

ISB-W890

User's Manual

CEB Motherboard with Intel® W890 Chipset for
Intel® XEON™ 600 Series workstation Processors



Manual Rev.:	0.8 Preliminary
Revision Date:	June 15, 2026
Part Number:	50M-31903-1000

Preface

Copyright

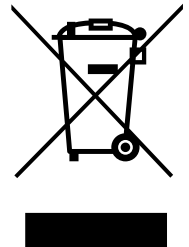
Copyright 2026 ADLINK Technology, Inc. This document contains proprietary information protected by copyright. All rights are reserved. No part of this manual may be reproduced by any mechanical, electronic, or other means in any form without prior written permission of the manufacturer.

Disclaimer

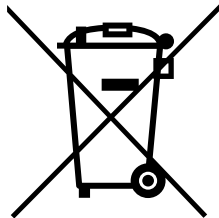
The information in this document is subject to change without prior notice in order to improve reliability, design, and function and does not represent a commitment on the part of the manufacturer. In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages.

Environmental Responsibility

ADLINK is committed to fulfill its social responsibility to global environmental preservation through compliance with the European Union's Restriction of Hazardous Substances (RoHS) directive and Waste Electrical and Electronic Equipment (WEEE) directive. Environmental protection is a top priority for ADLINK. We have enforced measures to ensure that our products, manufacturing processes, components, and raw materials have as little impact on the environment as possible. When products are at their end of life, our customers are encouraged to dispose of them in accordance with the product disposal and/or recovery programs prescribed by their nation or company.



Battery Labels (for products with battery)



California Proposition 65 Warning



WARNING: This product can expose you to chemicals including acrylamide, arsenic, benzene, cadmium, Tris(1,3-dichloro-2-propyl)phosphate (TDCPP), 1,4-Dioxane, formaldehyde, lead, DEHP, styrene, DINP, BBP, PVC, and vinyl materials, which are known to the State of California to cause cancer, and acrylamide, benzene, cadmium, lead, mercury, phthalates, toluene, DEHP, DIDP, DnHP, DBP, BBP, PVC, and vinyl materials, which are known to the State of California to cause birth defects or other reproductive harm. For more information go to www.P65Warnings.ca.gov.

Trademarks

Product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

Conventions

Take note of the following conventions used throughout this manual to make sure that users perform certain tasks and instructions properly.



NOTE:

Additional information, aids, and tips that help users perform tasks.



CAUTION:

Information to prevent **minor** physical injury, component damage, data loss, and/or program corruption when trying to complete a task.



WARNING:

Information to prevent **serious** physical injury, component damage, data loss, and/or program corruption when trying to complete a specific task.

Revision History

Revision	Description	Date	By
0.1	Preliminary release	2026-01-28	AL
0.2	Connector pinouts and jumper settings and specifications updated	2026-01-29	AL
0.3	BIOS settings updated	2026-02-02	AL
0.4	Specifications and block diagram updated	2026-02-05	AL
0.5	Block diagram updated	2026-02-09	AL
0.6	Connectors and jumpers settings updated	2026-02-13	AL
0.7	Mechanical layout and BIOS setup updated	2026-04-22	AL
0.8	Specifications, block diagram, and BIOS setup updated	2026-06-15	AL

Table of Contents

Preface	ii
List of Figures	vii
List of Tables	viii
1 Introduction.....	1
1.1 Features.....	1
1.2 Packing List	1
1.3 Optional Accessories	1
2 Specifications	3
3 Functional Block Diagram	5
4 Mechanical Layout	7
4.1 Mechanical Dimensions	7
4.2 Connector Locations	8
5 Connector Pinouts and Jumper Settings	9
5.1 Rear I/O Connectors	9
5.2 Onboard Headers and Connectors.....	16
5.3 Jumper and Switch Settings.....	25
5.4 Expansion Slots	29
6 Getting Started.....	43
6.1 Installing Memory Modules	43
6.2 PCIe Slot Secondary Power Supply	44
6.3 BMC LAN Configuration.....	44
6.4 BIOS Update.....	45
6.5 BMC Firmware Update via Network	45
6.6 CPLD Update.....	45
6.7 Create a RAID Volume.....	46
7 BIOS Settings.....	47
7.1 BIOS Setup Menu	47
7.2 Main Menu	48
7.3 Advanced Menu	50
7.4 Chipset Menu.....	62
7.5 Security Menu	77
7.6 Boot Menu	78
7.7 Save & Exit Menu	79
7.8 Server Management	80

7.9	View System Event Log	84
7.10	BMC User Settings	85
7.11	BMC Warm Reset	86
8	BMC	87
8.1	BMC Introduction	87
8.2	Web GUI Introduction.....	88
8.3	IPMI	139
8.4	Redfish	149
	Safety Instructions.....	180
	Consignes de Sécurité Importantes	182
	FCC Warning	184
	Getting Service.....	185

List of Figures

Figure 1: Functional block diagram.....	5
Figure 2: Mechanical dimensions	7
Figure 3: Onboard LED indicators	8
Figure 4: Jumper and switch locations	25
Figure 5: Expansion slot block diagram.....	29

List of Tables

Table 1: Motherboard layout descriptions.....	8
---	---

1 Introduction

ADLINK ISB-W890 CEB is a server/workstation motherboard supporting 6th-generation Intel® Xeon™ 600 workstation processors, the Intel® W890 chipset, and seven PCIe expansion slots, delivering a powerful edge computing solution. It features high-speed data transfer interfaces such as PCIe 5.0, USB 3.2 Gen 2, and SATA 6 Gb/s (SATA III), along with quad-channel DDR5 memory supporting up to 6400 MT/s for edge AI applications. With an abundant I/O port design, the ISB-W890 provides a significant competitive advantage for edge AI computing in terms of device compatibility, durable connectivity, and readiness for extreme environments.

1.1 Features

The main features of the ISB-W890 as follows:

- Supports a single Intel® Granite Rapids-Workstation family processor
- 8× DDR5 DIMMs, up to 6400 MT/s (4 channels, 1DPC)
- Supports up to 7 PCIe slots, including 3× PCIe x16 slots
- Supports up to 4 MCIO connectors
- Onboard VGA and DisplayPort (DP) ports
- 1× 1GbE (Intel® I210) and 1× 2.5GbE (Intel® I226); supports Wake-on-LAN (WOL) and PXE boot
- BMC with AST2600, compliant with IPMI v2.0 and Redfish
- CEB form factor: 12" × 10.5"

1.2 Packing List

- ISB-W890 CEB motherboard
- Rear I/O shield
- Front panel cable kit
- M.2 screw kit

1.3 Optional Accessories

- CPU cooler for 350W CPU (Part Number: xxx)
- CPU cooler for 200W CPU (Part Number: xxx)
- 2-port USB 2.0 cable with bracket (Part Number: 30-25010-3010)
- 2-port USB 3.0 cable with bracket (Part Number: 30-25046-0100)
- 2-port COM cable with bracket (Part Number: 30-25116-0000-A0)

This page intentionally left blank.

2 Specifications

Form Factor (CEB)	Dimensions	12" x 10.5" (305mm x 267mm)
Processor System	CPU	1x 6th Gen Intel® Granite Rapids workstation CPU, with over clocking and VROC support*1
System Memory	Supported Type	4 Channel DDR5, 8 slots DDR5 RDIMM ECC Memory speed: Up to 6400MT/S (1DPC), 5200 MT/S (2DPC)
	Max. Capacity	1TB, 128GBx 8 slot
PCIe Expansion Slots (Slot 7 nearest to CPU)	PCIe	Expert stream (128L): 3x PCIe 5.0 x16 2x PCIe 5.0 x8 2x PCIe 5.0 x4 Mainstream (80L): 2x PCIe 5.0 x16 2x PCIe 5.0 x8 2x PCIe 5.0 x4
	MCIO	4x MCIO x8 connectors*2
Storage	M.2	2x M.2 (M-Key) NVMe (2280/22110/25110)
	SlimSAS	2x SlimSAS slots from Intel W890
	SATA	8x SATA III slots, SATA RAID 0/1/5/10 supported by PCH



NOTE:

When a mainstream CPU (80 lanes) is used:

- *1 Overclocking support depends on the Intel® CPU SKU. Carrier boards for Intel® Xeon® W processors are not included.
- *2 When a mainstream CPU is used, only MCIO-1 /2(two MCIO x8 connectors) is enabled, while PCIe slot 1 (MCIO-3/4) is disabled. Installing a dual-slot GPU card will obstruct all board-edge connectors (USB, COM, VROC, etc.).

I/O	GbE	1x 1G (I210), 1x 2.5G (I226). Support Wake on LAN (WOL) and PXE boot IPMI Management LAN shared with I210
	USB	10 USB 3.0 ports 5x Type A USB 3.2 Gen2 10Gbps in rear IO 1x Type C USB 3.2 Gen2 10Gbps in rear IO 4x USB 3.2 Gen1 5Gbps through internal pin header 2x USB 2.0 ports pin header
	Serial Port	5x COM, including 1x DB-9 COM connector with RS-232/422/485 x1 in rear I/O+4x RS-232 internal pin header
	Display Port	1x D-Sub 15-pin VGA port in rear IO from AST2600 1x DP port in rear IO from AST2600
	Internal I/O Pin Header	1x TPM pin header with SPI interface 1x VROC connector 7x 4-pin Fan pin header (1 for CPU, 6 for system) 2x Chassis intrusion pin header 1x IPMC pin header (1x PMBus, 1x SMBus, 1x IPMB) 1x 24 pin ATX main PWR connector +2x8 pin ATX 12V PWR connector+ 2x8 pin in 12V PWR connector for PCIe 1x DIO pin header (4x DI, 4x DO) 1x backplane PCIe hotplug connector (Reserved) 2x SGPIO pin header (Reserved) 4x COM port pin header, 1x RS-232/422/485, 3x RS232 4x USB 3.2 Gen1 5Gbps through internal pin header 2x USB 2.0 ports pin header
	Front I/O & LED	3x button: Power button, Reset button, UID button, 7x LED: Power on/OFF LED, SATA HDD LED, Thermal alarm LED, System fault LED, 2x LAN (active), UID LED 2x USB 2.0
	Rear I/O Connector	1x VGA, 1x DP, USB 3.2 Gen2x1 (Type A) x5, USB 3.2 Gen2 (Type c) x1, 2x RJ45, 1x COM (RS-232/422/485x1), 3x Audio (Line in, out, mic) Clear CMOS reset hole

	DIO	in x4, out x4 > Pin header
	Power Requirement	• 12 V • 12 V_8P • 5 V_SB: 3.5A (Peak load: 5.2A) • 5 V • 3.3 V
Server Management	BMC Controller	ASPEED AST2600, with IPMI v2.0 & Redfish support
	TPM	TPM with header (TPM 2.0 module: 59-37610-000E)
	Watch Dog	Programmable 1 to 255 sec. (time put reset from Super I/O chip)
	Others	Wake up from USB ATX PWR: 24 Pin + 2x 8 Pin 12V + 2x8 Pin 12V for PCIe On board buzzer support On board RTC and co-design with 2-pin header 2x Chassis intrusion design
	OS	Windows® 11 LTSC (64 bit) Ubuntu 24.04 (64 bit)
	Environment	Operating: 0°C to +60°C (32°F to 140°F) Storage: -40°C to +70°C (-40°F to 158°F) Relative Humidity: 10% to 85% (long term), 5% to 90% (short term)

3 Functional Block Diagram

ISB-W890 Block Diagram

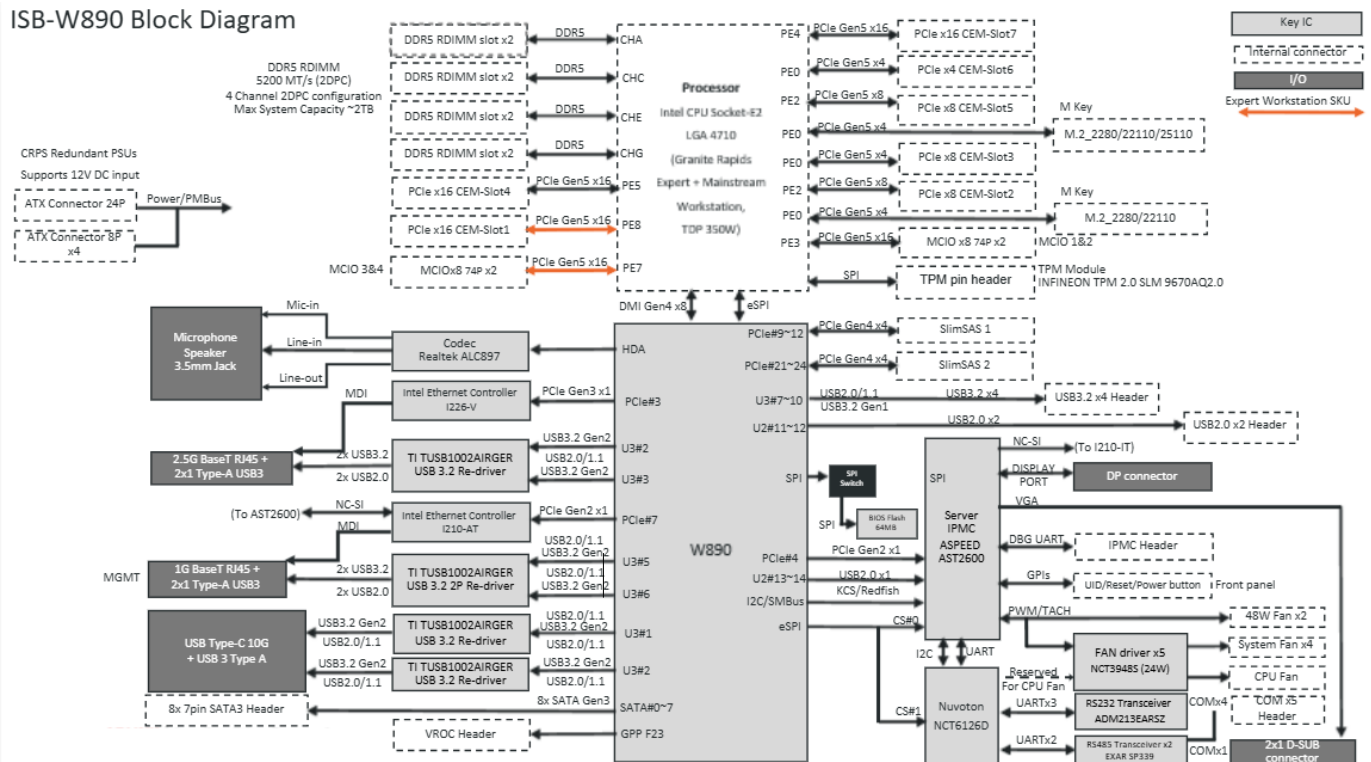


Figure 1: Functional block diagram

This page intentionally left blank.

4 Mechanical Layout

4.1 Mechanical Dimensions

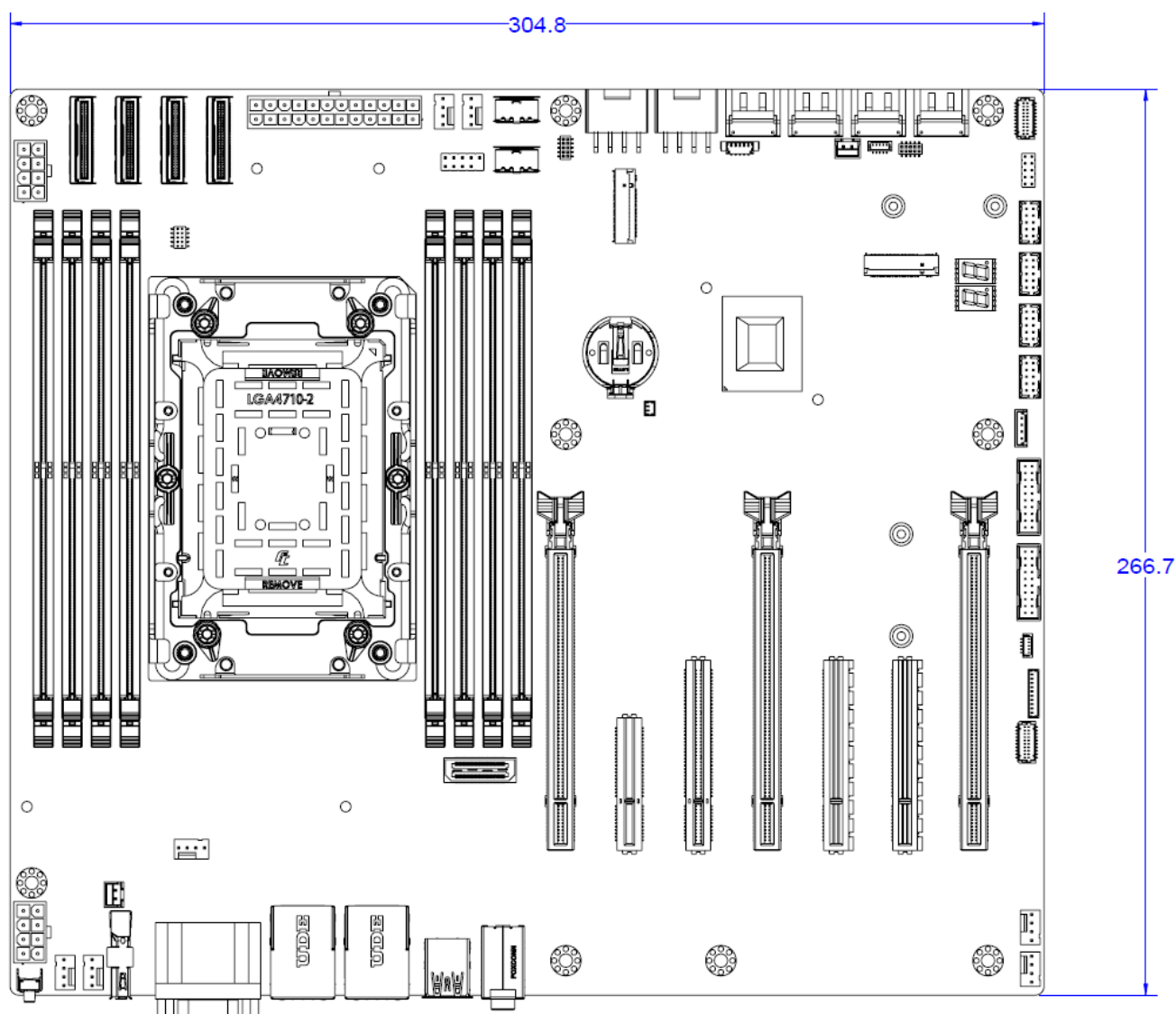


Figure 2: Mechanical dimensions

4.2 Connector Locations

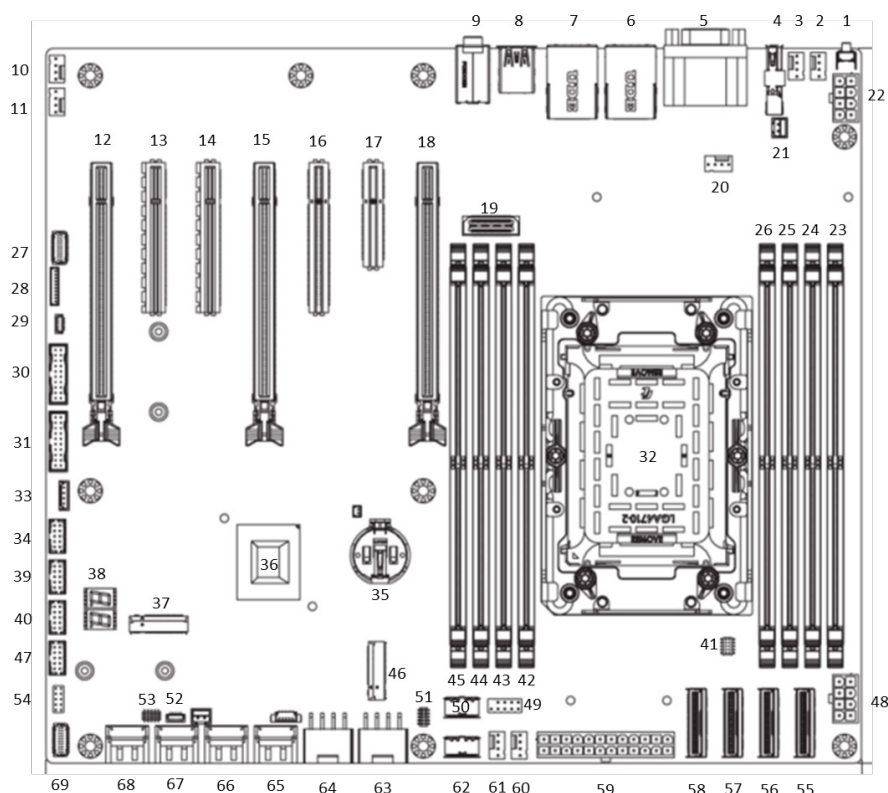


Figure 3: Onboard LED indicators

Table 1: Motherboard layout descriptions

No.	Description
1	Clear CMOS reset hole
2	System Fan
3	System Fan
4	DP connector
5	COM+VGA
6	2.5Gb LAN + USB3.2 Gen2
7	1Gb LAN+USB 3.2 Gen2
8	USB3.2 Gen2 + Type C
9	Audio
10	System Fan
11	System Fan
12	PCIe x16 (PCIE_CN1)
13	PCIe x8 (PCIE_CN2)
14	PCIe x4 with x8 connector (PCIE_CN3)
15	PCIex16 (PCIE_CN4)
16	PCIex8 (PCIE_CN5)
17	PCIex4 (PCIE_CN6)
18	PCIex16 (PCIE_CN7)
19	XDP (for debug)
20	CPU fan
21	Case open detection
22	CPU Power connector
23	DDR5 slot

No.	Description
24	DDR5 slot
25	DDR5 slot
26	DDR5 slot
27	CRPS power board header
28	DIDO header
29	IPMB header
30	USB3.2 Gen1 header
31	USB3.2 Gen1 header
32	CPU
33	VROC
34	COM port
35	CMOS battery
36	PCH-W890
37	M.2 connector
38	80 port display
39	COM port
40	COM port
41	COM port
42	DDR5 slot
43	DDR5 slot
44	DDR5 slot
45	DDR5 slot
46	M.2 connector

No.	Description
47	COM port
48	CPU Power connector
49	USB 2.0 header
50	SlimSAS
51	ESPI header
52	SMBus header
53	CPLD JTAG header
54	SGPIO header
55	MCIO connector(MCIO_CN3)
56	MCIO connector(MCIO_CN2)
57	MCIO connector(MCIO_CN4)
58	MCIO connector(MCIO_CN1)
59	ATX Power connector
60	System Fan
61	System Fan
62	SlimSAS
63	PCIe power connector
64	PCIe power connector
65	SATA III x2
66	SATA III x2
67	SATA III x2
68	SATA III x2
69	Front Panel header



NOTE:

Please ensure the correct pin definition when connecting the power cables.

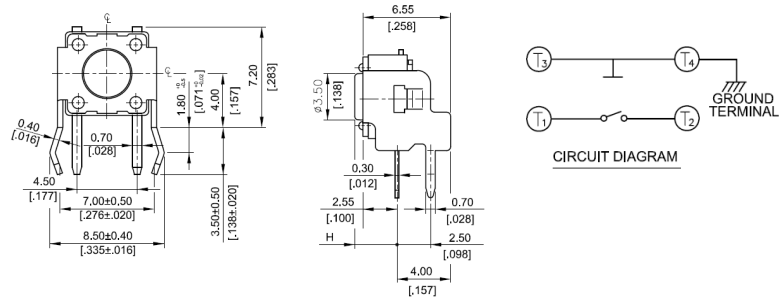
5 Connector Pinouts and Jumper Settings

5.1 Rear I/O Connectors

5.1.1 Clear CMOS Reset Button

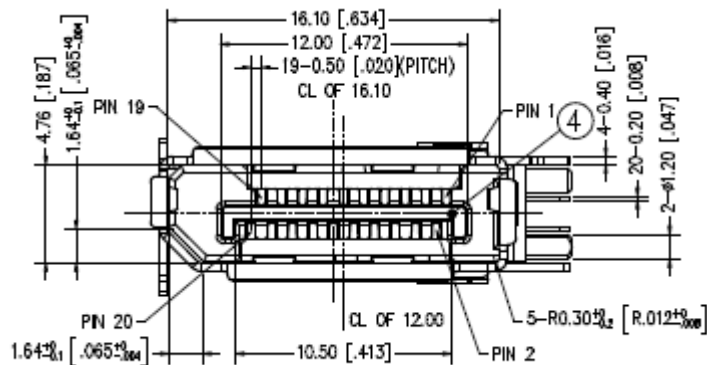
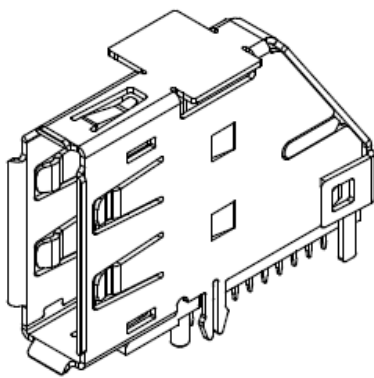
(SW2)

Signal	Pin
PCH_RTCRST-L	1
GND	2
GND	3
GND	4



5.1.2 DisplayPort Connector

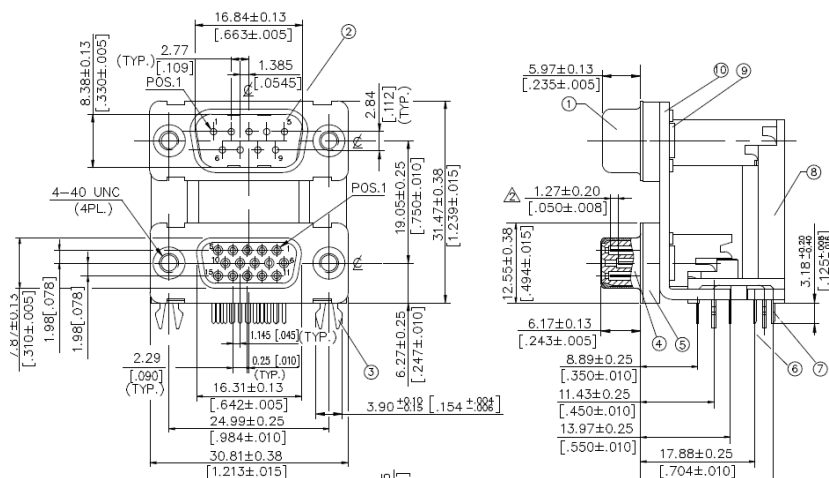
(DP_DDI1)

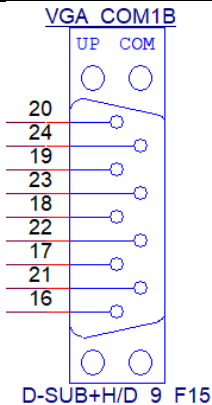


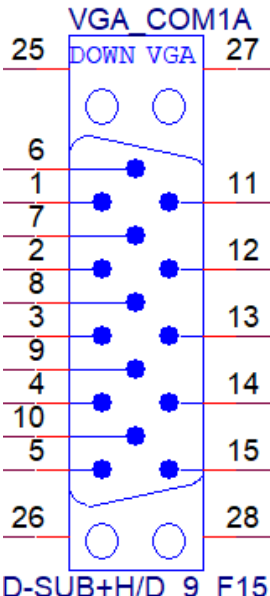
DP_DDI1		PIN#	Signal Name	PIN#	Signal Name
1	ML_LANE_0P	1	DDI2_PAIR0_P_Ch_CN	13	DP_CONN_CFG1 (1M ohm to GND)
2	GND1	2	GND	14	DP_CONN_CFG2 (1M ohm to GND)
3	ML_LANE_0N	3	DDI2_PAIR0_N_Ch_CN	15	DP_AUX_CONN_P
4	ML_LANE_1P	4	DDI2_PAIR1_P_Ch_CN	16	GND
5	GND2	5	GND	17	DP_AUX_CONN_N
6	ML_LANE_1N	6	DDI2_PAIR1_N_Ch_CN	18	CN_DDI2_HPD
7	ML_LANE_2P	7	NC	19	GND
8	GND3	8	GND	20	DP_3V3
9	ML_LANE_2N	9	NC	G1	GND
10	ML_LANE_3P	10	NC	G2	GND
11	GND4	11	GND	G3	GND
12	ML_LANE_3N	12	NC	G4	GND
13	CONFIG1				
14	CONFIG2				
15	AUX_CHP				
16	GND7				
17	AUX_CHN				
18	HPD				
19	RTN				
20	PWR				

5.1.3 VGA+ DSUB(9P)

VGA_COM1

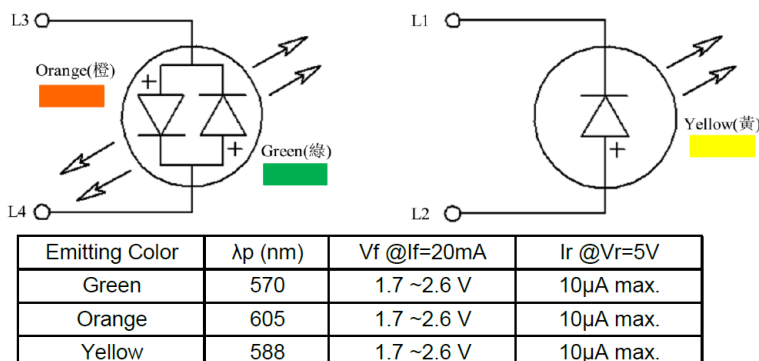
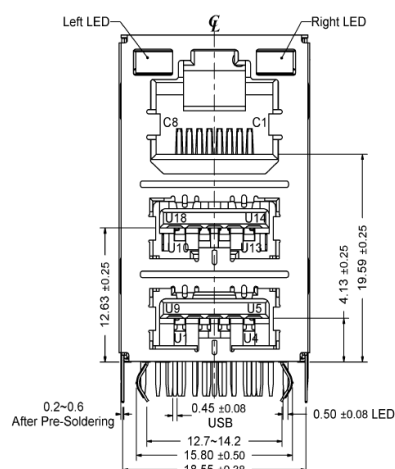


	PIN#	Signal Name	PIN#	Signal Name
	16	COM1_DCD-L	21	COM1_DSR-L
	17	COM1_RXD	22	COM1_RTS-L
	18	COM1_TXD	23	COM1_CTS-L
	19	COM1_DTR-L	24	P_+5V_PSU/P_+12V_PSU
	20	GND		

	PIN#	Signal Name	PIN#	Signal Name
	1	RED	13	CRT_HSYNC
	2	GREEN	14	CRT_VSYNC
	3	BLUE	15	SD_CLK
	4	NC	25	GND
	5	GND	26	GND
	6	GND	27	GND
	7	GND	28	GND
	8	GND		
	9	P_+5V_PSU		
	10	GND		
	11	NC		
	12	SD_DATA		

5.1.4 2.5G Base-T_RJ45 + USB3.2 Gen2 x2

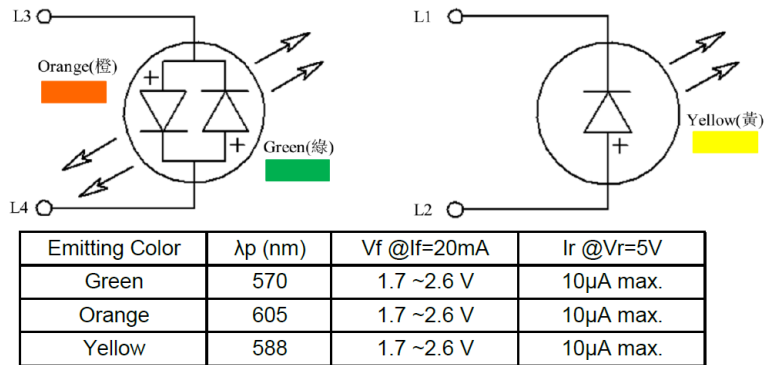
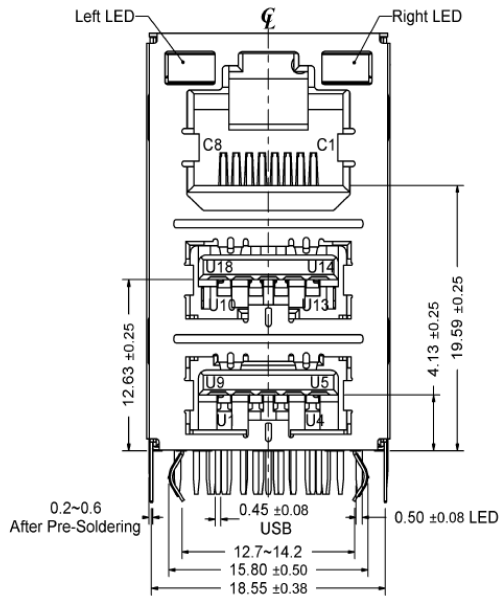
RJ45_USB1



				PIN#	Signal Name	PIN#	Signal Name
				R1	LAN1_CT	U7	GND
				R2	LAN1_MDI0_P	U8	USB31_3_TX_RE_CN_DN
				R3	LAN1_MDI0_N	U9	USB31_3_TX_RE_CN_DP
				R4	LAN1_MDI1_P	U10	USBVCC2
				R5	LAN1_MDI1_N	U11	USB2_P4_CMC_DN
				R6	LAN1_MDI2_P	U12	USB2_P4_CMC_DP
				R7	LAN1_MDI2_N	U13	GND
				R8	LAN1_MDI3_P	U14	USB31_4_RX_RE_CN_DN
				R9	LAN1_MDI3_N	U15	USB31_4_RX_RE_CN_DP
				R10	GND	U16	GND
				L1	LIINK_AT_1	U17	USB31_4_TX_RE_CN_DN
				L2	ACT_AT_1	U18	USB31_4_TX_RE_CN_DP
				L3	LINK1000J_1	G1	GND
				L4	LINK2500J_1	G2	GND
				U1	USBVCC1	G3	GND
				U2	USB2_P3_CMC_DN	G4	GND
				U3	USB2_P3_CMC_DP	G5	GND
				U4	GND	G6	GND
				U5	USB31_3_RX_RE_CN_DN	G7	GND
				U6	USB31_3_RX_RE_CN_DP	G8	GND

5.1.5 1G Base-T_RJ45 + USB3.2 Gen2 x2

RJ45_USB2

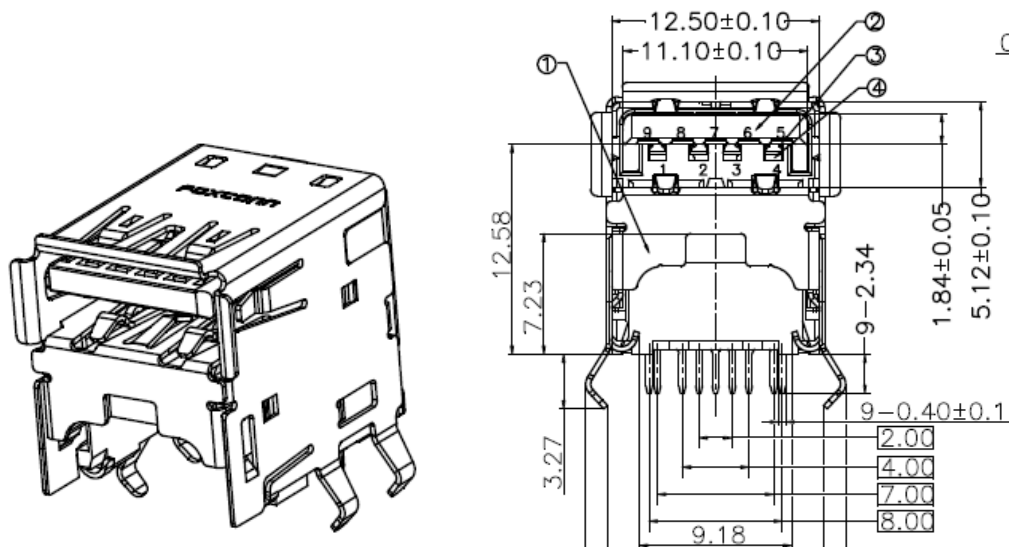


RJ45_USB2			
R2	TD1+	L1	L1
R3	TD1-	L2	L2
R4	TD2+	L3	L3
R5	TD2-	L4	L4
R6	TD3+		
R7	TD3-		
R8	TD4+		
R9	TD4-		
R1	VCC		
R10	GND_1		
U1	VBUS1	U10	VBUS2
U2	DM1	U11	DM2
U3	DP1	U12	DP2
U4	GND_2	U13	GND_4
U5	SSRXN1	U14	SSRXN2
U6	SSRXP1	U15	SSRXP2
U7	GND_3	U16	GND_5
U8	SSTXN1	U17	SSTXN2
U9	SSTXP1	U18	SSTXP2
G1	G2	G3	G4
G5	G6	G7	G8
RJ45-USB3			

PIN#	Signal Name	PIN#	Signal Name
R1	LAN2_CT	U7	GND
R2	LAN2_MDI0_P	U8	USB31_5_TX_RE_CN_DN
R3	LAN2_MDI0_N	U9	USB31_5_TX_RE_CN_DP
R4	LAN2_MDI1_P	U10	USBVCC4
R5	LAN2_MDI1_N	U11	USB2_P6_CMC_DN
R6	LAN2_MDI2_P	U12	USB2_P6_CMC_DP
R7	LAN2_MDI2_N	U13	GND
R8	LAN2_MDI3_P	U14	USB31_6_RX_RE_CN_DN
R9	LAN2_MDI3_N	U15	USB31_6_RX_RE_CN_DP
R10	GND	U16	GND
L1	LIINK_AT_2	U17	USB31_6_TX_RE_CN_DN
L2	ACT_AT_2	U18	USB31_6_TX_RE_CN_DP
L3	LINK1000J_2	G1	GND
L4	LINK2500J_2	G2	GND
U1	USBVCC3	G3	GND
U2	USB2_P5_CMC_DN	G4	GND
U3	USB2_P5_CMC_DP	G5	GND
U4	GND	G6	GND
U5	USB31_5_RX_RE_C_N_DN	G7	GND
U6	USB31_5_RX_RE_C_N_DP	G8	GND

5.1.6 USB3.2 Gen2 Type-A

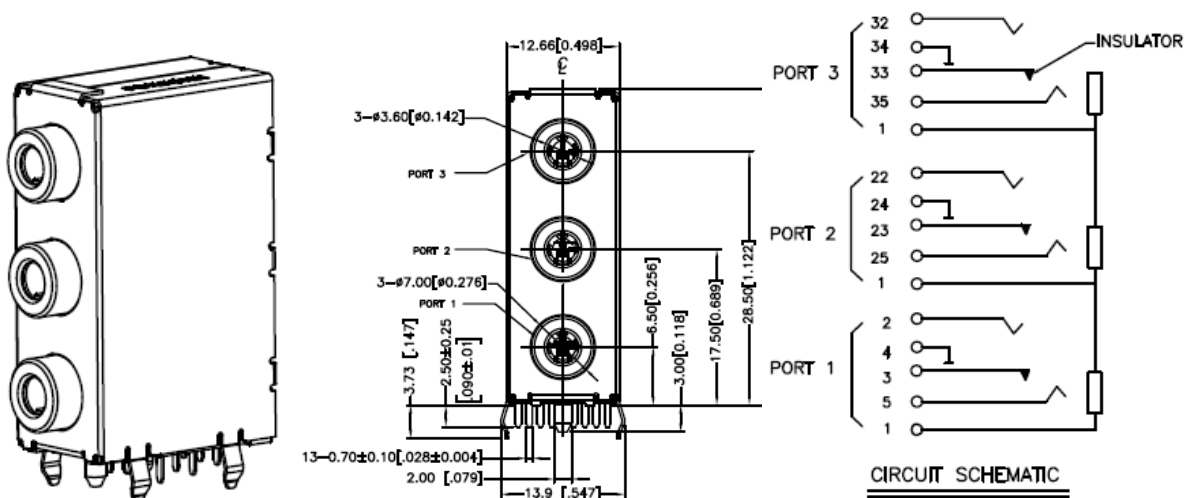
USB2



	PIN#	Signal Name	PIN#	Signal Name
	1	HUB_VBUS_USB1	8	USB31_2_TX_RE_CN_DN
	2	USB2_P2_CMC_DN	9	USB31_2_TX_RE_CN_DP
	3	USB2_P2_CMC_DP	G1	GND
	4	GND	G2	GND
	5	USB31_2_RX_RE_CN_D N	G3	GND
	6	USB31_2_RX_RE_CN_D P	G4	GND
	7	GND		

5.1.8 Audio Jack 3*1 Φ3.5

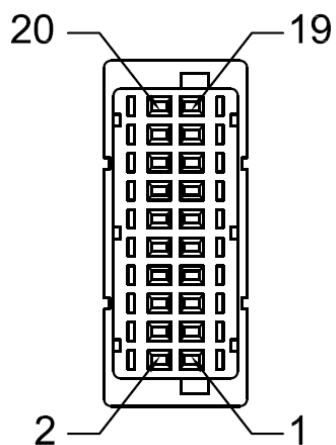
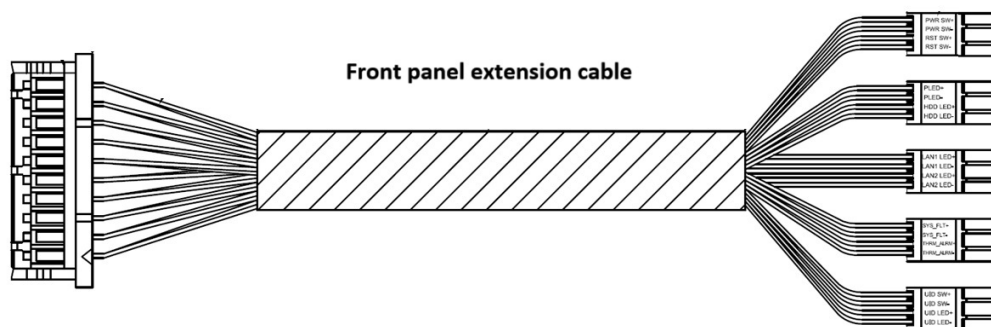
AUDIO1



AUDIO1		PIN#	Signal Name	PIN#	Signal Name
	G1	1	AGND_AU	32	CN_LINE1_L
	G2	2	CN_MIC1_L	33	LINE1_JD
	G3	3	MIC1_JD	34	AGND_AU
	G4	4	AGND_AU	35	CN_LINE1_R
	N1	5	CN_MIC1_R	G1	AU_CHGND
		22	CN_FRONT_L	G2	AU_CHGND
		23	FRONT_JD	G3	AU_CHGND
		24	AGND_AU	G4	AU_CHGND
		25	CN_FRONT_R		

5.2 Onboard Headers and Connectors

5.2.1 Chassis Intrusion Pin Header/Cable Definition

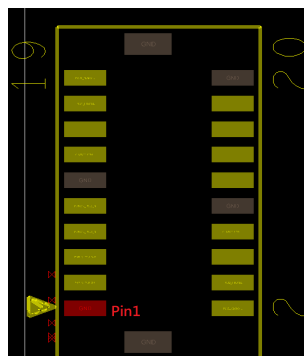


Pin	Signal	Pin	Signal
1	PWR SW-	2	SYS_FLT-
3	PWR SW+	4	SYS_FLT+
5	PLED+	6	UID SW+
7	PLED-	8	UID SW-
9	LAN1_LED+	10	LAN2_LED-
11	LAN1_LED-	12	LAN2_LED+
13	HDD_LED +	14	UID_LED-
15	HDD_LED -	16	UID_LED+)
17	THRM_ALRM+	18	RST SW+
19	THRM_ALRM-	20	RST_SW-

5.2.2 Common Redundant Power Supply

CRPS1

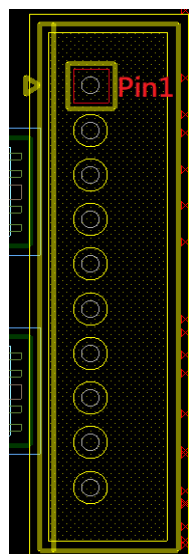
Pin	Signal	Pin	Signal
P1	GND	P2	PSU2_ALARM-L
P3	PMBUS_CLK_O	P4	PSU2_PSON-L
P5	PMBUS_DAT_O	P6	P_+3V3_DUAL
P7	PWROK_PSU1_N	P8	NC
P9	PWROK_PSU2_N	P10	GND
P11	GND	P12	CRPS_PSU1_DET#
P13	NC	P14	CRPS_PSU2_DET#
P15	EXT_SMBUS_ALERT-L	P16	EXT_SMBUS_SDA
P17	PSU1_PSON-L	P18	EXT_SMBUS_SCL
P19	PSU1_ALARM-L	P20	GND



5.2.3 DI and DO

CN21

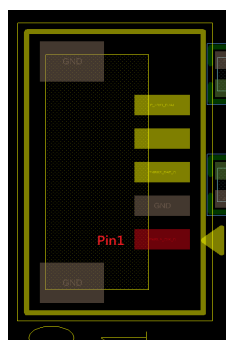
Pin	Signal
P1	GND
P2	DO0_CN
P3	DO1_CN
P4	DO2_CN
P5	DO3_CN
P6	DI0_CN
P7	DI1_CN
P8	DI2_CN
P9	DI3_CN
P10	DIDO_PWR



5.2.4 SMBus

SMBus2

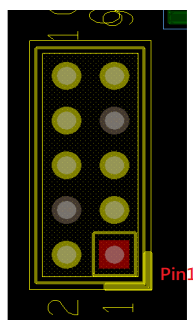
Pin	Signal
P1	PMBUS_CLK_O
P2	PMBUS_DAT_O
P3	SMBUS1_ALERT
P4	GND
P5	P_+3V3_DUAL



5.2.8 SPGIO

CN7

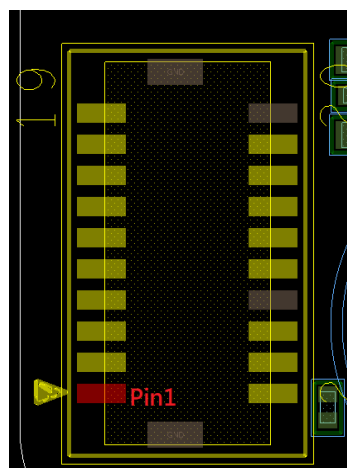
Pin	Signal	Pin	Signal
P1	SATA_SDATAOUT1	P2	N.C
P3	SATA_SLOAD	P4	GND
P5	SATA_SCLOCK	P6	SATA_SCLOCK
P7	GND	P8	SATA_SLOAD
P9	N.C	P10	SATA_SDATAOUT0



5.2.9 Misc

F_MISC1

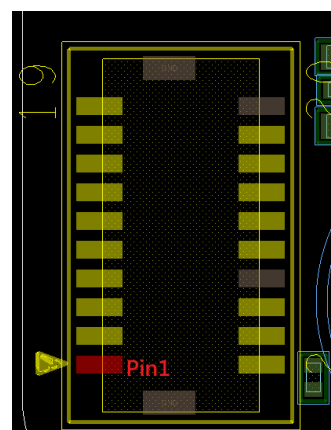
Pin	Signal	Pin	Signal
P1	GND	P2	CUSTOM_LED2-L
P3	PWRBTN-L	P4	CUSTOM_LED2_PWR(3V3)
P5	S0_LED_PWR(3V3)	P6	FP_ID_BTN_R_N
P7	S0_LED-L	P8	GND
P9	LAN1_LED_PWR(3V3)	P10	LAN2_LED_ACT-L
P11	LAN1_LED_ACT-L	P12	LAN2_LED_PWR(3V3)
P13	HDD_LED_PWR (5V)	P14	FP_ID_LED-U
P15	HDD_LED_N	P16	UID_LED_PWR(3V3)
P17	CUSTOM_LED1_PWR(3V3)	P18	RSTBTN_3V3-L
P19	CUSTOM_LED1-L	P20	GND



5.2.10 SATA

SATA_CN1, SATA_CN2, SATA_CN3, SATA_CN4

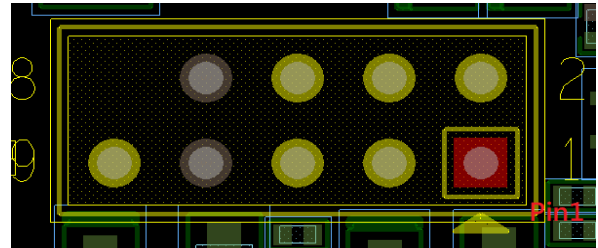
Pin	Signal	Pin	Signal
AS1	GND	BS1	GND
AS2	SATA_0_TX_DP	BS2	SATA_1_TX_DP
AS3	SATA_0_TX_DN	BS3	SATA_1_TX_DN
AS4	GND	BS4	GND
AS5	SATA_0_RX_DN	BS5	SATA_1_RX_DN
AS6	SATA_0_RX_DP	BS6	SATA_1_RX_DP
AS7	GND	BS7	GND



5.2.11 USB2 PH

CN6

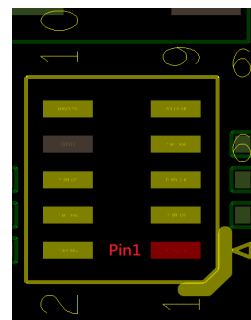
Pin	Signal	Pin	Signal
P1	P5VA_U2RT3_4	P2	P5VA_U2RT3_4
P3	USB2_P12_CMC_DN	P4	USB2_P11_CMC_DN
P5	USB2_P12_CMC_DP	P6	USB2_P11_CMC_DP
P7	GND	P8	GND
P9	N.C	P10	



5.2.12 eSPI PH

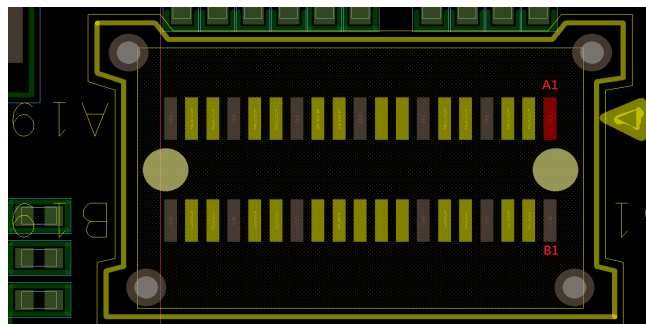
ESPDB1

Pin	Signal	Pin	Signal
P1	P_+DBPWR (1V8/3V3)	P2	GND
P3	ESPI_DB_DAT1	P4	ESPI_DB_DAT2
P5	ESPI_DB_CLK	P6	ESPI_DB_DAT0
P7	ESPI_DB_RST-L	P8	ESPI_DB_CS-L
P9	ESPI_DB_DAT3	P10	P_+DBPWR (1V8/3V3)



5.2.13 SlimSAS

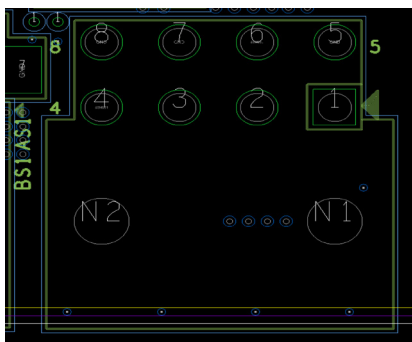
Pin	Signal	Pin	Signal
A1	GND	B1	GND
A2	PCIE_21_RX_DP	B2	PCIE_21_TX_DP
A3	PCIE_21_RX_DN	B3	PCIE_21_TX_DN
A4	GND	B4	GND
A5	PCIE_22_RX_DP	B5	PCIE_22_TX_DP
A6	PCIE_22_RX_DN	B6	PCIE_22_TX_DN
A7	GND	B7	GND
A8	N.C	B8	N.C
A9	N.C	B9	N.C
A10	GND	B10	N.C
A11	CLK_SRC6_DP	B11	SAS_RST-L
A12	CLK_SRC6_DN	B12	N.C
A13	GND	B13	GND
A14	PCIE_23_RX_DP	B14	PCIE_23_TX_DP
A15	PCIE_23_RX_DN	B15	PCIE_23_TX_DN
A16	GND	B16	GND
A17	PCIE_24_RX_DP	B17	PCIE_24_TX_DP
A18	PCIE_24_RX_DN	B18	PCIE_24_TX_DN
A19	GND	B19	GND



5.2.14 ATX_PCl_e

CN11, CN12

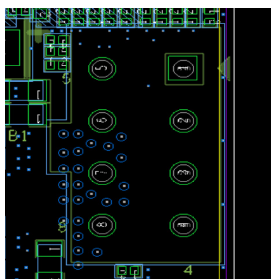
Pin	Signal	Pin	Signal
P1	P_+12V_PSU	P5	GND
P2	P_+12V_PSU	P6	SENSE0
P3	P_+12V_PSU	P7	GND
P4	SENSE1	P8	GND



5.2.15 ATX_CPU

CN9, CN10

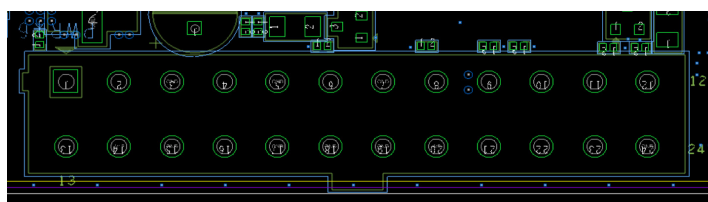
Pin	Signal	Pin	Signal
P1	GND	P5	P_+12V_PSU
P2	GND	P6	P_+12V_PSU
P3	GND	P7	P_+12V_PSU
P4	GND	P8	P_+12V_PSU



5.2.16 ATX_24P

PCN4

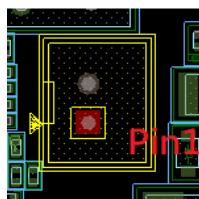
Pin	Signal	Pin	Signal
P1	P_+3V3_PSU	P13	P_+3V3_PSU
P2	P_+3V3_PSU	P14	-V12
P3	GND	P15	GND
P4	P_+5V_PSU	P16	PSON-L
P5	GND	P17	GND
P6	P_+5V_PSU	P18	GND
P7	GND	P19	GND
P8	PSU_PWROK	P20	-V5
P9	P_+5VSB_PSU	P21	P_+5V_PSU
P10	P_+12V_PSU	P22	P_+5V_PSU
P11	P_+12V_PSU	P23	P_+5V_PSU
P12	P_+3V3_PSU	P24	GND



5.2.18 Door Open Connector

CN19, CN20

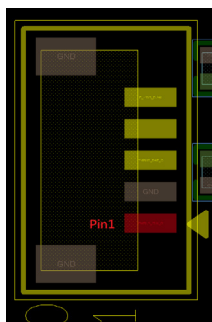
Pin	Signal
P1	FRONT_CHASSIS
P2	GND



5.2.19 IPMB

IPMB1

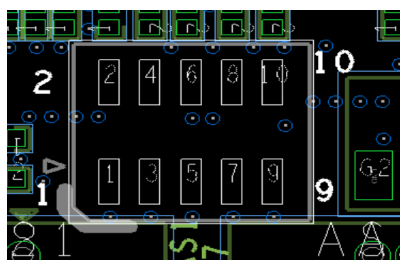
Pin	Signal
P1	IPMB_SDA
P2	IPMB_SCL
P3	NC
P4	GND
P5	P_+3V3_DUAL



5.2.20 CPLD_JTAG

CN28

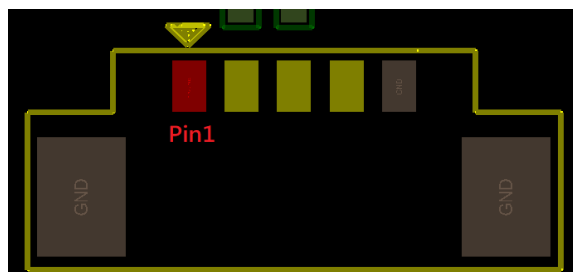
Pin	Signal	Pin	Signal
P1	GND	P2	P_+3V3SB
P3	GND	P4	FPGA_TMS
P5	GND	P6	FPGA_TCK
P7	GND	P8	FPGA_TDO
P9	GND	P10	FPGA_TDI



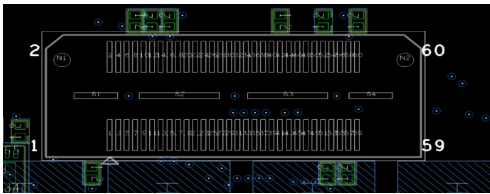
5.2.21 Backplane PCIe Header

CN24

Pin	Signal
P1	P_3V3_DUAL
P2	PCIE_HP_SCL
P3	PCIE_HP_SDA
P4	PCIE_HP_ALERT-L
P5	GND



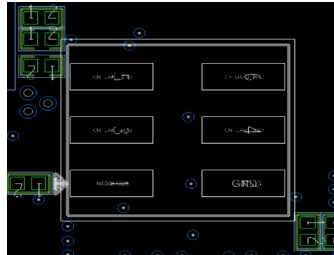
5.2.22 MIPI60



5.2.23 Debug UART

CN27

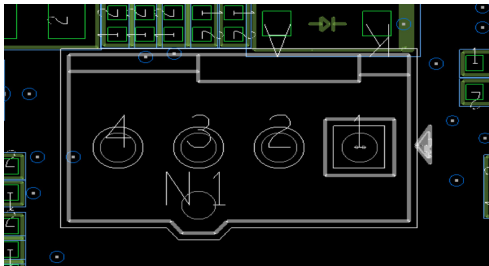
Pin	Signal	Pin	Signal
P1	P_+1V8_TPM	P2	GND
P3	CN_UART_RTS	P4	CN_UART_TXD
P5	CN_UART_CTS	P6	CN_UART_RXD



5.2.24 FAN Connector

FAN_*

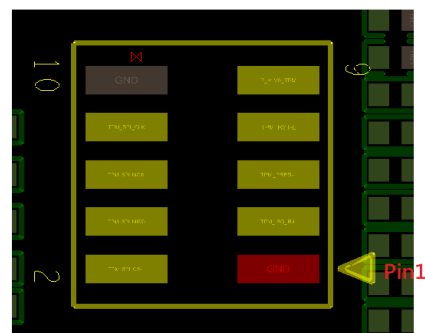
Pin	Signal
P1	GND
P2	P_12V_FAN_*
P3	*_FAN_TACH
P4	*U_PWMOUT



5.2.25 TPM Connector

TPM_CN1

Pin	Signal	Remark	Pin	Signal
P1	GND		P2	SPI_CPU0_TPM_CS-L
P3	TPM_IRQ-L		P4	SPI_CPU0_TPM_MISO
P5	TPM_PRESENT-L		P6	SPI_CPU0_TPM_MOSI
P7	LPC_RST-L		P8	SPI_CPU0_TPM_CLK
P9	P_+1V8_TPM	PWR	P10	GND



5.3 Jumper and Switch Settings

5.3.1 Jumper and Switch Locations

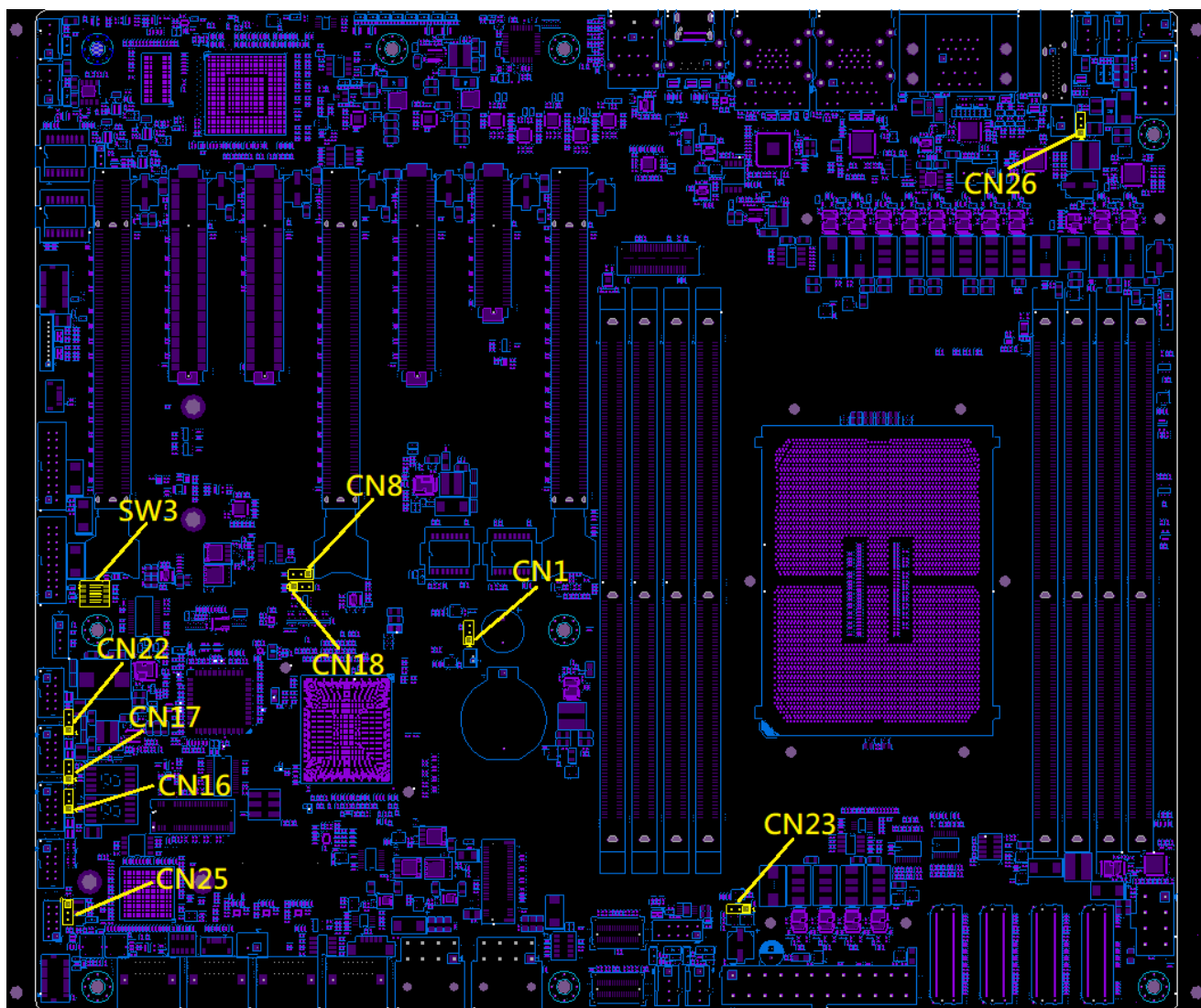
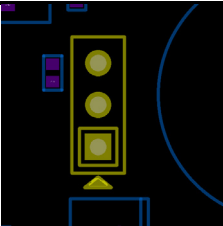


Figure 4: Jumper and switch locations

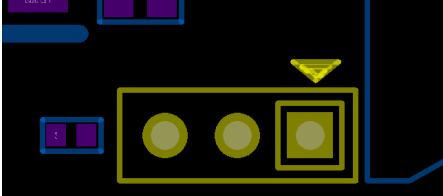
5.3.2 Clear CMOS Header

CN1	Settings
1-2	N/A (Default)
2-3	Clear CMOS

	PIN#	Signal Name
	1	NC
	2	PCH_RTRCRST-L
	3	CLR_CMOS (1K ohm to GND)

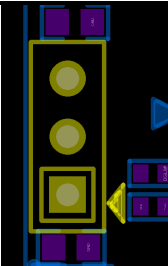
5.3.3 ME Reset Header

CN8	Settings
1-2	N/A (Default)
2-3	Reset ME (Please do not use except special situation)

	PIN#	Signal Name
	1	NC
	2	PCH_SRTCST-L
	3	1K ohm to GND

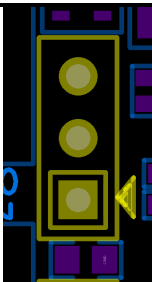
5.3.4 COM3 Power Supply Selection Header

CN16	Settings
NC	No Power Supply (Default)
1-2	5V Power Supply
2-3	12V Power Supply

	PIN#	Signal Name
	1	P_+5V_PSU
	2	COM3 Power Supply
	3	P_+12V_PSU

5.3.5 COM4 Power Supply Selection Header

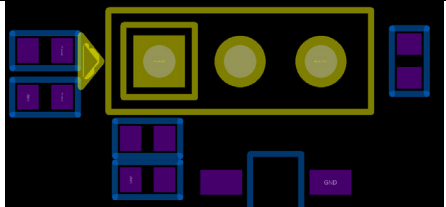
CN17	Settings
NC	No Power Supply (Default)
1-2	5V Power Supply
2-3	12V Power Supply

	PIN#	Signal Name
	1	P_+5V_PSU
	2	COM4 Power Supply
	3	P_+12V_PSU

5.3.6 Flash Descriptor Security Override (FDSO)

CN18

CN18	Settings
1-2	Enable FDSO
2-3	Disable FDSO (ME Lock) (Default)

	PIN#	Signal Name
	1	+VCCPGPPDR_3P3_1P8
	2	FLASH_DES_STRAP
	3	20K ohm to GND

5.3.7 COM5 Power Supply Selection Header

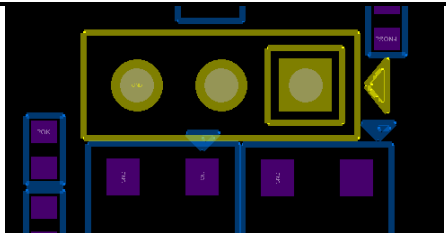
CN22	Settings
NC	No Power Supply (Default)
1-2	5V Power Supply
2-3	12V Power Supply

	PIN#	Signal Name
	1	P_+5V_PSU
	2	COM5 Power Supply
	3	P_+12V_PSU

5.3.8 Force Enable S0 Power

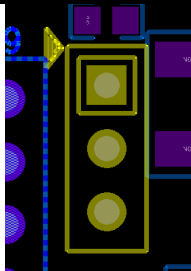
CN23 (Debug only, do not use)

CN23	Settings
1-2	N/A (Default)
2-3	Force Enable S0 Power (Debug only, do not use)

	PIN#	Signal Name
	1	NC
	2	PSON-L
	3	GND

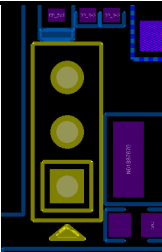
5.3.9 COM2 Power Supply Selection Header

CN25	Settings
NC	No Power Supply (Default)
1-2	5V Power Supply
2-3	12V Power Supply

	PIN#	Signal Name
	1	P_+5V_PSU
	2	COM2 Power Supply
	3	P_+12V_PSU

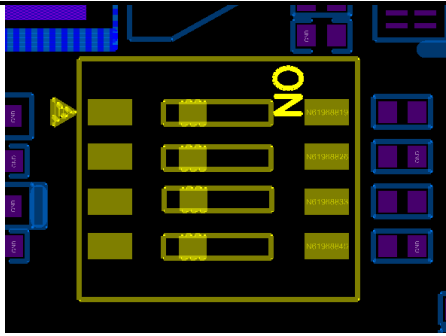
5.3.10 COM1 Power Supply Selection Header

CN26	Setting
NC	No Power Supply (Default)
1-2	5V Power Supply
2-3	12V Power Supply

	PIN#	Signal Name
	1	P_+5V_PSU
	2	COM1 Power Supply
	3	P_+12V_PSU

5.3.11 RS-485 Fail-Safe (Switch)

SW3	Setting OFF	Setting ON (Default)
1-8	COM1 RS-485 Fail-Safe Disable	COM1 RS-485 Fail-Safe Enable
2-7		
3-6	COM2 RS-485 Fail-Safe Disable	COM2 RS-485 Fail-Safe Enable
4-5		

	PIN#	Signal Name	PIN#	Signal Name
	1	COM1_RXD_B	5	1K ohm to GND
	2	COM1_DCD-L_B	6	1K ohm to P_+5V_PSU
	3	COM2_RXD_B	7	1K ohm to GND
	4	COM2_DCD-L_B	8	1K ohm to P_+5V_PSU

5.4 Expansion Slots

5.4.1 Expansion Slot Block Diagram

Project Name: AXE-7400 PCIe extension board_1
Board Name: 37233
Rev. A1

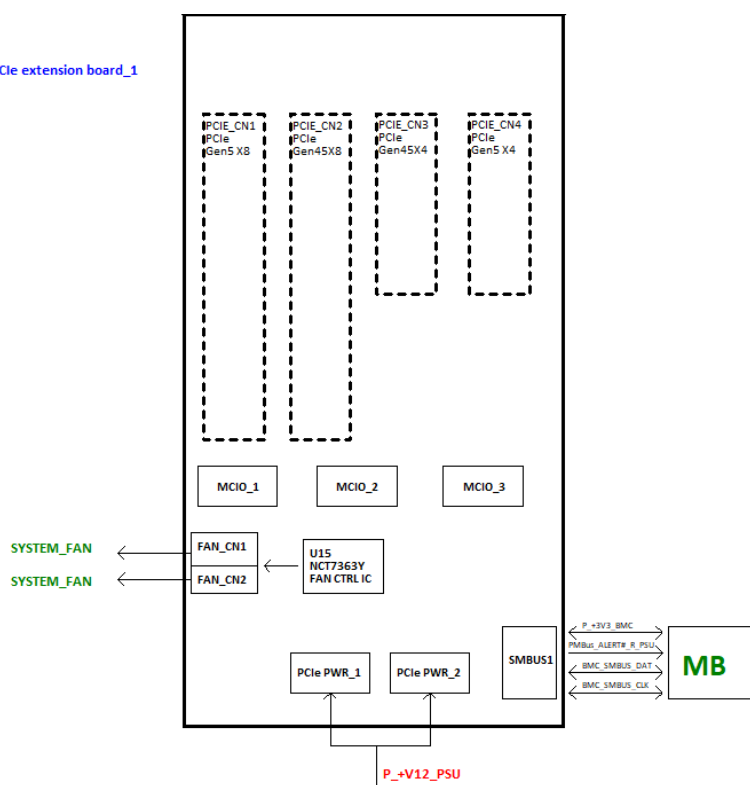
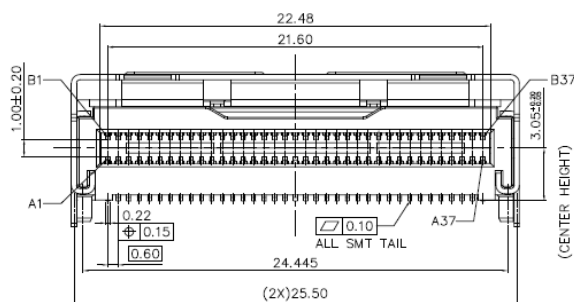
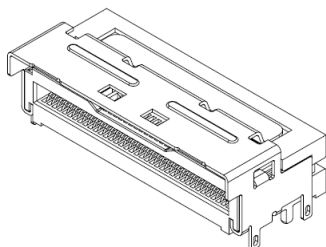


Figure 5: Expansion slot block diagram

5.4.2 MCIO Connectors

Location: MCIO_CN1; MCIO_CN2; MCIO_CN3

Description: MCIO x8, FML 74P RT



MCIO_CN1

Signal	Pin	Pin	Signal
GND	A1	B1	GND
MCIO_PCIE5_PE1_RX_0_DP	A2	B2	MCIO_PCIE5_PE1_TX_0_DP
MCIO_PCIE5_PE1_RX_0_DN	A3	B3	MCIO_PCIE5_PE1_TX_0_DN
GND	A4	B4	GND
MCIO_PCIE5_PE1_RX_1_DP	A5	B5	MCIO_PCIE5_PE1_TX_1_DP
MCIO_PCIE5_PE1_RX_1_DN	A6	B6	MCIO_PCIE5_PE1_TX_1_DN
GND	A7	B7	GND
MCIO_1A_PWRBRK_CLKREQ_N	A8	B8	SMB_MCIO1A_SCL
MCIO_1A_SMB_ALERT_WAKE_N	A9	B9	SMB_MCIO1A_SDA
GND	A10	B10	GND
CLK0_100M_MCIO_1_DP	A11	B11	MCIO_1A_RST_N
CLK0_100M_MCIO_1_DN	A12	B12	MCIO_1A_PRSENT_N
GND	A13	B13	GND
MCIO_PCIE5_PE1_RX_2_DP	A14	B14	MCIO_PCIE5_PE1_TX_2_DP
MCIO_PCIE5_PE1_RX_2_DN	A15	B15	MCIO_PCIE5_PE1_TX_2_DN
GND	A16	B16	GND
MCIO_PCIE5_PE1_RX_3_DP	A17	B17	MCIO_PCIE5_PE1_TX_3_DP
MCIO_PCIE5_PE1_RX_3_DN	A18	B18	MCIO_PCIE5_PE1_TX_3_DN
GND	A19	B19	GND
MCIO_PCIE5_PE1_RX_4_DP	A20	B20	MCIO_PCIE5_PE1_TX_4_DP
MCIO_PCIE5_PE1_RX_4_DN	A21	B21	MCIO_PCIE5_PE1_TX_4_DN
GND	A22	B22	GND
MCIO_PCIE5_PE1_RX_5_DP	A23	B23	MCIO_PCIE5_PE1_TX_5_DP
MCIO_PCIE5_PE1_RX_5_DN	A24	B24	MCIO_PCIE5_PE1_TX_5_DN
GND	A25	B25	GND
NC	A26	B26	NC
NC	A27	B27	NC
GND	A28	B28	GND
NC	A29	B29	NC

NC	A30	B30	NC
GND	A31	B31	GND
MCIO_PCIE5_PE1_RX_6_DP	A32	B32	MCIO_PCIE5_PE1_TX_6_DP
MCIO_PCIE5_PE1_RX_6_DN	A33	B33	MCIO_PCIE5_PE1_TX_6_DN
GND	A34	B34	GND
MCIO_PCIE5_PE1_RX_7_DP	A35	B35	MCIO_PCIE5_PE1_TX_7_DP
MCIO_PCIE5_PE1_RX_7_DN	A36	B36	MCIO_PCIE5_PE1_TX_7_DN
GND	A37	B37	GND
GND	G1	N1	NC
GND	G2	N2	NC
GND	G3		
GND	G4		

MCIO_CN2

Signal	Pin	Pin	Signal
GND	A1	B1	GND
MCIO_PCIE5_PE2_RX_0_DP	A2	B2	MCIO_PCIE5_PE2_TX_0_DP
MCIO_PCIE5_PE2_RX_0_DN	A3	B3	MCIO_PCIE5_PE2_TX_0_DN
GND	A4	B4	GND
MCIO_PCIE5_PE2_RX_1_DP	A5	B5	MCIO_PCIE5_PE2_TX_1_DP
MCIO_PCIE5_PE2_RX_1_DN	A6	B6	MCIO_PCIE5_PE2_TX_1_DN
GND	A7	B7	GND
MCIO_2A_PWRBRK_CLKREQ_N	A8	B8	SMB_MCIO2A_SCL
MCIO_2A_SMB_ALERT_WAKE_N	A9	B9	SMB_MCIO2A_SDA
GND	A10	B10	GND
CLK0_100M_MCIO_2_DP	A11	B11	MCIO_2A_RST_N
CLK0_100M_MCIO_2_DN	A12	B12	MCIO_2A_PRSENT_N
GND	A13	B13	GND
MCIO_PCIE5_PE2_RX_2_DP	A14	B14	MCIO_PCIE5_PE2_TX_2_DP
MCIO_PCIE5_PE2_RX_2_DN	A15	B15	MCIO_PCIE5_PE2_TX_2_DN
GND	A16	B16	GND
MCIO_PCIE5_PE2_RX_3_DP	A17	B17	MCIO_PCIE5_PE2_TX_3_DP
MCIO_PCIE5_PE2_RX_3_DN	A18	B18	MCIO_PCIE5_PE2_TX_3_DN
GND	A19	B19	GND
MCIO_PCIE5_PE2_RX_4_DP	A20	B20	MCIO_PCIE5_PE2_TX_4_DP
MCIO_PCIE5_PE2_RX_4_DN	A21	B21	MCIO_PCIE5_PE2_TX_4_DN
GND	A22	B22	GND
MCIO_PCIE5_PE2_RX_5_DP	A23	B23	MCIO_PCIE5_PE2_TX_5_DP
MCIO_PCIE5_PE2_RX_5_DN	A24	B24	MCIO_PCIE5_PE2_TX_5_DN
GND	A25	B25	GND
NC	A26	B26	NC

NC	A27	B27	NC
GND	A28	B28	GND
NC	A29	B29	NC
NC	A30	B30	NC
GND	A31	B31	GND
MCIO_PCIE5_PE2_RX_6_DP	A32	B32	MCIO_PCIE5_PE2_TX_6_DP
MCIO_PCIE5_PE2_RX_6_DN	A33	B33	MCIO_PCIE5_PE2_TX_6_DN
GND	A34	B34	GND
MCIO_PCIE5_PE2_RX_7_DP	A35	B35	MCIO_PCIE5_PE2_TX_7_DP
MCIO_PCIE5_PE2_RX_7_DN	A36	B36	MCIO_PCIE5_PE2_TX_7_DN
GND	A37	B37	GND
GND	G1	N1	NC
GND	G2	N2	NC
GND	G3		
GND	G4		

MCIO_CN3

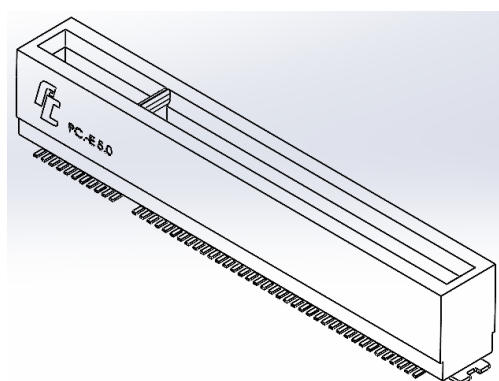
Signal	Pin	Pin	Signal
GND	A1	B1	GND
MCIO_PCIE5_PE3_RX_0_DP	A2	B2	MCIO_PCIE5_PE3_TX_0_DP
MCIO_PCIE5_PE3_RX_0_DN	A3	B3	MCIO_PCIE5_PE3_TX_0_DN
GND	A4	B4	GND
MCIO_PCIE5_PE3_RX_1_DP	A5	B5	MCIO_PCIE5_PE3_TX_1_DP
MCIO_PCIE5_PE3_RX_1_DN	A6	B6	MCIO_PCIE5_PE3_TX_1_DN
GND	A7	B7	GND
MCIO_3A_PWRBRK_CLKREQ_N	A8	B8	SMB_MCIO3A_SCL
MCIO_3A_SMB_ALERT_WAKE_N	A9	B9	SMB_MCIO3A_SDA
GND	A10	B10	GND
CLK0_100M_MCIO_3_DP	A11	B11	MCIO_3A_RST_N
CLK0_100M_MCIO_3_DN	A12	B12	MCIO_3A_PRSENT_N
GND	A13	B13	GND
MCIO_PCIE5_PE3_RX_2_DP	A14	B14	MCIO_PCIE5_PE3_TX_2_DP
MCIO_PCIE5_PE3_RX_2_DN	A15	B15	MCIO_PCIE5_PE3_TX_2_DN
GND	A16	B16	GND
MCIO_PCIE5_PE3_RX_3_DP	A17	B17	MCIO_PCIE5_PE3_TX_3_DP
MCIO_PCIE5_PE3_RX_3_DN	A18	B18	MCIO_PCIE5_PE3_TX_3_DN
GND	A19	B19	GND
MCIO_PCIE5_PE3_RX_4_DP	A20	B20	MCIO_PCIE5_PE3_TX_4_DP
MCIO_PCIE5_PE3_RX_4_DN	A21	B21	MCIO_PCIE5_PE3_TX_4_DN
GND	A22	B22	GND
MCIO_PCIE5_PE3_RX_5_DP	A23	B23	MCIO_PCIE5_PE3_TX_5_DP

MCIO_PCIE5_PE3_RX_5_DN	A24	B24	MCIO_PCIE5_PE3_TX_5_DN
GND	A25	B25	GND
MCIO_3B_PWRBRK_CLKREQ_N	A26	B26	SMB_MCIO3B_SCL
MCIO_3B_SMB_ALERT_WAKE_N	A27	B27	SMB_MCIO3B_SDA
GND	A28	B28	GND
CLK1_100M_MCIO_3_DP	A29	B29	MCIO_3B_RST_N
CLK1_100M_MCIO_3_DN	A30	B30	MCIO_3B_PRSENT_N
GND	A31	B31	GND
MCIO_PCIE5_PE3_RX_6_DP	A32	B32	MCIO_PCIE5_PE3_TX_6_DP
MCIO_PCIE5_PE3_RX_6_DN	A33	B33	MCIO_PCIE5_PE3_TX_6_DN
GND	A34	B34	GND
MCIO_PCIE5_PE3_RX_7_DP	A35	B35	MCIO_PCIE5_PE3_TX_7_DP
MCIO_PCIE5_PE3_RX_7_DN	A36	B36	MCIO_PCIE5_PE3_TX_7_DN
GND	A37	B37	GND
GND	G1	N1	NC
GND	G2	N2	NC
GND	G3		
GND	G4		

5.4.3 PCIe Slots (PCIe x8)

Location: PCIE_CN1; PCIE_CN2

Description: PCIe Slot 98P x8 ST



PCIE_CN1

Signal	Pin	Pin	Signal
P_+12V_PSU	B1	A1	MCIO_1A_PWRBRK_CLKREQ_N
P_+12V_PSU	B2	A2	P_+12V_PSU
P_+12V_PSU	B3	A3	P_+12V_PSU
GND	B4	A4	GND
SMB_MCIO1A_SCL	B5	A5	NC
SMB_MCIO1A_SDA	B6	A6	NC
GND	B7	A7	NC
P_+3V3_S0	B8	A8	NC

NC	B9	A9	P_+3V3_S0
P_+3V3_S0	B10	A10	P_+3V3_S0
MCIO_1A_SMB_ALERT_WAKE_N	B11	A11	MCIO_1A_RST_N
Separation Key			
NC	B12	A12	GND
GND	B13	A13	CLK_100M_MCIO_1A_DP
MCIO_PCIE5_PE1_TX_0_DP	B14	A14	CLK_100M_MCIO_1A_DN
MCIO_PCIE5_PE1_TX_0_DN	B15	A15	GND
GND	B16	A16	MCIO_PCIE5_PE1_RX_0_DP
MCIO_1A_PRSNT_N	B17	A17	MCIO_PCIE5_PE1_RX_0_DN
GND	B18	A18	GND
MCIO_PCIE5_PE1_TX_1_DP	B19	A19	NC
MCIO_PCIE5_PE1_TX_1_DN	B20	A20	GND
GND	B21	A21	MCIO_PCIE5_PE1_RX_1_DP
GND	B22	A22	MCIO_PCIE5_PE1_RX_1_DN
MCIO_PCIE5_PE1_TX_2_DP	B23	A23	GND
MCIO_PCIE5_PE1_TX_2_DN	B24	A24	GND
GND	B25	A25	MCIO_PCIE5_PE1_RX_2_DP
GND	B26	A26	MCIO_PCIE5_PE1_RX_2_DN
MCIO_PCIE5_PE1_TX_3_DP	B27	A27	GND
MCIO_PCIE5_PE1_TX_3_DN	B28	A28	GND
GND	B29	A29	MCIO_PCIE5_PE1_RX_3_DP
NC	B30	A30	MCIO_PCIE5_PE1_RX_3_DN
MCIO_1A_PRSNT_N	B31	A31	GND
GND	B32	A32	NC
MCIO_PCIE5_PE1_TX_4_DP	B33	A33	NC
MCIO_PCIE5_PE1_TX_4_DN	B34	A34	GND
GND	B35	A35	MCIO_PCIE5_PE1_RX_4_DP
GND	B36	A36	MCIO_PCIE5_PE1_RX_4_DN
MCIO_PCIE5_PE1_TX_5_DP	B37	A37	GND
MCIO_PCIE5_PE1_TX_5_DN	B38	A38	GND
GND	B39	A39	MCIO_PCIE5_PE1_RX_5_DP
GND	B40	A40	MCIO_PCIE5_PE1_RX_5_DN
MCIO_PCIE5_PE1_TX_6_DP	B41	A41	GND
MCIO_PCIE5_PE1_TX_6_DN	B42	A42	GND
GND	B43	A43	MCIO_PCIE5_PE1_RX_6_DP
GND	B44	A44	MCIO_PCIE5_PE1_RX_6_DN
MCIO_PCIE5_PE1_TX_7_DP	B45	A45	GND
MCIO_PCIE5_PE1_TX_7_DN	B46	A46	GND
GND	B47	A47	MCIO_PCIE5_PE1_RX_7_DP
MCIO_1A_PRSNT_N	B48	A48	MCIO_PCIE5_PE1_RX_7_DN
GND	B49	A49	GND

NC	N1	N2	NC
GND	G1	G2	GND

PCIE_CN2

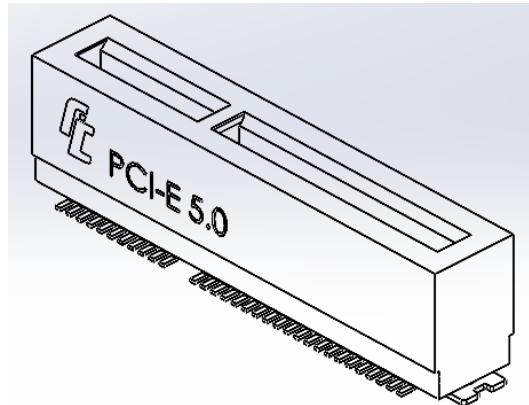
Signal	Pin	Pin	Signal
P_+12V_PSU	B1	A1	MCIO_2A_PWRBRK_CLKREQ_N
P_+12V_PSU	B2	A2	P_+12V_PSU
P_+12V_PSU	B3	A3	P_+12V_PSU
GND	B4	A4	GND
SMB_MCIO2A_SCL	B5	A5	NC
SMB_MCIO2A_SDA	B6	A6	NC
GND	B7	A7	NC
P_+3V3_S0	B8	A8	NC
NC	B9	A9	P_+3V3_S0
P_+3V3_S0	B10	A10	P_+3V3_S0
MCIO_2A_SMB_ALERT_WAKE_N	B11	A11	MCIO_2A_RST_N
Separation Key			
NC	B12	A12	GND
GND	B13	A13	CLK_100M_MCIO_2A_DP
MCIO_PCIE5_PE2_TX_0_DP	B14	A14	CLK_100M_MCIO_2A_DN
MCIO_PCIE5_PE2_TX_0_DN	B15	A15	GND
GND	B16	A16	MCIO_PCIE5_PE2_RX_0_DP
MCIO_2A_PRSENT_N	B17	A17	MCIO_PCIE5_PE2_RX_0_DN
GND	B18	A18	GND
MCIO_PCIE5_PE2_TX_1_DP	B19	A19	NC
MCIO_PCIE5_PE2_TX_1_DN	B20	A20	GND
GND	B21	A21	MCIO_PCIE5_PE2_RX_1_DP
GND	B22	A22	MCIO_PCIE5_PE2_RX_1_DN
MCIO_PCIE5_PE2_TX_2_DP	B23	A23	GND
MCIO_PCIE5_PE2_TX_2_DN	B24	A24	GND
GND	B25	A25	MCIO_PCIE5_PE2_RX_2_DP
GND	B26	A26	MCIO_PCIE5_PE2_RX_2_DN
MCIO_PCIE5_PE2_TX_3_DP	B27	A27	GND
MCIO_PCIE5_PE2_TX_3_DN	B28	A28	GND
GND	B29	A29	MCIO_PCIE5_PE2_RX_3_DP
NC	B30	A30	MCIO_PCIE5_PE2_RX_3_DN
MCIO_2A_PRSENT_N	B31	A31	GND
GND	B32	A32	NC
MCIO_PCIE5_PE2_TX_4_DP	B33	A33	NC
MCIO_PCIE5_PE2_TX_4_DN	B34	A34	GND
GND	B35	A35	MCIO_PCIE5_PE2_RX_4_DP
GND	B36	A36	MCIO_PCIE5_PE2_RX_4_DN

MCIO_PCIE5_PE2_TX_5_DP	B37	A37	GND
MCIO_PCIE5_PE2_TX_5_DN	B38	A38	GND
GND	B39	A39	MCIO_PCIE5_PE2_RX_5_DP
GND	B40	A40	MCIO_PCIE5_PE2_RX_5_DN
MCIO_PCIE5_PE2_TX_6_DP	B41	A41	GND
MCIO_PCIE5_PE2_TX_6_DN	B42	A42	GND
GND	B43	A43	MCIO_PCIE5_PE2_RX_6_DP
GND	B44	A44	MCIO_PCIE5_PE2_RX_6_DN
MCIO_PCIE5_PE2_TX_7_DP	B45	A45	GND
MCIO_PCIE5_PE2_TX_7_DN	B46	A46	GND
GND	B47	A47	MCIO_PCIE5_PE2_RX_7_DP
MCIO_2A_PRSENT_N	B48	A48	MCIO_PCIE5_PE2_RX_7_DN
GND	B49	A49	GND
NC	N1	N2	NC
GND	G1	G2	GND

5.4.4 PCIe Slots (PCIe x4)

Location: PCIE_CN3; PCIE_CN4

Description: PCIe Slot 64P x4 ST



PCIE_CN3

Signal	Pin	Pin	Signal
P_+12V_PSU	B1	A1	MCIO_3A_PWRBRK_CLKREQ_N
P_+12V_PSU	B2	A2	P_+12V_PSU
P_+12V_PSU	B3	A3	P_+12V_PSU
GND	B4	A4	GND
SMB_MCIO3A_SCL	B5	A5	NC
SMB_MCIO3A_SDA	B6	A6	NC
GND	B7	A7	NC
P_+3V3_S0	B8	A8	NC
NC	B9	A9	P_+3V3_S0
P_+3V3_S0	B10	A10	P_+3V3_S0

MCIO_3A_SMB_ALERT_WAKE_N	B11	A11	MCIO_3A_RST_N
Separation Key			
NC	B12	A12	GND
GND	B13	A13	CLK_100M_MCIO_3A_DP
MCIO_PCIE5_PE3_TX_0_DP	B14	A14	CLK_100M_MCIO_3A_DN
MCIO_PCIE5_PE3_TX_0_DN	B15	A15	GND
GND	B16	A16	MCIO_PCIE5_PE3_RX_0_DP
MCIO_3A_PRSENT_N	B17	A17	MCIO_PCIE5_PE3_RX_0_DN
GND	B18	A18	GND
MCIO_PCIE5_PE3_TX_1_DP	B19	A19	NC
MCIO_PCIE5_PE3_TX_1_DN	B20	A20	GND
GND	B21	A21	MCIO_PCIE5_PE3_RX_1_DP
GND	B22	A22	MCIO_PCIE5_PE3_RX_1_DN
MCIO_PCIE5_PE3_TX_2_DP	B23	A23	GND
MCIO_PCIE5_PE3_TX_2_DN	B24	A24	GND
GND	B25	A25	MCIO_PCIE5_PE3_RX_2_DP
GND	B26	A26	MCIO_PCIE5_PE3_RX_2_DN
MCIO_PCIE5_PE3_TX_3_DP	B27	A27	GND
MCIO_PCIE5_PE3_TX_3_DN	B28	A28	GND
GND	B29	A29	MCIO_PCIE5_PE3_RX_3_DP
NC	B30	A30	MCIO_PCIE5_PE3_RX_3_DN
MCIO_3A_PRSENT_N	B31	A31	GND
GND	B32	A32	NC
NC	N1	N2	NC
GND	G1	G2	GND

PCIE_CN4

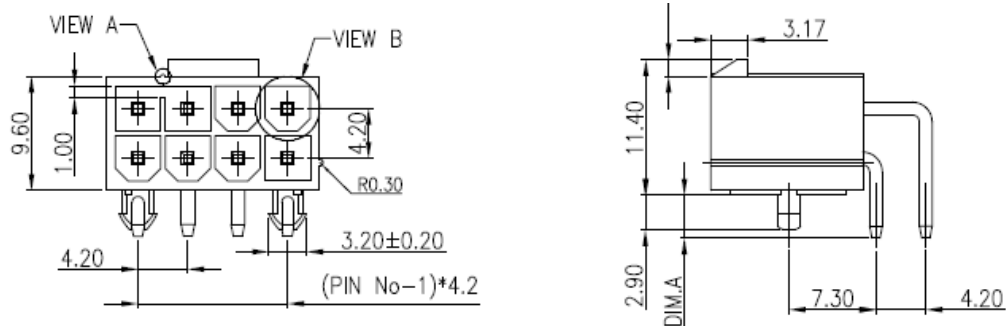
Signal	Pin	Pin	Signal
P_+12V_PSU	B1	A1	MCIO_3B_PWRBRK_CLKREQ_N
P_+12V_PSU	B2	A2	P_+12V_PSU
P_+12V_PSU	B3	A3	P_+12V_PSU
GND	B4	A4	GND
SMB_MCIO3B_SCL	B5	A5	NC
SMB_MCIO3B_SDA	B6	A6	NC
GND	B7	A7	NC
P_+3V3_S0	B8	A8	NC
NC	B9	A9	P_+3V3_S0
P_+3V3_S0	B10	A10	P_+3V3_S0
MCIO_3B_SMB_ALERT_WAKE_N	B11	A11	MCIO_3B_RST_N
Separation Key			
NC	B12	A12	GND

GND	B13	A13	CLK_100M_MCIO_3B_DP
MCIO_PCIE5_PE3_TX_4_DP	B14	A14	CLK_100M_MCIO_3B_DN
MCIO_PCIE5_PE3_TX_4_DN	B15	A15	GND
GND	B16	A16	MCIO_PCIE5_PE3_RX_4_DP
MCIO_3B_PRSENT_N	B17	A17	MCIO_PCIE5_PE3_RX_4_DN
GND	B18	A18	GND
MCIO_PCIE5_PE3_TX_5_DP	B19	A19	NC
MCIO_PCIE5_PE3_TX_5_DN	B20	A20	GND
GND	B21	A21	MCIO_PCIE5_PE3_RX_5_DP
GND	B22	A22	MCIO_PCIE5_PE3_RX_5_DN
MCIO_PCIE5_PE3_TX_6_DP	B23	A23	GND
MCIO_PCIE5_PE3_TX_6_DN	B24	A24	GND
GND	B25	A25	MCIO_PCIE5_PE3_RX_6_DP
GND	B26	A26	MCIO_PCIE5_PE3_RX_6_DN
MCIO_PCIE5_PE3_TX_7_DP	B27	A27	GND
MCIO_PCIE5_PE3_TX_7_DN	B28	A28	GND
GND	B29	A29	MCIO_PCIE5_PE3_RX_7_DP
NC	B30	A30	MCIO_PCIE5_PE3_RX_7_DN
MCIO_3B_PRSENT_N	B31	A31	GND
GND	B32	A32	NC
NC	N1	N2	NC
GND	G1	G2	GND

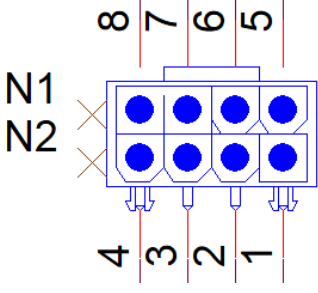
5.4.5 PCIe 12V Power Connectors

Location: CN1; CN2

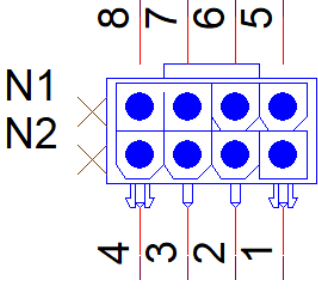
Description: Power Header ML 2x4P



CN1

	PIN#	Signal Name	PIN#	Signal Name
	1	P_+12V_PSU	5	CN1_SENSE0 (10K ohm to GND)
	2	P_+12V_PSU	6	GND
	3	P_+12V_PSU	7	GND
	4	CN1_SENSE1 (10K ohm to GND)	8	GND

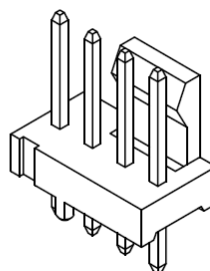
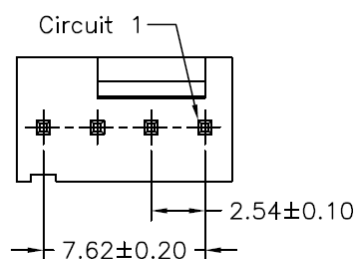
CN2

	PIN#	Signal Name	PIN#	Signal Name
	1	P_+12V_PSU	5	CN2_SENSE0 (10K ohm to GND)
	2	P_+12V_PSU	6	GND
	3	P_+12V_PSU	7	GND
	4	CN2_SENSE1 (10K ohm to GND)	8	GND

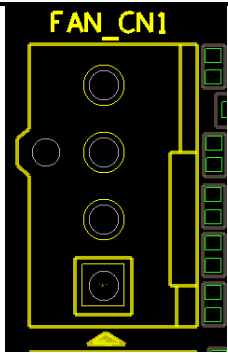
5.4.6 System Fan Connectors

Location: FAN_CN1; FAN_CN2

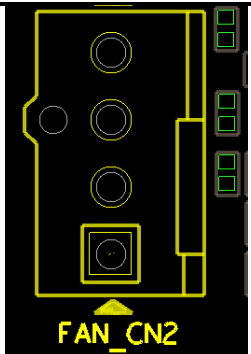
Description: WAFER ML 1x4P ST D2.54



FAN_CN1

	PIN#	Signal Name
	1	GND
	2	P_+12V_FAN1
	3	FAN1_PWM_IN
	4	FAN1_PWM_OUT

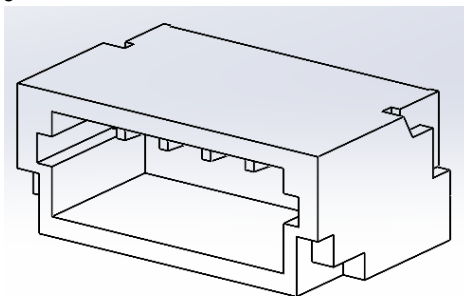
FAN_CN2

	PIN#	Signal Name
	1	GND
	2	P_+12V_FAN2
	3	FAN2_PWM_IN
	4	FAN2_PWM_OUT

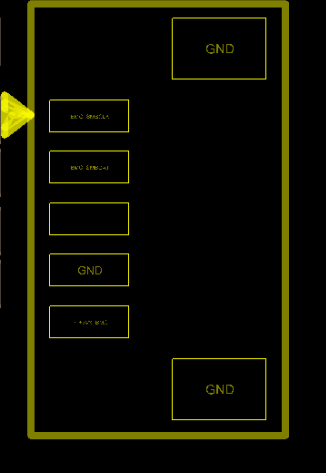
5.4.7 SMBus Connector

Location: SMBUS1

Description: WAFER ML 1x5P ST D1.0



SMBUS1

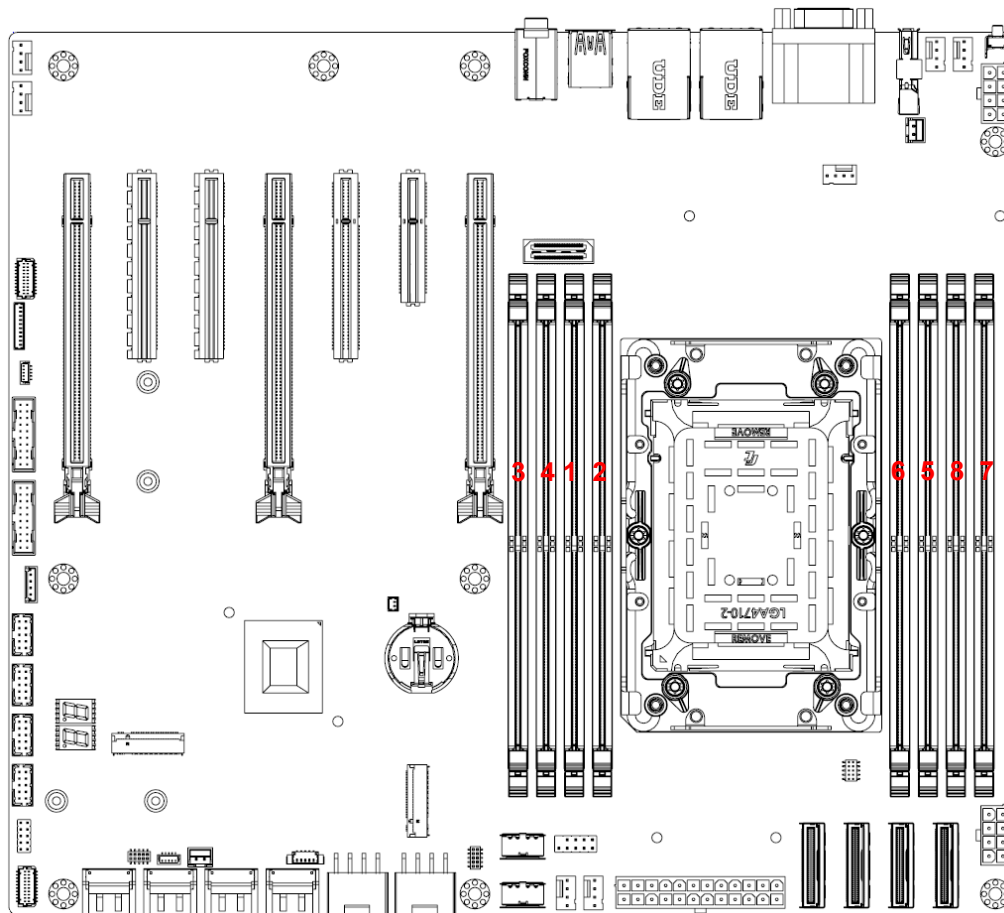
	PIN#	Signal Name
	1	BMC_SMBCLK
	2	BMC_SMBDAT
	3	BMC_ALERT
	4	GND
	5	P_+3V3_BMC
	G1	GND
	G2	GND

This page intentionally left blank.

6 Getting Started

6.1 Installing Memory Modules

Memory modules must be populated as shown (slots 1 > 2 > 3 > 4 > 5 > 6).



Granite Rapids DDR5 only DIMM configurations diagram

DIMM Quantity	ISB-W890 DIMM							
	DIMM3	DIMM4	DIMM1	DIMM2	DIMM6	DIMM5	DIMM8	DIMM7
1DIMM			V					
1DIMM						V		
2DIMM			V					V
2DIMM	V					V		
4DIMM	V		V			V		V
8DIMM	V	V	V	V	V	V	V	V

6.2 PCIe Slot Secondary Power Supply

The ISB-W890 is equipped with two 8-pin ATX-type 12V power connectors on the mainboard (see section 4.2 Connector Locations) The pin definitions of the connectors and cables are described below.



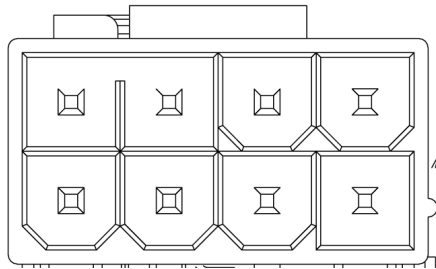
CAUTION:
mise en garde

All installation procedures are restricted to skilled personnel.

Toutes les procédures d'installation sont réservées au personnel qualifié.

6.2.1 8-Pin ATX-Type 12V Power Connector Pinout

Pin #	Signal
1	P12V
2	P12V
3	P12V
4	SENSE1
5	GND
6	SENSE0
7	GND
8	GND



6.3 BMC LAN Configuration

Users can modify the BMC IP via ipmitool commands.

Show the current LAN setting

- `ipmitool lan print 1`

[Static IP]

Set the IP source to static

- `ipmitool lan set 1 ipsrc static`

Set the IP address

- `ipmitool lan set 1 ipaddr xxx.xxx.xxx.xxx`

Set the netmask address

- `ipmitool lan set 1 netmask xxx.xxx.xxx.xxx`

Set the gateway address

- `ipmitool lan set 1 defgw ipaddr xxx.xxx.xxx.xxx`

[DHCP IP]

Set IP source to DHCP

- `ipmitool lan set 1 ipsrc dhcp`



NOTE:

BMC IP can be set in the BIOS.

6.4 BIOS Update

Users can update the ISB-W890 system BIOS via various interfaces (Gigabit LAN, KCS, and the console port).

6.4.1 Updating BIOS via Host with BIOS Tool

1. Boot/Login to the Shell
2. Update the BIOS from the host using the following commands:

Example:

AfuEfix64 BIOS.ROM /p /b /n /x (to update BIOS without ME)

```
FS0:\> cd AXE-7400GRW_00510_FullImage
FS0:\AXE-7400GRW_00510_FullImage> ls
Directory of: FS0:\AXE-7400GRW_00510_FullImage\
12/03/2025  14:54 <DIR>          16,384  .
12/03/2025  14:54 <DIR>           0  ..
12/03/2025  01:27          684,048  AfuEfix64.efi
12/03/2025  01:27       50,331,648  AXE-7400GRW_00510.ROM
12/03/2025  01:27       67,108,864  AXE-7400GRW_00510_Corporate.BIN
12/03/2025  01:27         6,202  HISTORY.txt
12/03/2025  01:27         405  pBIOS.nsh
           5 File(s) 118,131,167 bytes
           2 Dir(s)
FS0:\AXE-7400GRW_00510_FullImage>
```



NOTE:

Updating BIOS via BMC, please refer to Chapter 9 BMC.

6.5 BMC Firmware Update via Network

This section outlines the various methods available for updating the BMC firmware.

BMC firmware updates can be performed through four primary methods:

1. **Web interface update**
For detailed steps and guidelines, please refer to Section [8.2.8.1.1 BMC Update](#).
2. **Redfish update**
For detailed steps and guidelines, please refer to Section [8.4.4 BMC Update](#).

6.6 CPLD Update

This section outlines the various methods available for updating the BMC firmware.

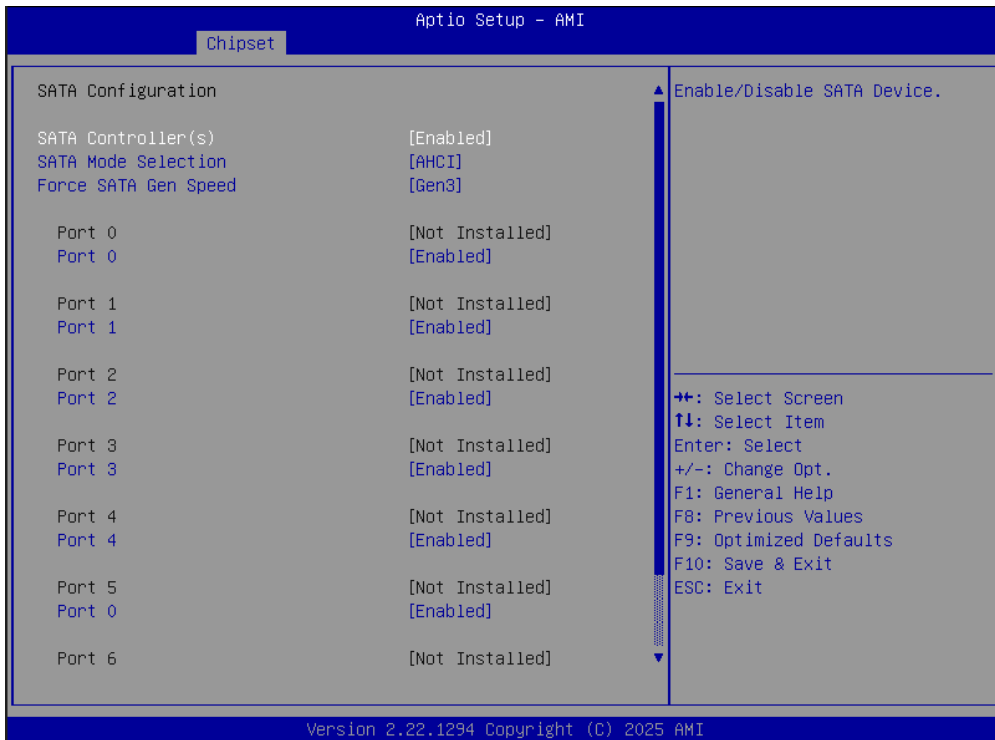
BMC firmware updates can be performed through four primary methods:

1. **Web interface update**
For detailed steps and guidelines, please refer to Section [8.2.8.2.1 HPM Firmware Update-CPLD/BIOS](#).
2. **Redfish update**
For detailed steps and guidelines, please refer to Section [8.4.6 CPLD Update](#).
3. **ipmitool update**
For detailed steps and guidelines, please refer to Section [8.3.2.6 CPLD Update](#).

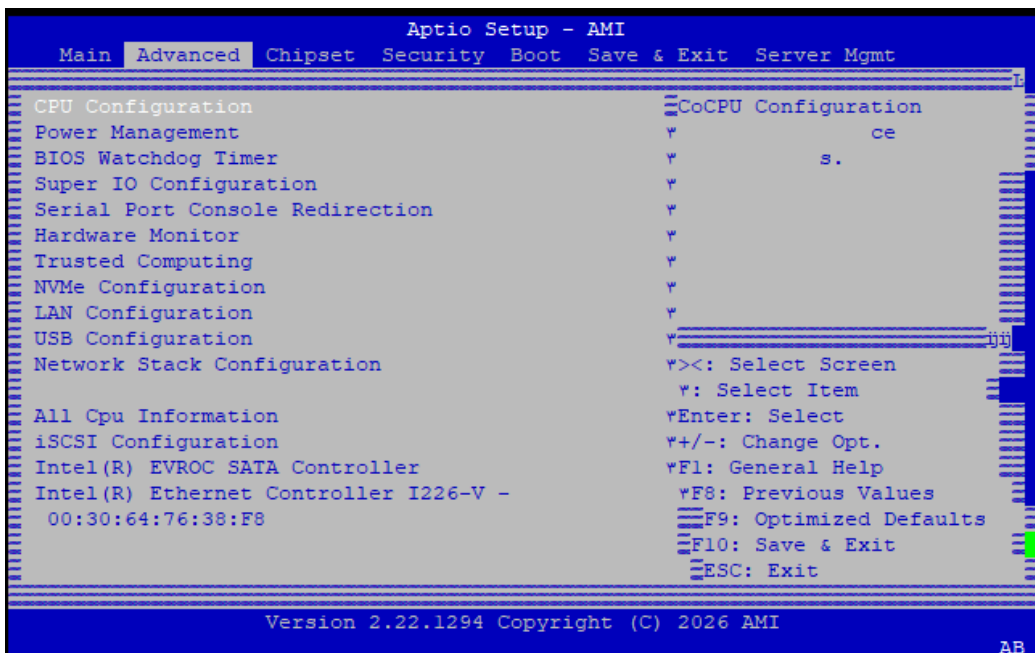
6.7 Create a RAID Volume

To create a RAID volume, the RAID option must be enabled in the BIOS so that the system loads the RAID option ROM code (see section 8.4.2.1 SATA Configuration)

1. Go to **Chipset > PCH Configurations > SATA Configuration**.
2. Set **SATA Mode Selection** to **RAID**, save changes, and reboot the system.



To create a RAID volume, go to the **Advanced** menu



Enter the **Intel(R) VROC sSATA Controller** submenu and click on **Create RAID Volume**.

7 BIOS Settings

To enter the BIOS setup screen, follow these steps:

1. Power on the ISB-W890.
2. Press the <Delete> or <ESC> key on your keyboard when you see the following text prompt: "Press DEL or ESC to enter Setup".
(Note: If Quick Boot is enabled, the screen below will not display, but pressing the <Delete> or <ESC> key will still allow you to enter the BIOS setup screen.)



3. After pressing the <Delete> or <ESC> key, the main BIOS setup menu will display. You can access the other setup screens from the main BIOS setup menu, such as Chipset and Power menus.

7.1 BIOS Setup Menu

The BIOS setup utility is invoked by pressing <ESC> or keys. User can change BIOS settings during setup utility runs. A system reset is required for new settings to take effect.

In the BIOS setup utility, there are several hot keys are designed for specific purposes, as listed below.

- <F1>: General help in setup menu
- <F8>: Load previous BIOS values
- <F9>: Load BIOS default in setup utility
- <F10>: Save & Exit setup utility

To navigate through the BIOS setup menu, use the following.

→←	Left/Right. The <i>Left and Right</i> < Arrow > keys allow you to select a setup screen. For example: Main screen, Advanced screen, Chipset screen, and so on.
↑↓	Up/Down The <i>Up and Down</i> < Arrow > keys allow you to select a setup item or sub-screen.
+ -	Plus/Minus The <i>Plus and Minus</i> < Arrow > keys allow you to change the field value of a particular setup item. For example: Date and Time.
Tab	The < Tab > key allows you to select setup fields.

7.1.1 Menu Selection Bar

The Menu Selection Bar is located at the top of the screen. It displays the top-level available menus to the user:

- Main Menu
- Advanced Menu
- Chipset Menu
- Security Menu
- Boot Menu
- Save & Exit Menu
- Server Mgmt

7.1.2 Menu Conventions

The appearance of the setup menu listed in this chapter is a sample to describe the item list. It is shown on a VT100 terminal via serial console. The menu conventions are as follows.

Using color

The mandatory BIOS setup fields are in black. The BIOS setup fields currently not used are in grey. The display only strings are in black.

Using brackets

Editable menu options are marketed with squares '[' and ']' to distinguish them from display only fields that can't be modified.

7.2 Main Menu

The Main Menu provides read-only information about the system and also allows you to set the system date and time. The tables below show screen shots of the Main menu details, submenus and settings.



7.2.1 BIOS Information

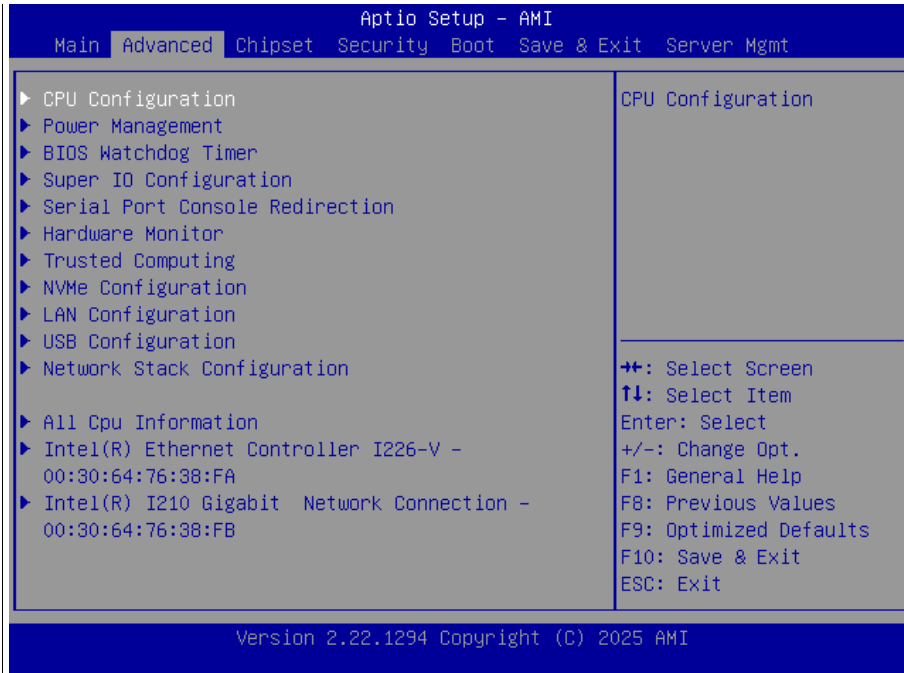
BIOS Item	Options	Description
BIOS Vendor	Info-only. American Megatrends	Display vendor name of system BIOS.
BIOS Version	Info-only. x.yy.zz	Display version of booting BIOS.
Build Date	Info-only. MM/DD/YYYY	It shows the date that BIOS was built.
MRC Version	Info-only. xxx.Ryy	Display the revision of MRC code which is implemented in BIOS.
ME FW Version	Info-only. ww:x.y.z.aaa	Display the version of Intel manageability firmware which is implemented in BIOS.

7.2.2 System Information

BIOS Item	Options	Description
Project Name	Info-only.	Shows Project Name
CPU Board Version	Info-only.	Shows Main Board Version
CPU Brand String	Info-only. Intel(R) Core, ...	Shows what CPU is booting the system.
CPU Frequency	Info-only. XXXX MHz	Shows CPU frequency.
Total Memory	Info-only. XXXX MB (DDR4)	Shows total memory size used on the motherboard and memory type.
Memory Frequency	Info-only. XXXX MHz	Shows memory frequency.
System Date	MM/DD/YYYY	For configuring/showing system date. When setting the Date, use <Tab> key to switch between Date elements.
System Time	HH:MM:SS	For configuring/showing system time. When setting the Time, use <Tab> key to switch between Time elements.
Access Level	Info-only. Administrator/User	It shows what access level is used to enter BIOS setup menu.

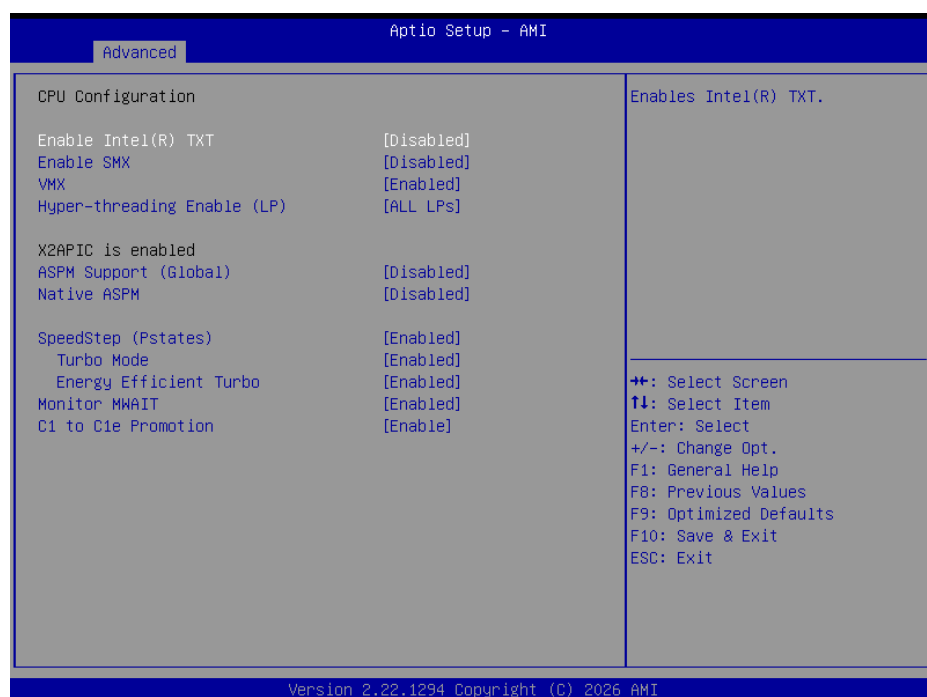
7.3 Advanced Menu

This menu contains the Advance settings.



BIOS Item	Options	Description
1CPU Configuration	Sub-Menu	For Cpu setting
2Power Management	Sub-Menu	For Power Management
3BIOS Watchdog Time	Sub-Menu	For BIOS Watchdog Time setting
4Super IO Configuration	Sub-Menu	For Super IO Configuration
5Serial Port Console Redirection	Sub-Menu	For configuring serial console
6Hardware Monitor	Sub-Menu	For Hardware Monitor
7Trusted Computing	Sub-Menu	For TPM settings
8NVMe Configuration	Sub-Menu	For NVMe Device Information
9Lan Configuration	Sub-Menu	For Lan settings
10USB Configuration	Sub-Menu	For USB settings
11Network Stack Configuration	Sub-Menu	For configuring Network Stack.
12All Cpu Information	Sub-Menu	
13Intel(R) Ethernet Contoller I226-V	Sub-Menu	Onboard Ethernet controller configuration loaded by EFI driver. The setup page is designed by Intel and is shown when running the Ethernet EFI driver. It is related to the "Network" settings on the Boot setup page.
14Intel(R) I210 Gigabit Network Connect	Sub-Menu	Onboard Ethernet controller configuration loaded by EFI driver. The setup page is designed by Intel and is shown when running the Ethernet EFI driver. It is related to the "Network" settings on the Boot setup page.

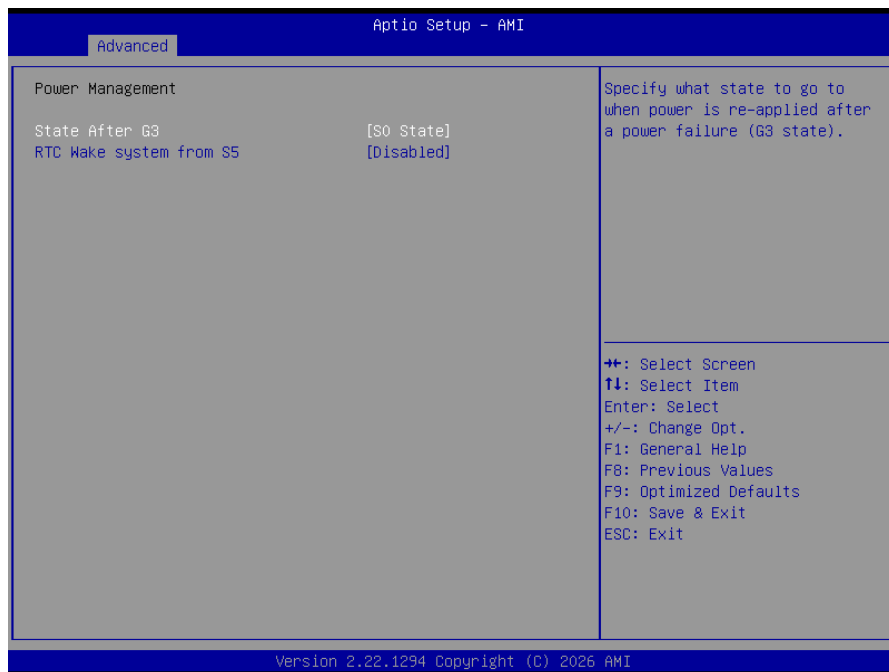
7.3.1 CPU Configuration



BIOS Item	Options	Description
Enable Intel(R) TXT	Disabled Enabled	Enables Intel(R) TXT.
Enable SMX	Disabled Enabled	Enables Safer Mode Extensions.
VMX	Disabled Enabled	Enables the <u>Vanderpool</u> Technology, takes effect after reboot.
Hyper-Threading Enable (LP)	All LPs Single LP	Enable Logical processor (software Method to Enable/Disable Logical Processor threads)
X2APIC is enable	Info	
ASPM Support (Global)	Disabled Enabled	This option can disable ASPM support for all PCIe root ports.
Native ASPM	Disabled Enabled	Enabled - OS Controlled ASPM, Disabled - ASPM Off, AUTO - BIOS Controlled ASPM
SpeedStep (PStates)	Disabled Enabled	Enable/Disable EIST (P-States)
Turbo mode	Disabled Enabled	Enable/Disable processor <u>Turbo</u> Mode
Energy Efficient Turbo	Disabled Enabled	Enable/Disable Energy Efficient <u>Turbo</u> . Enable: MSR 0x1FC Bit[19] = 0 ,Disable: MSR 0x1FC Bit[19] =1.
Monitor MWAIT	Disabled Enabled	Allows Monitor and MWAIT instructions.

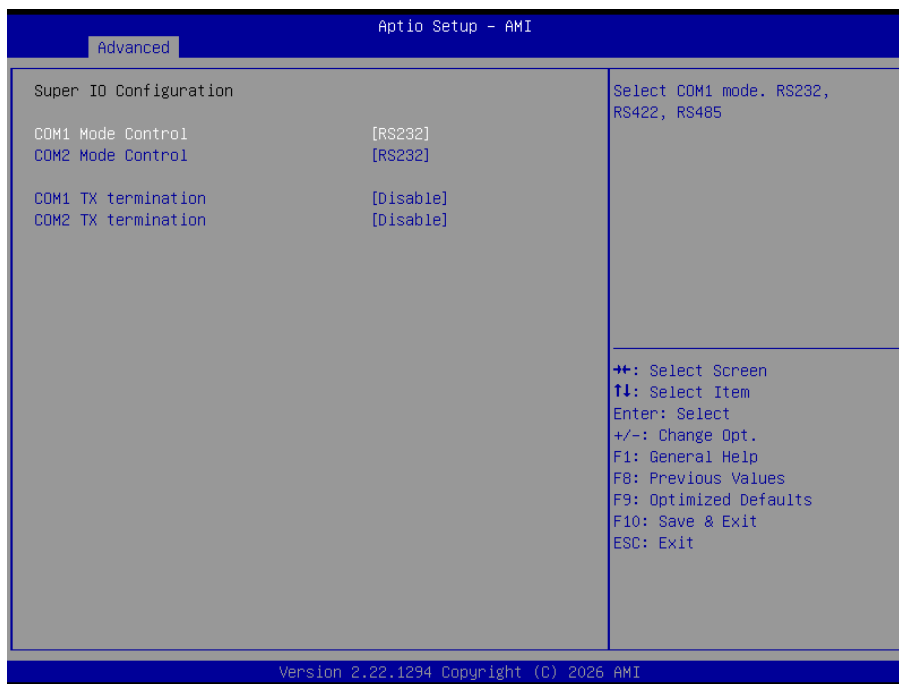
C1 to C1e Promotion	Disabled Enabled	CPU will promote C1 request to C1e state.
---------------------	----------------------------	---

7.3.2 Power Management



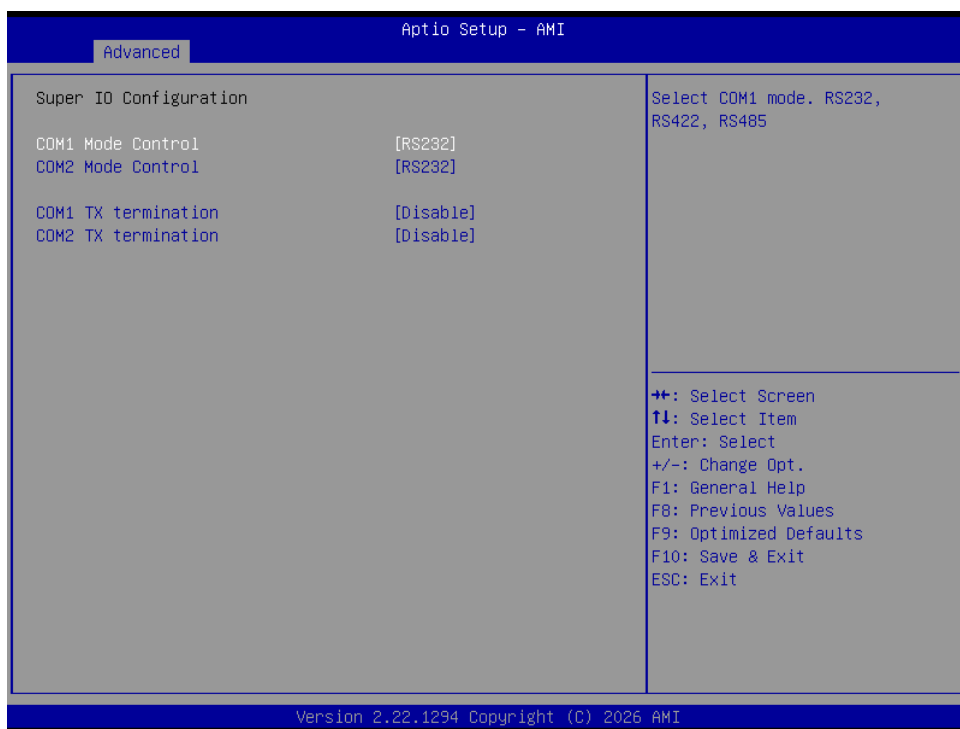
BIOS Item	Options	Description
State After G3	S0 State Disabled S5 State Last State	To enable or disable WOL
RTC Wake system from S5	Disabled Enabled Enable and Set wake on time	Enable: Enable Wake on RTC feature but not set RTC wake up value(used for set RTC value by OS tool). Disable: Disable Wake on RTC feature. Enabled and set wake time: Enable System wake on alarm event and set wake on the day::hr::min::sec specified.
Wake Up hour	0	
Wake Up minute	0	
Wake Up second	0	

7.3.3 Super IO Configuration



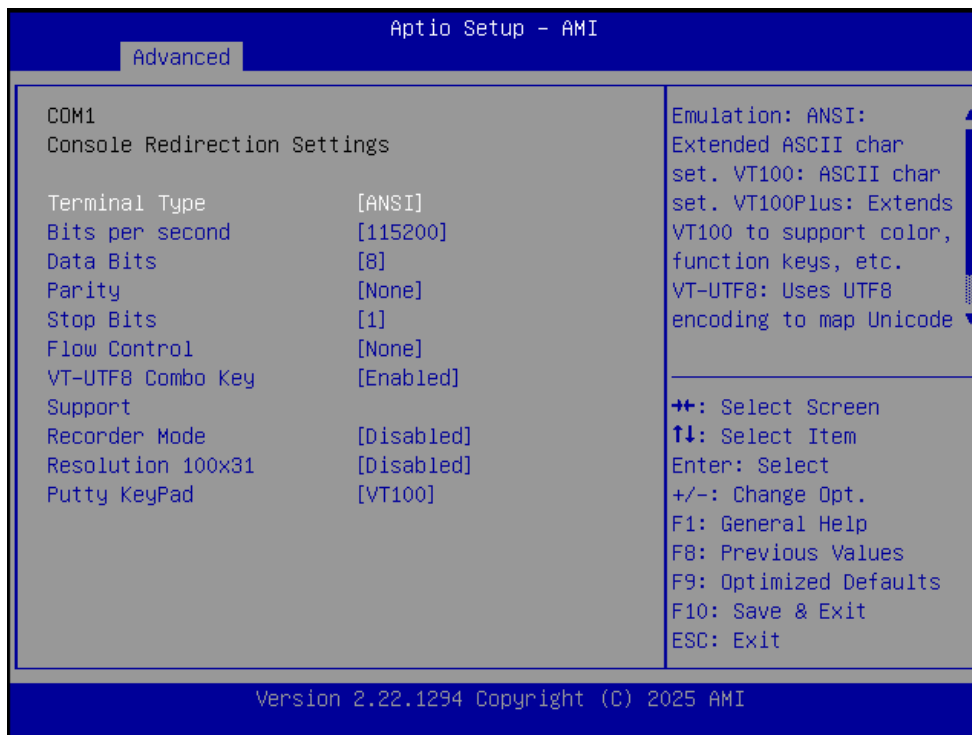
BIOS Item	Options	Description
COM1 Mode Control	RS232 RS422 RS485	Select COM1 mode. RS232, RS422, RS485
COM2 Mode Control	RS232 RS422 RS485	Select COM2 mode. RS232, RS422, RS485
Com1 TX termination	Disabled Enabled	COM1 TX termination Enable/Disable
Com2 TX termination	Disabled Enabled	COM2 TX termination Enable/Disable

7.3.4 Serial Port Console Redirection



BIOS Item	Options	Description
Console Redirection	Enabled Disabled	Enable or disable serial port console redirection function.
Console Redirection Settings	Sub-Menu	For configuring serial port settings when console redirection function is enabled.

7.3.4.1 Console Redirection Settings



BIOS Item	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	Configure type of console emulation. Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speed.
Data Bits	7 8	Configure the number of data bits in each transmitted or received serial character for both serial ports.
Parity	None Even Odd Mark Space	Configures if parity bit is generated (transmit data) or checked. A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	1 2	Configures the number of stop bits transmitted and received in each serial character for both serial ports. Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	None Hardware RTS/CTS	Configures flow control for console redirection. Hardware flow control uses RTC/CTS.
VT-UTF8 Combo Key Support	Disabled Enabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled Enabled	This mode only text will be sent
Resolution 100x31	Disabled Enabled	To enable or disable extended terminal resolution
Putty Keypad	VT100	Select Function Key and keypad on Putty

7.3.5 Trusted Computing

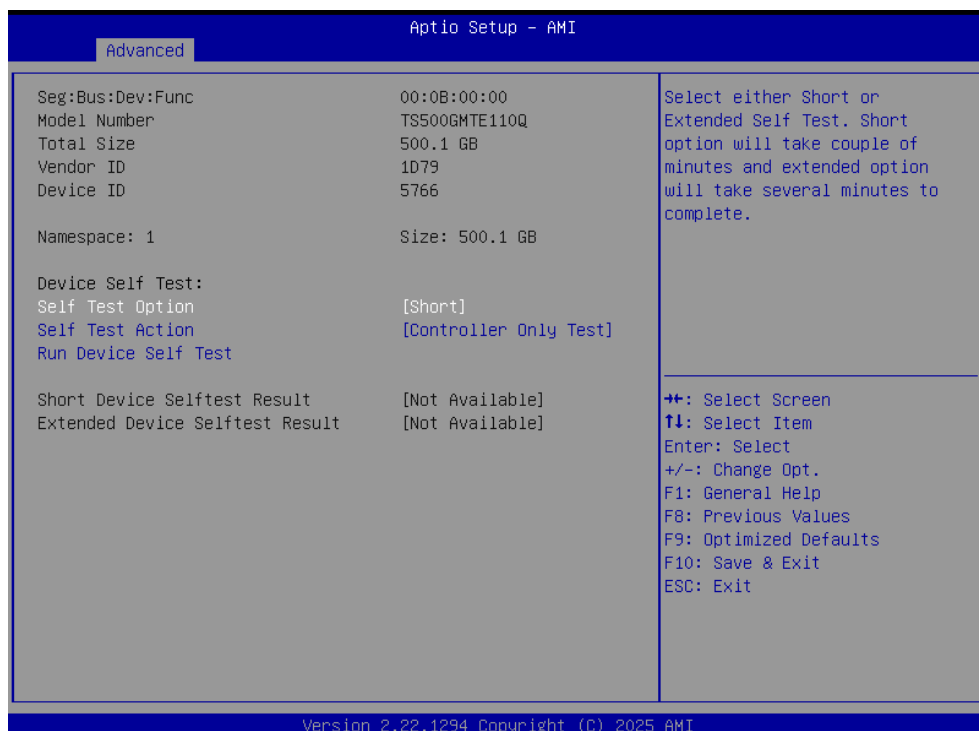


BIOS Item	Options	Description
Security Device Support	Enabled Disabled	Security Device Support

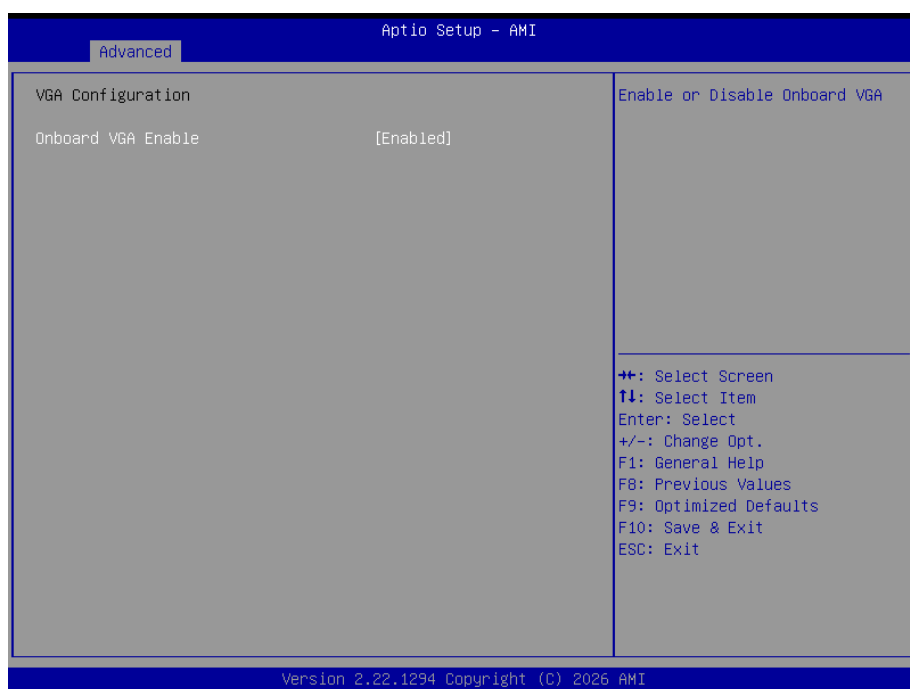
7.3.6 NVMe Configuration



BIOS Item	Options	Description
NVME Info	Sub-Menu	Dynamically generated information for NVME



7.3.7 VGA Configuration



BIOS Item	Options	Description
Onboard VGA Enable	Disabled Enabled	Enable or Disable onboard VGA

7.3.8 LAN Configuration

Aptio Setup - AMI

Advanced

LAN Configuration		Enable/Disable LAN 1 Controller
Onboard LAN1 Control (i226)	[Enabled]	
Onboard LAN2 Control (i210)	[Enabled]	
		++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

Version 2.22.1294 Copyright (C) 2026 AMI

BIOS Item	Options	Description
Onboard LAN1 control (i226)	Enabled Disabled	Enable/Disable Lan 1 Controller
Onboard LAN2 control (i210)	Enabled Disabled	Enable/Disable Lan 2 Controller

7.3.9 USB Configuration

Aptio Setup - AMI

Advanced

USB Configuration		
USB Module Version	40	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Controllers: 1 XHCI USB Devices: 9 Drives, 2 Keyboards, 1 Mouse, 1 Hub		
XHCI Hand-off	[Enabled]	++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
USB Mass Storage Driver Support	[Enabled]	
USB hardware delays and time-outs: USB transfer time-out [20 sec] Device reset time-out [20 sec] Device power-up delay [Auto]		
Mass Storage Devices: ADLINK Virtual CDROM0 1.00 [Auto] ADLINK Virtual HDisk0 1.00 [Auto] KingstonDT microDuo 3C PMAP [Auto] ADLINK Virtual CDROM1 1.00 [Auto] ADLINK Virtual CDROM2 1.00 [Auto] ADLINK Virtual CDROM3 1.00 [Auto] ADLINK Virtual HDisk1 1.00 [Auto]		

Version 2.22.1294 Copyright (C) 2026 AMI

BIOS Item	Options	Description
XHCI Hand-off	Enabled Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled Disabled	Configure the USB Mass Storage Devices.
USB transfer time-out	1 Sec 5Sec 10 Sec 20 Sec	The time-out value for Control, Bulk, and Interrupt transfers
Device reset time-out	10 Sec 20 Sec 30 Sec 40 Sec	USB mass storage device Start Unit command time-out.
Device power-up delay	Auto Manual	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 <u>ms</u> , for a Hub port the delay is taken from Hub descriptor.

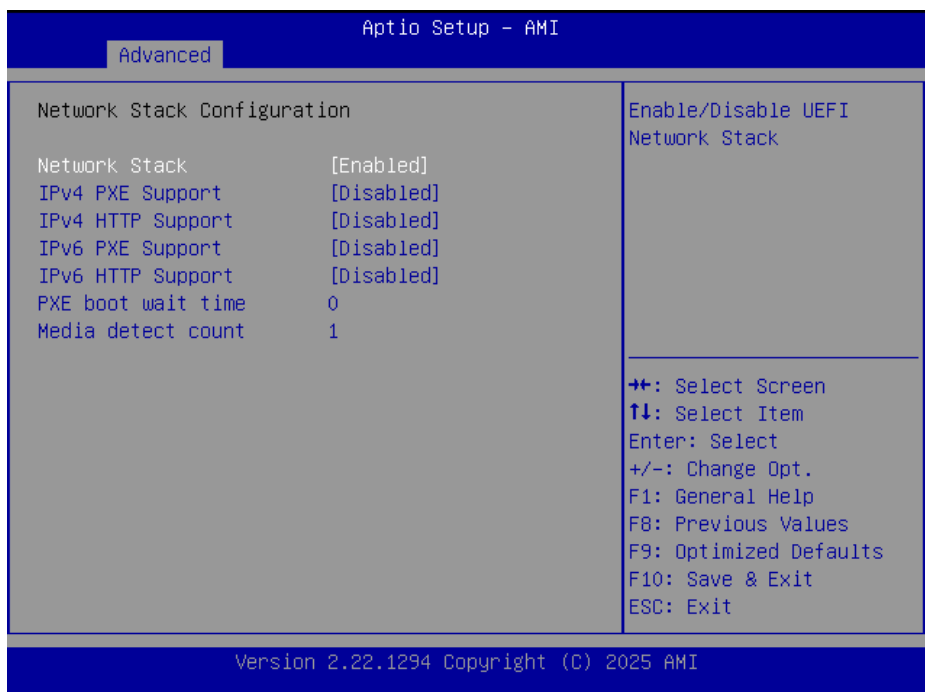
7.3.10 Miscellaneous



BIOS Item	Options	Description
PCIE Resizable BAR Support	Disabled Enabled	Enable/Disable PCIE Resizable BAR Support
Resizable BAR Max size	numeric	Set platform limit for max size to pick from Resizable BAR Capability register. Decimal value 'n' is interpreted as $2^{(n+20)}$, which means 0=>1MB, 1=>2MB, 2=>4MB, 3=>8MB, etc.

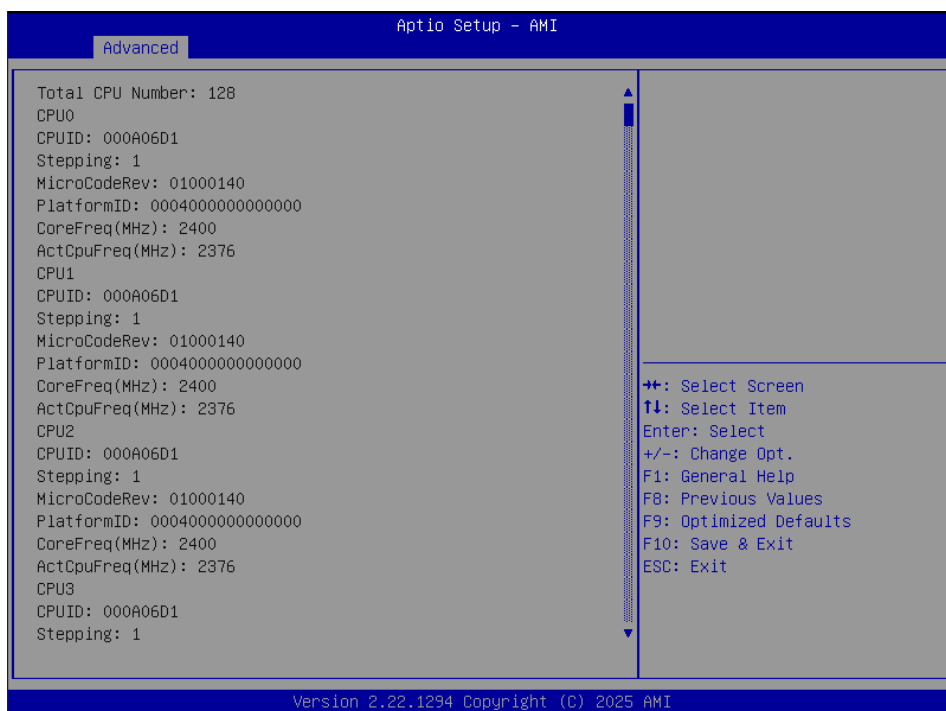
		Maximum possible to set is half of processor address width, i.e. address width - 1.
--	--	---

7.3.11 Network Stack Configuration

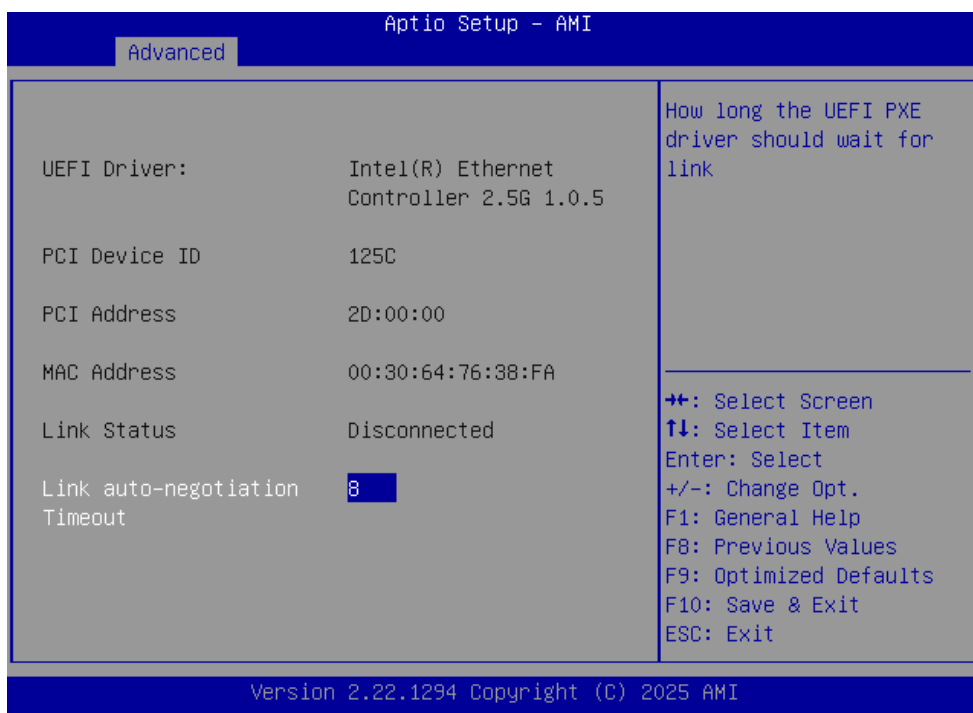


BIOS Item	Options	Description
Network stack	Enabled Disabled	Enable/Disable UEFI Network Stack
IPv4 PXESupport	Enabled Disabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	Enabled Disabled	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXESupport	Enabled Disabled	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv4 HTTP Support	Enabled Disabled	Enable/Disable IPv6 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
PXE Boot wait time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value
Media detect count	1	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

7.3.12 All CPU Information

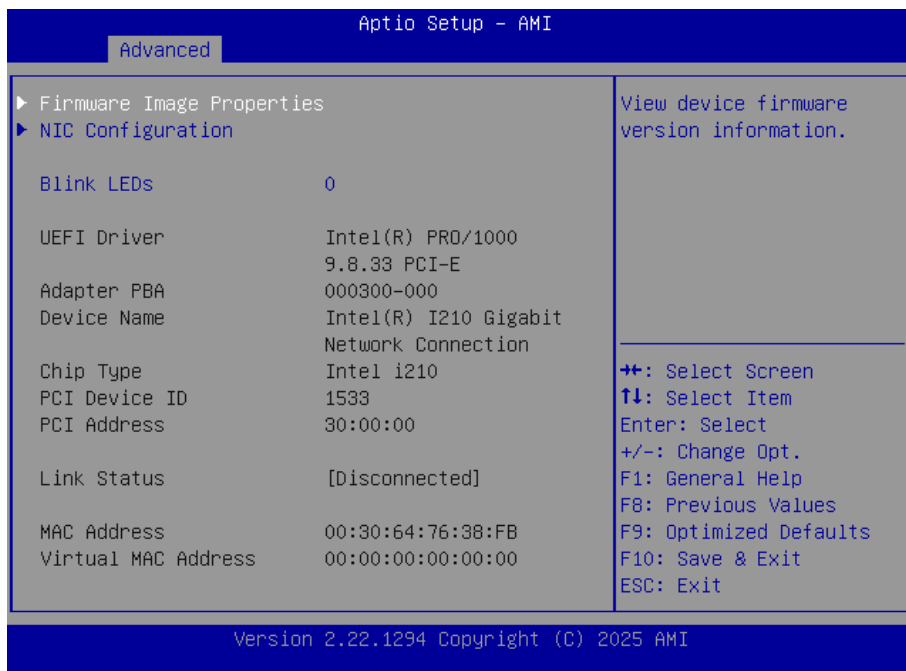


7.3.13 Intel(R) Ethernet Controller I226-V



BIOS Item	Options	Description
Link auto-negotiation Timeout	8	How long the UEFI PXE driver should wait for link

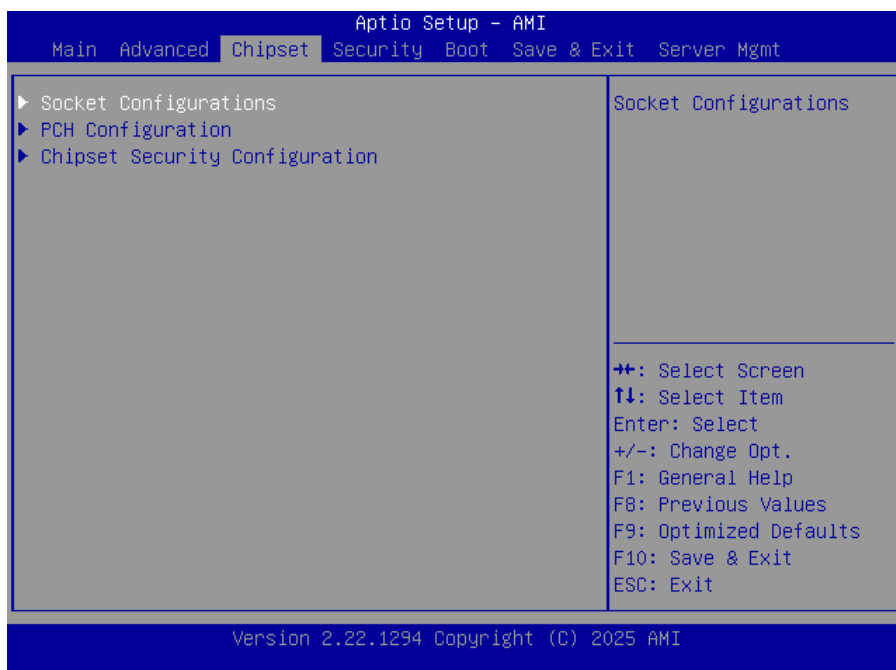
7.3.14 Intel(R) I210 Gigabit Network Connect



BIOS Item	Options	Description
Firmware Image Properties	Sub-Menu	View device firmware version information
NIC Configuration	Sub-Menu	
Blink LEDs	0	

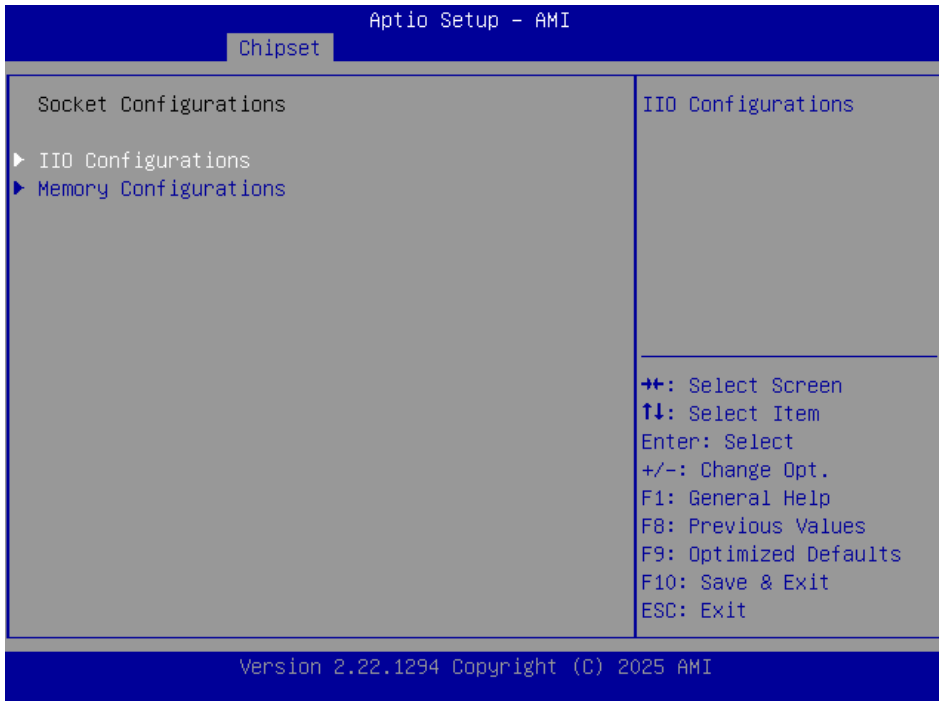
7.4 Chipset Menu

This menu contains the Chipset settings.



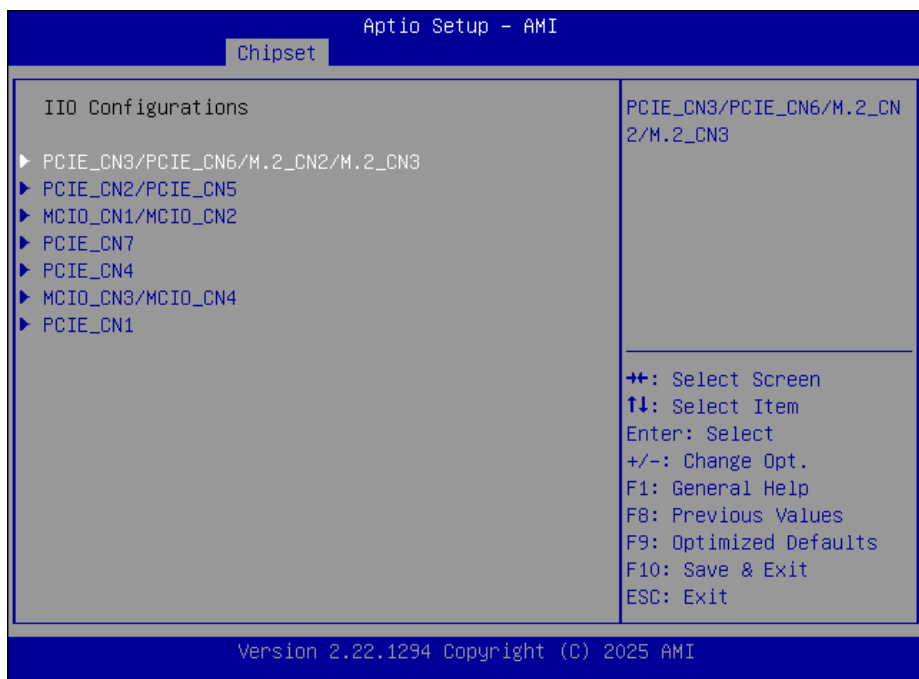
BIOS Item	Options	Description
Socket Configurations	Sub-Menu	For Socket Configurations.
PCH Configurations	Sub-Menu	For PCH Configurations.
Chipset Security Configurations	Sub-Menu	For Chipset Security Configurations

7.4.1 Socket Configuration



BIOS Item	Options	Description
IIO Configurations	Sub-Menu	For IIO Configurations
Memory Configurations	Sub-Menu	For Memory Configurations

7.4.1.1 IIO Configurations



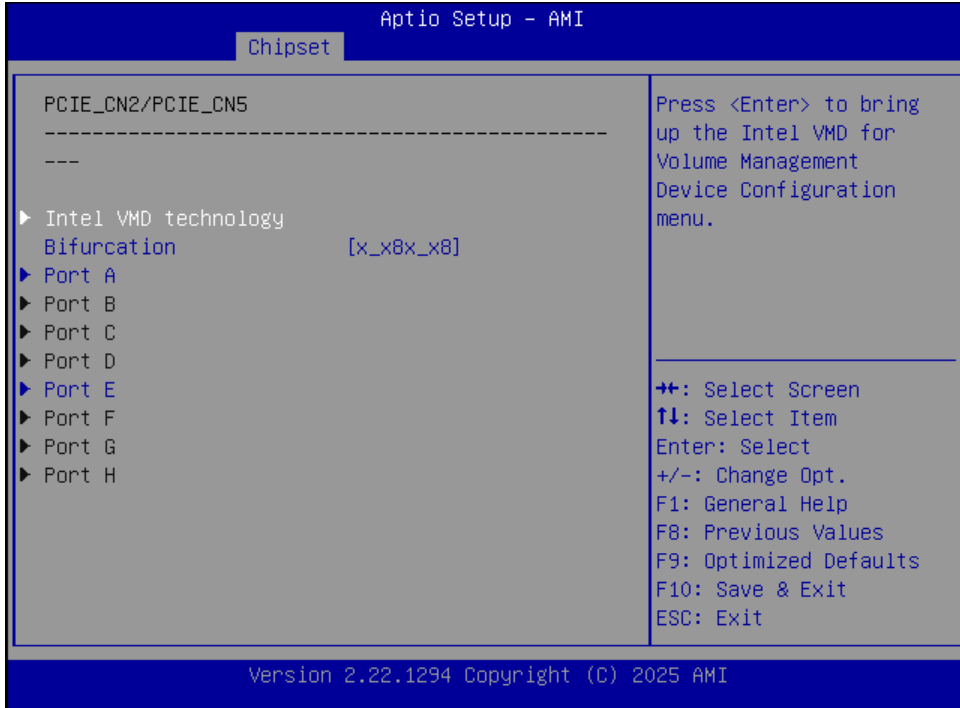
BIOS Item	Options	Description
PCIE_CN3/PCIE_CN6/ M.2_CN2/M.2_CN3	Sub-Menu	For PCIE_CN3/PCIE_CN6/ M.2_CN2/M.2_CN3
PCIE_CN2/PCIE_CN5	Sub-Menu	For PCIE_CN2/PCIE_CN5
MCIO_CN1/MCIO_CN2	Sub-Menu	For MCIO_CN1/MCIO_CN2
PCIE_CN7	Sub-Menu	For PCIE_CN7
PCIE_CN4	Sub-Menu	For PCIE_CN4
MCIO_CN1/MCIO_CN2	Sub-Menu	For MCIO_CN1/MCIO_CN2
PCIE_CN1	Sub-Menu	For PCIE_CN1

7.4.1.1.1 PCIE_CN3/PCIE_CN6/M.2_CN2/M.2_CN3



BIOS Item	Options	Description
Intel VMD technology	Sub-Menu	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCx4 The port can further be x2x2
Port A	Sub-Menu	
Port B	Sub-Menu	
Port C	Sub-Menu	
Port D	Sub-Menu	
Port E	Sub-Menu	
Port F	Sub-Menu	
Port G	Sub-Menu	
Port H	Sub-Menu	

7.4.1.1.2 PCIE_CN2/PCIE_CN5



BIOS Item	Options	Description
Intel VMD technology	Sub-Menu	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2
Port A	Sub-Menu	
Port B	Sub-Menu	
Port C	Sub-Menu	
Port D	Sub-Menu	

Port E	Sub-Menu	
Port F	Sub-Menu	
Port G	Sub-Menu	
Port H	Sub-Menu	

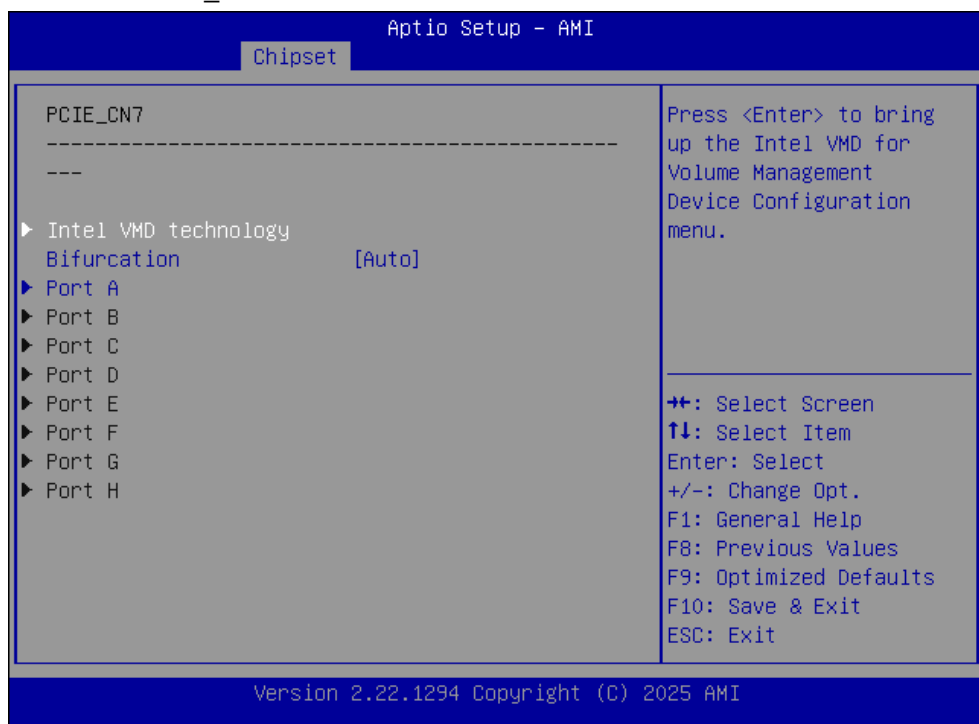
7.4.1.1.3 MCIO_CN1/MCIO_CN2



BIOS Item	Options	Description
Intel VMD technology	Sub-Menu	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2

	x4x2x2x2x2x2x2	
Port A	Sub-Menu	
Port B	Sub-Menu	
Port C	Sub-Menu	
Port D	Sub-Menu	
Port E	Sub-Menu	
Port F	Sub-Menu	
Port G	Sub-Menu	
Port H	Sub-Menu	

7.4.1.1.4 PCIE_CN7



BIOS Item	Options	Description
Intel VMD technology	Sub-Menu	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxCxA The port can further be x2x2

	x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2	
Port A	Sub-Menu	
Port B	Sub-Menu	
Port C	Sub-Menu	
Port D	Sub-Menu	
Port E	Sub-Menu	
Port F	Sub-Menu	
Port G	Sub-Menu	
Port H	Sub-Menu	

7.4.1.1.5 PCIE_CN4



BIOS Item	Options	Description
Intel VMD technology	Sub-Menu	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2
Port A	Sub-Menu	
Port B	Sub-Menu	
Port C	Sub-Menu	
Port D	Sub-Menu	
Port E	Sub-Menu	
Port F	Sub-Menu	
Port G	Sub-Menu	
Port H	Sub-Menu	

7.4.1.1.6 MCIO_CN3/MCIO_CN4



BIOS Item	Options	Description
Intel VMD technology	Sub-Menu	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2
Port A	Sub-Menu	
Port B	Sub-Menu	
Port C	Sub-Menu	
Port D	Sub-Menu	
Port E	Sub-Menu	

Port F	Sub-Menu	
Port G	Sub-Menu	
Port H	Sub-Menu	

7.4.1.1.7 PCIE_CN1



BIOS Item	Options	Description
Intel VMD technology	Sub-Menu	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCx4 The port can further be x2x2

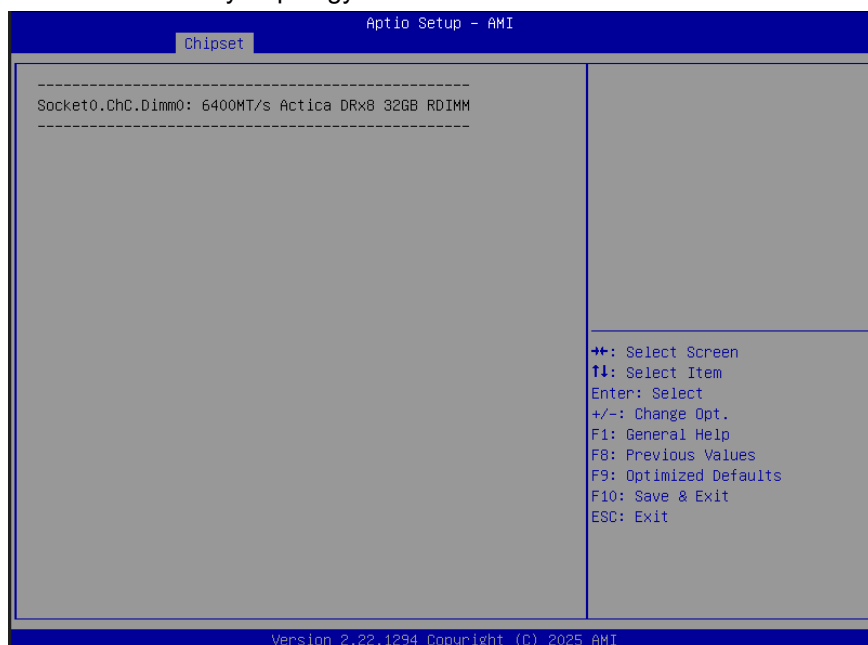
Port A	Sub-Menu	
Port B	Sub-Menu	
Port C	Sub-Menu	
Port D	Sub-Menu	
Port E	Sub-Menu	
Port F	Sub-Menu	
Port G	Sub-Menu	
Port H	Sub-Menu	

7.4.1.2 Memory Configurations

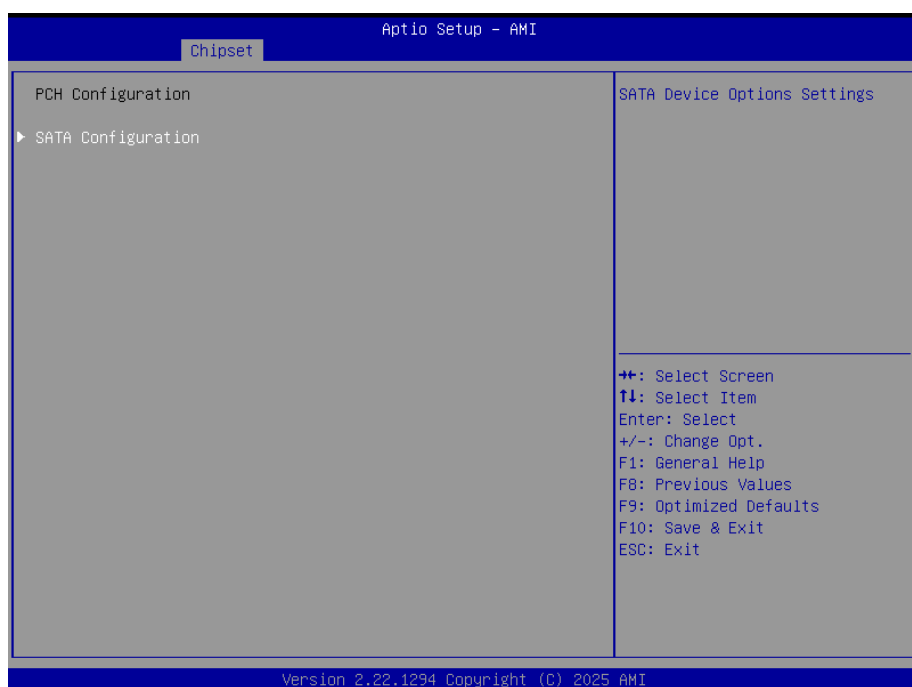


BIOS Item	Options	Description
Host Memory Frequency	Auto 4800 5200 5600 6000 6400	Maximum Host DDR Memory Frequency Selections in MT/s. If the "AUTO" option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Note: For MRDIMM, DDR DRAM frequency is half of Host frequency
Memory Topology	Sub-Menu	Displays memory topology with Dimm population information

7.4.1.2.1 Memory Topology

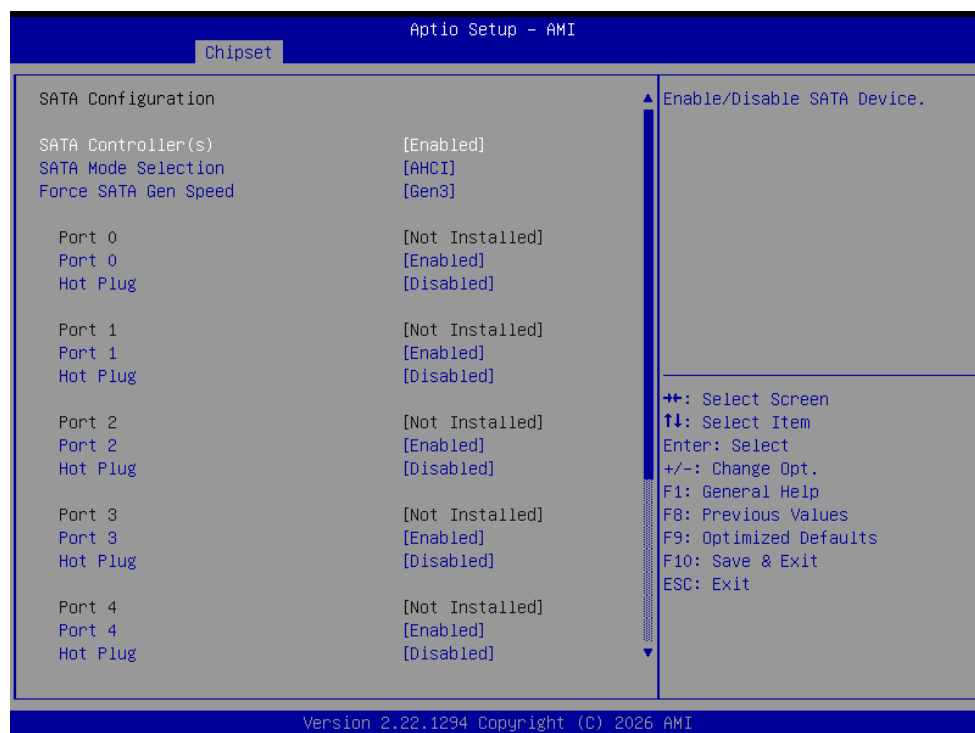


7.4.2 PCH Configurations



BIOS Item	Options	Description
SATA Configuration	Sub-Menu	SATA Device options Settings

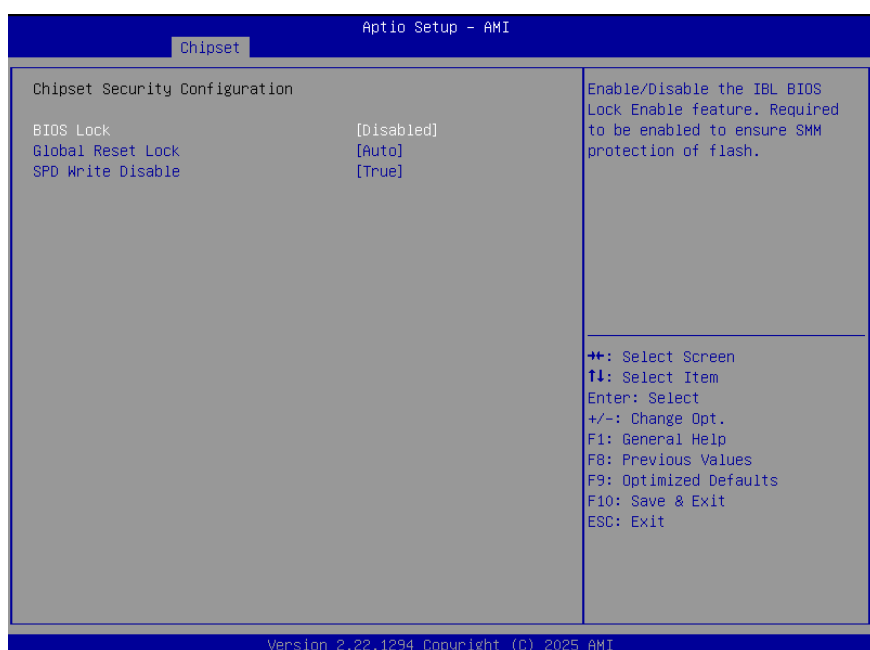
7.4.2.1 SATA Configuration



BIOS Item	Options	Description
SATA Controller(s)	Enabled Disabled	Enable/Disable SATA Device.
SATA Mode Selection	AHCI RAID	Determines how SATA controller(s) operate.
Force SATA Gen Speed	Gen1 Gen2 Gen3	Changes SATA Gen Speed for port.
Port 0	Not Installed	Software Preserve
Port 0	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.
Port 1	Not Installed	Software Preserve
Port 1	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.
Port 2	Not Installed	Software Preserve
Port 2	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.
Port 3	Not Installed	Software Preserve
Port 3	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.
Port 4	Not Installed	Software Preserve
Port 4	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.
Port 5	Not Installed	Software Preserve

Port 5	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.
Port 6	Not Installed	Software Preserve
Port 6	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.
Port 7	Not Installed	Software Preserve
Port 7	Enabled Disabled	Enable or Disable SATA Port
Hot Plug	Enabled/ Disabled	Designates this port as Hot Pluggable.

7.4.3 Chipset Security Configurations



BIOS Item	Options	Description
BIOS Lock	Disabled Enabled	Enable/Disable the IBL BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.
Global Reset Lock	Disable Enable Auto	Enable/Disable locking global host reset
SPD Write Disable	True False	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.

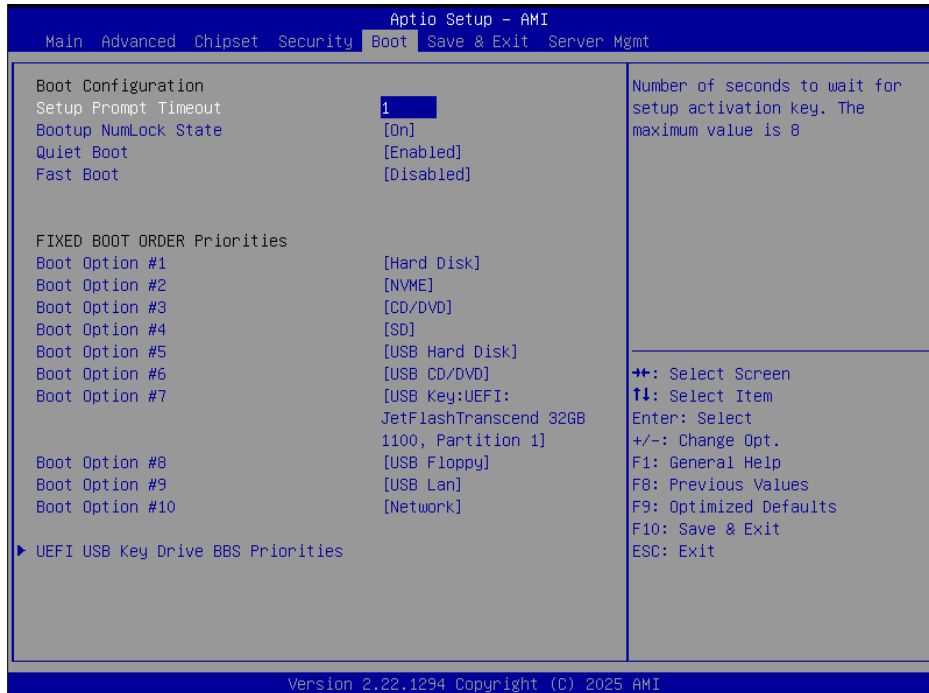
7.5 Security Menu



BIOS Item	Options	Description
Administrator Password	Enter to set password	Configure/Clear Administrator Password. When pressing enter, a menu will be popped up for creating new password. When password installed, press enter without inputting password, it will clear password.
User Password	Enter to set password	Configure/Clear User Password. When pressing enter, a menu will be popped up for creating new password. When password installed, press enter without inputting password, it will clear password.
Secure Boot	Sub-Menu	Secure Boot Menu. Default is Disabled.

7.6 Boot Menu

This menu contains the settings for bootable devices in the system.



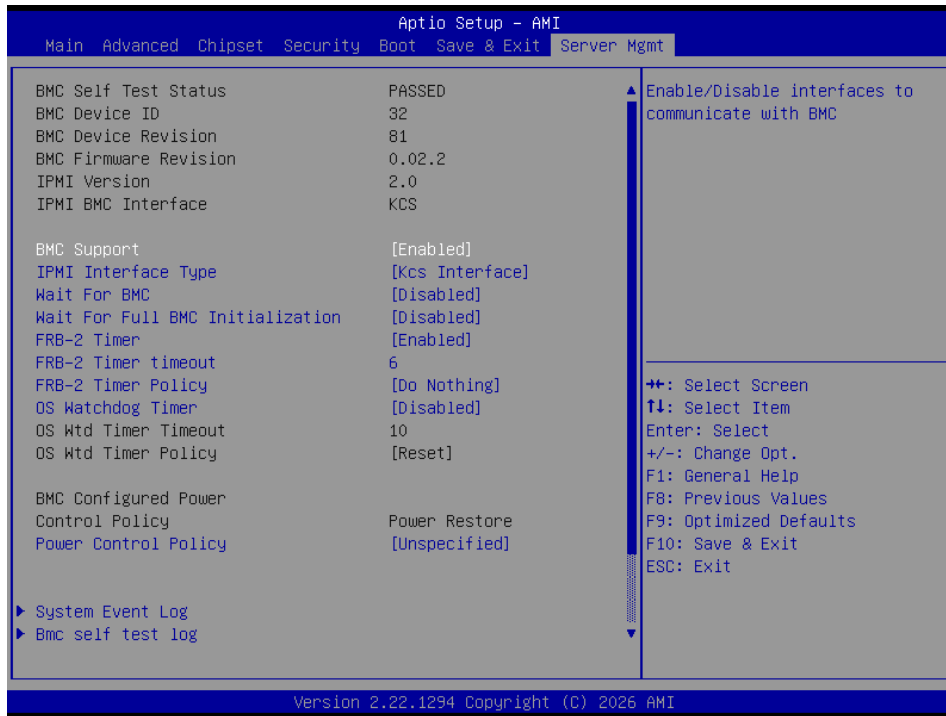
BIOS Item	Options	Description
Setup Prompt Timeout	1	Number of seconds to wait for setup activation
Bootup NumLock State	On Off	Select the keyboard NumLock state
Quiet Boot	Enabled Disabled	Enables or disables Quiet Boot option
Fast Boot	Disable Enable	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
Boot Option #1 ~ #9	#1: Hard Disk #2: CD/DVD #3: SD #4: USB Hard Disk #5: USB CD/DVD #6: USB Key #7: USB Floppy #8: USB LAN #9: Network	For boot priority setting.
XXXX Drive BBS Priorities	Sub-Menu	When the bootable device is attached to system and found by BIOS, it will be listed at boot option #. If there are many devices with the same device type found, it can set priority among these devices through this sub-menu.

7.7 Save & Exit Menu



BIOS Item	Options	Description
Save Changes and Exit	Enter	Save changed settings and exit BIOS setup utility.
Discard Changes and Exit	Enter	Skip changed setting and exit BIOS setup utility.
Save Changes and Reset	Enter	Save all changed settings and let system do reset to boot system.
Discard Changes and Reset	Enter	Discard all changed settings and let system do reset to boot system.
Save Changes	Enter	Save all changed settings.
Discard Changes	Enter	Discard changes done so far to any of the setup options.
Restore Default	Enter	Load the default made when BIOS was built.
Save as User Default	Enter	Save all changed done so far as User Defaults.
Restore User Default	Enter	Load the default that user save as user defaults.
Boot Override	Info-only	

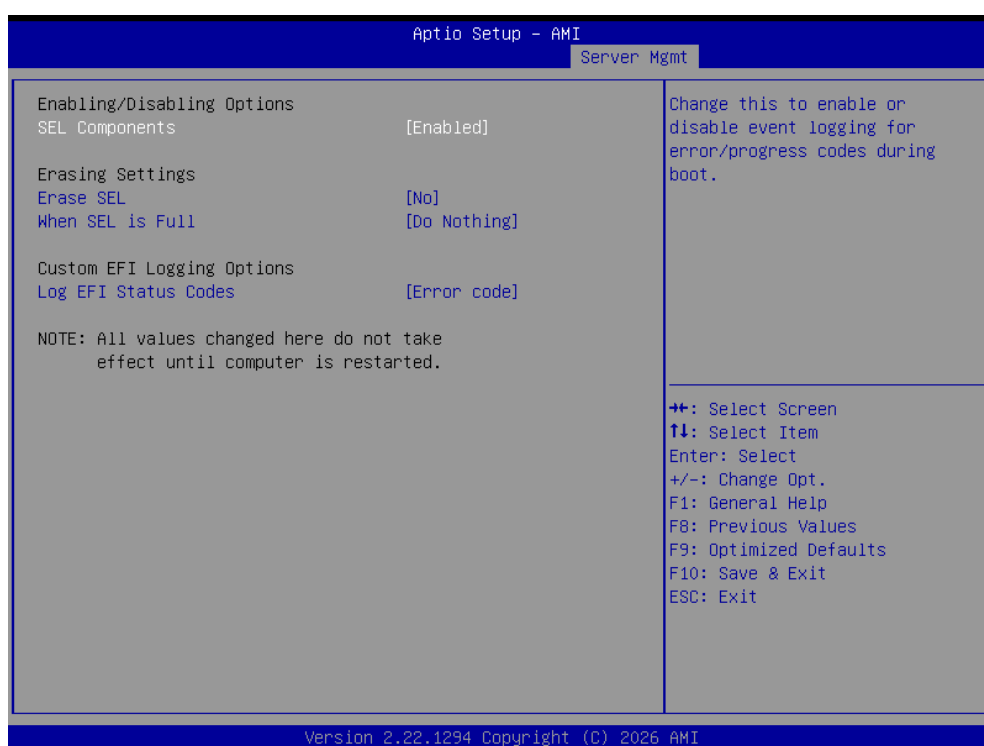
7.8 Server Management



BIOS Item	Options	Description
BMC Support	Enabled Disabled	Enable/Disable interfaces to communicate with BMC.
IPMI Interface Type	Kcs Interface	Type of Interface to communicate BMC from HOST.
Wait For BMC	Enabled Disabled	Wait for BMC response for specified time out. In PILOT II, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize HOST to BMC interfaces.
Wait For Full BMC Initialization	Enabled Disabled	Based on above rules, additional provide user can manually increase the waiting time on different platforms if necessary.
FRB-2 Timer	Enabled Disabled	Enable/Disable Fault Resilient Boot level 2 timer in POST stage.
FRB-2 Timer timeout	6	Enter value between 1 to 30 min for FRB-2 timer expiration.
FRB-2 Timer Policy	Do Nothing Reset Power Down Power Cycle	Configure how the system should respond if the FRB-2 timer expires. Not available if FRB-2 timer is disabled.
OS Watchdog Timer	Enabled Disabled	If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.
OS Wtd Timer Timeout	10	Enter the value between 1 to 30 min for OS Boot Watchdog Timer expiration. Not available if OS Boot Watchdog Timer is disabled.

OS Wtd Timer Policy	Do Nothing Reset Power Down Power Cycle	Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.
BMC Configured Power Control Policy	Power Restore	
Power Control Policy	Do Not Power Up Last Power State Power Restore Unspecified	Configure how the system should respond if AC power is lost, reset not required as selected power policy will be set in BMC when policy is saved.

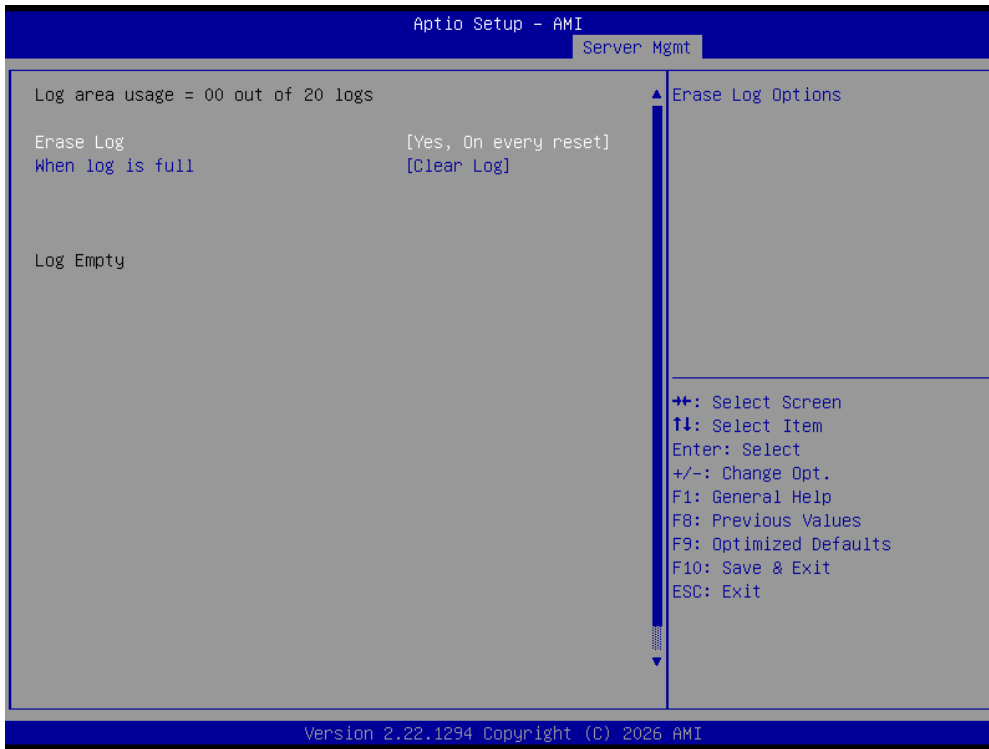
7.8.1 System Event Log



BIOS Item	Options	Description
SEL Components	Enabled Disabled	Enable/Disable event logging for error/progress codes during boot.
Erase SEL	No Yes, on next reset Yes, on every reset	Choose options for erasing SEL.
When SEL is Full	Do Nothing Erase Immediately Delete Oldest Record	Choose options for reactions to a full SEL.
Log EFI Status Codes	Disabled Both Error code	Choose options for logging EFI Status Codes.

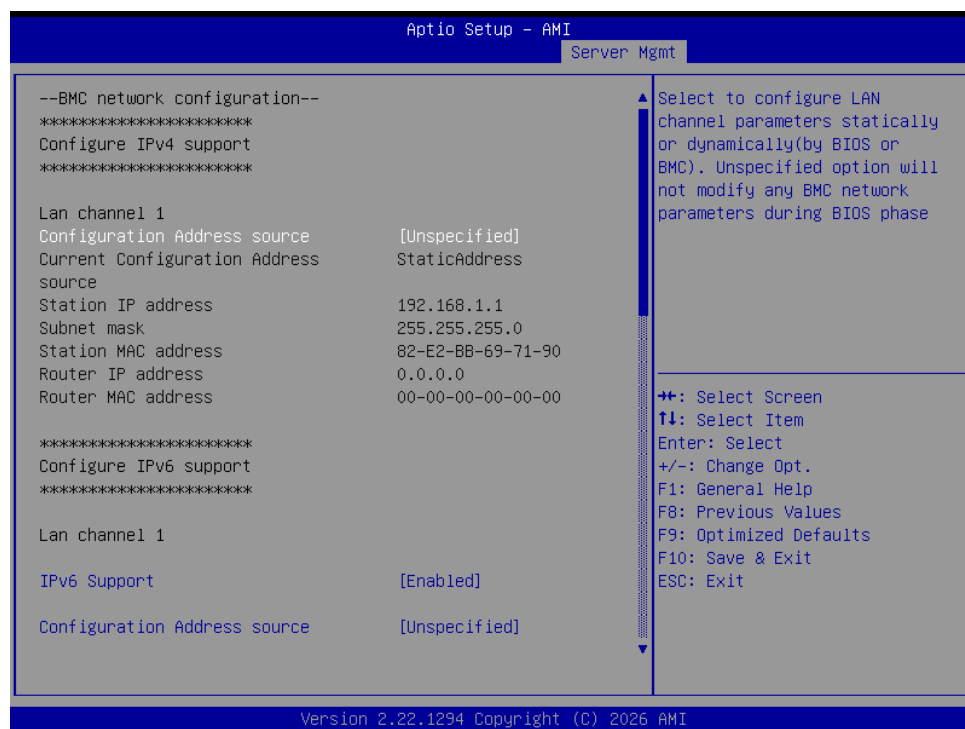
	Progress code	
--	---------------	--

7.8.2 BMC Self Test Log



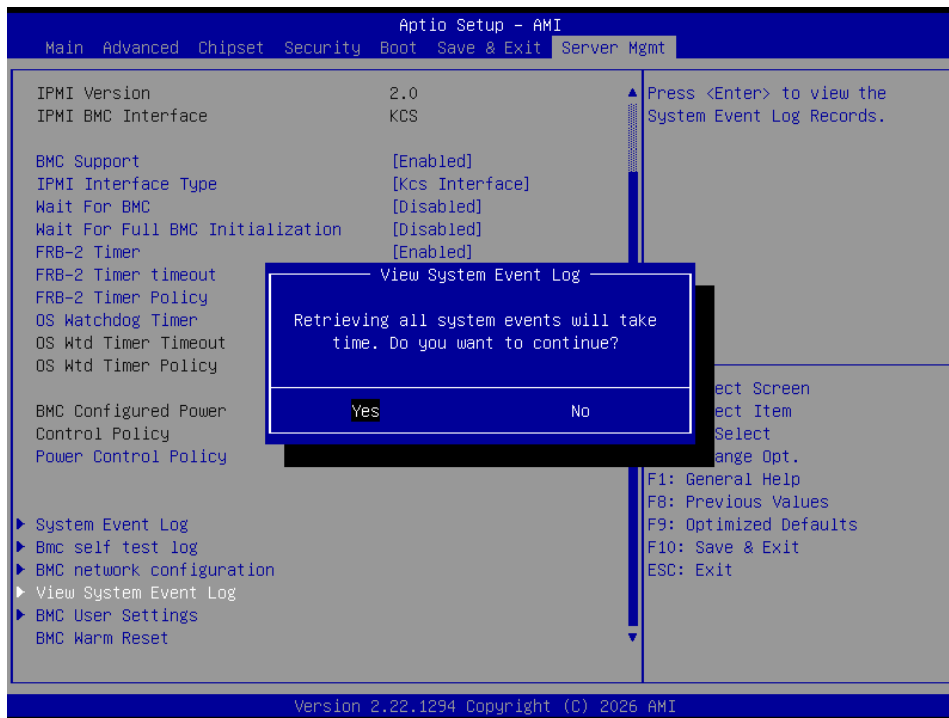
BIOS Item	Options	Description
Erase Log	Yes, on every reset No	Choose options for erasing logs.
When log is full	Clear Log Do not log any more	Choose options for reactions to a full log.

7.8.3 BMC Network Configuration



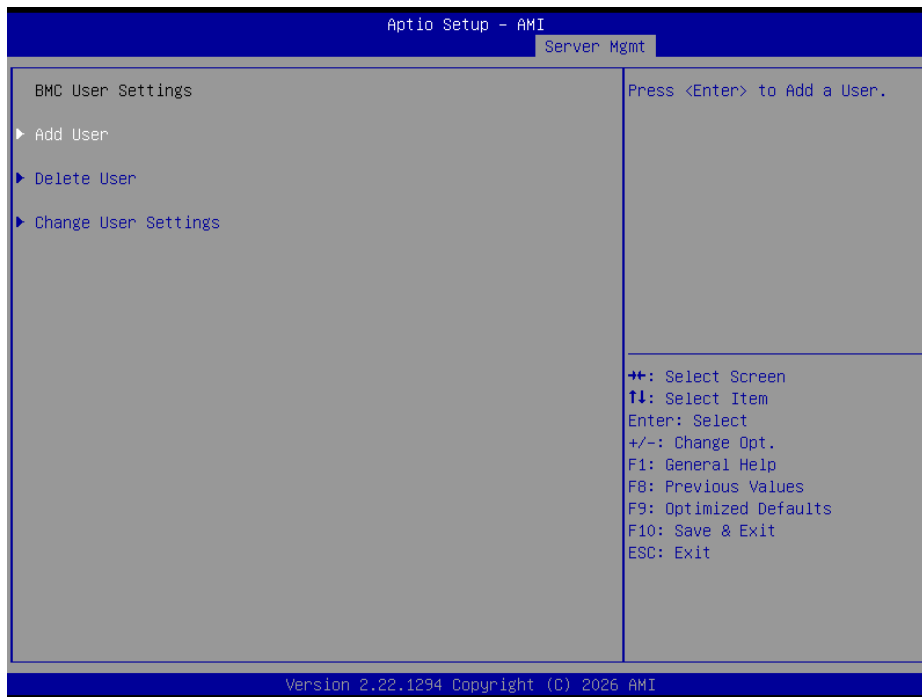
BIOS Item	Options	Description
IPv4 Configuration Address source	Unspecified Static DynamicBmcDhcp DynamicBmcNonDhcp	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.
IPv6 Support	Enabled Disabled	Enable/Disable LAN1 IPv6 Support
IPv6 Configuration Address source	Unspecified Static DynamicBmcDhcp DynamicBmcNonDhcp	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.
IPv6 Configuration Router Lan1 Address source	Unspecified Static DynamicBmcDhcp	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
VLAN Support	Enabled Disabled Unspecified	Enable VLAN Support to specify the 802.1q VLAN ID

7.9 View System Event Log



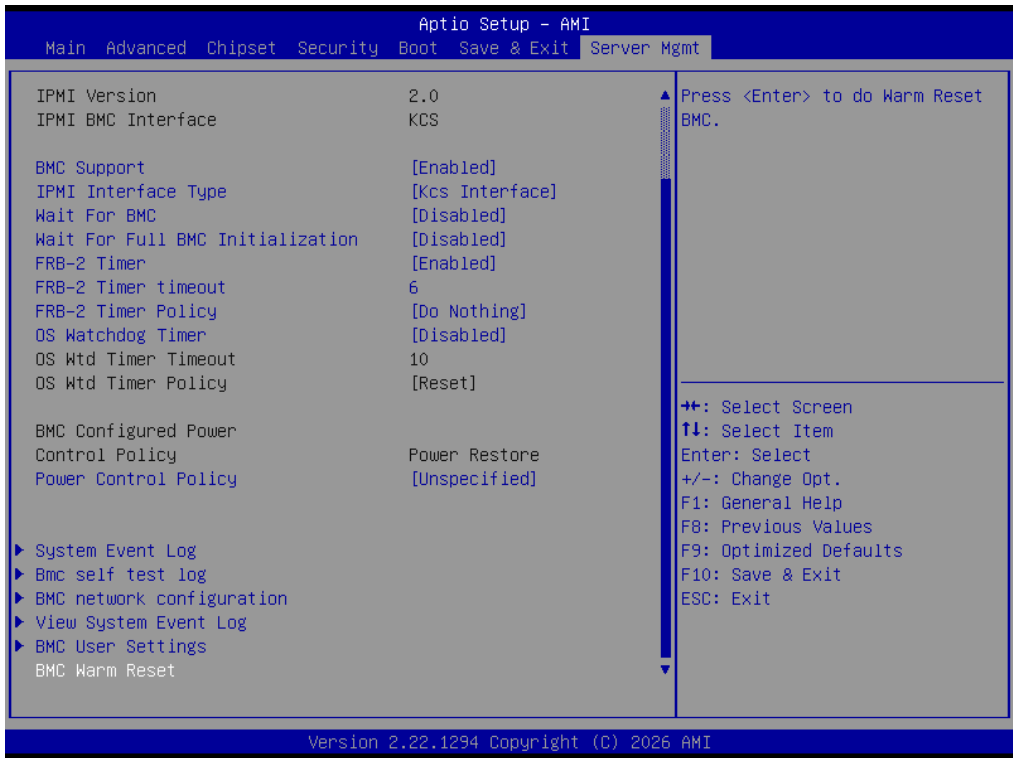
BIOS Item	Options	Description
View System Event Log	Yes	Retrieving all system events will take time. Do you want to continue?
	No	

7.10 BMC User Settings



BIOS Item	Options	Description
Add User	Enter	Press <Enter> to Add a User.
Delete User	Enter	Press <Enter> to Delete a User.
Change User Settings	Enter	Press <Enter> to Change User Settings.

7.11 BMC Warm Reset



BIOS Item	Options	Description
BMC Warm Reset	Enter	Press <Enter> to do Warm Reset BMC.

8 BMC

This chapter provides detailed information on understanding, configuring, and managing the BMC.

Abbreviation	Description
BMC	Baseboard management controller
CLI	Command line interface
FRU	Field replaceable unit
GUI	Graphical user interface
IPMI	Intelligent platform management interface
IPU	Intelligence Processing Unit
NTP	Network time protocol
PSU	Power supply unit
SDR	Sensor data record
SEL	System event log
SNMP	Simple network management protocol
SoL	Serial over LAN

8.1 BMC Introduction

8.1.1 Software Interface

BMC (Baseboard Management Controller) is equipped with a multitude of interfaces, each designed to cater to different aspects of server management and monitoring. These interfaces provide comprehensive control and insight, ensuring administrators can effectively oversee server operations.

8.1.1.1 Web GUI

The product supports Web GUI access through HTTPS (port 443), with HTTP disabled by default for enhanced security. The Web GUI offers a management interface, enabling users to view system information, system events, and status, as well as to control the managed servers.

8.1.1.2 IPMI Interface

The IPMI (Intelligent Platform Management Interface) is a standardized interface used for remote monitoring and management of server systems. It provides a powerful set of tools for system administrators to control and monitor servers independently of the operating system.

Features of IPMI

Event Logging: Critical system events and hardware status changes are logged, facilitating efficient troubleshooting.

Security: IPMI supports secure interfaces and protocols for safe remote management.

8.1.1.3 Redfish

Redfish is a modern, RESTful API used for the management of servers, storage, and networking equipment in data centers and large-scale enterprise environments. It's designed to replace older, less efficient management interfaces with a standardized, scalable, and secure approach.

8.2 Web GUI Introduction

The Web GUI of BMC is a critical component that offers an intuitive and user-friendly platform for managing and monitoring server operations remotely. This web-based interface ensures administrators can efficiently interact with the server's BMC from anywhere.

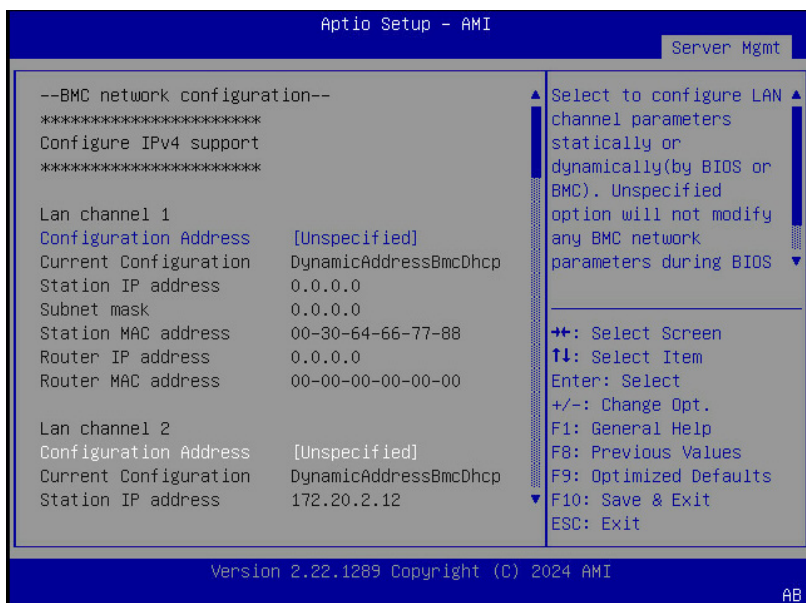
8.2.1 Web Login

Web login to the BMC interface is a straightforward process designed to provide secure and easy access to server management tools.

8.2.1.1 Environment Setup

Before logging into the BMC's Web GUI, certain environmental prerequisites must be met:

- ✦ **Network Configuration**
Ensure the server and the device used for access are on the same network or have a route to connect.
- ✦ **Browser Requirements:**
Verify that the web browser used is compatible with the BMC's Web GUI. Commonly supported browsers include Chrome, Firefox, Safari, and Edge.
- ✦ **BMC IP Address**
You can setup the BMC IP address from the server's BIOS interface or ipmitool command listed in the section 5.3 BMC LAN Configuration. To setup from BIOS interface, navigate to the "Server Mgmt" tab and select the "BMC network configuration" option.



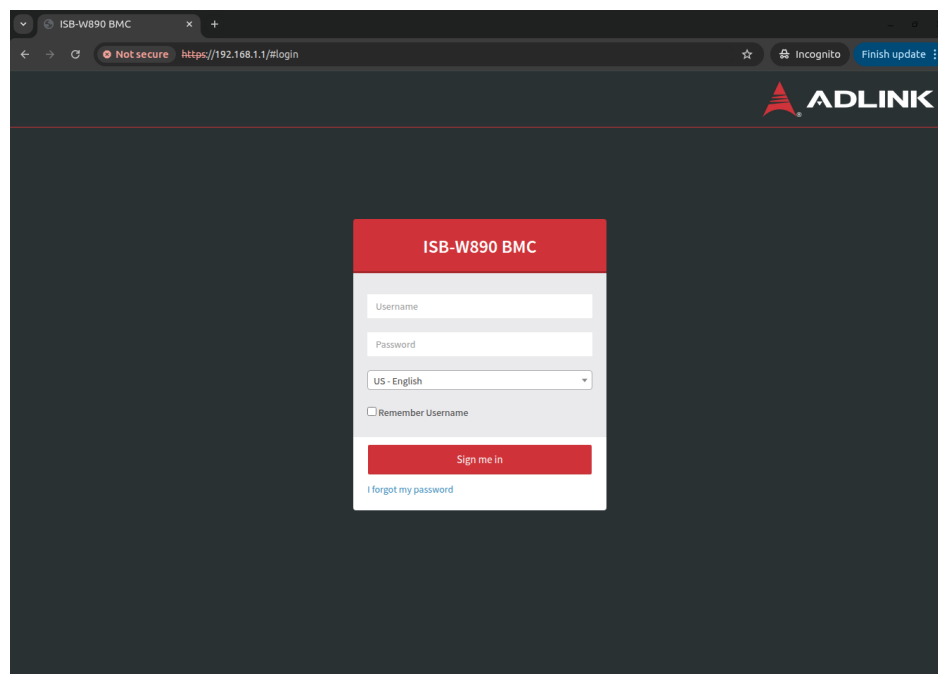
- ✦ **Security Considerations**
For security reasons, access to the BMC Web GUI is exclusively through HTTPS.

8.2.1.2 User Sign-In

✦ Accessing the Login Page

Open your web browser and type in the BMC's IP address, obtained from the BIOS, preceded by "https://". For example, https://[BMC-IP-Address].

This action will direct you to the BMC Web GUI login page.



✦ Selecting Language

Below the login fields, there is an option to select your preferred language.

The BMC Web GUI supports multiple languages, including Simplified Chinese, Traditional Chinese, and English.

Choose your desired language from the dropdown menu before logging in.

✦ Entering Login Credentials

On the login page, you will be prompted to enter your username and password.

The default username: admin

The default password: admin

After entering these credentials, click the **"Sign me in"** button to proceed.

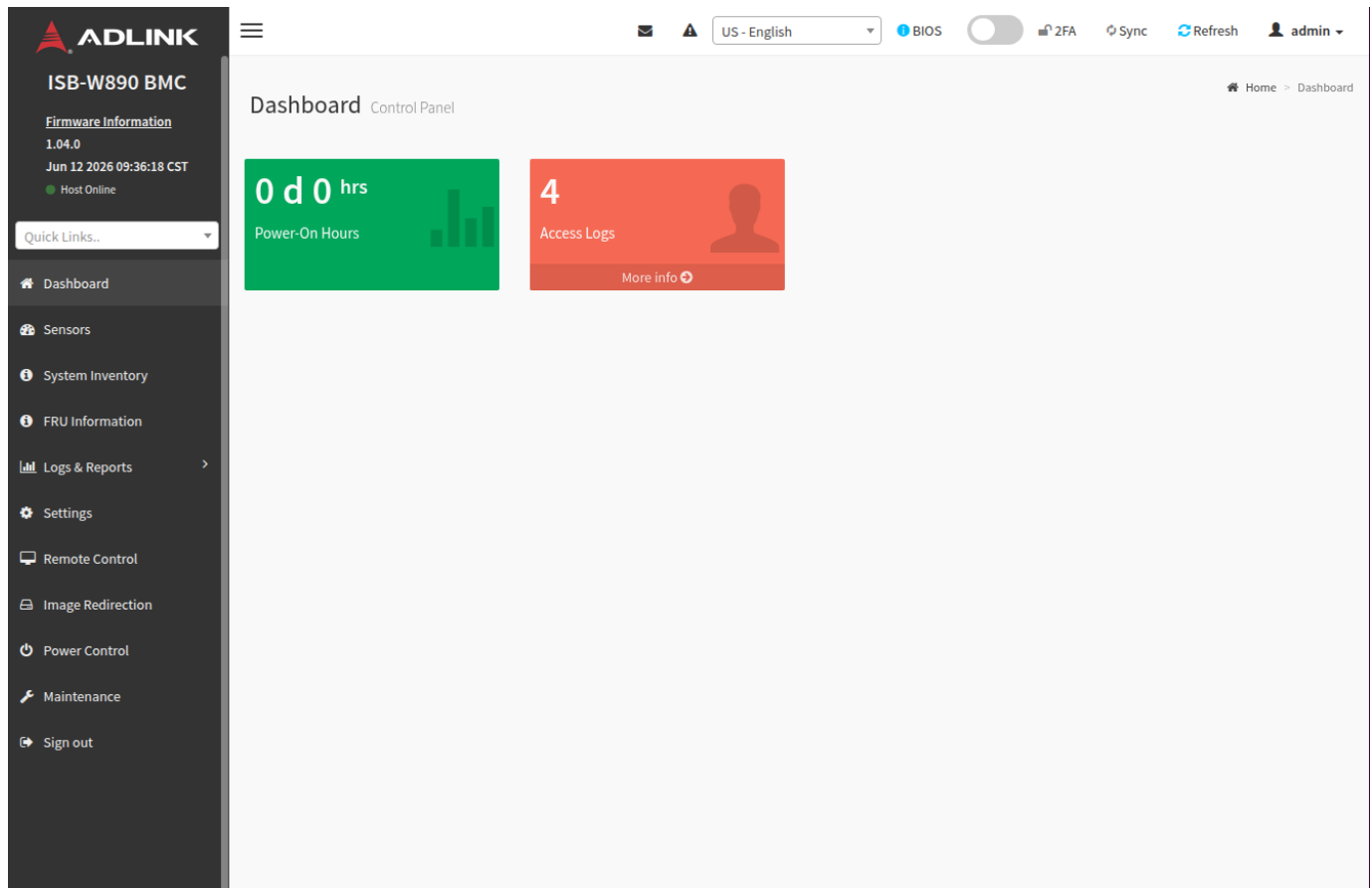
✦ Other fields

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.

I Forgot my Password: If you forget your password, you can generate a new password using this link.

8.2.2 Web Interface Overview

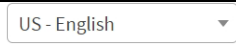
This section provides an overview of the BMC's Web Interface, emphasizing the functionalities and information displayed on the main interface. The primary purpose of the main interface is to offer a quick and comprehensive understanding of the current status of the BMC.



The BMC Web GUI is primarily divided into three sections, each offering specific functionalities and information crucial for server management.

1. Top Menu Bar

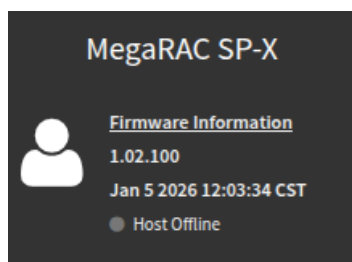
Functionality: The top menu bar is designed for receiving and viewing server messages, setting BMC global configurations, and accessing the BIOS configuration interface. This area serves as a quick access point for important notifications and system adjustments.

Function	Icon	Detailed Description
Message		Display the messages received.
Notification		Display the notifications received.
Language		Set Board Language.
Bios interface		Open the new window or popup to configure the BIOS settings.
Dashboard Expansion		Show/Hide limited Dashboard Widgets.
2FA		Enable/Disable Two Factor Authentication.
Synchronization		On/Off to synchronize with latest Sensor and Event Log updates.

Function	Icon	Detailed Description
Refresh		Reload the current page.
Profile	 admin ▼	Set the User Profile.

2. Server Version Information

This section of the interface displays the current version information of various server components, listed in the following order:



- BMC Version Information
- BMC Image Build Date and Time
- Chassis Power Status

The version information window provides a quick overview of the server's hardware and firmware status, ensuring that administrators are immediately aware of the current versions and operational status.

The Chassis Power Status will be displayed as Host Online / Host Offline. To Change the Power Control Status, click Host Online / Host Offline link.

3. Function Menu bar

The menu bar displays the following.

- ✧ Dashboard
- ✧ Sensor
- ✧ System Inventory
- ✧ FRU Information
- ✧ Logs & Reports
- ✧ Settings
- ✧ Remote Control
- ✧ Image Redirection
- ✧ Power Control
- ✧ Maintenance
- ✧ Sign out

8.2.3 Server Information

8.2.3.1 FRU Information

FRU
Field Replaceable Units
Home > FRU

Available FRU Devices

FRU Device ID
0
FRU Device Name
BMC_FRU

Chassis Information

Chassis Information Area Format Version
1
Chassis Type
Unspecified
Chassis Part Number
91-XXXX-XXX
Chassis Serial Number
00000000000000000000
Chassis Extra

Board Information

Board Information Area Format Version
1
Language
English
Manufacture Date Time
Fri Nov 17 19:33:00 2023
Board Manufacturer
ADLINK Technology
Board Product Name
MECS-7120
Board Serial Number
00000000000000000000
Board Part Number
91-XXXX-XXX
FRU File ID
Board Extra

Product Information

Product Information Area Format Version
1
Language
English
Product Manufacturer
ADLINK Technology
Product Name
MECS-7120
Product Part Number
91-XXXX-XXX
Product Version
1
Product Serial Number
00000000000000000000
Asset Tag
TEST
FRU File ID
Product Extra

The FRU (Field Replaceable Unit) Information interface in the BMC Web GUI is accessed by clicking on the "FRU Information" option in the left-hand function bar. This feature allows users to view electronic label information for the motherboard and other components, providing detailed FRU data.

Structure and Functionality of the FRU Information Interface. The FRU information is divided into four main sections, each offering specific insights:

Information Category	Description
Available FRU Devices	Details about each FRU device: FRU Device ID FRU Device Name
Chassis Information	Information related to the server's chassis, featuring: Chassis Information Area Format Version Chassis Type Chassis Part Number Chassis Serial Number Chassis Extra
Board Information	Data about the server's mainboard, encompassing: Board Information Area Format Version Language Manufacture Date Time Board Manufacturer Board Product Name

Information Category	Description
	Board Serial Number Board Part Number FRU File ID Board Extra
Product Information	Comprehensive details about the product, including: 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

8.2.3.2 Sensor Information

The Sensor Information panel in the BMC Web GUI provides a detailed overview of the current status and readings from various sensors within the server. Accessing and understanding this data is essential for maintaining the server's health and performance.

- Accessing the Sensor Information Panel
- Navigating to the Panel
- Click on the "Sensor" button located on the left side of the BMC Web GUI

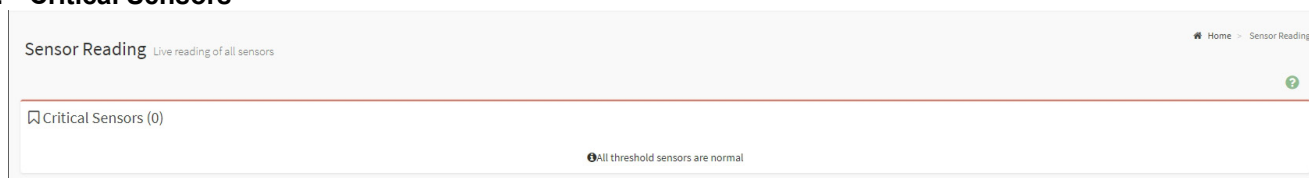
8.2.3.2.1 Introduction to Sensor Interface

This will lead you to the Sensor Information interface, which is central for real-time sensor status monitoring.

Sensor Information Interface Layout

The Sensor Information interface is divided into four distinct sections, each providing specific types of sensor data:

1. Critical Sensors



This section displays the status of critical sensors, highlighting if any sensor has exceeded its threshold or is showing abnormal readings.

It's a focal point for quickly identifying potential issues that require immediate attention.

2. Discrete Sensor States

Discrete Sensor States (12)

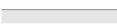
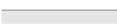
Sensor Name	State
ACPI_Power	S0/G0 Working
FAN1_Presence	Device Inserted / Device Present
FAN2_Presence	Device Inserted / Device Present
FAN3_Presence	Device Inserted / Device Present
FAN4_Presence	Device Inserted / Device Present
FAN5_Presence	Device Inserted / Device Present
HDD1_Status	Drive Presence
HDD2_Status	Drive Absence
PSU1_Presence	Device Inserted / Device Present
PSU1_Status	Presence Detected, Power Supply Failure Detected, Power Supply Input Lost (AC/DC)
PSU2_Presence	Device Inserted / Device Present
PSU2_Status	Presence Detected

Shows the status of discrete sensors, particularly focusing on those that are offline.

This part is crucial for identifying sensors that are not functioning or are disconnected.

3. Normal Sensors

Normal Sensors (46)

Sensor Name	Reading	Behavior
CPU_Outlet_Temp	28 °C	
CPU_Power	34 Watts	
CPU_TJMAX	99 °C	
CPU_Temp	31 °C	
DIMM_A1_Temp	23 °C	
FAN1_Speed_Inner	7050 Rpm	
FAN1_Speed_Outer	6000 Rpm	
FAN2_Speed_Inner	7050 Rpm	
FAN2_Speed_Outer	6000 Rpm	
FAN3_Speed_Inner	7050 Rpm	
FAN3_Speed_Outer	6000 Rpm	
FAN4_Speed	6750 Rpm	

Displays the actual readings from various sensors.

These readings include data such as temperature, fan speeds, voltage levels, and more.

The section provides a comprehensive view of the real-time operating conditions of the server.

4. Disabled Sensors

Disabled Sensors (16)

✖DIMM_B1_Temp	✖DIMM_C1_Temp	✖DIMM_E1_Temp	✖DIMM_G1_Temp
✖DIMM_H1_Temp	✖PSU2_Inlet_Temp	✖PSU2_Sec_Temp	✖PSU2_Prm_Temp
✖TBF100_Up_Temp	✖TBF100_Down_Temp	✖PSU2_VOUT	✖PSU2_POUT
✖PSU2_PIN	✖PSU2_Status	✖TBF100_Up_PWR	✖TBF100_Down_PWR

Lists sensors that are currently not in operation or are disabled.

This section helps in identifying which sensors are not contributing to the monitoring process and may need reactivation or maintenance.

8.2.3.2.2 Detailed Sensor Information

Accessing and Viewing Sensor Details. To view detailed information about a specific sensor, simply click on the desired sensor listed in the Sensor Information panel. This action will lead you to a dedicated detail page for that sensor.

On this detailed page, extensive information about the selected sensor is displayed, including its current operational status, various parameters, and any unique specifications.

The screenshot shows the 'Sensor detail' page for the 'ACPI_Power' sensor. The page has a breadcrumb trail: Home > Sensor Reading > Sensor detail. Below the breadcrumb, there is a section titled 'ACPI_Power Sensor Information' with a sub-header 'Sensor State Reading - 0x8001'. Below this, there is a section titled 'ACPI_Power Sensor Events' with a date filter for 'January 2024'. A vertical timeline on the left side of the events section shows six events, each with a blue circular icon containing a person silhouette. The events are listed in a table-like format with columns for the event ID, description, and time ago.

ID	Description	Time Ago
ID: 48	ACPI_Power sensor of type System ACPI Power State logged a s5 or g2 soft off	3 days ago
ID: 36	ACPI_Power sensor of type System ACPI Power State logged a s0 or g0 working	3 days ago
ID: 34	ACPI_Power sensor of type System ACPI Power State logged a s5 or g2 soft off	3 days ago
ID: 18	ACPI_Power sensor of type System ACPI Power State logged a s0 or g0 working	3 days ago
ID: 16	ACPI_Power sensor of type System ACPI Power State logged a s5 or g2 soft off	3 days ago
ID: 12	ACPI_Power sensor of type System ACPI Power State logged a s0 or g0 working	3 days ago

Customizing Sensor Thresholds:

For general sensors, the detailed interface provides the capability to adjust various sensor threshold parameters. Administrators have the flexibility to modify several threshold levels including:

Upper Non-Recoverable

Upper Critical

Upper Non-Critical

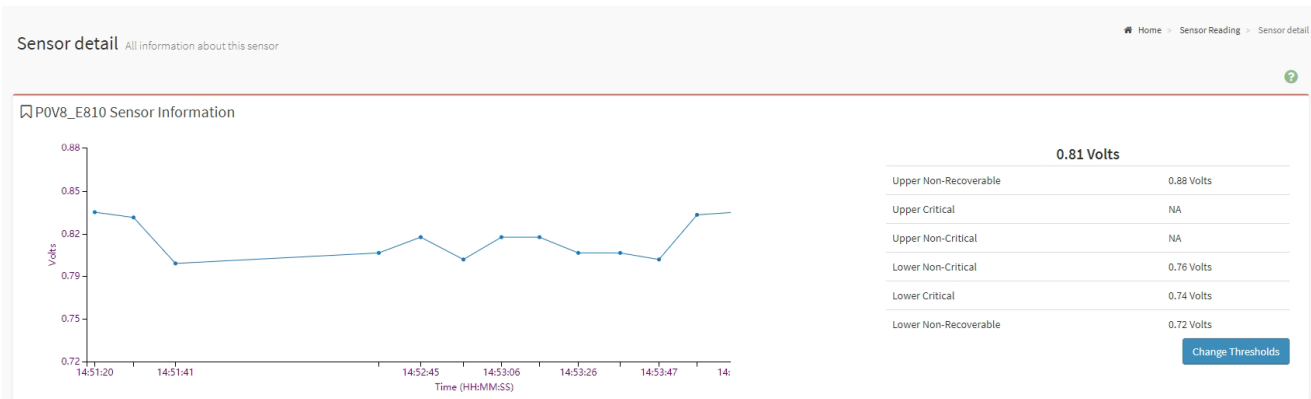
Lower Non-Critical

Lower Critical

Lower Non-Recoverable

Practical Application:

Adjusting these thresholds is vital for preemptive alerts and ensuring that sensors are operating within safe and optimal ranges.



If the synchronization button in the top menu bar is active, accessing the detail interface for a general sensor will enable a graphing feature. This feature provides a line graph depicting the sensor's data over time. It serves as a visual tool for quickly assessing the sensor's performance.

8.2.3.2.3 Modifying Sensor Thresholds

Accessing Sensor Thresholds Modification Interface. In the Sensor Details interface, locate and click on the "Change Thresholds" button. This action will redirect you to the Sensor Thresholds interface.

Sensor Thresholds

Change Threshold Values

NOTE:

- All available Threshold values should have numbers or numbers with two decimal places.
- As per design, Retain Threshold Values will always be used to set the sensor threshold values across resets and Checkbox value will not be retained between the page navigations/refresh hence Checkbox will always be in unchecked state.

Sensor Name
P12V_AUX

Upper Non-recoverable
13.20

Upper Critical
12.84

Upper Non-critical
12.60

Lower Non-critical
11.40

Lower Critical
11.16

Lower Non-recoverable
10.80

☐ Retain Threshold Values

Save

Sensor Thresholds Interface:

- The Sensor Thresholds interface displays each sensor's name along with its threshold values.
- Users can view and modify thresholds for each sensor, including upper and lower warning and critical limits.
- Thresholds not applicable or unavailable for a sensor are marked as "NA".

Retaining Threshold Values

At the bottom of the interface, a **"Retain Threshold Values"** checkbox is provided.

Note: If this option is not selected, threshold adjustments will be temporary, reverting to default upon BMC reboot or power loss.

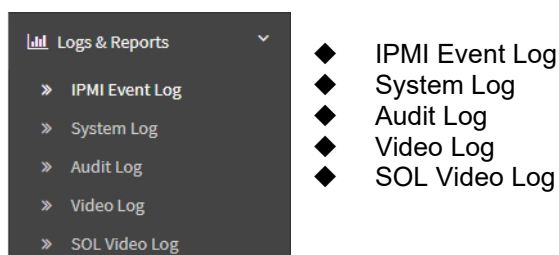
8.2.4 Server Information

BMC provides various logging functions that are crucial for system diagnosis, monitoring, and security. Logs are divided into different types, each with a specific purpose.

Accessing BMC Logs

To view these logs, navigate to the BMC web interface:

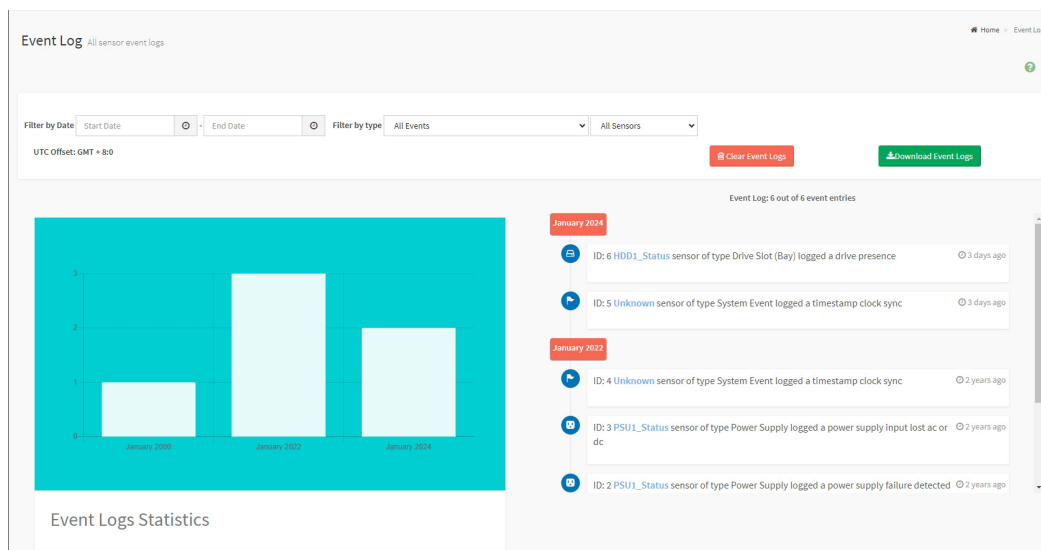
- From the left-side functional panel, click on "Logs & Reports".
- A dropdown menu will appear, listing the following types of logs available for viewing:



8.2.4.1 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.



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 ByDate 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.

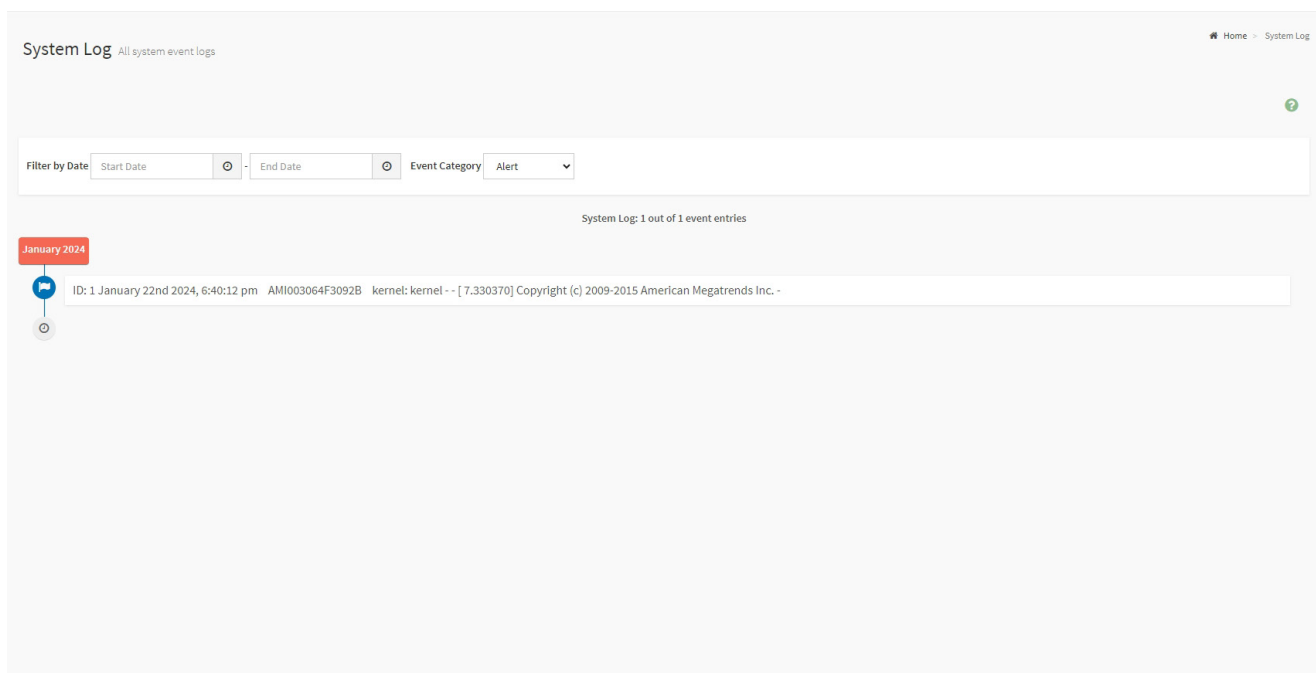
Note: When Clear All Event Logs action is performed, there might be some events present even after clearing those events are generated after performing clear operation which can be verified using its timestamp.

8.2.4.2 System Log

System 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** in order to display any entries.

To open the Event Log page, click **Logs & Reports > System Log** from the menu bar.



Procedure

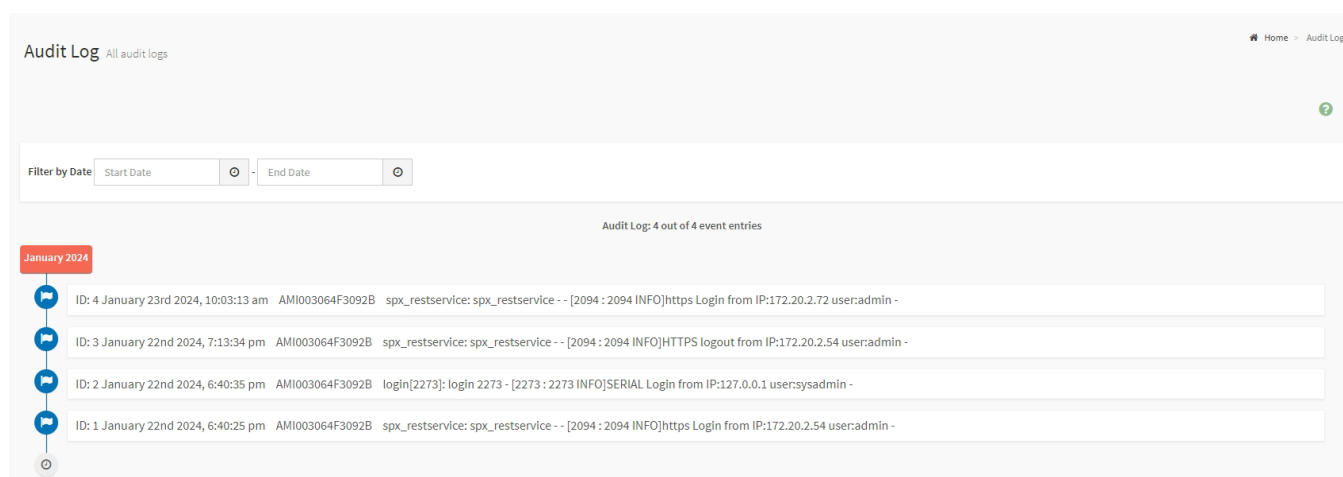
To view System Log, click the **System Log** tab to view all system events. Entries can be filtered based on Filter By Date (Start Date and End Date) and Event Category like Alert, Critical, Error, Notification, Warning, Debug, Emergency and Information.

8.2.4.3 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.

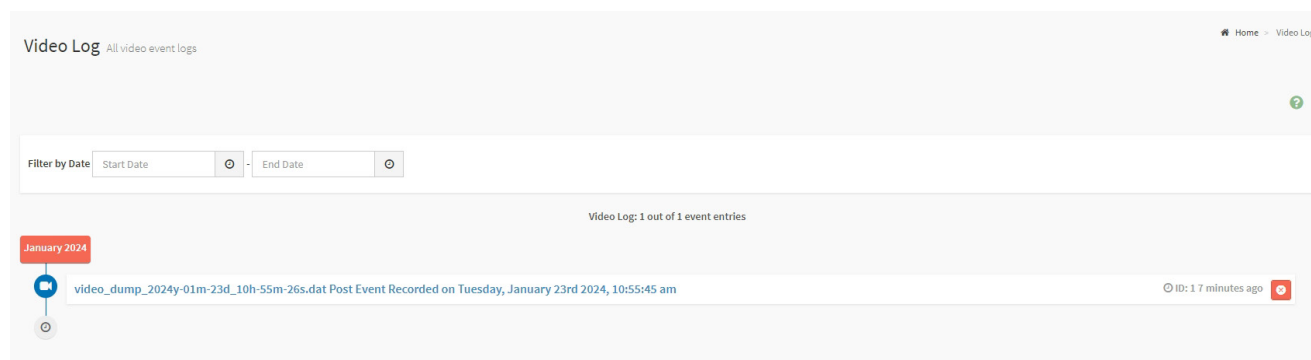


8.2.4.4 Video Log

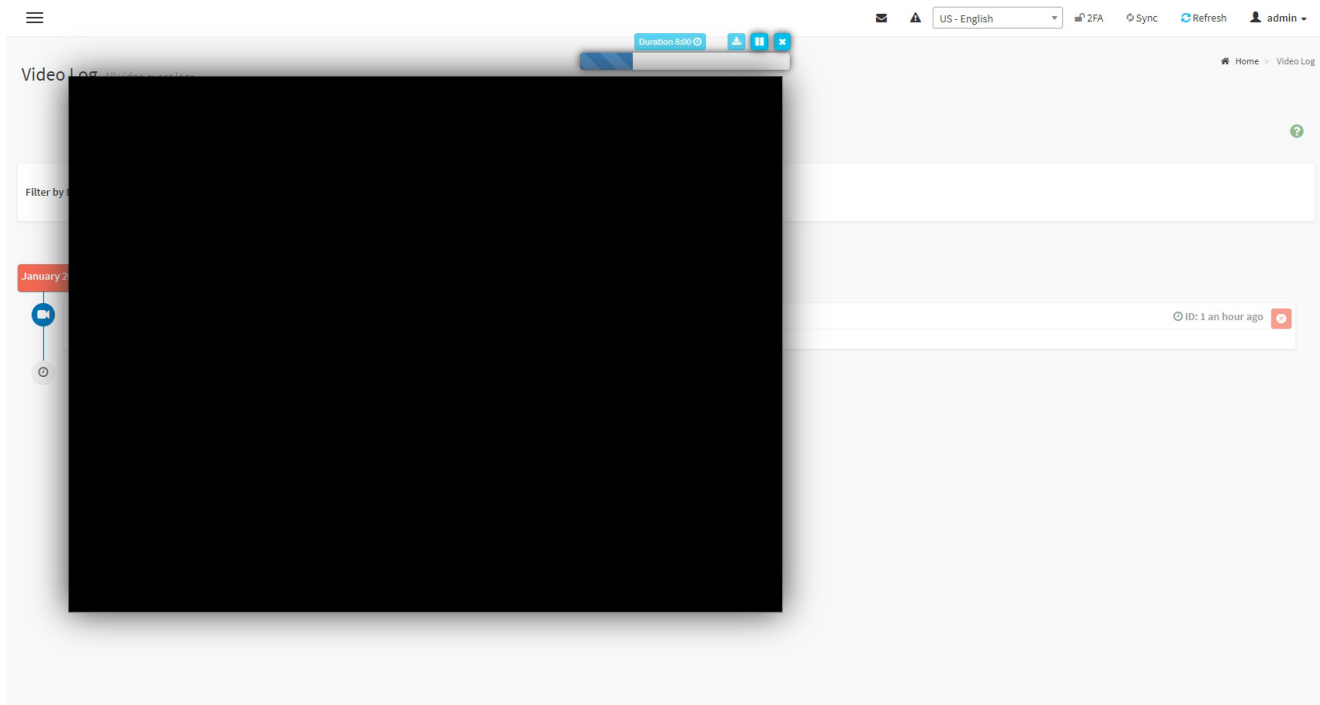
The video log page will record the configured system events in the device in a video format that has been already configured.

Note: Video Trigger Settings should be enabled, to display the Video Log page. Video Trigger Settings can be configured under **Settings > Video Recording > Auto Video Settings > Video Trigger Settings**.

To open the Video Log page, click **Logs & Reports > Video Log** from the menu bar. A sample screenshot of Video Log page is shown below



After clicking on the video event, the video conversation box will pop up. Play the current video. In this interface, you can choose to download or delete the current video log.



Note: Video will be allowed to play/download only if file size is lesser than 40MB. Browsers have various memory restrictions, due to this browser cannot store and process data greater than 40MB (approximately). If file size is greater than 40MB, user will be notified with a message to use Java player Application.

The video data may not be proper if the browser zoom in/out settings are changed during video playback.

To download a video, you need to wait for the video buffering to complete before downloading.

8.2.4.5 SOL Video Log

The sol log page will record configured system events through sol.

Note: SOL Trigger Settings should be enabled, to display the SOL Log page. SOL Trigger Settings can be configured under **Settings > Video Recording > SOL Settings > SOL Trigger Settings**.

SOL Configurations can set the baud rate of the serial port.

To open the Video Log page, click **Logs & Reports > SOL Log** from the menu bar. A sample screenshot of SOL Log page is shown below.

SOL Video log All SOL Video log		
S.No	File Name	File Information
1	SOLHostCapture_Archive_1_01232024_13_26_08.log	Tuesday, January 23rd 2024, 1:26:08 pm

S.No - The serial number

File Name - The video filename

File Information - Day, date, and time of video upload

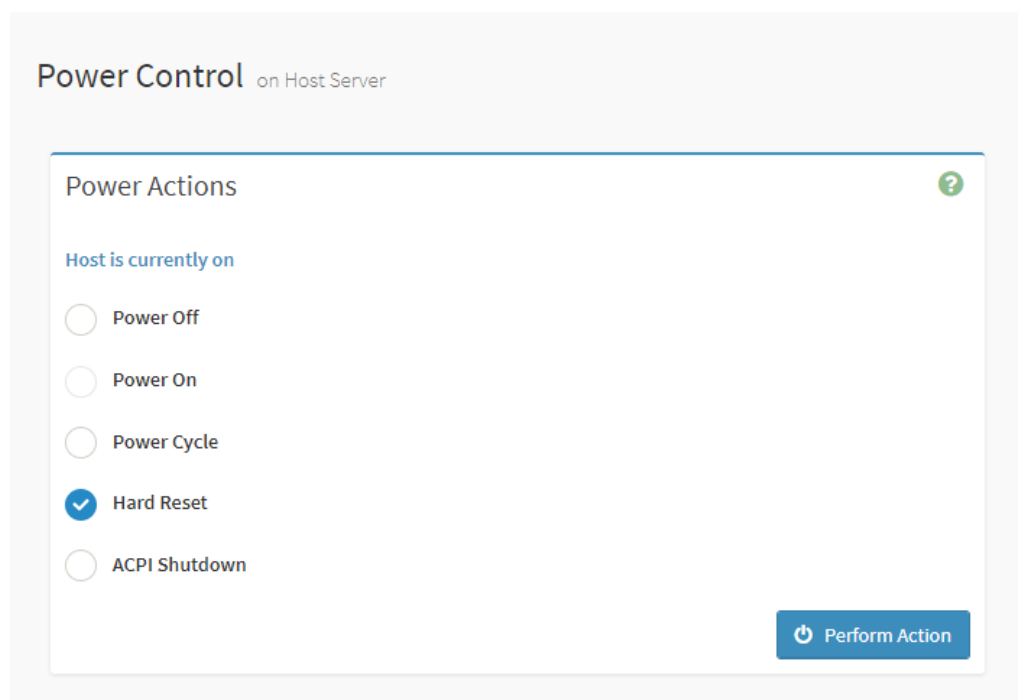
Download - To download the selected video

Delete - To delete the selected video.

Note: *The timestamp displayed in the file information represents last modified time, and it will be updated (if the file is modified) when the webpage is refreshed.*

8.2.5 Power Control

It is used to control power on the WEB. A sample screenshot of service management is shown as below.



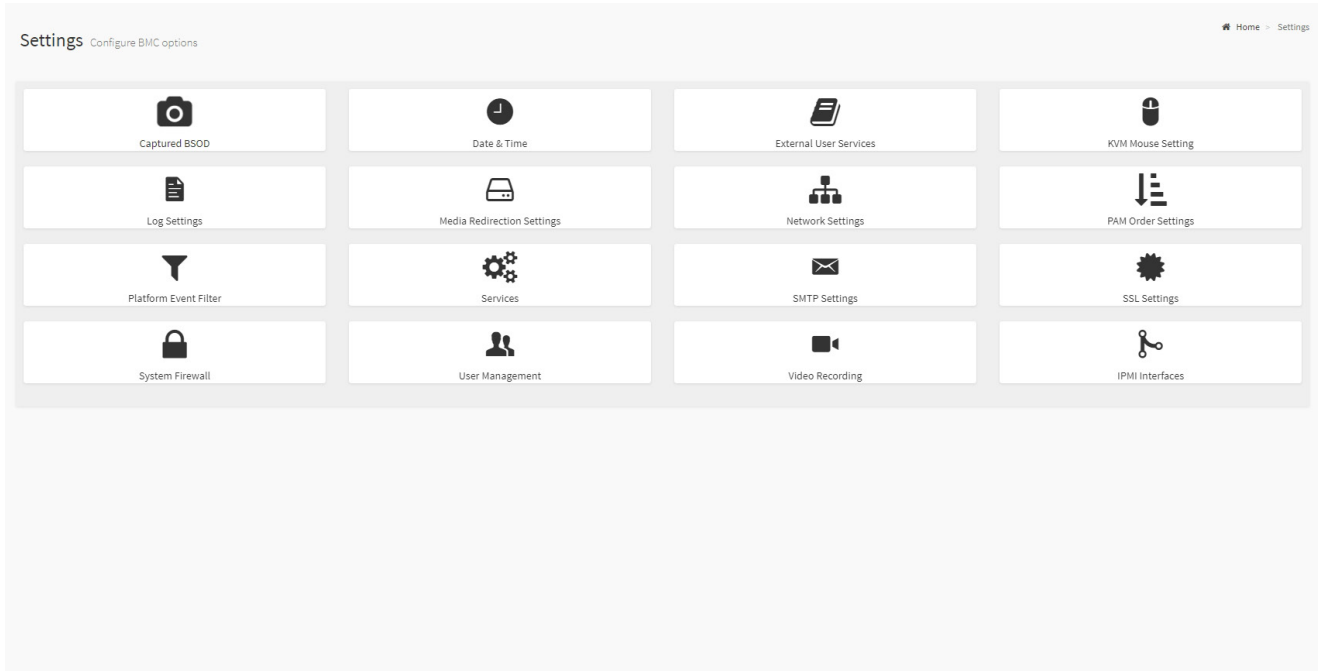
The power control consists of the following items.

- **Power off:** Power on the chassis.
- **Power on:** Power off the chassis.
- **Power Cycle:** Power off the chassis and power on the chassis.
- **Hard Reset:** Restart the chassis.
- **ACPI Shutdown:** Soft power off the chassis.

8.2.6 BMC Settings

The BMC Settings section in the BMC web interface is a centralized location for accessing and modifying a wide range of configuration settings for the BMC.

1. In the BMC web interface, click on the **"Settings"** button located in the functional menu on the left side.
2. This action will open a group menu that displays various configurable options and settings.



Features

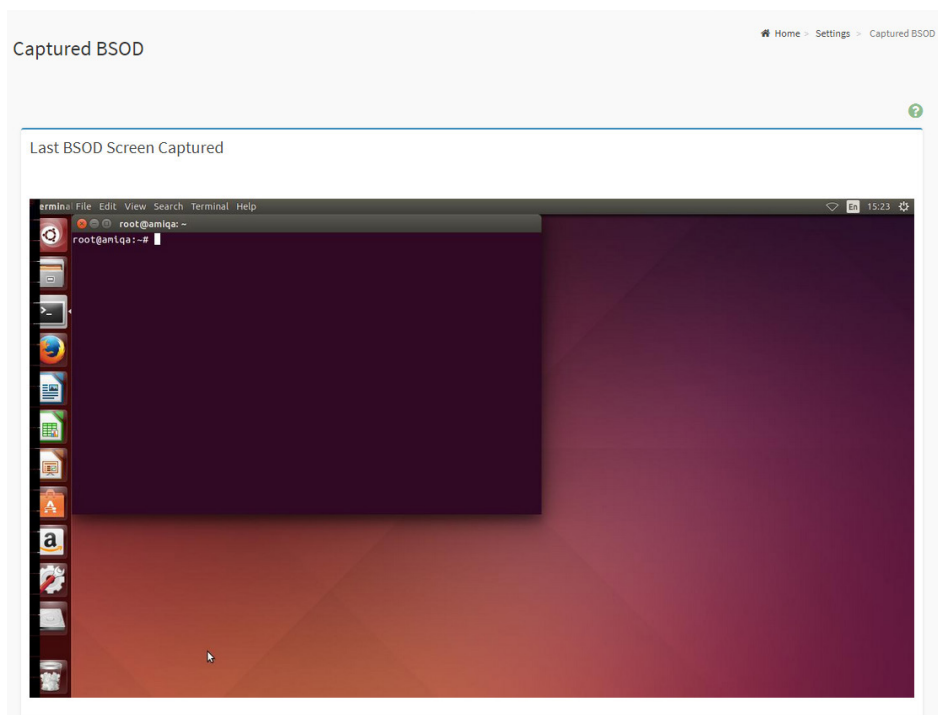
Comprehensive Configuration: This interface allows you to adjust and set most of the BMC's configurations, tailoring the controller to your specific needs and preferences.

Information Retrieval: Besides configuration, this section also provides access to essential information about the BMC and the server it manages.

8.2.6.1 Captured BSOD

This page displays a snapshot of the blue screen captured if the host system crashed since last reboot.

A screenshot of Captured BSOD is shown below.



Note: KVM service should be enabled to display the BSOD screen. KVM Service can be configured under **Settings > Services > KVM**.

8.2.6.2 Date & Time

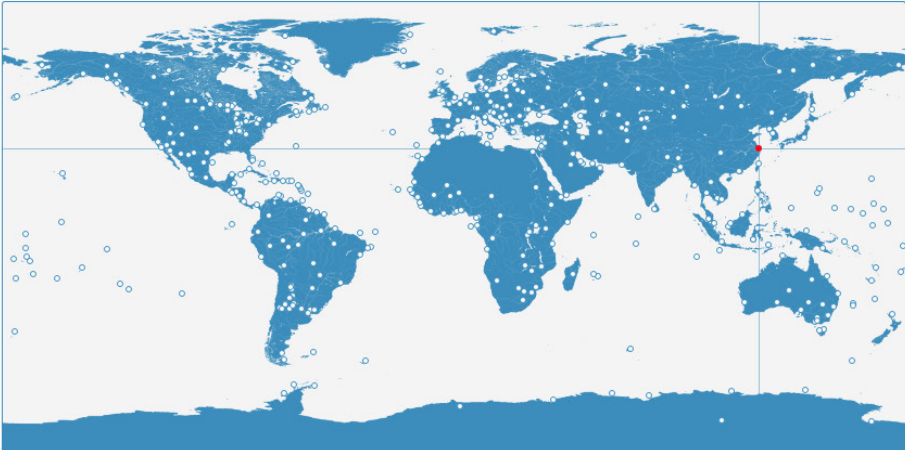
This field is used to set the date and time on the BMC. A sample screenshot of Date & Time is shown as below.

Date & Time

[Home](#) > [Settings](#) > [Date & Time](#)

Note:
If the time zone is selected from the group of Manual offset (GMT/ETC time zones), the interactive map selection feature will be disabled.
The new Time Zone settings will be reflected on the page only after being saved.

Configure Date & Time



Select Time Zone

Feb 26, 2024 10:45:52 AM(GMT+08:00 CST) - Asia/Shanghai

☐ Automatic NTP Date & Time

☒ Automatic PTP Date & Time

PTP Interface

PTP Transport

Ipv4

PTP Unicast IP

PTP Unicast IP

PTP Inbound Latency

0

PTP Priority1

0

☐ Panic Mode

PTP Preset

Slaveonly

PTP Ipmode

Unicast

PTP Delay Mechanism

E2E

PTP Outbound Latency

0

PTP Max Master capacity

5

PTP Log request delay

1

Save

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.

Note: Based on the manual selection of GMT or ETC/GMT, time zone alone will be changed and date & time will remain the same.

Automatic NTP 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. The following address formats & Domain name format are supported:
 - ✧ IPv4 Address format
 - ✧ IPv6 Address format
 - ✧ Domain name format allowed 'A-Z', 'a-z', '0-9', dash (-), underscore (_) and dot(.) characters
- **Secondary NTP Server:** To configure a secondary NTP server to use when automatically setting the date and time. The following address formats & Domain name format are supported
 - ✧ IPv4 Address format
 - ✧ IPv6 Address format
 - ✧ Domain name format allowed 'A-Z', 'a-z', '0-9', dash (-), underscore (_) and dot(.) characters
- **Automatic PTP Date & Time:** To enable/disable the use of PTP servers to automatically set the date and time.
- **PTP Interface:** To configure a PTP server interface to use when automatically setting the date and time.
- **PTP Preset:** To configure a PTP Preset type to use when automatically setting the date and time.
- **PTP Transport:** To configure a PTP Transport type to use when automatically setting the date and time.
- **PTP Ipmode:** To configure a PTP Ipmode type to use when automatically setting the date and time.
- **PTP Unicast IP:** To configure a Unicast IP when ipmode is unicast and server to use when automatically setting the date and time.
- **PTP Delay Mechanism:** To configure a PTP Delay Mechanism type to use when automatically setting the date and time.
- **PTP Inbound Latency:** To configure an Inbound latency of the server to use when automatically setting the date and time.
- **PTP Outbound Latency:** To configure a PTP outbound latency server to use when automatically setting the date and time.
- **PTP Priority1:** To configure a priority of PTP clock to use when automatically setting the date and time.
- **PTP Max Master capacity:** To configure a max master capacity of the PTP clock to use when automatically setting the date and time.
- **Panic Mode:** To configure a PTP clock to not reset if jump is more than 1 second, use when automatically setting the date and time.

Save: To save the settings.

Note: If the time zone is selected as Manual Offset, the map selection will be disabled. The Time-Zone settings will be reflected only after saving the settings.
If disable the Automatic Date & Time, the time needs to select by users themselves or the time would not change.

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. Enable **Automatic PTP Date &Time** to enable/disable the use of PTP servers to automatically set the date and time.
 - a) Enter the Interface, Preset, Transport, Ipmode, Unicast IP, Delay Mechanism, Inbound Latency, Outbound Latency, Priority1, Max Master capacity and Log request delay details in their corresponding fields.
 - b) Enable/Disable Panic Mode to not reset if jump is more than 1 second, use when automatically setting the date and time.
4. Click **Save** button to save the settings.

8.2.6.3 External User Services

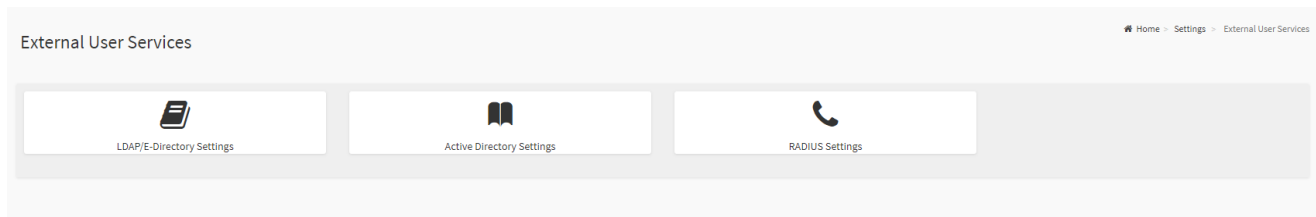
8.2.6.3.1 LDAP/E-Directory Settings

The Lightweight Directory Access Protocol (LDAP)/E-Directory Settings is an application

protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

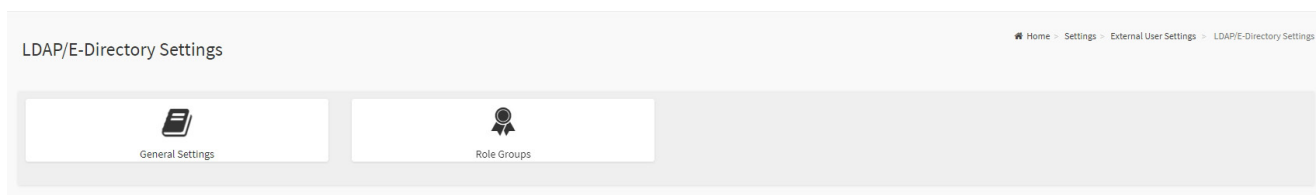
In MegaRAC GUI, LDAP is an Internet protocol that MegaRAC® card can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate MegaRAC® card users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the MegaRAC card. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group-based policies to control access.

To open External User Services page, click **Settings -> External User Services** from the menu bar. A sample screenshot of External User Services page is shown below.



To open LDAP/E-DIRECTORY Settings page, click **Settings > External User Services > LDAP/E-Directory Settings** from the menu bar.

A sample screenshot of External User Services page is shown below.



The fields of LDAP/E-Directory Settings Page are explained below.

General Settings: To configure LDAP/E-Directory Settings. Options are Enable LDAP/E-Directory Authentication, IP Address, Port and Search base.

Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Note: It is recommended to Enable LDAP configuration from configure general settings page otherwise error message will pop-up stating that "LDAP configuration is not enabled" while trying to create/view LDAP role groups.

Procedure

Entering the details in General LDAP/E-Directory Settings Page.

1. In the LDAP/E-Directory Settings Page, click General Settings. A sample screenshot of General LDAP Settings page is given below.

General LDAP Settings

Home > Settings > External User Settings > LDAP/E-Directory Settings > General LDAP Settings

☐ Enable LDAP/E-Directory Authentication

Encryption Type
☒ No Encryption ☐ SSL ☐ StartTLS

Common Name Type
☒ IP Address ☐ FQDN

Server Address

Port

Bind DN

Password

Search Base

Attribute of User Login

[Save](#)

2. Click Enable LDAP/E-Directory Authentication, to enable LDAP/E-Directory Settings.

Note: During login prompt, use username to login as an LDAP Group member.

3. Select the encryption type for LDAP/E-Directory from the Encryption Type.

Note: Configure proper port number, when SSL is enabled.

4. Select the Common Name Type as IP Address.

5. Enter the IP address of LDAP server in the Server Address 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.

Configure FQDN address, when using StartTLS with FQDN.

5. Specify the LDAP Port in the Port field.

Note:

Default Port is 389. For SSL connections, default port is 636. The Port value ranges from 1 to 65535.

6. Specify the Bind DN that is used during bind operation, which authenticates the client to the server.

Note:

Bind DN is a string of 4 to 253 alpha-numeric characters.

It must start with an alphabetical character.

Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.

Example: cn=manager,ou=login, dc=domain,dc=com

7. Enter the password in the Password field.

Note:

Password must be at least 1 character long.

White space is not allowed.

This field will not allow more than 48 characters.

8. Enter the Search Base. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directory.

Note:

Search base is a string of 4 to 253 alpha-numeric characters.

It must start with an alphabetical character.

Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.

Example: ou=login,dc=domain,dc=com.

9. Select Attribute of User Login to find the LDAP/E-Directory server which attribute should be used to identify the user.

Note: *It only supports cn or uid.*

10. Select CA Certificate File from the Browse field to identify the certificate of the trusted CA certs.

11. Select the **Certificate File** to find the client certificate filename.

12. Select **Private Key** to find the client private key filename.

Note: *All the 3 files are required, when SSL or StartTLS is enabled.*

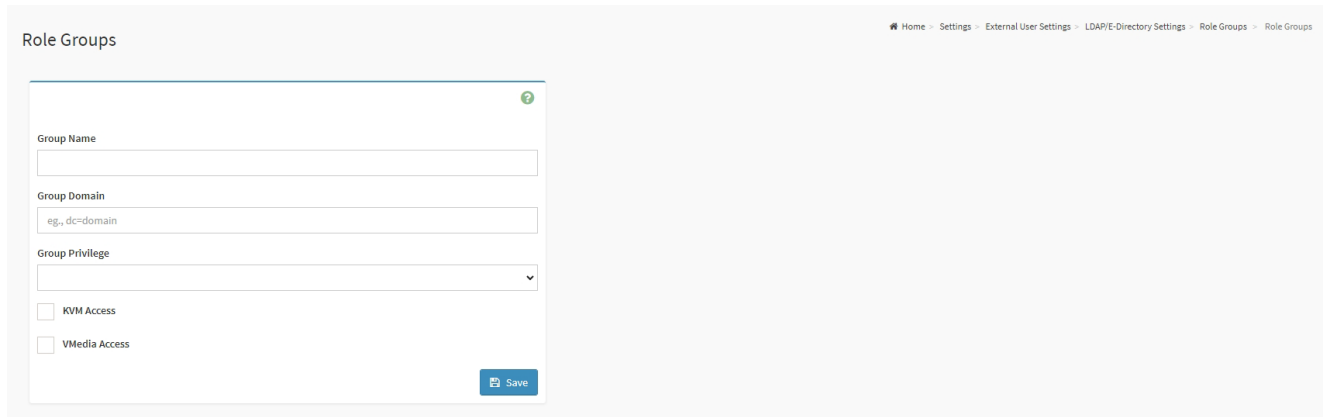
13. Click **Save** to save the settings.

To add a new Role Group

1. In the LDAP/E-Directory Settings Page, Click Role Groups and select a blank row.

Note: *It is recommended to Enable LDAP configuration from configure general settings page otherwise error message will pop-up stating that "LDAP configuration is not enabled" while trying to create/view LDAP role groups.*

2. Click Add Role Group or alternatively double click on the blank row to open the Add Role group Page as shown in the screenshot below.



3. In the Group Name field, enter the name that identifies the role group.

Note:

Maximum size of Role Group Name is 255 bytes.

Special symbols hyphen and underscore are allowed.

4. In the Group Domain field. Enter the Role Group Domain where the role group is located.

Note:

Maximum size of Group Domain Name is 255 bytes.

It must start with an alphabetical character.

Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.

Example: cn=manager,ou=login, dc=domain,dc=com

5. In the Group Privilege field, enter the level of privilege (User, Administrator, Operator, None) to assign to this role group.
6. Select the required options or both.
 - ✧ KVM Access
 - ✧ VMedia Access

Note: VMedia privilege is not applicable for LMedia and RMedia clients.
7. Click **Save** to save the new role group and return to the Role Group List.

8.2.6.3.2 Active Directory Settings

An active directory is a directory structure used on Microsoft Windows based computers and

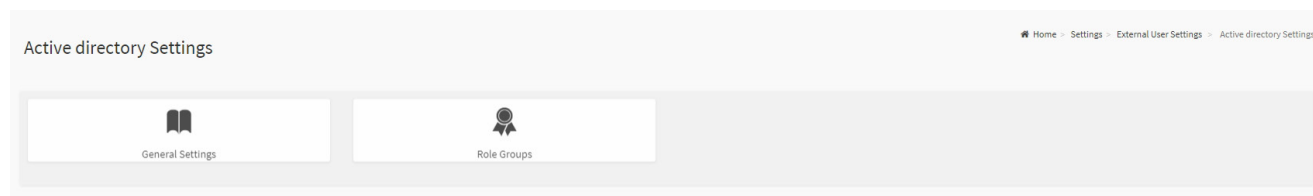
servers to store information and data about networks and domains. An active directory (sometimes referred to as AD) does a variety of functions including the ability to provide information on objects. It also helps to organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.

In MegaRAC SP-X application, Active Directory allows you to configure the Active Directory

Server Settings. The displayed table shows any configured Role Groups and the available slots. You can modify, add or delete role groups from here. Group domain can be the AD domain or a trusted domain. Group Name should correspond to the name of an actual AD group.

Note: To view the page, you must be at least a User and to modify or add a group, you must be an Administrator.

To open Active Directory Settings page, click **Settings > External User Settings > Active Directory** from the menu bar. A sample screenshot of Active Directory Settings page is shown below.



The fields of Active Directory page are explained below.

General Settings: This option is used to configure Active Directory General Settings. Options are Enable Active Directory Authentication, Secret User Name, Secret Password, User Domain name, and up to three Domain Controller Server Addresses.

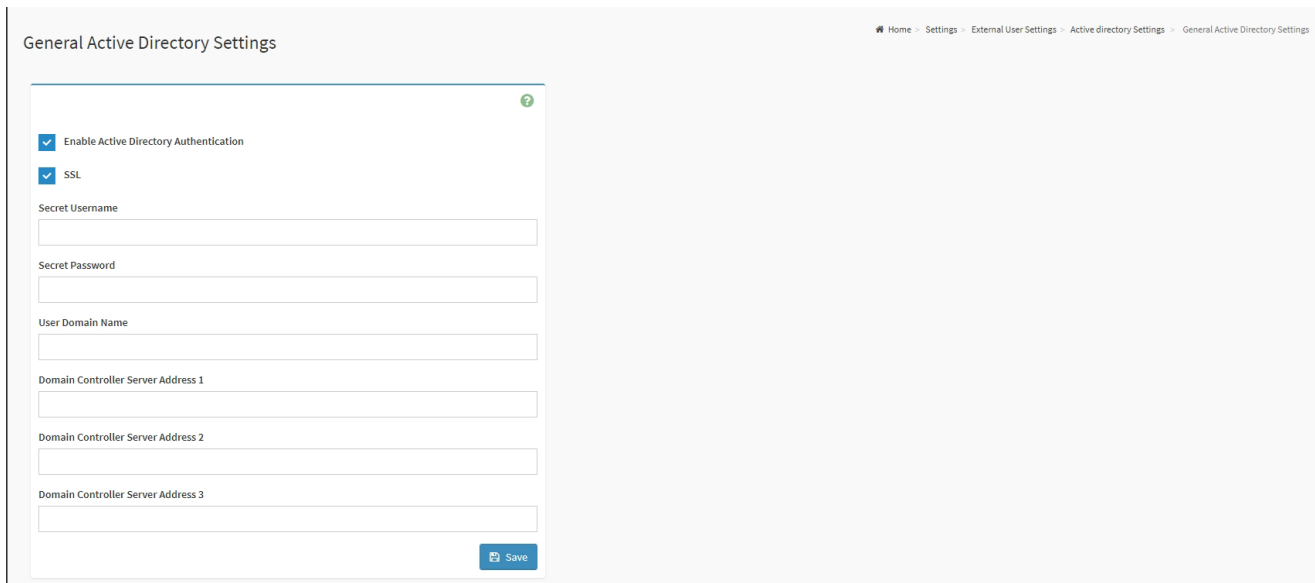
Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Note: It is recommended to Enable AD configuration from configure general settings page otherwise error message will pop-up stating that "AD configuration is not enabled" while trying to create/view AD role groups.

Procedure

Entering the details in General Active Directory Settings Page

1. Click on **General Settings** to open the General Active Directory Settings Page.



2. In the Active Directory Settings page, check or uncheck the **Enable Active directory Authentication** check box to enable or disable Active Directory Authentication respectively.
Note: If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.
3. **SSL:** Check or uncheck to enable or disable the SSL.
4. Specify the Secret user name and password in the **Secret UserName** and **Secret Password** fields respectively.
Note:
 - Secret username/password for AD is not mandatory. When secret username & password is empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods.
 - User Name is a string of 1 to 64 alpha-numeric characters.
 - It must start with an alphabetical character.
 - It is case-sensitive.
 - Special characters like comma, period, colon, semicolon, slash, backslash, square brackets, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed.
 - Password must be at least 6 character long and will not allow more than 127 characters.
 - White space is not allowed.
5. Specify the Domain Name for the user in the **User Domain Name** field. e.g., MyDomain.com
6. Configure IP addresses in **Domain Controller Server Address1**, **Domain Controller Server Address2** and **Domain Controller Server Address3**.
Note:

IP address of Active Directory server: At least one Domain Controller Server Address must be configured.

 - 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.
 - Domain Controller Server Addresses will support IPv4 Address format and IPv6 Address format.

7. Click **Save** to save the entered settings and return to Active Directory Settings Page.

The fields of Role Group page are explained below.

Role Group Name: The name that identifies the role group in the Active Directory.

Note:

- Maximum size of Role Group Name is 255 bytes.
- Special symbols hyphen and underscore are allowed.

Group Domain: The domain where the role group is located.

Note:

- Maximum size of Group Domain Name is 255 bytes.
- Special symbols hyphen, underscore and dot are allowed.

Group Privilege: The level of privilege to assign to this role group.

KVM Access: To provide access to KVM for AD authenticated role group user.

VMedia Access: To provide access to VMedia for AD authenticated role group user.

To Add a New Role Group

1. In the Active Directory Settings page, select a Role Group and click Add Role Group or alternatively double click on the blank row to open the Add Role group Page as shown in the screenshot below.

Note: It is recommended to Enable AD configuration from configure general settings page otherwise error message will pop-up stating that "AD configuration is not enabled" while trying to create/view AD role groups.

2. In the **Group Name** field, enter the name that identifies the role group in the Active Directory.

Note:

- *Maximum size of Role Group Name is 255 bytes.*
- *Special symbols hyphen and underscore are allowed.*

3. In the **Group Domain** field, enter the domain where the role group is located.

Note:

- *Maximum size of Group Domain Name is 255 bytes.*
- *Special symbols hyphen, underscore and dot are allowed.*

4. In the **Group Privilege** field, enter the level of privilege to assign to this role group.

5. Select the required options

- ✧ KVM Access
- ✧ VMedia Access

Note: VMedia privilege is not applicable for LMedia and RMedia clients.

6. Click Save to add the new role group and return to the Role Group List.

To Delete a Role Group

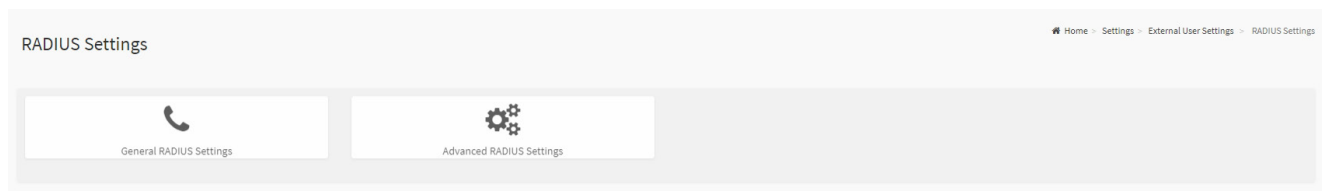
1. In the Role Groups Page, select the row that you wish to delete.
2. Click Delete Role Group.

8.2.6.4 RADIUS Settings

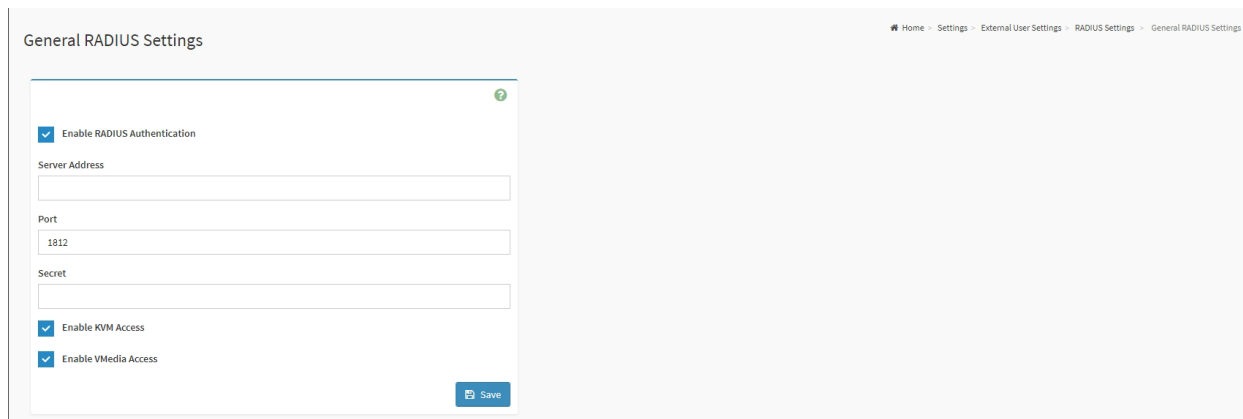
RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.

In MegaRAC GUI, this page is used to set the RADIUS Authentication.

To open RADIUS Settings page, click **Settings -> External User Settings -> RADIUS Settings** from the menu bar. A sample screenshot of RADIUS Settings page is shown below.



General RADIUS Settings



The screenshot shows the 'General RADIUS Settings' form. It includes a checkbox for 'Enable RADIUS Authentication' which is checked. Below this are input fields for 'Server Address', 'Port' (with '1812' entered), and 'Secret'. There are also checkboxes for 'Enable KVM Access' and 'Enable VMedia Access', both of which are checked. A 'Save' button is located at the bottom right of the form area. The breadcrumb trail at the top right reads: Home > Settings > External User Settings > RADIUS Settings > General RADIUS Settings.

The fields of General RADIUS Settings page are explained below.

Enable RADIUS Authentication: Option to enable/disable RADIUS authentication.

Server Address: The IP address of RADIUS server.

Note:

- *IP Address (Both IPv4 and IPv6 format).*
- *FQDN (Fully Qualified Domain Name) format.*

Port: The RADIUS Port number.

Note:

- *Default Port is 1812.*
- *Port value ranges from 1 to 65535.*

Secret: The Authentication Secret for RADIUS server.

Note:

- *This field will not allow more than 31 characters.*
- *Secret must be at least 4 characters long.*
- *White space is not allowed.*

Enable KVM Access: This field provides access to KVM for RADIUS authenticated users.

Enable VMedia Access: This field provides access to VMedia for RADIUS authenticated users.

Save: To save the settings.

Procedure

1. Enable the RADIUS Authentication check box to authenticate the RADIUS.
2. Click Advanced RADIUS Settings. This opens the Radius Authorization window as shown below.

Note:

It will not allow more than 127 characters. Special characters like ‘;’ and ‘#’ are not allowed.

It is recommended to Enable Radius configuration from configure general RADIUS settings page otherwise error message will pop-up stating that "Radius configuration is not enabled" while trying to create/view Advanced RADIUS Settings.

Advanced RADIUS Settings Home > Settings > External User Settings > RADIUS Settings > Advanced RADIUS Settings

RADIUS Authorization ?

Administrator
H=4

Operator
H=3

User
H=2

OEM Proprietary
H=1

No Access
H=0

 Save

For Authorization Purpose, configure the Radius user with Vendor Specific Attribute in server side.

Example:1

testadmin Auth-Type :=PAP,Cleartext-Password:= "admin"

Auth-Type :=PAP, Vendor-Specific="H=4"

Example:2

testoperator Auth-Type := PAP, Cleartext-Password := "operator"

Auth-Type :=PAP, Vendor-Specific="H=3"

If you change the Vendor-Specific value in server then you should change the same values in this page.

3. Click **Save** to save the changes made.

8.2.6.5 Service Management

It is used to set service information on the BMC. A sample screenshot of service management is shown as below.

Services Home					
Service	Status	Interfaces	Secure Port	Timeout	Maximum Sessions
web	Active	both	443	1800	20
kvm	Active	both	443	1800	4
cd-media	Active	both	443	N/A	4
hd-media	Active	both	443	N/A	4
ssh	Active	NA	22	600	N/A
watchdog	Inactive	NA	N/A	N/A	1

The service management consists of the following items.

- web
- kvm
- cd-media
- hd-media
- ssh
- watchdog

(Click the "edit" button in the "watchdog" column to enter the "watchdog" configuration interface (the interface is as follows), watchdog default state is inactive, if watchdog is set to the active state, it will monitor the BMC in real time.)

Service Configuration

Service Name

watchdog

☐ Active

Maximum Sessions

1

Save

8.2.6.6 Network Configuration

Note: Change the IP settings of the management ports will disconnect the network.

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

8.2.6.6.1 Network IP Settings

This section is used to configure the network IP settings.

To open the Network IP Settings page, click **Settings -> Network Settings -> Network IP Settings**.

The fields of Network IP Settings page are explained below.

- ✧ **Enable LAN:** Enable or disable the LAN settings.
- ✧ **LAN Interface:** Select the LAN interface to be configured.
- ✧ **MAC Address:** Display the read-only MAC Address of the selected interface.
- ✧ **Enable IPv4:** Enable or disable the IPv4 settings for the selected interface.
- ✧ **Enable IPv4 DHCP:** Enable or disable the IPv4 DHCP support for the selected interface. If disable the IPv4 DHCP support, then **static IP address** is selected, configure the static **IPv4 Address**, **IPv4 Subnet**, and **IPv4 Gateway**.

Notes:

- ✓ An IP address consists of 4 numbers separated by dots, as in "xxx.xxx.xxx.xxx".
- ✓ Each number ranges from 0 to 255.
- ✓ The first number must not be 0.

☒ Enable IPv6

☐ Enable IPv6 DHCP

IPv6 Index

IPv6 Address

Subnet Prefix Length

IPv6 Gateway

- ✧ **Enable IPv6:** Enable or disable the IPv6 configuration settings.
- ✧ **Enable IPv6 DHCP:** Enable or disable the IPv6 DHCP support for the selected interface. It dynamically configures IPv6 address using DHCP (Dynamic Host Configuration Protocol).
Note: Disable this **Enable IPv6 DHCP** field and enter the values in following fields such as **IPv6 Index**, **IPv6 Address**, **Subnet Prefix Length** and **IPv6 Gateway**.
- ✧ **IPv6 Index:** Specify a static IPv6 index to be configured to the device. E.g.: 0
- ✧ **IPv6 Address:** Specify a static IPv6 address to be configured to the device. E.g.: 2004::2010.
- ✧ **Subnet Prefix Length:** Specify the subnet prefix length for the IPv6 settings. The value ranges from 0 to 128.
- ✧ **IPv6 Gateway:** Specify an IPv6 default gateway for the IPv6 settings.

☐ Enable VLAN

VLAN ID

VLAN Priority

- ✧ **Enable VLAN:** Enable or disable VLAN support for the selected interface.
- ✧ **VLAN ID:** Value ranges from 2 to 4094. VLAN ID 0, 1 & 4095 are reserved VLAN IDs.
- ✧ **VLAN Priority:** Value ranges from 0 to 7. 7 is the highest priority for VLAN.
- ✧ **Save:** Save the entries.

8.2.6.6.2 Network Link Configuration

This section is used to configure the network link.

To open Network Link Configuration page, click **Settings > Network Settings > Network Link Configuration**.

Network Link Configuration

Home > Settings > Network Settings > Network Link Configuration

LAN Interface

eth1

☒ Auto Negotiation

Link Speed

100 Mbps

Duplex Mode

FULL Duplex

NCSI Interface

Enabled

Save

The fields of the 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 are to be configured.
- ✧ **Auto Negotiation:** Enable 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:** This field could be either **Half Duplex** or **Full Duplex**.
- ✧ **NCSI Interface:** The NCSI interface status could be either **Enabled** or **Disabled** for the selected LAN interface.
- ✧ **Save:** Save the settings.

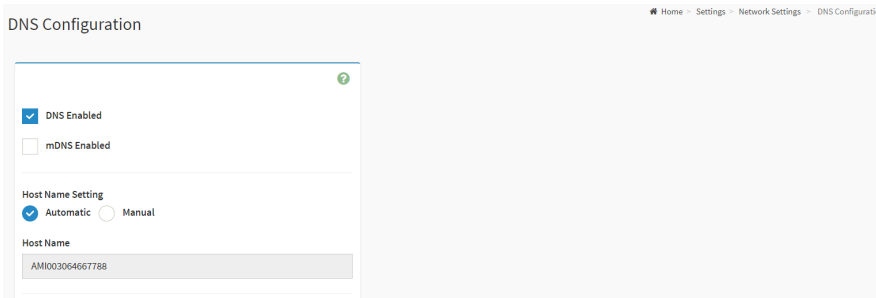
8.2.6.6.3 DNS Configuration

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.

This section is used to manage the DNS settings of a device.

To open DNS Configuration page, click **Settings > Network Settings > DNS Configuration**.



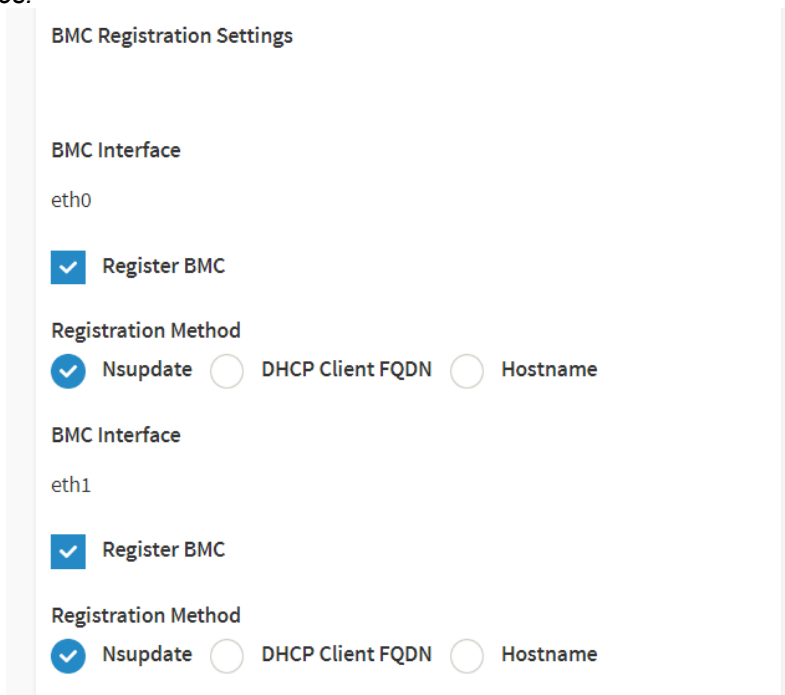
The fields of DNS Configuration page are explained below.

Domain Name Service Configuration

- ✧ **DNS Enabled:** Enable or disable all the DNS service configurations.
- ✧ **mDNS Enabled:** Enable or disable the multicast DNS.
- ✧ **Host Name Setting:** Choose either **Automatic** or **Manual** settings.
- ✧ **Host Name:** Display host name of the device.
 - If the Host setting is chosen as **Manual**, then specify the host name of the device.

Notes:

- ✓ Value ranges from 1 to 64 alpha-numeric characters.
- ✓ Special character '-'(hyphen) is allowed.
- ✓ It must not start or end with a '-'(hyphen).
- ✓ The underscore (_) character and double hyphen (--) character are not a legal character for use in host names.



BMC Registration Settings

- ✧ **BMC Interface:** Options to register the BMC through the Interfaces (eth0ð1).
- ✧ **Register BMC:** Register BMC through registration method.
- ✧ **Registration Method:** Options to register the BMC through **Nsupdate** or **DHCP Client FQDN** or **Hostname**.

The screenshot shows the BMC Registration Settings interface. At the top, there is a checkbox labeled "Both". Below this, the "Eth0 TSIG Configuration" section contains a checkbox for "TSIG Authentication Enabled", a section for "Current TSIG Private File Information" showing "Not Available", and a "New TSIG Private File" section with a file upload button. The "Eth1 TSIG Configuration" section follows a similar layout with its own checkboxes and file upload options.

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 Information:** The information of current TSIG private file along with its uploaded date and time will be displayed (read only).
 - **New TSIG Private File:** Browse and navigate to the TSIG private file.

The screenshot shows the Domain Setting configuration interface. It features two radio buttons: "Automatic" (which is selected) and "Manual". Below this is a "Domain Interface" section with a dropdown menu currently displaying "eth1_v4".

- ✧ **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.
 - **Manual:** If you select **Manual**, then specify the domain name of the device.

Notes:

- ✓ If you select **Automatic**, it displays the **Domain Interface** option. If you select **Manual**, it displays **Domain name**.
- ✓ Domain name must be a string of 4 to 253 alphanumeric characters. (254 characters are allowed only if the last byte is dot.)

- ✓ Domain name must start with a letter and end with a letter or digit. (Must contain at least one dot character) Only letters, digits, dot and hyphen are allowed.

Domain Name Server Setting

☒ Automatic
 ☐ Manual

DNS Interface

eth0

IP Priority

☒ IPv4
 ☐ IPv6

Save

- ✧ **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:**
 - **IPv4:** It will have 2 IPv4 DNS servers and 1 IPv6 DNS server.
 - **IPv6:** It will have 2 IPv6 DNS servers and 1 IPv4 DNS server.
 - Note:** This is not applicable for Manual configuration.
- ✧ **DNS Server 1, 2 & 3:**
Specify the DNS (Domain Name System) server address to be configured for the BMC.
- Notes:**
 - 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:** Save the entered changes.

8.2.6.6.4 Sideband Interface (NC-SI)

This section is used to configure Network Controller Sideband Interface (NCSI) settings.

To open the Sideband Interface (NC-SI) page, click **Settings > Network Settings > Sideband Interface (NC-SI)**.

Sideband Interface (NC-SI) Home > Settings > Network Settings > Sideband Interface (NC-SI)

NCSI Mode

☒ Auto Failover Mode ☐ Manual Switch Mode

NCSI Interface

eth1

Package ID

0 (active)

Channel Number

0 (package 0)(active)

Save

The fields of the Sideband Interface (NC-SI) page are explained below.

- ✧ **NCSI Mode:**
 - If you select **Auto Failover Mode**, the NCSI interface and other settings will be configured automatically.
 - If you select **Manual Switch Mode**, you are allowed to configure the below settings.
- ✧ **NCSI Interface:** Select the NCSI interface for which you need to configure NCSI settings.
- ✧ **Package ID:** Select the package ID to be configured for the selected interface.
- ✧ **Channel Number:** Select the channel number to be configured for the selected interface.
- ✧ **Save:** Save the settings.

8.2.7 Remote Management

The "Remote Control" includes two functions: KVM and SOL, KVM is mainly used to remotely access the x86 system through WEB, and SOL is mainly to access x86 BIOS configuration information through WEB, WEB UI is as follows.

Remote Control Remote KVM & SOL

H5Viewer

[Click here to go to Remote Session Settings.](#)

Launch H5Viewer

Serial Over LAN

Activate

8.2.7.1 KVM

Launch H5Viewer

The system and browser requirements for Remote Control are given below.

System Requirements

Client machine with 8GB RAM.

If the client machine has 4GB RAM or lower, there will be lag in Video/Keyboard/ Mouse/Media redirection functionality.

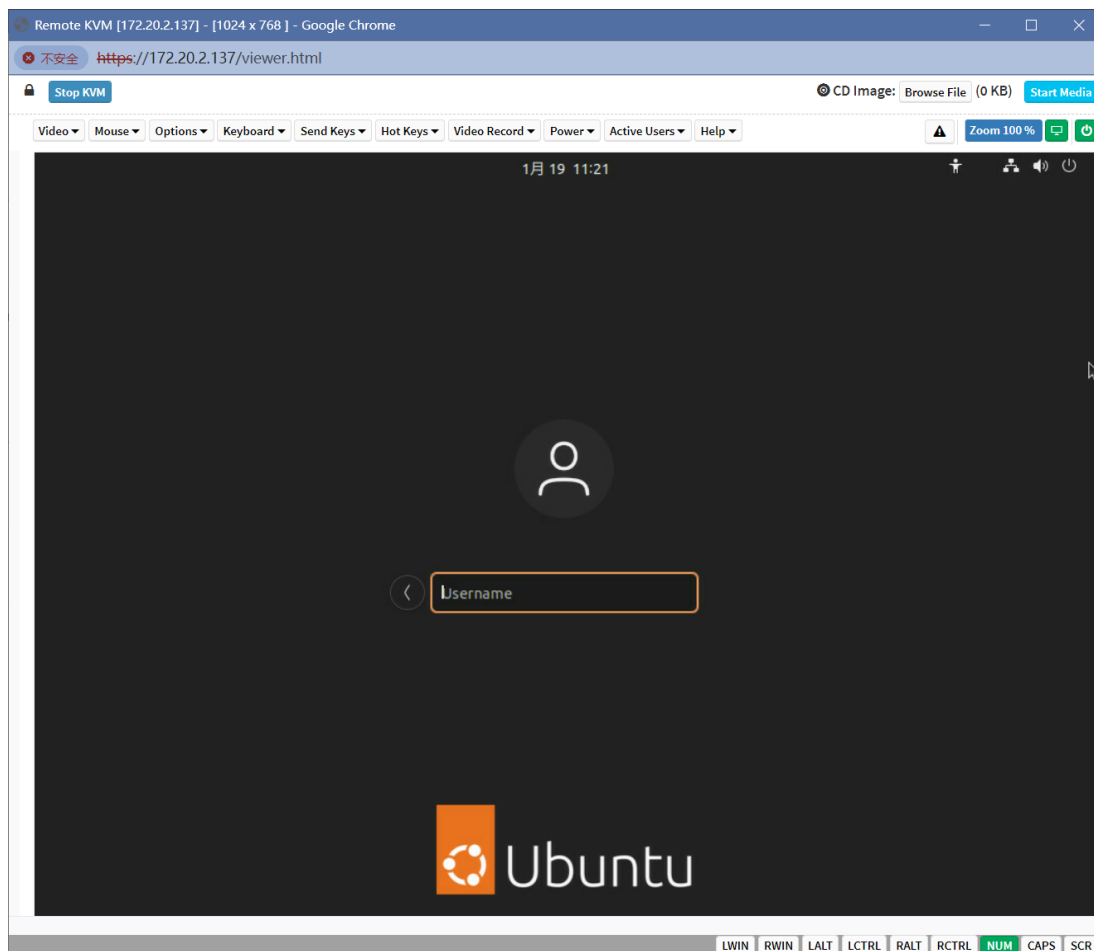
Supported Browsers

- ✧ Chrome latest version
- ✧ IE11 and above
- ✧ Firefox (with limited support)
- ✧ Edge
- ✧ Safari (On Mac only)

Note: It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations.

To open Remote Control page, click Remote Control from the menu bar. A detailed description of the menu items is given below.

Open the "Remote Control" page, click "Launch H5Viewer". A sample screenshot of the Remote KVM page is shown below.

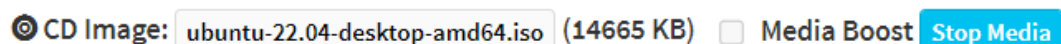


Procedure to Start KVM

1. Click Launch H5Viewer to open the Remote Control KVM page.
2. To stop the H5Viewer video redirection, click Stop KVM.

Procedure to Start /Stop Media

1. Click **Browse File** to select CD Image. After selecting the image, **Select/Unselect** media boost option.
2. Click **Start Media** to redirect the selected CD image file to the Host. A sample screenshot is as shown below.
Note: If media boost mode is selected, the processes related to media redirection will have high priority than other processes. This will improve media performance but other processes will have limited access to CPU cycle.



3. To stop the CD Image redirection, click **Stop Media**.

A detailed description of menu items are given below.

Video

This menu contains the following sub menu items.

Pause Video: This option is used for pausing Console Redirection.

Resume Video: This option is used to resume the Console Redirection when the session is paused.

Refresh Video: This option can be used to update the display shown in the Console Redirection window.

Capture Screen: This option helps to take the screenshot of the host screen and save it in the client's system.

Mouse

Show Client Cursor: This menu item can be used to show or hide the local mouse cursor on the remote client system.

Mouse Mode: This option handles mouse emulation from local window to remote screen using either of the two methods. Only Administrator has the right to configure this option.

- **Absolute mouse mode:** The absolute position of the local mouse is sent to the server if this option is selected.
- **Relative mouse mode:** The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.
- **Other mouse mode:** This mouse mode sets the client cursor in the middle of the client system and sends the deviation to the host. This mouse mode is specific for SUSE Linux installation.

Note: AMI MegaRAC SP-X suggests users to use Linux version of OS except SUSE11.4 with BMC to avoid mouse sync issue in absolute mouse mode.

Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu.

Options

Zoom:

Normal - By default, this option is selected.

Zoom In - For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%

Zoom Out - For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%

Block Privilege Request: To enable or disable the access privilege of the user.

***Compression Mode:** This option helps to compress the Video data transfer to the specific mode.

***DTC Quantization Table:** This option helps to choose the video quality.

Note: *Specific to AST SOC.

Keyboard

Keyboard Layout: This feature is fully compatible when host and client has the same keyboard language layout. If the client and host language layouts differ, some special characters will not be compatible.

List of Host Physical Keyboard languages supported in SPX H5Viewer.

- English U.S.
- German.
- Japanese.

Send Keys

This option is used to key items. This menu contains the following sub menu items.

Hold Down
Press and Release

Hold Down

This menu contains the following sub menu items.

Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.

Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection.

Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.

Left Alt Key: This menu item can be used to act as the left-side <ALT> key when in Console Redirection.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Press and Release

Ctrl+Alt+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT>and keys down simultaneously on the server that you are redirecting.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection.

Context Menu Key: This menu item can be used to act as the context menu key, when in Console Redirection.

Print Screen Key: This menu item can be used to act as the print screen key, when in Console Redirection.

Hot Keys

This menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.

This menu contains the following sub menu items.

- **Add Hot Keys** - This menu is used to enable macros. Click **Add** to macros.

Video Record

This menu contains the following sub menu items.

Record Video: This option is to start recording the screen.

Stop Recording: This option is used to stop the recording.

Record Settings: This option is used to set video record duration and video compression value. Video record duration value should be in the range of 1 to 1800 seconds. Video Compression value should be in the range of 0.1 (Low image quality) to 1.0 (High image quality).

Normalized video resolution to 1024 X 768 (*specific to AST SOC): Host video will be scaled to 1024 x 768 in the recorded video file. Enabling this option improves client-side video recording performance in H5Viewer.

Disable this option to record video at same resolution as host video. The host video capture depends on client system performance. If this option is disabled, recorded video file may have inconsistency. (i.e., Recorded video file duration may not be the same as configured value).

Note:

The Maximum video file size allowed is around 40MB. If the video file size reaches its max size limit, the recorded file is downloaded and recording will be in progress until the configured video recording time is reached. The video file is saved as video date-month-year hr-min-sec part no in client side video recording.

User have to take care of saving the video files in different browsers.

When H5Viewer focus is lost and if video recording is in progress, the recording will be stopped with a notification message and the recorded video file will be discarded.

Due to browser limitation, Set timeout/set interval will be delayed from specified time of interval when browser window loses focus, hence video server will not send the video packets to H5Viewer and so the video recording will be stopped.

Power

The power options are to perform any power cycle operation. Click on the required option to perform the following operation.

Reset Server: To reboot the system without powering off (warm boot).

Immediate Shutdown: To perform Power OFF Immediately.

Orderly Shutdown: To Power OFF the server in proper order.

Power ON Server: To Power ON the server.

Power Cycle Serve: To first power off, and then reboot the system (cold boot).

Active Users

Click this option to display the active users and their system IP address.

Active KVM Session can be terminated when there are multiple KVM Session from Master [FULL Privilege KVM Session].

Help

Click this option to get more information About H5Viewer. The KVM Remote Console utility version and plugin version will be displayed.

Quick Buttons

Quick Buttons: The upper right of H5Viewer window displays all the quick buttons. These quick buttons allow you to perform the below functions by clicking them.

Quick Buttons	Explanation
	This quick button will show / hide notifications dropdown menu, which will contain the list of notifications displayed by H5Viewer.
	It shows the current zoom value in percentage.
	This quick button is used to display the current host monitor status. If icon is in green color, then host monitor is unlocked. If the icon is in red color host monitor is locked. By clicking the button, host monitor status can be toggled.

Quick Buttons	Explanation
	This quick button is used to display the current server power status. If the icon is in green color, the server status is powered on. If the icon is in red color, the server status is powered off. Click the button to toggle immediate power off / power on the host.

Status bar buttons



Num/Caps/Scroll lock buttons are LED status buttons that denotes the current status of Num/Caps/ Scroll lock in the host.

Keyboard LED Sync

When the H5Viewer is launched, the keyboard locks status and LEDs denoting the lock status of the host machine, should be in sync with the client machine. That is, if the Num/Caps/Scroll lock is enabled/disabled in the client machine, the same should be updated in the host machine as well.

Note:

Client-Side Limitations

Due to web browser related security concerns, this feature has following limitations.

- Host LED status will be synced with client LED status, only if user presses any key in client keyboard when H5Viewer window is in focus.
- Client keyboard LED status cannot be updated from web browsers.

Host Side Limitations

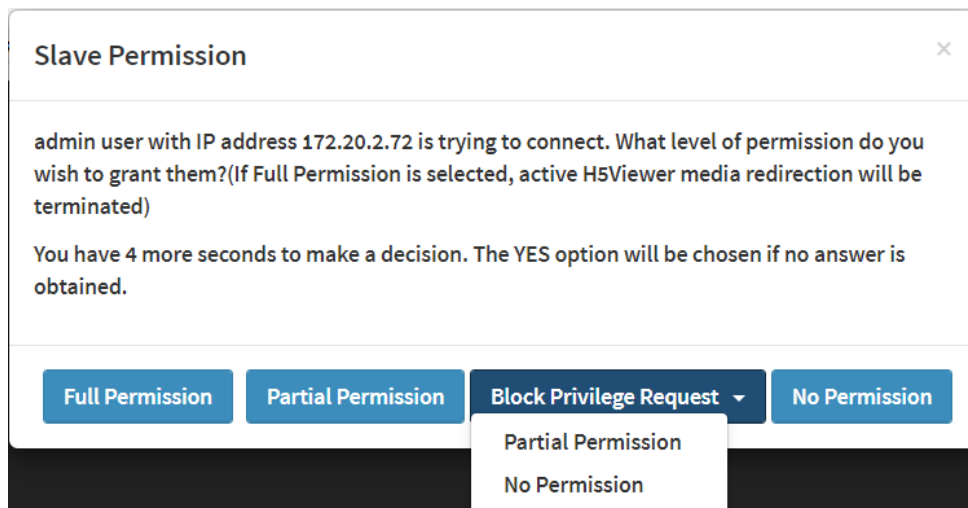
- In some Linux hosts, when the host is booted into text mode, CAPS LOCK LED status will not be updated properly. CAPS LOCK LED will not turn ON/OFF while changing the CAPS lock status in the host OS.
- In such cases, H5Viewer CAPS LOCK synchronization functionality will not work properly.
- Example - Typing letters in H5Viewer (after pressing CAPS LOCK) will toggle between lower to upper case inside host.

KVM Sharing

MegaRAC SP-X stack supports N number of KVM redirection sessions. Only one full permission H5Viewer session at a time. With Full permission in H5Viewer, the user can control the KVM redirection, and the other H5Viewer users can only view the video redirected from the server without intervention.

When the First user launches H5Viewer, the user will get full permission to control the host during KVM redirection. When another H5Viewer session is launched, the Video server will send KVM sharing permission request packet to the current session, for the new Requesting session.

Once the requesting session is authenticated, a packet containing the information such as the client IP/hostname and user name of the newly authenticated or logged in user, will be send to the current session. The first client shows the dialog as a shown below:



Clicking the button in the dialog box will trigger specified action:

Full Permission: When this button is clicked, the requesting session will receive full access permission, and the current (full permission) session will have a partial KVM access permission only.

Partial Permission: When this button is clicked, the requesting session will receive partial permission and can only view server display (Video only).

Block Privilege Request > Partial Permission: Once this option is selected, both newly requesting session and active partial privileged session will get partial permission as auto response and can only view server display. Further request will be served by auto response mechanism.

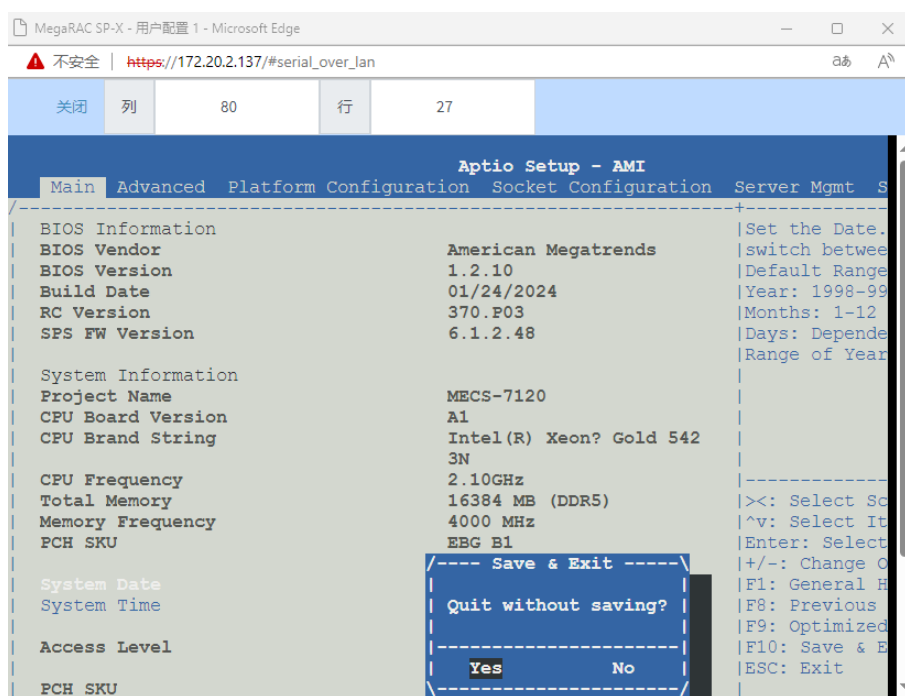
Block Privilege Request > No Permission: Once this option is selected, both newly requesting session and active partial privileged session access will be denied as auto response. Further request will be served by auto response mechanism.

No Permission: When this button is clicked, the requesting session access will be denied.

8.2.7.2 SOL

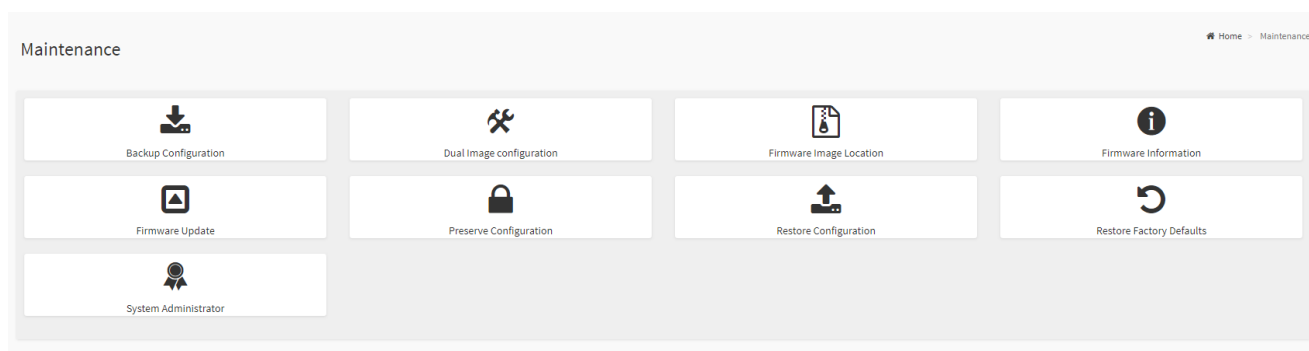
The serial over LAN (SOL) feature is very useful, and the SOL redirects the local serial interface via an IPMI session, allowing remote access to the console.

Click the "**Active**" button on the "Remote Control" interface to enter the SOL output window, and then enter the BIOS configuration interface, and the content of the BIOS configuration will be redirected to the WEB UI, as shown in the following figure.



8.2.8 Server Maintenance

This function is mainly maintenance tasks on the device. Click Maintenance on the left function bar to enter the following interface.



8.2.8.1 Firmware Update

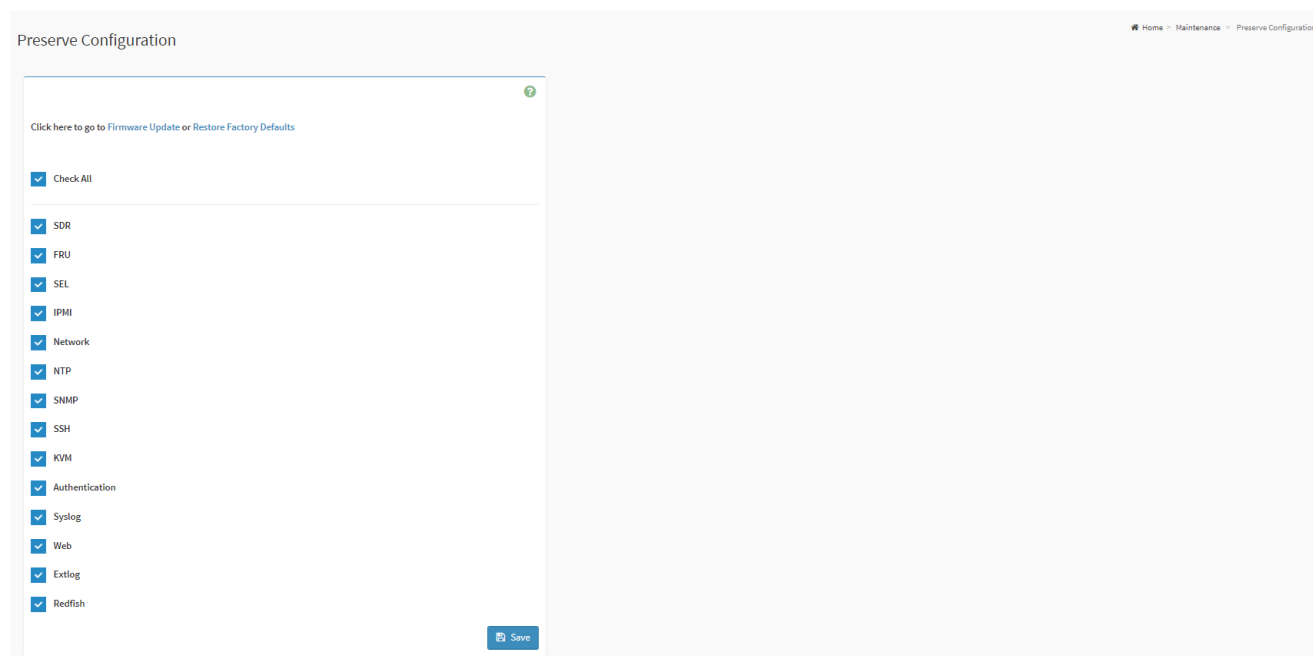
The system upgrade function is for updating and maintaining the system. Mainly used to update BMC and BIOS. Here's how to update via the Web.

8.2.8.1.1 BMC Update

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.



The various fields of Preserve Configuration are as follows.

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

Check All: To check the entire configuration list.

Save: To save any changes made.

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.

Firmware Update

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

To perform Dual Firmware Update operation, click **Maintenance > Firmware Update** from the menu bar.

Procedure

1. Click **Browse** to select firmware image.
Note: A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of upload.
2. Click **Start firmware update** to load the Firmware Update information. A sample screenshot is displayed below.

Firmware Update

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

- Dual Firmware update.
 - HPM Firmware update supports the following components.
 - BOOT and APP
 - BIOS
 - BIOS Firmware update

Select Firmware Image

Start firmware update

Protocol Type: HTTPS

The dual image formation to be used for firmware update is displayed as follows. To configure Image to be booted from upon Reset, choose 'Dual Image Configuration' under Maintenance.

Current Active Image: Image-1

Image to be Updated: Inactive Image

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

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

[Edit Preserve Configuration](#)

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

Proceed to Flash

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

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

• **Image to be Updated:** To update an Image (Inactive, Image 1, Image 2 or Both) to be flashed. If You select an Inactive image, the Inactive image will be flashed. If you select both images, then Both Image 1 and Image 2 will be flashed with uploaded image file.

• **reboot the device after update:** This option is used to reboot the device after the firmware update.

Protocol Type: HTTPS

The dual image formation to be used for firmware update is displayed as follows. To configure Image to be booted from upon Reset, choose 'Dual Image Configuration' under Maintenance.

Current Active Image: Image-1

Image to be Updated

Inactive Image

Inactive Image

Image 1

Image 2

Both Images

4. Click **Preserve** all Configuration to preserve all configuration.
 - **Preserve all Configuration:** To preserve all configuration.
 - **Edit Preserve Configuration:** To modify the Preserve status settings.
5. Click **Proceed** to Flash, it will prompt you with the warning message. Click **Ok** to start the Firmware update.

The Dual Firmware Update undergoes the following steps:

- a) Closing all active client requests
- b) Preparing Device for Firmware Upgrade
- c) Uploading Firmware Image
- d) Verifying Firmware Image:
 - In **Section Based Firmware Update**, you can configure the firmware image for section-based flashing. Check the required sections and click **Proceed** to update the firmware.
 - If flashing is required for all images, select the option **Full Flash**.
 - If you select **Version Compare Flash** option from web, the current and uploaded module versions, FMHlocation, size will be compared.
 - If the modules differ in size and location, proceed with force firmware upgrade.
 - If all the module versions are same, restart BMC by saying all the module versions are similar.
 - If only a few module versions differ, those modules will be flashed.

Section Based Firmware Update

The following section is used to allow the user to configure the firmware image for section based flashing.

☐ Version Compare Flash

☐ Full Flash

Section Name	Image-1 Version	Image-2 Version	Uploaded version	Upgradable/Non-Upgradable
boot	13.5.000000	13.5.000000	13.5.000000	☐
conf	13.5.000000	13.5.000000	13.5.000000	☐
root	13.5.000000	13.5.000000	13.5.000000	☐
osimage	13.5.000000	13.5.000000	13.5.000000	☐
www	13.5.000000	13.5.000000	13.5.000000	☐
extlog	13.5.000000	13.5.000000	13.5.000000	☐
extlog	13.5.000000	0.0.	13.5.000000	☐
bootlogo	1.0.000000	1.0.000000	1.0.000000	☐
arcity	13.5.010003	13.5.010002	13.5.010003	☐

- e) Flashing Firmware Image
- f) Resetting the image

8.2.8.2 BIOS Update

This wizard takes you through the process of BIOS firmware upgradation.

To perform BIOS Firmware Update operation, click **Maintenance > Firmware Update**.

[Home](#) > [Maintenance](#) > [Firmware Update](#)

?

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

- Dual Firmware update.
- HPM Firmware update supports the following components.
 - BOOT and APP
 - BIOS
- BIOS Firmware update.

Select Firmware Image

MECS-7120_1110.BIN

...

Start firmware update

Preparing to flash...

Proceed

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

Procedure

1. Click **Browse** to select BIOS Firmware Image.
Note: Firmware update wizard will detect *.bin* and *.bin_enc* extensions, and validate as BIOS firmware image.
2. Click **Start firmware update** to load the BIOS firmware image information.
3. Click **Proceed**, it will prompt you with the warning message. Click **OK** to start the firmware update.

172.20.2.12 says

Are you sure you want to flash?

OK

Cancel

4. Select the components from the list to flash. **BIOS** is mandatory, **ME** and **NVRAM** are optional.

Firmware Update

Home > Maintenance > Firmware Update

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

- Dual Firmware update.
- HPM Firmware update supports the following components.
 - BOOT and APP
 - BIOS
- BIOS Firmware update.

Select Firmware Image

MECS-7120_1110.BIN

Start firmware update

Preparing to flash...

List of Components

#	Component Name	Existing Version	Uploaded Version	Upgrade	Progress
1	BIOS		2280811	☒	In progress...
2	ME			☐	
3	NVRAM			☐	

Proceed to flash image Cancel

Uploading 100%

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

5. Click **Proceed to flash image**, it will prompt you with the selection message. Click **Cancel**, the update will be cancelled.

172.20.2.12 says

Are you sure the BIOS upgrade takes effect immediately? If yes, BMC will power off and power on the chassis after flash update. If no, the BIOS upgrade will take effect when the chassis is powered off.

OK

Cancel

- Click **OK**: Update the device immediately, the chassis will be powered cycle. Once the BIOS firmware update is completed, it will prompt you with the success message. Click **OK** to complete the process.

172.20.2.12 says

The device has been updated successfully.

OK

- Click **Cancel**: Update the device when the chassis is powered off. It will prompt you with the notification message. Click **OK** to complete the process.

172.20.2.12 says

The BIOS upgrade will take effect when the chassis is powered off.

OK

8.2.8.2.1 HPM Firmware Update – CPLD/BIOS

To perform HPM Firmware Update operation, click **Maintenance > Firmware Update** from the menu bar.

Note: For BIOS or CPLD firmware update, it is required to hash its uploaded image via creating HPM image utility.

Create HPM Image

```
./CreateHPMImage create hpmimage.conf
```

CreateHPMImage is the creating HPM image utility from AML.

Sample of hpmimage.conf

```
[GLOBAL]
DeviceID = 0x20 ;1B Device ID as per IPMI
ManufacturerID = 0x005f13 ;3B Manufacturer ID as per IPMI
ProductID = 0x7120 ;2B Product ID
HPMImage = /home/bmc/outputjbc_02b4.hpm ;Path & Filename of final output HPM Image
[CPLD] ;Component Type: BIOS, CPLD
UpgradeActionType = 0x02 ;1B Upgrade Action Type: 0x02 = Upload, 0x03 - 0xFF = Reserved
FwVersionMajor = 0x02 ;1B This component's Major Version
FwVersionMinor = 0x04 ;1B This component's Minor Version
FwVersionAux = 0x02200000 ;4B This component's Aux Version
FwDescription = "cpld" ;21B Firmware Description String to be used
FwData = /home/bmc/cpld_02b4.jbc ;Path & Filename of Component's Image
SectionFlash = 0x0 ;For Section based flashing of the particular component 0 -
disabled 1 - enabled
```

Note: The CPLD Image should be a .jbc file and enable the option "**Enable real-time ISP to allow background programming when available**".

☒ Enable real-time ISP to allow background programming when available

Procedure for CPLD Firmware Update

1. Select HPM format of CPLD supported image to perform the CPLD Firmware Update.
2. Click **Start firmware update** to load the Firmware Update information. Once the image is successfully uploaded, the uploaded image information such as **Component Name**, **Existing Version**, **Uploaded Version** and **Upgrade** will be displayed as shown in the screenshot below. In addition, all the CPLD devices information such as **Name**, **Interface**, **Interface Number**, **ID code** and **Firmware Version** will be displayed as well. User can select the device that needs to be updated.

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

- Dual Firmware update.
- HPM Firmware update supports the following components.
 - BOOT and APP
 - BIOS
 - CPLD
- BIOS Firmware update

Select Firmware Image

outputjbc_02b4.hpm

Start firmware update

Preparing to flash...

☒ Update All

List of Components

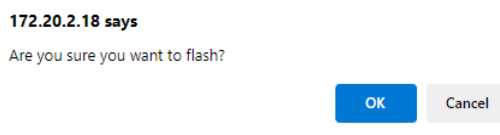
#	Component Name	Existing Version	Uploaded Version	Upgrade
1	CPLD	0.0.0	2.4.35651584	☒

List of CPLD devices

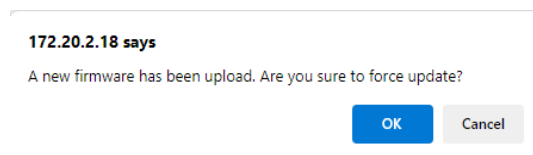
Name	Interface	Interface Number	ID Code	Firmware Version
ALTERA 10M50DA CPLD	JTAG	0x0	0x31050dd	0x65bba5

Proceed

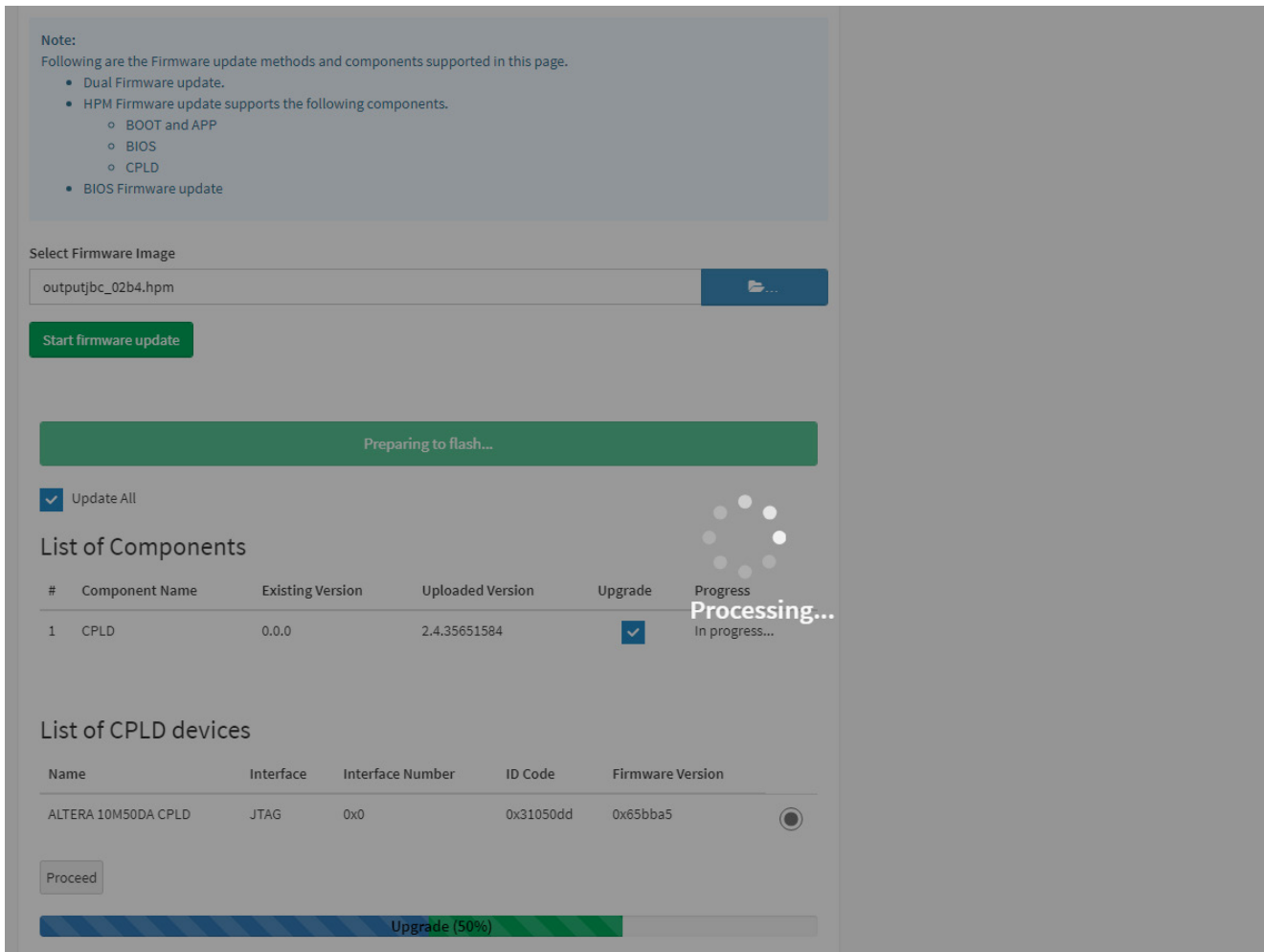
3. Click **Proceed**, it will prompt you with the warning message. Click **OK** to start the firmware update.



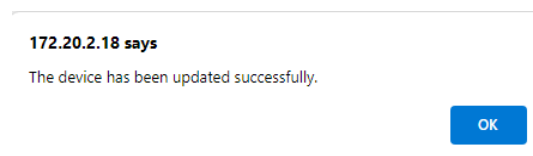
If a CPLD firmware has been uploaded, it will prompt you with the selection message. Click **Cancel**, the update will be cancelled.



A sample screenshot is shown below:



- Once the CPLD Firmware Update process is completed, an alert message will be displayed as shown in the screenshot below.



8.2.8.3 Firmware Configuration

8.2.8.3.1 Dual Image Configuration

This page is used to configure the dual image information. Dual Image support feature is helpful to store two firmware images on two SPI flash, and boot any of the image according to users request.

The running firmware is responsible for setting the Boot Selector options and Firmware Upload Selector options.

To open Dual Image Configuration, click **Maintenance > Dual Image Configuration** from the menu bar. A sample screenshot of Dual Image Configuration page is shown below.

Dual Image configuration

Home > Maintenance > Dual Image configuration

IMAGE 1

Firmware Version	13.05.10003
State	Active
☒ Image to be booted from upon reset	

IMAGE 2

Firmware Version	13.05.10002
State	stand-by
☐ Image to be booted from upon reset	

☐ Higher firmware version
☐ Lower firmware version
☐ Most recently updated firmware
☐ Least recently updated firmware

Save

The various options of Dual Image Configuration are given below.

Firmware Version: Displays the firmware version of both images.

State: Displays the current state of both images.

Image to be booted from upon reset: This option is to boot particular image (either 1 or 2) in the next boot up process.

Higher firmware version: This option is to boot higher firmware version image among the dual images in the next boot up process.

Lower firmware version: This option is to boot lower firmware version image among the dual images in the next boot up process.

Most recently updated firmware: This option is to boot most recently updated firmware image among the dual images in the next boot up process.

Least recently updated firmware: This option is to boot least recently updated firmware image among the dual images in the next boot up process.

Procedure

1. Select the required image to be configured or the required option for Image setting.
2. Click **Save** to save the changes.

Fail Safe Booting Configuration:

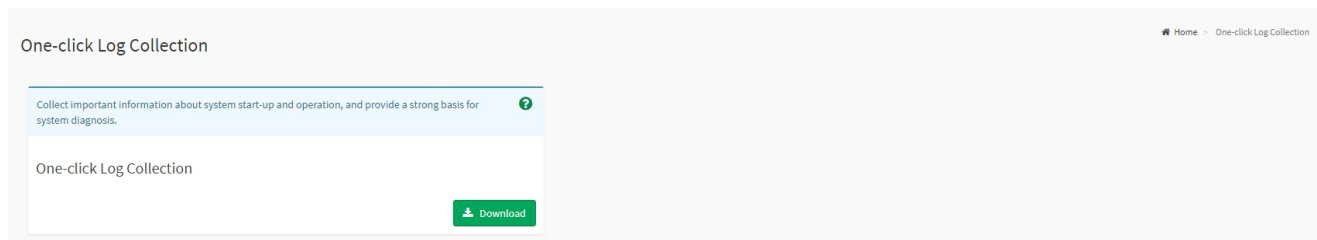
Hardware based fail safe boot support: This feature supports switching to secondary image as failsafe using hardware configurations. Using this feature, the user can boot into secondary image, even though primary uboot is crashed. Please verify whether SOC supports this feature.

Software FailSafe Boot: Legacy AMI dual image support. This feature uses common UBOOT which switches between 2 different images based on user requirement. This feature does not requires a special hardware support.

8.2.9 One-Click Log Collection

The One-Click Log Collection feature enables users to download essential BMC information data for detailed analysis of BMC status or issue identification.

To open the One-Click Log Collection, click **One-click Log collection** from the menu bar. A sample screenshot of Event Log page is shown below.



Click the "**Download**" button to automatically download the Log to the system.

The log package is named:

One-Click_Collection_Log_[time].zip

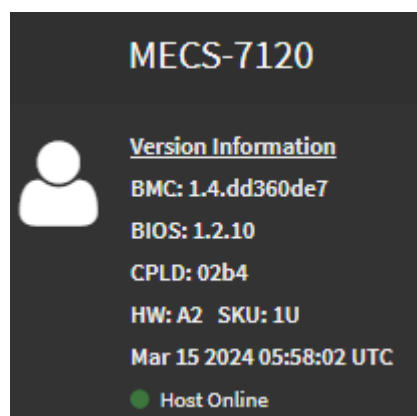
Inside the zip file, you will find the following folders:

- conf: Configuration files
- tmp: Temporary files
- var: Variable files

8.2.10 Firmware and Hardware versions

To get the version info of BMC, BIOS, CPLD and hardware, please refer to home page, up-left corner.

For example:



8.3 IPMI

Intelligent Platform Management Interface (IPMI) is a standardized interface used for managing a computer system and monitoring its operation. It provides a set of specifications for hardware-based management, independent of the operating system.

8.3.1 Overview of ipmitool

The ipmitool is a command-line utility that interfaces with the IPMI system. It allows administrators to execute a range of IPMI commands to manage and monitor servers. This tool is essential for system management, providing an interface to the IPMI functionalities of the server's BMC.

8.3.1.1 General Usage of ipmitool

The ipmitool allows for a range of operations through its command-line interface. The general syntax includes various parameters for network communication and authentication.

Common Parameters:

-H or --hostname: Hostname or IP address of the target server (for network interfaces).

-U or --user: Username for login.

-P or --password: Password for login (it's recommended to input interactively for security).

Parameter	Alias	Description
-H	--hostname	Hostname or IP address of the target server (for network interfaces).
-U	--user	Username for login.
-P	--password	Password for login (recommended to be input interactively for security).

8.3.1.2 Specific Interface Options

LAN Interface (lan)

Usage: ipmitool -I lan -H [hostname] -U [username] -P [password] [command]

Note: The LAN interface is suitable for local communication with IPMI. For remote management capabilities, the LANplus interface should be used.

Example:

```
~ # ipmitool -I lan -H 127.0.0.1 -U admin -P admin.123 mc info
IOCTL to get IP failed: -1
Device ID           : 32
Device Revision     : 1
Firmware Revision   : 1.03
IPMI Version        : 2.0
Manufacturer ID     : 24339
Manufacturer Name   : ADLINK Technology Inc.
Product ID          : 28960 (0x7120)
Product Name        : Unknown (0x7120)
Device Available    : yes
Provides Device SDRs : yes
Additional Device Support :
  Sensor Device
  SDR Repository Device
  SEL Device
  FRU Inventory Device
  IPMB Event Receiver
  IPMB Event Generator
  Chassis Device
Aux Firmware Rev Info :
  0x11
  0x0d
  0x10
  0xb9
```

LANplus Interface (lanplus)

Usage: ipmitool -I lanplus -H [hostname] -U [username] -P [password] [command]

Enhanced LAN interface with better encryption and additional features for secure remote communication.

Example:

```
root@adlink-Default-string:/home/adlink# ipmitool -I lanplus -H 172.20.2.137 -U admin -P admin.123 mc info
Device ID           : 32
Device Revision     : 1
Firmware Revision   : 1.03
IPMI Version        : 2.0
Manufacturer ID     : 24339
Manufacturer Name    : ADLINK Technology Inc.
Product ID          : 28960 (0x7120)
Product Name        : Unknown (0x7120)
Device Available     : yes
Provides Device SDRs : yes
Additional Device Support :
  Sensor Device
  SDR Repository Device
  SEL Device
  FRU Inventory Device
  IPMB Event Receiver
  IPMB Event Generator
  Chassis Device
Aux Firmware Rev Info :
  0x11
  0x0d
  0x10
  0xb9
```

KCS Interface (kcs)

Usage: ipmitool [command]

KCS (Keyboard Controller Style) is used for communication between the x86 segment and the BMC directly, without needing the -I parameter. It's used for local, direct communication with BMC.

Example:

```
root@adlink-Default-string:/home/adlink#
root@adlink-Default-string:/home/adlink# ipmitool mc info
Device ID           : 32
Device Revision     : 1
Firmware Revision   : 1.03
IPMI Version        : 2.0
Manufacturer ID     : 24339
Manufacturer Name    : ADLINK Technology Inc.
Product ID          : 28960 (0x7120)
Product Name        : Unknown (0x7120)
Device Available     : yes
Provides Device SDRs : yes
Additional Device Support :
  Sensor Device
  SDR Repository Device
  SEL Device
  FRU Inventory Device
  IPMB Event Receiver
  IPMB Event Generator
  Chassis Device
Aux Firmware Rev Info :
  0x11
  0x0d
  0x10
  0xb9
root@adlink-Default-string:/home/adlink#
```

8.3.2 ipmitool Command Introduction

This section is dedicated to introducing and explaining a variety of ipmitool commands, with detailed descriptions of their specific uses.

8.3.2.1 Sensor Information

The `ipmitool` command is used to retrieve sensor information, allowing system users to monitor various hardware sensors within the server. These sensors can include temperature, voltage, fan speed, and other key operating metrics.

List sensor information using `ipmitool` command:

Command:

```
ipmitool sensor
ipmitool sensor list
```

Return Details:

Return Details	Description
Sensor Name	Identifies the sensor.
Reading	The current value or status reported by the sensor.
Units	The measurement units for the sensor reading.
Status	Indicates the operational status of the sensor.
Lower/Upper Thresholds	The predefined limits for the sensor values, indicating warning or critical conditions.

Example:

```
root@adlink-Default-string:/home/adlink# ipmitool sensor list
P12V_PSU      12.230    Volts      ok         10.800    11.160    11.400    12.600    12.840    13.200
P12V_AUX      12.200    Volts      ok         10.800    11.160    11.400    12.600    12.840    13.200
P3V3         3.315    Volts      ok         2.970    3.069    3.135    3.465    3.531    3.630
P5V          5.120    Volts      ok         4.500    4.650    4.750    5.250    5.350    5.500
PVNN_PCH_AUX 0.905    Volts      ok         0.810    0.837    0.855    0.941    0.963    0.990
P1V05_PCH_AUX 1.057    Volts      ok         0.945    0.977    0.998    1.082    1.124    1.155
P1V8_AUX     1.816    Volts      ok         1.620    1.674    1.728    1.864    1.926    1.980
P3V_BAT      2.998    Volts      ok         2.002    2.302    2.500    3.148    3.208    3.298
PVCCIN_CPU   1.813    Volts      ok         1.441    1.489    1.519    1.891    1.927    1.981
P0V8_E810    0.822    Volts      ok         0.720    0.744    0.760    na        na        0.880
PVCCINF80N   1.090    Volts      ok         0.856    0.900    0.930    1.130    1.150    1.180
P3V3_AUX     3.300    Volts      ok         2.970    3.069    3.135    3.465    3.531    3.630
PVCCFA_EHV_FIVRA 1.812    Volts      ok         1.620    1.674    1.710    1.890    1.926    1.980
P0V9_E810    0.888    Volts      ok         0.810    0.837    0.855    0.945    0.963    0.990
PVCCD_HV     1.124    Volts      ok         0.990    1.030    1.050    1.192    1.220    1.270
P12V_S3_DIMM 12.060    Volts      ok         10.800    11.160    11.400    12.600    12.840    13.200
PCIE_Outlet_Temp 27.000    degrees C  ok         na        na        na        55.000    60.000    65.000
CPU_Outlet_Temp 33.000    degrees C  ok         na        na        na        na        na        na
SYS_Inlet_Temp 28.000    degrees C  ok         na        na        na        na        na        na
HDD_BP_Temp  22.000    degrees C  ok         na        na        na        47.000    51.000    55.000
CPU_Temp     37.000    degrees C  ok         na        na        na        91.000    95.000    99.000
CPU_TJMAX    97.000    degrees C  ok         na        na        na        na        na        na
PCH_Temp     31.000    degrees C  ok         na        na        na        na        na        na
DIMM_A1_Temp na        degrees C  na        na        na        106.000    116.000    125.000
DIMM_B1_Temp na        degrees C  na        na        na        106.000    116.000    125.000
DIMM_C1_Temp na        degrees C  na        na        na        106.000    116.000    125.000
DIMM_E1_Temp 31.000    degrees C  ok         na        na        na        106.000    116.000    125.000
DIMM_G1_Temp na        degrees C  na        na        na        106.000    116.000    125.000
DIMM_H1_Temp na        degrees C  na        na        na        106.000    116.000    125.000
ACPI_Power   0x0      discrete  0x0180    na        na        na        na        na        na
```

Other ipmitool Commands Related to Sensor Information

Below is a table summarizing additional `ipmitool` commands pertinent to sensor management and monitoring:

8.3.2.2 Power Control

Using ipmitool commands, you can effectively control the power mode.

8.3.2.2.1 Power Control Method

Using ipmitool command, it can control the power, such as power on, power off, power cycle, power reset.

Command:

```
ipmitool power <on | off | cycle | reset>
```

Command Element	Description
ipmitool power on	Power on the chassis.
ipmitool power off	Power off the chassis.
ipmitool power cycle	Power off the chassis and power on the chassis.
ipmitool power reset	Restart the chassis.

Example:

```
root@bmc:/# ipmitool power on
Chassis Power Control: Up/On

root@bmc:/# ipmitool power off
Chassis Power Control: Down/Off

root@bmc:/# ipmitool power cycle
Chassis Power Control: Cycle

root@bmc:/# ipmitool power reset
Chassis Power Control: Reset
```

8.3.2.3 Network Configuration

8.3.2.3.1 Get the current configuration of the management port

```
ipmitool lan print [<channel number>]
```

Note: To determine on which channel the LAN interface is located, issue the 'ipmitool channel info number' command until you come across a valid 802.3 LAN channel.

Example:

```

root@bmc:/# ipmitool lan print 8
Set in Progress           : Set Complete
Auth Type Support         :
Auth Type Enable          : Callback :
                           : User      :
                           : Operator :
                           : Admin    :
                           : OEM       :
IP Address Source         : DHCP Address
IP Address                : 192.168.1.12
Subnet Mask               : 255.255.255.0
MAC Address               : 00:30:64:a8:7b:04
SNMP Community String     : AMI
IP Header                 : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control           : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Intrvl     : 1.0 seconds
Default Gateway IP        : 192.168.1.1
Default Gateway MAC       : 50:7b:9d:25:56:a1
Backup Gateway IP         : 0.0.0.0
Backup Gateway MAC        : 00:00:00:00:00:00
802.1q VLAN ID           : Disabled
802.1q VLAN Priority      : 0
RMCP+ Cipher Suites       : 3,17
Cipher Suite Priv Max     : XXXaXXXXXXXXaXXX
                           :      X=Cipher Suite Unused
                           :      c=CALLBACK
                           :      u=USER
                           :      o=OPERATOR
                           :      a=ADMIN
                           :      O=OEM
Bad Password Threshold    : 0
Invalid password disable: no
Attempt Count Reset Int.: 0
User Lockout Interval     : 0

```

8.3.2.3.2 Set the IP address source

```
ipmitool lan set <channel number> ipsrc <source>
```

source:

- ✧ static: manually configured static IP address
- ✧ dhcp: address obtained by BMC running DHCP

8.3.2.3.3 Set the IP Address

```
ipmitool lan set <channel number> ipaddr <x.x.x.x>
```

Example:

```
root@bmc:/# ipmitool lan set 8 ipaddr 192.168.1.100
Setting LAN IP Address to 192.168.1.100
```

8.3.2.3.4 Set the Netmask

```
ipmitool lan set <channel number> netmask <x.x.x.x>
```

8.3.2.3.5 Set the Default Gateway IP Address

```
ipmitool lan set <channel number> defgw ipaddr <x.x.x.x>
```

Note: Make sure the gateway IP address is pingable.

8.3.2.3.6 Set Network Configuration via BIOS

Enter **BIOS Setup > Server Mgmt > BMC network configuration**.

```

                                Aptio Setup - AMI

                                Server Mgmt

/-----+-----\
| --BMC network configuration-- ^|Select to configure LAN ^|
| *****                      *|channel parameters      *|
| Configure IPv4 support        *|statically or          *|
| *****                      *|dynamically(by BIOS or    *|
|                               +|BMC). Unspecified          *|
|                               +|option will not modify     *|
| Lan channel 1                +|any BMC network          +|
| Configuration Address [Unspecified] +|parameters during BIOS v|
| Current Configuration DynamicAddressBmcDhcp +|
| Station IP address 0.0.0.0 +|
| Subnet mask 0.0.0.0 +|-----|
| Station MAC address 00-30-64-66-77-88 +|><: Select Screen |
| Router IP address 0.0.0.0 +|^v: Select Item |
| Router MAC address 00-00-00-00-00-00 +|Enter: Select |
|                               +|+/-: Change Opt. |
| Lan channel 2                +|F1: General Help |
| Configuration Address [Unspecified] +|F8: Previous Values |
| Current Configuration DynamicAddressBmcDhcp +|F9: Optimized Defaults |
| Station IP address 192.168.1.12 v|F10: Save & Exit |
|                               |ESC: Exit |
\-----+-----/

Version 2.22.1289 Copyright (C) 2024 AMI

```

Aptio Setup - AMI

Server Mgmt

```

/-----+-----\
|  --BMC network configuration--          ^|Select to configure LAN ^|
|  *****                               *|channel parameters      *|
|  Configure IPv4 support                 *|statically or           *|
|  *****                               *|dynamically(by BIOS or  *|
|                                          +|BMC). Unspecified      *|
|  Lan channel 1                         +|option will not modify *|
|  Configuration Address      [Static]    +|any BMC network        +|
|  Station IP address         188.188.1.2 +|parameters during BIOS v|
|  Subnet mask                255.255.255.0 +|                        |
|  Station MAC address        00-30-64-66-77-88 +|-----|
|  Router IP address          188.188.1.1  +|><: Select Screen      |
|  Router MAC address         00-00-00-00-00-00 +|^v: Select Item        |
|                                          +|Enter: Select          |
|  Lan channel 2                     +|+/-: Change Opt.      |
|  Configuration Address      [Unspecified] +|F1: General Help       |
|  Current Configuration       DynamicAddressBmcDhcp +|F8: Previous Values    |
|  Station IP address          192.168.1.12 +|F9: Optimized Defaults |
|  Subnet mask                 255.255.255.0 v|F10: Save & Exit        |
|                                          |ESC: Exit              |
\-----+-----/

```

Version 2.22.1289 Copyright (C) 2024 AMI

BIOS Item	Options	Description
Configuration Address source	Static DynamicBmcDhcp	Set the IP address source
Station IP address	x.x.x.x	Set the IP address
Subnet mask	x.x.x.x	Set the netmask
Router IP address	x.x.x.x	Set the default gateway IP address
Router MAC address	xx:xx:xx:xx:xx:xx	Set the default gateway MAC address

8.3.2.4 SOL

The serial over LAN (SOL) feature is very useful, and the SOL redirects the local serial interface via an IPMI session, allowing remote access to the console.

Open SOL functionality using ipmitool command:

Command:

```
ipmitool sol activate
```

Example:

```

Aptio Setup - AMI
Main Advanced Platform Configuration Socket Configuration Server Mgmt >
/-----\
| BIOS Information |Set the Date| |
| BIOS Vendor      |American Megatrends|switch betwe|
| BIOS Version     |1.2.10            |Default Rang|
| Build Date       |01/24/2024        |Year: 1998-9|
| RC Version       |370.P03           |Months: 1-12|
| SPS FW Version   |6.1.2.48          |Days: Depend|
|                  |                   |Range of Yea|
|
| System Information
| Project Name      |MECS-7120         | |
| CPU Board Version |/---- Save & Exit ----\|
| CPU Brand String  |                   |
|                  |Quit without saving?|
| CPU Frequency     |                   |-----|
| Total Memory      |-----|><: Select S|
| Memory Frequency  |YesNo| ^v: Select I|
| PCH SKU           |\-----/|Enter: Selec|
|                  |+/-: Change |
| System Date       |[Fri 01/26/2024]|F1: General|
| System Time       |[03:01:19]|F8: Previous|
|                  |F9: Optimize|
| Access Level      |Administrator|F10: Save &|
|                  |ESC: Exit|
|
|
|
|
|
|-----\
Version 2.22.1292 Copyright (C) 2024 AMI

```

Enter the "ipmitool sol activate" command on CLI to enter the SOL output window, then enter the BIOS configuration interface, and the content of the BIOS field interface will be redirected to the local terminal, as shown in the above figure.

Other ipmitool Commands Related to SOL

Below is a table summarizing additional ipmitool commands related to SOL:

Command Element	Description
ipmitool sol deactivate	Close SOL functionality
ipmitool sol info	Show SOL detailed information
ipmitool sol set <set-in-progress enabled force-encryption force-authentication privilege-level character-accumulate-level character-send-threshold retry-count retry-interval non-volatile-bit-rate volatile-bit-rate> <value>	Set SOL parameter value

Command Element	Description
ipmitool sol payload <enable disable status>	Set SOL payload value
ipmitool sol looptest	SOL connection stress test

8.3.2.5 BMC Information

To get the BMC information via ipmitool please refer to the following command:

```
ipmitool mc info
```

For example:

```
root@bmc:/# ipmitool mc info
Device ID                : 32
Device Revision          : 1
Firmware Revision        : 1.03
IPMI Version             : 2.0
Manufacturer ID          : 24339
Manufacturer Name        : ADLINK Technology Inc.
Product ID               : 28960 (0x7120)
Product Name             : Unknown (0x7120)
Device Available         : yes
Provides Device SDRs     : yes
Additional Device Support :
Sensor Device
SDR Repository Device
SEL Device
FRU Inventory Device
IPMB Event Receiver
IPMB Event Generator
Chassis Device
Aux Firmware Rev Info    :
0x64
0x00
0x00
0x00
```

The full BMC version number is composed of the “**Firmware Revision**” and the “**Aux Firmware Rev Info**”. The Firmware Revision contains the major and minor version numbers. The Aux Firmware Rev Info contains the auxiliary version number, which is in little-endian format.

The full version number in the example above is as follows:

Major: 1

Minor: 3

Aux: 0x00000064 (hex) -> 100 (decimal)

8.3.2.6 CPLD Update

```
ipmitool -z 0x3fff hpm upgrade <hpm file> component 5 force
```

Note: If a CPLD firmware has been uploaded, it will print "Firmware upgrade procedure failed".

Example:

```
root@bmc:/# ipmitool -I lanplus -H 172.20.2.18 -U admin -P admin.123 -z 0x3fff hpm upgrade
outputjbc_02b4.hpm component 5 force
```

```
Setting large buffer to 16383
```

```
PICMG HPM.1 Upgrade Agent 1.0.9:
```

```
Validating firmware image integrity...OK
```

```
Performing preparation stage...
```

```
Services may be affected during upgrade. Do you wish to continue? (y/n): y
```

```
OK
```

```
Performing upgrade stage:
```

```
-----
|ID  | Name          |              Versions              | %  |
|    |              |      Active      |      Backup      |      File      |    |
|----|-----|-----|-----|-----|-----|
|* 5|CPLD          | 0.00 00000000 | ---.-- - - - - - | 2.04 00002002 |100%|
|    |Upload Time: 00:00          | Image Size: 454924 bytes          |    |
-----
```

```
(*) Component requires Payload Cold Reset
```

```
Firmware upgrade procedure successful
```

8.4 Redfish

Redfish is a modern, RESTful API used for the management of servers, storage, and networking equipment in data centers and large-scale enterprise environments. It's designed to replace older, less efficient management interfaces with a standardized, scalable, and secure approach.

8.4.1 Network Configuration

8.4.1.1 GET - Ethernet Interface Collection

Request:

```
GET https://{bmc ip}/redfish/v1/Managers/Self/EthernetInterfaces
```

Response:

The response status is 200 OK.

Example:

```
GET https://172.20.2.12/redfish/v1/Managers/Self/EthernetInterfaces
```

```
{
  "@odata.context": "/redfish/v1/$metadata#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "@odata.etag": "\"1705564980\"",
  "@odata.id": "/redfish/v1/Managers/Self/EthernetInterfaces",
  "@odata.type": "#EthernetInterfaceCollection.EthernetInterfaceCollection",
  "Description": "Collection of Ethernet Interfaces for this Manager",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Managers/Self/EthernetInterfaces/eth0"
    },
    {
      "@odata.id": "/redfish/v1/Managers/Self/EthernetInterfaces/eth1"
    },
    {
      "@odata.id": "/redfish/v1/Managers/Self/EthernetInterfaces/usb0"
    }
  ],
  "Members@odata.count": 3,
  "Name": "Ethernet Network Interface Collection"
}
```

8.4.1.2 GET - Ethernet Interface Instance

Request:

```
GET https://{bmc ip}/redfish/v1/Manaqers/Self/EthernetInterfaces/{instance}
```

Response:

The response status is **200 OK**. The format is JSON.

Ethernet Interface Properties:

Name	Type	Read Only	Description
AutoNeg	Boolean	×	Auto negotiation of speed and duplex on this interface is enabled or not.
DHCPv4	Object	×	Refer to DHCPv4 properties.
DHCPv6	Object	×	Refer to DHCPv6 properties.
Description	String	√	
FullDuplex	Boolean	×	The value of this property shall represent the duplex status of the Ethernet connection on this interface.
HostName	String	×	DNS Hostname without any domain information. Maximum string size limit is 64. Minimum string size limit is 2.
IPv4Addresses	Array of Objects	√	Refer to IPv4 Address properties.
IPv4StaticAddresses	Array of Objects	×	Refer to IPv4 Address properties.
IPv6Addresses	Array of Objects	√	Refer to IPv6 Address properties.
IPv6StaticAddresses	Array of Objects	×	Refer to IPv6 Address properties.
IPv6DefaultGateway	String	√	
Id	String	√	
InterfaceEnabled	Boolean	×	
LinkStatus	String	√	
MACAddress	String	√	
MTUSize	Number	×	Maximum size limit is 1500. Minimum size limit is 576.
MaxIPv6StaticAddresses	Number	√	
Name	String	√	
NameServers	Array of Strings	√	
Oem	Object	√	
PermanentMACAddress	String	√	
SpeedMbps	Number	×	The current link speed of the interface in Mbps.

Name	Type	Read Only	Description
StatelessAddressAutoConfig	Object	×	This object shall contain the IPv4 and IPv6 Stateless Address Automatic Configuration (SLAAC) properties for this interface.
StaticNameServers	Array of Strings	×	Statically-defined set of DNS server IPv4 and IPv6 addresses.
Status	Object	√	
VLAN	Object	×	VLANId: 0~4094.

DHCPv4 properties:

Name	Type	Read Only	Description
DHCPEnabled	Boolean	×	Determines whether DHCPv4 is enabled on this interface.

DHCPv6 properties:

Name	Type	Read Only	Description
OperatingMode	Boolean	×	This property shall control the operating mode of DHCPv6 on this interface. DHCPv6 stateful mode is used to configure addresses, and when it is enabled, stateless mode is also implicitly enabled.

IPv4 Address properties:

Name	Type	Read Only	Description
Address	String	-	IPv4 address.
AddressOrigin	String	-	IPv4 address source.
Gateway	String	-	IPv4 default gateway IP address.
SubnetMask	String	-	IPv4 netmask.

IPv6 Address properties:

Name	Type	Read Only	Description
Address	String	-	IPv6 address.
AddressOrigin	String	-	IPv6 address source.
PrefixLength	String	-	IPv6 network prefix length in bits. Max is 128.

Example:

GET

<https://172.20.2.12/redfish/v1/Managers/Self/EthernetInterfaces/eth1>

```
{
  "@odata.context": "/redfish/v1/$metadata#EthernetInterface.EthernetInterface",
  "@odata.etag": "\"1705564980\"",
  "@odata.id": "/redfish/v1/Managers/Self/EthernetInterfaces/eth1",
  "@odata.type": "#EthernetInterface.v1_6_2.EthernetInterface",
  "AutoNeg": true,
  "DHCPv4": {
    "DHCPEnabled": true
  },
  "DHCPv6": {
    "OperatingMode": "Stateless"
  },
  "Description": "Ethernet Interface eth1",
  "FullDuplex": true,
  "HostName": "AMI003064667788",
  "IPv4Addresses": [
    {
      "Address": "172.20.2.12",
      "AddressOrigin": "DHCP",
      "Gateway": "172.20.2.1",
      "SubnetMask": "255.255.255.0"
    }
  ],
  "IPv6Addresses": [
    {
      "Address": "fe80::230:64ff:feaf:b104",
      "AddressOrigin": "LinkLocal",
      "PrefixLength": 64
    }
  ],
  "IPv6DefaultGateway": null,
  "Id": "eth1",
  "InterfaceEnabled": true,
```

```

"LinkStatus": "LinkUp",

"MACAddress": "00:30:64:A1:B1:04",

"MTUSize": 1500,

"MaxIPv6StaticAddresses": 16,

"Name": "eth1",

"NameServers": [

    "192.168.1.213",

    "192.168.1.214"

],

"Oem": {

    "Ami": {

        "@odata.type": "#AMIDNSConfiguration.v1_0_0.AMIDNSConfiguration",

        "DNSEnabled": true,

        "HostNameSetting": "Auto"

    }

},

"PermanentMACAddress": "00:30:64:A1:B1:04",

"SpeedMbps": 100,

"StatelessAddressAutoConfig": {

    "IPv4AutoConfigEnabled": false,

    "IPv6AutoConfigEnabled": false

},

"StaticNameServers": [

    null,

    null,

    null

],

"Status": {

    "Health": "OK",

    "State": "Enabled"

},

"VLAN": {

    "VLANEnable": false,

    "VLANId": 0

}

}

```

8.4.1.3 PATCH - Ethernet Interface Instance

Request:

PATCH `https://{bmc ip}/redfish/v1/Managers/Self/EthernetInterfaces/{instance}`

Please refer to the **Ethernet Interface Properties** that are patchable for which Read Only is False that can be sent as Request body in JSON format.

Response:

The response status is **202 Accepted**, with newly created Task details.

Example: Disable IPv4 DHCP and set static IPv4 address.

Add a key **"If-Match"** in request **Headers** tab. The value is your **ETag** value.

PATCH

https://172.20.2.12/redfish/v1/Managers/Self/EthernetInterfaces/eth1

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

Headers

9 hidden

	Key	Value
☒	If-Match	"1705564980"
	Key	Value

Add **raw** body data in request **Body** tab. The data format is **JSON**.

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

JSON

```

{
  "DHCPv4": {
    "DHCPEnabled": false
  },
  "IPv4StaticAddresses": [
    {
      "Address": "172.20.2.234",
      "Gateway": "172.20.2.1",
      "SubnetMask": "255.255.255.0"
    }
  ]
}

```

Response body content.

```
{
  "@odata.context": "/redfish/v1/$metadata#Task.Task",
  "@odata.id": "/redfish/v1/TaskService/Tasks/1",
  "@odata.type": "#Task.v1_4_2.Task",
  "Description": "Task for EthernetInterface Action",
  "Id": "1",
  "Name": "EthernetInterface Action",
  "TaskMonitor": "/redfish/v1/TaskService/TaskMonitors/1",
  "TaskState": "New"
}
```

8.4.2 BIOS Configuration

8.4.2.1 GET - HostInterface Instance

Request:

```
GET https://{bmc ip}/redfish/v1/Managers/Self/HostInterfaces/Self
```

Response:

The response status is 200 OK.

Example:

```
GET https://172.20.2.12/redfish/v1/Managers/Self/HostInterfaces/Self
```

```
{
  "@odata.context": "/redfish/v1/$metadata#HostInterface.HostInterface",
  "@odata.etag": "\"1705997262\"",
  "@odata.id": "/redfish/v1/Managers/Self/HostInterfaces/Self",
  "@odata.type": "#HostInterface.v1_3_0.HostInterface",
  "AuthenticationModes": [
    "BasicAuth",
    "RedfishSessionAuth"
  ],
  "CredentialBootstrapping": {
    "EnableAfterReset": false,
    "Enabled": true,
    "RoleId": "HostInterfaceAdministrator"
  },
  "Description": "Host Interface",
}
```

```
"ExternallyAccessible": false,

"HostEthernetInterfaces": {

    "@odata.id": "/redfish/v1/Managers/Self/HostInterfaces/Self/HostEthernetInterfaces"

},

"HostInterfaceType": "NetworkHostInterface",

"Id": "Self",

"InterfaceEnabled": true,

"Links": {

    "ComputerSystems": [

        {

            "@odata.id": "/redfish/v1/Systems/Self"

        }

    ],

    "ComputerSystems@odata.count": 1,

    "CredentialBootstrappingRole": {

        "@odata.id": "/redfish/v1/AccountService/Roles/HostInterfaceAdministrator"

    }

},

"ManagerEthernetInterface": {

    "@odata.id": "/redfish/v1/Managers/Self/EthernetInterfaces/usb0"

},

"Name": "Host Interface",

"NetworkProtocol": {

    "@odata.id": "/redfish/v1/Managers/Self/NetworkProtocol"

},

"Status": {

    "Health": "OK",

    "State": "Enabled"

}

}
```

8.4.2.2 GET – BIOS and BIOS/SD

Request:

Get current BIOS Settings:

```
GET https://{bmc ip}/redfish/v1/Systems/Self/Bios
```

Get future BIOS Settings:

```
GET https://{bmc ip}/redfish/v1/Systems/Self/Bios/SD
```

Response:

The response status is 200 OK.

Example:

```
GET https://172.20.2.12/redfish/v1/Systems/Self/Bios
```

```
{
  "@Redfish.Settings": {
    "@odata.type": "#Settings.v1_2_2.Settings",
    "SettingsObject": {
      "@odata.id": "/redfish/v1/Systems/Self/Bios/SD"
    }
  },
  "@odata.context": "/redfish/v1/$metadata#Bios.Bios",
  "@odata.etag": "\"1705640880\"",
  "@odata.id": "/redfish/v1/Systems/Self/Bios",
  "@odata.type": "#Bios.v1_2_0.Bios",
  "Actions": {
    "#Bios.ChangePassword": {
      "@Redfish.ActionInfo": "/redfish/v1/Systems/Self/Bios/ChangePasswordActionInfo",
      "target": "/redfish/v1/Systems/Self/Bios/Actions/Bios.ChangePassword"
    },
    "#Bios.ResetBios": {
      "target": "/redfish/v1/Systems/Self/Bios/Actions/Bios.ResetBios"
    }
  },
  "AttributeRegistry": "BiosAttributeRegistry22808.1.1.0",
  "Attributes": {
    "ACPI004": false,
    "CRCS005": "CRCS005Enable",
    "FBO001": "FBO001UEFI",
```

```

    "FBO101": "FBO101HardDisk",

    "FBO102": "FBO102NVME",

    ...

},

"Description": "Current BIOS Settings",

"Id": "Bios",

"Name": "Current BIOS Settings",

"ResetBiosToDefaultsPending": false

}

```

8.4.2.3 POST – Reset BIOS Settings

Request:

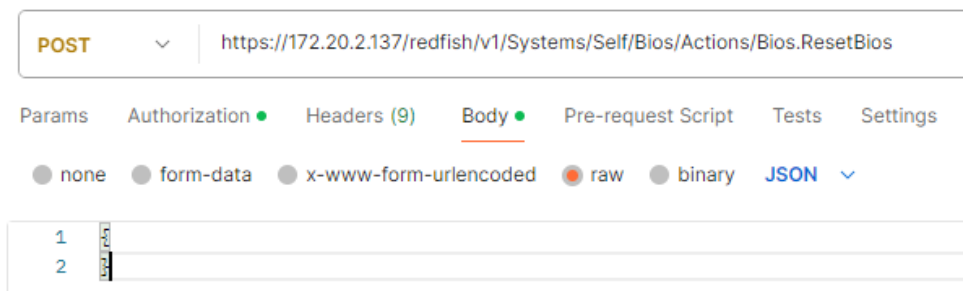
POST <https://{{bmc ip}}/redfish/v1/Systems/Self/Bios/Actions/Bios.ResetBios>

Response:

The response status is **204 No Content**.

Example:

Add **raw** body data in request **Body** tab. The data format is **JSON**.



POST <https://172.20.2.137/redfish/v1/Systems/Self/Bios/Actions/Bios.ResetBios>

Params Authorization Headers (9) **Body** Pre-request Script Tests Settings

☐ none ☐ form-data ☐ x-www-form-urlencoded ☒ raw ☐ binary **JSON** ▾

```

1 {
2   "FBO101": "FBO101HardDisk",

```

8.4.2.4 POST – Change BIOS Password

Request:

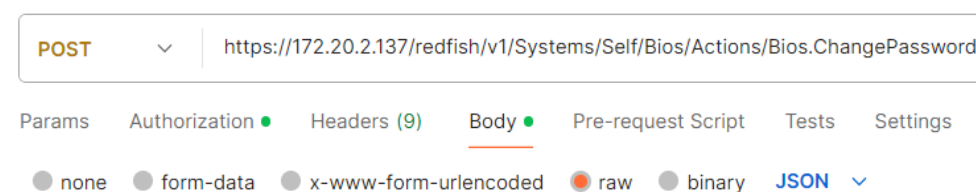
POST <https://{{bmc ip}}/redfish/v1/Systems/Self/Bios/Actions/Bios.ChangePassword>

Response:

The response status is **204 No Content**.

Example:

Add **raw** body data in request **Body** tab. The data format is **JSON**.



POST <https://172.20.2.137/redfish/v1/Systems/Self/Bios/Actions/Bios.ChangePassword>

Params Authorization Headers (9) **Body** Pre-request Script Tests Settings

☐ none ☐ form-data ☐ x-www-form-urlencoded ☒ raw ☐ binary **JSON** ▾

```
{
  "PasswordName": "SETUP001",
  "OldPassword": "old",
  "NewPassword": "new"
}
```

8.4.2.5 PATCH – BIOS SD

Change the values of the attributes.

Request:

```
PATCH https://{bmc ip}/redfish/v1/Systems/Self/Bios/SD
```

Response:

The response status is **204 No Content**.

Refer to **PATCH - BIOS Watchdog Configuration**.

8.4.3 Sensor Information

This section is dedicated to explaining how to obtain sensor information through Redfish.

Users can obtain the specific data of the required sensor through the following command.

Request:

```
GET https://{bmc ip}/redfish/v1/Chassis/Self/Sensors/{Sensor ID}
```

Response:

The response status is **200 OK**.

Example:

```
GET https://172.20.2.36/redfish/v1/Chassis/Self/Sensors/1
```

```
{
  "@odata.context": "/redfish/v1/$metadata#Sensor.Sensor",
  "@odata.etag": "\"1708661966\"",
  "@odata.id": "/redfish/v1/Chassis/Self/Sensors/1",
  "@odata.type": "#Sensor.v1_0_2.Sensor",
  "Accuracy": null,
  "AdjustedMaxAllowableOperatingValue": null,
  "AdjustedMinAllowableOperatingValue": null,
  "ApparentVA": null,
  "Description": null,
  "ElectricalContext": null,
  "Id": "1",
```

```
"LoadPercent": null,

"Location": {

  "AltitudeMeters": null,

  "Contacts": [

    null

  ],

  "Latitude": null,

  "Longitude": null,

  "PartLocation": {

    "LocationOrdinalValue": null,

    "LocationType": null,

    "Orientation": null,

    "Reference": null,

    "ServiceLabel": null

  },

  "Placement": {

    "AdditionalInfo": null,

    "Rack": null,

    "RackOffset": null,

    "RackOffsetUnits": null,

    "Row": null

  },

  "PostalAddress": {

    "AdditionalCode": null,

    "AdditionalInfo": null,

    "Building": null,

    "City": null,

    "Community": null,

    "Country": null,

    "District": null,

    "Division": null,

    "Floor": null,

    "HouseNumber": null,

    "HouseNumberSuffix": null,

    "Landmark": null,

    "LeadingStreetDirection": null,
```

```

        "Name": null,
        "Neighborhood": null,
        "POBox": null,
        "PlaceType": null,
        "PostalCode": null,
        "Road": null,
        "RoadBranch": null,
        "RoadPostModifier": null,
        "RoadPreModifier": null,
        "RoadSection": null,
        "RoadSubBranch": null,
        "Room": null,
        "Seat": null,
        "Street": null,
        "StreetSuffix": null,
        "Territory": null,
        "TrailingStreetSuffix": null,
        "Unit": null
    }
},
"MaxAllowableOperatingValue": null,
"MinAllowableOperatingValue": null,
"Name": "P12V_PSU",
"PeakReading": null,
"PeakReadingTime": null,
"PhysicalContext": "VoltageRegulator",
"PhysicalSubContext": null,
"PowerFactor": null,
"Precision": null,
"ReactiveVAR": null,
"Reading": 12.22,
"ReadingRangeMax": 13.25,
"ReadingRangeMin": 10.7,
"ReadingType": "Voltage",
"ReadingUnits": null,
"SensingFrequency": null,

```

```
"SensorResetTime": null,

"Status": {

    "Health": "OK",

    "HealthRollup": null,

    "State": "Enabled"

},

"Thresholds": {

    "LowerCaution": {

        "Activation": null,

        "DwellTime": null,

        "Reading": 11.4

    },

    "LowerCritical": {

        "Activation": null,

        "DwellTime": null,

        "Reading": 11.16

    },

    "LowerFatal": {

        "Activation": null,

        "DwellTime": null,

        "Reading": 10.8

    },

    "UpperCaution": {

        "Activation": null,

        "DwellTime": null,

        "Reading": 12.6

    },

    "UpperCritical": {

        "Activation": null,

        "DwellTime": null,

        "Reading": 12.84

    },

    "UpperFatal": {

        "Activation": null,

        "DwellTime": null,

        "Reading": 13.2

    },

}
```

```

    }

    },

    "VoltageType": null

}

```

Other commands to access sensor information using Redfish:

General Thermal Sensors Information

```
GET https://{bmc ip}/redfish/v1/Chassis/Self/Thermal
```

Retrieves detailed information about the server's thermal sensors, including current temperature readings.

Temperature Sensor IDs

```
GET https://{bmc ip}/redfish/v1/Chassis/Self/ThermalSubsystem/ThermalMetrics
```

Retrieves IDs and specific metrics of temperature-related sensors.

General Power Sensors Information

```
GET https://{bmc ip}/redfish/v1/Chassis/Self/Power
```

Retrieves comprehensive data about power-related sensors, including power supply status and output power.

Power Sensor IDs

```
GET https://{bmc ip}/redfish/v1/Chassis/Self/PowerSubsystem
```

Retrieves IDs and detailed metrics related to power sensors.

8.4.4 BMC Update

This section specifically explains how to obtain and upgrade BMC through Redfish.

Users can upgrade BMC and set Preserve Configuration through the following commands.

8.4.4.1 GET - Preserve Configuration

This section describes how to use redfish to **Get** Preserve Configuration before upgrading BMC.

Request:

```
GET https://{bmc ip}/redfish/v1/UpdateService
```

Response:

The response status is **200 OK**.

Example:

```
GET https://172.20.2.36/redfish/v1/UpdateService
```

```

{
  "@odata.context": "/redfish/v1/$metadata#UpdateService.UpdateService",
  "@odata.etag": "\"1708925760\"",
  "@odata.id": "/redfish/v1/UpdateService",

```

```
"@odata.type": "#UpdateService.v1_6_0.UpdateService",

"Actions": {

  "#UpdateService.SimpleUpdate": {

    "@Redfish.ActionInfo": "/redfish/v1/UpdateService/SimpleUpdateActionInfo",

    "target": "/redfish/v1/UpdateService/Actions/SimpleUpdate"

  },

  "Oem": {

    "#UpdateService.UploadCABundle": {

      "@Redfish.ActionInfo": "/redfish/v1/UpdateService/UploadCABundleActionInfo",

      "target": "/redfish/v1/UpdateService/Actions/Oem/UpdateService.UploadCABundle"

    }

  }

},

"Description": "Redfish Update Service",

"FirmwareInventory": {

  "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory"

},

"Id": "UpdateService",

"MaxImageSizeBytes": 496611328,

"MultipartHttpPushUri": "/redfish/v1/UpdateService/upload",

"Name": "Update Service",

"Oem": {

  "AMIUpdateService": {

    "@odata.type": "#AMIUpdateService.v1_0_0.AMIUpdateService",

    "FlashPercentage": null,

    "PreserveConfiguration": {

      "Authentication": false,

      "EXTLOG": false,

      "FRU": false,

      "IPMI": false,

      "KVM": false,

      "NTP": false,

      "Network": false,

      "REDFISH": false,

      "SDR": false,

      "SEL": false,
```

```

        "SNMP": false,

        "SSH": false,

        "Syslog": false,

        "WEB": false

    },

    "UpdateStatus": null,

    "UpdateTarget": null

},

"BMC": {

    "@odata.type": "#AMIUpdateService.v1_0_0.BMC",

    "DualImageConfigurations": {

        "ActiveImage": "2",

        "BootImage": "2",

        "FirmwareImage1Name": "Image1",

        "FirmwareImage1Version": "13.05.010004",

        "FirmwareImage2Name": "Image2",

        "FirmwareImage2Version": "13.05.010003"

    }

}

},

"ServiceEnabled": true,

"Status": {

    "Health": "OK",

    "State": "Enabled"

}

}

```

8.4.4.2 PATCH - Preserve Configuration

This section describes how to use redfish to **Set** Preserve Configuration before upgrading BMC.

Request:

```
PATCH https://{bmc_ip}/redfish/v1/UpdateService
```

Please refer to the **GET - Preserve Configuration**.

Response:

The response status is **204 No Content**.

Example: Enable saving IPMI and SEL when upgrading BMC.

Add a key **"If-Match"** in request **Headers** tab. The value is your **ETag** value. This value can be obtained from **GET - Preserve Configuration**.

PATCH ▼ | https://172.20.2.36/redfish/v1/UpdateService

Params Authorization ● Headers (8) Body Pre-request Script Tests ● Settings

Headers 7 hidden

	Key	Value
☒	If-Match	"1706750916"
	Key	Value

Add **raw** body data in request **Body** tab. The data format is **JSON**.

Params Authorization ● Headers (10) Body ● Pre-request Script Tests Settings

☐ none
 ☐ form-data
 ☐ x-www-form-urlencoded
 ☒ raw
 ☐ binary
 JSON ▼

```
{
  "Oem": {
    "AMIUpdateService": {
      "PreserveConfiguration": {
        "IPMI": true,
        "SEL": true
      }
    }
  }
}
```

8.4.4.3 POST – Firmware Update

This section describes how to use redfish to **Update BMC firmware**.

Request:

POST https://{bmc ip}/redfish/v1/UpdateService/upload

Response:

The response status is **202 Accepted**.

Example:

Using POSTMAN, please follow the steps as given below.

1. Ensure that all necessary files mentioned in the subsequent steps are placed in your working directory. Go to the top right corner of POSTMAN and click on the **settings button**. In the general settings, make the necessary adjustments.

Working directory

Collaborate on files used in requests by sharing your working directory. Learn how to [setup your working directory](#) ↗

Location

Read files outside working directory

⚠ Enabling this will allow any 3rd party collections to potentially read any file on your system.



2. Create a JSON file **parameters.json** with content like below.

```
{
  "Targets" : [
    "/redfish/v1/UpdateService/FirmwareInventory/BMCImage1"
  ]
}
```

3. Create a JSON file **oem_parameters.json** with content like below.

```
{
  "ImageType" : "BMC"
}
```

4. Open POSTMAN and enter the **URI** to POST the request.
5. Select **POST** method.
6. In the **Authorization** tab, select Basic Auth and update request.
7. In the **Body** tab, select form-data and provide the key name as **UpdateFile** in the KEY section and change its type from **Text** to File.
8. Click on **Select File** in the **VALUE** section to select the signed image which is available in your local machine to update.
9. Like step 7 and 8, provide key name **UpdateParameters** and select **parameters.json** created in step 2.
10. Like step 7 and 8, provide key name **OemParameters** and select **oem_parameters.json** created in step 3.
11. Click **Send**.

POST

Params Authorization Headers (9) **Body** Pre-request Script Tests Settings [Cookies](#)

● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL

Key	Value	Description
☒ UpdateParameters	File parameters.json	
☒ OemParameters	File oem_parameters.json	
☒ UpdateFile	File rom.ima	
Key	Text Value	Description

Response:

```

Body  Cookies  Headers (14)  Test Results  Status: 202 Accepted
Pretty  Raw  Preview  Visualize  JSON  [icon]
1  {
2    "@odata.type": "#UpdateService.v1_6_0.UpdateService",
3    "Messages": [
4      {
5        "@odata.type": "#Message.v1_0_8.Message",
6        "Message": "A new task /redfish/v1/TaskService/Tasks/4 was created.",
7        "MessageArgs": [
8          "/redfish/v1/TaskService/Tasks/4"
9        ],
10       "MessageId": "Task.1.0.New",
11       "Resolution": "None",
12       "Severity": "OK"
13     },
14     {
15       "@odata.type": "#Message.v1_0_8.Message",
16       "Message": "The action UpdateService.MultipartPush was submitted to do firmware update.",
17       "MessageArgs": [
18         "UpdateService.MultipartPush"
19       ]
20     }
21   ]
22 }

```

Note:

The details of UpdateParameters are given in the table below.

Allowed value	Description
redfish/v1/UpdateService/FirmwareInventory/BMC	When the system does not support Dual Flash
redfish/v1/UpdateService/FirmwareInventory/BMCImage1	For systems with Dual Flash support, to upgrade Image 1
redfish/v1/UpdateService/FirmwareInventory/BMCImage2	For systems with Dual Flash support, to upgrade Image 2

8.4.5 BIOS Update

This section specifically explains how to obtain and upgrade BIOS through Redfish.

Users can upgrade BIOS through the following commands.

8.4.5.1 GET - BIOS Update Status

Request:

```
GET https://{bmc ip}/redfish/v1/UpdateService
```

Response:

The response status is 200 OK.

Name	Type	Read Only	Description
BIOSFlashEffectStatus	String	√	Indicates the BIOS update effect status: Waiting: there is a BIOS update task waiting to take effect. Updating: someone is updating BIOS. null: no BIOS update task.

Example:

GET

▼

https://172.20.2.18/redfish/v1/UpdateService

```
{
  "@odata.context": "/redfish/v1/$metadata#UpdateService.UpdateService",
  "@odata.etag": "\"1708587273\"",
  "@odata.id": "/redfish/v1/UpdateService",
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Actions": {
    "#UpdateService.SimpleUpdate": {
      "@Redfish.ActionInfo": "/redfish/v1/UpdateService/SimpleUpdateActionInfo",
      "target": "/redfish/v1/UpdateService/Actions/SimpleUpdate"
    },
    "Oem": {
      "#UpdateService.UploadCABundle": {
        "@Redfish.ActionInfo": "/redfish/v1/UpdateService/UploadCABundleActionInfo",
        "target": "/redfish/v1/UpdateService/Actions/Oem/UpdateService.UploadCABundle"
      }
    }
  },
  "Description": "Redfish Update Service",
  "FirmwareInventory": {
    "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory"
  },
  "Id": "UpdateService",
  "MaxImageSizeBytes": 496717824,
  "MultipartHttpPushUri": "/redfish/v1/UpdateService/upload",
  "Name": "Update Service",
  "Oem": {
    "AMIUpdateService": {
      "@odata.type": "#AMIUpdateService.v1_0_0.AMIUpdateService",
      "BIOSFlashEffectStatus": null,
      "FlashPercentage": null,
      "PreserveConfiguration": {
        "Authentication": false,
        "EXTLOG": false,

```

```
    "FRU": false,

    "IPMI": false,

    "KVM": false,

    "NTP": false,

    "Network": false,

    "REDFISH": false,

    "SDR": false,

    "SEL": false,

    "SNMP": false,

    "SSH": false,

    "Syslog": false,

    "WEB": false

  },

  "UpdateStatus": null,

  "UpdateTarget": null

},

"BMC": {

  "@odata.type": "#AMIUpdateService.v1_0_0.BMC",

  "DualImageConfigurations": {

    "ActiveImage": "1",

    "BootImage": "1",

    "FirmwareImage1Name": "Image1",

    "FirmwareImage1Version": "13.05.010004",

    "FirmwareImage2Name": "Image2",

    "FirmwareImage2Version": "13.05.010003"

  }

}

},

"ServiceEnabled": true,

"Status": {

  "Health": "OK",

  "State": "Enabled"

}

}
```

8.4.5.2 POST – Firmware Update

This section describes how to use redfish to **Update BIOS firmware**.

Request:

```
POST https://{bmc ip}/redfish/v1/UpdateService/upload
```

Response:

The response status is **202 Accepted**.

Example:

Using POSTMAN, please follow the steps as given below.

1. Ensure that all necessary files mentioned in the subsequent steps are placed in your working directory. Go to the top right corner of POSTMAN and click on the **settings button**. In the general settings, make the necessary adjustments.

Working directory

Collaborate on files used in requests by sharing your working directory. Learn how to [setup your working directory](#) ↗

Location

D:\Redfish

Choose

Read files outside working directory

⚠ Enabling this will allow any 3rd party collections to potentially read any file on your system.



2. Create a JSON file **parameters.json** with content like below.

```
{
  "Targets" : [
    "/redfish/v1/UpdateService/FirmwareInventory/BIOS"
  ]
}
```

3. Create a JSON file **oem_parameters.json** with content like below.

```
{
  "ImageType" : "BIOS",
  "update_me" : false,
  "update_nvram" : false,
  "effect_poweroff" : false,
  "force_update" : false
}
```

Name	Type	Description
update_me	Boolean	Optional. Default value is false. true: update ME. false: skip ME.
update_nvram	Boolean	Optional. Default value is false. true: update NVRAM. false: skip NVRAM.
effect_poweroff	Boolean	Optional. Default value is false. true: take effect when powered off. false: take effect immediately.
force_update	Boolean	Optional. Default value is false. true: force to update. false: do not update when other user is in in update mode or a BIOS firmware has been uploaded.

- Open POSTMAN and enter the **URI** to POST the request.
- Select **POST** method.
- In the **Authorization** tab, select Basic Auth and update request.
- In the **Body** tab, select form-data and provide the key name as **UpdateFile** in the KEY section and change its type from **Text** to File.
- Click on **Select File** in the **VALUE** section to select the signed image which is available in your local machine to update.
- Like step 7 and 8, provide key name **UpdateParameters** and select **parameters.json** created in step 2.
- Like step 7 and 8, provide key name **OemParameters** and select **oem_parameters.json** created in step 3.
- Click **Send**.

POST
https://172.20.2.18/redfish/v1/UpdateService/upload
Send

Params
Authorization
Headers (10)
Body
Pre-request Script
Tests
Settings
Cookies

none
form-data
x-www-form-urlencoded
raw
binary

Key	Value	...	Bulk Edit
☒ UpdateFile	MECS-7120_1210.BIN ×		⚠
☒ UpdateParameters	parameters.json ×		⚠
☒ OemParameters	oem_parameters.json ×		⚠
Key	Value		

Response:

```
{
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",
      "MessageArgs": [
        "/redfish/v1/TaskService/Tasks/1"
      ],
      "MessageId": "Task.1.0.New",
      "Resolution": "None",
      "Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "The action UpdateService.MultipartPush was submitted to do firmware update.",
      "MessageArgs": [
        "UpdateService.MultipartPush"
      ],
      "MessageId": "UpdateService.1.0.StartFirmwareUpdate",
      "Resolution": "None",
      "Severity": "OK"
    }
  ]
}
```

8.4.6 CPLD Update

This section specifically explains how to obtain and upgrade BIOS through Redfish. Users can upgrade BIOS through the following commands.

8.4.6.1 GET - CPLD Update Status

Request:

```
GET https://{bmc ip}/redfish/v1/UpdateService
```

Response:

The response status is **200 OK**.

Name	Type	Read Only	Description
CPLDFlashEffectStatus	String	√	Indicates the CPLD update effect status: Waiting: there is a CPLD update waiting to take effect. Updating: someone is updating Firmware. null: no CPLD update.

Example:

GET
▼
https://172.20.2.18/redfish/v1/UpdateService

```
{
  ...
  "Oem": {
    "AMIUpdateService": {
      "@odata.type": "#AMIUpdateService.v1_0_0.AMIUpdateService",
      "BIOSFlashEffectStatus": null,
      "CPLDFlashEffectStatus": null,
      "FlashPercentage": null,
    }
  }
}
```

8.4.6.2 POST – Firmware Update

This section describes how to use redfish to **Update CPLD firmware**.

Request:

POST https://{bmc ip}/redfish/v1/UpdateService/upload

Response:

The response status is **202 Accepted**.

Example:

Using POSTMAN, please follow the steps as given below.

1. Ensure that all necessary files mentioned in the subsequent steps are placed in your working directory. Go to the top right corner of POSTMAN and click on the **settings button**. In the general settings, make the necessary adjustments.

Working directory

Collaborate on files used in requests by sharing your working directory. Learn how to [setup your working directory](#) ↗

Location

D:\Redfish

Choose

Read files outside working directory



⚠ Enabling this will allow any 3rd party collections to potentially read any file on your system.

2. Create a JSON file **parameters.json** with content like below.

```
{
  "Targets" : [
    "/redfish/v1/UpdateService/FirmwareInventory/CPLD"
  ]
}
```

3. Create a JSON file **oem_parameters.json** with content like below.

```
{
  "ImageType" : "HPM",
  "force_update" : false
}
```

Name	Type	Description
force_update	Boolean	Optional. Default value is false. true: force to update. false: do not update when other user is in in update mode or a CPLD firmware has been uploaded.

4. Open POSTMAN and enter the **URI** to POST the request.
5. Select **POST** method.
6. In the **Authorization** tab, select Basic Auth and update request.
7. In the **Body** tab, select form-data and provide the key name as **UpdateFile** in the KEY section and change its type from **Text** to File.
8. Click on **Select File** in the **VALUE** section to select the signed image which is available in your local machine to update.
9. Like step 7 and 8, provide key name **UpdateParameters** and select **parameters.json** created in step 2.
10. Like step 7 and 8, provide key name **OemParameters** and select **oem_parameters.json** created in step 3.
11. Click **Send**.

POST
https://172.20.2.18/redfish/v1/UpdateService/upload
Send

Params
Authorization
Headers (10)
Body
Pre-request Script
Tests
Settings
Cookies

none
form-data
x-www-form-urlencoded
raw
binary

	Key	Value	...	Bulk Edit
☒	UpdateFile	outputjbc_02b4.hpm		
☒	UpdateParameters	parameters.json		
☒	OemParameters	oem_parameters.json		
	Key	Value		

Response:

```
{
  "@odata.type": "#UpdateService.v1_6_0.UpdateService",
  "Messages": [
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "A new task /redfish/v1/TaskService/Tasks/1 was created.",
      "MessageArgs": [
        "/redfish/v1/TaskService/Tasks/1"
      ],
      "MessageId": "Task.1.0.New",
      "Resolution": "None",
      "Severity": "OK"
    },
    {
      "@odata.type": "#Message.v1_0_8.Message",
      "Message": "The action UpdateService.MultipartPush was submitted to do firmware update.",
      "MessageArgs": [
        "UpdateService.MultipartPush"
      ],
      "MessageId": "UpdateService.1.0.StartFirmwareUpdate",
      "Resolution": "None",
      "Severity": "OK"
    }
  ]
}
```

8.4.7 Power Control

This section is dedicated to explaining how to control power through Redfish.

Request:

POST `https://{bmc ip}/redfish/v1/Chassis/Self/Actions/Chassis.Reset`

Response:

The response status is **202 Accepted**.

Example:

POST
▼
https://172.20.2.16/redfish/v1/Chassis/Self/Actions/Chassis.Reset

Params
 Authorization ●
 Headers (10)
 Body ●
 Pre-request Script
 Tests
 Settings

● none
 ● form-data
 ● x-www-form-urlencoded
 ● raw
 ● binary
 JSON ▼

```
{
  "ResetType": "ForceRestart"
}
```

Note: The `ResetType` can be one of the following values: "On", "ForceOff", "GracefulShutdown", "ForceRestart", "PowerCycle".

Response:

```
{
  "@odata.context": "/redfish/v1/$metadata#Task.Task",
  "@odata.id": "/redfish/v1/TaskService/Tasks/1",
  "@odata.type": "#Task.v1_4_2.Task",
  "Description": "Task for Chassis Reset",
  "Id": "1",
  "Name": "Chassis Reset",
  "TaskMonitor": "/redfish/v1/TaskService/TaskMonitors/1",
  "TaskState": "New"
}
```

8.4.8 BMC Firmware Version

To get BMC version, use "Managers" class.

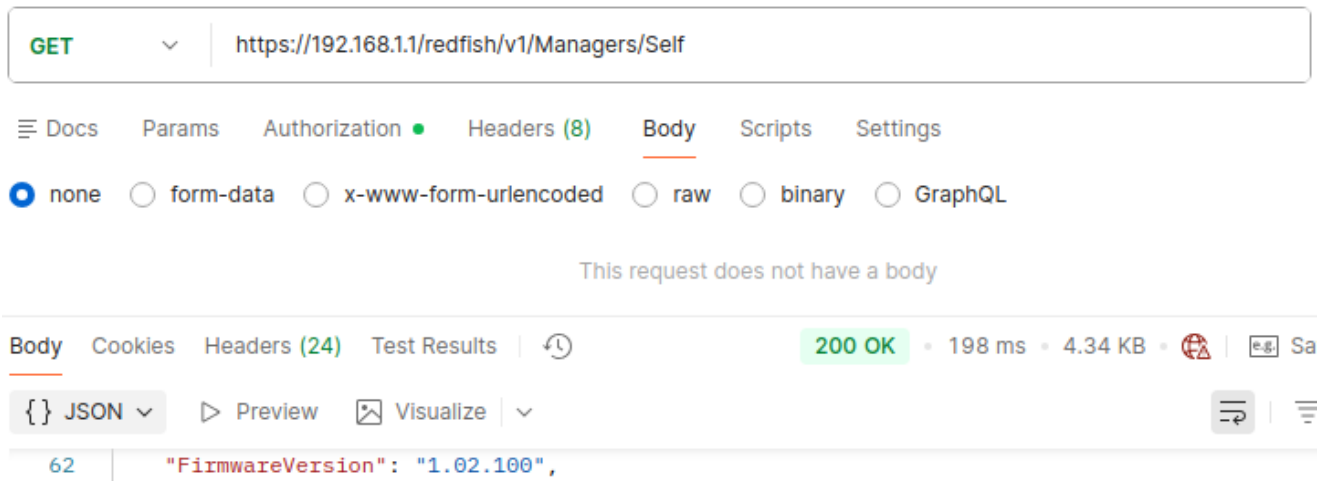
Request:

```
POST https://{bmc ip}/redfish/v1/Managers/Self
```

Response:

The response status is 200 OK.

Example:



The screenshot shows a REST client interface. At the top, a GET request is defined for the URL `https://192.168.1.1/redfish/v1/Managers/Self`. Below the URL bar, tabs for Docs, Params, Authorization, Headers (8), Body, Scripts, and Settings are visible. The 'Body' tab is selected, and the content area shows 'This request does not have a body'. Below the request area, the response details are shown: '200 OK' with a status bar indicating 198 ms, 4.34 KB, and a globe icon. The response body is displayed in JSON format: `{ "FirmwareVersion": "1.02.100",`. The JSON is partially visible, showing the first line and the start of the second line.

Member "**FirmwareVersion**" consists of:

BMC version - 1.02.100

8.4.9 BIOS Version

To get BIOS version, use "Systems" class.

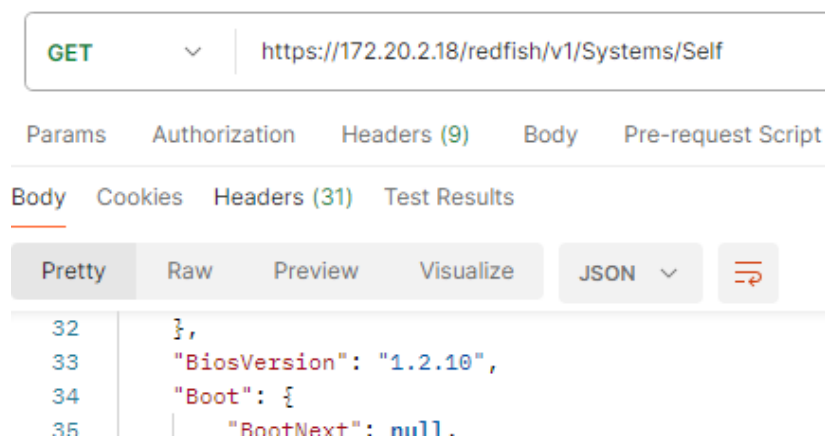
Request:

```
POST https://{bmc ip}/redfish/v1/Systems/Self
```

Response:

The response status is 202 OK.

Example:



Member "**BiosVersion**" has the value.

"1.2.10" - Leading version.Major version.Minor version

Please note that **minor version** of BIOS is **always represented in hexadecimal number**.

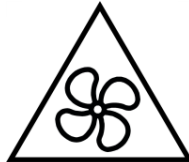
Safety Instructions

For user safety, please read and follow all **instructions**, **WARNINGS**, **CAUTIONS**, and **NOTES** marked in this manual and on the associated equipment before handling/operating the equipment.

1. Read these safety instructions carefully.
2. Keep this user's manual for future reference.
3. Read the specifications section of this manual for detailed information on the operating environment of this equipment.
4. The equipment can be operated at an ambient temperature of 55°C.
5. When installing/mounting or uninstalling/removing equipment; or when removal of the chassis lid required for user servicing (Section 3.1-3.5):
 - Turn off power and unplug any power cords/cables, and
 - Reinstall the chassis lid before restoring power.



Hazardous moving parts. Keep body parts out of the motion path.



6. To avoid electrical shock and/or damage to equipment:
 - Keep equipment away from water or liquid sources;
 - Keep equipment away from high heat or high humidity;
 - Keep equipment properly ventilated (do not block or cover ventilation openings);
 - Make sure to use recommended voltage and power source settings;
 - Always install and operate equipment near an easily accessible electrical socket-outlet;
 - Secure the power cord (do not place any object on/over the power cord);
 - Only install/attach and operate equipment on stable surfaces and/or recommended mountings;
 - If the equipment will not be used for long periods of time, turn off and unplug the equipment from its power source.
 - The power cord must be connected to a socket or outlet with a ground connection.
7. Never attempt to fix the equipment. Equipment should only be serviced by qualified personnel.
8. An RTC battery may be provided for uninterrupted, backup or emergency power.



Risk of explosion if battery is replaced with one of an incorrect type. Discard used batteries according to the manufacturer's instructions.

9. Equipment is not suitable for use in locations where children are likely to be present.
10. Equipment must be serviced by authorized technicians when:
 - The power cord or plug is damaged;
 - Liquid has penetrated the equipment;
 - It has been exposed to high humidity/moisture;
 - It is not functioning or does not function according to the user's manual;
 - It has been dropped and/or damaged; and/or,
 - It has an obvious sign of breakage.
11. Please pay strict attention to all warnings and advisories appearing on the device, to avoid injury or damage.

12. The equipment may have more than one power supply input. To reduce the risk of electrical shock, trained personnel should disconnect all power supply inputs before servicing.



Shock hazard! Disconnect all power supply inputs before servicing.



Shock hazard!



Multiple power sources

13. It is recommended that equipment be installed only in a server room or computer room where access is:
- Restricted to qualified service personnel or users familiar with restrictions applied to the location, reasons therefor, and any precautions required;
 - Only afforded by the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.
14. Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.
15. This product is intended to be supplied by a certified DC power source providing reinforced/double insulation from AC mains with an output rating of 36V to 72V DC ,20A min., Tma = 55°C. All power connection wiring must be performed by a qualified electrician in accordance with National Electrical Code, ANSI/NFPA 70 and Canadian Electrical Code, Part I, CSA C22.1. The DC power supply should be well-grounded to ensure safe operation. The protective earthing conductor shall be minimum 14 AWG and having green-and-yellow insulation. The ground wire should be installed first (before "+" and "-") and then removed.
16. When using a Fiber Optic Small-Form Pluggable (SFP) module, ensure it is IEC 60825-1, IEC 60825-2 and IEC 60950-1 or IEC 62368-1 certified and a Class 1 Laser Product.

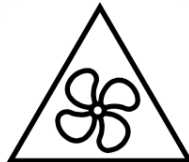
Consignes de Sécurité Importantes

Pour assurer la sécurité de l'utilisateur, veuillez lire et suivre toutes les **directives**, ainsi que les **AVERTISSEMENTS**, **MISES EN GARDE** et **REMARQUES** de ce manuel et indiqués sur l'équipement associé avant de manipuler ou utiliser l'équipement.

1. Veuillez lire attentivement ces instructions de sécurité avec soin.
2. Veuillez conserver ce manuel pour référence future.
3. Veuillez lire la section des spécifications de ce manuel pour avoir des informations détaillées sur l'environnement d'exploitation de cet équipement.
4. L'équipement peut être utilisé à une température ambiante de 55 °C.
5. Lors de l'installation ou du montage et de la désinstallation ou de la dépose de l'équipement; ou lors de la dépose du couvercle du châssis pour procéder à l'entretien par l'utilisateur (Sections 3.1-3.5):
 - Coupez l'alimentation et débranchez les cordons et les câbles d'alimentation, et
 - Reposez le couvercle du châssis avant de remettre l'alimentation.



Pièces mobiles dangereuses. Gardez les parties du corps hors de la trajectoire.



6. Pour éviter un risque d'électrocution et pour éviter d'endommager l'équipement :
 - Éloignez l'équipement de l'eau et de toute source liquide;
 - Éloignez l'équipement de toute source de chaleur ou d'humidité élevée;
 - Gardez l'équipement correctement ventilé (ne pas bloquer ou couvrir les ouvertures de ventilation);
 - Veillez à utiliser la tension recommandée et les réglages adéquats pour la source d'alimentation;
 - Veuillez toujours installer et exploiter l'équipement à proximité d'une prise de courant facilement accessible;
 - Assurez-vous que le cordon d'alimentation est acheminé de manière sécuritaire (ne déposez aucun objet dessus);
 - Installez, fixez et utilisez l'équipement sur des surfaces stables ou sur les fixations recommandées uniquement;
 - Si l'équipement n'est pas utilisé pendant une longue période, éteignez-le et débranchez-le de sa source d'alimentation.
 - Le cordon d'alimentation doit être connecté à une prise ou à une prise de courant avec mise à la terre.
7. N'essayez jamais de réparer l'équipement. L'équipement ne doit être réparé que par du personnel qualifié.

8.



Risque d'explosion si la batterie est remplacée par une batterie d'un type incorrect. Jetez les piles usagées conformément aux instructions du fabricant.

9. Cet équipement ne convient pas à une utilisation dans des lieux pouvant accueillir des enfants.
10. L'équipement doit être entretenu par des techniciens agréés lorsque :
 - le cordon d'alimentation est endommagé ou lorsque la fiche électrique est endommagée;
 - du liquide a pénétré à l'intérieur de l'équipement;
 - l'équipement a été exposé à un taux d'humidité élevé;
 - l'équipement ne fonctionne pas ou ne fonctionne pas conformément au manuel de l'utilisateur;
 - l'équipement est tombé ou lorsqu'il a été endommagé;
 - l'équipement présente un signe évident de défaillance.
11. Veuillez porter une attention rigoureuse à tous les avertissements et à tous les avis figurant sur l'appareil, pour éviter des blessures ou des dommages.

12. L'équipement peut avoir plus d'une entrée d'alimentation. Pour réduire le risque d'électrocution, le personnel qualifié devrait déconnecter toutes les entrées d'alimentation avant de procéder à l'entretien.



Risque d'électrocution! Débranchez toutes les entrées d'alimentation avant de procéder à l'entretien.



Shock hazard!
Risque d'électrocution!



Multiple power sources
Sources d'alimentation multiples

13. Il est recommandé que l'équipement soit installé que dans une salle de serveur ou de la salle informatique où:
- L'accès est limité au personnel de maintenance qualifié ou utilisateurs familiers avec les restrictions appliquées à l'emplacement, motifs, et tout les précautions nécessaires, et;
 - L'accès est uniquement assurée par l'utilisation d'un outil ou clé, ou d'autres moyens de sécurité, et est contrôlé par l'autorité responsable de l'emplacement.
14. Peut être installé dans des salles de matériel de traitement de l'information conformément à l'article 645 du National Electrical Code et à la NFPA 75.
15. Ce produit est destiné à être alimenté par une source d'alimentation CC certifiée fournissant une isolation renforcée/double du secteur CA avec une puissance de sortie de -48 V à -60 V CC, 12 A min., T_{ma} = 55°C. Tout le câblage de connexion d'alimentation doit être effectué par un électricien qualifié conformément au Code national de l'électricité, ANSI / NFPA 70 et au Code canadien de l'électricité, Partie I, CSA C22.1. L'alimentation CC doit être bien mise à la terre pour garantir un fonctionnement sûr. Le conducteur de mise à la terre de protection doit être au minimum 14 AWG et avoir une isolation verte et jaune. Le fil de terre doit être installé en premier (avant «+» et «-») puis retiré.

FCC Warning

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for assistance.

Getting Service

Ask an Expert: <https://www.adlinktech.com/en/Askanexpert>

ADLINK Technology, Inc.

Address: No. 66, Huaya 1st Road, Guishan District
Taoyuan City 333, Taiwan
Tel: +886-3-216-5088
Fax: +886-3-328-5723
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.

Address: 6450 Via Del Oro, San Jose, CA 95119-1208, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-600-1189
Email: info@adlinktech.com

ADLINK Technology (China) Co., Ltd.

Address: 300 Fang Chun Rd., Zhangjiang Hi-Tech Park, Pudong New Area
Shanghai, 201203 China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

ADLINK Technology GmbH

Address: Hans-Thoma-Strasse 8-10, 68163, Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

Please visit the Contact page at www.adlinktech.com for information on how to contact the ADLINK regional office nearest you.