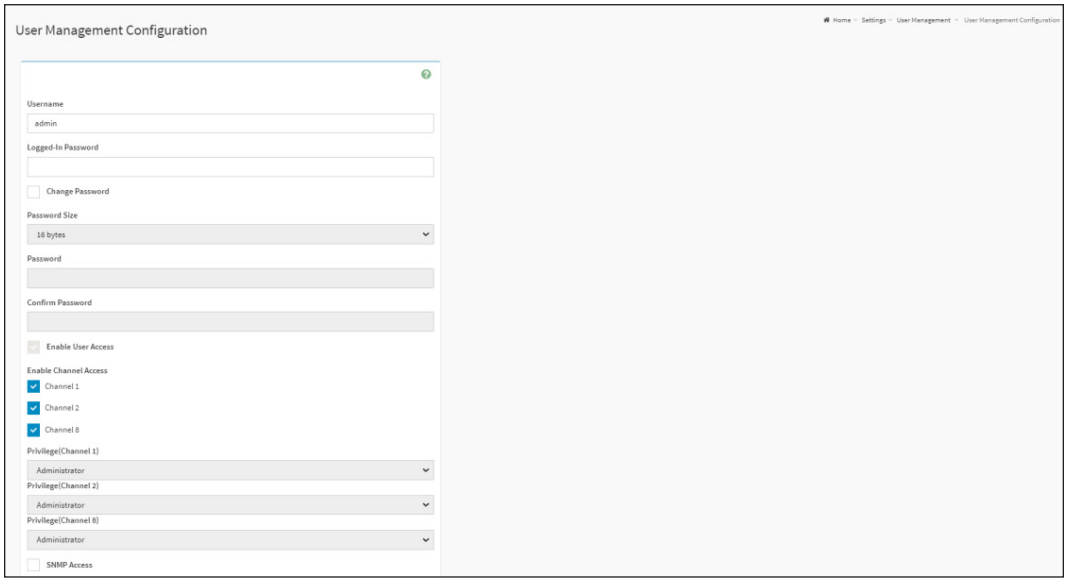
13. In the Upload SSH Key field, click Browse and select the SSH key file.

> **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. This opens a User screen as shown in the screenshot below.

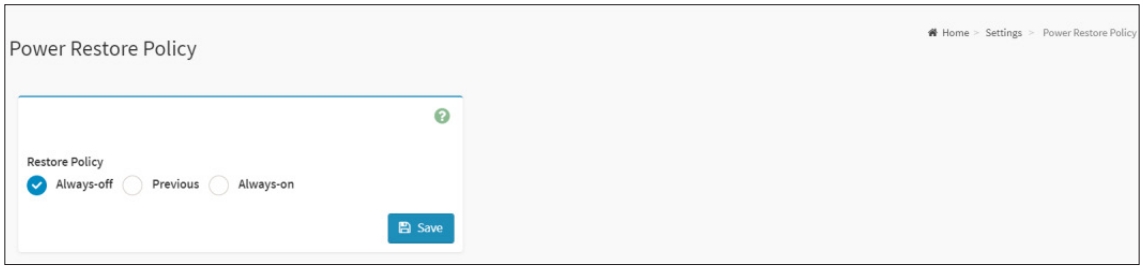


2. Check **Change Password**, if you wish to change the existing Password.
3. Follow the steps (3 to 15) of **Procedure to add a new User**.
4. Click Save to save the changes and return to the users list.
5. Click Delete to delete the user.

> **NOTE**
> There is a list of reserved users which cannot be added / modified as BMC users.
> ***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*

5.9.10 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

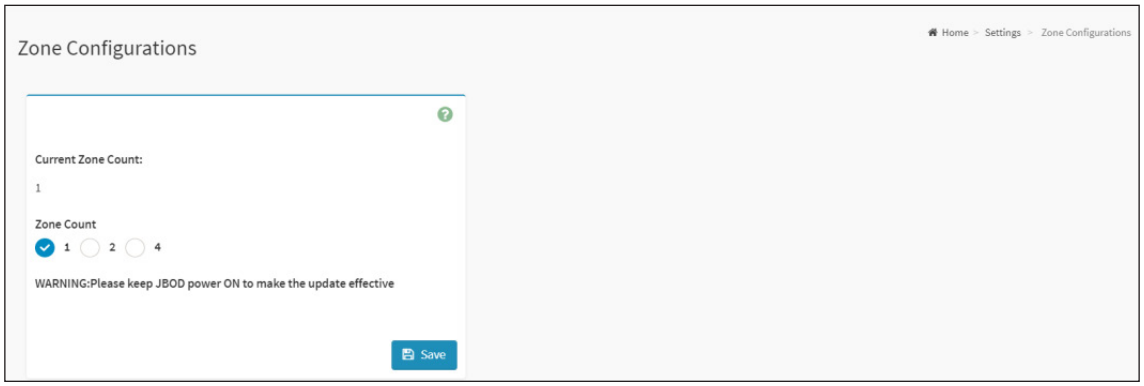
Previous: Restore to the previous state

Always-on: Keep power on

5.9.11 Zone Configurations

Remove the SAS cable (SFF-8644) between the HBA/RAID card and the JBOD-4U60 before configuration T10 zoning. After configuring T10 zoning, please power cycle the JBOD-4U60 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.



Zone Configuration page

In the BMC Web UI, we only provide three predefined T10 zoning settings: 1 (disabled), 2 and 4. The PHYs of the SAS expanders for the wideport (Hub) and disks (Edge) will be separated into different zoning groups if the zoning is enabled.
The predefined zoning groups for different settings are as followed:

Zone Count 1: (Disable Zoning)

Hub:

Zoning Group	1
Wideport	1,2,3,4

Edge:

Zoning Group	1
Disk Slot	1~24

Zone Count 2:

Hub:

Zoning Group	1	2
Wideport	1,2	3,4

Edge:

Zoning Group	1	2
Disk Slot	1~12	13~24

Zone Count 4:

Hub:

Zoning Group	1	2	3	4
Wideport	1	2	3	4

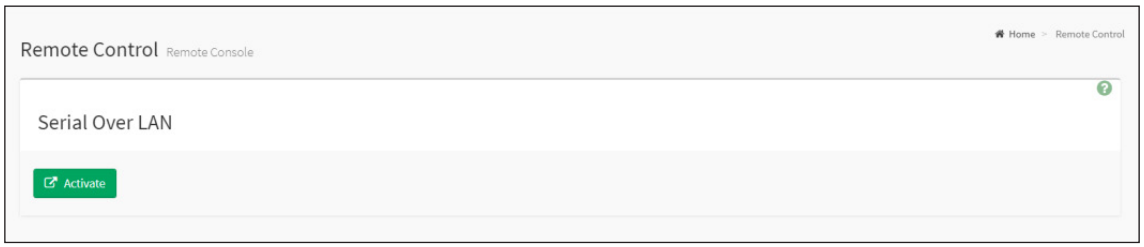
Edge:

Zoning Group	1	2	3	4
Disk Slot	1~6	7~12	13~18	19~24

5.10 Remote Control

To open the Settings page, click Remote Control from the menu bar.

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



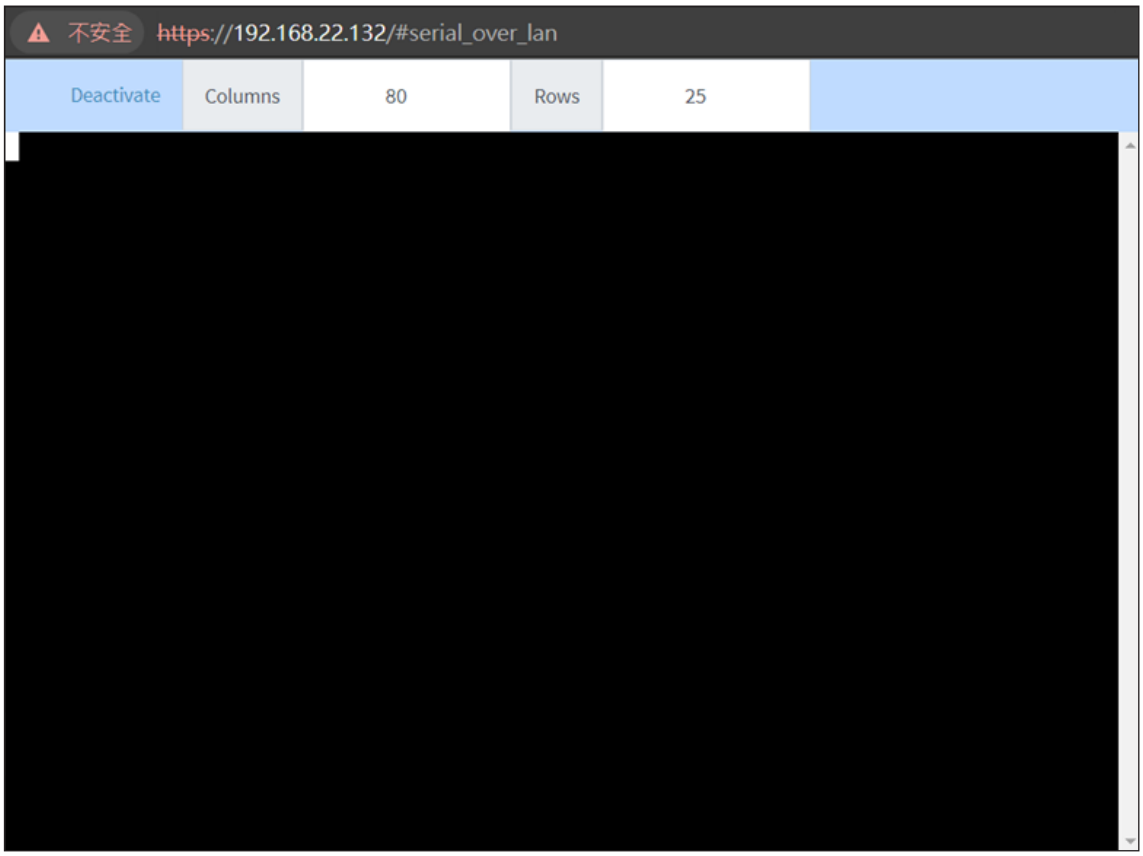
Remote Control page

5.10.1 Launch Serial Over LAN

Serial Over LAN (SOL) is a mechanism that enables the input and output of the serial port for a managed system to be redirected over IP; In this feature, Serial data is transmitted to HTML5 Web UI through websocket.

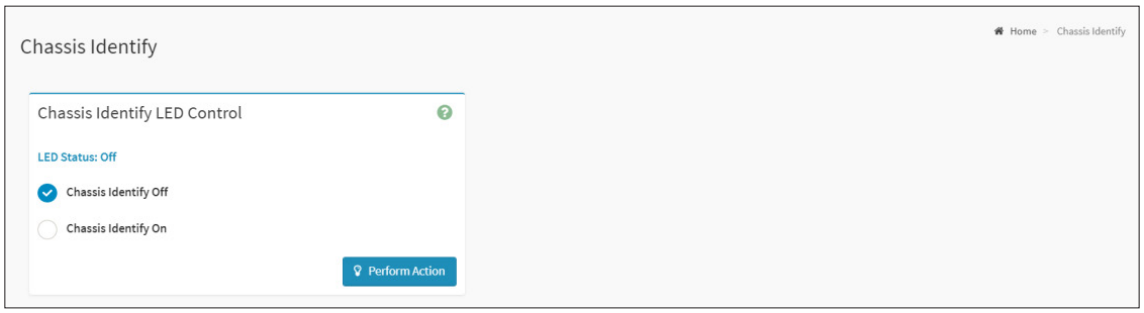
To activate SOL function, follow the below procedures:

1. Click Activate to activate SOL. A blank screen will appear as shown below.



5.11 Chassis Identify

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



Chassis Identify page

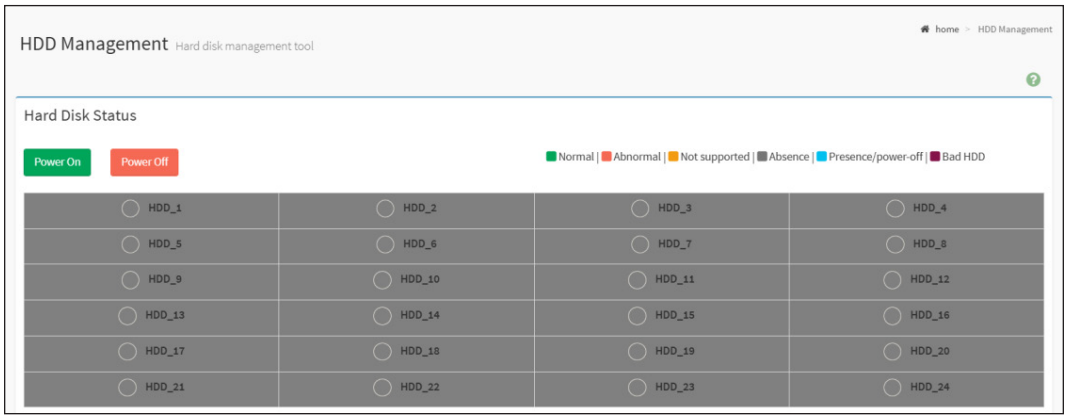
The various options of Chassis Identify LED Control are given below.

Chassis Identify Off: Turn off the chassis identify LED.

Chassis Identify On: Turn on the chassis identify LED.

5.12 HDD Management

To open HDD Management, click HDD Management from the menu bar. This page allows you to view and control the hard disk drives. A sample screenshot of the hdd management page is shown below.



HDD Management page

Each hard disk drive will display a different color representing a different state including normal, abnormal and absence, etc.

The various options of HDD Power Control are given below.

Power on: To power on the hard disk driver.

Power off: To power off the hard disk driver.

> **NOTE**
>
> The function can only work when the system power is on

5.13 Power Control

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

To open Power Control, click Power Control from the menu bar. A sample screenshot of Power Control is shown below.

Power Control page

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).

Procedure

Select an action and click Perform Action to proceed with the selected action.

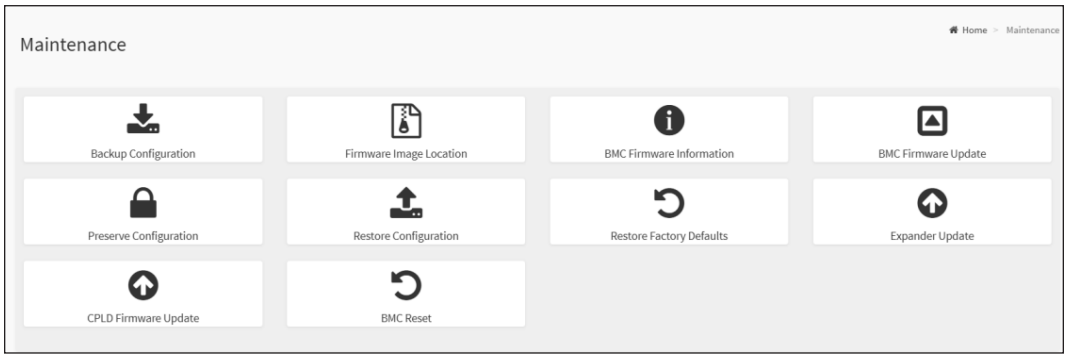
> **NOTE**
>
> During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.

5.14 Maintenance Group

To open the Maintenance page, click Maintenance from the menu bar. This group of pages allows you to do maintenance tasks on the device. The menu contains the following items:

- Backup Configuration
- Firmware Image Location
- BMC Firmware Information
- BMC Firmware Update
- Preserve Configuration
- Restore Configuration
- Restore Factory Defaults
- Expander Update
- CPLD Firmware Update
- BMC Reset

A sample screenshot of Maintenance page is displayed below.

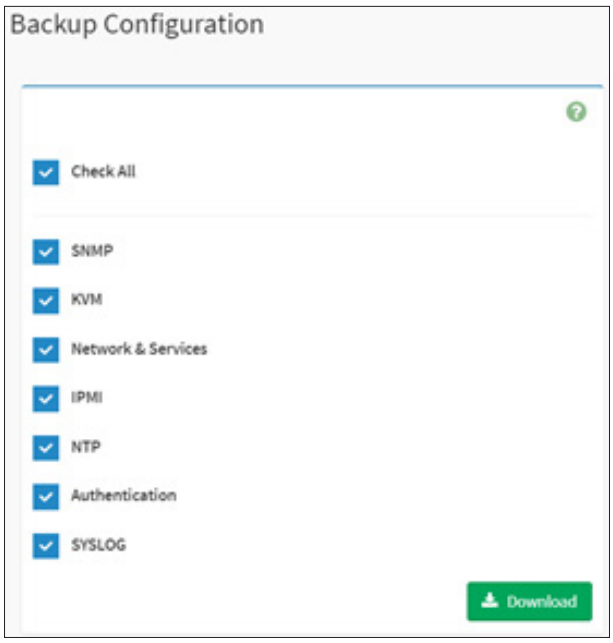


Maintenance page

5.14.1 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

The various fields of Backup Configuration page are given below.

Check All: To select all the configuration list.

Download Config: 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.
3. Click OK to perform the backup action. The Backup file will be saved in the client system.
4. Click Cancel to cancel the backup process.

> **NOTE**
>
> If select sd/emmc for backup conf space, has to create /confbkup folder in sd/emmc parti¬tion before backup.

TFTP server configuration

The TFTP server configuration is used for exporting the backup file.

> **NOTE**
>
> Ensure that no other TFTP servers are enabled, if so remove all other servers with all con- figuration files. Login as “super” user means “root” user.

Procedure to make the default tftp server

1. Install the application which are needed.

   ```
   apt-get install xinetd tftp tftpd
   ```

2. Edit the configuration file for TFTP.

   A. Edit tftp

   ```
   vi /etc/xinetd.d/tftp
   ```

   Edit the file as below:

   ```
   service tftp
   {
   protocol = udp
   port = 69
   socket_type = dgram
   wait = yes
   user = nobody
   server = /usr/sbin/in.tftpd
   server_args = <DIR to which the file to be access>
   disable = no
   }
   #EOF
   #example:server_args = /tftpboot
   ```

   > **NOTE**
   >
   > No arguments to be passed to the server_args other than directory.

B. Edit xinetd.conf

```
vi /etc/xinetd.conf
```

Add to the file:

defaults

{

Please note that you need a log_type line to use log_on_success and log_on_failure.

The default is the following :

```
# log_type = SYSLOG daemon info
}
includedir /etc/xinetd.d
```

3. Restart the server.

```
/etc/init.d/xinetd restart
```

4. Give permission to the file to access by all.

```
mkdir <DIR>
```

```
chmod -R 777 <DIR>
```

```
chown -R nobody <DIR>
```

For Example:

```
mkdir /tftpboot
```

```
chmod -R 777 /tftpboot
```

```
chown -R nobody /tftpboot
```

5. To receive the file you have to touch the file and give permission to access by all users

```
touch <DIR>/conf.bak
```

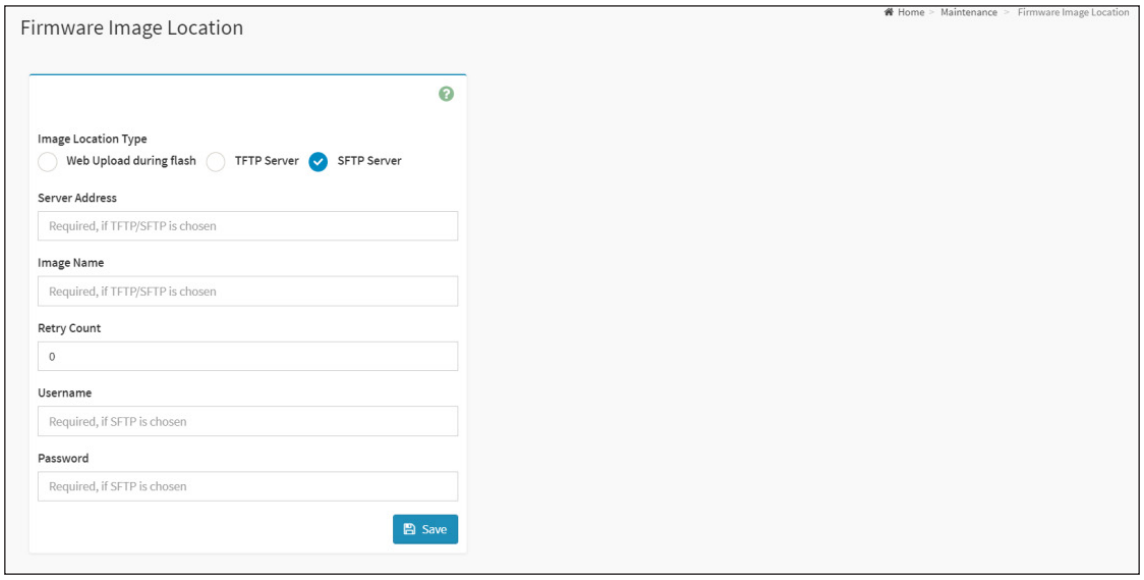
```
chmod 777 <DIR>/conf.bak
```

6. Even after all this step has been done and still facing error of timeout:
   A. Check with /etc/xinetd.d/tftp file and uncomment the EOF (Remove the '#' before the EOF alone).
   B. Restart the server.

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

TFTP/SFTP 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.

Procedure

1. Select the **Image Location Type** (Web Upload during flash/ TFTP Server/ SFTP Server).
2. If the protocol selected is TFTP/SFTP, enter the IP address of the server in the **Server Address** field.
3. If the protocol selected is TFTP/SFTP, enter the **Image Name** in the given field.
4. If the protocol selected is TFTP/SFTP, enter the **Retry Count** value.
5. If the protocol selected is SFTP, enter the **Username** and **Password** value.
6. Click **Save** to save the changes.

5.14.3 BMC Firmware Information

This page is used to configure the Firmware Information settings.

To open System Administrator page, click Maintenance → BMC Firmware Information from the menu bar. A sample screenshot of BMC Firmware Information page is shown below.

BMC Firmware Information page

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.

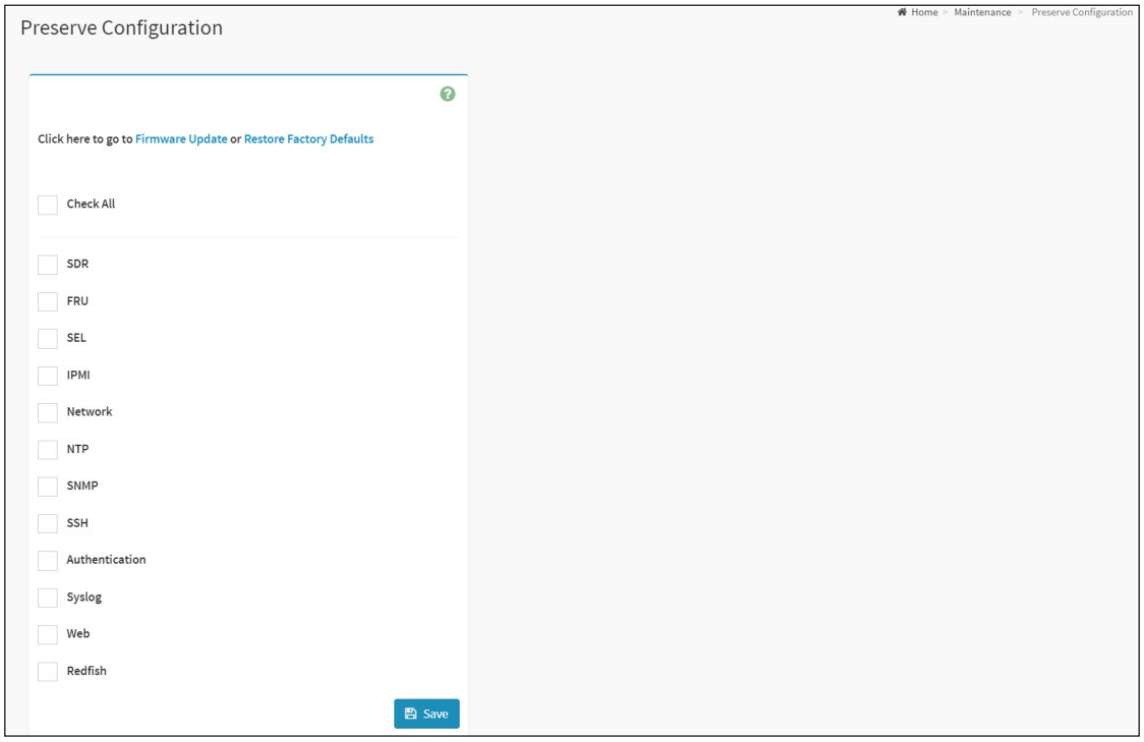
Firmware version: Describes the Firmware version of the active BMC image.

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

5.14.4 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.



Preserve Configuration page

The various fields of Preserve Configuration are as follows.

Click here to go to Firmware Update or Restore Configuration: This link will redirect to the Firmware Update or Restore Configuration 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.

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

Files Preserved

SDR

Following files will be preserved.

SDR.dat: This file contains the sensor data record information that is used in IPMI.

Dependency Configurations – NIL

FRU

Following files will be preserved.

FRU.bin: This file contains the logical field replaceable unit data that are used by IPMI.

Dependency Configurations - SDR

SEL

Following files will be preserved when Delete SEL reclaim space is disabled.

SEL.dat: This file contains the system event logs that are being logged by the IPMI.

Following files will be preserved when Delete SEL reclaim space is enabled.

Selreclaiminfo.ini – The file contains the SEL repository information.

SEL folder – This folder contains the multiple files of event logs.

Dependency Configurations – IPMI

IPMI

Select “IPMI” will automatically select another option “Network” and it’s vice versa. The following files are preserved in IPMI configuration.

IPMI.conf: This file contains the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.

Dcmi.conf: This file contains the DCMI1.5 specification parameters such as DHCP Timing1, DHCP Timing2, DHCP Timing3. The files are preserved only when DCMI1.5 feature is enabled in the MDS project configuration.

pwdEncKey: This file contains the keys that are used to decrypt the passwords. When the user password option is enabled in the MDS project configuration, this file will be preserved.

Dependency Configurations – Network

Network

To save network settings related with IPMI (LAN IP or DHCP configuration), selecting “IPMI” will automatically select the another option “Network” and it’s vice versa. After restore configuration, the Network Configuration will be preserved successfully. Following files will also be preserved.

dhcp.conf: This file is to configure the host name in the FQDN format.

dns.conf: This file is used to configure the DNS registration method and DNS server for the particular interface.

hostname: This file is used to store the Hostname of the BMC.

hostname.conf: This file is used to configure the host name creation method Manual/ Automatic for the BMC.

Vlaninterfaces: This file helps to enable the vlan interface for the particular LAN interface

vlansetting.conf: This file is to store the vlan ID and Vlan priority for the particular VLAN interface entry.

bond.conf: This file is to enable the bond interface for the specified LAN interfaces.

Interfaces: This file is to configure the IP/IPV6 addresses for the LAN interface using static/ DHCP method.

activeslave.conf: This file is to configure the active interface for the specified bond interface. This file depends on bond.conf.

hosts: This file is used to store the host name to map the IP address.

hosts.allow: This file contains the list of hosts that has permission to access the system.

hosts.deny: This file contains the list of host that does not allow accessing the system.

resolv.conf: This file is used to store the name server and domain name for hostname registration.

dhcp6c-script: This file is used to configure the domain name, DNS server IPv6 address and NTP address.

dhcp6c.conf: This file is to configure the IPv6 parameters for the DHCPv6 clients.

ncsicfg.conf: This file is to configure the NCSI related configurations.

nsupdate.conf: This file is to configure the channel ID, package ID for the NCSI interface.

phycfg.conf: This file is to configure the link speed, duplex and MTU value for the specified interface.

dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.

ncml.conf: This file contains service configuration details.

Dependency Configurations - IPMI

NTP

Following files will be preserved.

Ntp.conf: This file contains the NTP dameon protocol configuration parameters such as synchronization sources, nodes and other related information.

Ntp.stat: This file contains the auto or manual network type protocols.

adjtime: This file contains the time to synchronize the system clock.

Localtime: This file is the system link to the file local time or to the correct time zone in the system timezone directly.

Dependency Configurations - IPMI

SNMP

Following files will be preserved.

snmp_users.conf: This file contains the SNMP user configurations such as user name and password encryption mechanism for the specific users.

Snmpcfg.conf: This file contains the SNMP users privilege levels such as ro user and rw user.

Dependency Configurations - NIL

SSH

Following files will be preserved.

snmp_users.conf: This file contains the keyword argument pairs of configurations such as Address family, Accept Env, Allow, users, authorized key files etc.

ssh_host_dsa_key , ssh_host_rsa_key: These files contain the private parts of the host keys.

ssh_host_dsa_key.pub, ssh_host_rsa_key.pub: These files contain the public parts of the host keys.

Dependency Configurations - NIL

Authentication

Following files will be preserved.

activedir.conf: This file contains the configurations such as sslenable, timeout, racdomain, adtype, adfilterdc1, adfilterdc2, adfilterdc3, username, password, and rolegroup information such as name domain and privileges.

openLdapGroup.conf: This file contains the oprnm ldap role group information such as name domain and privilege.

nsswitch.conf: This file contains the sources to obtain the name service information in the range of categories and in what order.

pam_withunix: This file contains the PAM Order of modules such as IPMI, LDAP, RADIUS and UNIX.

pam_wounix: This contains the PAM Order of modules such as IPMI, LDAP and RADIUS.

group: This file contains the Linux group. It stores the group information or defines the user group information in Linux.

passwd: This file contains the user login information for the Linux system.

shadow: This file contains the encrypted password information for the clients.

ldap.conf: This file contains the ldap server configuration details such as bindn, binpw, pam_ password, nss_reconnect_tries, port, port secondary, host, host secondary.

radius.conf: This file contains the radius server IP address, port number, secret, timeout, privilege etc.

Dependency Configurations – NIL

Syslog

The following files will be preserved.

syslog.conf

rotate.conf

rsyslog.conf

These files contain the system log configuration details to preserve different event categories such as alert, critical, error notification etc.

Dependency Configurations – NIL

Web

The following files will be preserved.

updatefirmware.conf: This file contains the firmware image location details to update firmware configuration.

Dependency Configurations – NIL

Redfish

Following files will be preserved.

redis-dump.rdb.gz: This gzip file contains compressed redis db data.

RedisdbChecksum: This is the checksum value of redis-dump.rdb.gz file.

redfish: This folder contains the multiple files of Redfish.

Dependency Configurations – IPMI

Procedure

1. Click Firmware Update or Restore Configuration link to view Firmware Update or Restore Configuration page accordingly.
2. Select the required Preserve Configuration items by either choosing the items individually by selecting the appropriate check boxes or by selecting all or none using **Check All**.
3. Click Save to save the changes.

5.14.5 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

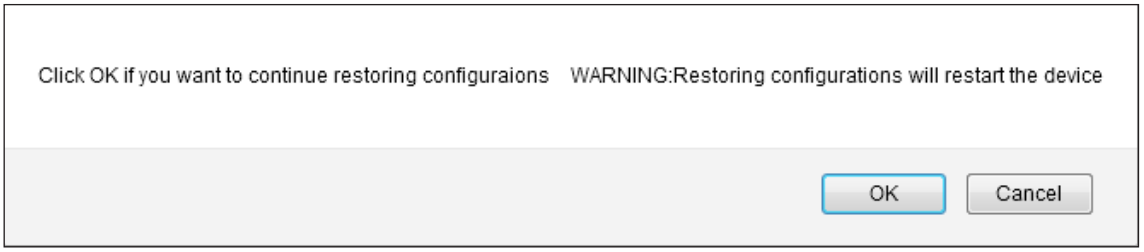
The various fields Restore Configuration page are given below.

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.

Procedure for Restore Configuration

1. Click Browse to select the configuration file that needs to be backup and used to Restore the configuration, when needed.
2. Click Upload to restore the backup files. The Restore Configuration page will appear as shown below.



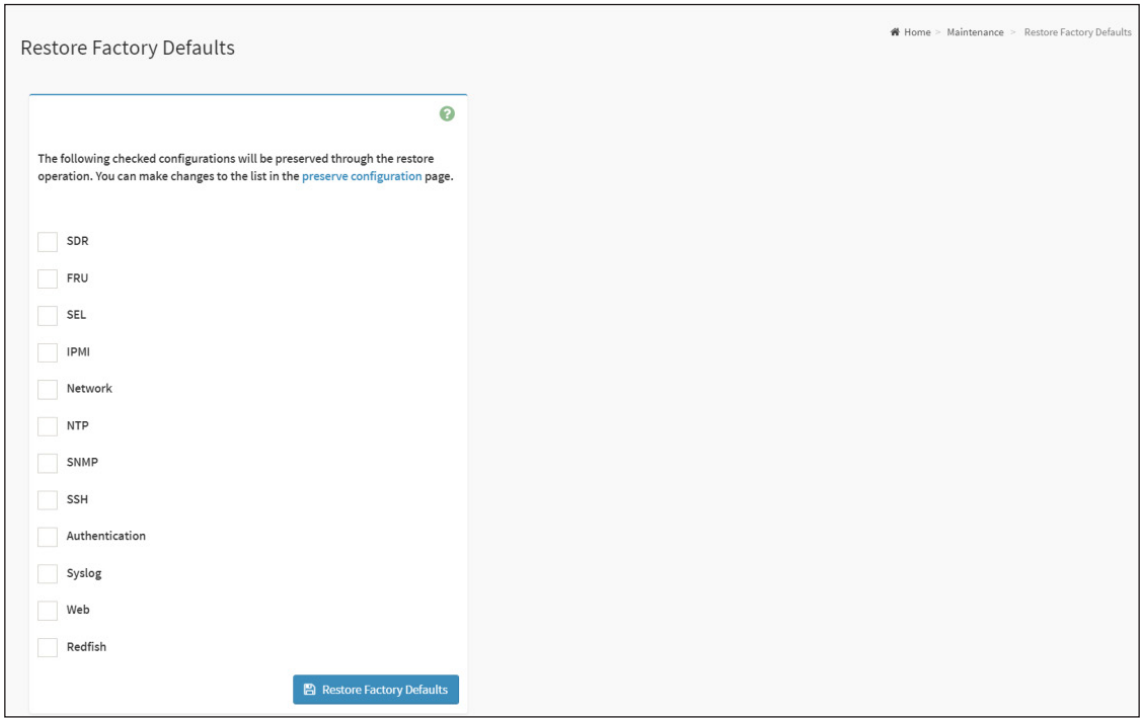
3. Click OK to upload the new configuration file and restore.

5.14.6 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

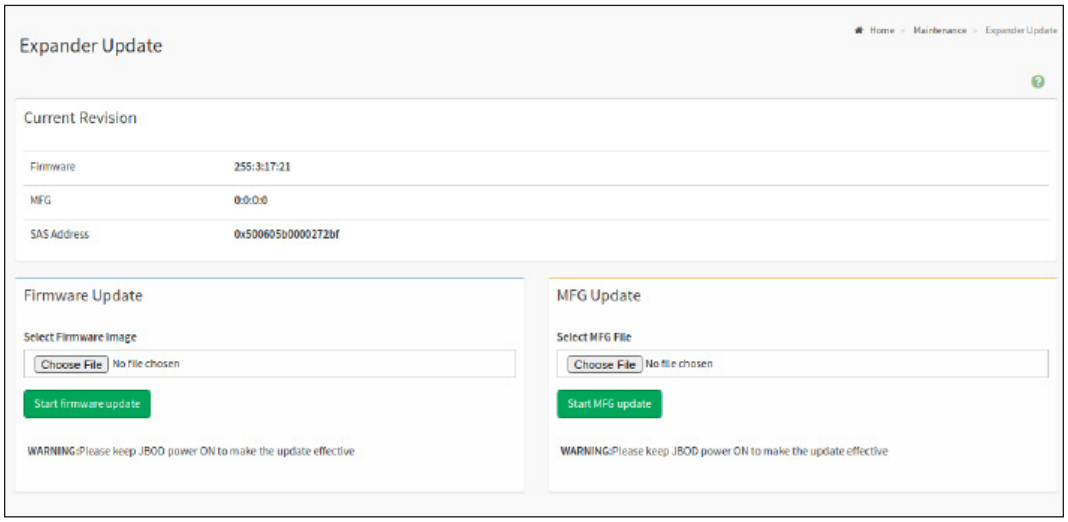
1. Click Preserve Configuration to redirect to **Preserve Configuration** page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click Restore Factory Defaults to restore the factory defaults of the device firmware.

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.

5.14.7 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

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

Firmware Update:

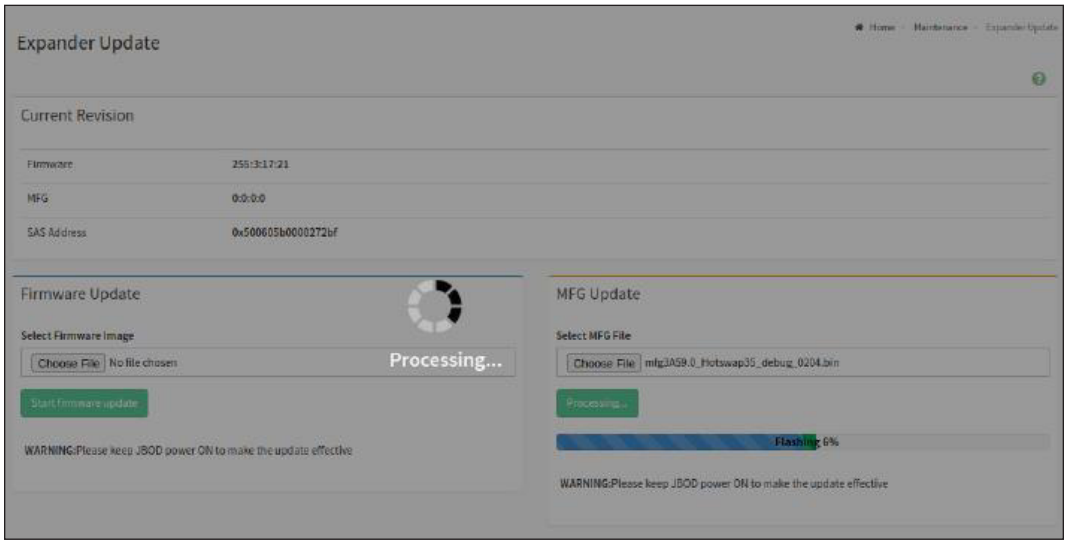
a. Click Choose File to select firmware image.

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

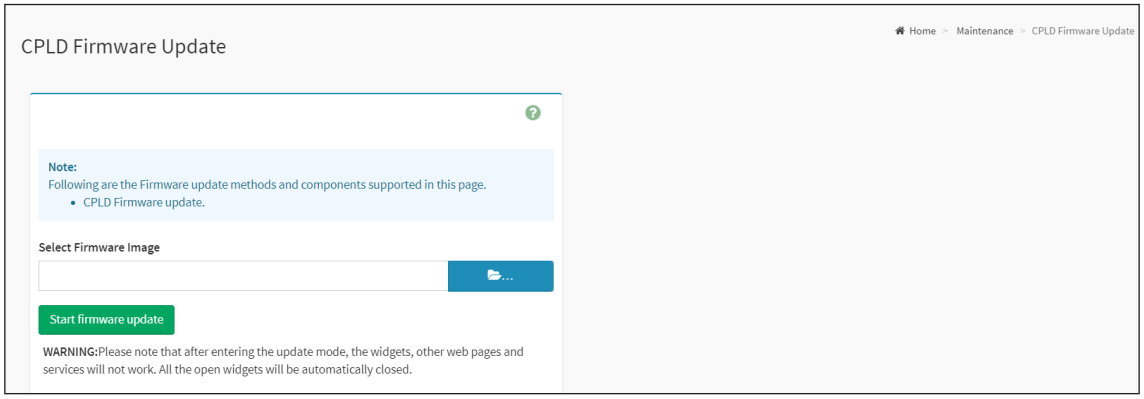


Expander Firmware Update page

5.14.8 CPLD Firmware Update

This page is used to update CPLD firmware.

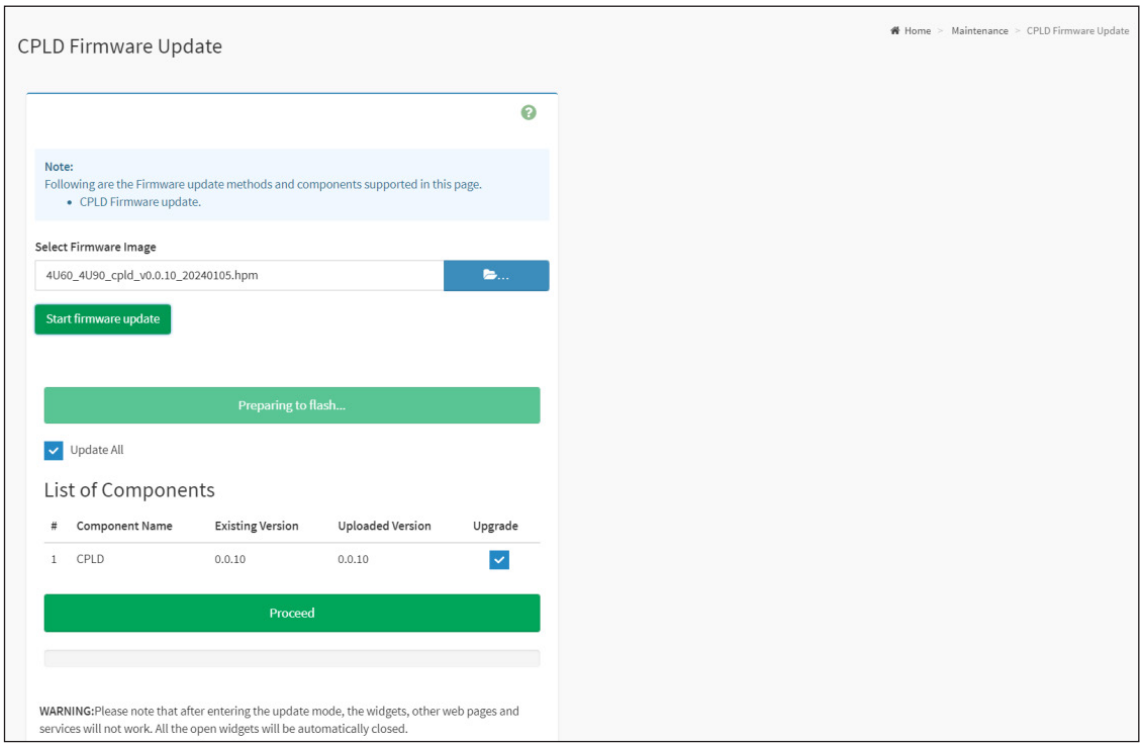
To open BMC Rest page, click Maintenance → CPLD Firmware Update from the menu bar. A sample screenshot of CPLD Firmware Update page is shown below.



CPLD Firmware Update page

Procedure for CPLD Firmware Update

1. Click Choose File to select firmware image.
2. Click Start firmware update to load the Firmware Update information

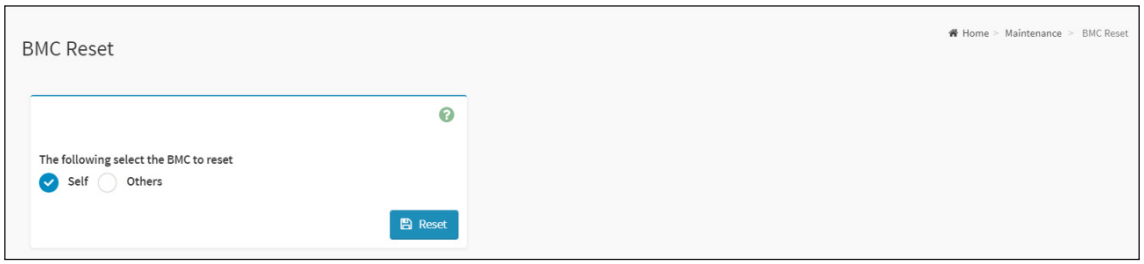


3. Check the correctness of the firmware version and click Proceed to update CPLD Firmware.

5.14.9 BMC Reset

This page is used to reset BMC firmware.

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

The various options of Power Control are given below.

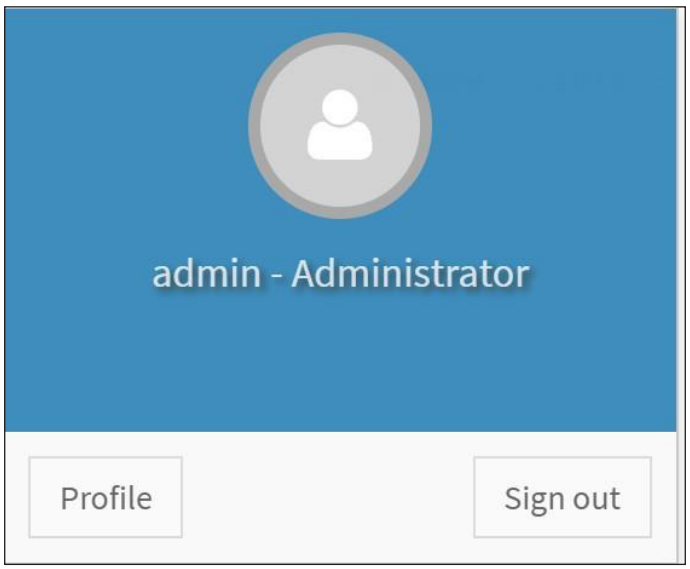
Self: activate BMC

Others: other BMC

Click **Reset** button to reset the selected BMC firmware.

5.15 Sign Out

To log out from , click the admin on the top right corner of the screen. A sample screenshot of admin option is shown below.



Sign out

Click Sign Out to perform log out. A Warning message will be prompted you to proceed further, click OK to log out or Cancel to retain the interface.

5.16 Utility & Tool

5.16.1 Flash Tools

The Flash Tools are command line utility programs used to upgrade the firmware using different medium like KCS, USB, and LAN. There are three tools, which are being used **YAFUFlash**.

5.16.1.1 YAFUFlash

Yet **Another Firmware Upgrade Flash** is a tool used for flashing the BMC. This utility is used for flashing in both Linux and Windows environment. There are three types of mediums used to flash the BMC. They are,

- Network
- USB (Not supported in this platform)
- KCS (Not supported in this platform)

All the three mediums are applicable for Windows and Linux environment. But only KCS medium can be used in DOS 1.2. environment. The medium can be selected as per your requirement.

NOTE

YAFU based firmware update using Signed Hashed image is only possible if enough RAM is available to upload the full firmware image before the update starts.

In YAFU firmware upgrade, only YAFU command set is allowed if **Enable IPMI Command handling during flashing** support is disabled in project configuration.

YAFU flashing process has the following timeout values

LAN interface: 3600 seconds

USB interface: 1800 seconds

KCS interface: 5400 seconds

If Secure Boot Support is enabled in the PRJ, YAFUFlash options for Section Based Flashing or Interactive mode will not be used. Hence any feature or options that rely on Section Based Flashing or Interactive mode cannot be used when Secure Boot Support is enabled.

5.16.1.2 Installation in Windows

1. Open the command prompt in administrator mode and enter YafuFlash\Windows path.
2. This contains two files, **Yafuflash.exe** and **LIBIPMI.dll**.
3. Format: **Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE]**, where Perform BMC Flash Update
   - -? Displays the utility usage
   - -h Displays the utility usage
   - -V Displays the version of the tool
   - -e List outs a few examples of the tool

[OPTIONS]

-info	Displays information about existing FW and new FW.
-msi,-img-section-info	Displays information about current FW Sections.
-mi,-img-info	Displays information about current FW Versions.
- fb, -force-boot	Option to FORCE BootLoader upgrade during full upgrade. Also, skips user interaction in Interactive upgrade mode. This option is not allowed with Interactive upgrade option.
- pc, -preserve-config	Option to preserve Config Module during full upgrade. If platform supports Dual Image, this option skips user interaction, preserves config and continues update process. This option is not allowed with interactive upgrade option.
-q, -quite	Use the option to show the minimum flash progress details.
- i	Option to interactive upgrade (Upgrade only required modules)**
-f, -full	Performs full upgrade in Interactive Upgrade mode. Skips module wise upgrade
- ipc, -ignore-platform-check	If this image is for a different platform, this option skips user interaction and continues update process.
-idi,-ignore-diff-image	If this image differs from the currently programmed image, this option skips user interaction and continues update process.
-isi, -ignore-same-image	If this image is same as the currently programmed image, this option skips user interaction and continues update process.
-iml, -ignore-module-location	If module(s) of this image is/are in different locations, this option skips user interaction and continues update process.
-ibv, -ignore-boot-version	If bootloader version is different and -force-boot is not specified, this option skips user interaction and continues update process. The bootloader will be updated.
-iri, -ignore –reselect-image	Option skips reselecting the active image.

-inc, -ignore-non-preserve-config	Option skips the restore to default factor setting if the image shares the same configuration area.
-mse, -img-select	Option to specify the Image to be updated 0 - Inactive Image 1 - Image 1 2 - Image 2 3 - Both Images
-rp,-replace-publickey	Option to replace the Signed Image Key in Existing Firmware.
-vcf, -version-cmp-flash	Option to skip flashing modules only if the versions are same by selecting (N/n). Option (Y/y) Selects full firmware upgrade mode.
-non-interactive	This option skips user interaction. This option cannot be used along with 'ignore-diff-image', 'ignore-sameimage','-ignore- module-location'&'-ignoreboot-version' options.
-pXXX, -preserve-XXX	Option to preserve XXX configuration, where XXX falls in sdr, fru, sel, ipmi, auth, net, ntp, snmp, ssh, kvm and syslog. If the preserve status of the other configuration enabled then it will ask to confirm that those configuration is to be preserved.
-ieo, -ignore-existing-overrides	Clears the existing overrides and preserves only the overrides given in command line if any.
-msp,-split-img	Option to flash the split image.
-f -XXX, -flash-XXX	Option to flash specific section in non-interactive mode. If it is split image need to give split-image along with this option, where XXX denotes name of the section, e.g. -flash-conf.
-sc, -skip-crc	Option to skip the CRC check
-sf, -skip-fmh	Option to skip the FMH check
-d	Option to specify the peripheral(Only for Dual Image Support) <bit0> - BMC <bit1> - BIOS <bit2> - CPLD <BIT4> - ME
-a, -activate	Option to activate peripheral devices <BIT0> - BMC <BIT1> - BIOS <BIT2> - CPLD
-nr, -no-reboot	Option to skip the reboot. With online-flash support, if conf/ extlog is not preserved, BMC will still reboot.
-bu, -block-upgrade	Option to Flash using Block by Block method
-netfn <NETFN>	Option to specify AMI OEM Net Function (default 0x32)

[MEDIUM]

-cd	Option to use USB Medium
-nw,-ip,-u,-p,-host, _p	Option to use Network Medium: '-ip' Option to enter IP, when using Network Medium '-host' Option to enter host name, when using Network Medium. '-u' Option to enter UserName, when using Network Medium. '-p' Option to enter Password, when using Network Medium. '_p' Option to enter Port Number.
-kcs	Option to use KCS medium.
Option to use KCS medium.	Option to use serial interface.
-term	Option to use serial command, e.g. /dev/ttyS0.
-baudrate	Option to use baudrate of the serial terminal, e.g. 115200.

[FW_IMAGE_FILE] Firmware image file name [rom.ima].

-pe,-preserve-extlog	Option to preserve extlog configuration during firmware flash.

NOTE
'-preserve-config' and '-force-boot' option not be used in interactive upgrade.

Examples for Network Medium

Eg1:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima -info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of both existing firmware and new firmware.

Eg2:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware.

Eg3:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –force-boot
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –preserve-config
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with preserve config params.

Eg5:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –force-boot
-preserve-config
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg6:

```
./Yafuflash –nw –host spxbmc –force-boot –preserve-config rom.ima
```

Description: This command works with network medium using the host name spxbmc, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg7:

```
./Yafuflash –nw –ip 2000::2005 –force-boot rom.ima
```

Description: This command works with network medium using the ipv6 address 2000::2005, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg8:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima -i
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima using interactive upgrade mode and user will be prompt to select the Number of modules and module names to upgrade.

Eg9:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin -img-section-info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg10:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin -img-info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of existing firmware Version.

Eg11:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin public.pem –replace-publickey
```

Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in firmware.

Eg12:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-sdr
```

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg13:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-snmp -preserve-ntp
```

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg14:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -ignore-existing-overrides
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg15:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -preserve-snmp -ignore-existingoverrides
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg16:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-reselect-image
```

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg17:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-non-preserveconfig
```

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg18:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 0 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg19:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 1 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg20:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 2 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg21:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 3 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg22:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima -quite
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima with minimum progress details.

Eg23:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –split-img boot.ima
```

Description: This command works with network medium to flash the boot split image.

Eg24:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin –split-img root.ima
```

Description: This command works with network medium to flash the root split image.

Eg25:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin rom.ima –flash-root –flash-conf
```

Description: This command works with network medium to flash root and conf section from rom. ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg26:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin boot.ima -split-img –flash-boot
```

Description: This command works with network medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg27:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima -split-img –flash-www –flash-osimage
```

Description: This command works with network medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg28:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin rom.ima -preserve-extlog
```

Description: This command works with network medium to preserve extended log configuration.

Eg29:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –split-img -preserve-extlog
```

Description: This command works with network medium to preserve extended log configuration from split image.

Eg30:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –d 1 rom.ima
```

Description: This command works with network medium to flash the image on specific peripheral device.

Eg31:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –d 1 root.ima –split-img
```

Description: This command works with network medium to flash the split image on specific peripheral device.

Eg32:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin -bu root.ima.
```

Description: This command works with network medium to flash the image on specific peripheral device by block by block upgrade.

Eg33:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –netfn 0x36
```

Description: This command works with network medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

Examples for USB Medium

Power Save Mode should be disabled for Flashing with Yafu USB Interface.

Eg1:

```
./Yafuflash –cd rom.ima -info
```

Description: This command works with USB medium which displays the details of both Existing Firmware and new firmware.

Eg2:

```
./Yafuflash –cd rom.ima
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware.

Eg3:

```
./Yafuflash –cd rom.ima –force-boot
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

```
./Yafuflash –cd rom.ima –preserve-config
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

```
./Yafuflash –cd rom.ima –force-boot –preserve-config
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6:

```
./Yafuflash –cd rom.ima –i
```

Description: This command works with USB medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the number of modules and module names to upgrade.

Eg7:

```
./Yafuflash –cd -img-section-info
```

Description: This command works with USB medium which displays the details of Existing Firmware.

Eg8:

```
./Yafuflash –cd -img-info
```

Description: This command works with USB medium which displays the details of Existing Firmware Version.

Eg9:

```
./Yafuflash –cd public.pem –replace-publickey
```

Description: This command works with USB medium which replaces the public key in Existing Firmware.

Eg10:

```
./Yafuflash -cd rom.ima -preserve-sel -preserve-ipmi
```

Description: This command works with USB medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

```
./Yafuflash -cd rom.ima -preserve-sel -ignore-existing-overrides
```

Description: This command works with USB medium, which start to flash the new rom. ima to the existing firmware with preserving FRU configurations only.

Eg12:

```
./Yafuflash –cd rom.ima –ignore-reselect-image
```

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

```
./Yafuflash –cd rom.ima –ignore-non-preserve-config
```

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

```
./Yafuflash -cd –img-select 0 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the active image to be flashed.

Eg15:

```
./Yafuflash -cd –img-select 1 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the first image to be flashed.

Eg16:

```
./Yafuflash -cd –img-select 2 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the second image to be flashed.

Eg17:

```
./Yafuflash -cd –img-select 3 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting both the images to be flashed.

Eg18:

```
./Yafuflash –cd rom.ima -quite
```

Description: This command works with USB medium, which start to flash the new rom. ima with minimum progress details.

Eg19:

```
./Yafuflash –cd –split-img boot.ima
```

Description: This command works with USB medium to flash the boot split image.

Eg20:

```
./Yafuflash –cd –split-img root.ima
```

Description: This command works with USB medium to flash the root split image.

Eg21:

```
./Yafuflash –cd rom.ima –flash-root –flash-conf
```

Description: This command works with USB medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg22:

```
./Yafuflash –cd boot.ima -split-img –flash-boot
```

Description: This command works with USB medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg23:

```
./Yafuflash –cd root.ima -split-img –flash-www –flash-osimage
```

Description: This command works with USB medium to flash www and osimage from root.ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg24:

```
./Yafuflash –cd rom.ima -preserve-extlog
```

Description: This command works with USB medium to preserve extended log configuration.

Eg25:

```
./Yafuflash –cd root.ima –split-img -preserve-extlog
```

Description: This command works with USB medium to preserve extended log configuration from split image.

Eg26:

```
./Yafuflash –cd root.ima –d 1 rom.ima
```

Description: This command works with USB medium to flash the image on specific peripheral device.

Eg27:

```
./Yafuflash –cd root.ima –d 1 root.ima –split-img
```

Description: This command works with USB medium to flash the split image on specific peripheral device.

Eg28:

```
./Yafuflash –cd rom.ima -netfn 0x36
```

Description: This command works with USB medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

Examples for KCS Medium

Eg1:

```
./Yafuflash –kcs rom.ima -info
```

Description: This command works with KCS medium which displays the details of both Existing Firmware and new firmware.

Eg2:

```
./Yafuflash –kcs rom.ima
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware.

Eg3:

```
./Yafuflash –kcs rom.ima –force-boot
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

```
./Yafuflash –kcs rom.ima –preserve-config
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

```
./Yafuflash –kcs rom.ima –force-boot –preserve-config
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6:

```
./Yafuflash –kcs rom.ima -i
```

Description: This command works with KCS medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the Number of modules and module names to upgrade.

Eg7:

```
./Yafuflash –kcs -img-section-info
```

Description: This command works with KCS medium which displays the details of Existing Firmware.

Eg8:

```
./Yafuflash –kcs -img-info
```

Description: This command works with KCS medium which displays the details of Existing Firmware Version.

Eg9:

```
./Yafuflash –kcs public.pem –replace-publickey
```

Description: This command works with KCS medium which replaces the public key in Existing Firmware.

Eg10:

```
./Yafuflash -kcs rom.ima -preserve-sel -preserve-ipmi
```

Description: This command works with KCS medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

```
./Yafuflash -kcs rom.ima -preserve-sel -ignore-existing-overrides
```

Description: This command works with KCS medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg12:

```
./Yafuflash –kcs rom.ima –ignore-reselect-image
```

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

```
./Yafuflash –kcs rom.ima –ignore-non-preserve-con
```

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

```
./Yafuflash -kcs –img-select 0 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

```
./Yafuflash -kcs –img-select 1 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

```
./Yafuflash -kcs –img-select 2 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg17:

```
./Yafuflash -kcs –img-select 3 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg18:

```
./Yafuflash –kcs rom.ima -quite
```

Description: This command works with KCS medium, which start to flash the new rom.ima with minimum progress details.

Eg19:

```
./Yafuflash –kcs –split-img boot.ima
```

Description: This command works with KCS medium to flash the boot split image.

Eg20:

```
./Yafuflash –kcs –split-img root.ima
```

Description: This command works with KCS medium to flash the root split image.

Eg21:

```
./Yafuflash –kcs rom.ima –flash-root –flash-conf
```

Description: This command works with KCS medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg22:

```
./Yafuflash –kcs boot.ima -split-img –flash-boot
```

Description: This command works with KCS medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg23:

```
./Yafuflash –kcs root.ima -split-img –flash-www –flash-osimage
```

Description: This command works with KCS medium to flash www and osimage from root.ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg24:

```
./Yafuflash –kcs rom.ima -preserve-extlog
```

Description: This command works with KCS medium to preserve extended log configuration.

Eg25:

```
./Yafuflash –kcs root.ima –split-img -preserve-extlog
```

Description: This command works with KCS medium to preserve extended log configuration from split image.

Eg26:

```
./Yafuflash –kcs root.ima –d 1 rom.ima
```

Description: This command works with KCS medium to flash the image on specific peripheral device.

Eg27:

```
./Yafuflash –kcs root.ima –d 1 root.ima –split-img
```

Description: This command works with KCS medium to flash the split image on specific peripheral device.

Eg28:

```
./Yafuflash –kcs rom.ima –netfn 0x36
```

Description: This command works with KCS medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

5.16.1.3 Installation in Linux

1. OpenSSL is pre-requisite for YafuFlash.
2. Open Terminal and go to YafuFlash/Linux path.
3. This contains Yafuflash tool.
4. Run ./Yafuflash in the terminal.
5. Format: Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE], where Perform BMC Flash Update
   - -? Displays the utility usage
   - -h Displays the utility usage
   - -V Displays the version of the tool
   - -e List outs a few examples of the tool

[OPTIONS]

-info	Displays information about existing FW and new FW.
-msi,-img-section-info	Displays information about current FW Sections.
-mi,-img-info	Displays information about current FW Versions.
- fb, -force-boot	Option to FORCE BootLoader upgrade during full upgrade. Also, skips user interaction in Interactive upgrade mode. This option is not allowed with Interactive upgrade option.
- pc, -preserve-config	Option to preserve Config Module during full upgrade. If platform supports Dual Image, this option skips user interaction, preserves config and continues update process. This option is not allowed with interactive upgrade option.
-q, -quite	Use the option to show the minimum flash progress details.
- i	Option to interactive upgrade (Upgrade only required modules)**
-f, -full	Performs full upgrade in Interactive Upgrade mode. Skips module wise upgrade
- ipc, -ignore-platform-check	If this image is for a different platform, this option skips user interaction and continues update process.
-idi,-ignore-diff-image	If this image differs from the currently programmed image, this option skips user interaction and continues update process.
-isi, -ignore-same-image	If this image is same as the currently programmed image, this option skips user interaction and continues update process.
-iml, -ignore-module-location	If module(s) of this image is/are in different locations, this option skips user interaction and continues update process.
-ibv, -ignore-boot-version	If bootloader version is different and -force-boot is not specified, this option skips user interaction and continues update process. The bootloader will be updated.
-iri, -ignore –reselect-image	Option skips reselecting the active image.

-inc, -ignore-non-preserve-config	Option skips the restore to default factor setting if the image shares the same configuration area.
-rp, -replace-publickey	Option to replace the Signed Image Key in Existing Firmware.
-vcf, -version-cmp-flash	Option to skip flashing modules only if the versions are same by selecting (N/n). Option (Y/y) Selects full firmware upgrade mode.
-non-interactive	This option skips user interaction. This option cannot be used along with 'ignore-diff-image', 'ignore-sameimage','-ignore- module-location'&'-ignoreboot-version' options.
-pXXX, -preserve-XXX	Option to preserve XXX configuration, where XXX falls in sdr, fru, sel, ipmi, auth, net, ntp, snmp, ssh, kvm and syslog. If the preserve status of the other configuration enabled then it will ask to confirm that those configuration is to be preserved.
-ieo, -ignore-existing-overrides	Clears the existing overrides and preserves only the overrides given in command line if any.
-msp,-split-img	Option to flash the split image.
-f -XXX, -flash-XXX	Option to flash specific section in non-interactive mode. If it is split image need to give split-image along with this option, where XXX denotes name of the section, e.g. -flash-conf.
-sc, -skip-crc	Option to skip the CRC check
-sf, -skip-fmh	Option to skip the FMH check
-d	Option to specify the peripheral(Only for Dual Image Support) <bit0> - BMC <bit1> - BIOS
-a, -activate	Option to activate peripheral devices <BIT0> - BMC <BIT1> - BIOS
-nr, -no-reboot	Option to skip the reboot. With online-flash support, if conf/extlog is not preserved, BMC will still reboot.
-bu, -block-upgrade	Option to Flash using Block by Block method
-netfn <NETFN>	Option to specify AMI OEM Net Function (default 0x32)

[MEDIUM]

-cd	Option to use USB Medium
-nw, -ip, -u, -p, -host, _pa	Option to use Network Medium: '-ip' Option to enter IP, when using Network Medium. '-host' Option to enter host name, When using Network Medium. '-u' Option to enter UserName, When using Network Medium. '-p' Option to enter Password, When using Network Medium. '_p' Option to enter Port Number.
-kcs	Option to use KCS medium.
-serial	Option to use serial interface.
-term	Option to use serial command, e.g. /dev/ttyS0.
-baudrate	Option to use baudrate of the serial terminal, e.g. 115200.

[FW_IMAGE_FILE] Firmware image file name [rom.ima].

-pe, -preserve-extlog	Option to preserve extlog configuration during firmware flash.

NOTE

-'preserve-config' and '-force-boot' option not be used in interactive upgrade.

*IPv6 Support is added after the tool version 2.7. IPv6 Support can be used with latest Yafuflash tool and firmware, older version of Yafuflash (and/or) firmware will not work.

**Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if it is built with Enable/Disable Interactive Upgrade YafuFlash option selected in Project Configuration file (*.PRJ) using MDS.

Examples for Network Medium

Eg1:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima -info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of both existing firmware and new firmware.

Eg2:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware.

Eg3:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –force-boot
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –preserve-config
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with preserve config params.

Eg5:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –force-boot
-preserve-config
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg6:

```
./Yafuflash –nw –host spxbmc –force-boot –preserve-config rom.ima
```

Description: This command works with network medium using the host name spxbmc, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg7:

```
./Yafuflash –nw –ip 2000::2005 –force-boot rom.ima
```

Description: This command works with network medium using the ipv6 address 2000::2005, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg8:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima -i
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima using interactive upgrade mode and user will be prompt to select the Number of modules and module names to upgrade.

Eg9:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin -img-section-info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg10:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin -img-info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of existing firmware Version.

Eg11:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin public.pem –replace-publickey
```

Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in firmware.

Eg12:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-sdr
```

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg13:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-snmp -preserve-ntp
```

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg14:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -ignore-existing-overrides
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg15:

```
./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -preserve-snmp -ignore-existingoverrides
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg16:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-reselect-image
```

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg17:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-non-preserveconfig
```

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg18:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 0 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg19:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 1 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg20:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 2 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg21:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 3 rom.ima
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg22:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima -quite
```

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima with minimum progress details.

Eg23:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –split-img boot.ima
```

Description: This command works with network medium to flash the boot split image.

Eg24:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin –split-img root.ima
```

Description: This command works with network medium to flash the root split image.

Eg25:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin rom.ima –flash-root –flash-conf
```

Description: This command works with network medium to flash root and conf section from rom. ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg26:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin boot.ima -split-img –flash-boot
```

Description: This command works with network medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg27:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima -split-img –flash-www –flash-osimage
```

Description: This command works with network medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg28:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin rom.ima -preserve-extlog
```

Description: This command works with network medium to preserve extended log configuration.

Eg29:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –split-img -preserve-extlog
```

Description: This command works with network medium to preserve extended log configuration from split image.

Eg30:

```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –d 1 rom.ima
```

Description: This command works with network medium to flash the image on specific peripheral device.

Eg31:

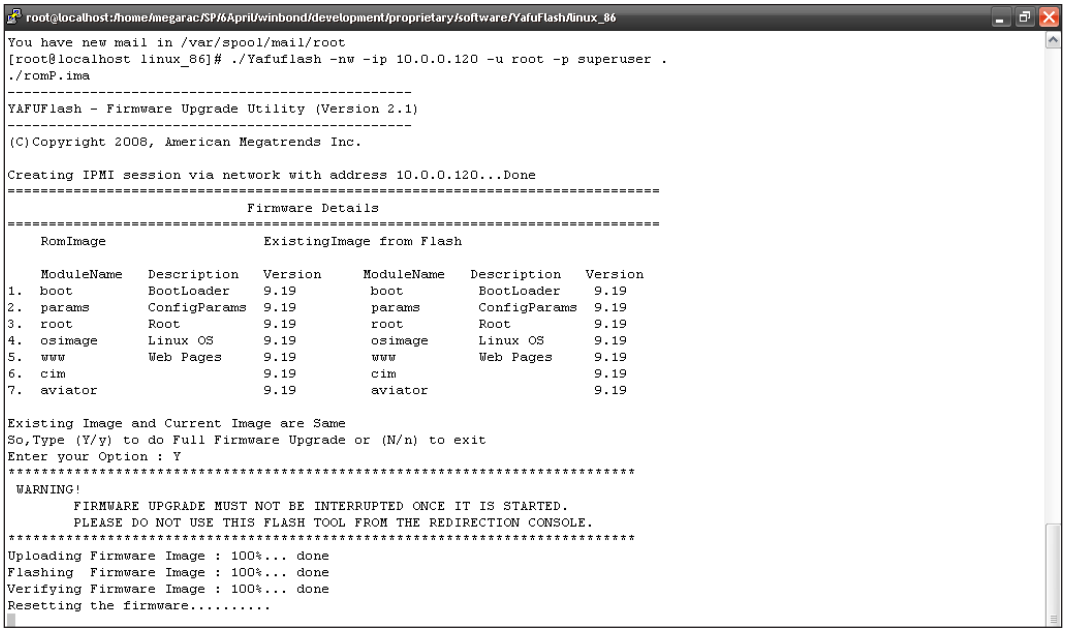
```
./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –d 1 root.ima –split-img
```

Description: This command works with network medium to flash the split image on specific peripheral device.

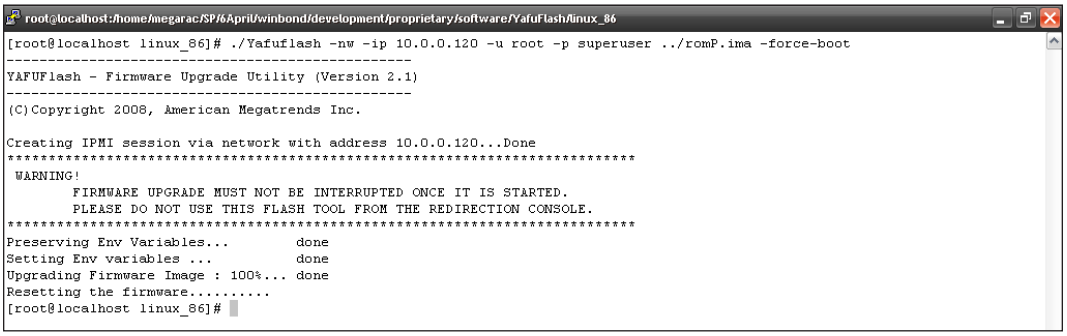
Eg32:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –netfn 0x36
```

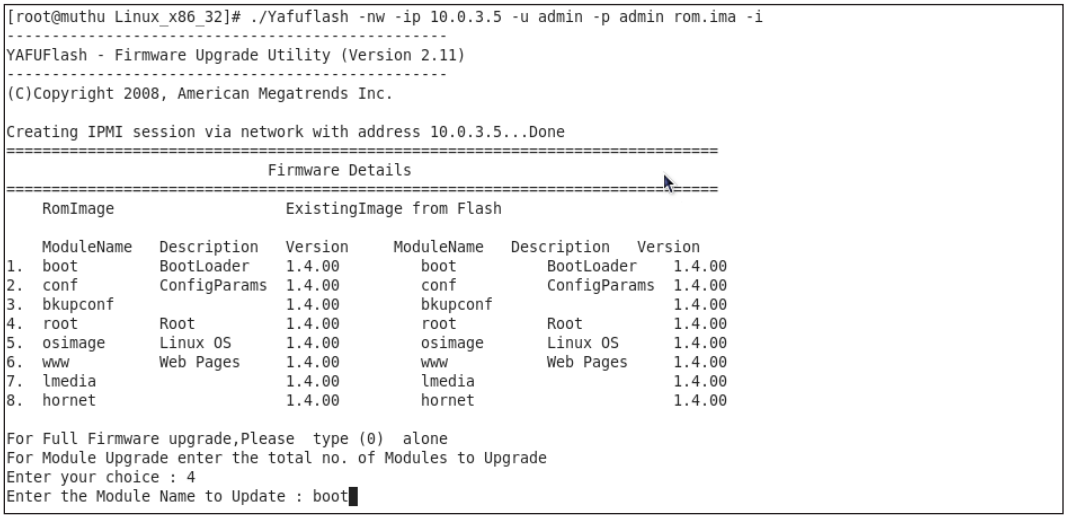
Description: This command works with network medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.



Screen: If Existing and current images are same



Existing and current are different



Interactive Upgrade Mode

Examples for USB Medium

Power Save Mode should be disabled for Flashing with Yafu USB Interface.

Eg1:

```
./Yafuflash –cd rom.ima -info
```

Description: This command works with USB medium which displays the details of both Existing Firmware and new firmware.

Eg2:

```
./Yafuflash –cd rom.ima
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware.

Eg3:

```
./Yafuflash –cd rom.ima –force-boot
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

```
./Yafuflash –cd rom.ima –preserve-config
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

```
./Yafuflash –cd rom.ima –force-boot –preserve-config
```

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6:

```
./Yafuflash –cd rom.ima –i
```

Description: This command works with USB medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the number of modules and module names to upgrade.

Eg7:

```
./Yafuflash –cd -img-section-info
```

Description: This command works with USB medium which displays the details of Existing Firmware.

Eg8:

```
./Yafuflash –cd -img-info
```

Description: This command works with USB medium which displays the details of Existing Firmware Version.

Eg9:

```
./Yafuflash –cd public.pem –replace-publickey
```

Description: This command works with USB medium which replaces the public key in Existing Firmware.

Eg10:

```
./Yafuflash -cd rom.ima -preserve-sel -preserve-ipmi
```

Description: This command works with USB medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

```
./Yafuflash -cd rom.ima -preserve-sel -ignore-existing-overrides
```

Description: This command works with USB medium, which start to flash the new rom. ima to the existing firmware with preserving FRU configurations only.

Eg12:

```
./Yafuflash –cd rom.ima –ignore-reselect-image
```

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

```
./Yafuflash –cd rom.ima –ignore-non-preserve-config
```

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

```
./Yafuflash -cd –img-select 0 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the active image to be flashed.

Eg15:

```
./Yafuflash -cd –img-select 1 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the first image to be flashed.

Eg16:

```
./Yafuflash -cd –img-select 2 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the second image to be flashed.

Eg17:

```
./Yafuflash -cd –img-select 3 rom.ima
```

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting both the images to be flashed.

Eg18:

```
./Yafuflash –cd rom.ima -quite
```

Description: This command works with USB medium, which start to flash the new rom. ima with minimum progress details.

Eg19:

```
./Yafuflash –cd –split-img boot.ima
```

Description: This command works with USB medium to flash the boot split image.

Eg20:

```
./Yafuflash –cd –split-img root.ima
```

Description: This command works with USB medium to flash the root split image.

Eg21:

```
./Yafuflash –cd –split-img root.ima
```

Description: This command works with USB medium to flash the root split image.

Eg22:

```
./Yafuflash –cd rom.ima –flash-root –flash-conf
```

Description: This command works with USB medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg23:

```
./Yafuflash –cd boot.ima -split-img –flash-boot
```

Description: This command works with USB medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg24:

```
./Yafuflash –cd root.ima -split-img –flash-www –flash-osimage
```

Description: This command works with USB medium to flash www and osimage from root.ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg25:

```
./Yafuflash –cd rom.ima -preserve-extlog
```

Description: This command works with USB medium to preserve extended log configuration.

Eg26:

```
./Yafuflash –cd root.ima –split-img -preserve-extlog
```

Description: This command works with USB medium to preserve extended log configuration from split image.

Eg27:

```
./Yafuflash –cd root.ima –d 1 rom.ima
```

Description: This command works with USB medium to flash the image on specific peripheral device.

Eg28:

```
./Yafuflash –cd root.ima –d 1 root.ima –split-img
```

Description: This command works with USB medium to flash the split image on specific peripheral device.

Eg29:

```
./Yafuflash –cd rom.ima –netfn 0x36
```

Description: This command works with USB medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

Examples for KCS Medium

Eg1:

```
./Yafuflash –kcs rom.ima –info
```

Description: This command works with KCS medium which displays the details of both Existing Firmware and new firmware.

Eg2:

```
./Yafuflash –kcs rom.ima
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware.

Eg3:

```
./Yafuflash –kcs rom.ima –force-boot
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

```
./Yafuflash –kcs rom.ima –preserve-config
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

```
./Yafuflash –kcs rom.ima –force-boot –preserve-config
```

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6:

```
./Yafuflash –kcs rom.ima -i
```

Description: This command works with KCS medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the Number of modules and module names to upgrade.

Eg7:

```
./Yafuflash –kcs -img-section-info
```

Description: This command works with KCS medium which displays the details of Existing Firmware.

Eg8:

```
./Yafuflash –kcs -img-info
```

Description: This command works with KCS medium which displays the details of Existing Firmware Version.

Eg9:

```
./Yafuflash –kcs public.pem –replace-publickey
```

Description: This command works with KCS medium which replaces the public key in Existing Firmware.

Eg10:

```
./Yafuflash -kcs rom.ima -preserve-sel -preserve-ipmi
```

Description: This command works with KCS medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

```
./Yafuflash -kcs rom.ima -preserve-sel -ignore-existing-overrides
```

Description: This command works with KCS medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg12:

```
./Yafuflash –kcs rom.ima –ignore-reselect-image
```

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

```
./Yafuflash –kcs rom.ima –ignore-non-preserve-con
```

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

```
./Yafuflash -kcs –img-select 0 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

```
./Yafuflash -kcs –img-select 1 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-section-info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg17:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-info
```

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware Version.

Eg18:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin public.pem –replace-publickey
```

Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in Existing Firmware.

Eg19:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-sdr
```

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg20:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-snmp –preserve-ntp
```

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg21:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-fru –ignore-existing-overrides
```

Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg22:

```
./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-fru –preserve-snmp –ignore-existing -overrides
```

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg23:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-reselect-image
```

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg24:

```
./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-non-preserve-config
```

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg25:

```
./Yafuflash –kcs –img-select 2 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg26:

```
./Yafuflash –kcs –img-select 3 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg27:

```
./Yafuflash –kcs rom.ima -quite
```

Description: This command works with KCS medium, which start to flash the new rom. ima with minimum progress details.

Eg28:

```
./Yafuflash –kcs –split-img boot.ima
```

Description: This command works with KCS medium to flash the boot split image.

Eg29:

```
./Yafuflash –kcs –split-img root.ima
```

Description: This command works with KCS medium to flash the root split image.

Eg30:

```
./Yafuflash –kcs rom.ima –flash-root –flash-conf
```

Description: This command works with KCS medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg31:

```
./Yafuflash –kcs boot.ima –split-img –flash-boot
```

Description: This command works with KCS medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg32:

```
./Yafuflash –kcs root.ima –split-img –flash-www –flash-osimage
```

Description: This command works with KCS medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg33:

```
./Yafuflash –kcs rom.ima –preserve-extlog
```

Description: This command works with KCS medium to preserve extended log configuration.

Eg34:

```
./Yafuflash –kcs root.ima –split-img –preserve-extlog
```

Description: This command works with KCS medium to preserve extended log configuration from split image.

Eg35:

```
./Yafuflash –kcs root.ima –d 1 rom.ima
```

Description: This command works with KCS medium to flash the image on specific peripheral device.

Eg36:

```
./Yafuflash –kcs root.ima –d 1 root.ima –split-img
```

Description: This command works with KCS medium to flash the split image on specific peripheral device.

Eg37:

```
./Yafuflash –kcs rom.ima –netfn 0x36
```

Description: This command works with KCS medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

5.16.1.4 YAFUFlash OS Compatibility

KCS/USB	LAN
Windows Server 2012	Ubuntu 16.04
Windows Server 2008	Windows 8.1
Windows Server 2016 Standard (Exclude Nano Server)	Ubuntu 14.04
Ubuntu Server 16.04	Windows 10
Ubuntu Server 14.04	Fedora 24
RHEL 7.2	
RHEL 6.5	
SLES Server 12.1	
SLES Server 11.4	

5.16.1.5 Installation in DOS

1. Copy **Yafuflash.exe** into DOS machine.
2. Run **Yafuflash** utility.
3. Format: **Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE]** where, Perform BMC Flash Update.
   - -? Displays the utility usage
   - -h Displays the utility usage
   - -V Displays the version of the tool
   - -e List outs a few examples of the tool

[OPTIONS]

-info	Displays information about existing FW and new FW.
-msi,-img-section-info	Displays information about current FW Sections.
-mi,-img-info	Displays information about current FW Versions.
- fb, -force-boot	Option to FORCE BootLoader upgrade during full upgrade. Also, skips user interaction in Interactive upgrade mode. This option is not allowed with Interactive upgrade option.
- pc, -preserve-config	Option to preserve Config Module during full upgrade. If platform supports Dual Image, this option skips user interaction, preserves config and continues update process. This option is not allowed with interactive upgrade option.
-q, -quite	Use the option to show the minimum flash progress details.
- i	Option to interactive upgrade (Upgrade only required modules)**
-f, -full	Performs full upgrade in Interactive Upgrade mode. Skips module wise upgrade
- ipc, -ignore-platform-check	If this image is for a different platform, this option skips user interaction and continues update process.
-idi,-ignore-diff-image	If this image differs from the currently programmed image, this option skips user interaction and continues update process.
-isi, -ignore-same-image	If this image is same as the currently programmed image, this option skips user interaction and continues update process.
-iml, -ignore-module-location	If module(s) of this image is/are in different locations, this option skips user interaction and continues update process.
-ibv, -ignore-boot-version	If bootloader version is different and -force-boot is not specified, this option skips user interaction and continues update process. The bootloader will be updated.
-iri, -ignore –reselect-image	Option skips reselecting the active image.
-inc, -ignore-non-preserve-config	Option skips the restore to default factor setting if the image shares the same configuration area.
-rp, -replace-publickey	Option to replace the Signed Image Key in Existing Firmware.
-vcf, -version-cmp-flash	Option to skip flashing modules only if the versions are same by selecting (N/n). Option (Y/y) Selects full firmware upgrade mode.
-non-interactive	This option skips user interaction. This option cannot be used along with ‘ignore-diff-image’, ‘ignore-same- image’,‘-ignore-module-location’&‘- ignore- boot-version’ options.
-pXXX, -preserve-XXX	Option to preserve XXX configuration, where XXX falls in sdr, fru, sel, ipmi, auth, net, ntp, snmp, ssh, kvm and syslog. If the preserve status of the other configuration enabled then it will ask for the other configuration to be preserved.

-ieo, -ignore-existing-overrides	Clears the existing overrides and preserves only the overrides given in command line if any.
-msp, -split-img	Option to flash the split image.
-f -XXX, -flash-XXX	Option to flash specific section in non-interactive mode. If it is split image need to give split-image along with this option, where XXX denotes name of the section, e.g. -flash-conf.
-sc, -skip-crc	Option to skip the CRC check
-sf, -skip-fmh	Option to skip the FMH check
-d	Option to specify the peripheral(Only for Dual Image Support) <bit0> - BMC <bit1> - BIOS
-a, -activate	Option to activate peripheral devices <BIT0> - BMC <BIT1> - BIOS
-nr, -no-reboot	Option to skip the reboot. With online-flash support, if conf/ extlog is not preserved, BMC will still reboot.
-bu, -block-upgrade	Option to Flash using Block by Block method
-netfn <NETFN>	Option to specify AMI OEM Net Function (default 0x32)

[MEDIUM]

-cd	Option to use USB Medium
-nw, -ip, -u, -p, -host, _p	Option to use Network Medium: '-ip' Option to enter IP, when using Network. '-host' Option to enter host name, When using Network Medium. '-u' Option to enter UserName, When using Network Medium. '-p' Option to enter Password, When using Network Medium. '_p' Option to enter Port Number.
-kcs	Option to use KCS medium.

[FW_IMAGE_FILE] Firmware image file name [rom.ima].

-pe, -preserve-extlog	Option to preserve extlog configuration during firmware flash.

Firmware image file name [rom.ima].

**Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if it is built with Enable/Disable Interactive Upgrade YafuFlash option selected in Project Configuration file (*.PRJ) using MDS.

Examples

Eg1:

```
Yafuflash –kcs –info rom.ima
```

Description: Displays the details of both Existing Firmware and new firmware.

Eg2:

```
Yafuflash –kcs rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware.

Eg3:

```
Yafuflash –kcs –force-boot rom.ima
```

Description: This command starts to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.

Eg4:

```
Yafuflash –kcs –preserve-config rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

```
Yafuflash –kcs –force-boot –preserve-config rom.ima
```

Description: This command starts to flash the new rom.ima to the firmware with FORCE BootLoader upgrade and preserving config params.

Eg6:

```
Yafuflash –kcs –i rom.ima
```

Description: This command starts to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the number of modules and module names to upgrade.

Eg7:

```
Yafuflash –kcs –img-section-info
```

Description: Displays the details of Existing Firmware.

Eg8:

```
Yafuflash –kcs –img-info
```

Description: Displays the details of Existing Firmware Version.

Eg9:

```
Yafuflash –kcs public.pem –replace-publickey
```

Description: Replaces the public key in Existing Firmware.

Eg10:

```
Yafuflash –kcs rom.ima –preserve-sdr
```

Description: This command will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg11:

```
Yafuflash –kcs rom.ima –preserve-snmp –preserve-ntp
```

Description: This command will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg12:

```
Yafuflash –kcs rom.ima –preserve-fru –ignore-existing-overrides
```

Description: This command starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg13:

```
Yafuflash –kcs rom.ima –preserve-fru –preserve-snmp –ignore-existing-overrides
```

Description: This command starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg14:

```
Yafuflash –kcs –img-select 0 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

```
Yafuflash –kcs –img-select 1 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

```
Yafuflash –kcs –img-select 2 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg17:

```
Yafuflash –kcs –img-select 3 rom.ima
```

Description: This command starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg18:

```
Yafuflash –kcs –split-img boot.ima
```

Description: This command works with KCS medium to flash the boot split image.

Eg19:

```
Yafuflash –ksc –split-img root.ima
```

Description: This command works with KCS medium to flash the root split image.

Eg20:

```
Yafuflash –ksc rom.ima –flash-root –flash-conf
```

Description: This command works with KCS medium to flash the root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom. ima.

Eg21:

```
Yafuflash –ksc boot.ima –split-img –flash-boot
```

Description: This command works with KCS medium to flash the root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg22:

```
Yafuflash –ksc root.ima –split-img –flash-www –flash-osimage
```

Description: This command works with KCS medium to flash www and osimage from root. ima split image. --flash-<xxx>, where xxx specifies the modules in root.ima.

Eg23:

```
Yafuflash –ksc rom.ima –preserve-exlog
```

Description: This command works with KCS medium to preserve extended log configuration.

Eg24:

```
Yafuflash –ksc root.ima –split-img –preserve-exlog
```

Description: This command works with KCS medium to preserve extended log configuration from split image.

Eg25:

```
Yafuflash –ksc root.ima –d 1 rom.ima
```

Description: This command works with KCS medium to flash the image on specific peripheral device.

Eg26:

```
Yafuflash –ksc root.ima –d 1 root.ima –split-img
```

Description: This command works with KCS medium to flash the split image on specific peripheral device.

Eg27:

```
Yafuflash –nw–ip 155.166.132.12 –u admin –p admin -bu root.ima.
```

Description: This command works with network medium to flash the image on specific peripheral device by block by block upgrade.

Eg28:

```
Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –netfn 0x36
```

Description: This command works with network medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32

5.17 SOL (Serial Over LAN)

One of the powerful tools in IPMI is Serial Over LAN (SOL) which provides serial line access over the management LAN. The baseboard management controller (BMC) microcontroller embedded on the server motherboard does this by redirecting information destined for the serial port over to the LAN. With SOL console redirection system administrators can remotely view the text-based console on their remote servers from anywhere and perform any task that doesn't require a GUI.

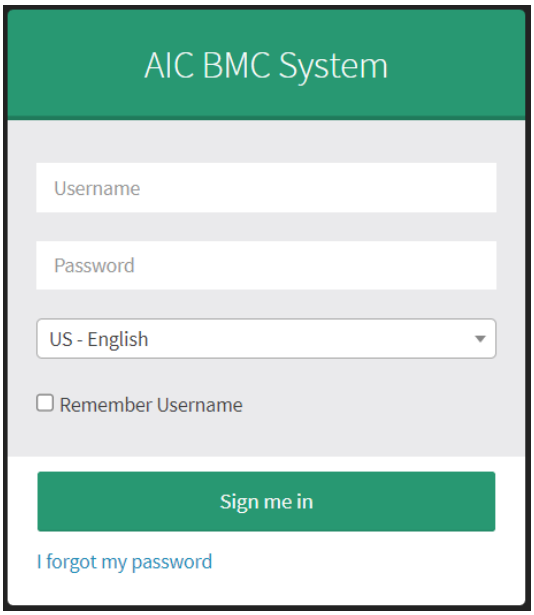
Transporting serial data over IP networks using telnet, serial over IP, SOL and the likes is the way forward for server serial communications. Just as the KVM functions in embedded service processors is displacing the need for external KVM appliances, so the SOL capability of BMCs and console redirection in service processors is reducing the need for serial console servers for server console management.

5.18 OTP (One Time Password)

OTP Support for Password Reset

OTP mechanism is used to generate temporary password. Forgot Password option in Log-in page Web UI can be used to generate OTP which will be sent to already configured e-mail ID. This generated temporary password will be valid for only 5 minutes.

Initial access of Web UI 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. For example, if browser language is configured with Simplified Chinese language (ZH-CN), then option value will be auto selected as China - .

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.

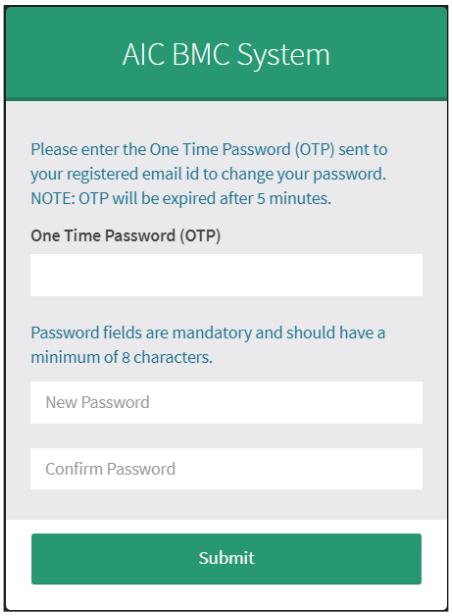
Remember Username: Check this option to remember your login Username. If you select this option, the browser will save your credentials internally in its memory, and when you open that site the next time, it will auto-fill Username for you.

Sign me in: After entering the required credentials, click the Sign me in to login to MegaRAC GUI.

I Forgot my Password: If you forget your password, you can generate a new password using this link.

Procedure to Reset Password

1. Enter the **Username**, and click on **Forgot Password** link. A pop-up message will prompt you to proceed further, click **OK** to proceed.



Forgot Password Page

2. Enter **One Time Password (OTP)** sent to your registered Email-ID for changing the password, and click **Submit**.

> **NOTE**
> OTP will be expired after 5 minutes.

3. Enter a password in the New Password and Confirm Password fields, and click Submit.
4. Once all the above steps are success, your password will be reset.

> **NOTE**
> - Default password should contain minimum of 8 and maximum of 16 alphanumeric characters.
> - White space is not allowed.

Chapter 6. Technical Support

www.aicipc.com

Taiwain, 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.

Appendix

Ports Usage

Port #	Owner Module	Usage
80	Web server(lighttpd)	Listening for network connections on HTTP://
443	Web server(lighttpd)	Listening for secured network connections on HTTPS://
22	SSH	SSH session
623	**IPMI**	**LAN interface**
123	NTP	Network Time Protocol (NTP) - used for time synchronization (UDP Connection)
161	SNMP	SNMP listens on this port for incoming SNMP requests. (UDP)
546	DHCPv6	DHCPv6 clients listen for DHCP messages on this port (UDP)