

ORION HF210-G5

User Manual



1. About this User Manual

This user manual contains the information on Installation and maintenance of the ORION HF210-G5.



Caution: Experienced technicians should perform the Installation and maintenance.

Document title: **ORION HF210-G5**
Document number: **Revision 03**
Document update date: **January 2021**

The following Notes, Cautions and Warnings might appear in this user manual.



Note: Explains an important point or tip to help you to better use of the product.



Caution: Indicates the potential damage to hardware or loss of data, security problems, or performance issues and tells you to avoid the problem.



Warning: Indicates that an action or step can result in physical harm, property or hardware damage.

To avoid damaging your server, perform the following steps before you begin working inside the server.

1. Ensure that you follow the Safety Instruction.
2. Ensure that your work surface is flat and clean to prevent the server cover from being scratched.
3. Turn off your server.
4. Disconnect all network cables from the server.

CAUTION: To disconnect a network cable, first unplug the cable from your server and then unplug the cable from the network device. After you finish working inside the server, replace all covers, panels, and screws before connecting to the power source.

Safety instructions:

Use the following safety guidelines to protect your server from potential damage and to ensure your personal safety. Unless otherwise noted, each procedure included in this document assumes that the following conditions exist:

You have read the safety information that shipped with your server.

A component can be replaced or, if purchased separately, installed by performing the removal procedure in the reverse order.

Copyright © 2019 CIARA Technologies, a Hypertec brand. All Rights Reserved.

2. Table of Contents

Contents

1.	About this User Manual.....	1
2.	Table of Contents	2
3.	ORION HF210-G5 Specifications	5
4.	Chassis Overview.....	6
5.	Front Panel Components.....	7
6.	Back Panel Components	8
7.	Accessory Boxes & Rails	9
8.	Labelling	10
8.1	Power supplies cage	10
8.2	Serial Number and Model Number Labels on Mylar	11
8.3	HDD trays	11
8.4	Support and Certification Labels	12
9.	Chassis Layout.....	13
10.	Motherboard Layout	14
11.	Detailed Motherboard Layout.....	16
11.1	Connector Functionality	17
11.2	Jumper Functionality	18
11.3	LED Functionality.....	20
11.4	Block Diagram.....	21
12.	Removing the Chassis Cover.....	22
13.	Installing the Chassis Cover	23
14.	How to clear the CMOS with battery and pad	24
14.1	Clear CMOS by Battery	24
14.2	Clear CMOS by CMOS Pad	26
15.	How to replace the CMOS battery:.....	27
16.	Replacing PCIE Card.....	29
16.1	Replacing PCIE Card 1	29
16.2	Replacing PCIE 2 Card	32
17.	Removing and Installing Memory Modules.....	34
17.1	Removing Memory Module.....	34
17.2	Installing Memory Module	35
18.	Replacing Swappable SSD.....	37
19.	Replacing GPU	39
20.	Rack Mounting	44
21.	Plugging the Power Cords.....	47
22.	Turning on the System.....	48
23.	Dr. Debug codes	49
24.	Accessing BIOS:	50
24.1	BIOS Menu.....	51
24.2	Navigation Keys.....	51
25.	Configuring BMC IP-Address Settings for remote management.....	52
25.1	Configuring the BMC IP-Address Settings for Remote management in BIOS Utility.....	52
25.2	Configuring the Static BMC IP-Address Settings for Remote management in BMC Web-GUI.....	55
26.	Using the BMC (IPMI) Web User Interface	59
27.	Accessing the BMC (IPMI) Management Console.....	60
28.	Viewing and Configuring the BMC (IPMI) Management Console	61
28.1	Menu bar	62
28.2	Quick Button and Logged-in User.....	62
28.3	Dashboard	63

28.3.1 Product Information	63
28.3.2 Firmware Information	63
28.3.3 Network Information	64
28.3.4 Sensor Monitoring	64
28.3.5 Event Logs	64
28.4 Sensors	65
28.4.1 Sensor detail:	65
28.5 System Information	66
28.5.1 FRU Information	66
28.5.2 Chassis Information	66
28.5.3 Board Information	66
28.5.4 Product Information	66
28.6 Logs & Reports	68
28.6.1 IPMI Event Log	68
28.6.2 Video Log	69
28.7 Settings	70
28.7.1 Data & Time	71
28.7.2 External User Services	72
28.7.2.1 External User Services Page	72
28.7.2.2 LDAP/E-directory Settings	72
28.7.2.3 Active Directory Settings	74
28.7.2.4 RADIUS Settings	75
28.7.3 KVM Mouse Settings	78
28.7.4 Log Settings	79
28.7.4.1 Log Settings Policy	79
28.7.5 Media Redirection Settings	80
28.7.5.1 General Settings	81
28.7.5.2 VMedia Instance Settings	81
28.7.5.3 Remote Session	82
28.7.6 Network Settings	83
28.7.6.1 Network IP Settings	83
28.7.6.2 Network Bond Configuration	85
28.7.6.3 DNS Configuration	85
28.7.7 PAM Order Settings	87
28.7.8. Platform Event Filter	88
28.7.8.1 Event Filters	88
28.7.8.2 Alert Policies	90
28.7.8.3 LAN Destinations	91
28.7.9 Services	93
28.7.10 SMTP Settings	95
28.7.11 SSL Settings	96
28.7.11.1 View SSL Certificate	96
28.7.11.2 Generate SSL Certificate	97
28.7.11.3 Upload SSL Certificate	97
28.7.12 System Firewall	98
28.7.12.1 General Firewall Settings	98
28.7.12.2 General Firewall Settings	99
28.7.13 User Management	101
28.7.14 Video Recording	103
28.7.14.1 Port Firewall Rules	104
28.7.15 Keep Share NIC Link Up	106
28.7.16 FAN Settings	107
28.7.16.1 Open Loop Control Table	107
28.7.16.2 Close Loop Control Table	107
28.7.16.3 Temperature Sensor and Corresponding Fan Table	108
28.7.16.4 FAN Mode	109

28.7.17. CPU Profile Selection	110
28.8 Remote Control	111
28.9 Image Redirection	112
28.9.1 Remote Media	112
28.10 Power Control	113
28.11 Miscellaneous.....	114
28.11.1 UID Control.....	114
28.11.2 Post Snoop.....	114
28.12 Maintenance	115
28.12.1 Backup Configuration	115
28.12.2 Restore Configuration	115
28.12.3 Firmware Image Location	115
28.12.4 Firmware Update.....	116
28.12.5 BIOS Update	116
28.12.6 Restore Factory Defaults	117
28.12.7 Reset.....	117
28.13 Sign Out	118
29. Updating Bios and ME	119
30. Profile Loading in BIOS	126
31. Downloading and Uploading a Profile in Linux.....	128
31.1 Downloading an existing Overclocking Profile.....	128
31.2 Uploading a Overclocking Profile.....	130
32. Drivers & Tools	132
32.1 Drivers Downloading	132
32.2 Monitoring CPU Frequency in Linux	133
32.2.1 i7z	133
32.2.2 Turbostat.....	134
32.3 Verifying CPU Frequency for Windows.....	134

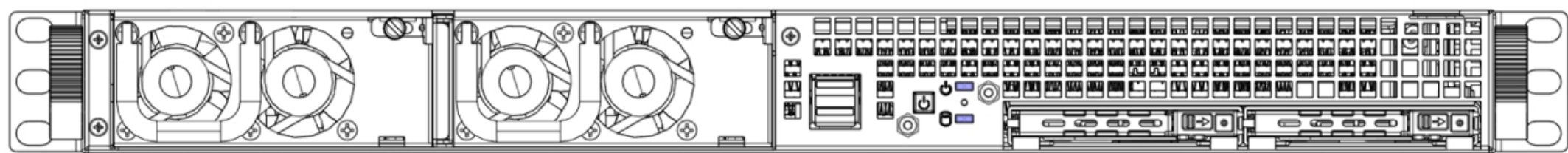
3. ORION HF210-G5 Specifications

The ORION HF210-G5 is a single socket, 1U rackmount form factor server and supports the following specification.

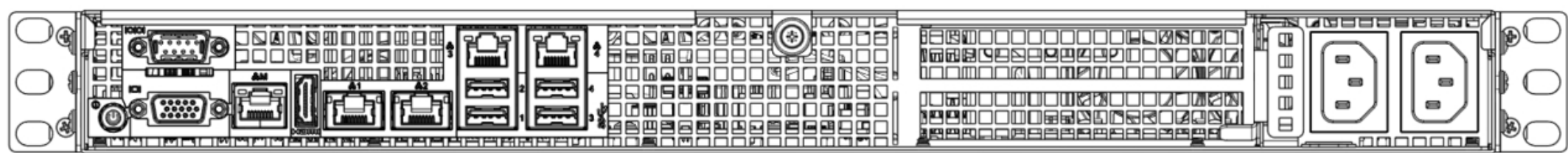
Form Factor	1U
Chipset	Intel® Z490
Processor	Intel® Core™ i9-10900KF - 10 Cores Overclocked Up to 5.3GHz*, 20.00 MB Cache, LGA1200 Highly Overclocked L3 Cache (Ring Architecture)
Cooling System	High Performance Liquid Cooled System, Closed Loop and Maintenance Free
Memory	Up to 128 GB (4x 32GB) DDR4-3600MHz non-ECC Dual Channel Low Latency CAS Memory
Network Controller	(2) Intel® X710 10GbE RJ45 Port + (1) Intel® i210AT 1GbE RJ45 Port (NCSI) + (1) Dedicated Management 1GbE RJ45 Port
Storage Controller	Onboard Intel® Z490 Express Chipset SATA 6Gbps Controller Support RAID 0, 1, 5 and 10 Intel® Rapid Storage Technology (Optional Hardware RAID)
Drive Bays	(2) 2.5” SATA 6Gbps hot-swap drives HDD/SSD (1) M.2 PCIe 3.0 x4 NGFF-2242/2280 (42mm or 80mm) (1) M.2 PCIe 3.0 x4 NGFF-2242/2280/22110 (42mm, 80mm or 110mm)
Expansion Slots	(1) PCIe 3.0 x16 Full Height Full Length Dual Width (FHFLDW) or (2) PCIe 3.0 x8 Full Height Full Length Single Width (FHFL)
Validated Network Adapters	SolarFlare / Xilinx: Flaeron Series & X2 Series Mellanox: ConnectX-3, 4, 5 & 6 Series ExaBlaze: ExaNIC X10, X25 & X40 Series
Validated FPGA Adapters	SolarFlare / Xilinx X2 Series Mellanox ConnectX-3, 4, 5 and 6 Series ExaBlaze ExaNIC X10, X25 and X40 Series
I/O Ports	(2) USB 3.1 Gen2 Type-A, (2) USB 3.1 Gen1 Type-A, (1) HDMI DB15, (1) Serial Port DB9, (2) 10GbE RJ45 LAN, (1) 1GbE RJ45 LAN, (1) 1GbE RJ45 Management LAN
System Management	AST2500 Advanced Graphics & Remote Management Processor IPMI 2.0 Compliant Web-based user interface for remote management & iKVM Remote, unblocked, BIOS-level access and control
Chassis Features	QCode for easy troubleshooting Tool-Less Rail kit
Power Supply	820W Redundant (1+1) High Efficiency 80 PLUS® Platinum
Environment	Operating: 10°C to 35°C (50°F to 95°F) @ 8% to 80% (non-condensing) Non-operating: -40°C to 60°C (-40°F to 140°F) @ 20% to 95% (non-condensing)
Dimensions (DxWxH)	30.6” x 17.3” x 1.7” (778mm x 440mm x 44mm)
Estimated Weight	37.4 lb / 16.5 kg
Warranty	CIARA’s limited hardware warranty includes a one year, parts and labour with return to CIARA USA or Canada. Customers may purchase an extended warranty of up to 3 years on parts and labour with different support levels. Please contact CIARA at 1-877-242-7272 for complete warranty details including limitations and transferability.
OS Support	Microsoft® Windows® Server 2016 R2, Microsoft® Windows® Server 2019, Linux® RHEL 7.5 (minimum KERNEL: 3.10.0-862.el7), CentOS™ 7.5 (minimum KERNEL: 3.10.0-862.el7), Debian 9.5 (minimum KERNEL: 4.15), Ubuntu 18.04 (minimum KERNEL: 4.15), support for other versions available upon request.
Notes	*Maximum clock speed may vary depending on applications and workloads.

4. Chassis Overview

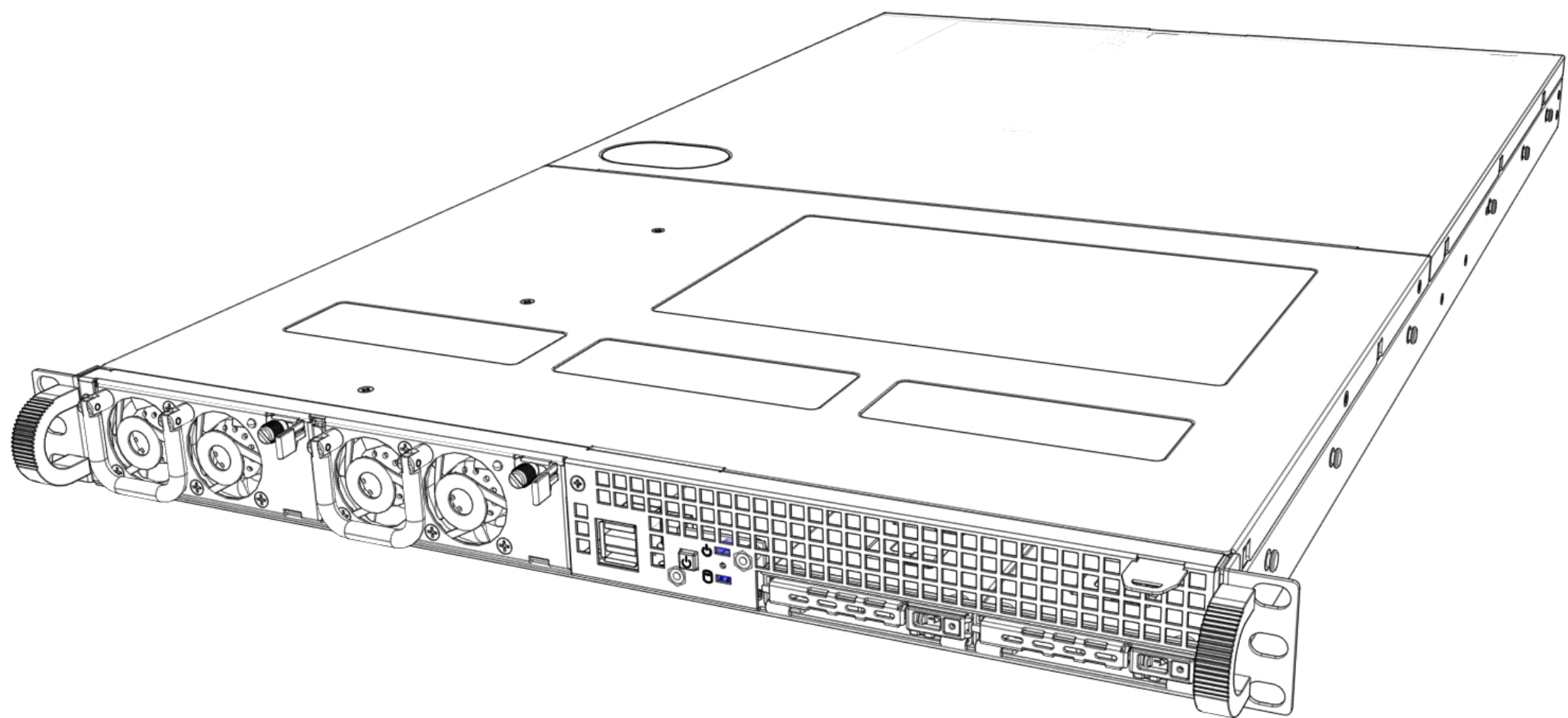
The following illustrations are the ORION HF210-G5 chassis Front, Back and Side views.



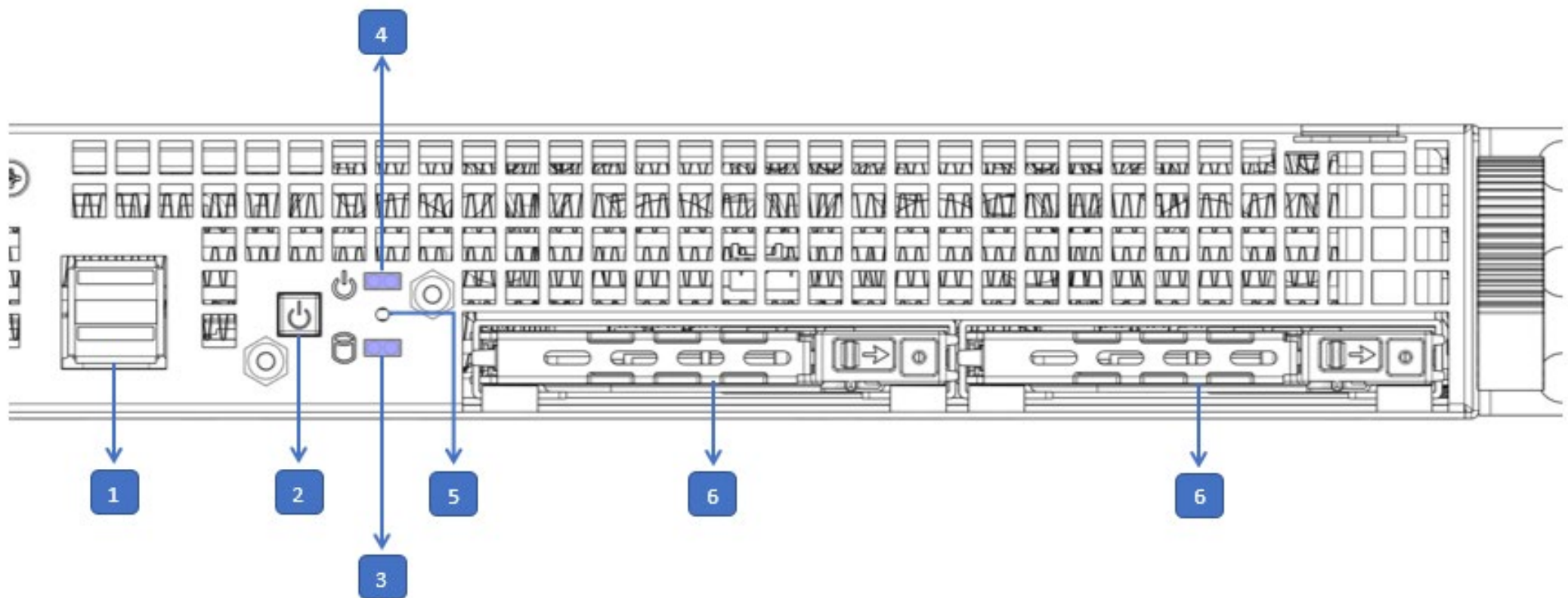
Front



Back

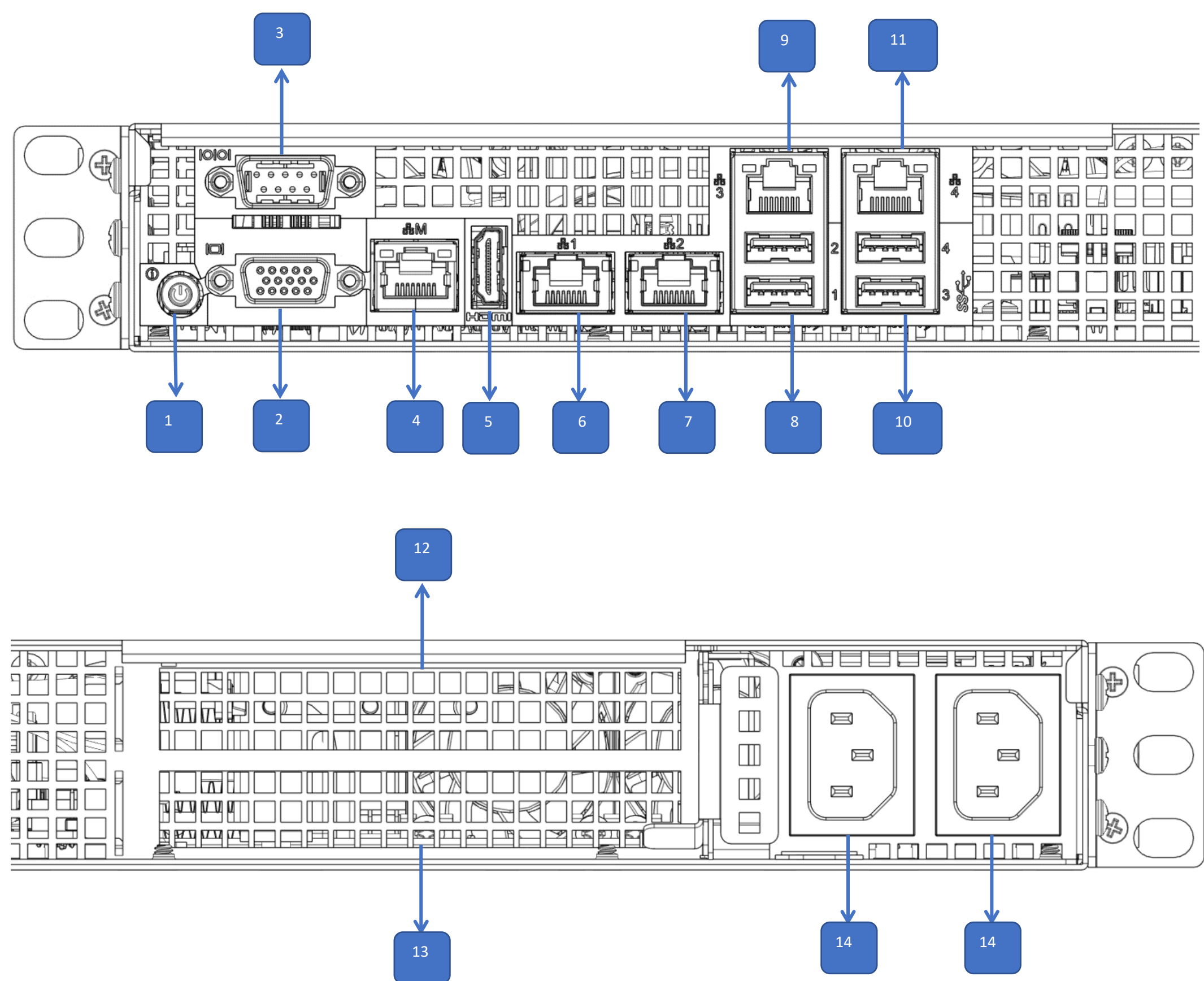


5. Front Panel Components



ITEM	DESCRIPTION
1	2x USB 3.1 Gen1
2	Power Button
3	HDD LED
4	Power LED
5	Reset
6	2x Drive Bay

6. Back Panel Components

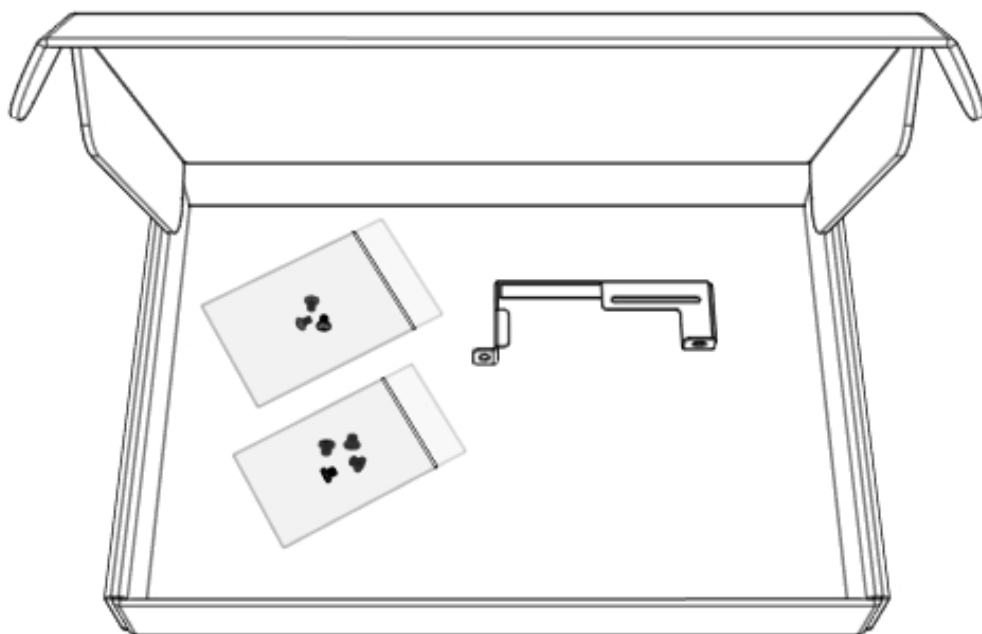


ITEM	DESCRIPTION
1	UID Switch (UID1)
2	VGA Port (VGA1)
3	Serial Port (COM1)
4	LAN RJ-45 Port (IPMI_LAN)
5	HDMI Port (HDMI)
6	10G LAN RJ-45 Port (LAN1)
7	10G LAN RJ-45 Port (LAN2)
8	USB 3.1 Gen2 Ports (USB31_1_2)
9	1G LAN RJ-45 Port (LAN3)
10	USB 3.1 Gen2 Ports (USB31_3_4)
11	1G LAN RJ-45 Port (LAN4)
12	PCIe x16 (FH/FL/DW)
13	PCIe x8
14	2x Power Outlet

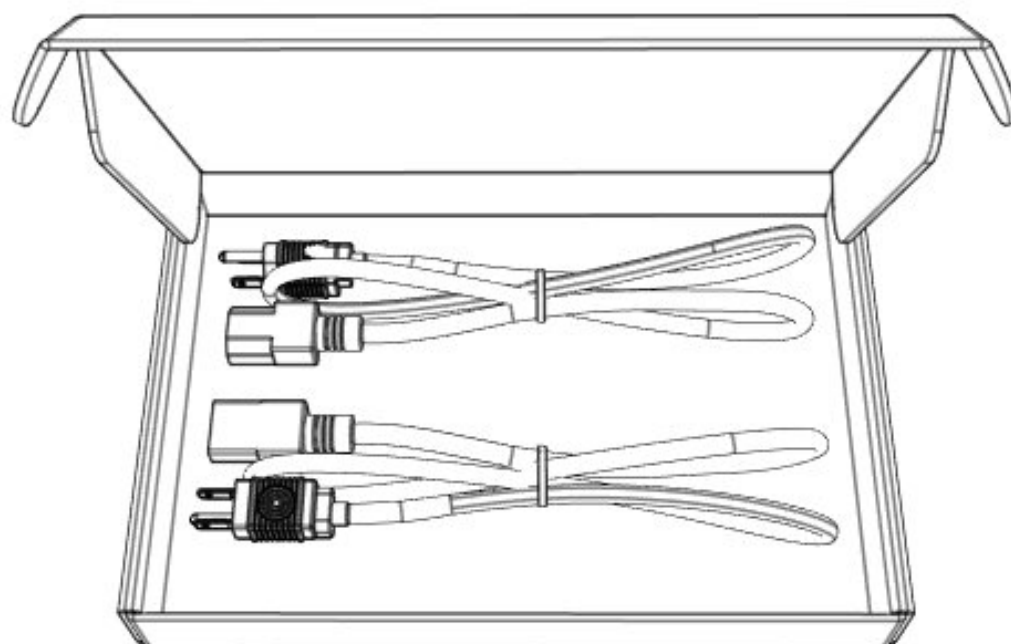
7. Accessory Boxes & Rails

The ORION HF210-G5 server includes (2) accessory boxes:

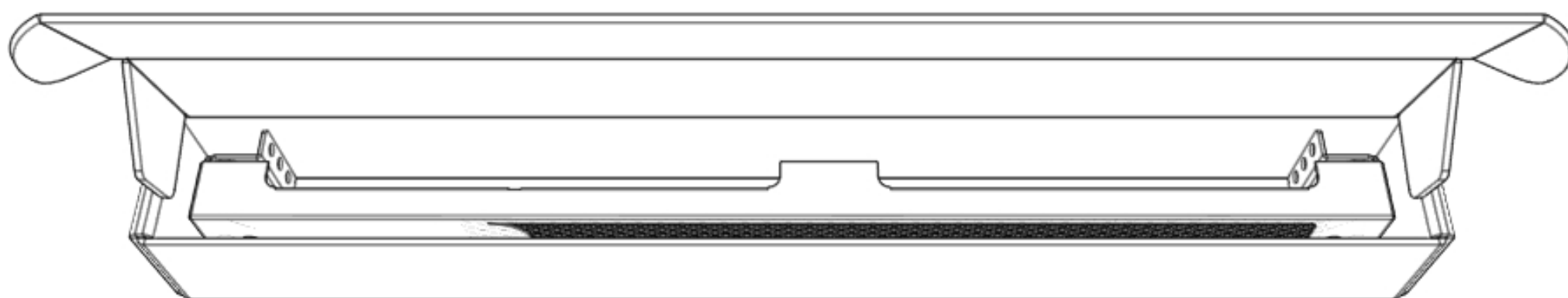
Accessory Box #1 with GPU Cables and Brackets



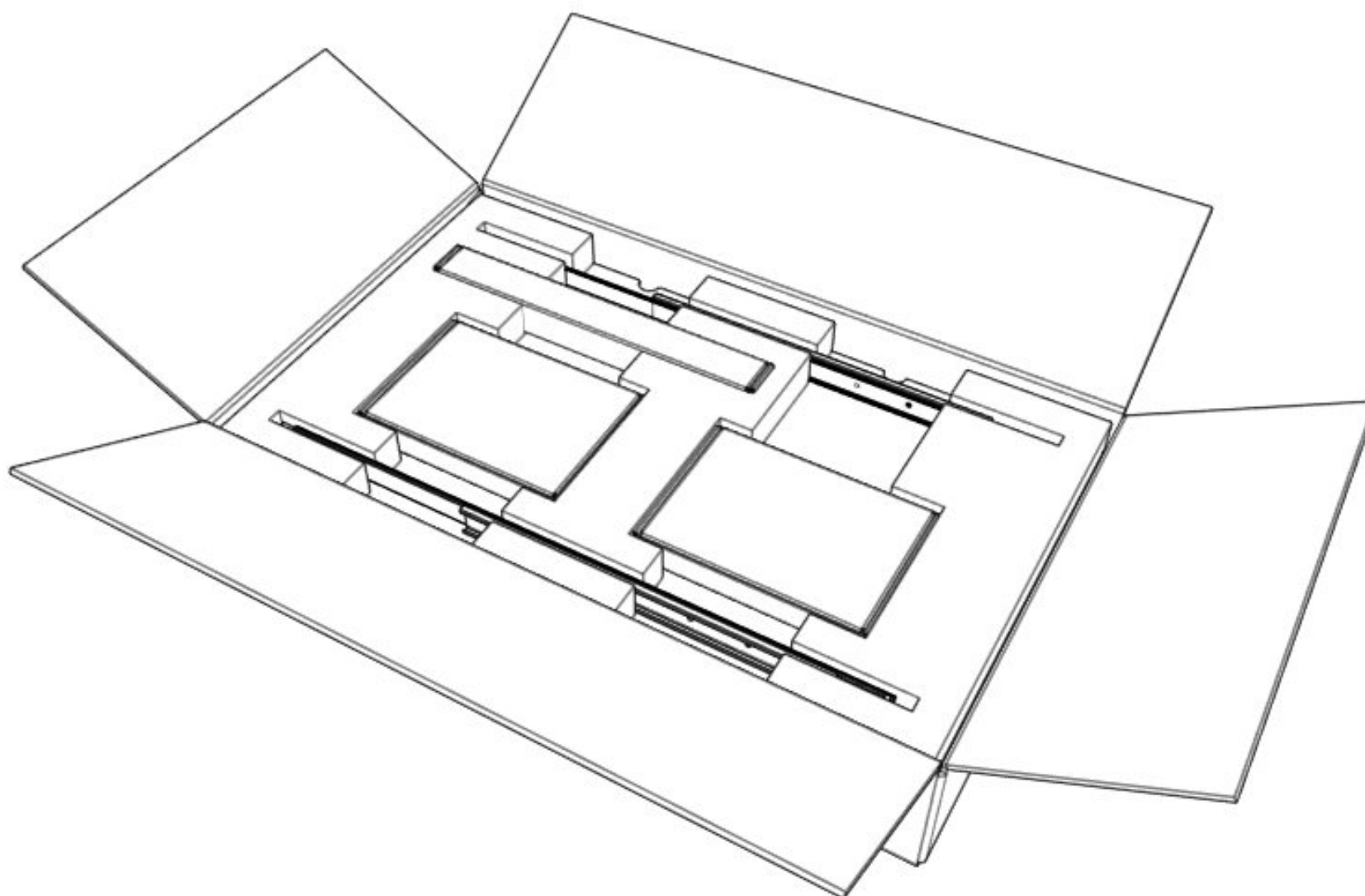
Accessory Box #2 with (2) Power Cables



Also the ORION HF210-G5 server includes (1) bezel box:



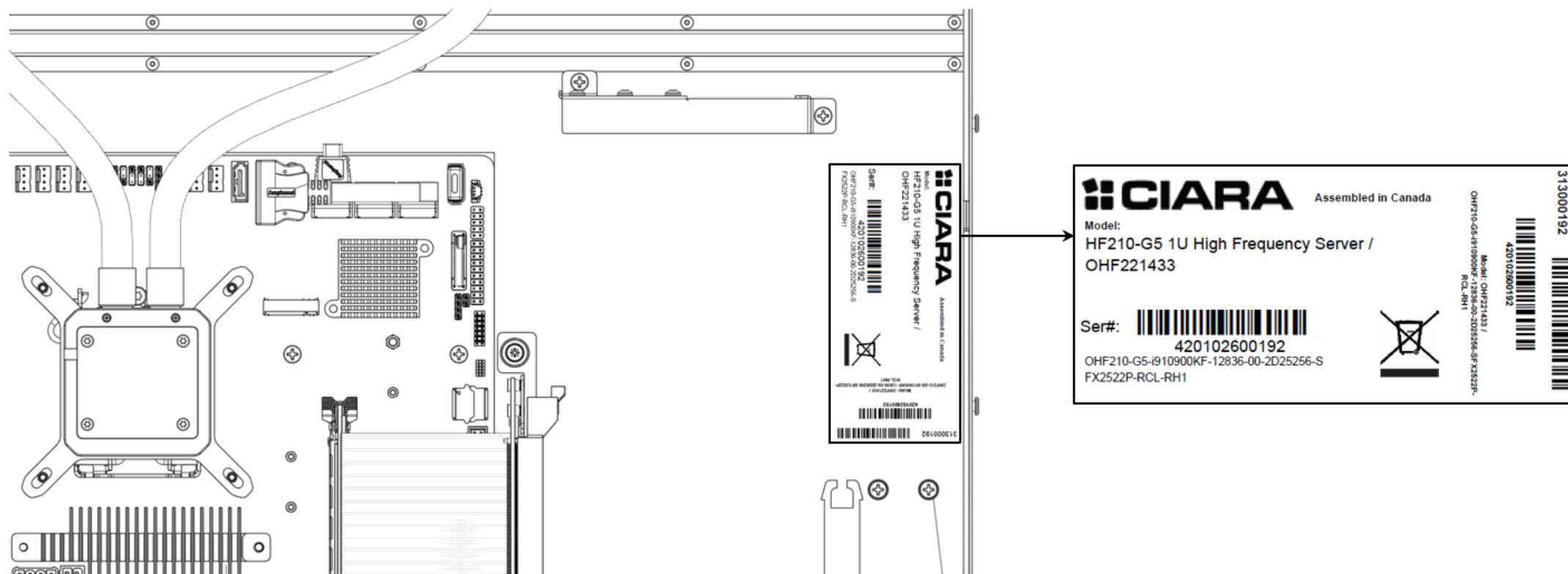
The rails, bezel box and both accessory boxes are placed as shown below in the box with the server.



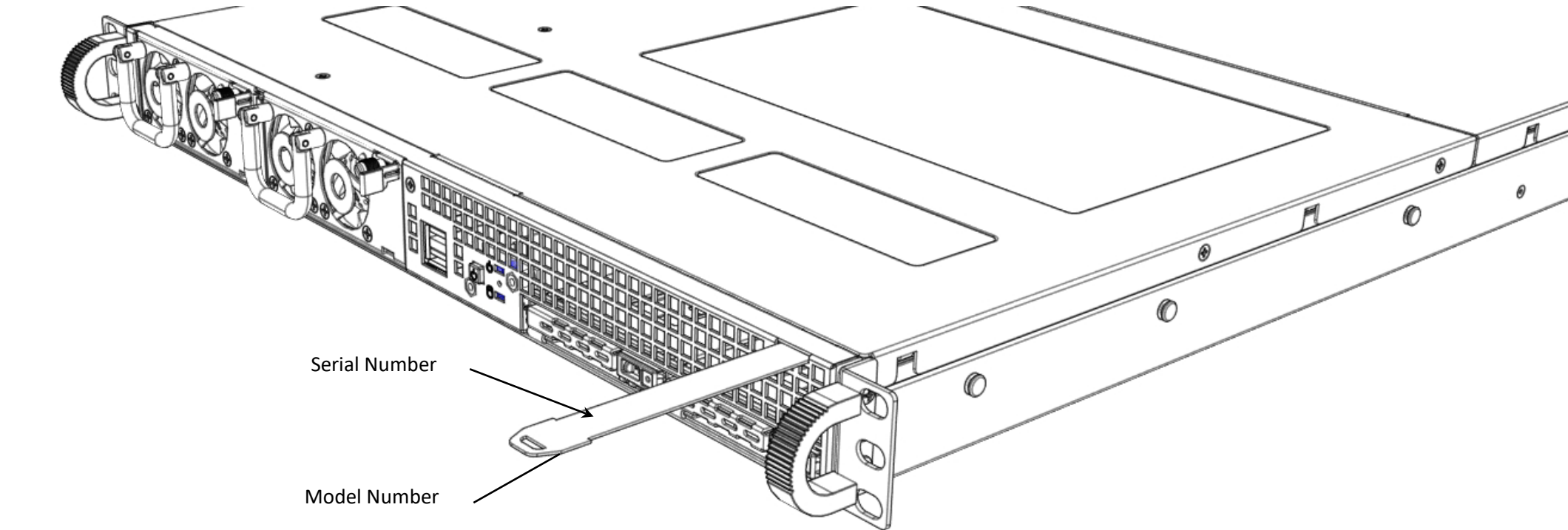
8. Labelling

This section contains information on the different labels found on the server.

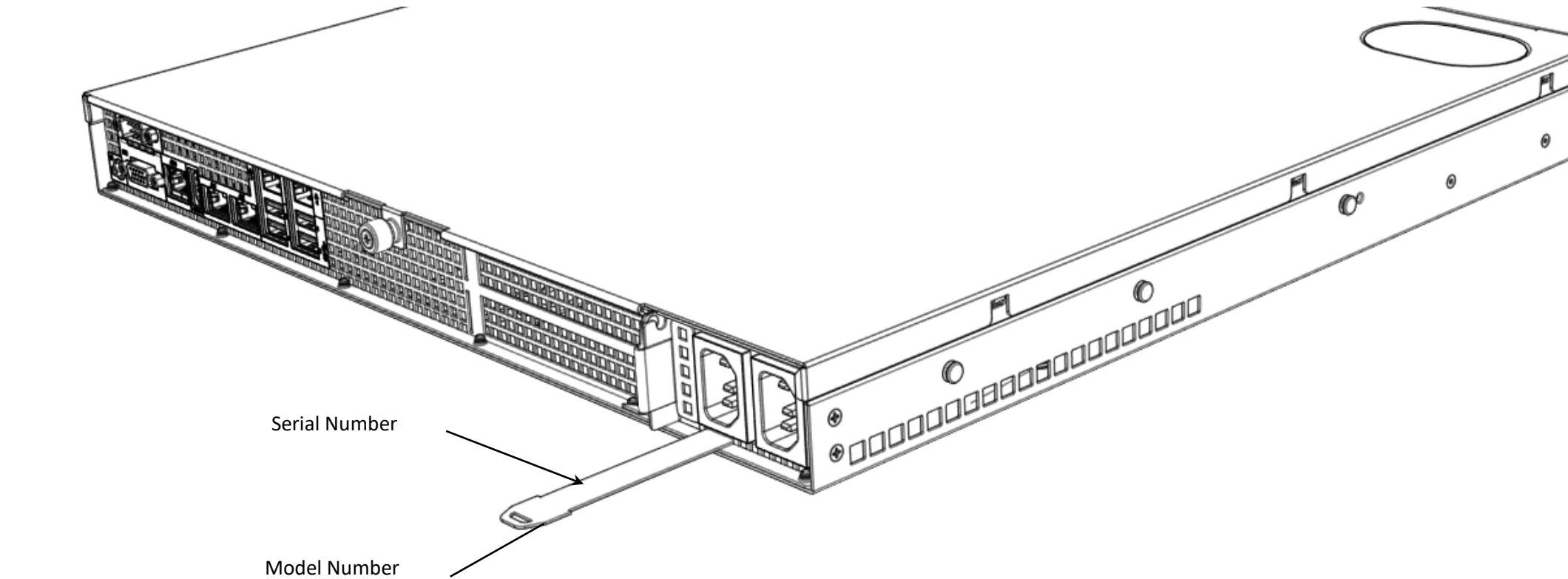
8.1 Power supplies cage



8.2 Serial Number and Model Number Labels on Mylar

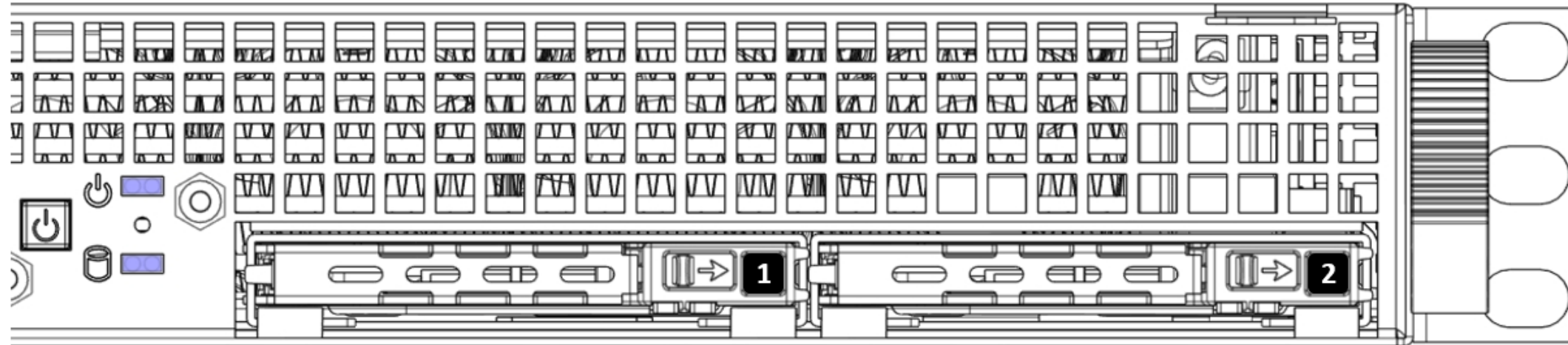


Front



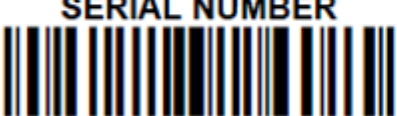
Back

8.3 HDD trays



8.4 Support and Certification Labels

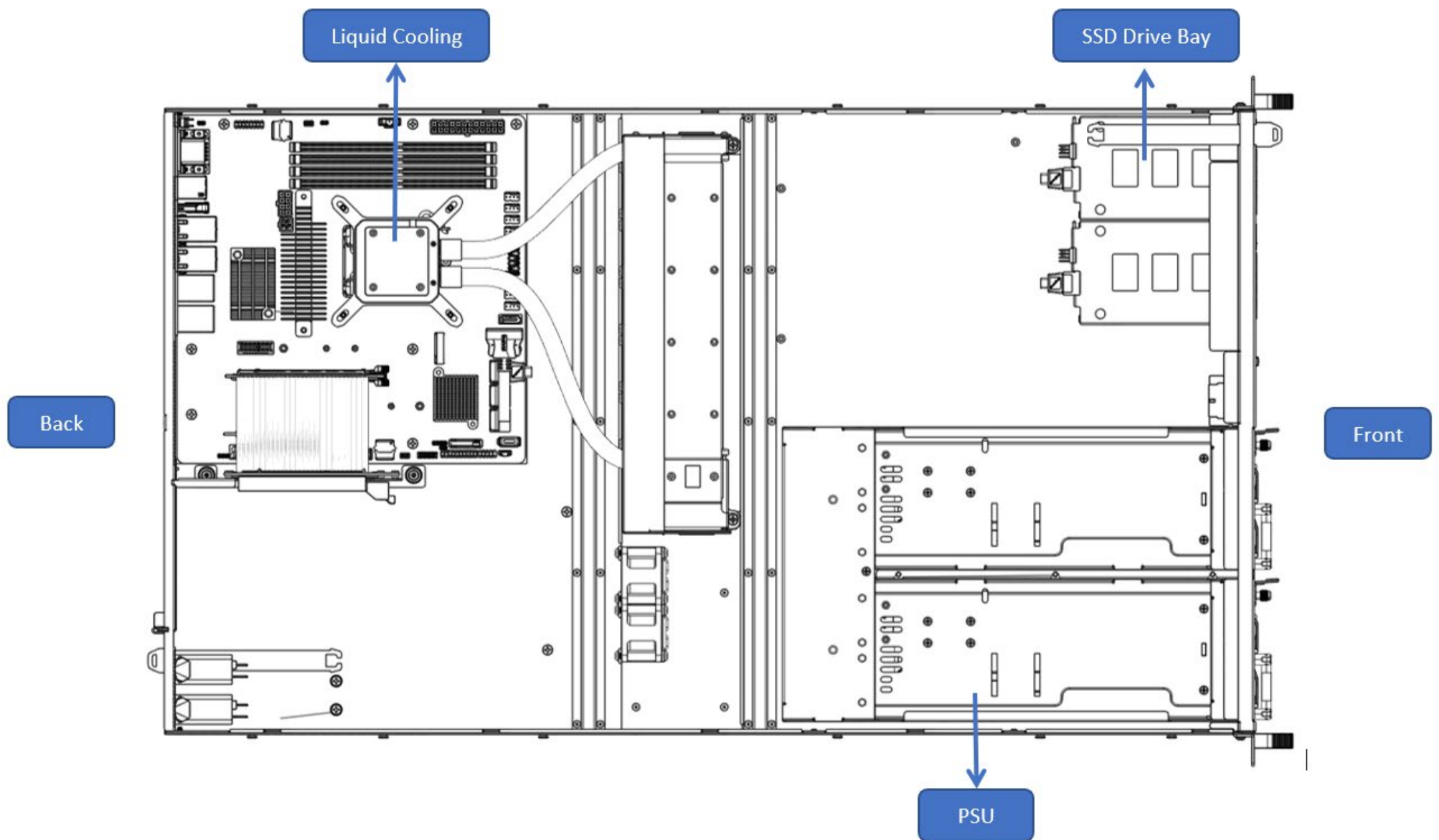
		OHF210-G5-i910900KF-12836-00-2D25256-SFX2522P-RCL-RH1	
MODEL CODE OHF221433		SERIAL NUMBER	
MFG DATE 2020-12			
SUPPORT INFORMATION		420102600192	
CIARA SUPPORT			
T: 1-855-597-4913 E: ORIONHFSUPPORT@CIARATECH.COM			
27706			

		OHF210-G5-i910900KF-12836-00-2D25256-SFX2522P-RCL-RH1	
MODEL CODE OHF221433		INPUT 100-240V~ 50/60 Hz 15A	
CUSTOM SN 420102600192		ASSET TAG	
		This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. CAN ICES3[A]	
420102600192		 Made in Canada	
27706			

		This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. CAN ICES-3 (A)/NMB-3(A)		 R-R-HYP-ORION-HF210-G5	
型号 (Model):		ORION HF210-G5			
AC 输入 (INPUT): 100-240Vac, 13A/6A (x2), 47-63 Hz					
警告! 在进行维修之前, 请断开所有电源连接 此為甲類資訊技術設備, 於居住環境中使用時, 可能會造成射頻擾動, 在此種情況下, 使用者會被要求採取某些適當的對策。 警告: 此为A级产品, 在生活环境中, 该产品可能会造成无线电干扰。在这种情况下, 可能需要用户对其干扰采取可行的措施。		Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.		Laite on liitettävä suojamdoituskoskettimilla varustettuun pistorasiaan. Apparatet må tilkoples jordat stikkontakt. Apparaten skall anslutas till jordat uttag. Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada 制造商 (manufacturer): Hypertechnologie Ciara Inc 服务器 Rack-Mountable Server 加拿大制造 Assembled in Canada 制造商 Manufactured on: /	
CAUTION: Slide/rail mounted equipment is not to be used as a shelf or a work space. Disconnect all power to the unit before servicing.					

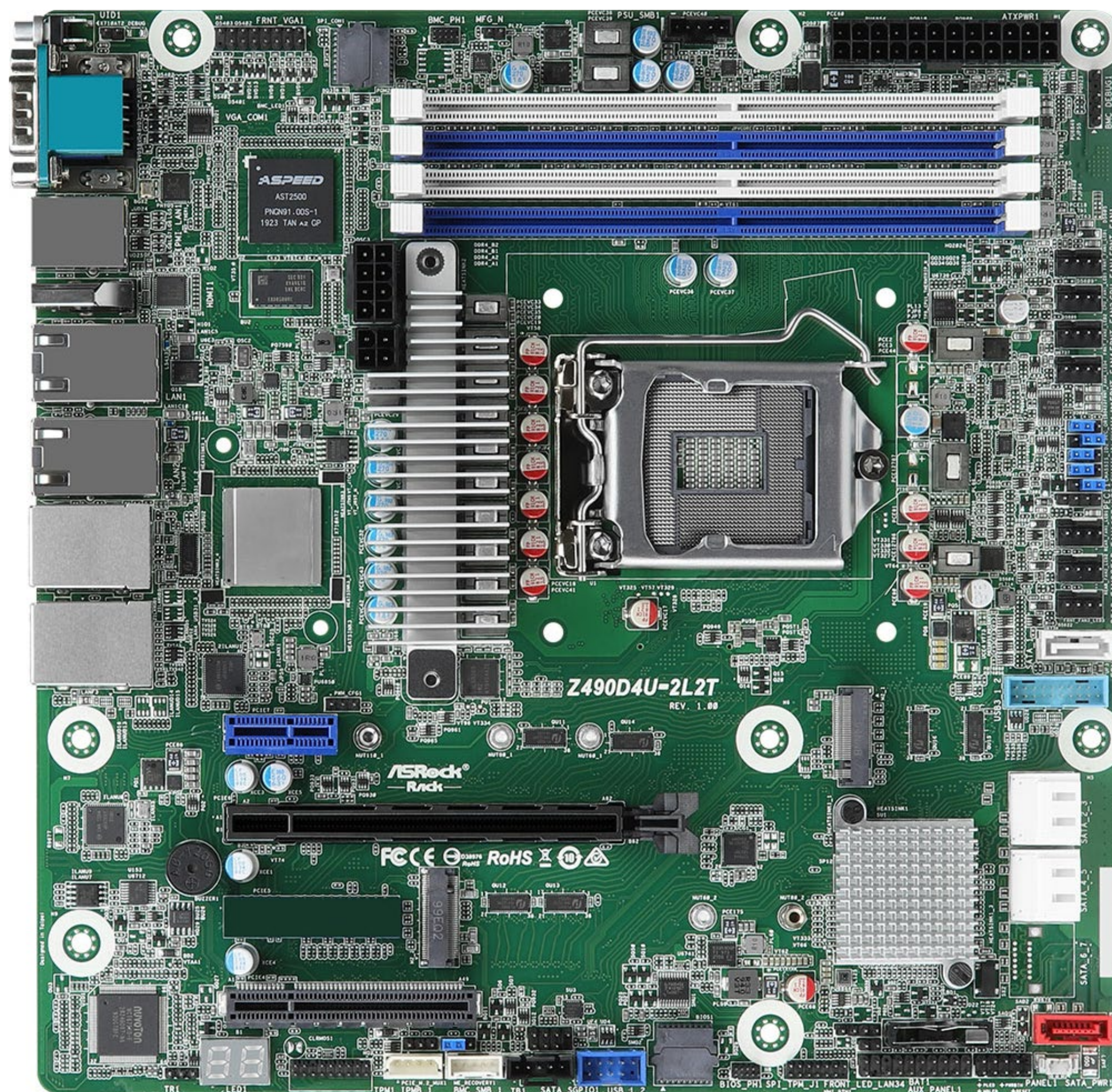
9. Chassis Layout

The following illustration shows inside of the ORION HF210-G5 system.



10. Motherboard Layout

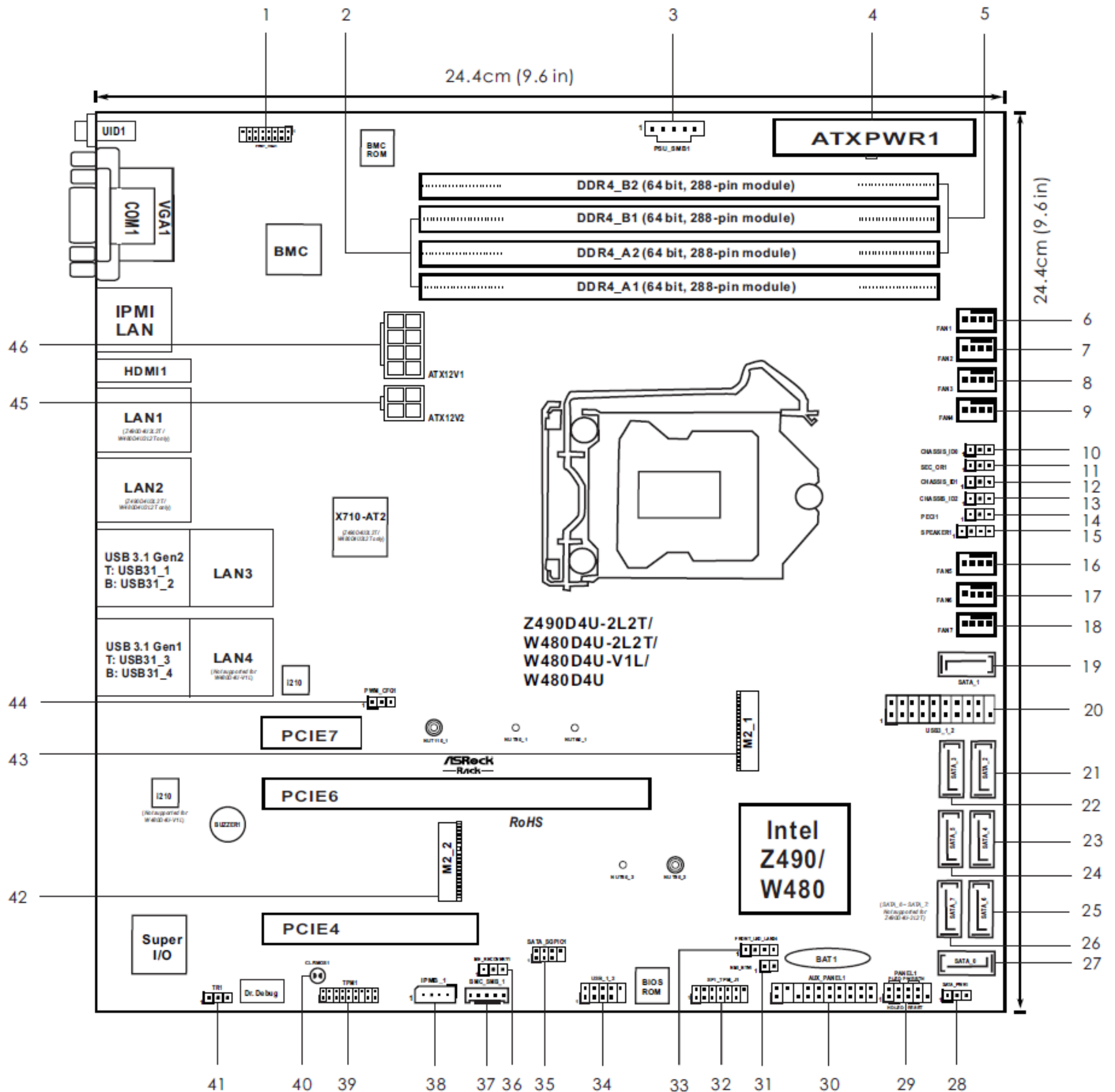
The following picture shows the motherboard layout in the ORION HF210-G5 system.



Feature	Specification
Form factor	mATX
Processor Support	Support Intel® 10th Gen. Core™ i9/i7/i5/i3, Pentium, Celeron® Series Processors
Chipset	Intel® Z490
Memory	4 x 288-pin DDR4 DIMM slots Support up to 128GB DDR4 non-ECC UDIMM
LAN	2 x RJ45 GLAN by Intel® i210 2 x RJ45 10G base-T by Intel® X710-AT2 1 x RJ45 Dedicated IPMI LAN port by RTL8211E Supports Wake-On-LAN Supports Energy Efficient Ethernet 802.3az Supports Dual LAN with Teaming function Supports PXE LAN1 supports NCSI
VGA / VRAM	Integrated in BMC with DDR4 256MB VRAM
BMC	ASPEED AST2500
Expansion Slot	Slot 6: Gen3 x16 link, auto switch to x8 link if Slot 4 is occupied (Physical x16, EE x16/x8 (from CPU), shared with Slot 4) Slot 4: Gen3 x8 link (Physical x8, EE x0/x8 (from CPU), shared with Slot 6) Slot 7: Gen3 x1 link (Physical x1, EEx1 (from PCH))
Storage	6 x SATA3 6Gb/s (SATA0-5, SATA_0 supports SATA DOM)
Rear IO Connector	1x HDMI Port, 1x VGA Port, 1x Serial Port, 1x UID 2x USB 3.2 Gen1 Type-A (5Gbps), 2x USB 3.2 Gen2 Type-A (10Gbps) 4 +1 RJ45 Gigabit Ethernet LAN ports LAN Ports with LED (ACT/LINK LED and SPEED LED)
Internal Connector	ATX Power 1x (24-pin) + 1x (8-pin) + 1x (4-pin) Front Panel Connector 1x (RST, PWRBTN, HDDLED, PWRLED) Fan Header 7x (1CPU/4Front/2Rear) USB 3.2 Gen1 Header 1x (supports 2 USB 3.1 Gen1 ports) USB 2.0 Header 1x (supports 2 USB 2.0 ports)

11. Detailed Motherboard Layout

The following illustration shows the detailed motherboard layout in the ORION HF210-G5 system.



1. Front VGA Header (FRNT_VGA1)

2. 2 x 288-pin DDR4 DIMM Slots (DDR4_A1, DDR4_B1, Blue)

3. PSU SMBus (PSU_SMB1)

4. ATX Power Connector (ATXPWR1)

5. 2 x 288-pin DDR4 DIMM Slots (DDR4_A2, DDR4_B2, White)

6. Chassis Fan Connector (FAN1)

7. Chassis Fan Connector (FAN2)

8. Chassis Fan Connector (FAN3)

9. Chassis Fan Connector (FAN4)

10. Chassis ID0 Jumper (CHASSIS_ID0)

11. Security Override Jumper (SEC_OR1)

12. Chassis ID1 Jumper (CHASSIS_ID1)

13. Chassis ID2 Jumper (CHASSIS_ID2)

14. CPU PECI Mode Jumper (PECI1)

15. Chassis Speaker Header (SPEAKER1)

16. Chassis Fan Connector (FAN5)

17. Chassis Fan Connector (FAN6)

18. Chassis Fan Connector (FAN7)

19. SATA3 Connector (SATA_1)

20. USB 3.1 Gen1 Header (USB3_1_2)

21. SATA3 Connector (SATA_2)

22. SATA3 Connector (SATA_3)

23. SATA3 Connector (SATA_4)
24. SATA3 Connector (SATA_5)

25. SATA3 Connector (SATA_6) (Not supported for Z490D4U-2L2T)

26. SATA3 Connector (SATA_7) (Not supported for Z490D4U-2L2T)

27. SATA3 DOM Connector (SATA_0), Red

28. SATA DOM Power Connector (SATA_PWR1)

29. System Panel Header (PANEL1)

30. Auxiliary Panel Header (AUX_PANEL1)

31. Non Maskable Interrupt Button (NMI_BTN1)

32. SPI TPM Header (SPI_TPM_J1)

33. Front LAN LED Connector (FRONT_LED_LAN34)

34. USB 2.0 Header (USB_1_2)

35. SATA SGPIO Connector (SATA_SGPIO1)

36. ME Recovery Jumper (ME_RECOVERY1)

37. BMC SMBus Header (BMC_SMB_1)

38. Intelligent Platform Management Bus Header (IPMB_1)

39. TPM Header (TPM1)

40. Clear CMOS Pad (CLRMOS1)

41. Thermal Sensor Header (TR1)

42. M.2 Socket (M2_2) (Type 2260/2280)

43. M.2 Socket (M2_1) (Type 2260/2280/22110)

44. PWM Configuration Header (PWM_CFG1)

45. ATX 12V Power Connector (ATX12V2)

46. ATX 12V Power Connector (ATX12V1)

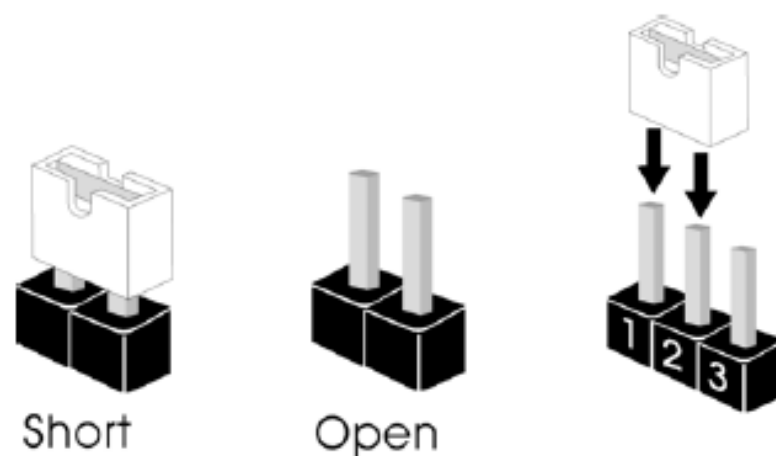
Connectors, Jumpers, and LED Functionality

11.1 Connector Functionality

Item	Connector	Description
3	PSU SMBus (PSU_SMB1)	Power Management Bus
4	ATX Power Connector (ATXPWR1)	24pin ATX Power Connector
19	SATA3 Connector (SATA_1)	SATA Connector
20	USB 3.1 Gen1 Header (USB3_1_2)	USB 3.1 Connector
21	SATA3 Connector (SATA_2)	SATA Connector
22	SATA3 Connector (SATA_3)	SATA Connector
23	SATA3 Connector (SATA_4)	SATA Connector
24	SATA3 Connector (SATA_5)	SATA Connector
27	SATA3 DOM CONNECTOR (SATA_0), RED	SATA Connector
29	System Panel Header (PANEL1)	Front Panel Connector
43	M.2 Socket (M2_1) (Type 2260/2280/22110)	M.2 Drive Connector
45	ATX 12V Power Connector (ATX12V2)	4pin ATX 12V Power Connector
46	ATX 12V Power Connector (ATX12V1)	8pin ATX 12V Power Connector

11.2 Jumper Functionality

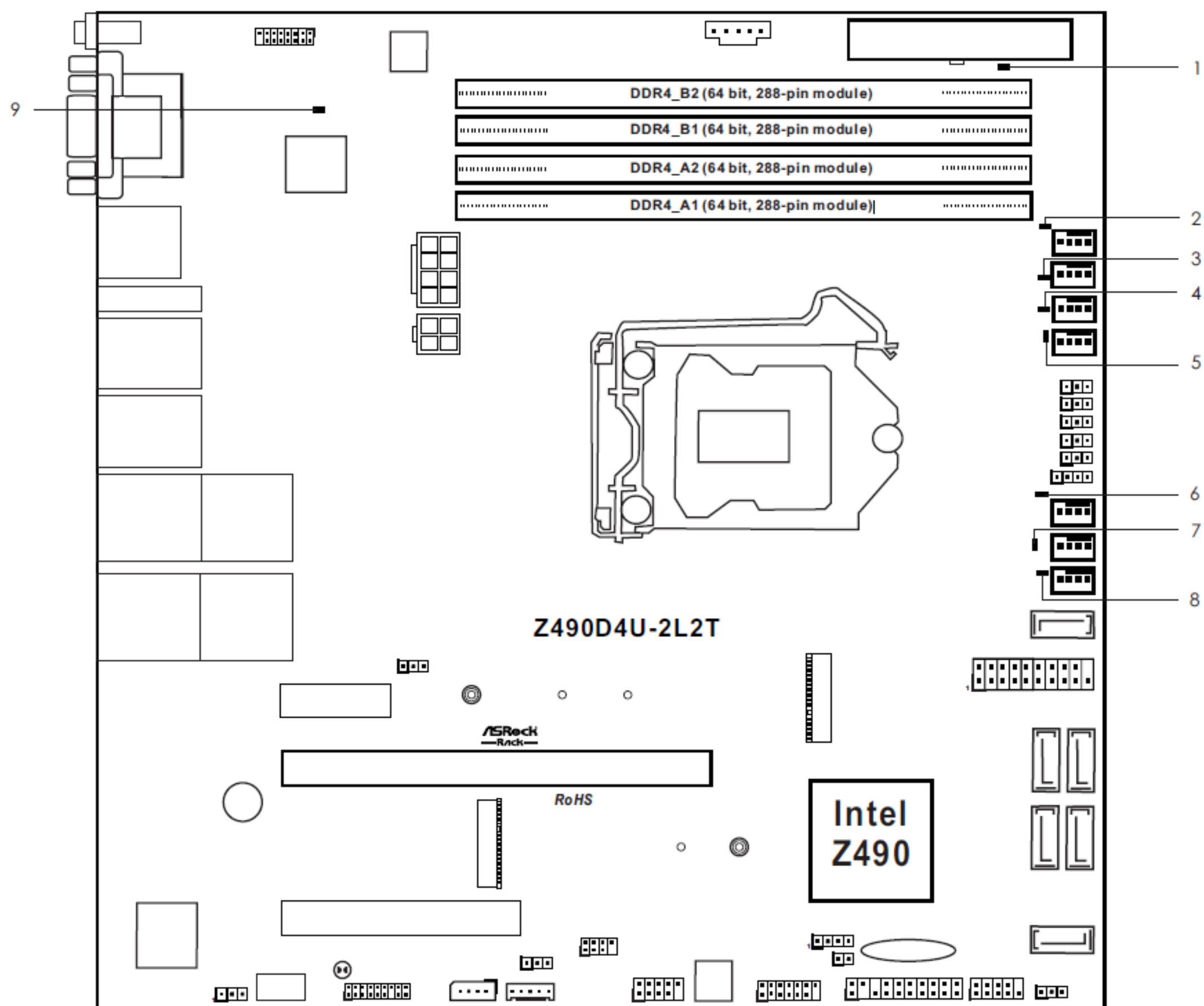
The illustration shows how jumpers are setup. When the jumper cap is placed on the pins, the jumper is “Short”. If no jumper cap is placed on the pins, the jumper is “Open”. The illustration shows a 3-pin jumper whose pin1 and pin2 are “Short” when a jumper cap is placed on these 2 pins.



ME Recovery Jumper (3-pin ME_RECOVERY1) (see p.7)	1_2 	2_3
	Normal Mode (Default)	ME force update
CPU Peci Mode Jumper (3-pin Peci1) (see p.7)	1_2 	2_3
	CPU Peci connected to PCH	CPU Peci connected to BMC (Default)
Security Override Jumper (3-pin SEC_OR1) (see p.7,	1_2 	2_3
	Descriptor Security Override	Not override (Default)

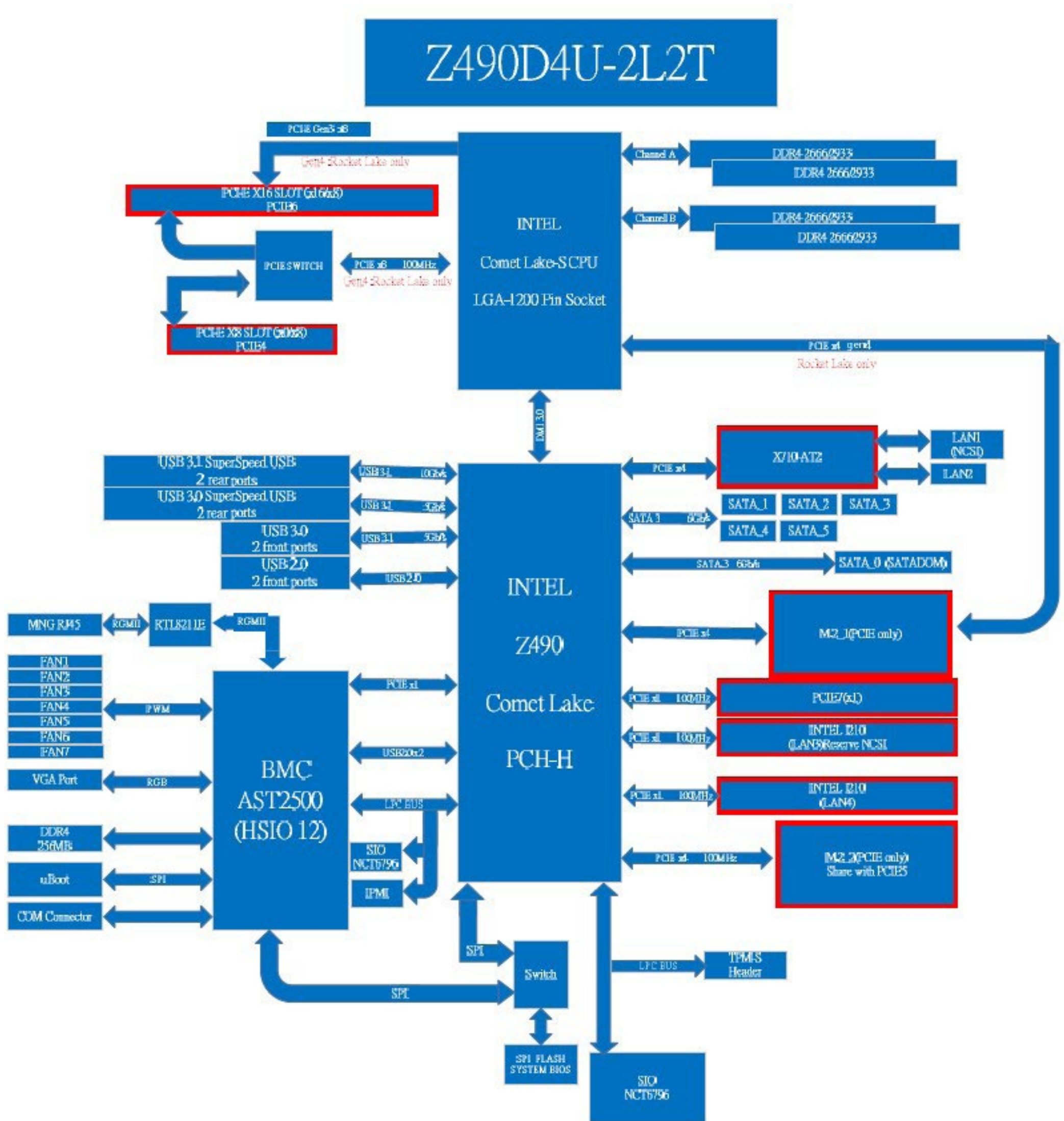
Chassis ID0 Jumper (3-pin CHASSIS_ID0) (see p.7	1_2 	1_2 
Chassis ID1 Jumper (3-pin CHASSIS_ID1) (see p.7,	1_2 	1_2 
Chassis ID2 Jumper (3-pin CHASSIS_ID2) (see p.7,	1_2 	2_3 
	Board Level SKU (Default)	Reserved for system level use
Chassis ID0 Jumper (3-pin CHASSIS_ID0) (see p.7,	1_2 	1_2 
Chassis ID1 Jumper (3-pin CHASSIS_ID1) (see p.7,	2_3 	2_3 
Chassis ID2 Jumper (3-pin CHASSIS_ID2) (see p.7,	2_3 	1_2 
	Reserved for system level use	Reserved for system level use
Chassis ID0 Jumper (3-pin CHASSIS_ID0) (see p.7,	2_3 	2_3 
Chassis ID1 Jumper (3-pin CHASSIS_ID1) (see p.7,	1_2 	1_2 
Chassis ID2 Jumper (3-pin CHASSIS_ID2) (see p.7,	1_2 	2_3 
	Reserved for system level use	Reserved for system level use

11.3 LED Functionality



No.	Item	Status	Description
1	SB_PWR1	Green	STB PWR ready
2	FAN1_LED1	Amber	FAN1 failed
3	FAN2_LED1	Amber	FAN2 failed
4	FAN3_LED2	Amber	FAN3 failed
5	FAN4_LED4	Amber	FAN4 failed
6	FAN5_LED2	Amber	FAN5 failed
7	FAN6_LED1	Amber	FAN6 failed
8	FAN7_LED3	Amber	FAN7 failed
9	BMC_LED1	Green	BMC heartbeat LED

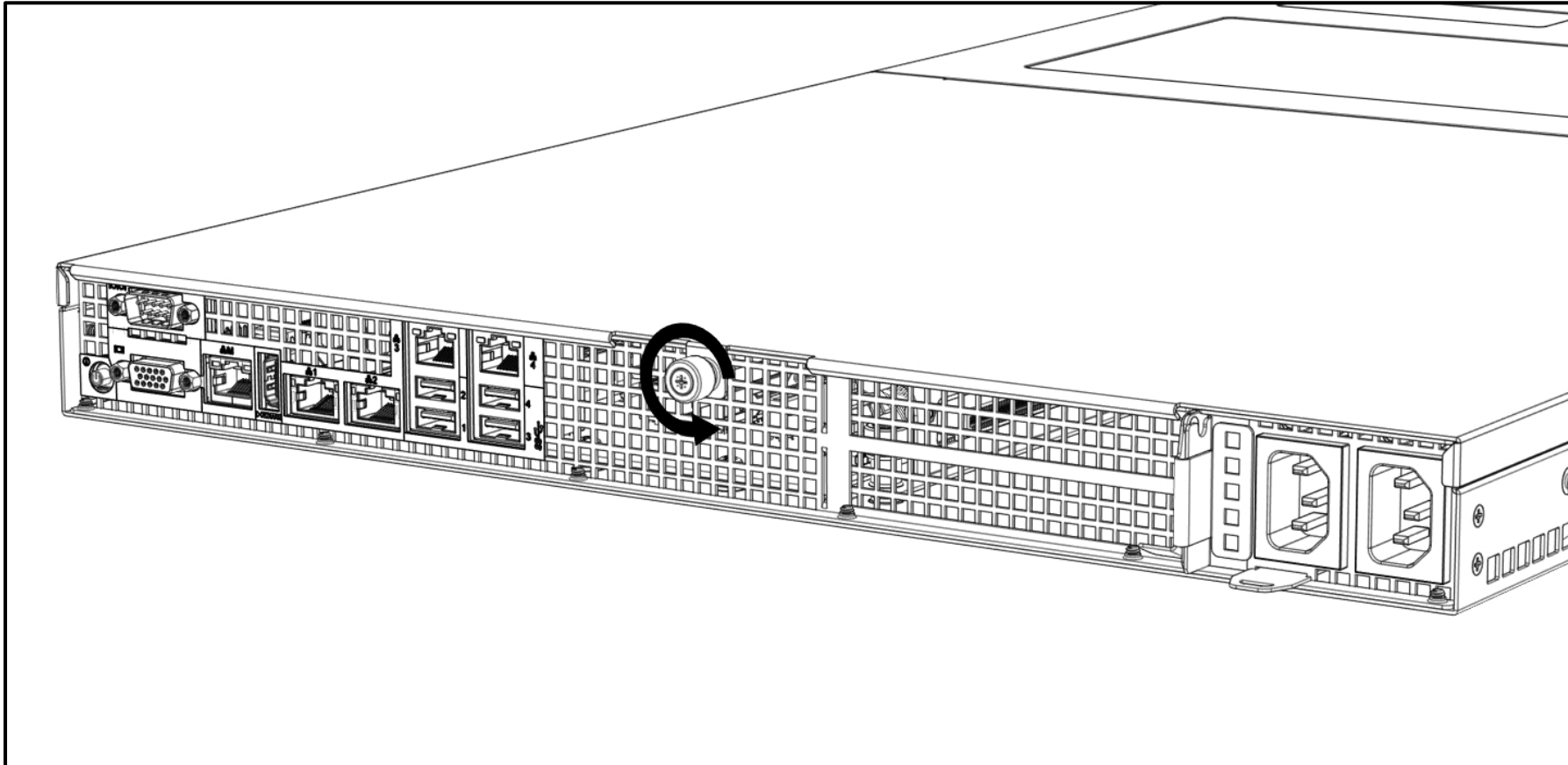
11.4 Block Diagram



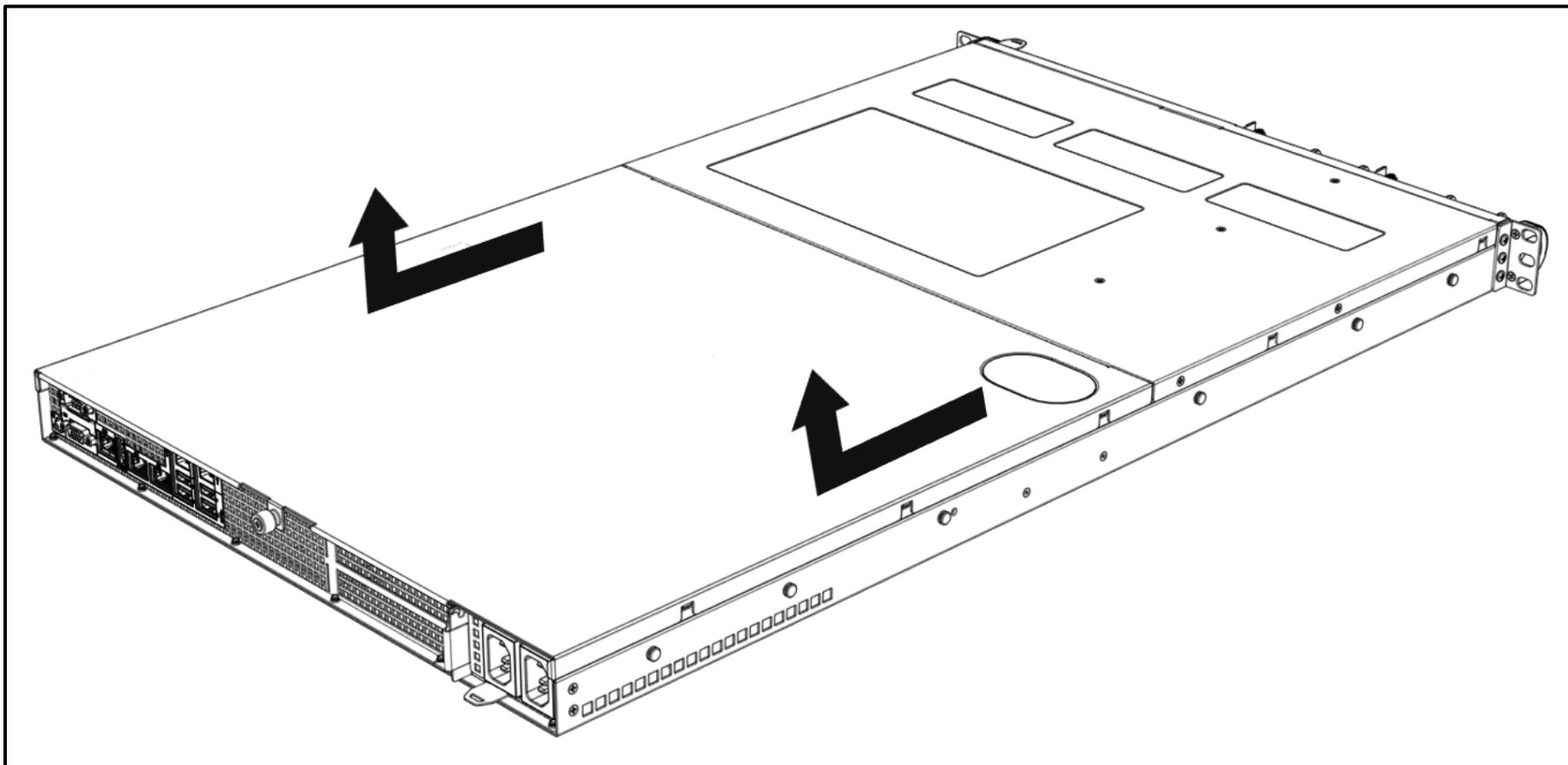
12. Removing the Chassis Cover

This section contains information on how to remove the chassis cover from the system.

Step 1: Turn the Knob anti-clockwise by using Philips screwdriver type 2.



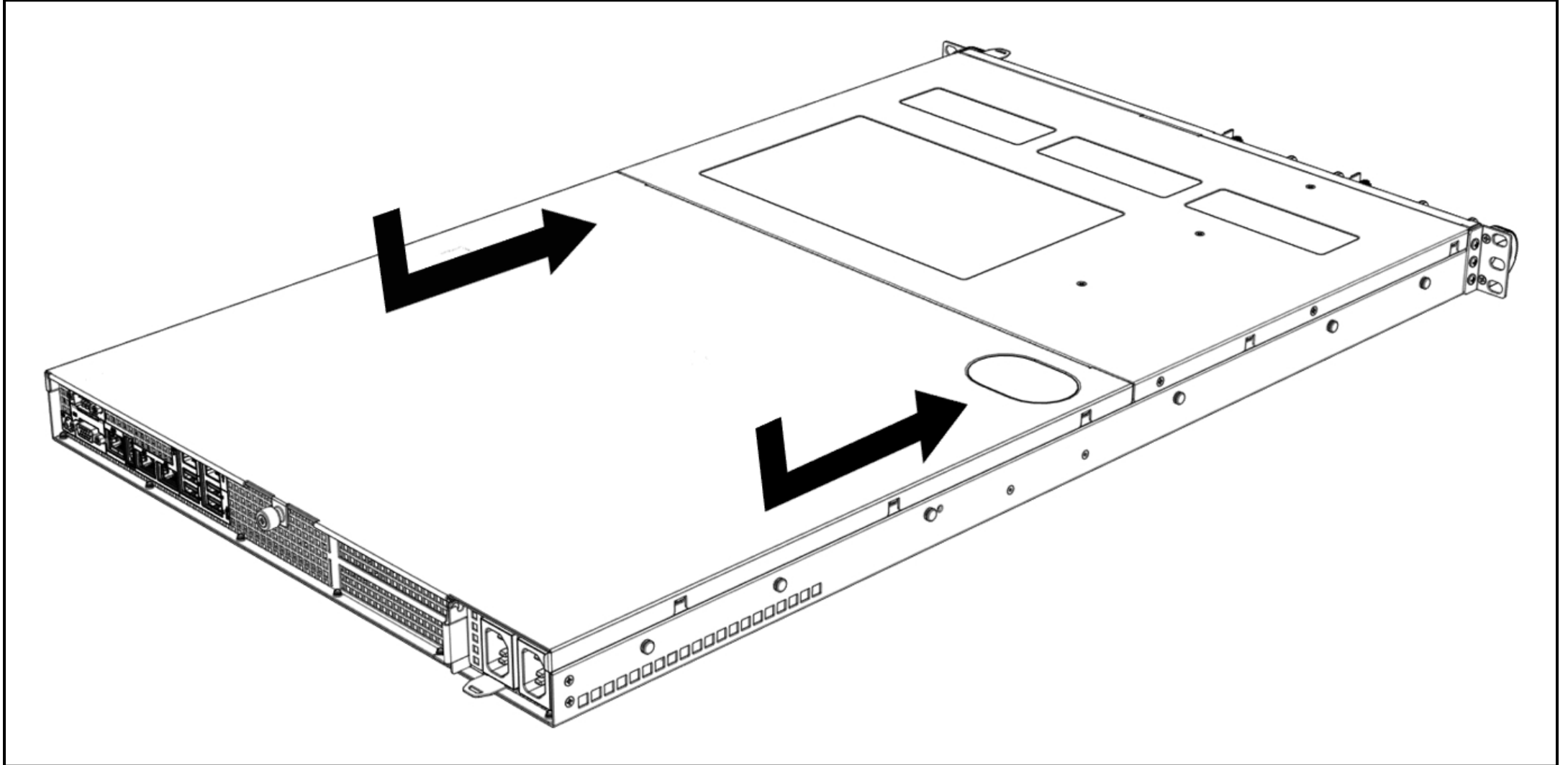
Step 2: Slide the Rear Top Cover towards the back of the system to release the cover.



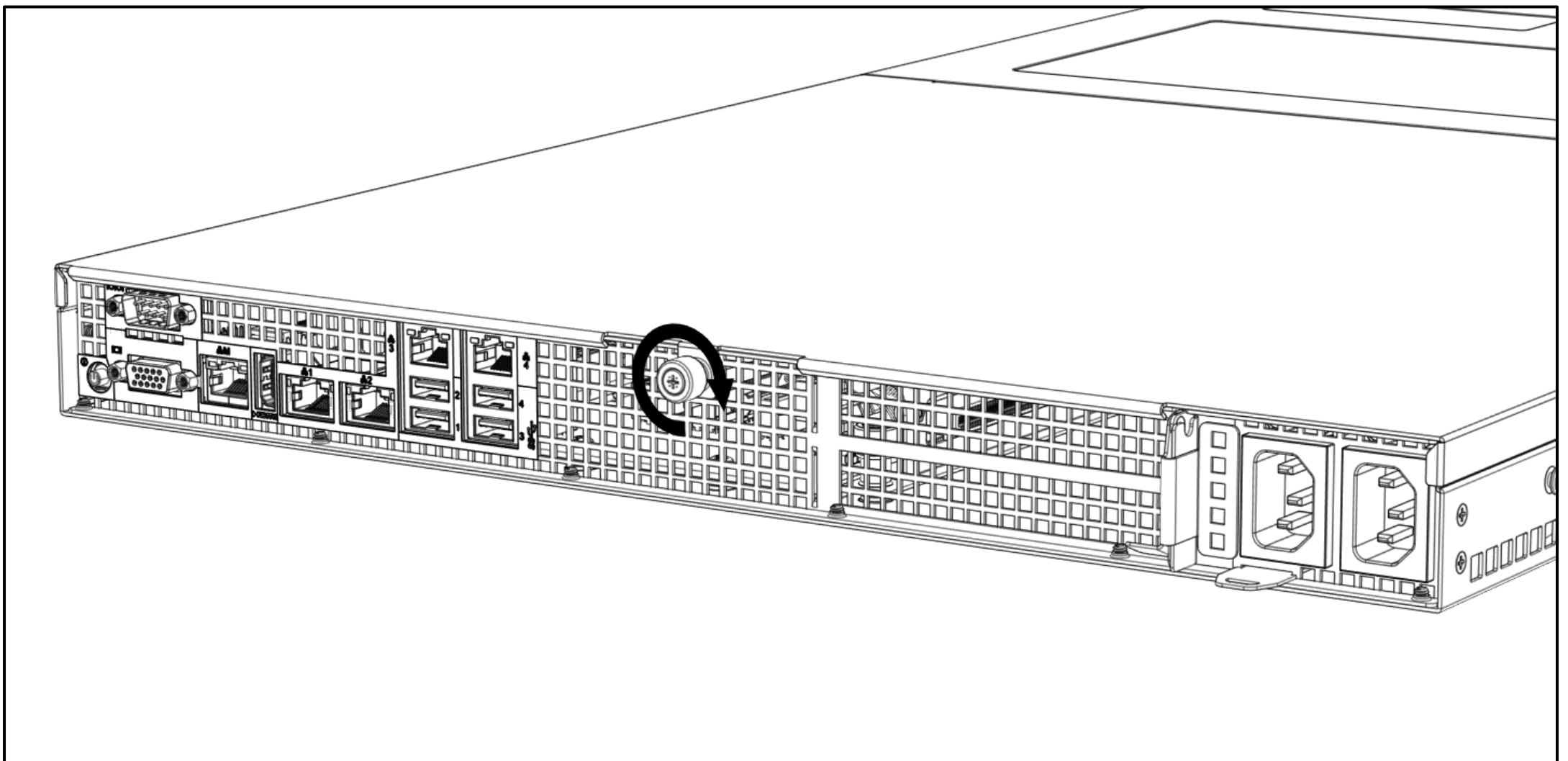
13. Installing the Chassis Cover

This section contains information on how to install the Chassis cover in the system.

Step 1: Slide the cover towards the front of the system to close the cover.



Step 2: Turn the Knob clockwise by using Philips screwdriver type 2.



14. How to clear the CMOS with battery and pad

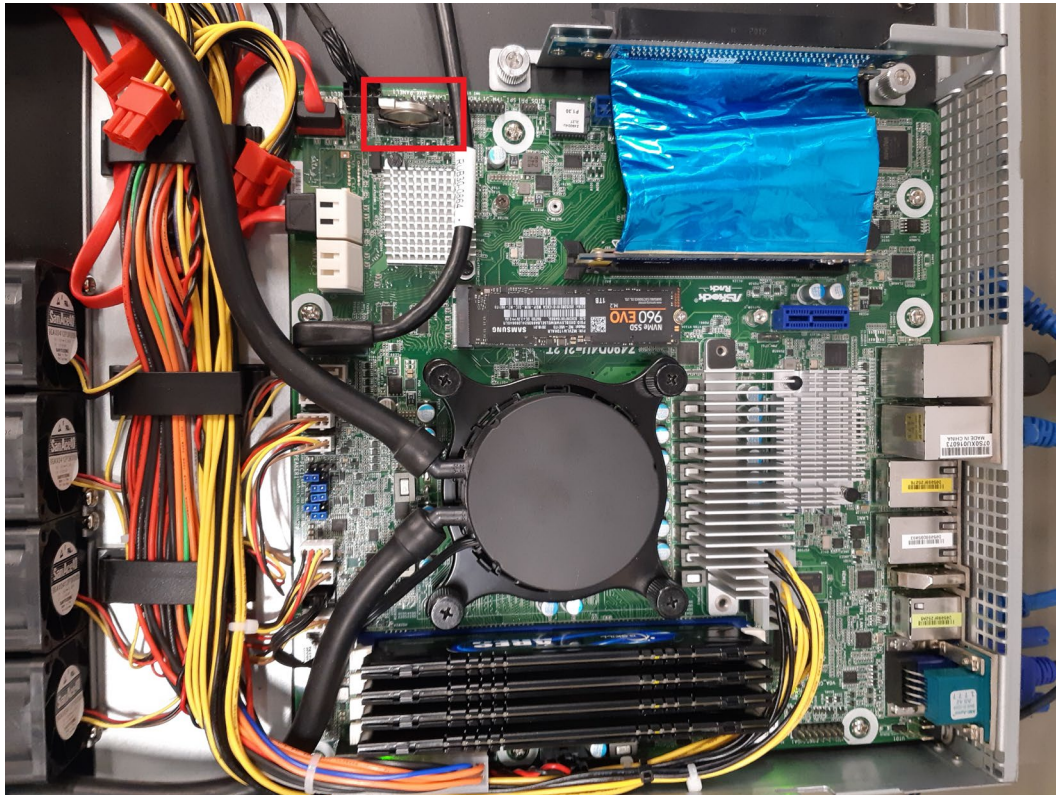
This section contains information on how to clear the CMOS by and battery and CMOS Pad.

14.1 Clear CMOS by Battery

Step 1: Power system off.

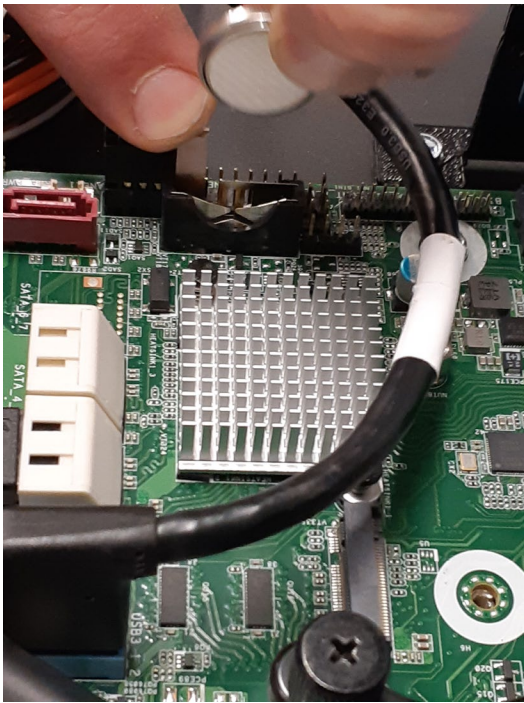
Step 2: Unplugged power cable from system.

Step 3: Take off the chassis top cover and then locate the CMOS battery on the motherboard.

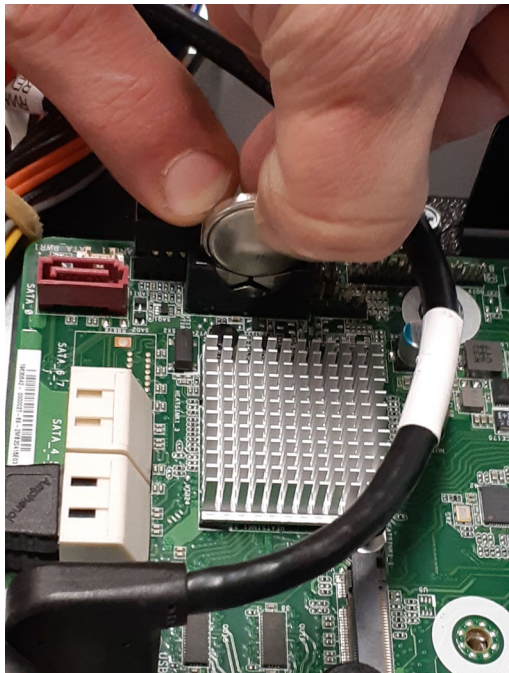


Step 4: Press the lock on the left side in order to CMOS battery to come up. Gently pull off the battery from the motherboard and Wait for 5-10 seconds.





Step 5: Press the lock on the left side and place the CMOS battery again gently.



Step 6: Cover up the Chassis top cover and then Plug the power cable back in.

Step 7: Turn system ON

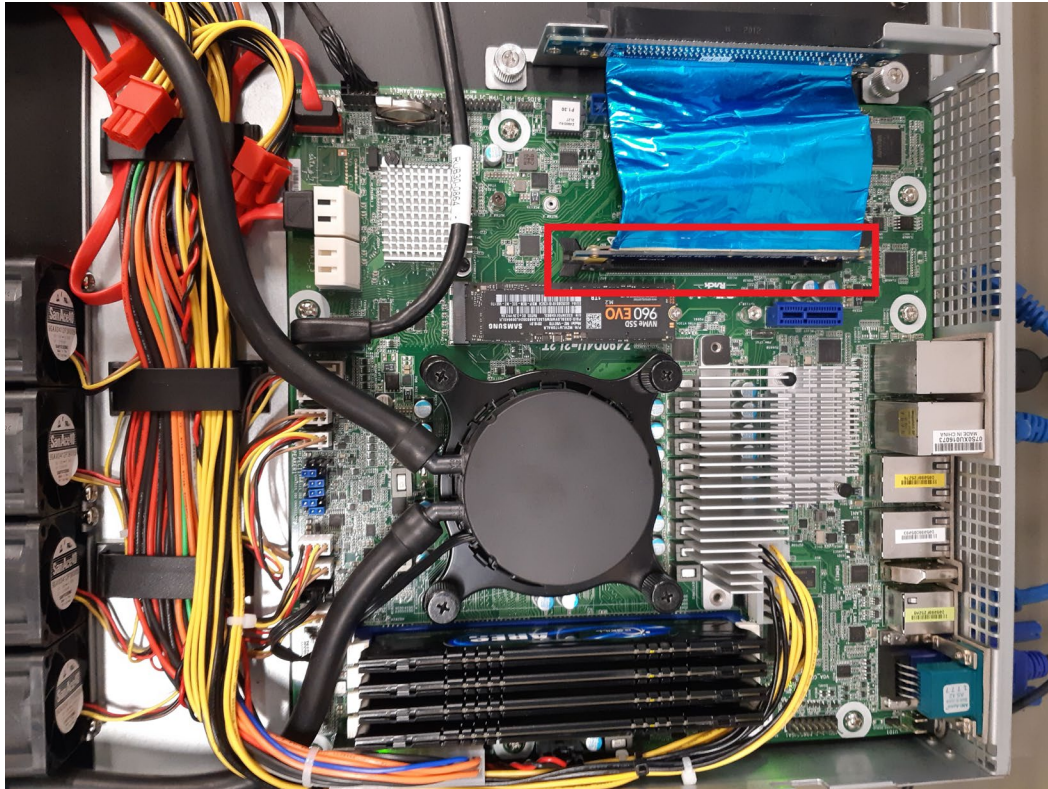
Step 8: Allow system to go through a complete power cycle in order to initialize all components.

14.2 Clear CMOS by CMOS Pad

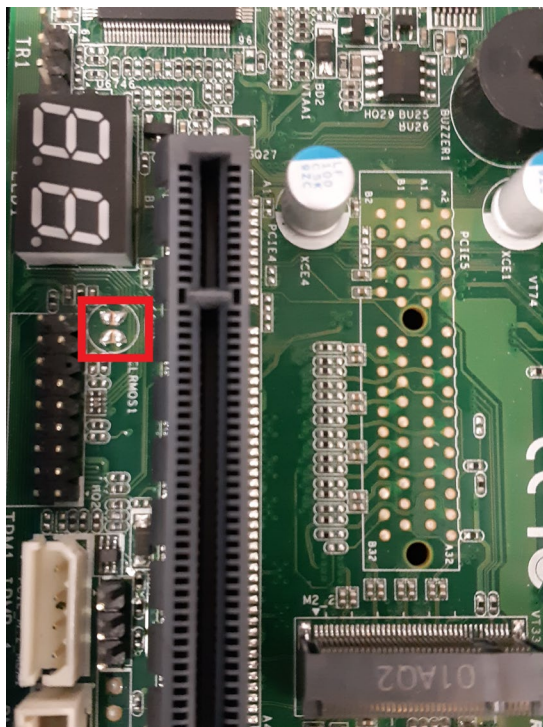
Step 1: Power system off.

Step 2: Take off the chassis cover.

Step 3: Remove the both PCI-e riser extender from the PCI-e connector on the motherboard.



Step 4: Locate the clear CMOS Pad. (Squared in red).



Step 5: Use a flathead screwdriver or other piece of metal to short the two halves together for 30 seconds.

Step 6: After insert the both of the PCI-e riser extender to the PCI-e connector on the motherboard.

Step 7: Power on the system.

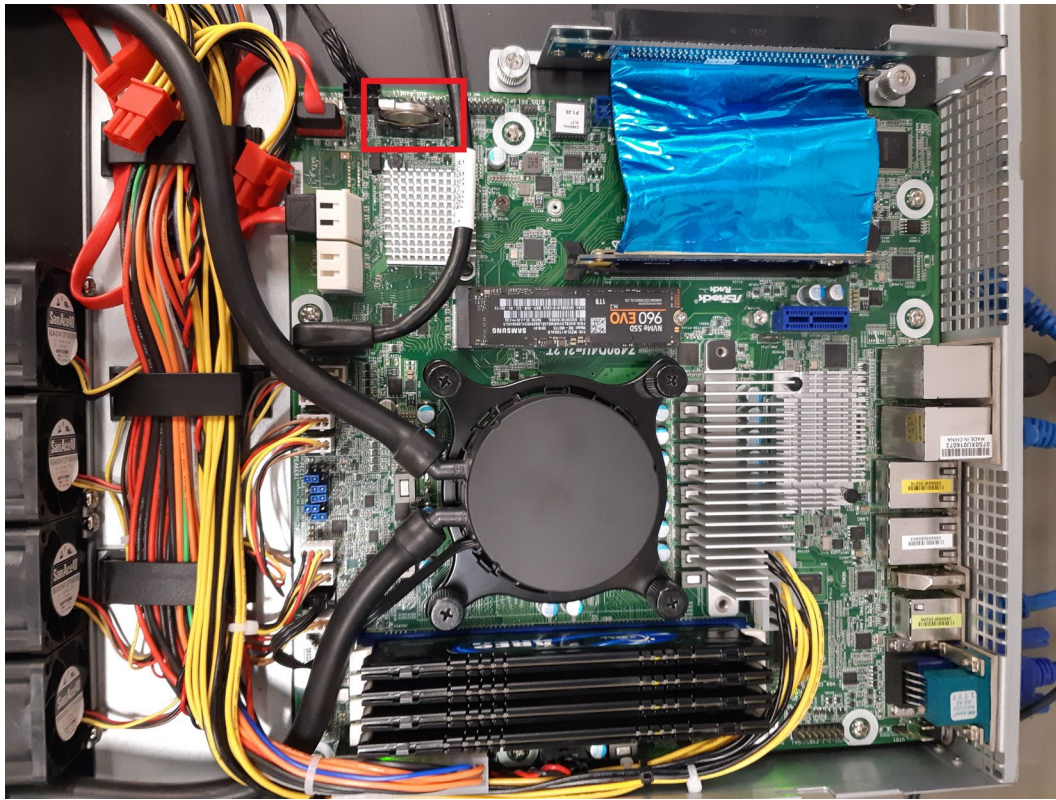
15. How to replace the CMOS battery:

This section contains information on how to replace the CMOS battery in the system.

Step 1: Power system off.

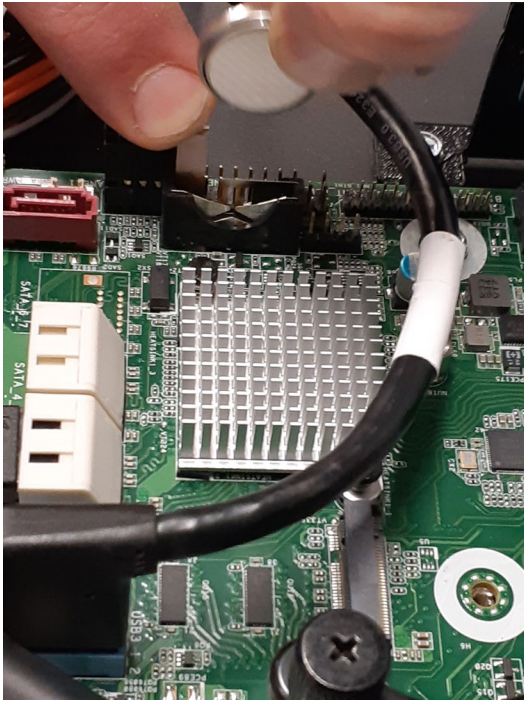
Step 2: Unplugged power cable from system.

Step 3: Take off the chassis top cover and then locate the CMOS battery on the motherboard.

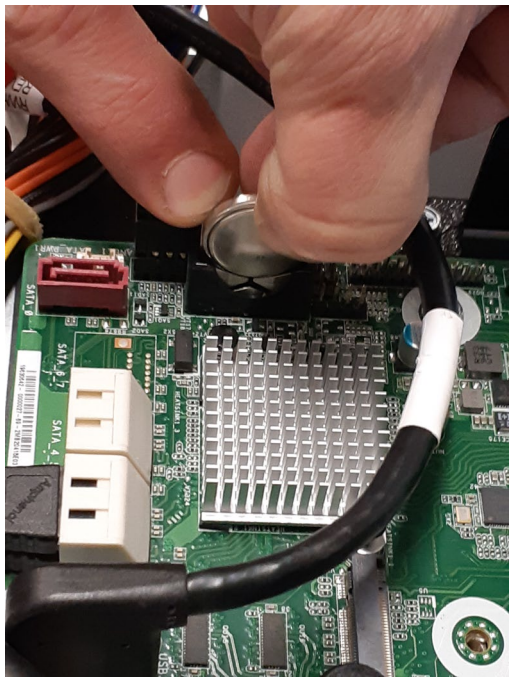


Step 4: Press the lock on the left side in order to CMOS battery to come up. Gently pull off the battery from the motherboard and Wait for 5-10 seconds.





Step 5: Press the lock on the left side and replace the new CMOS battery gently.



Step 6: Cover up the Chassis top cover and then Plug the power cable back in.

Step 7: Turn system ON

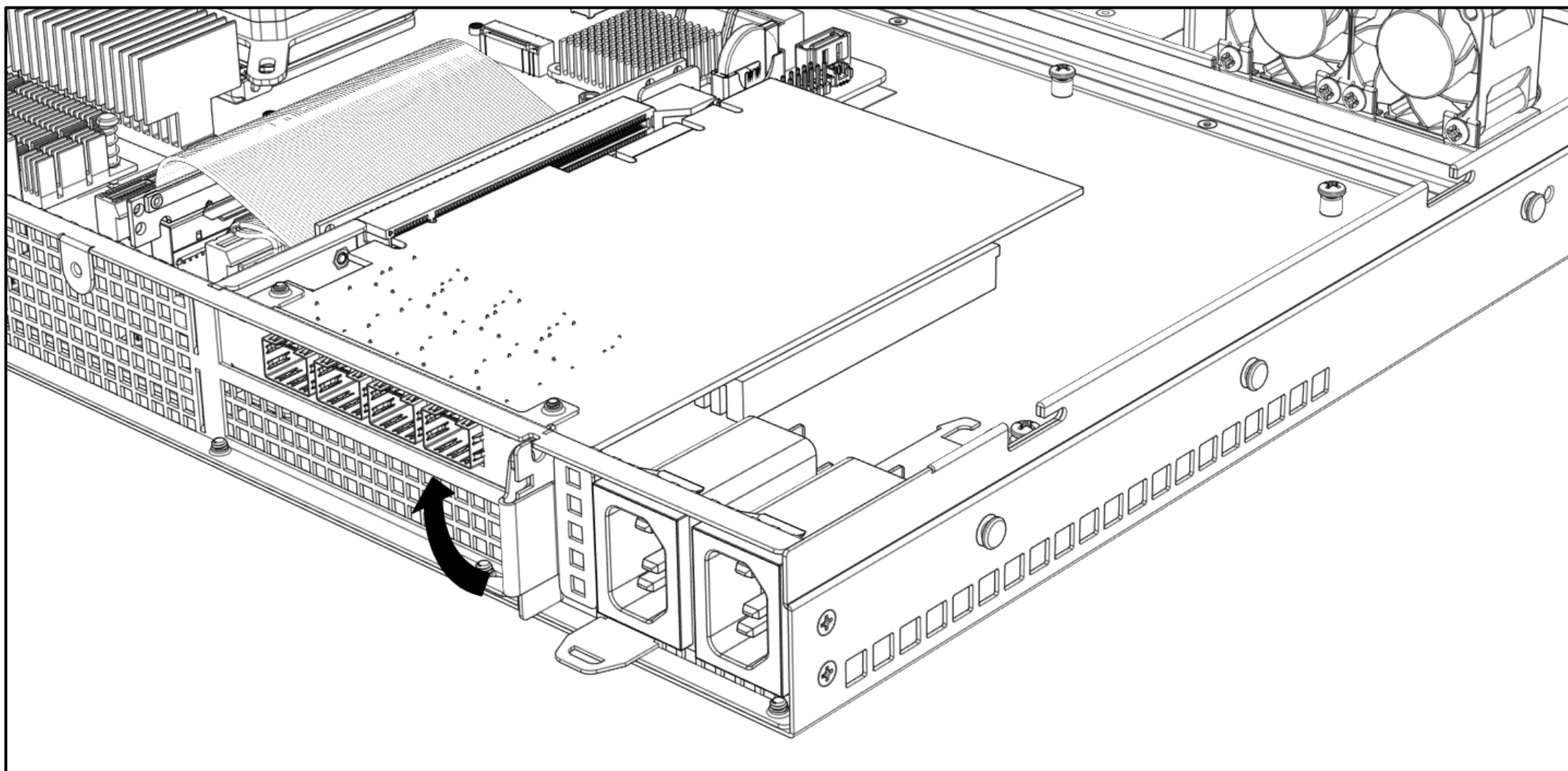
Step 8: Allow system to go through a complete power cycle in order to initialize all components.

16. Replacing PCIe Card

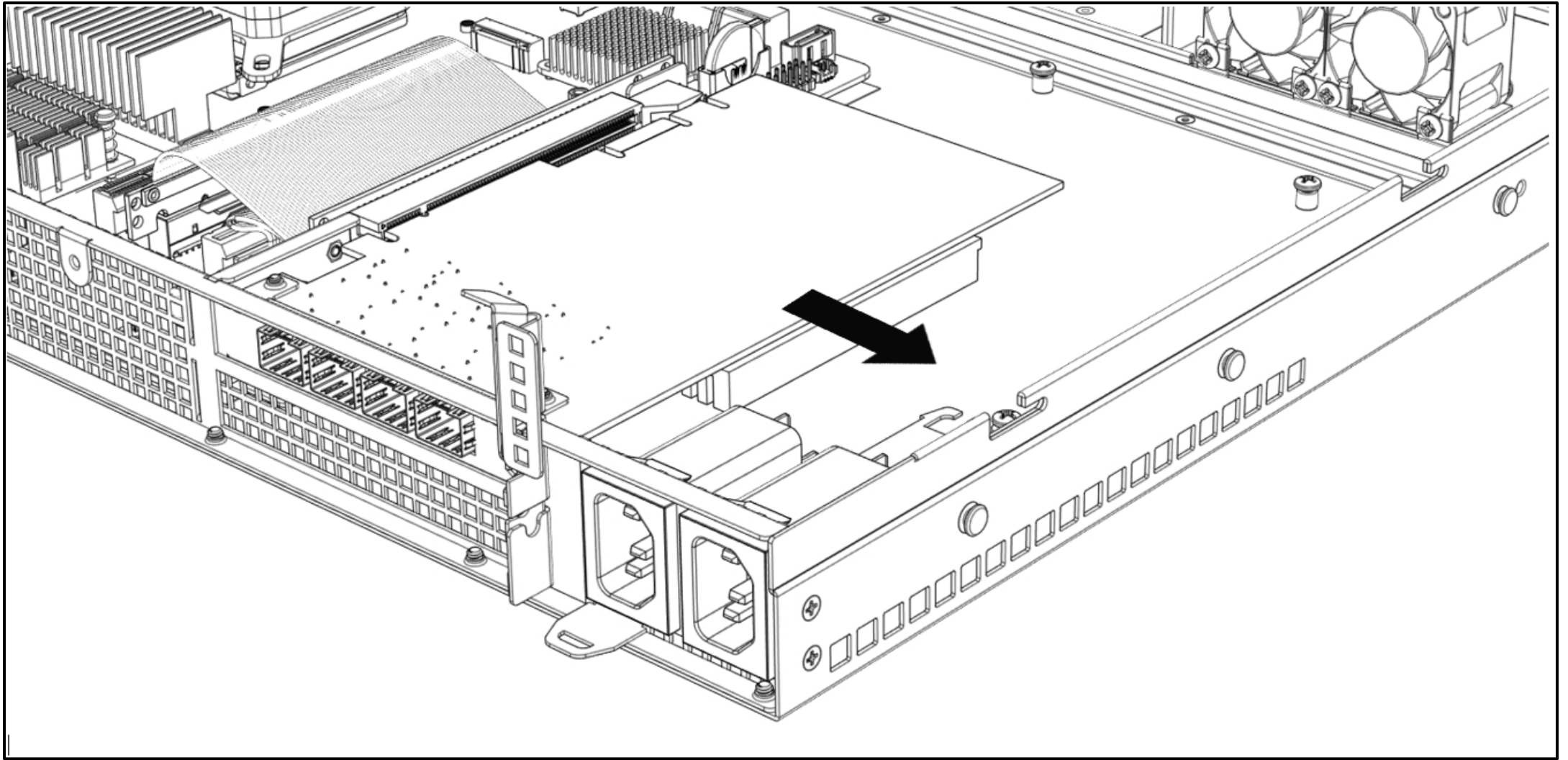
This section contains information on how to replace the PCIe card 1 and 2.

16.1 Replacing PCIe Card 1

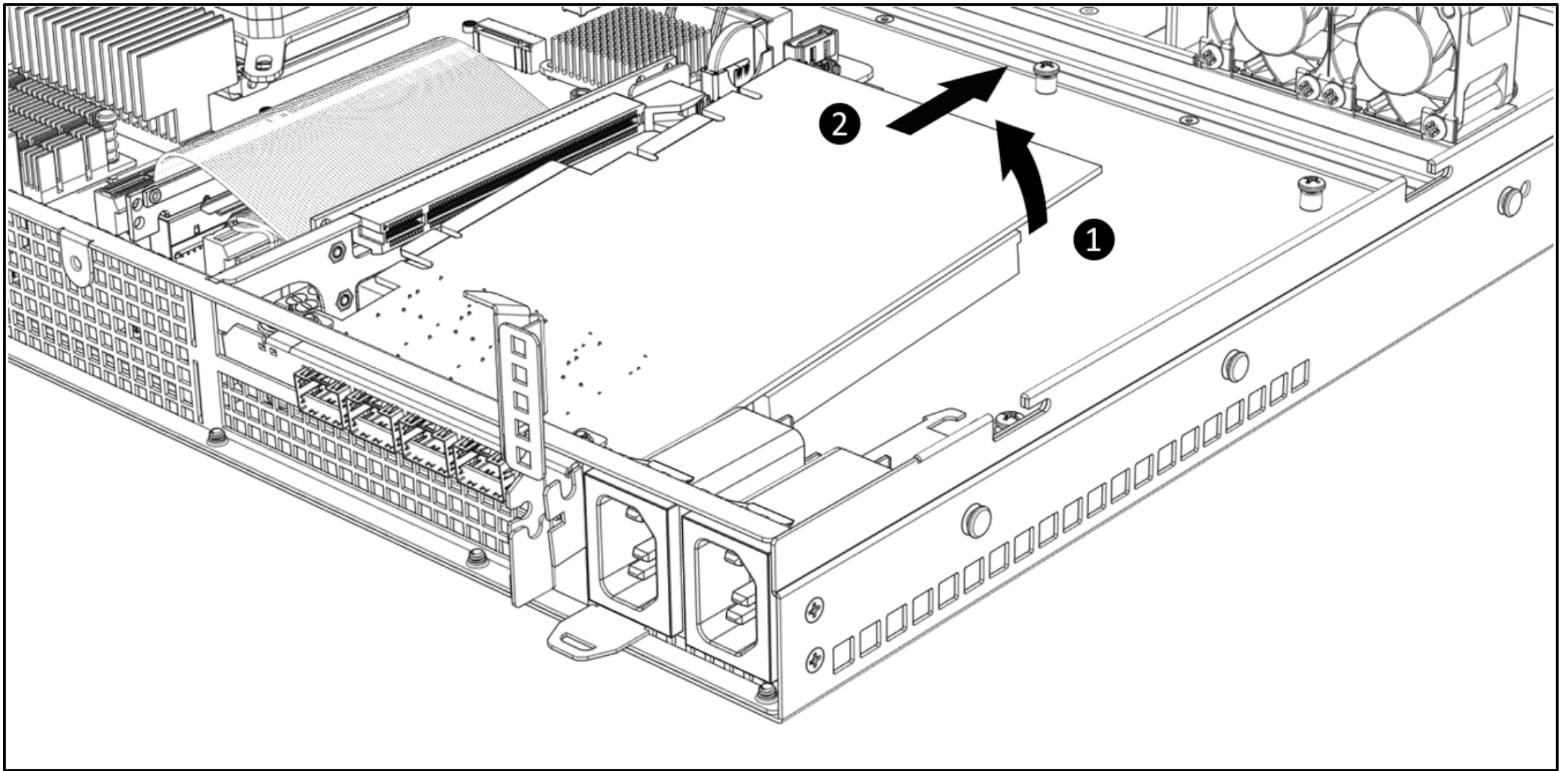
Step 1: Pull the tab of the PCIe release latch and rotate to the top.



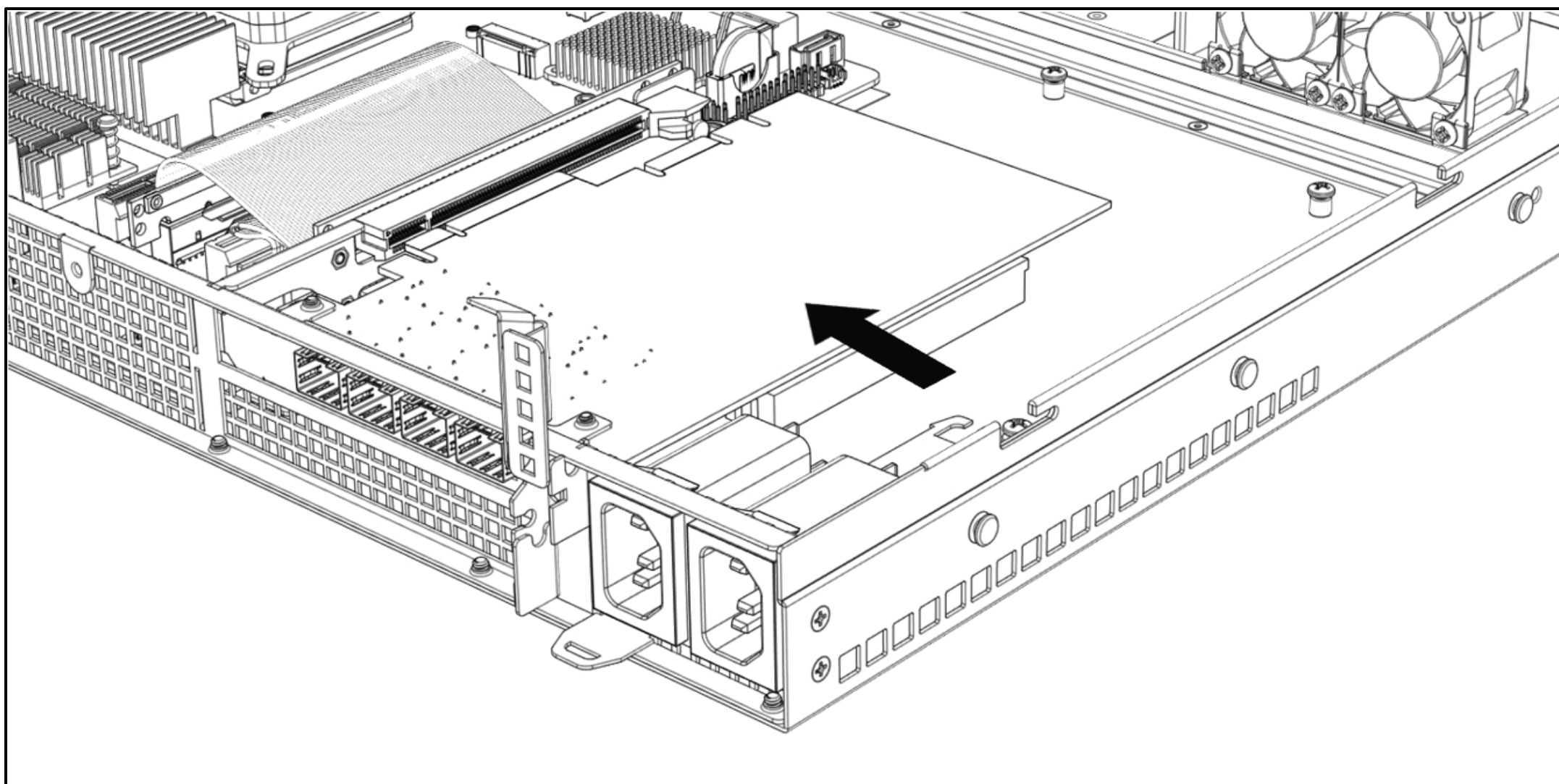
Step 2: Pull the PCIe card out of the slot.



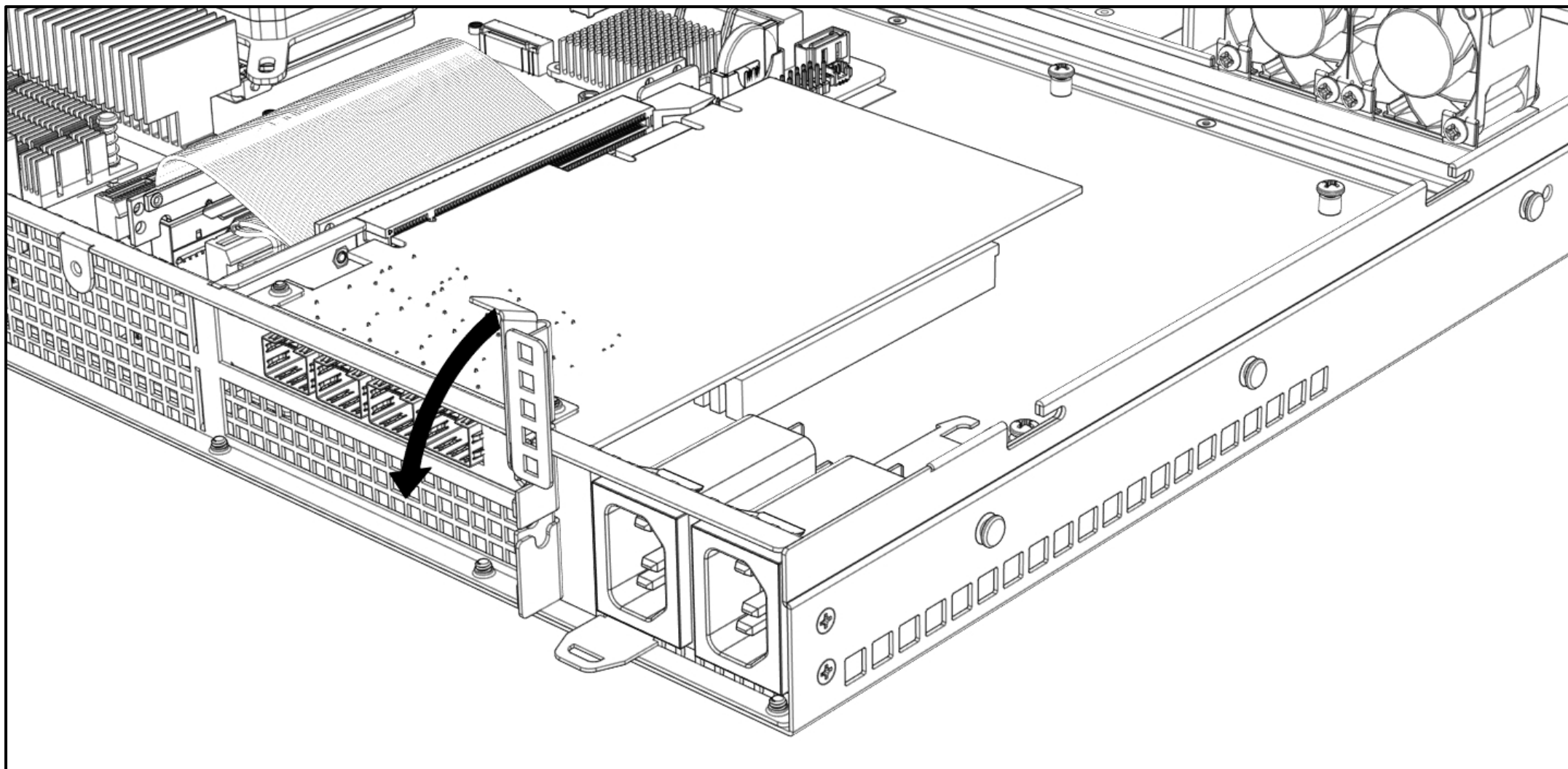
Step 3: Twist the card and remove from chassis.



Step 4: Put another PCIe card in and install into the slot.



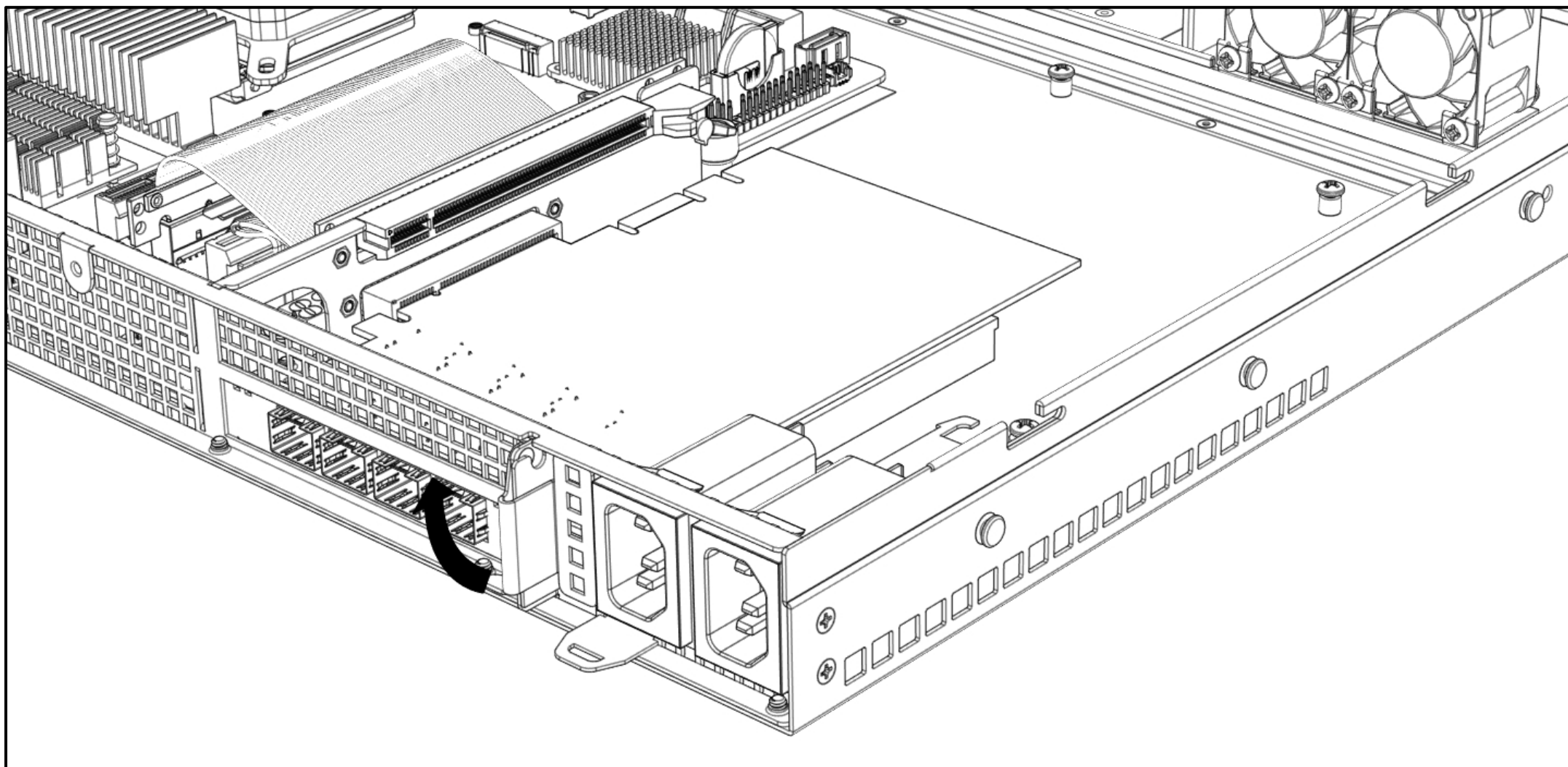
Step 5: Rotate and close the PCIe release latch.



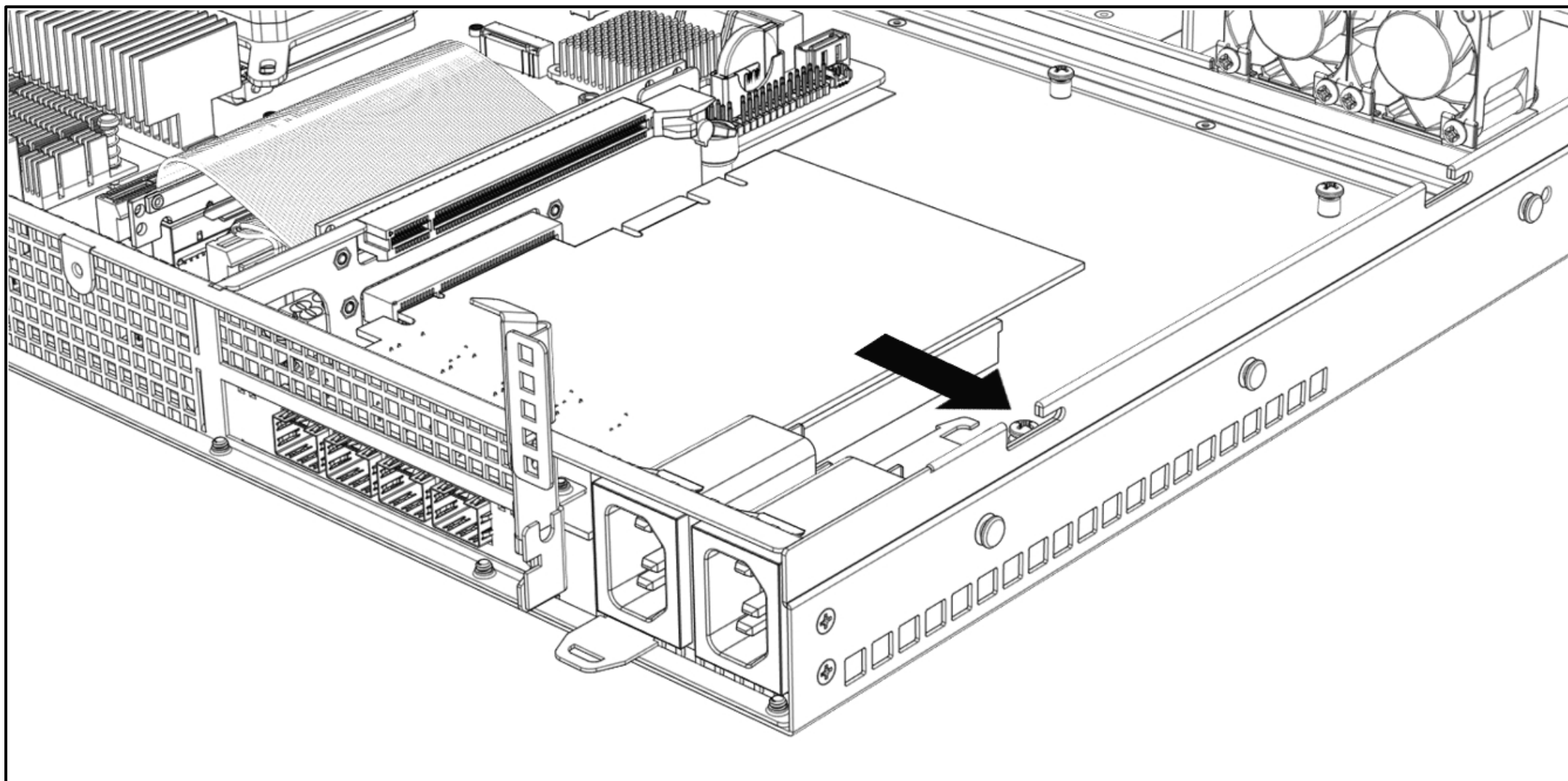
16.2 Replacing PCIe 2 Card

This section contains information on how to replace the PCIe 2 card.

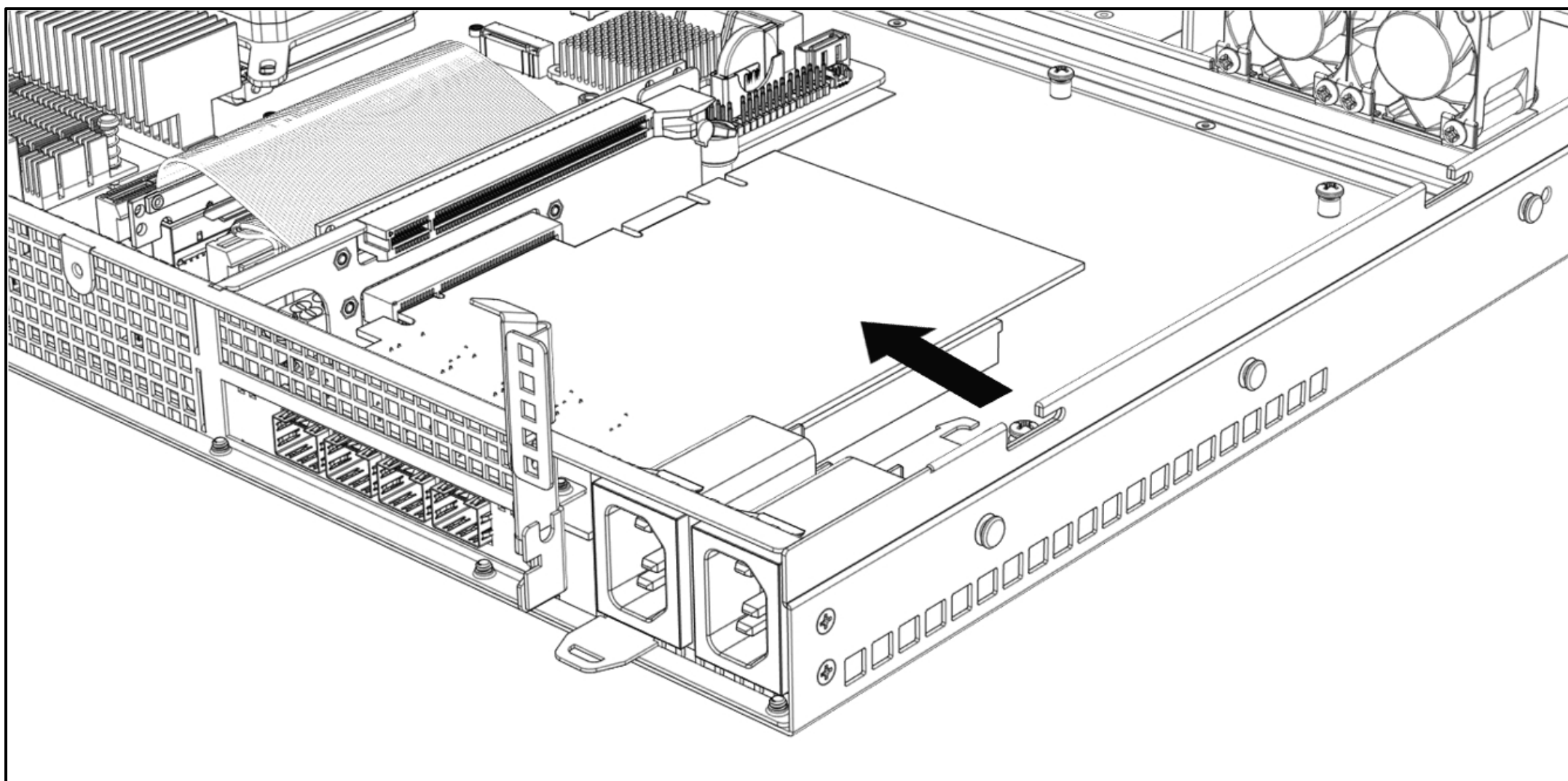
Step 1: Pull the tab of the PCIe release latch and rotate to the top.



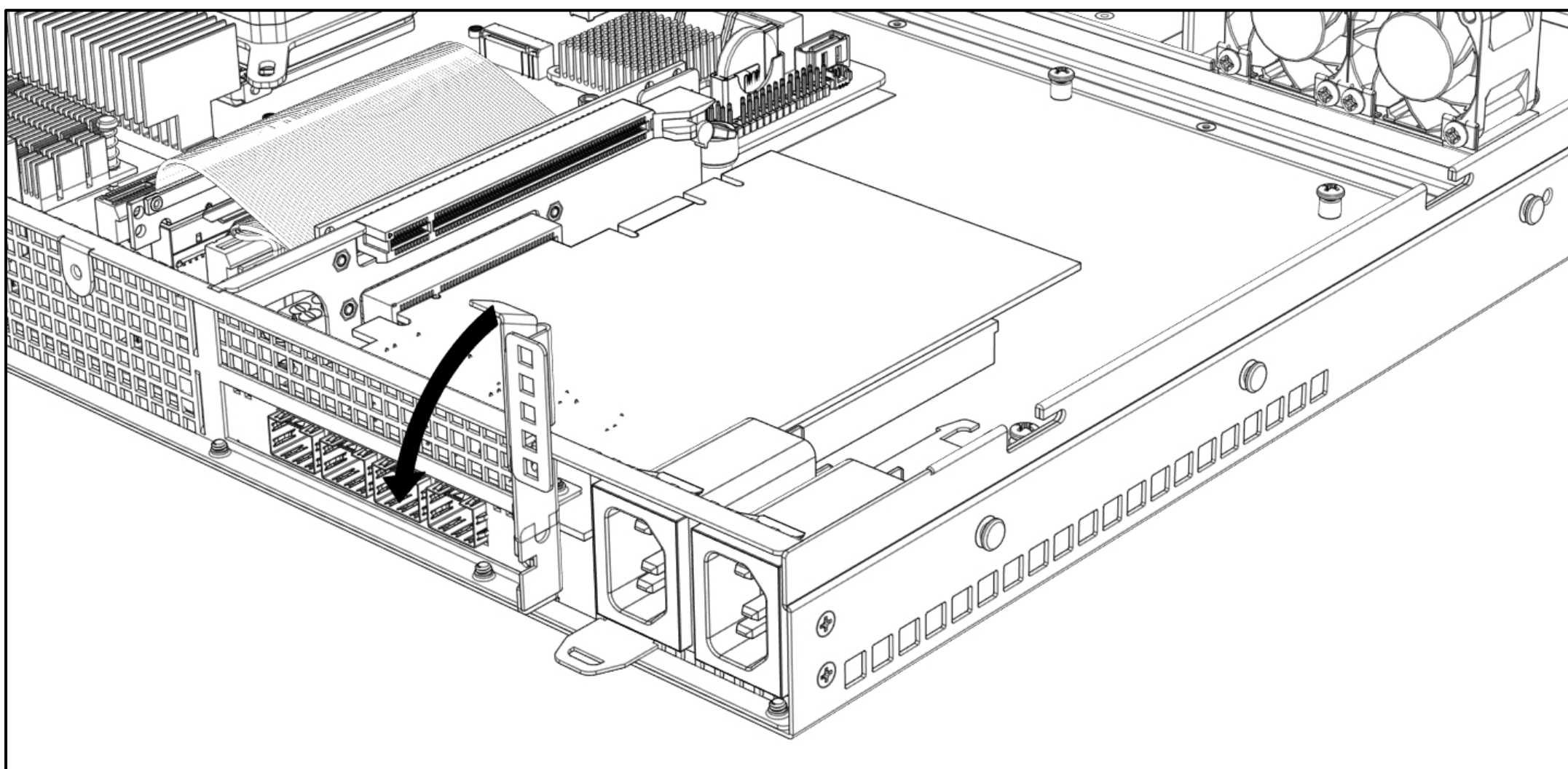
Step 2: Pull the PCIe card out of the slot and remove it.



Step 3: Put another PCIe card in and install into the slot.



Step 4: Rotate and close the PCIe release latch.



17. Removing and Installing Memory Modules

This section contains information on how to remove and install the Memory Modules.

This motherboard provides four 288-pin DDR4 (Double Data Rate 4) DIMM slots, and supports Dual Channel Memory Technology.

DIMM Size Per DIMM:

Non-ECC UDIMM : 32GB, 16GB, 8GB, 4GB

Dual Channel Memory Configuration

Priority	DDR4_A1	DDR4_A2	DDR4_B1	DDR4_B2
1		Populated		Populated
2	Populated		Populated	
3	Populated	Populated	Populated	Populated

 **Caution:** Handle each memory module only by the memory cards edges, ensuring not touching the middle of memory module or metallic contacts.

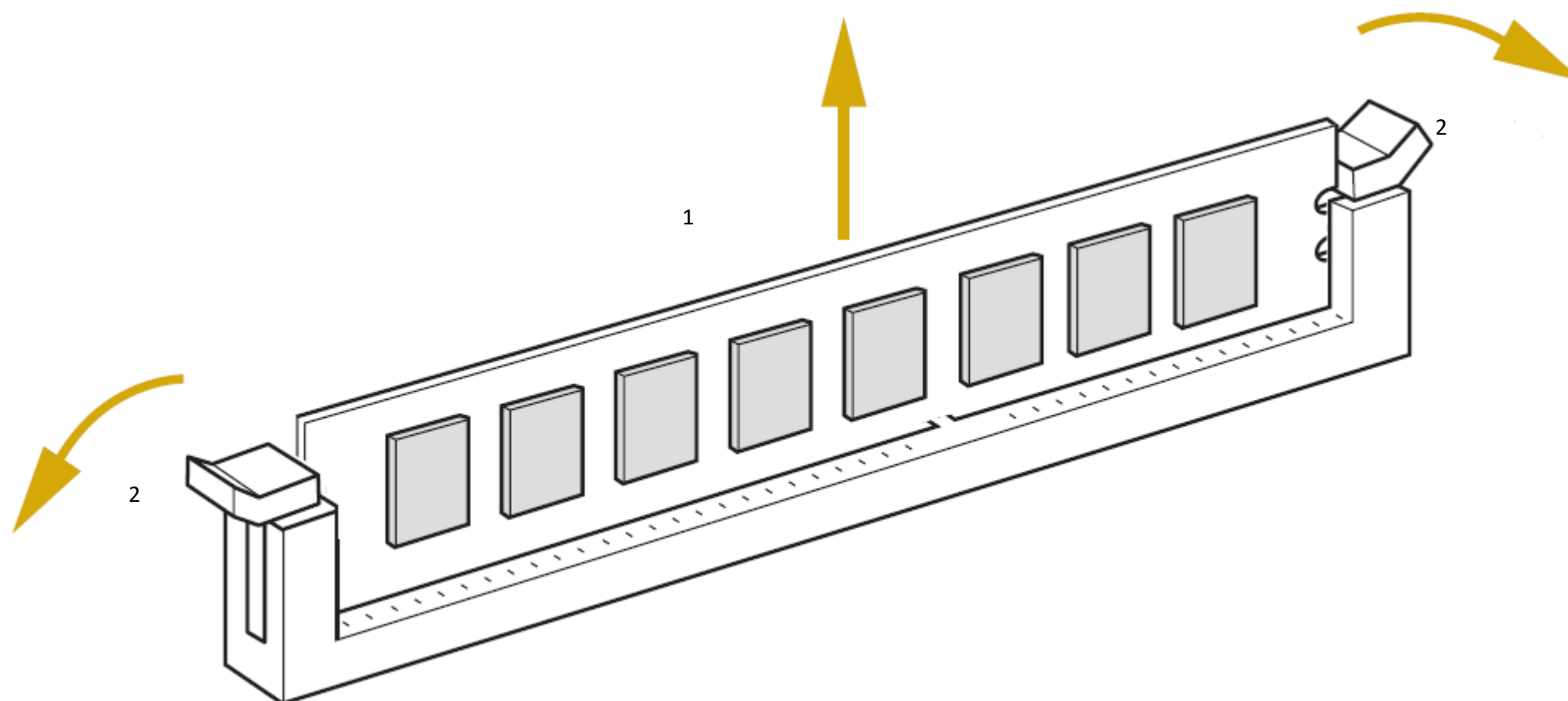
17.1 Removing Memory Module

Step 1: Identify the memory module socket.

Step 2: Press the Memory Module Ejectors (2) on both ends of the memory module socket as show below.

Step 3: Lift the memory module (1) from the memory socket.

- 1. Memory Module
- 2. Memory Module Ejector

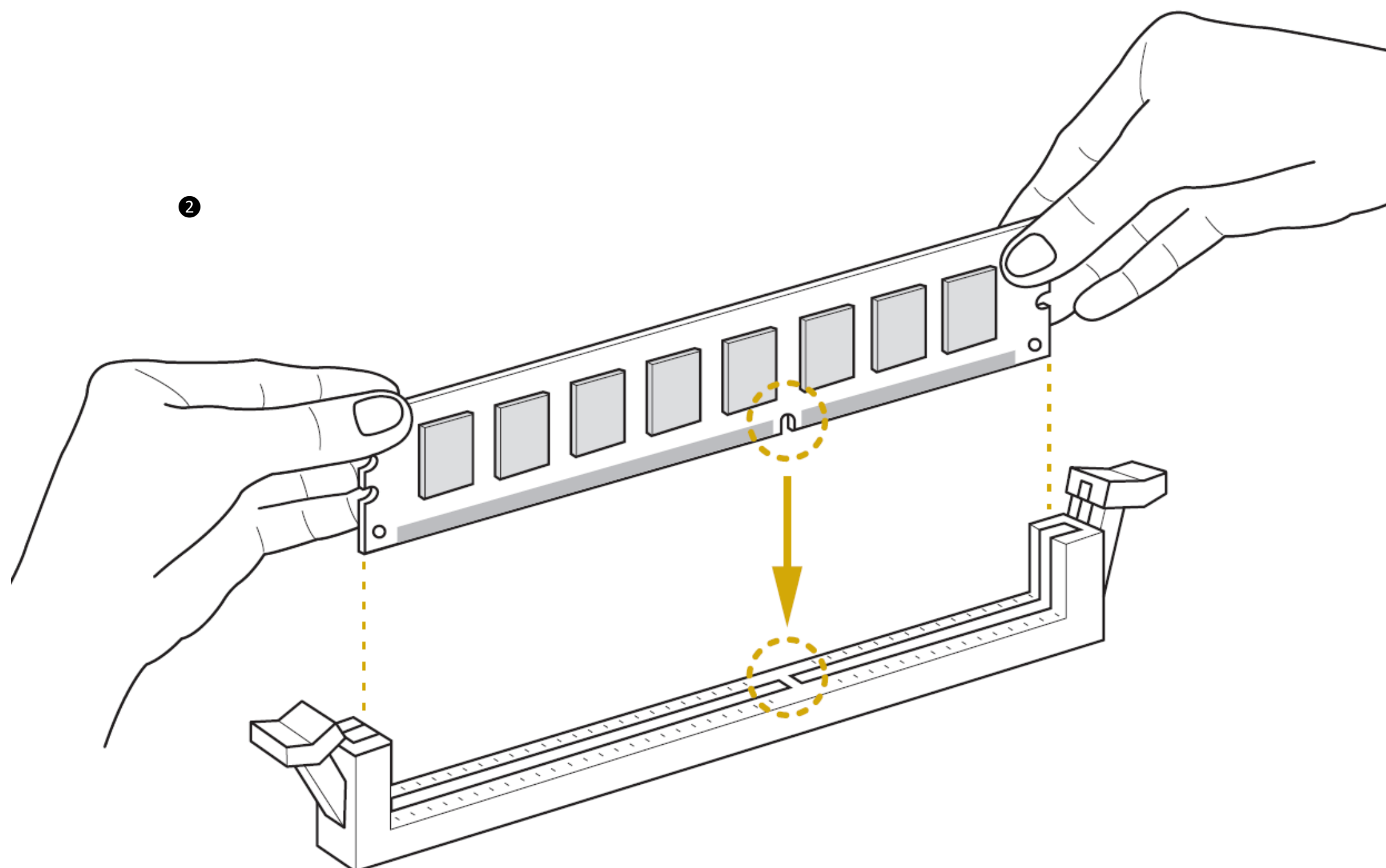
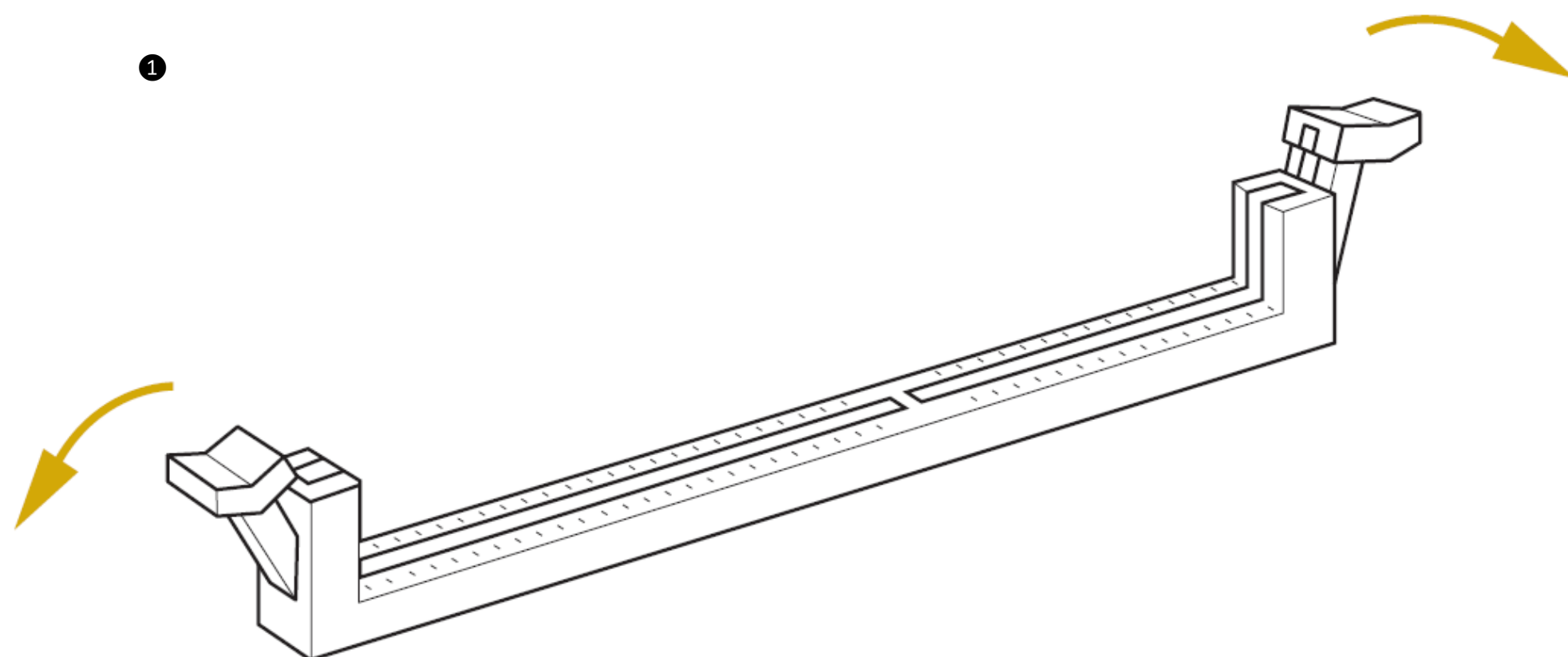


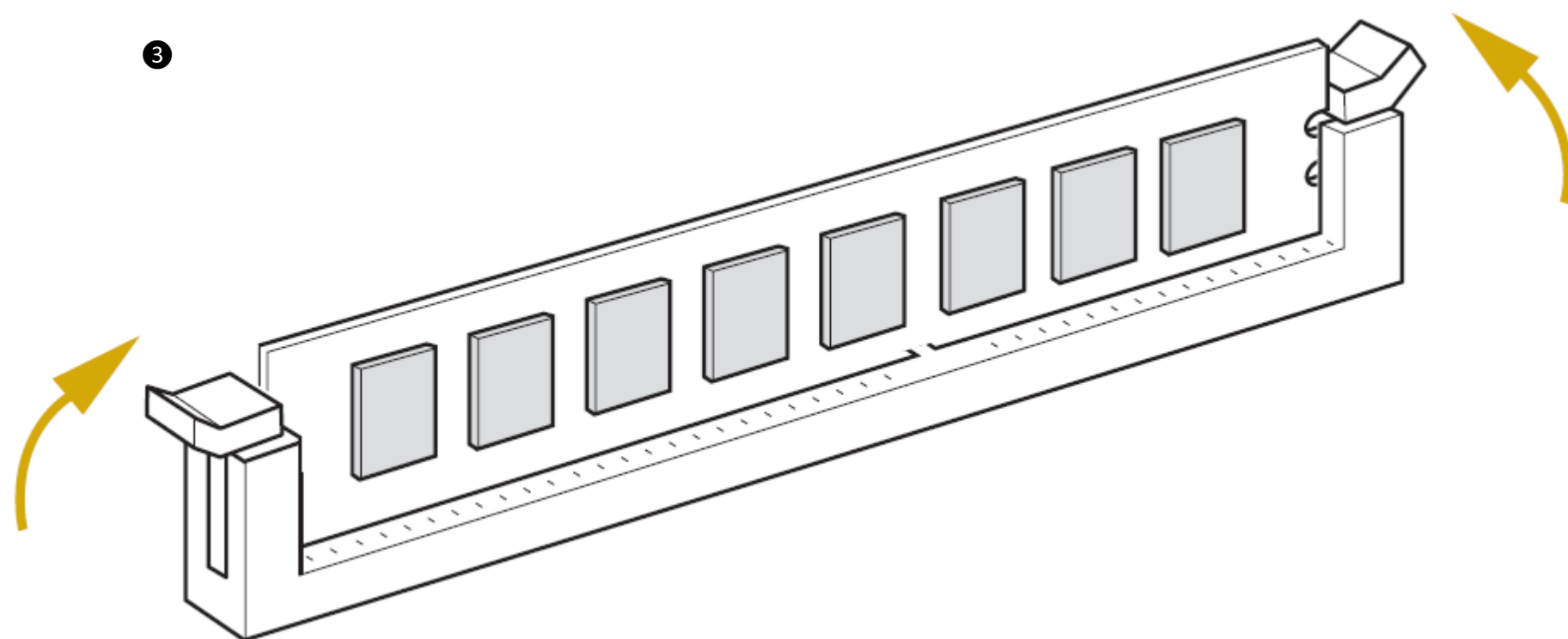
17.2 Installing Memory Module

Step 1: Identify the memory module socket.

Step 2: Make sure that the Memory Module Ejectors on both ends are released.

Step 3: Vertically press the memory module with your thumbs until the memory sits firmly in the memory socket.

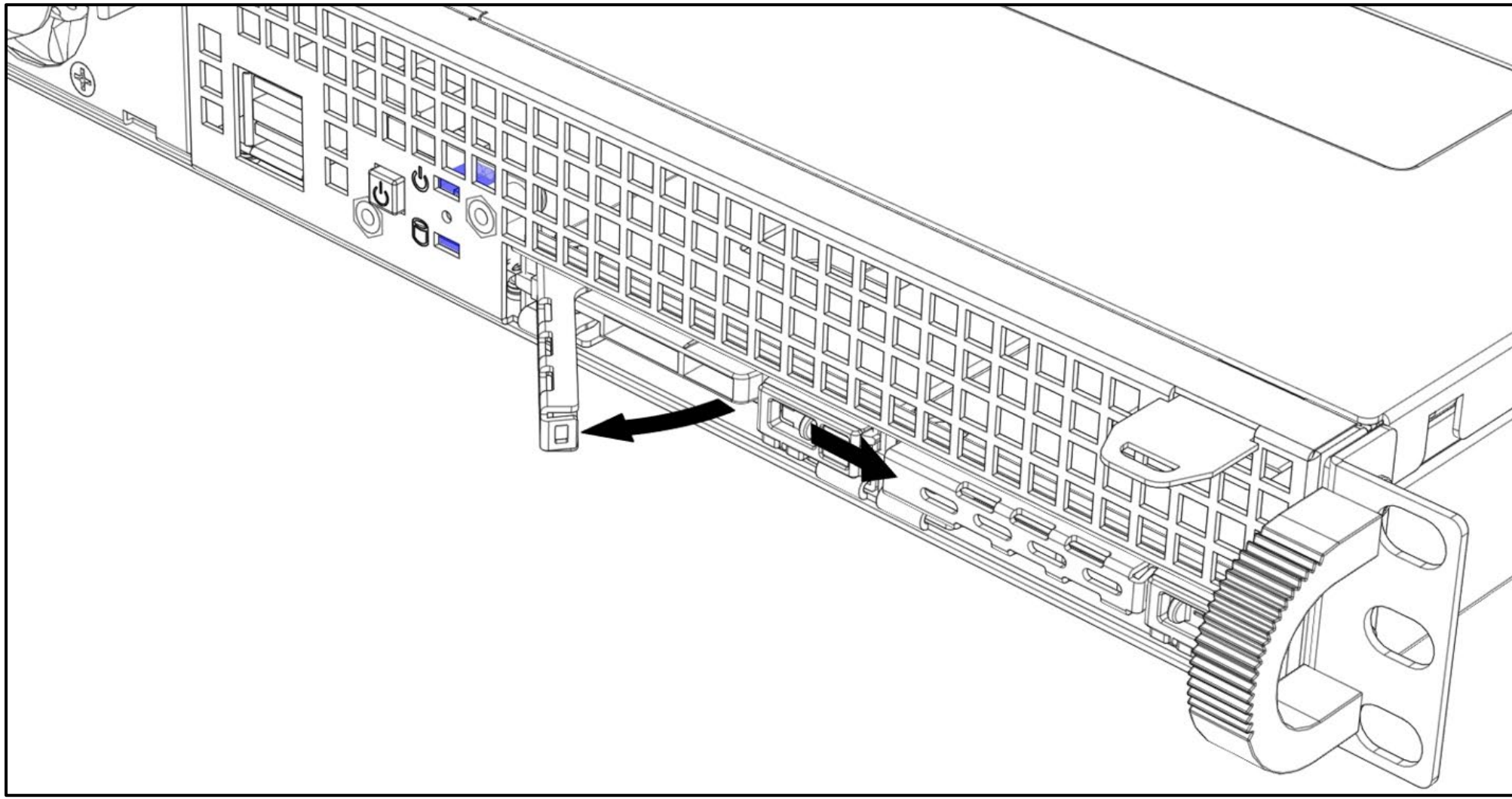




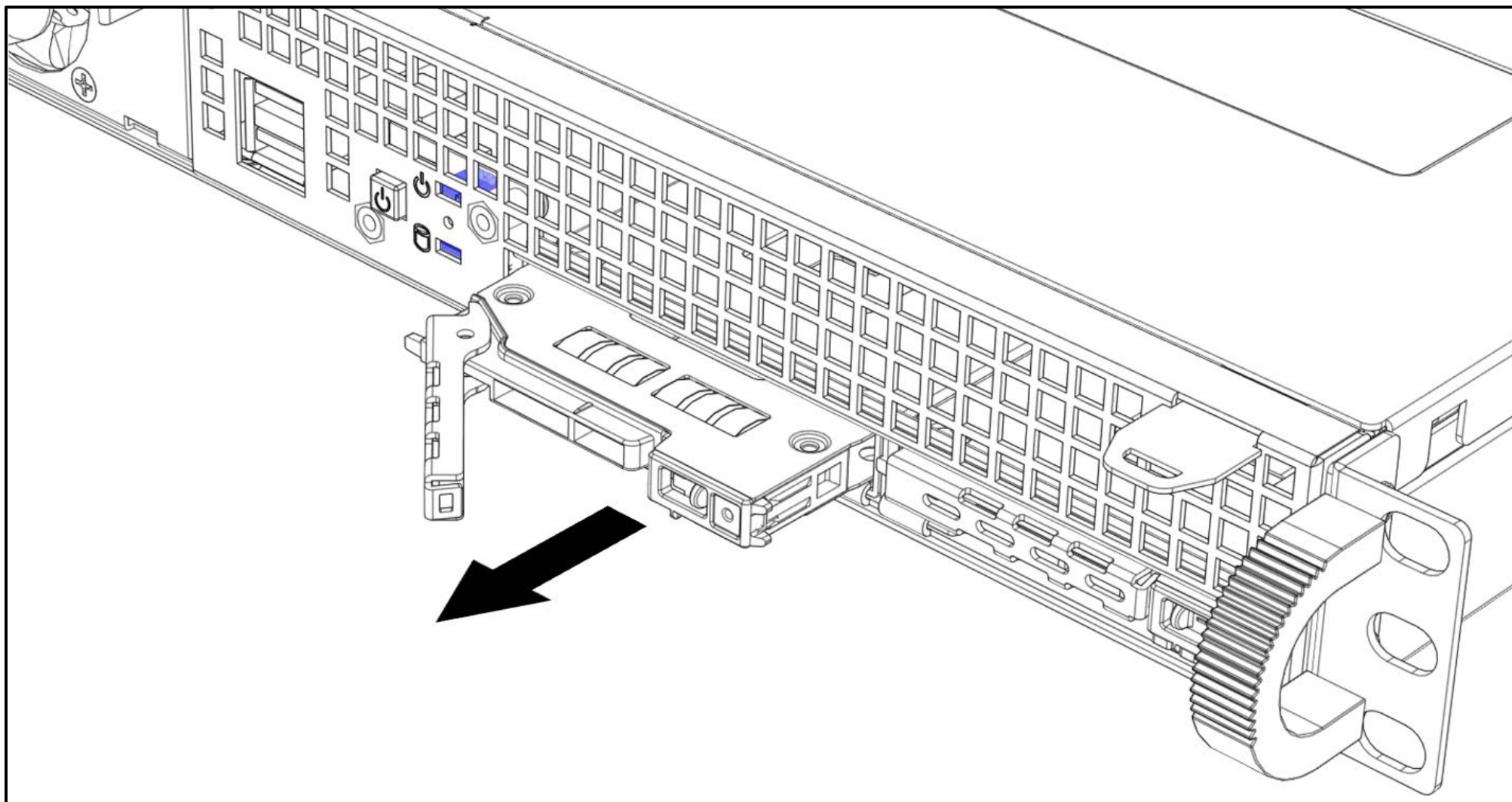
18. Replacing Swappable SSD

This section contains information on how to replace the swappable SSD in the front of the system.

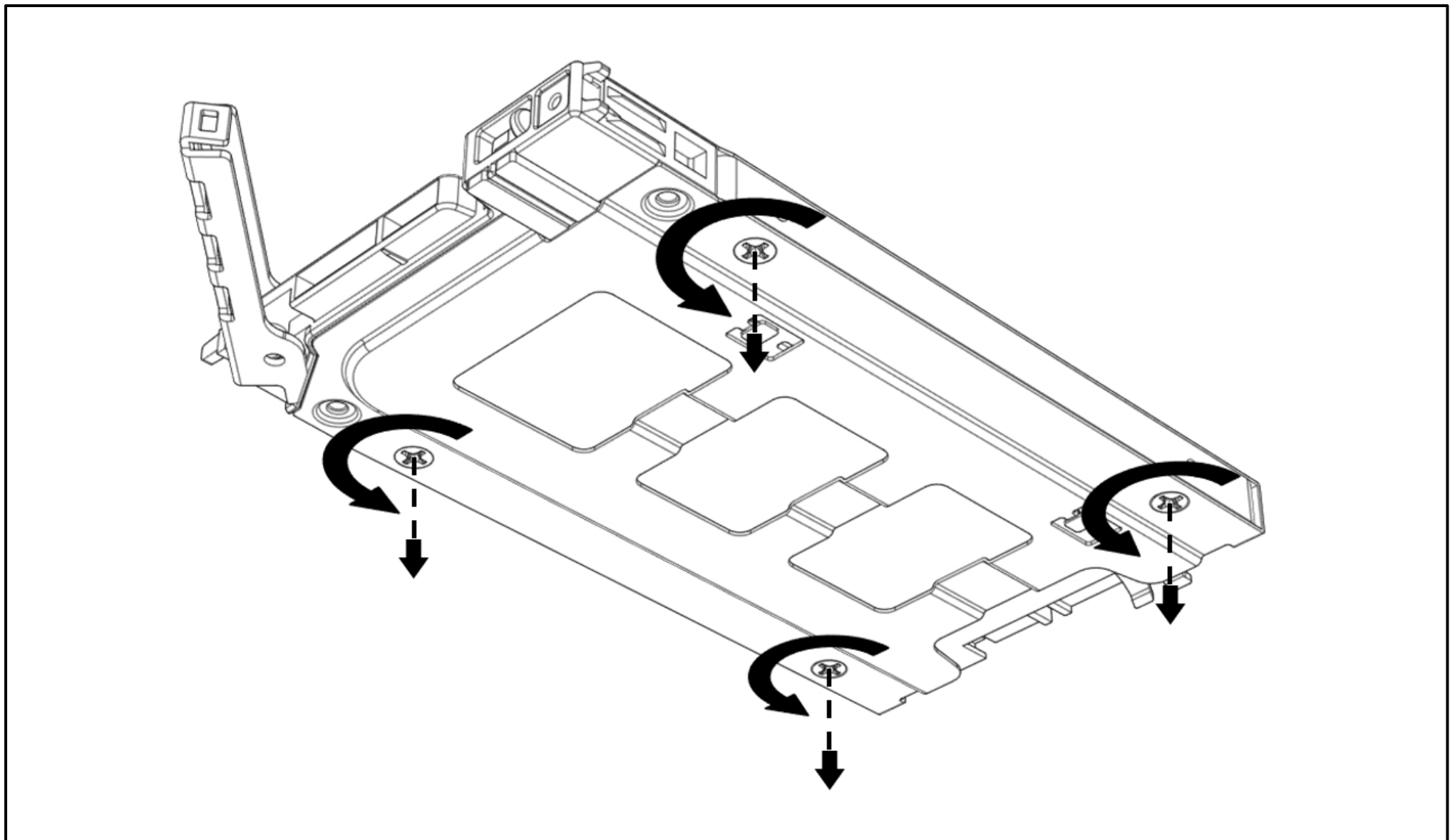
Step 1: Flip the button to the right and the latch pops out.



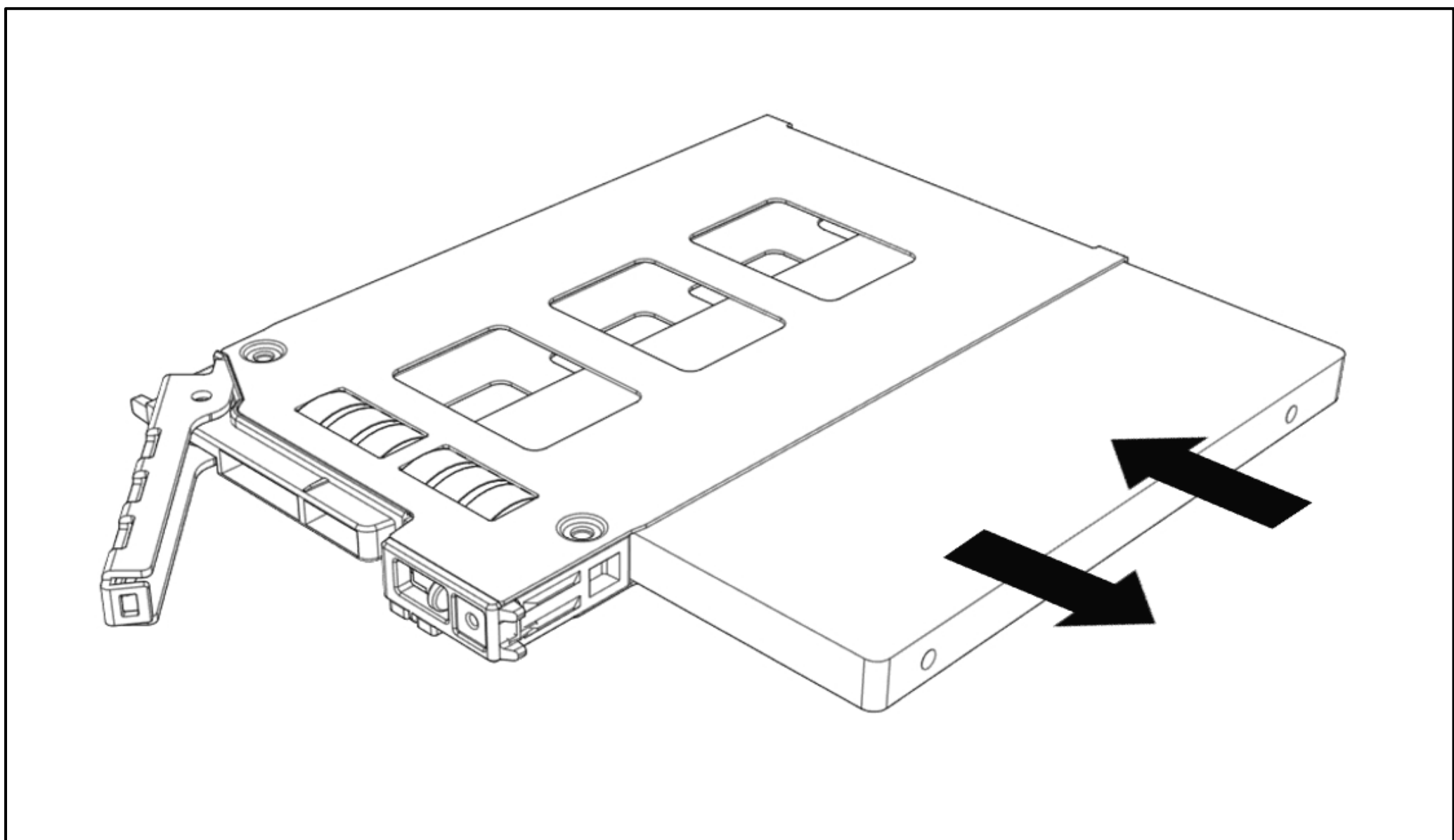
Step 2: Pull out the SSD cage.



Step 3: Turn over the cage and unscrew 4 screws.



Step 4: Replace the SSD.

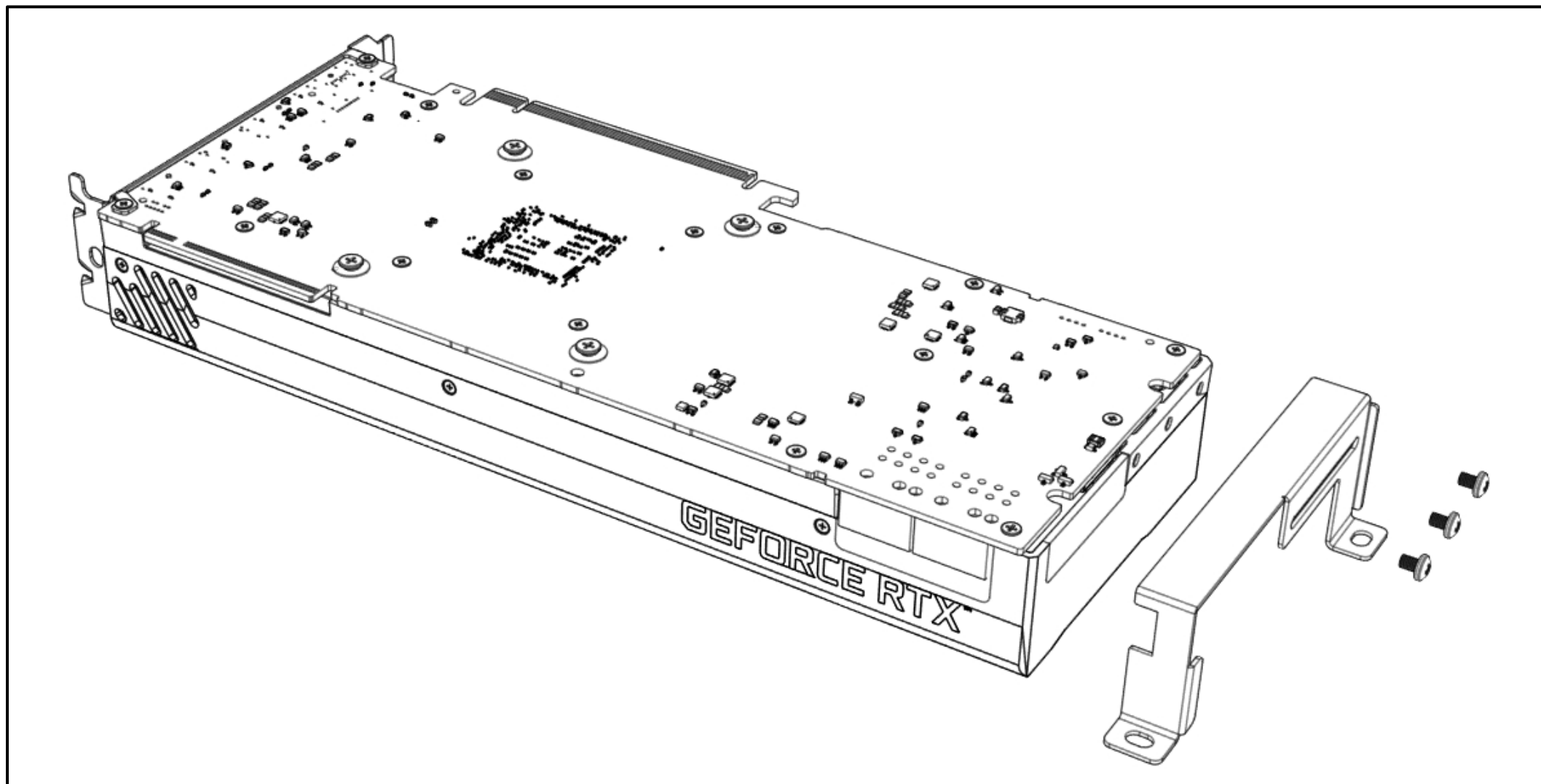


19. Replacing GPU

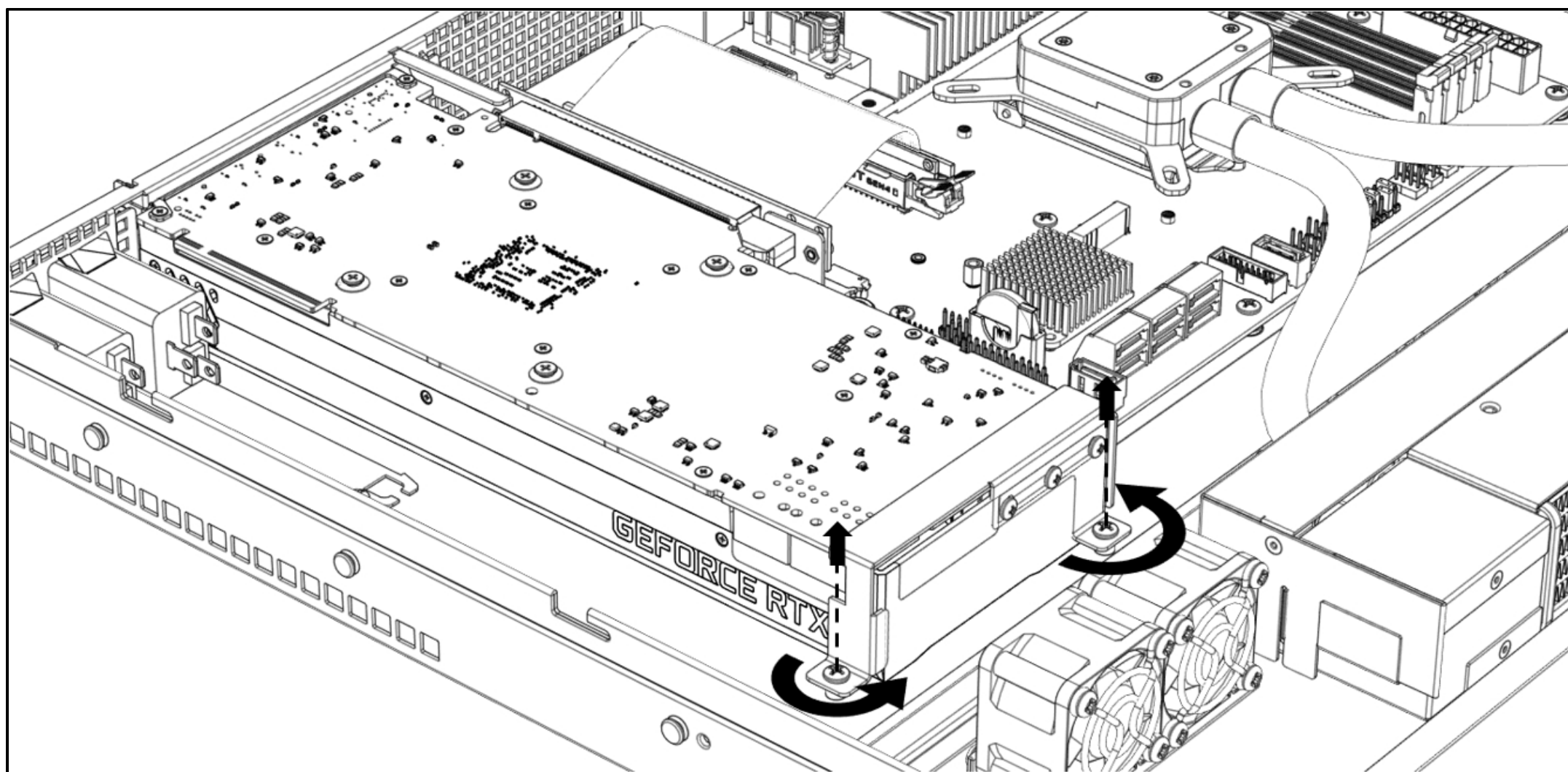
This section contains information on how to replace the GPU in the Orion HF210-G5 system, in the PCIe 1 expansion slot.

 **Caution:** For all the GPUs used in the Orion HF210-G5 system, please install the GPU bracket assembly before installing the card.

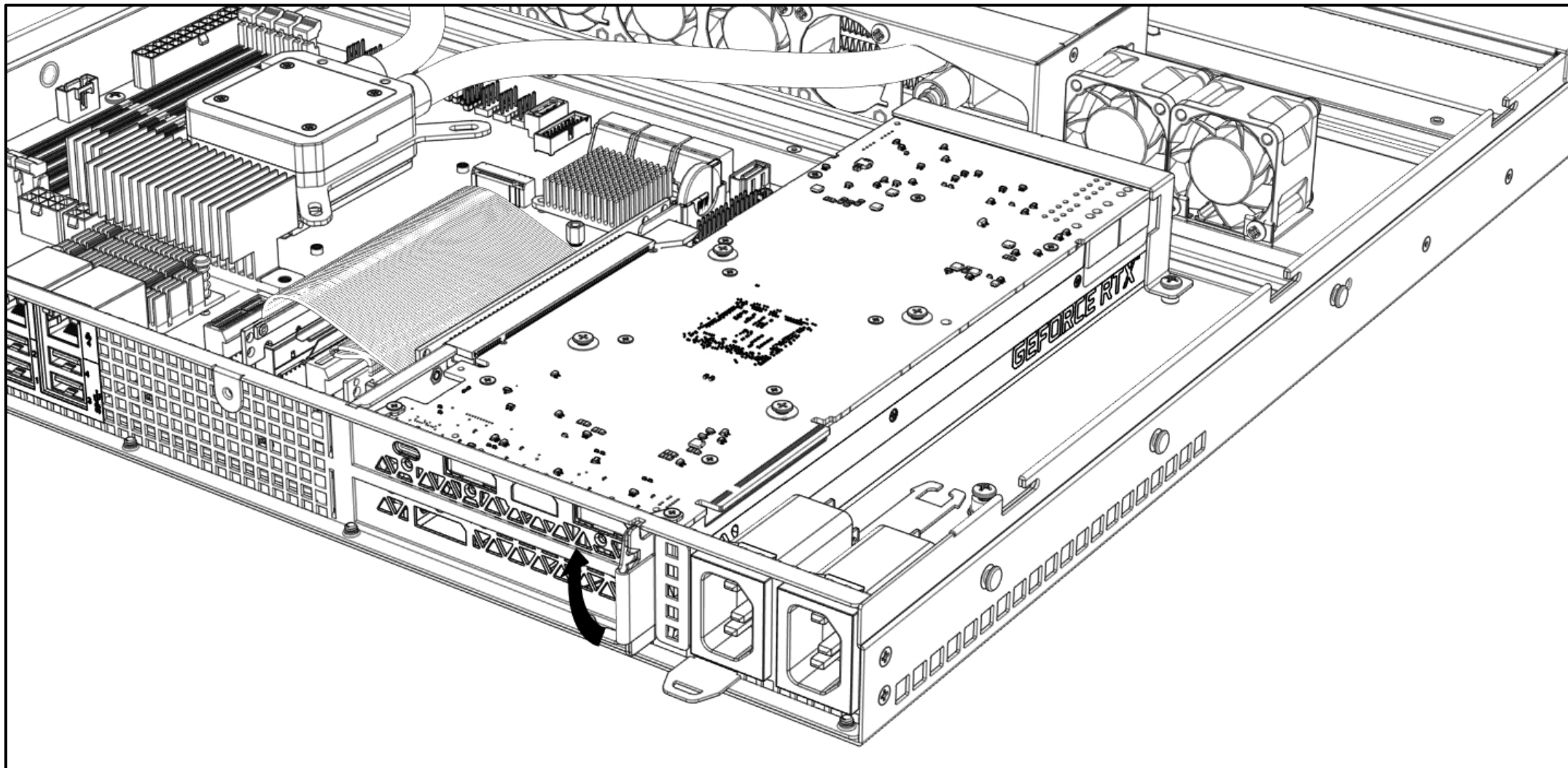
The GPU bracket assembly is provided in the accessory box.



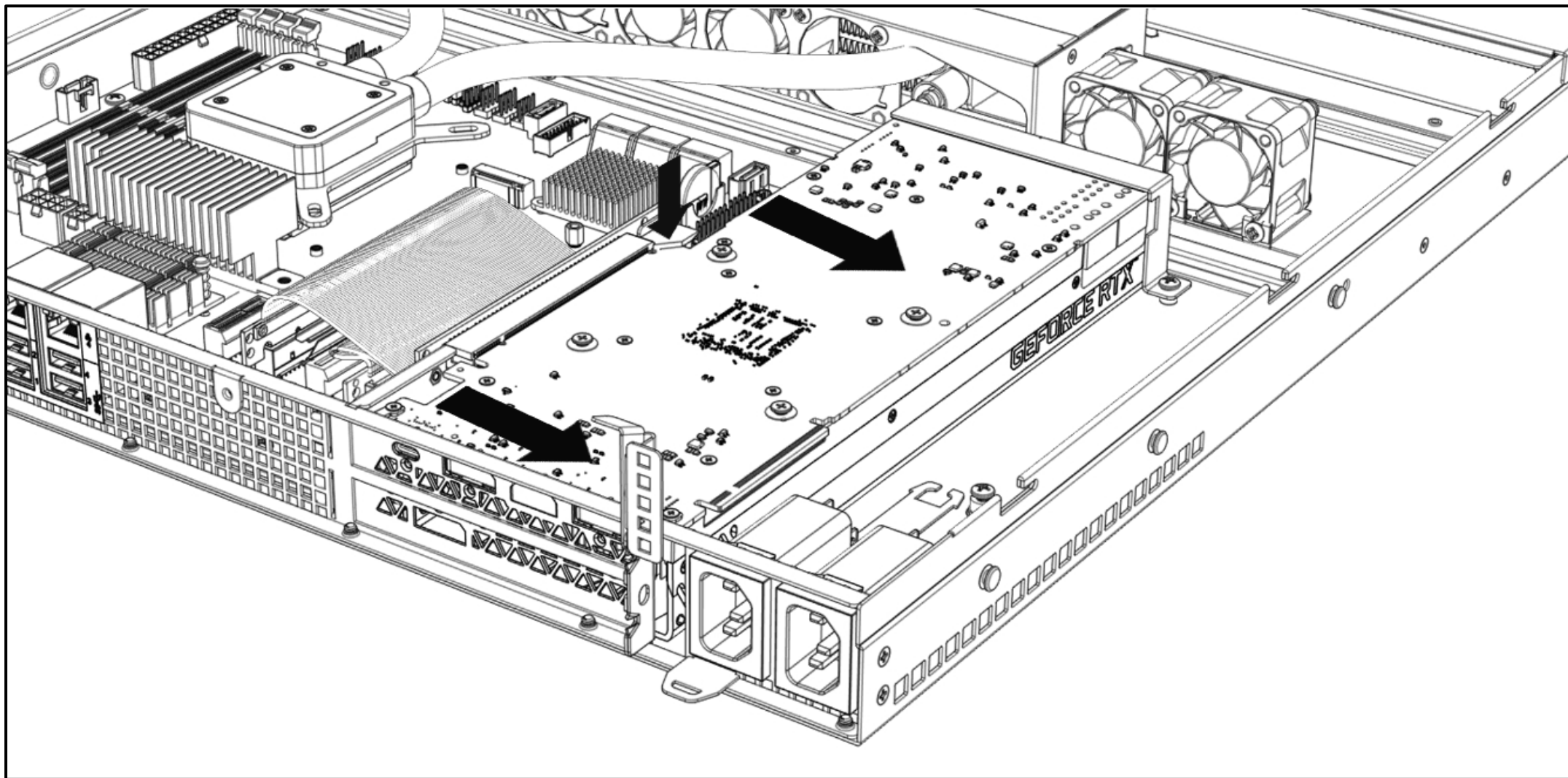
Step 1: Unscrew the two screws from GPU bracket assembly.



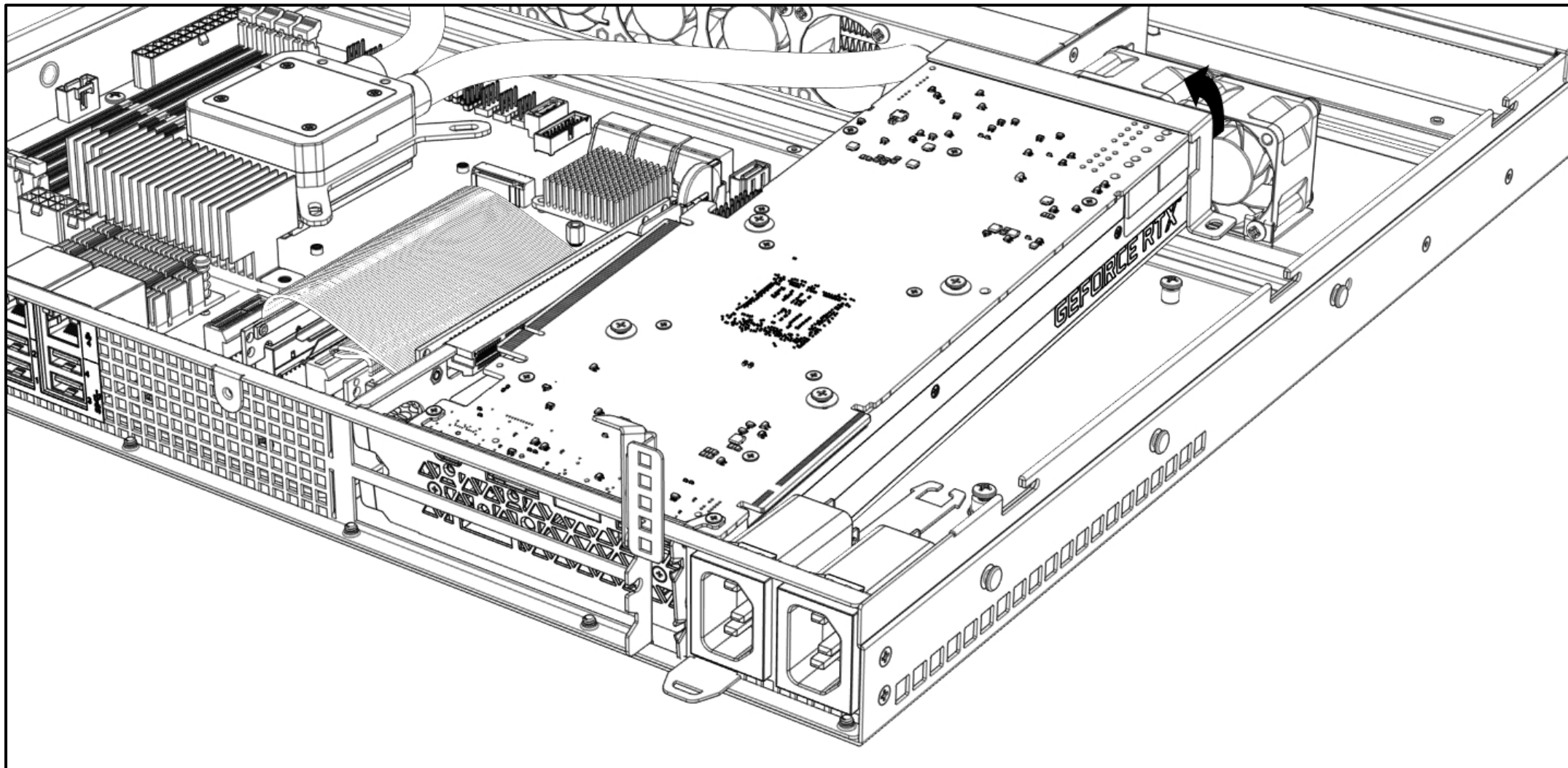
Step 2: Remove the power cables, and rotate the PCIe release latch to the top.



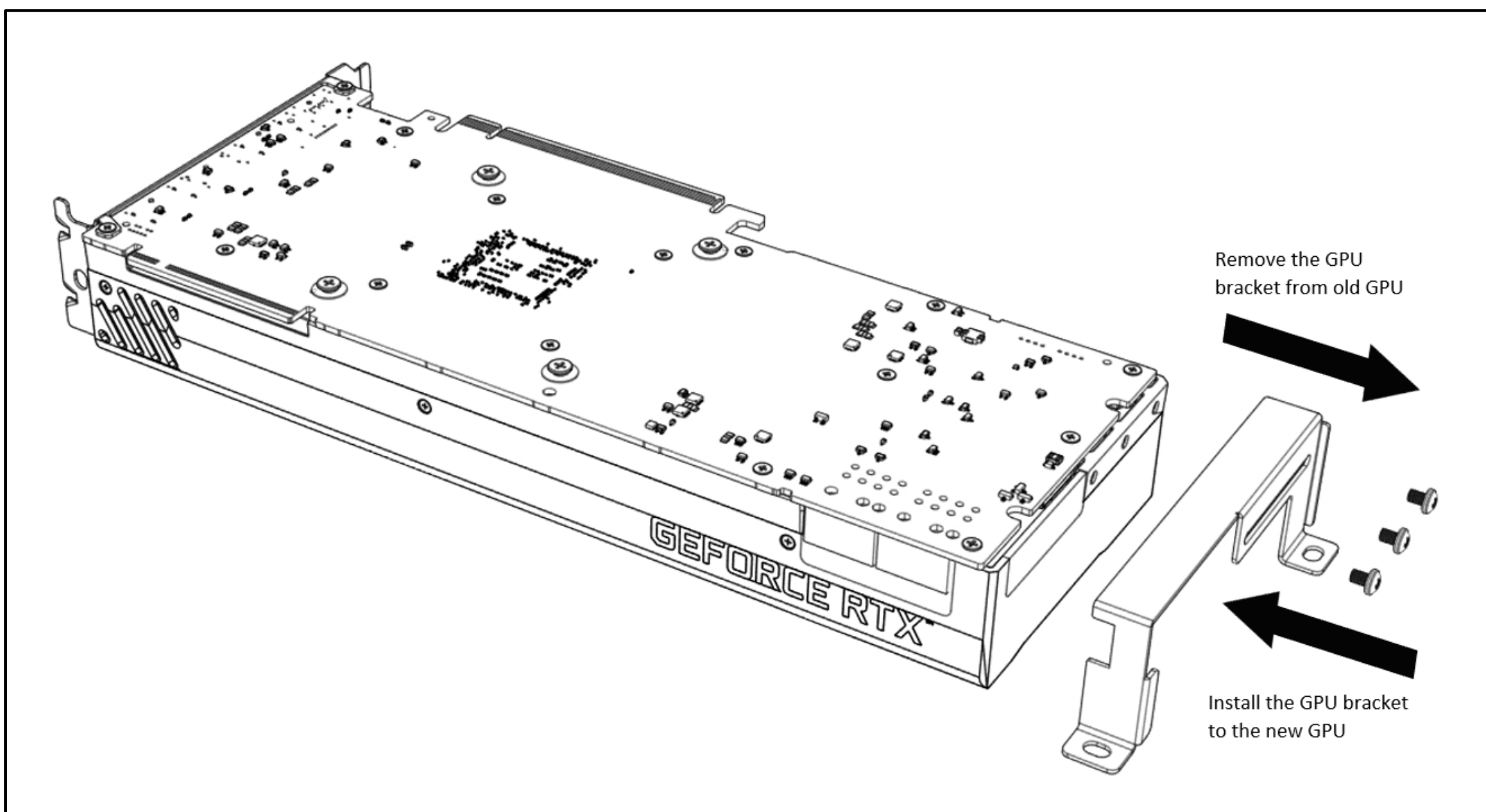
Step 3: Press down the PCIe slot lever and then pull the GPU out of slot.



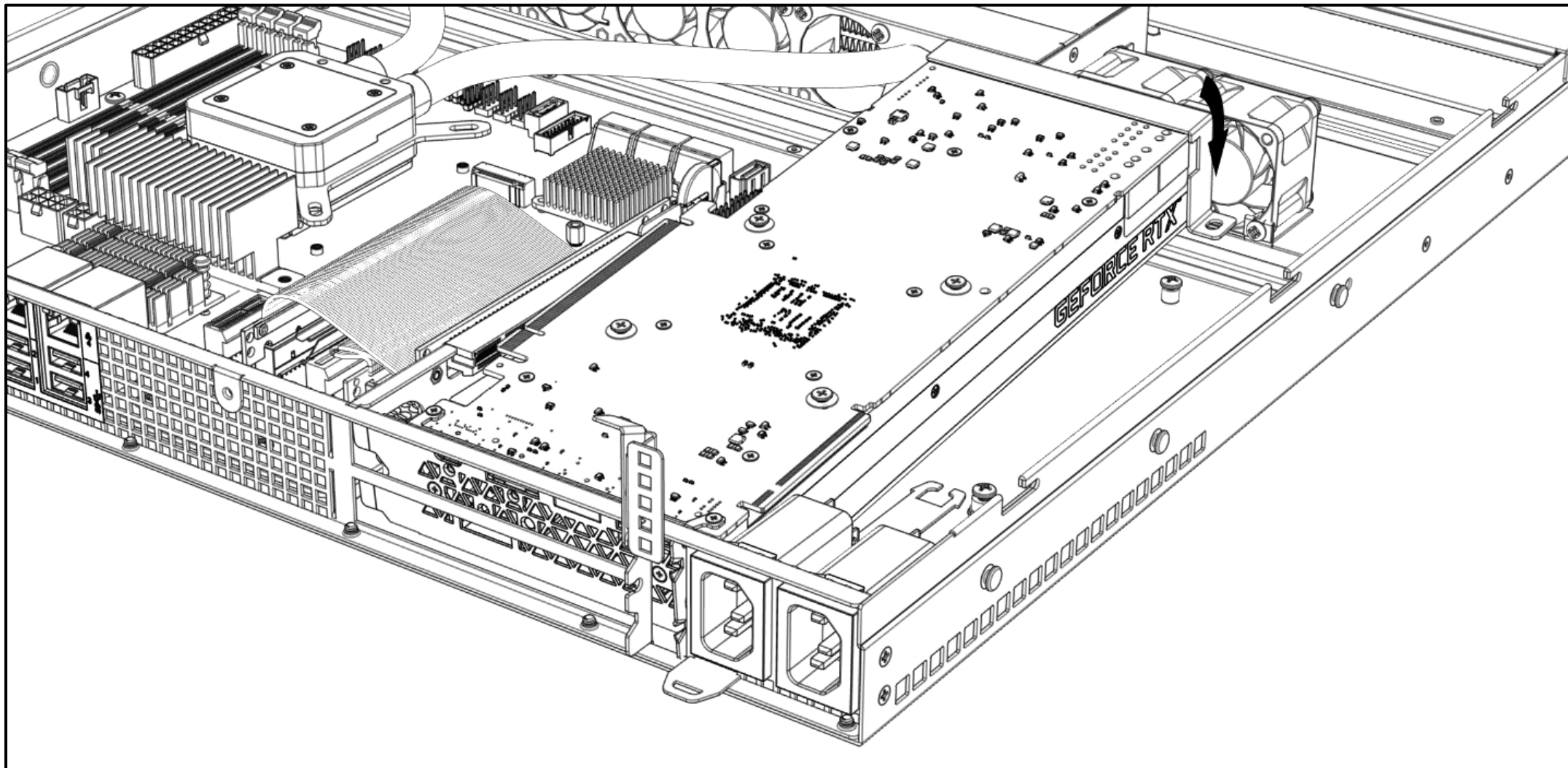
Step 4: Twist the GPU and remove the GPU.



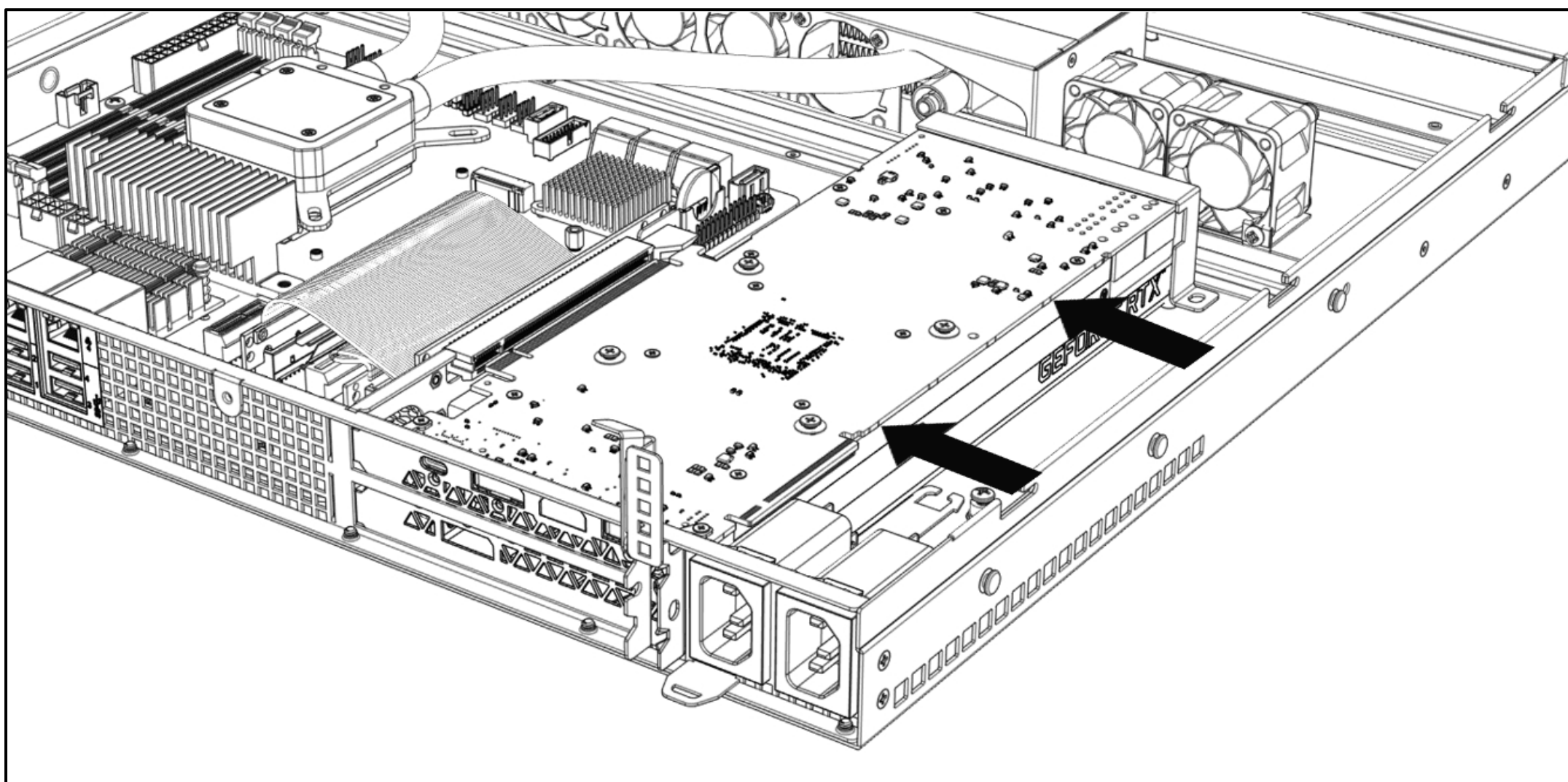
Step 5: Remove the GPU bracket assembly and install to the new GPU.



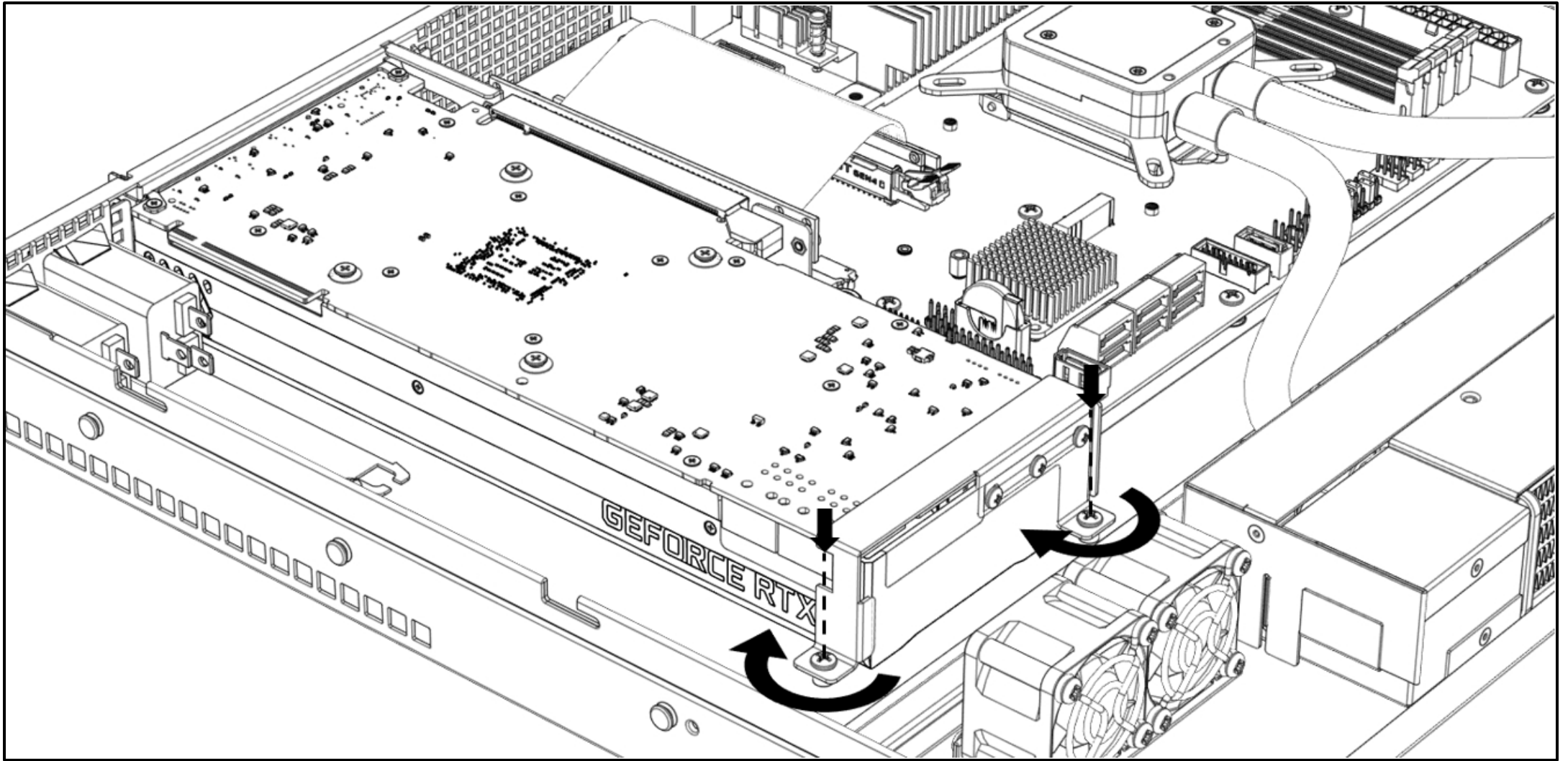
Step 6: Align the metal plate on the GPU with the rear panel then drop down the GPU.



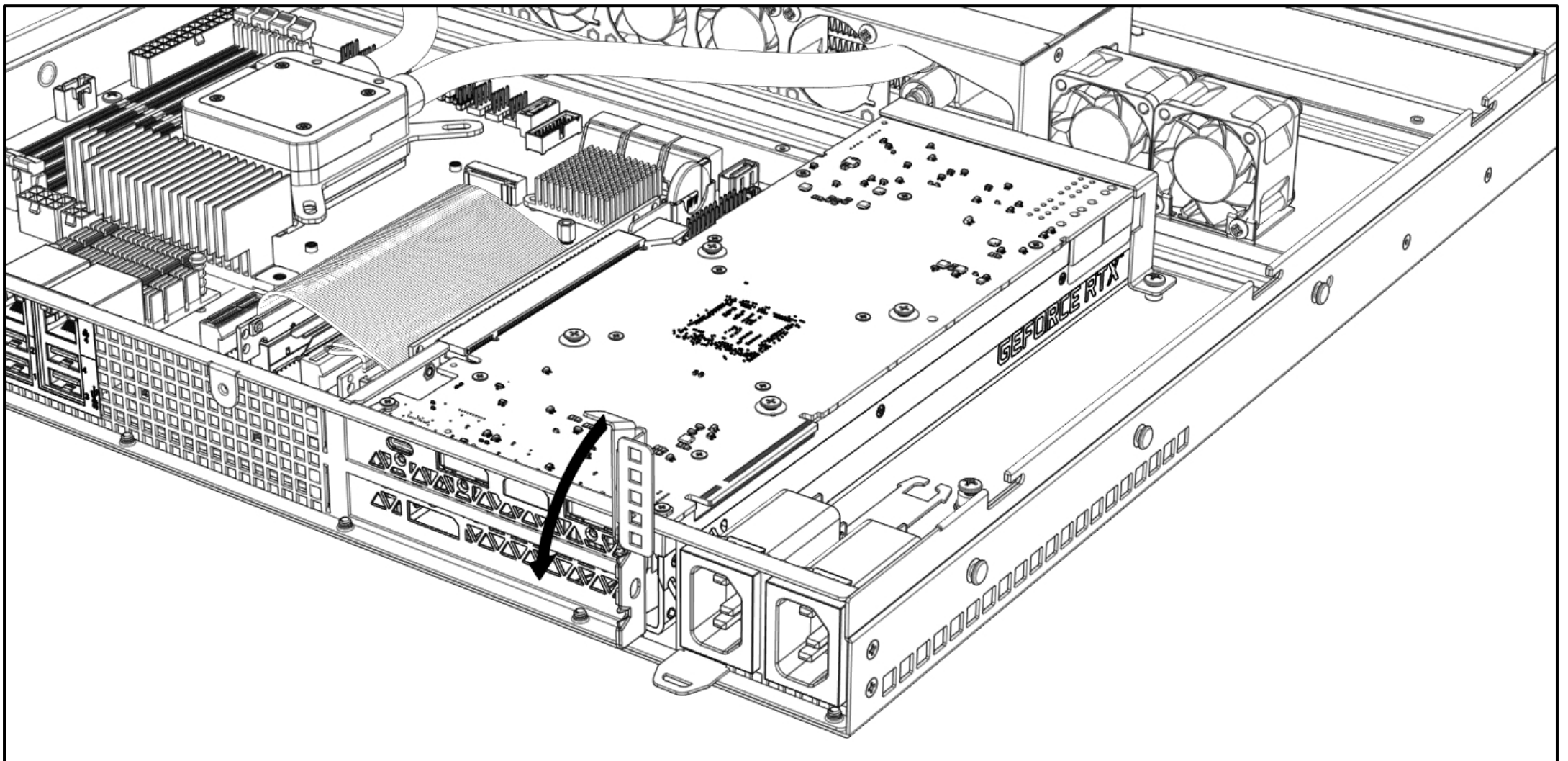
Step 7: Slide the new GPU into the PCIe slot on the riser card.



Step 8: Fasten the screws to mount the GPU bracket assembly with the chassis base.



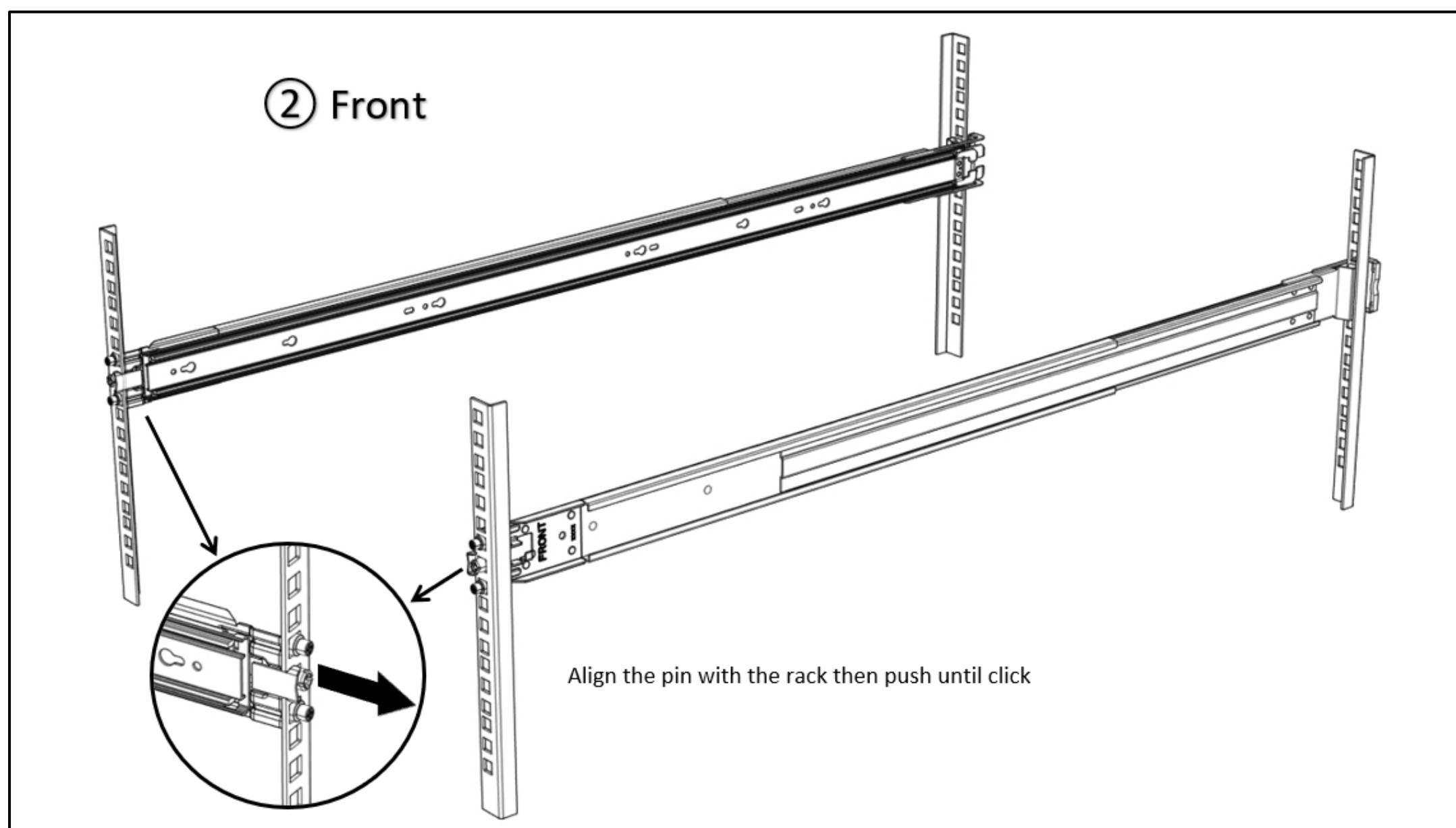
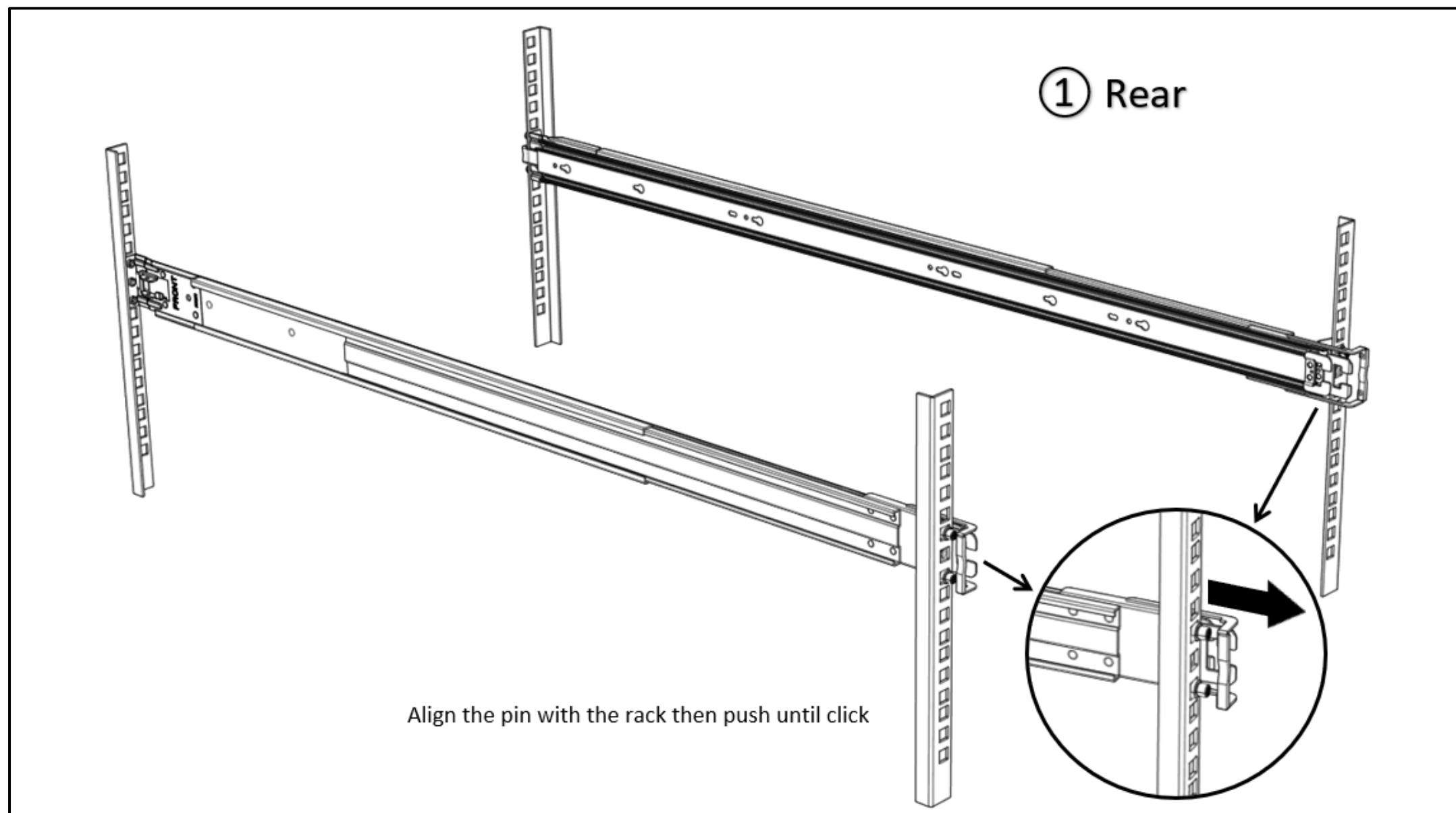
Step 9: Rotate and close the PCIe release latch.



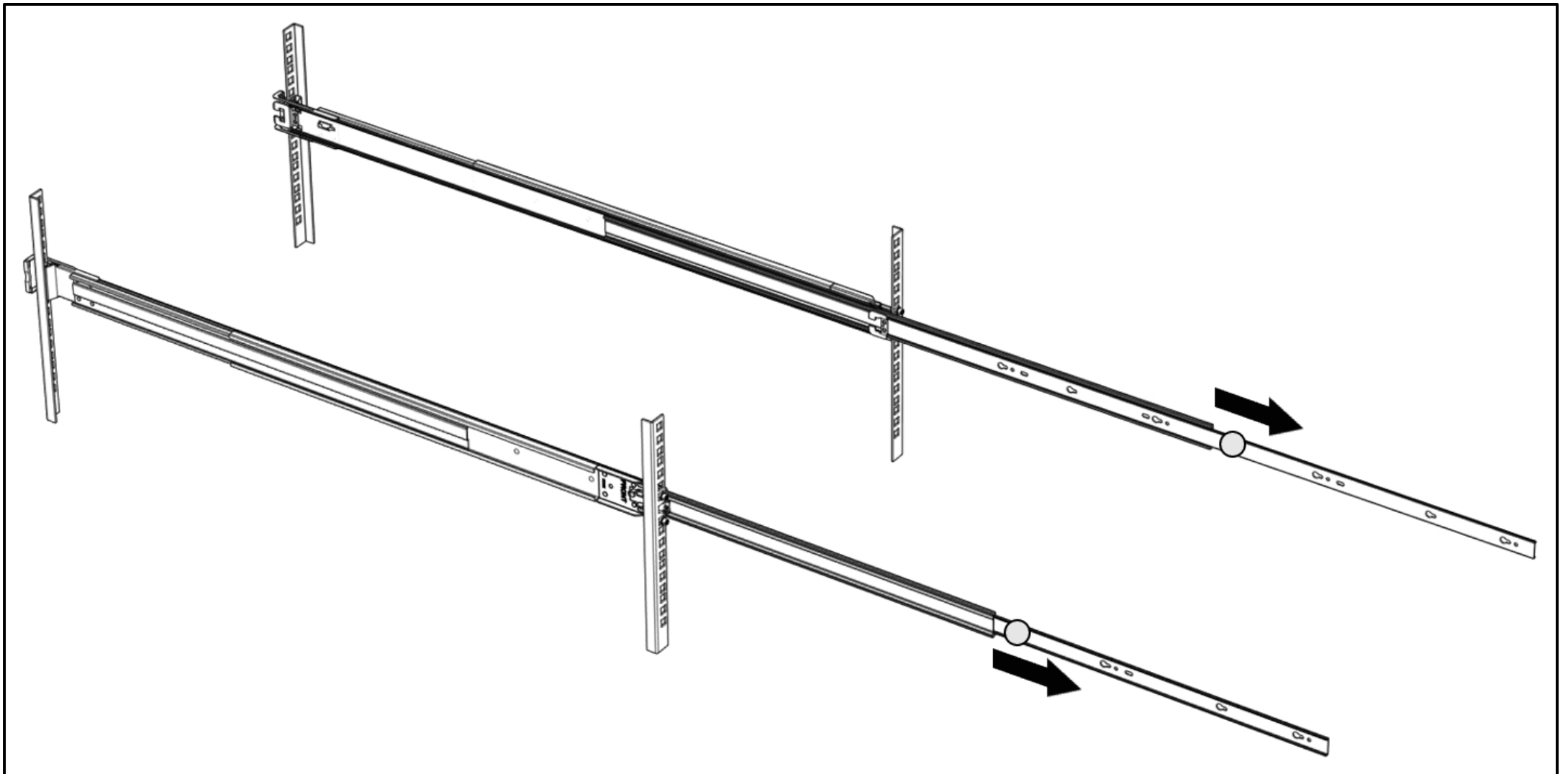
20. Rack Mounting

This section contains information on how to mount a system into the rack with the rack rails.

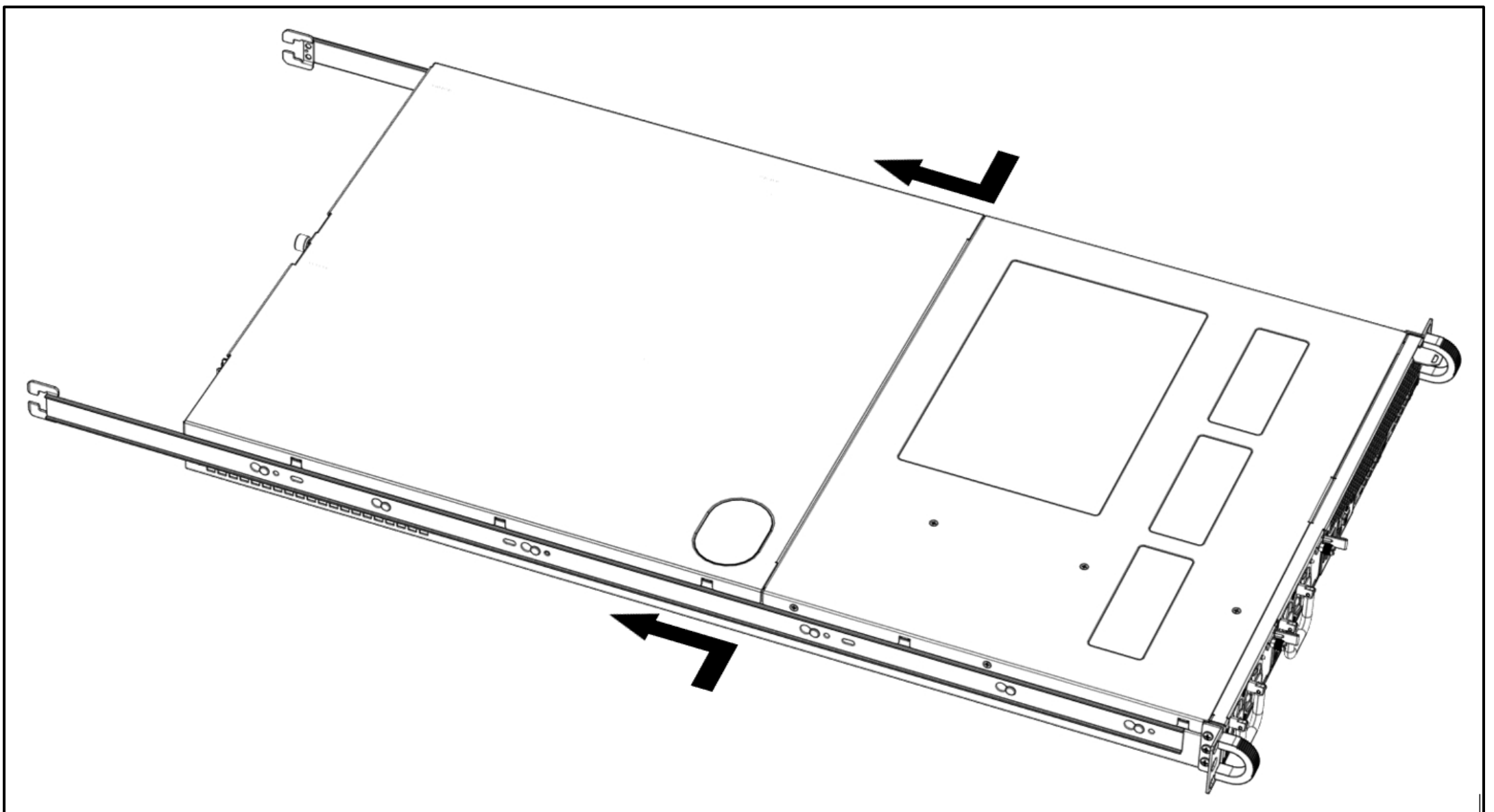
Step 1. Install the rails into the rack.



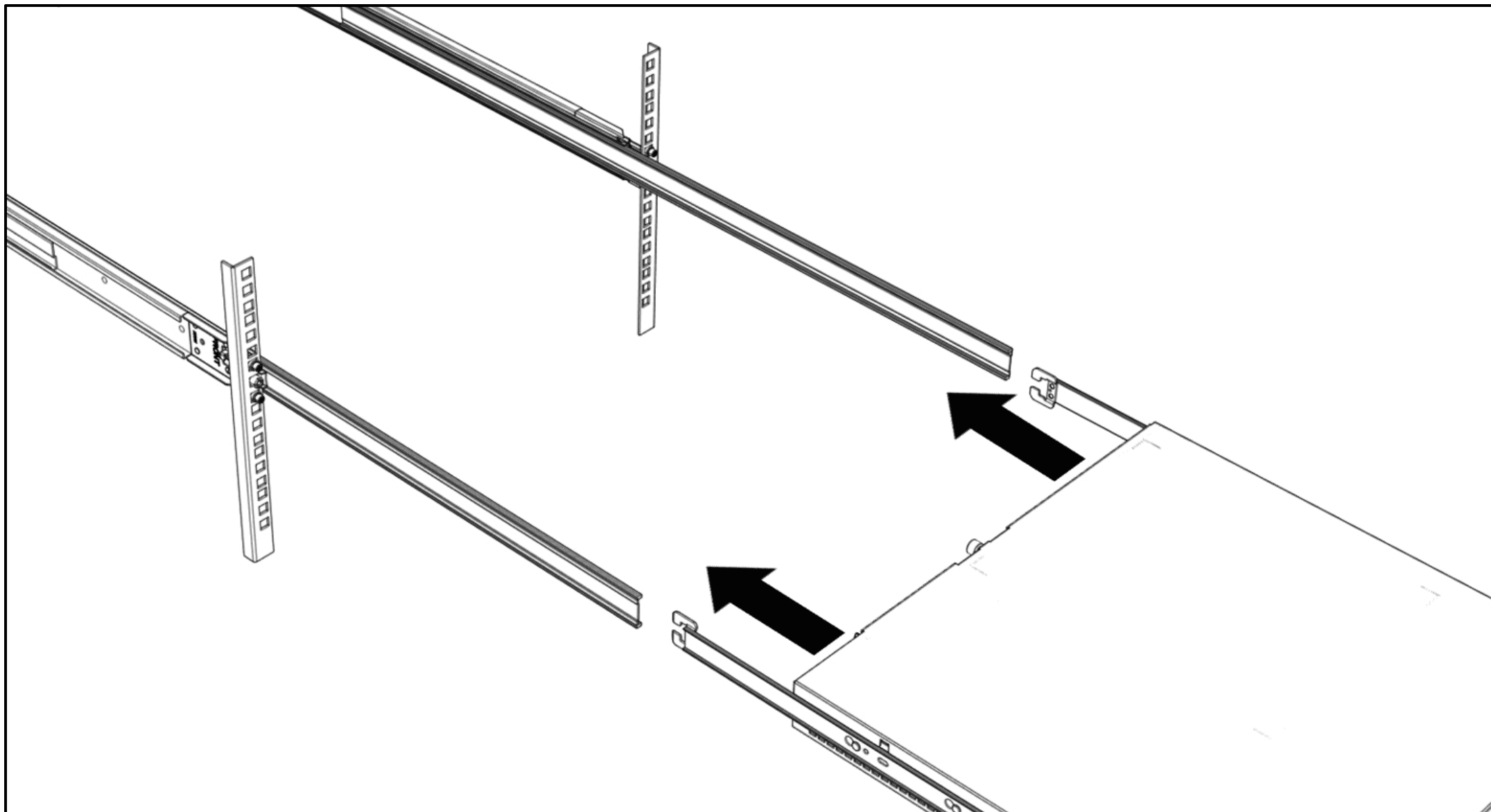
Step 2. Pull the inner and middle rails fully extended in lock position. Pull the white release button to slide out the inner rail.



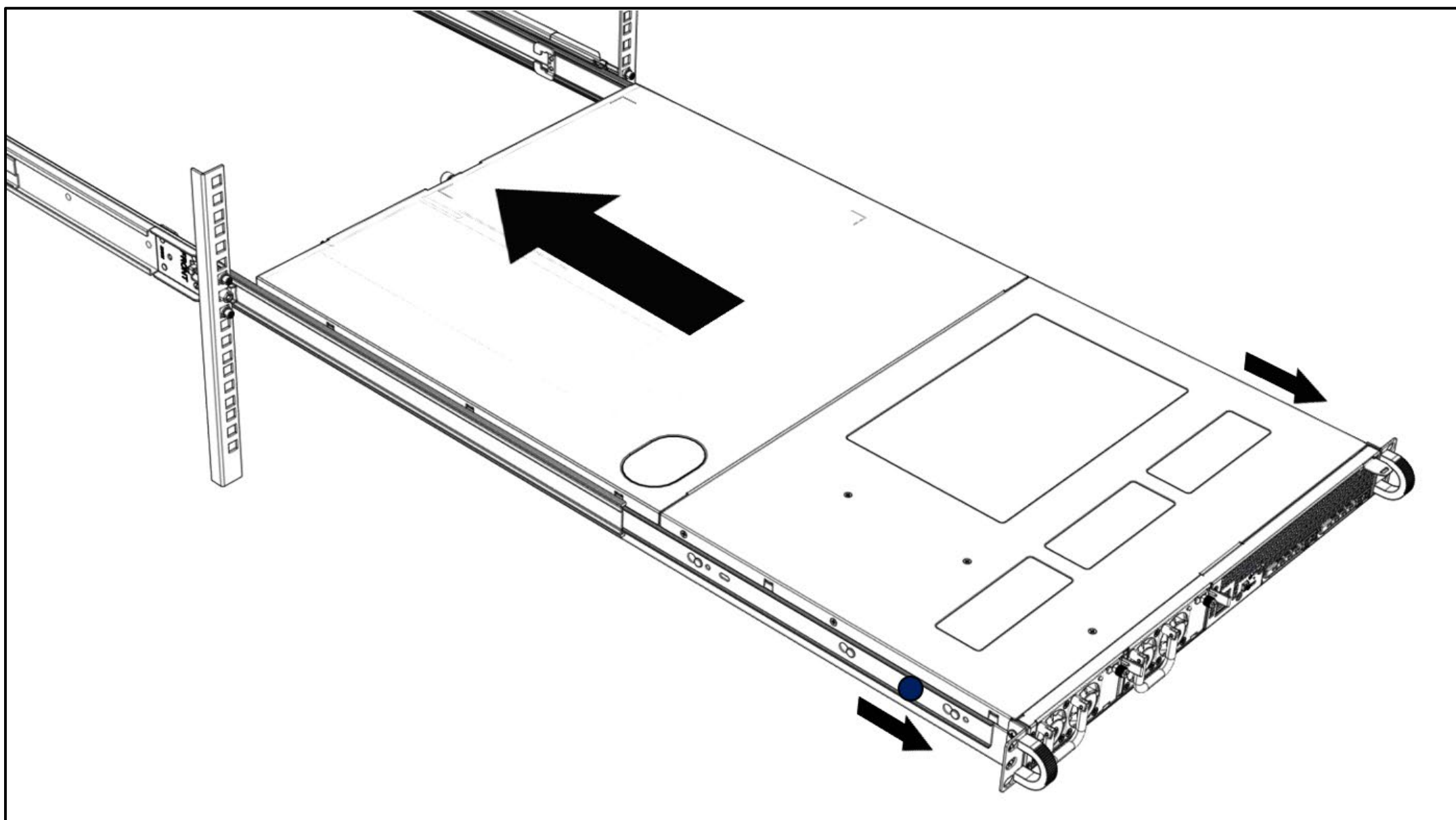
Step 3. Align the inner rail with the chassis mounting key, push and slide to lock.



Step 4. Horizontally slide the chassis into the middle rail until click.

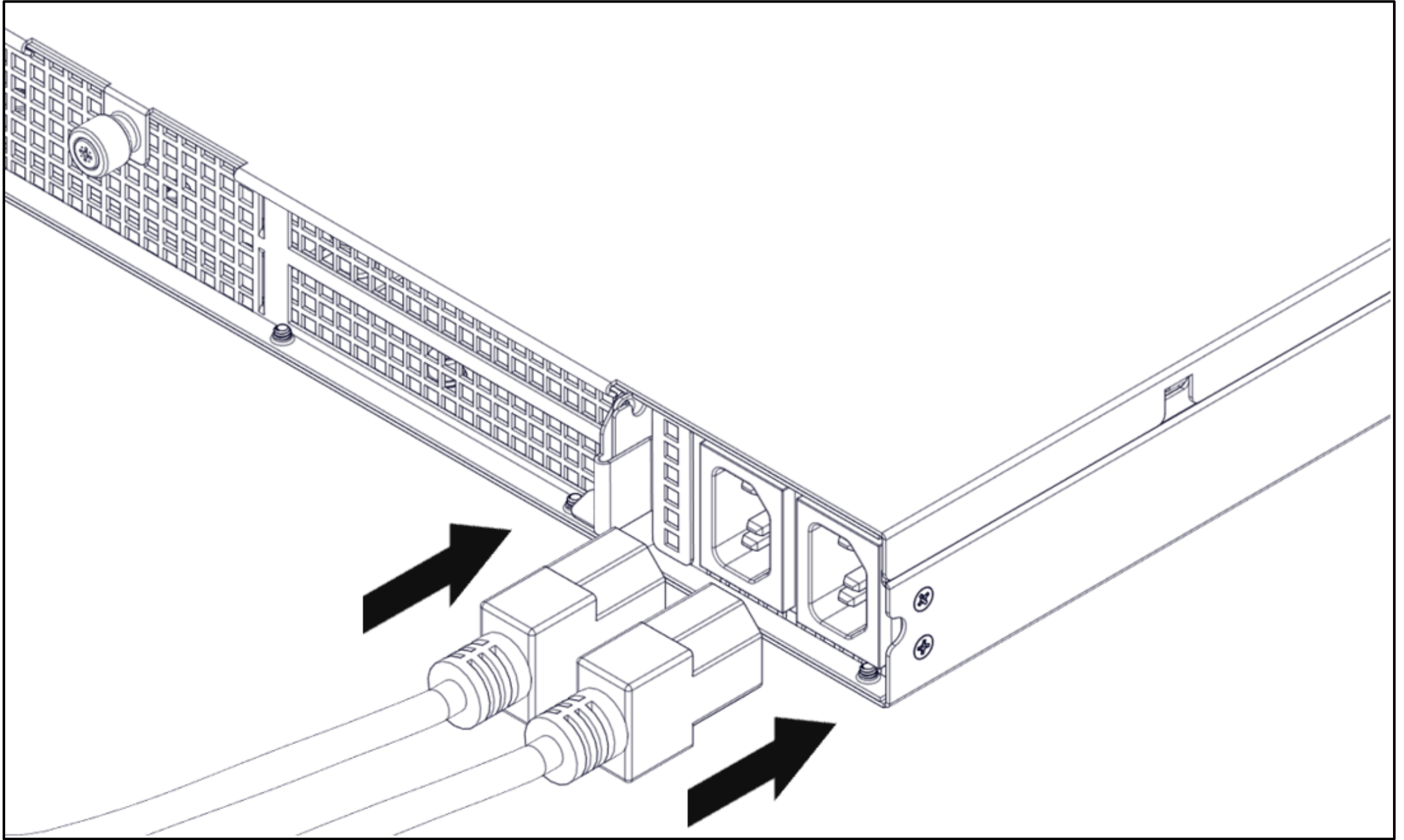


Step 5. Pull/Push the blue release button on the inner rail to unlock the chassis and then push the chassis into rack.



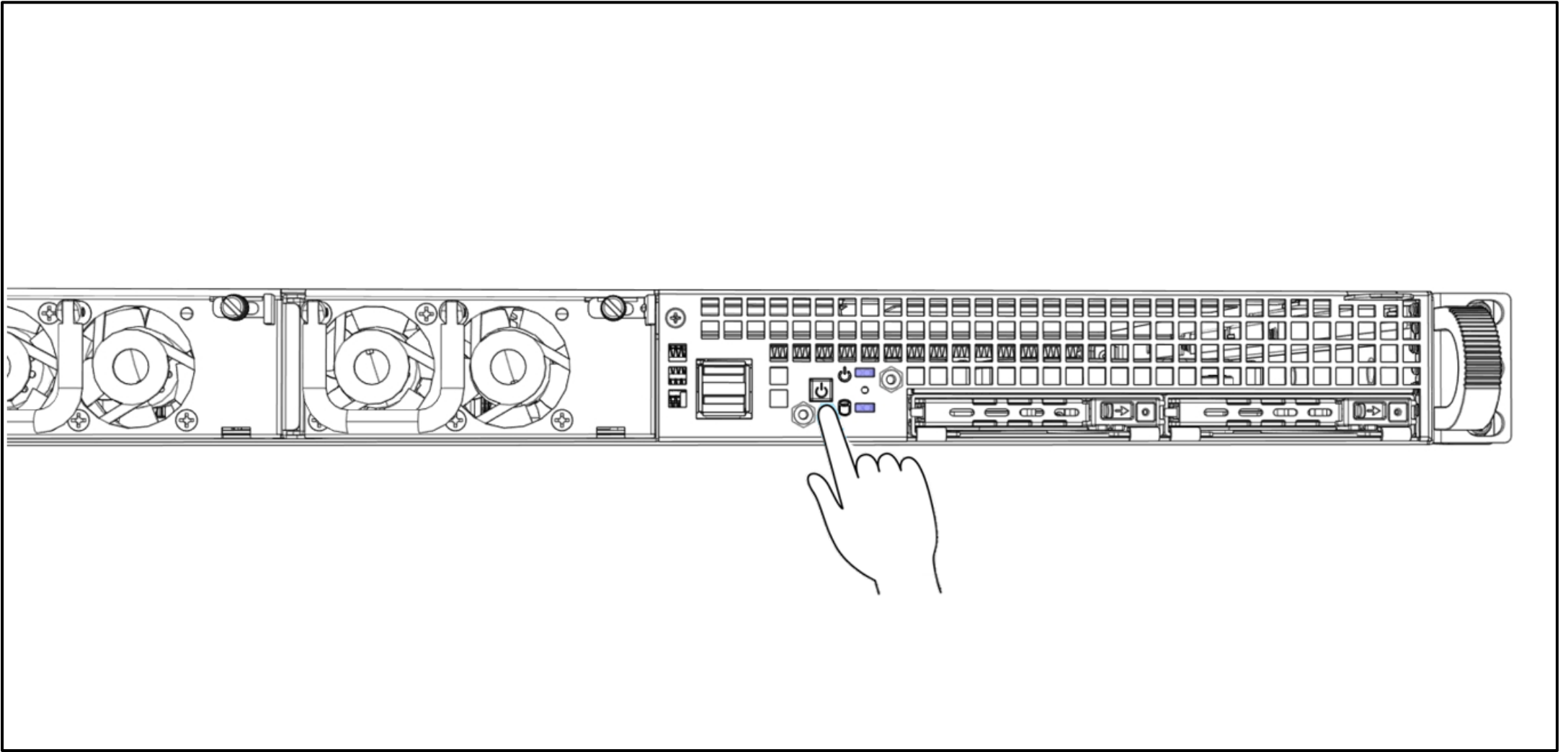
21. Plugging the Power Cords

The following illustration shows how to connect the power cords to the back of the system.



22. Turning on the System

The following illustration indicates where the power button is located on the front of the server.



23. Dr. Debug codes

Dr. Debug is used to provide code information, which makes troubleshooting even easier. Please see the diagrams below for reading the Dr. Debug codes.

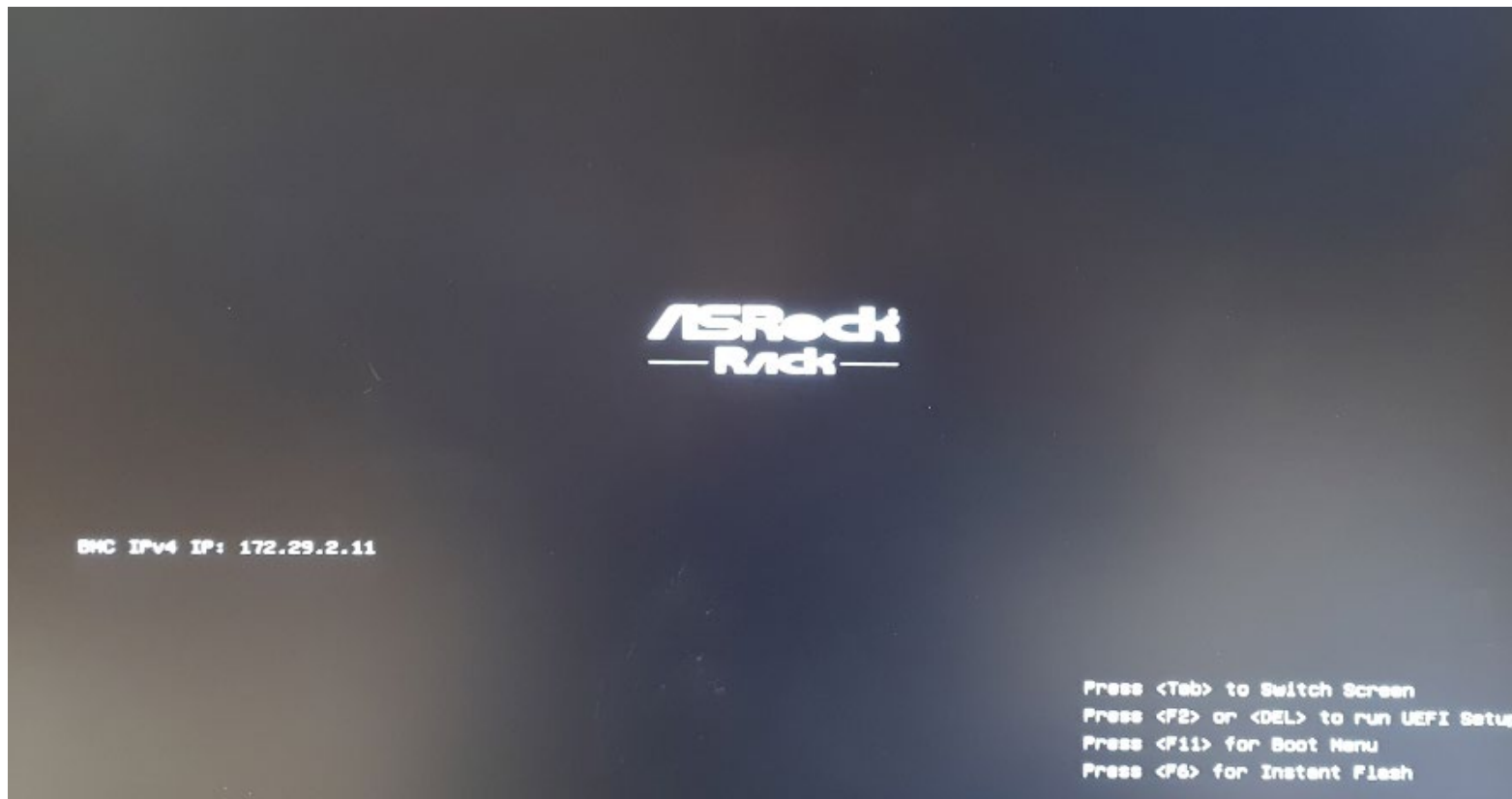
Code	Description	Code	Description
0x10	PEI_CORE_STARTED	0xA9	DXE_SETUP_START
0x11	PEI_CAR_CPU_INIT	0xAB	DXE_SETUP_INPUT_WAIT
0x15	PEI_CAR_NB_INIT	0xAD	DXE_READY_TO_BOOT
0x19	PEI_CAR_SB_INIT	0xAE	DXE_LEGACY_BOOT
0x31	PEI_MEMORY_INSTALLED	0xAF	DXE_EXIT_BOOT_SERVICES
0x32	PEI_CPU_INIT	0xB0	RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN
0x33	PEI_CPU_CACHE_INIT	0xB1	RT_SET_VIRTUAL_ADDRESS_MAP_END
0x34	PEI_CPU_AP_INIT	0xB2	DXE_LEGACY_OPROM_INIT
0x35	PEI_CPU_BSP_SELECT	0xB3	DXE_RESET_SYSTEM
0x36	PEI_CPU_SMM_INIT	0xB4	DXE_USB_HOTPLUG
0x37	PEI_MEM_NB_INIT	0xB5	DXE_PCI_BUS_HOTPLUG
0x3B	PEI_MEM_SB_INIT	0xB6	DXE_NVRAM_CLEANUP
0x4F	PEI_DXE_IPL_STARTED	0xB7	DXE_CONFIGURATION_RESET
0x60	DXE_CORE_STARTED	0xF0	PEI_RECOVERY_AUTO
0x61	DXE_NVRAM_INIT	0xF1	PEI_RECOVERY_USER
0x62	DXE_SBRUN_INIT	0xF2	PEI_RECOVERY_STARTED
0x63	DXE_CPU_INIT	0xF3	PEI_RECOVERY_CAPSULE_FOUND
0x68	DXE_NB_HB_INIT	0xF4	PEI_RECOVERY_CAPSULE_LOADED
0x69	DXE_NB_INIT	0xE0	PEI_S3_STARTED
0x6A	DXE_NB_SMM_INIT	0xE1	PEI_S3_BOOT_SCRIPT
0x70	DXE_SB_INIT	0xE2	PEI_S3_VIDEO_REPOST
0x71	DXE_SB_SMM_INIT	0xE3	PEI_S3_OS_WAKE
0x72	DXE_SB_DEVICES_INIT	0x50	PEI_MEMORY_INVALID_TYPE
0x78	DXE_ACPI_INIT	0x53	PEI_MEMORY_NOT_DETECTED
0x79	DXE_CSM_INIT	0x55	PEI_MEMORY_NOT_INSTALLED
0x90	DXE_BDS_STARTED	0x57	PEI_CPU_MISMATCH
0x91	DXE_BDS_CONNECT_DRIVERS	0x58	PEI_CPU_SELF_TEST_FAILED
0x92	DXE_PCI_BUS_BEGIN	0x59	PEI_CPU_NO_MICROCODE
0x93	DXE_PCI_BUS_HPC_INIT	0x5A	PEI_CPU_ERROR
0x94	DXE_PCI_BUS_ENUM	0x5B	PEI_RESET_NOT_AVAILABLE
0x95	DXE_PCI_BUS_REQUEST_RESOURCES	0xD0	DXE_CPU_ERROR
0x96	DXE_PCI_BUS_ASSIGN_RESOURCES	0xD1	DXE_NB_ERROR
0x97	DXE_CON_OUT_CONNECT	0xD2	DXE_SB_ERROR
0x98	DXE_CON_IN_CONNECT	0xD3	DXE_ARCH_PROTOCOL_NOT_AVAILABLE
0x99	DXE_SIO_INIT	0xD4	DXE_PCI_BUS_OUT_OF_RESOURCES
0x9A	DXE_USB_BEGIN	0xD5	DXE_LEGACY_OPROM_NO_SPACE
0x9B	DXE_USB_RESET	0xD6	DXE_NO_CON_OUT
0x9C	DXE_USB_DETECT	0xD7	DXE_NO_CON_IN
0x9D	DXE_USB_ENABLE	0xD8	DXE_INVALID_PASSWORD
0xA0	DXE_IDE_BEGIN	0xD9	DXE_BOOT_OPTION_LOAD_ERROR
0xA1	DXE_IDE_RESET	0xDA	DXE_BOOT_OPTION_FAILED
0xA2	DXE_IDE_DETECT	0xDB	DXE_FLASH_UPDATE_FAILED
0xA3	DXE_IDE_ENABLE	0xDC	DXE_RESET_NOT_AVAILABLE
0xA4	DXE_SCSI_BEGIN	0xE8	PEI_MEMORY_S3_RESUME_FAILED
0xA5	DXE_SCSI_RESET	0xE9	PEI_S3_RESUME_PPI_NOT_FOUND
0xA6	DXE_SCSI_DETECT	0xEA	PEI_S3_BOOT_SCRIPT_ERROR
0xA7	DXE_SCSI_ENABLE	0xEB	PEI_S3_OS_WAKE_ERROR
0xA8	DXE_SETUP_VERIFYING_PASSWORD		

24. Accessing BIOS:

This section contains information on how to access to the system's BIOS.

Turn on the system and press the **DEL** or **F2** button on the keyboard immediately after you see the following windows during the POST (Power-On-Self-Test) to enter in to the Bios.

If you miss the step and would like to enter to the BIOS utility after POST then restart the system by pressing **<Ctrl> + <Alt> + <Delete>**, or by pressing the reset button on the system chassis.



24. 1 BIOS Menu

The BIOS Menu has the following sections:

Main: To set up the system time/date information

OC Tweaker: To load the user profiles.

Advanced: To set up the advanced BIOS features

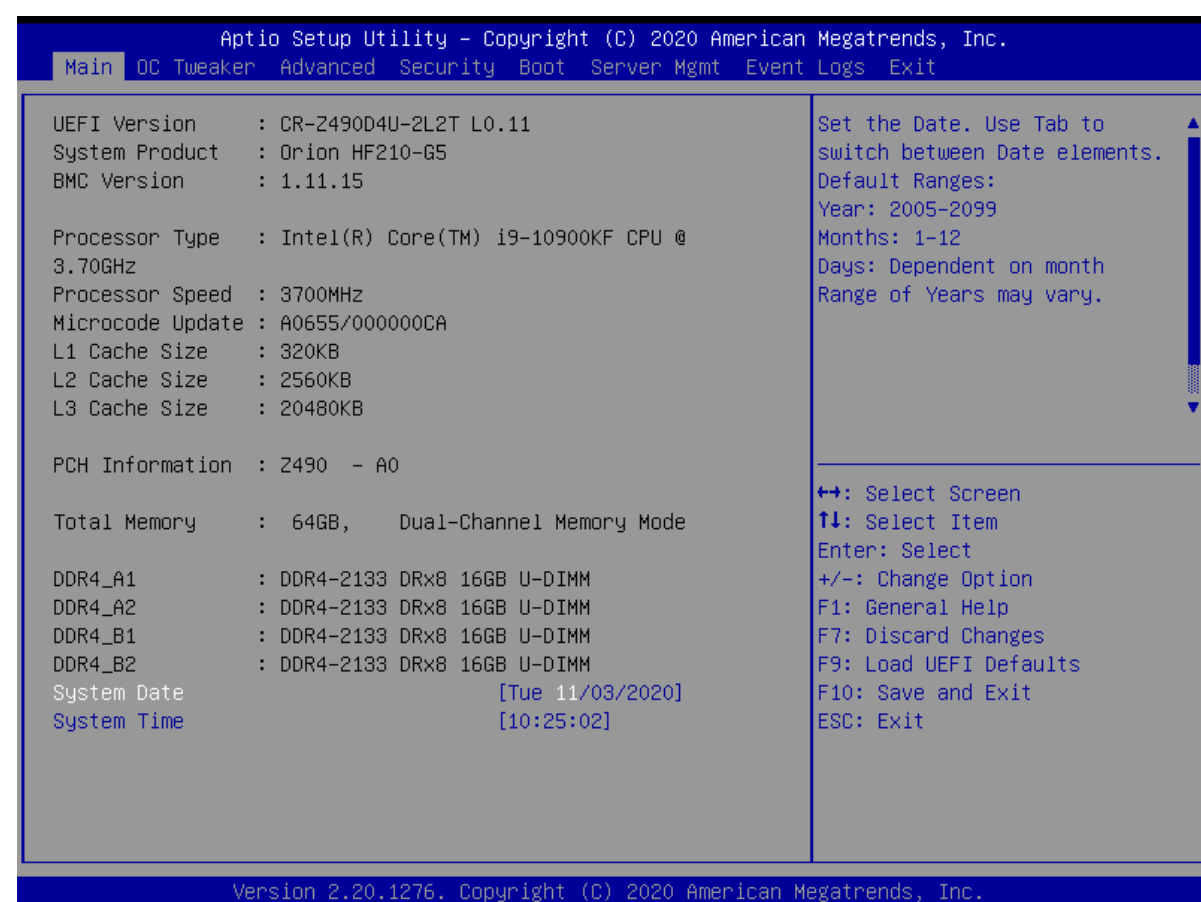
Security: To set up the security features such as Supervisor Password and Enabling/Disabling Secure Boot.

Boot: To set up the default system device to locate and load the Operating System.

Server Mgmt: To manage the server such as System Event Logs and BMC Network Configuration settings.

Event Logs: For event log configuration and Event logs.

Exit: To exit the current screen or the BIOS Utility.



24.2 Navigation Keys

The following tables shows the Navigation Keys functions.

Navigation Key(s)	Function Description
← / →	Moves cursor left or right to select Screens
↑ / ↓	Moves cursor up or down to select items
+ / -	To change option for the selected items
<Tab>	Switch to next function
<Enter>	To bring up the selected screen
<PGUP>	Go to the previous page
<PGDN>	Go to the next page
<HOME>	Go to the top of the screen
<END>	Go to the bottom of the screen
<F1>	To display the General Help Screen
<F7>	Discard changes and exit the UEFI SETUP UTILITY
<F9>	Load optimal default values for all the settings
<F10>	Save changes and exit the UEFI SETUP UTILITY
<F12>	Print screen
<ESC>	Jump to the Exit Screen or exit the current screen

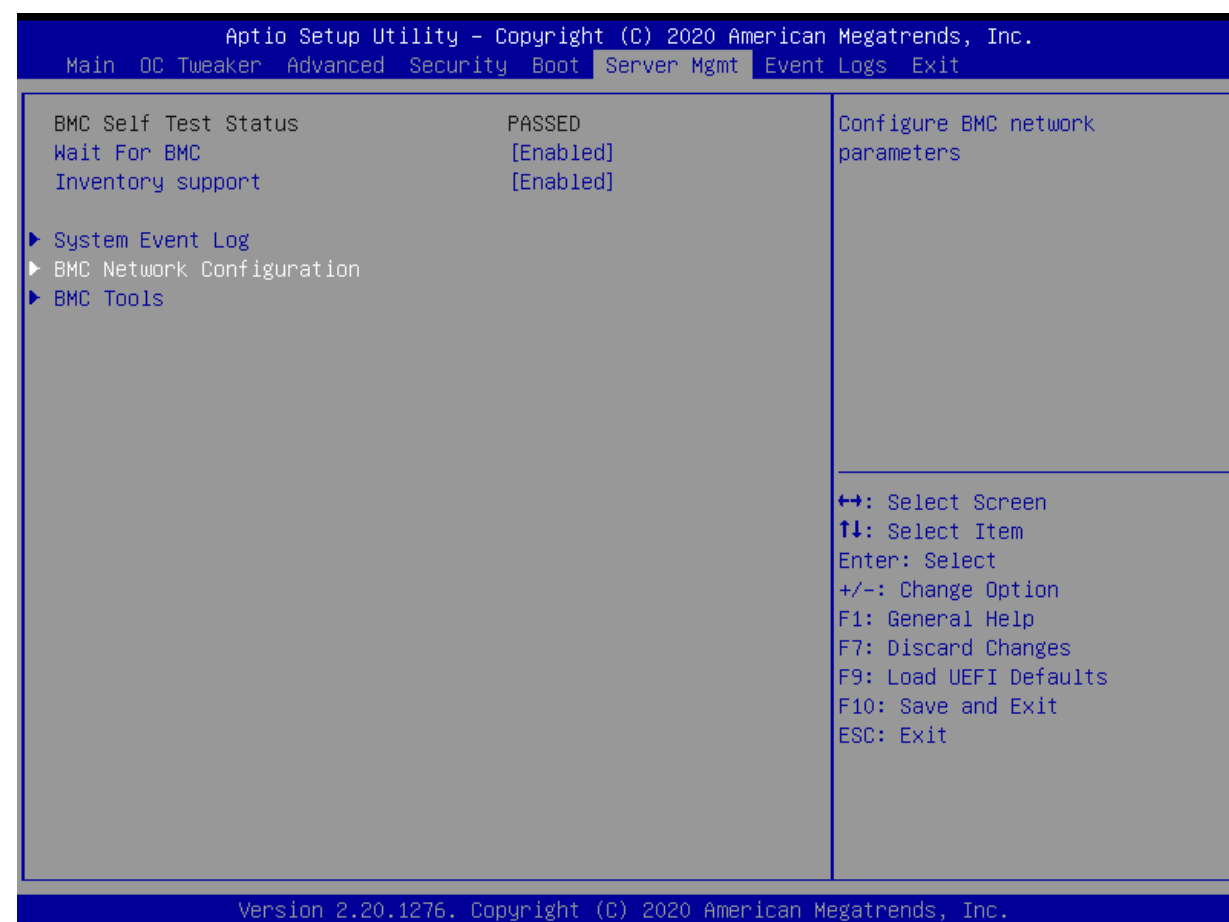
25. Configuring BMC IP-Address Settings for remote management

This section provides information on how to configure BMC IP-address settings for remote management from BIOS utility and BMC Web-GUI.

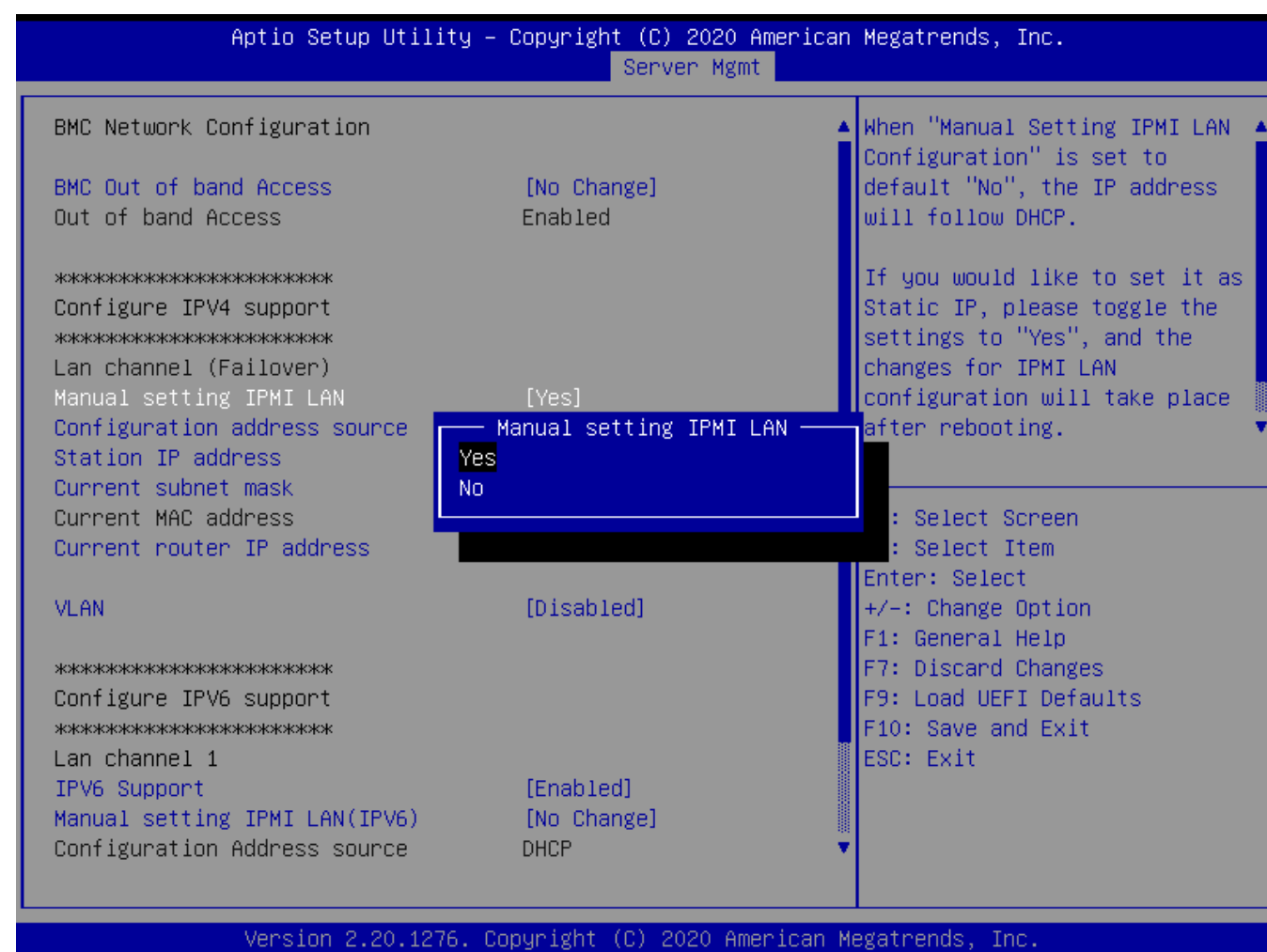
25.1 Configuring the BMC IP-Address Settings for Remote management in BIOS Utility

This section contains information on how to configure BMC IP-address settings for remote management. The BMC IP-address can be set either static or through DHCP (Default Settings).

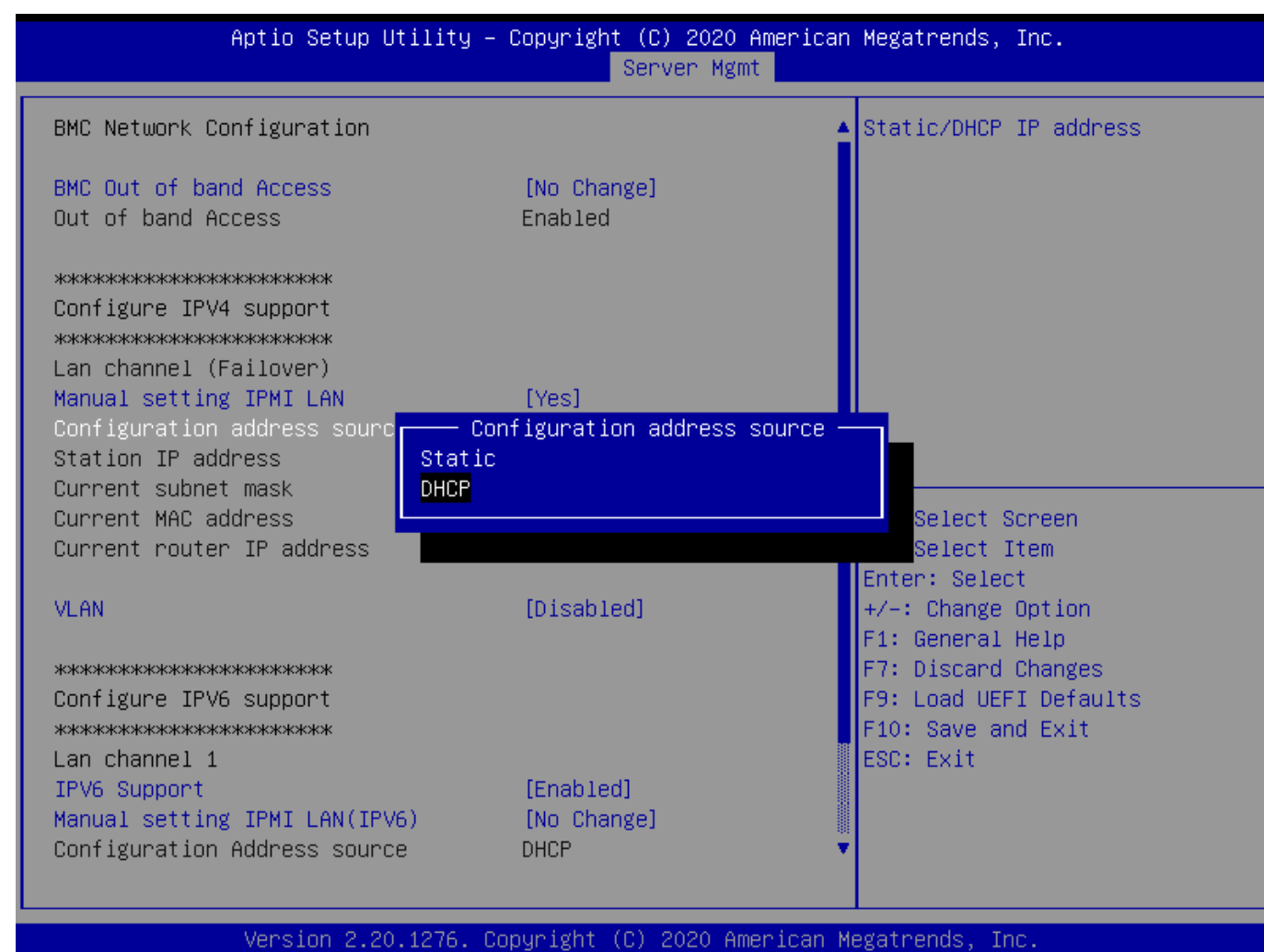
Step 1: Go in to the BIOS, In the Setup menu, under the Server Mgmt menu and then select BMC Network Configuration.



Step 2: Under the Configure IPV4 support, select the Manual setting IPMI LAN and Choose Yes to choose the IP-address manually.



Step 3: Under the Configuration address source, select either the Static or DHCP to choose the static IP-address source. If you select DHCP then IP-address assignment is done automatically and you can skip the later steps and press F10 to save changes and Exit to reboot the machine.



Step 4: If the Static IP selected then enter the values for the Station IP address, Current Subnet mask and Current Router IP address. Press F10 to Save and Exit to reboot the machine.

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Server Mgmt

BMC Network Configuration

BMC Out of band Access

[No Change]

Out of band Access

Enabled

Configure IPV4 support

Lan channel (Failover)

Manual setting IPMI LAN

[Yes]

Configuration address source

[Static]

Station IP address

0.0.0.0

Current subnet mask

Current MAC address

Current router IP address

VLAN

[Disabled]

Configure IPV6 support

Lan channel 1

IPV6 Support

[Enabled]

Manual setting IPMI LAN(IPV6)

[No Change]

Configuration Address source

DHCP

Static IP Address

0.0.0.0 - 255.255.255.255

↔: Select Screen

↑↓: Select Item

Enter: Select

+/-: Change Option

F1: General Help

F7: Discard Changes

F9: Load UEFI Defaults

F10: Save and Exit

ESC: Exit

Version 2.20.1276. Copyright (C) 2020 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Server Mgmt

BMC Network Configuration

BMC Out of band Access

[No Change]

Out of band Access

Enabled

Configure IPV4 support

Lan channel (Failover)

Manual setting IPMI LAN

[Yes]

Configuration address source

[Static]

Station IP address

172.29.2.11

Current subnet mask

255.255.0.0

Current MAC address

D0-50-99-F2-52-A5

Current router IP address

172.29.0.2

VLAN

[Disabled]

Configure IPV6 support

Lan channel 1

IPV6 Support

[Enabled]

Manual setting IPMI LAN(IPV6)

[No Change]

Configuration Address source

DHCP

Router IP address from BMC

↔: Select Screen

↑↓: Select Item

Enter: Select

+/-: Change Option

F1: General Help

F7: Discard Changes

F9: Load UEFI Defaults

F10: Save and Exit

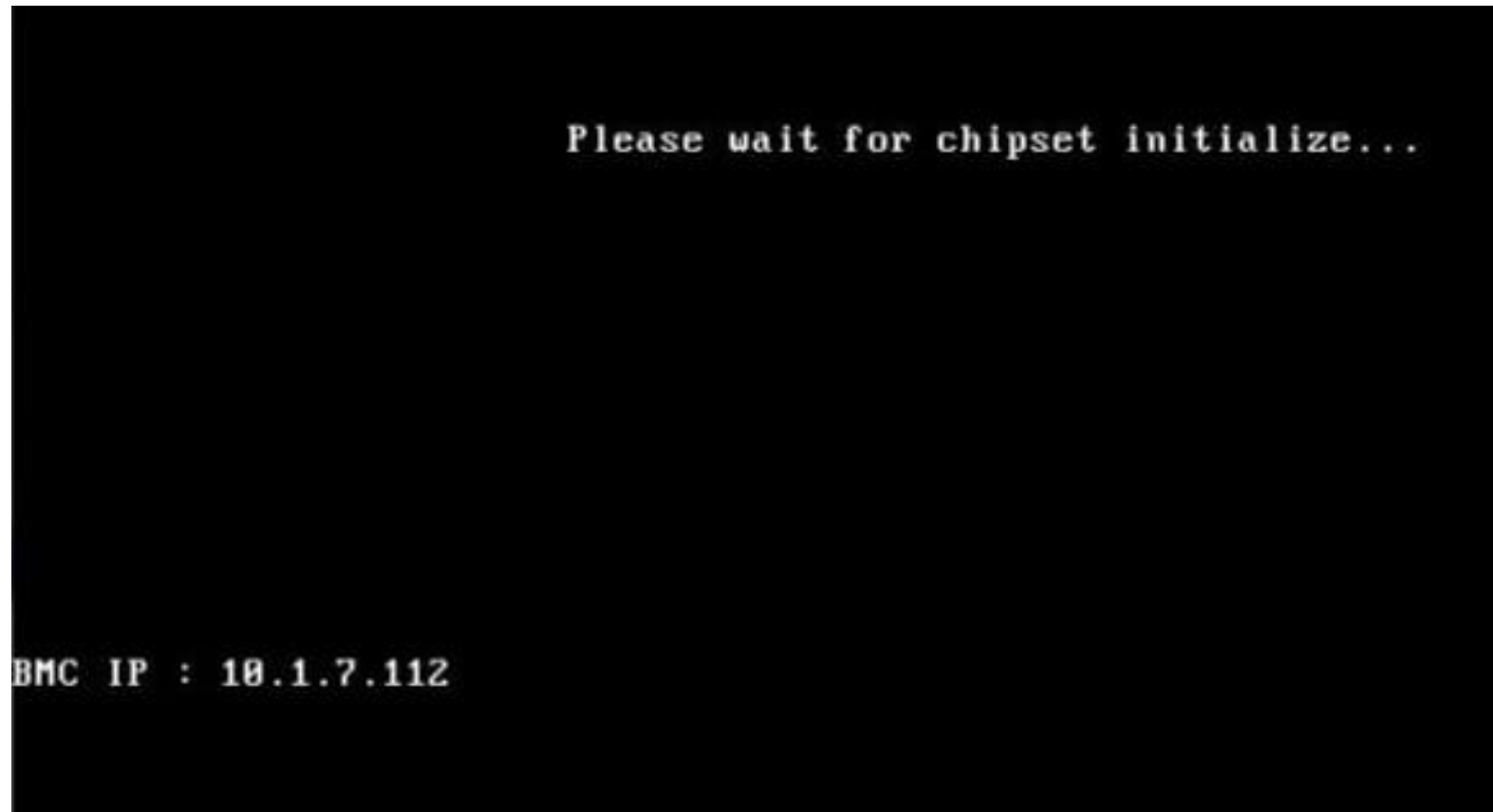
ESC: Exit

Version 2.20.1276. Copyright (C) 2020 American Megatrends, Inc.

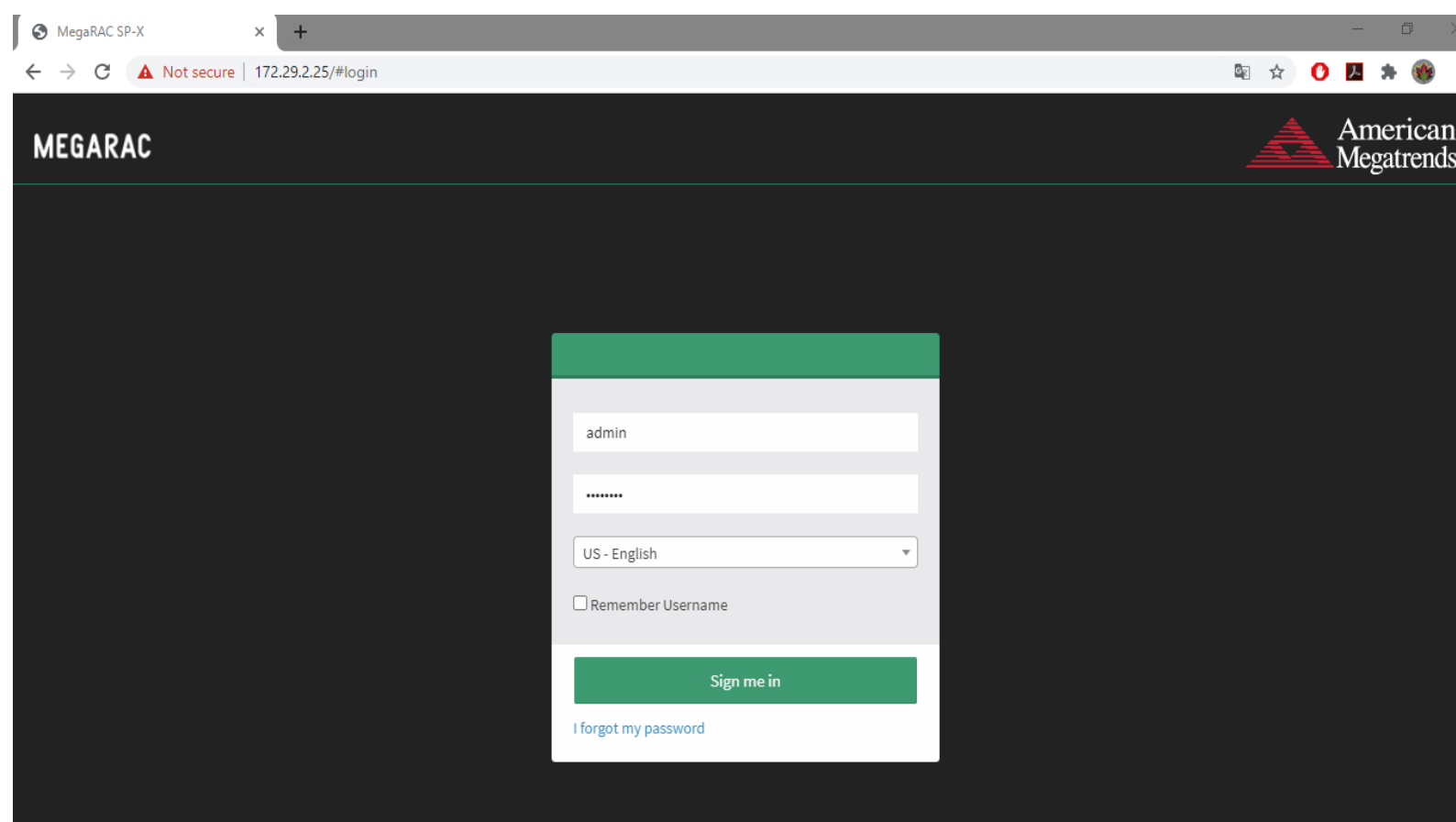
25.2 Configuring the Static BMC IP-Address Settings for Remote management in BMC Web-GUI

This section contains information on how to set a Static BMC IP-address settings for remote management in the BMC Web GUI.

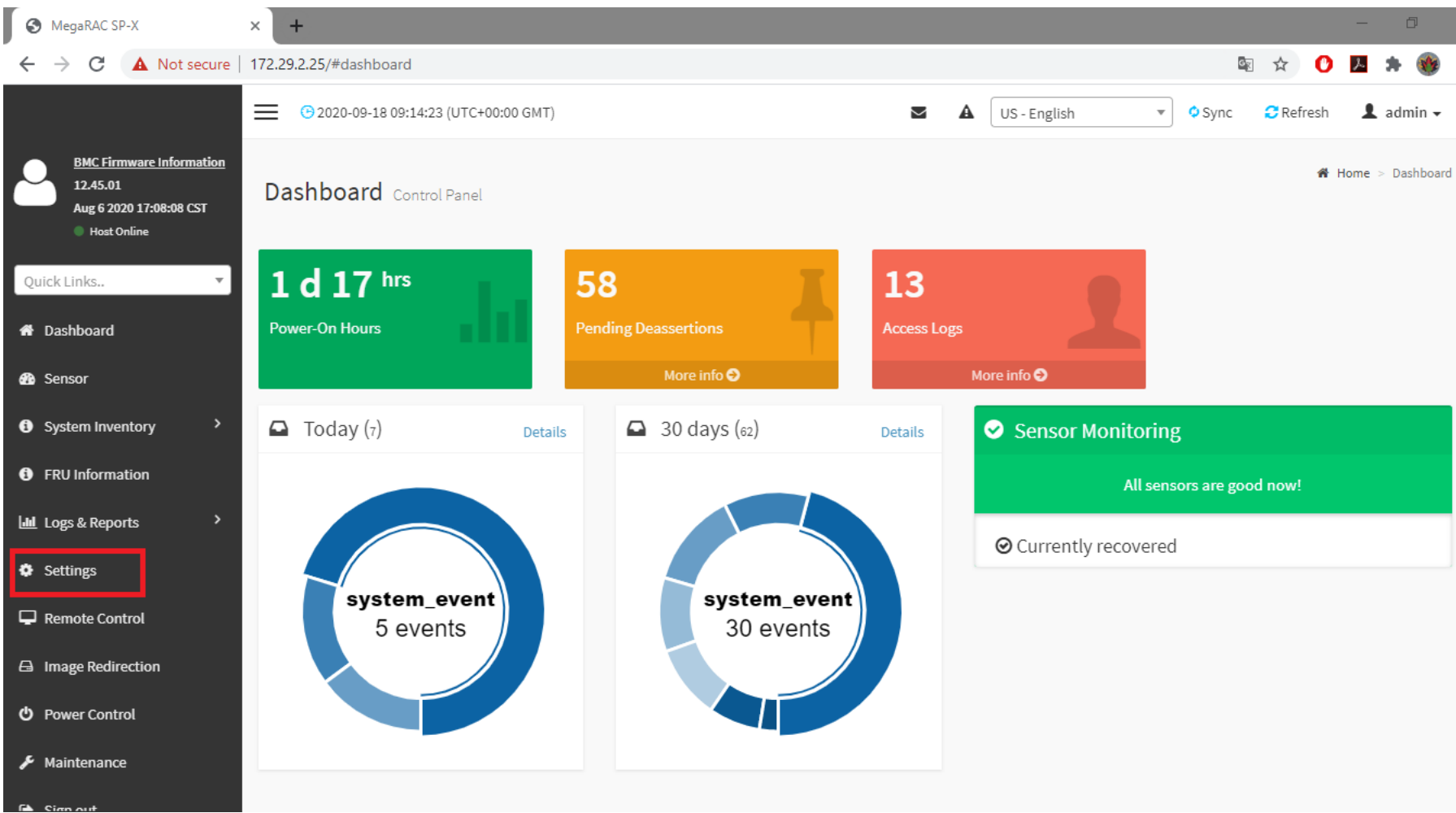
Step 1: In order to configure the Static IP-address through BMC Web-GUI, Turn ON the system and note down the BMC IP as seen below.



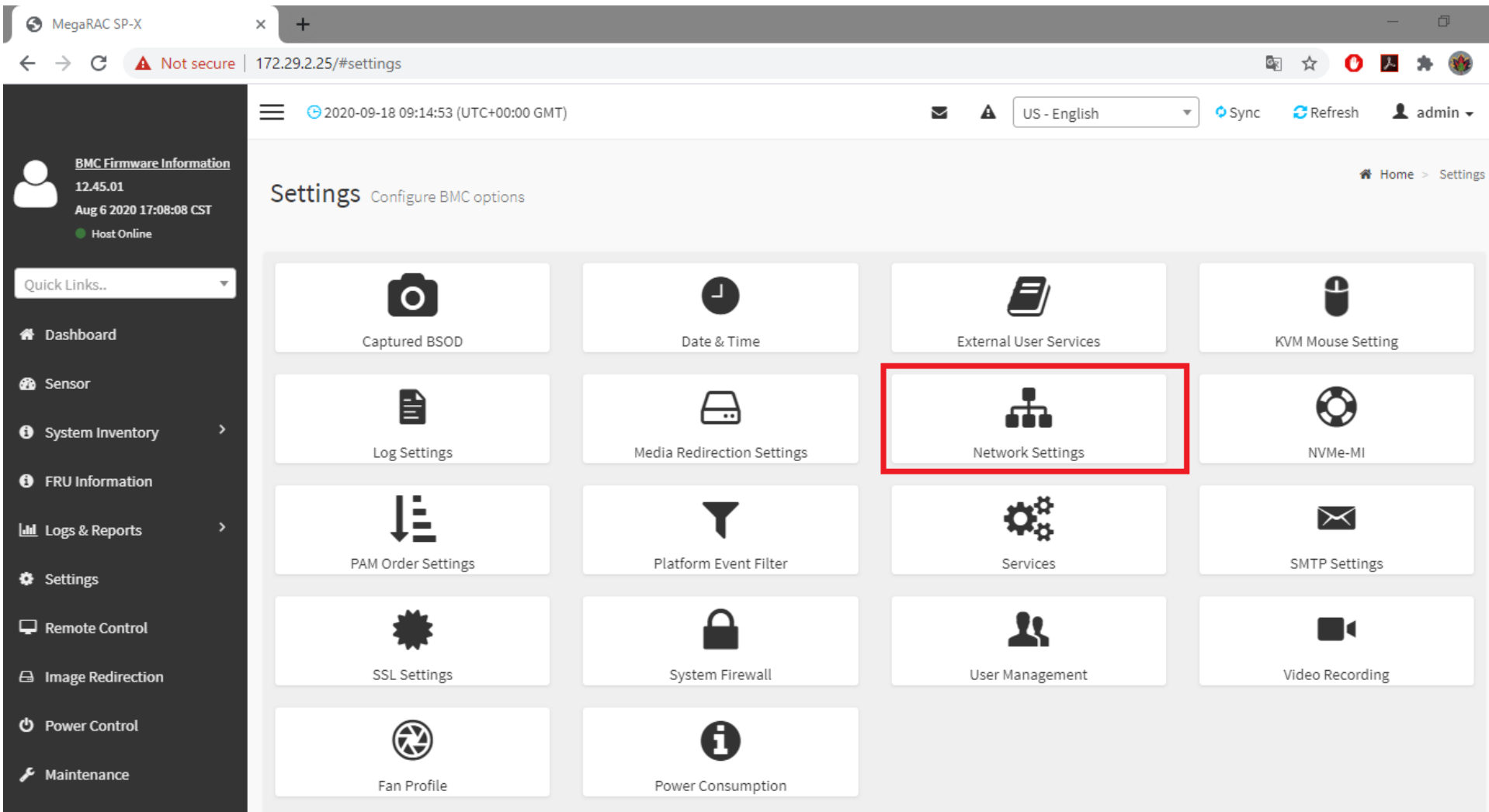
Step 2: Launch the web browser, Type the current IP-address of the BMC, and enter the **username** as **admin** and **password** as **admin**. Then click on **Sign me in**



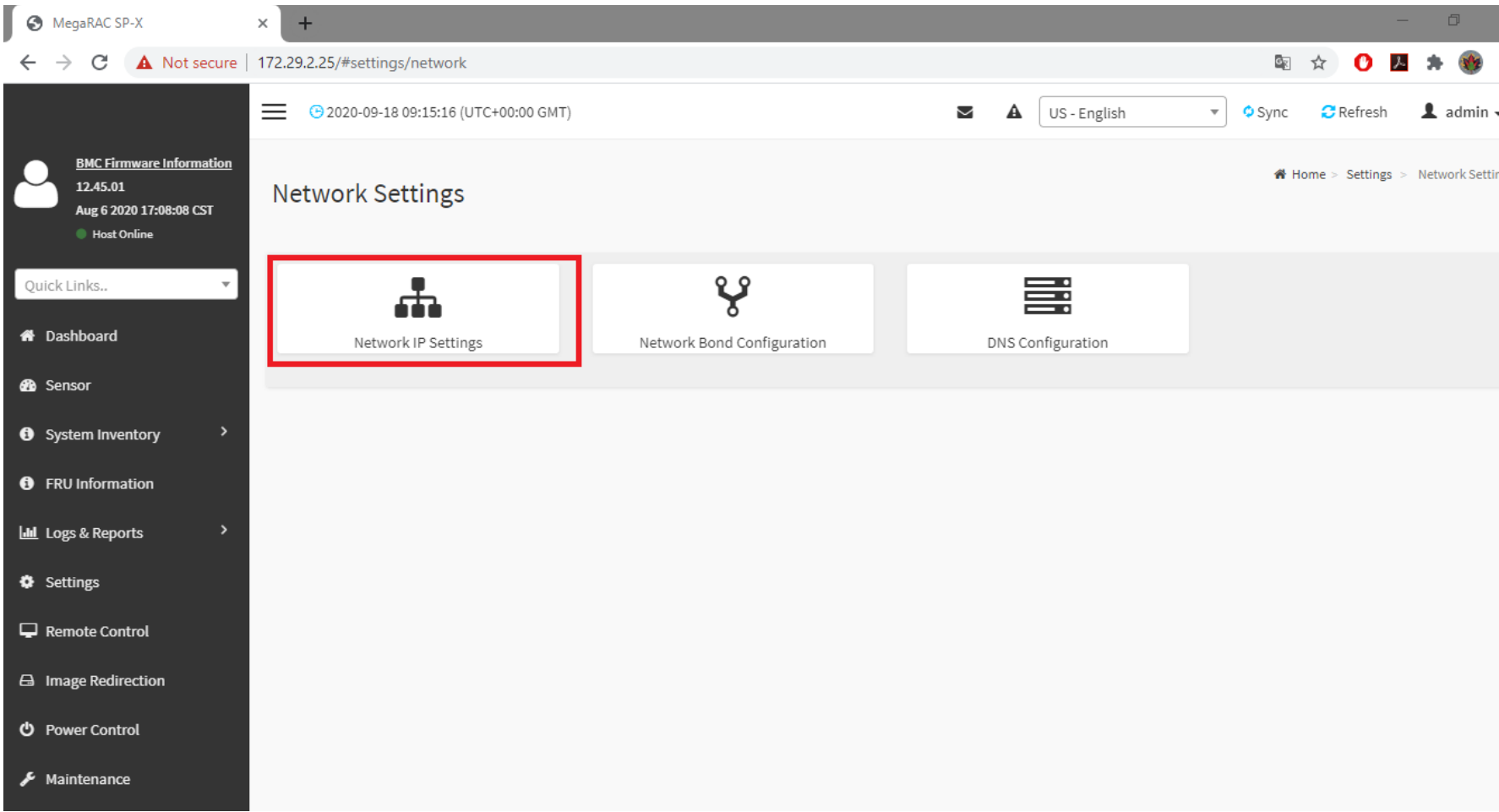
Step 3: When main menu of BMC appears then click on the **Settings**



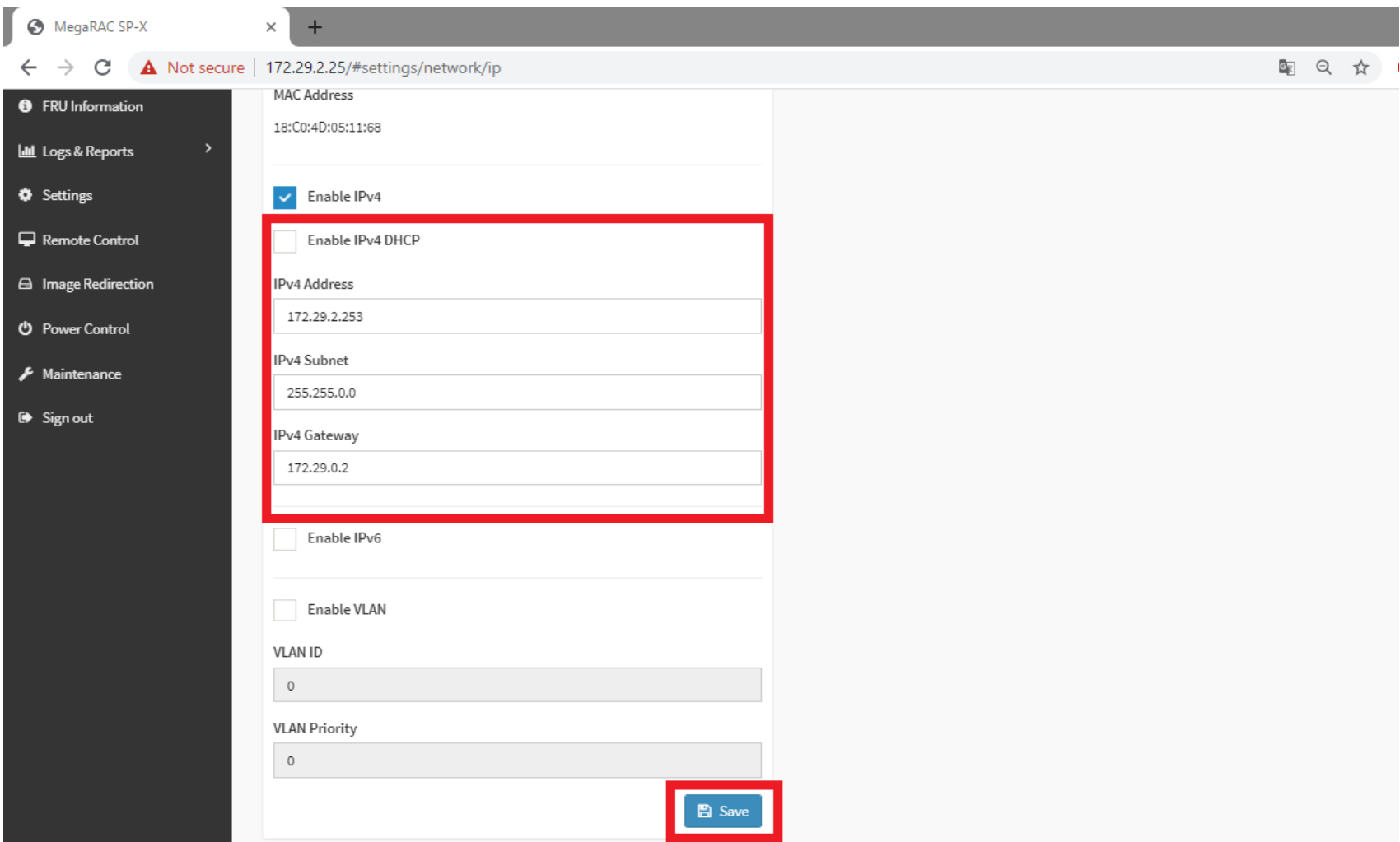
Step 4: Select the Network Settings



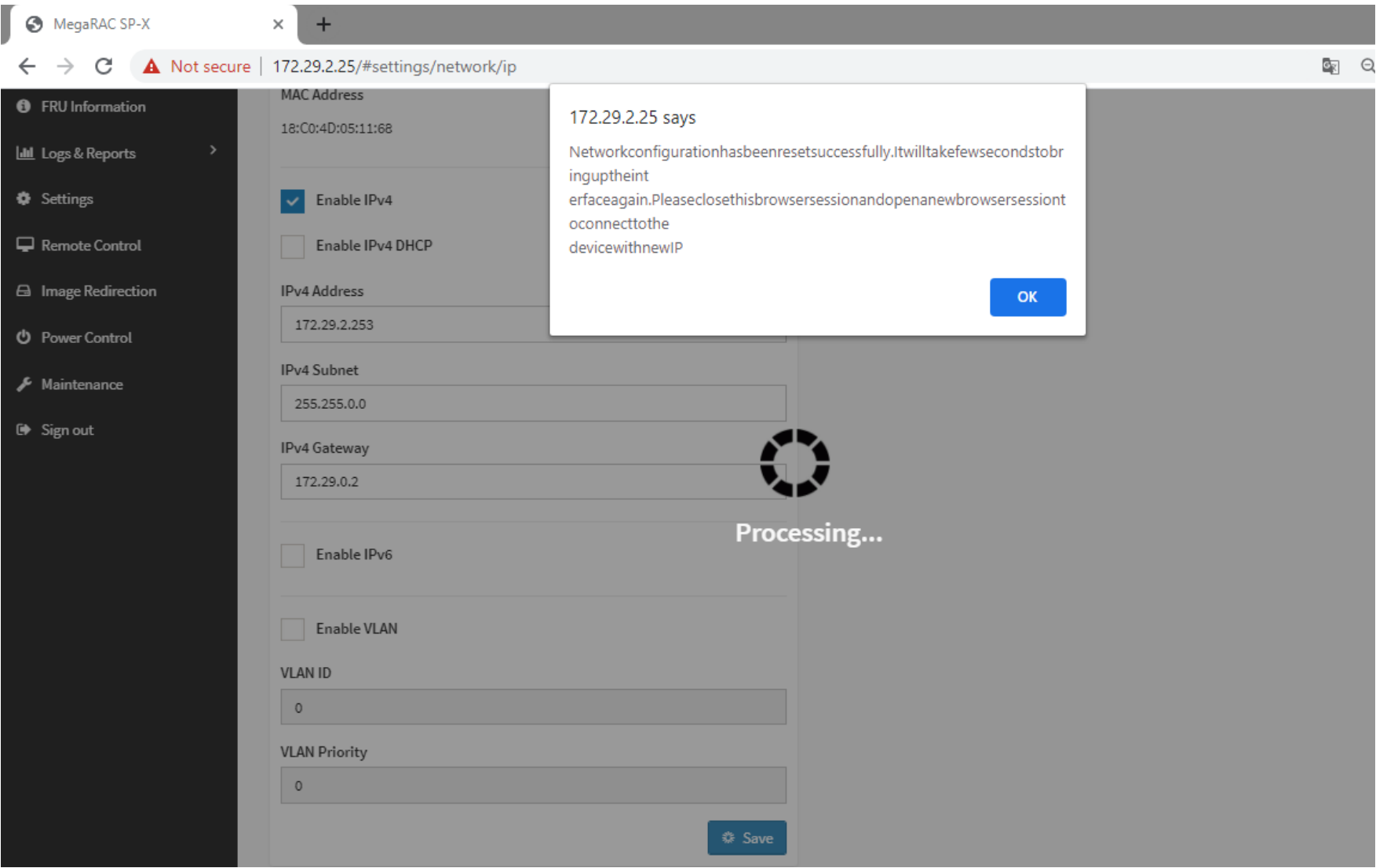
Step 5: Select the Network IP Settings



Step 6: Uncheck the Enable IPv4 DHCP, then enter the IPv4 Address, IPv4 Subnet and IPv4 Gateway and then click on Save



Step 7: Click on OK and close the browser tab or browser. Launch the browser or new tab with the new BMC IP Address to verify if the changes has been successful.



26. Using the BMC (IPMI) Web User Interface

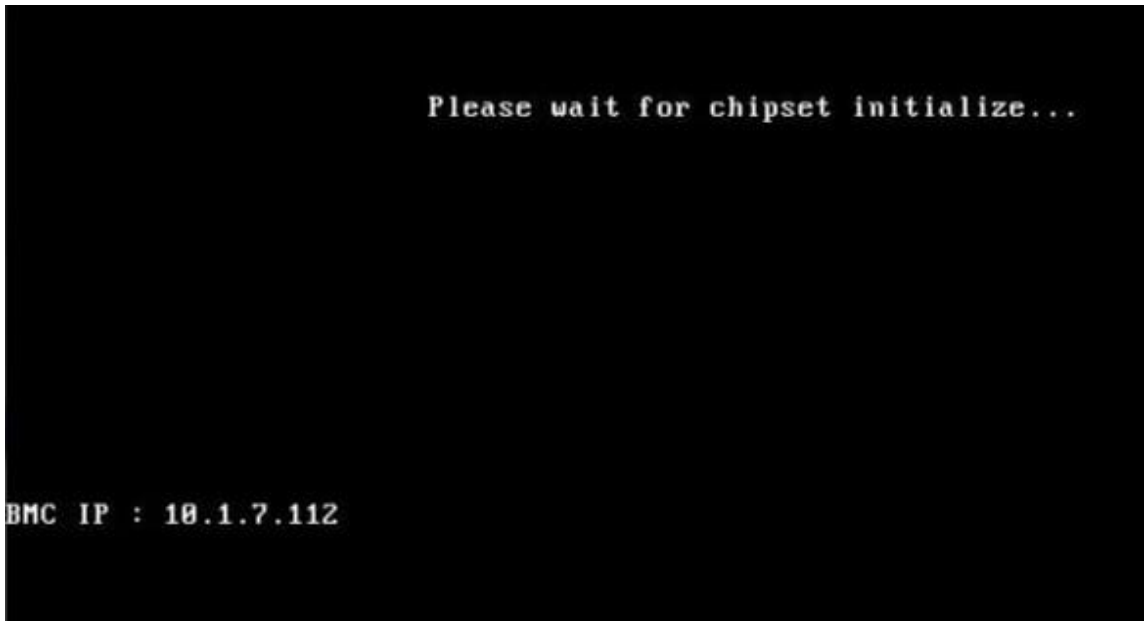
The BMC (IPMI) Web user interface (GUI) provides an interface to access BMC (IPMI) Management Console which is used to configure, monitor and administer the ORION HF210-G5 systems. This Web-based GUI is supported on the following web browsers.

Supported Browsers:

- Chrome latest version.
- IE11 and above.
- Firefox (with limited support).

27. Accessing the BMC (IPMI) Management Console

In order to access the Management Console, Turn ON the system and note down the BMC (IMPI) IP address as seen below.



Open the browser, type in the BMC (IPMI) IP address, you must have a valid **Username** and a **Password**. Both fields are required.

A login page for ASROCKRACK. It has a green header with the text "ASROCKRACK". Below the header are two input fields for "Username" and "Password". There is a checkbox labeled "Remember Username". A green button labeled "Sign me in" is below the password field. Below the button is a link "I forgot my password". At the bottom is a "Language" dropdown menu with "English" selected.

Login Page

The default **username** and **password** are both “**admin**”.

 **Note:** When you log in using the root user name and password, you have full administrative powers. The recommendation is that once you log in, you change the root password.

Username: Enter your username in this field.

Password: Enter your password in this field.

Remember Username: Check this option to remember your login credentials.

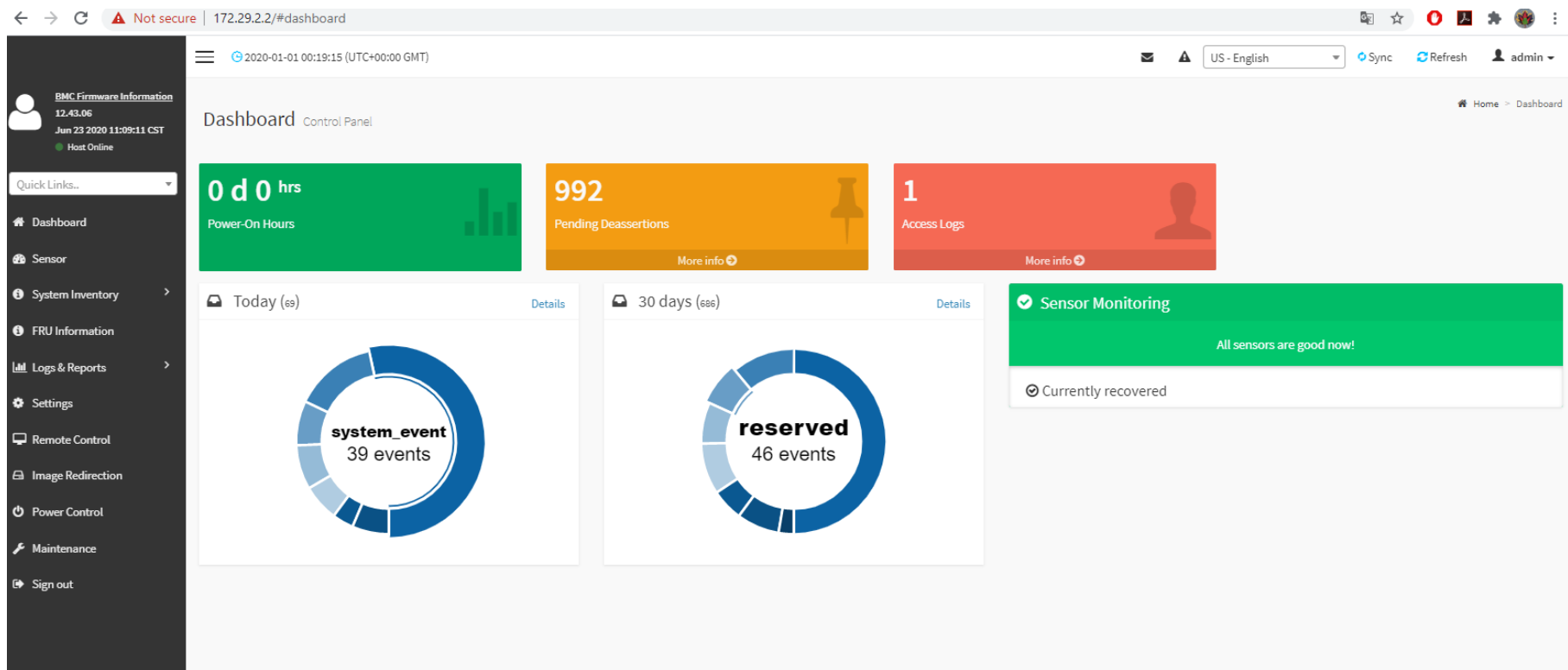
Sign me in: After entering the required credentials, click the Sign me in to login to Web GUI.

I Forgot my Password: If you forget your password, you can generate a new one using this link. Enter the username, click on Forgot Password link. This will send the newly generated password to the configured Email-ID for the user.

Language: Select the language of Web GUI, you can choose English, Traditional Chinese or Simplified Chinese.

28. Viewing and Configuring the BMC (IPMI) Management Console

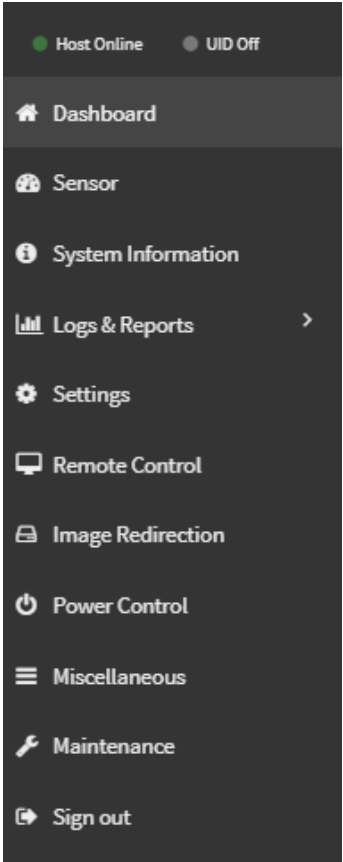
After you successfully log into your Management Console, the Remote Management Console GUI appears.



28.1 Menu bar

The **menu bar** displays the following items.

- Power Status
- Dashboard
- Sensor
- System Information
- Logs & Reports
- Settings
- Remote Control
- Image Redirection
- Power Control
- Miscellaneous
- Maintenance
- Sign out



28.2 Quick Button and Logged-in User

The user information and quick buttons are located at the top right of the Web GUI.



Quick Button and User Information

Sync: Click the button to synchronize with latest chassis state.

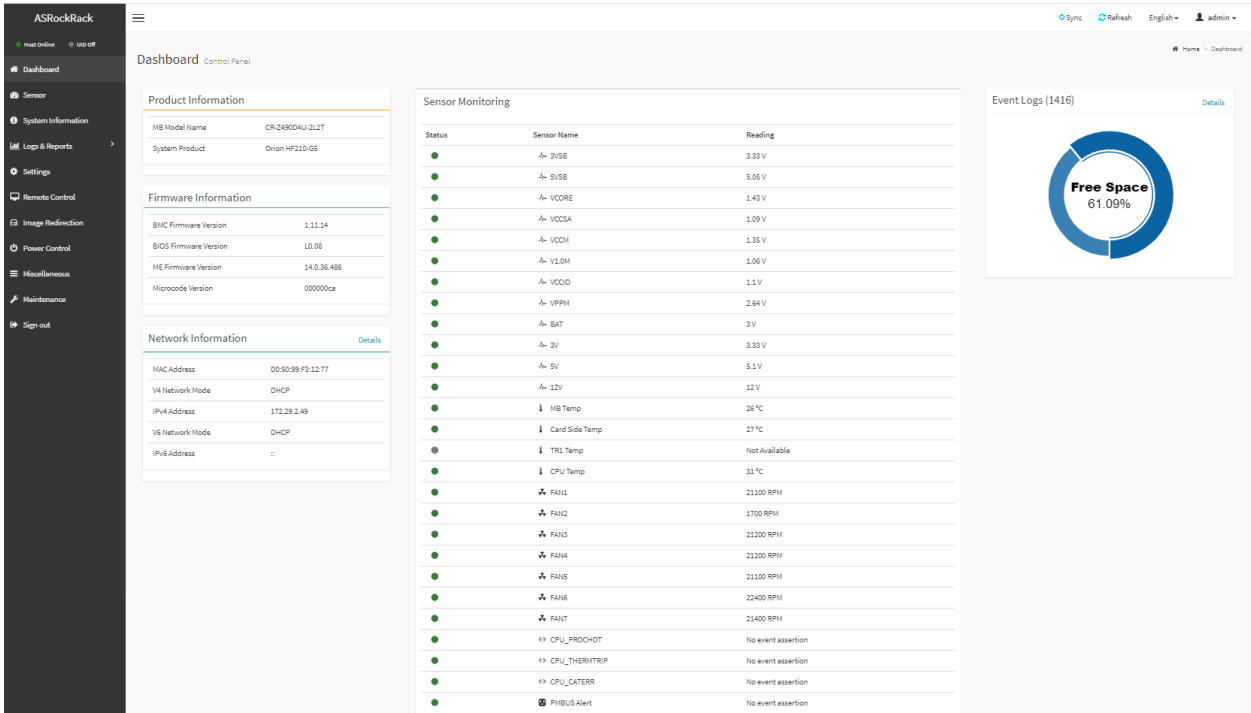
Refresh: Click the button to reload the current page.

Language: Click the option to change the language (English, Traditional Chinese or Simplified Chinese) for Web GUI.

User Information: This option shows the logged-in user name and privilege. Click **Profile** to view more information. Click the **Sign out** to log out of the Web GUI.

28.3 Dashboard

The Dashboard displays the overall information about the status of the device.



28.3.1 Product Information

The Product Information displays the following information.

MB Model Name: Displays the motherboard model name.

System Product: Displays the system product name.

28.3.2 Firmware Information

The Firmware Information displays the following information.

BMC Firmware Version: Displays the BMC firmware version of the device.

BIOS Firmware Version: Displays the BIOS firmware version of the device.

ME Firmware Version: Displays the ME (or PSP) firmware version of the device.

Microcode Version: Displays the microcode version of the device.

CPLD Version: Displays the version of CPLD of the device.

 **Note:** BIOS version, ME (or PSP) version and Microcode version will be refreshed when the system POST, please restart the system if you see nothing on screen.

28.3.3 Network Information

The Network Information of the device with the following fields is shown here. Click **Details** to view more information.

- MAC Address:** Read-only field shows the MAC address of the device.
- V4 Network Mode:** The v4 network mode of the device can be either static or DHCP.
- IPv4 Address:** The IPv4 address of the device can be static or DHCP.
- V6 Network Mode:** The v6 network mode of the device can be either static or DHCP.
- IPv6 Address:** The IPv6 address of the device can be static or DHCP.

28.3.4 Sensor Monitoring

Here lists all the available sensors on the device with the following information.

Status: This column displays the state of the device.

-  - Normal state
-  - Critical State
-  - Not Available

Sensor Name: Displays the name of the sensor.
Reading: Displays the value of sensor readings.

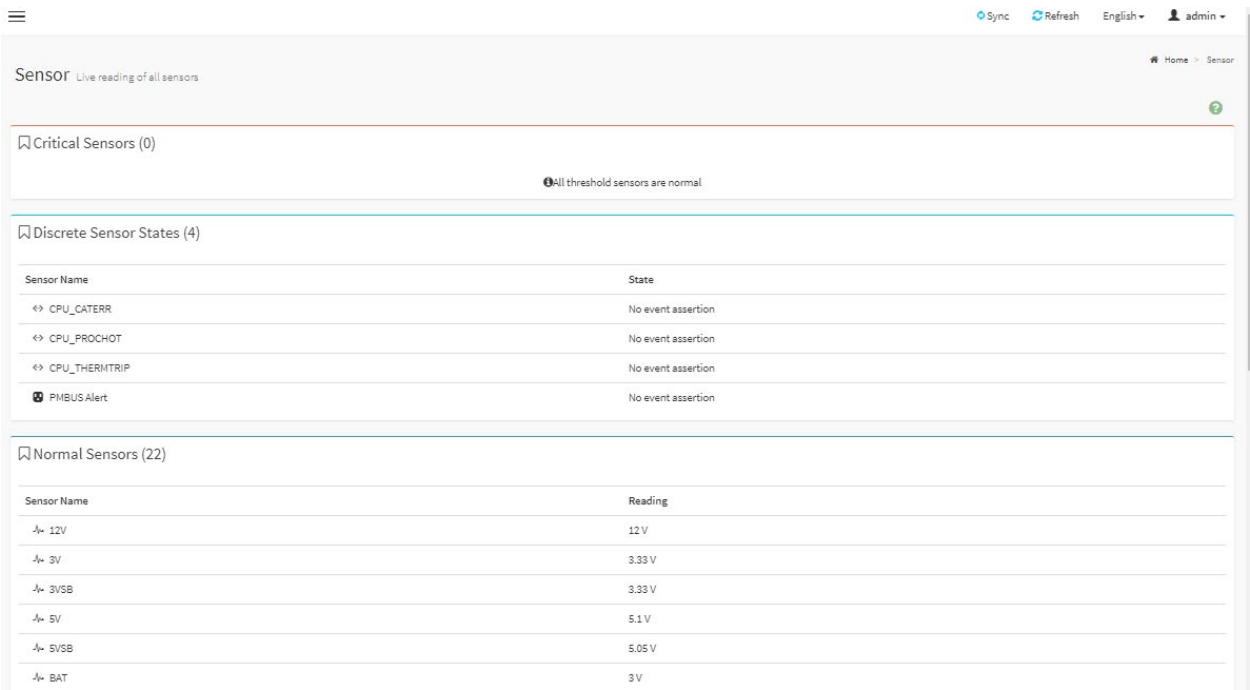
28.3.5 Event Logs

Here displays a graphical representation of all events and occupied/available space in logs. Click **Details** to view more information.

28.4 Sensors

The Sensor Readings page displays all the sensor related information.

To open the Sensor Readings page, click **Sensor** from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.

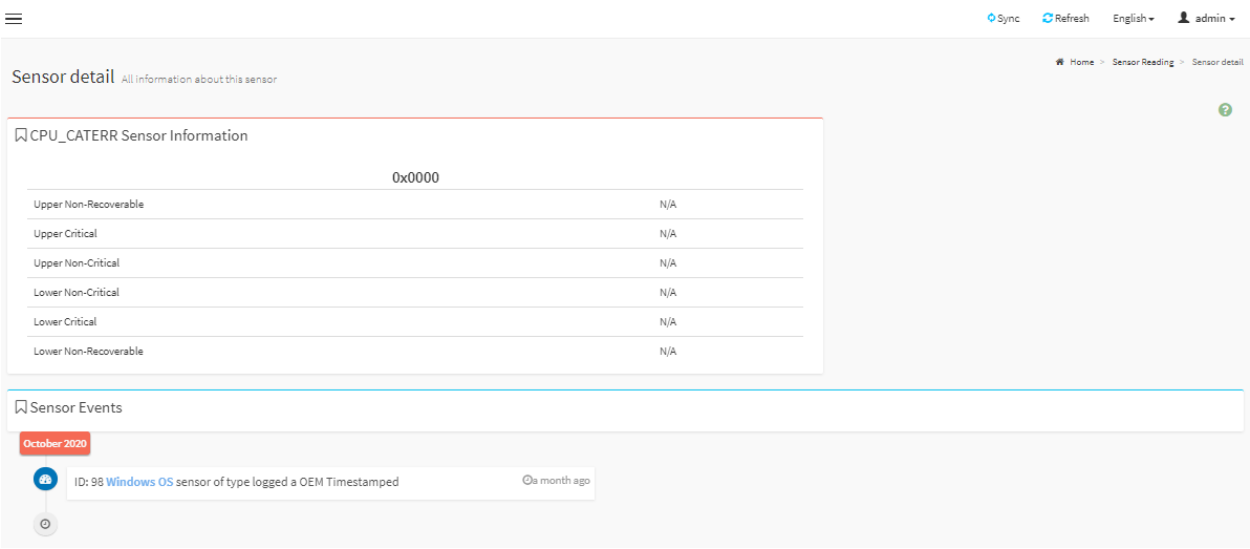


Sensor Page

In this Sensor Reading page, live readings for all the available sensors with details like Sensor Name, Status and Current Reading are shown.

28.4.1 Sensor detail:

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



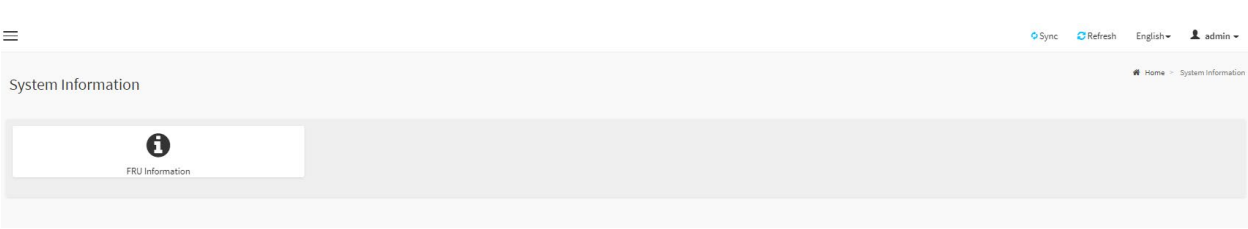
Sensor detail Page

Types of the thresholds:

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

28.5 System Information

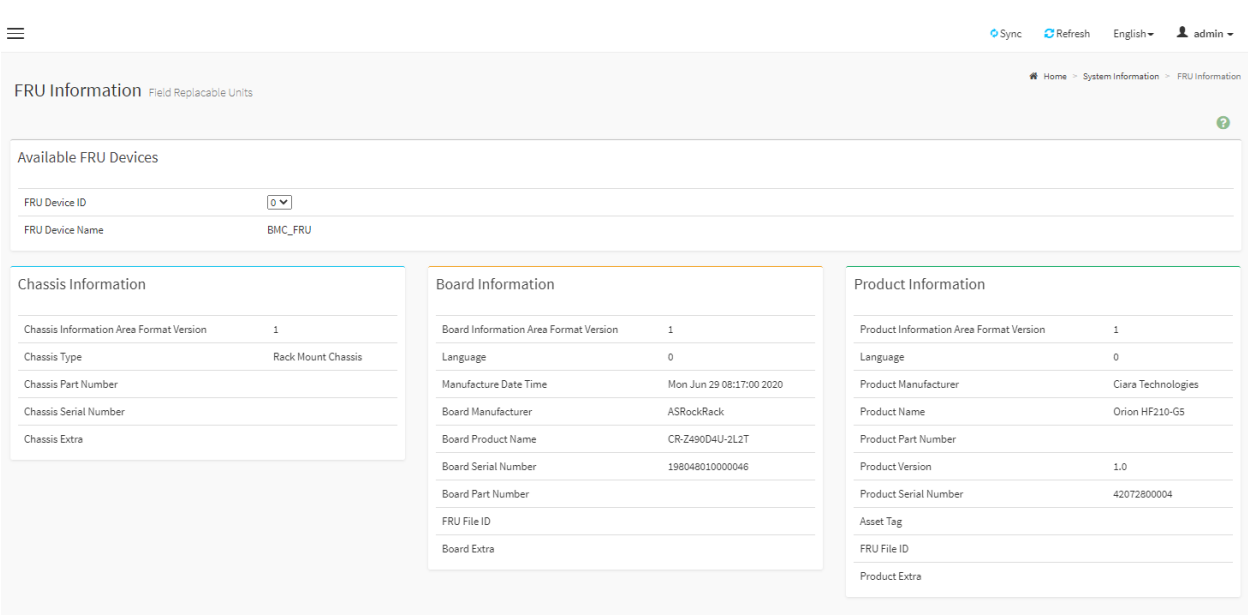
This group of pages allows you to view system information.



FRU Page

FRU Information

This page displays the FRU information. Select a FRU Device ID from the FRU Information section to view the details of the selected device.



Sensor detail Page

Available FRU Devices

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

Chassis Information

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

Board Information

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

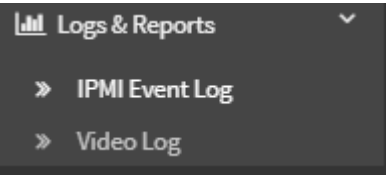
Product Information

- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Serial Number
- Product Version
- Product Serial Number
- Asset Tag

- FRU File ID
- Product Extra

28.6 Logs & Reports

This group of pages allows you to view the logs. There are two pages under the Logs & Report.



28.6.1 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.

Sync

Refresh

English

admin

IPMI Event Log

All sensor event logs

All Events

Filter by: All Sensors

IPMI Event Log: 961event entries, 20page(s)

BMC Timezone

Client Timezone

UTC Offset: GMT - 5:0

<<

<

1

>

>>

Event ID	Time Stamp	Sensor Name	Sensor Type	Description
972	11/11/2020, 13:51:30	BIOS	System Event	Timestamp Clock Synch - Asserted
971	11/11/2020, 13:51:30	Unknown	System Event	Timestamp Clock Synch - Asserted
970	Pre-init Timestamp	Unknown	System Event	Timestamp Clock Synch - Asserted
969	Pre-init Timestamp	BIOS	System Event	Timestamp Clock Synch - Asserted
968	11/11/2020, 10:58:43	BIOS	System Event	Timestamp Clock Synch - Asserted
967	11/11/2020, 10:58:43	Unknown	System Event	Timestamp Clock Synch - Asserted
966	Pre-init Timestamp	Unknown	System Event	Timestamp Clock Synch - Asserted
965	Pre-init Timestamp	BIOS	System Event	Timestamp Clock Synch - Asserted
964	11/10/2020, 13:32:16	BIOS	System Event	Timestamp Clock Synch - Asserted
963	11/10/2020, 13:32:16	Unknown	System Event	Timestamp Clock Synch - Asserted
962	Pre-init Timestamp	Unknown	System Event	Timestamp Clock Synch - Asserted
961	Pre-init Timestamp	BIOS	System Event	Timestamp Clock Synch - Asserted
960	11/10/2020, 10:31:18	BIOS	System Event	Timestamp Clock Synch - Asserted
959	11/10/2020, 10:31:18	Unknown	System Event	Timestamp Clock Synch - Asserted
958	Pre-init Timestamp	Unknown	System Event	Timestamp Clock Synch - Asserted
957	Pre-init Timestamp	BIOS	System Event	Timestamp Clock Synch - Asserted
956	11/10/2020, 08:34:49	BIOS	System Event	Timestamp Clock Synch - Asserted
955	11/10/2020, 08:34:49	Unknown	System Event	Timestamp Clock Synch - Asserted
954	Pre-init Timestamp	Unknown	System Event	Timestamp Clock Synch - Asserted
953	Pre-init Timestamp	BIOS	System Event	Timestamp Clock Synch - Asserted
952	11/10/2020, 08:27:47	Windows OS	Shutdown	Operating System: Upgrade (Planned) - A planned restart or shutdown to upgrade the operating system configuration. - Asserted
951	11/10/2020, 08:27:46	OS	OS Stop / Shutdown	OS Graceful Shutdown - Asserted
950	11/09/2020, 16:01:18	Windows OS	Boot Up	Boot Up OEM Event Record - Deasserted
949	11/09/2020, 16:01:18	OS	Base OS Boot / Installation Status	Ci boot completed - Asserted
948	11/09/2020, 15:55:13	BIOS	System Event	Timestamp Clock Synch - Asserted
947	11/09/2020, 15:55:13	Unknown	System Event	Timestamp Clock Synch - Asserted
946	Pre-init Timestamp	Unknown	System Event	Timestamp Clock Synch - Asserted
945	Pre-init Timestamp	BIOS	System Event	Timestamp Clock Synch - Asserted

Clear Event Logs

Download Event Logs

Download Event Logs Raw Data

IPMI Event Log Page

Filter By Type: The category can be 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, or TerminalMode Remote Console software Events.

Filter By Sensor: Filtering can be done with the sensors mentioned in the list.

BMC Timezone: Displays the events with BMC UTC Offset timestamp.

Client Timezone: Displays the events with Client UTC Offset timestamp.

UTC Offset: Displays the current UTC Offset value based on which event Time Stamps will be updated.

Clear MCA Log: To delete MCA log.

Download MCA Log: To download the existing MCA log.

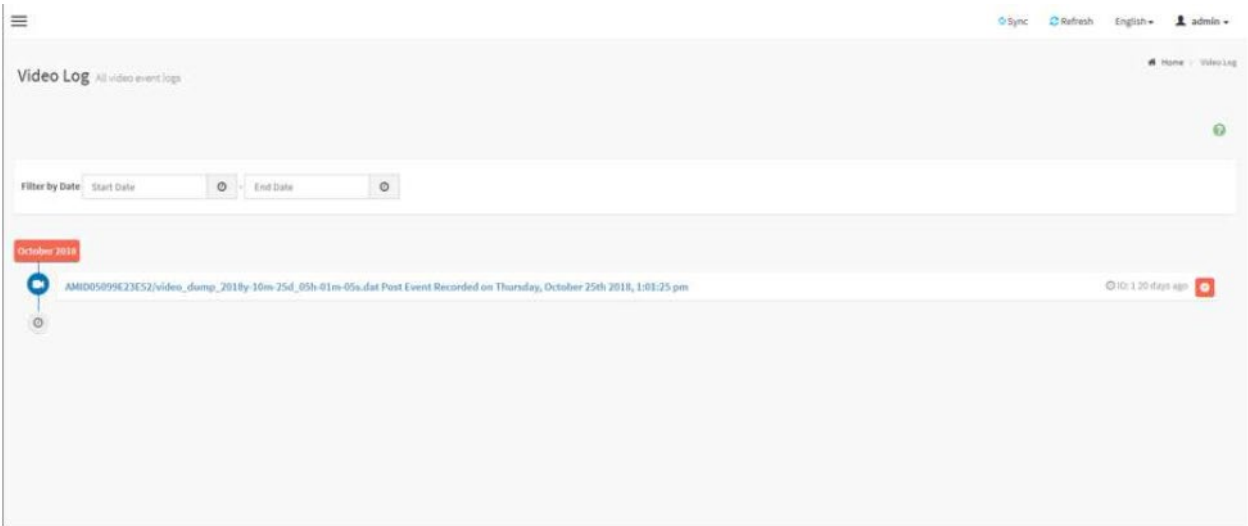
Clear Event Logs: To delete all the event logs.

Download Event Logs: To download all the existing Event Log records as text file.

Download Event Logs Raw Data: To download all the existing Event Log records as hex format file.

28.6.2 Video Log

This page displays the list of video logs occurred by the different events on this device.

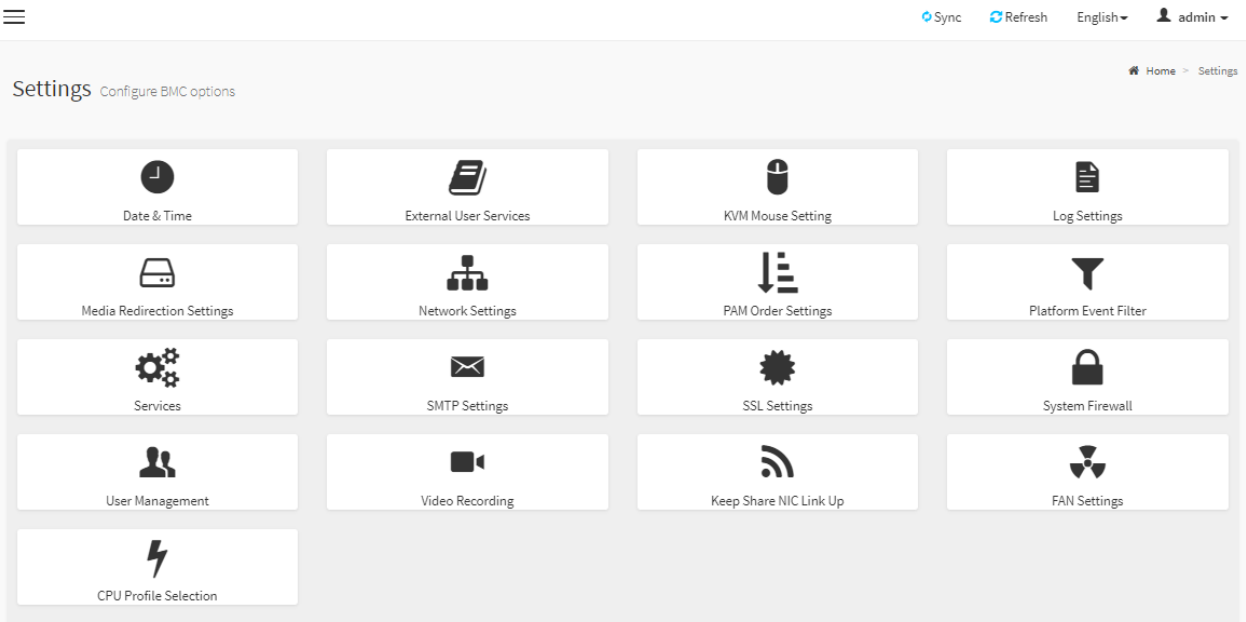


Video Log Page

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

28.7 Settings

This group of pages allows you to access various configuration settings.



Settings Page

28.7.1 Data & Time

This page allows administrator to set the date and time on the BMC. It can be used to configure either Date & Time or NTP (Network Time Protocol) server settings for the device.

SyncRefreshEnglishadmin

Date & Time

Home>Settings>Date & Time

Configure Date & Time

Date & Time :
Nov 12, 2020 4:27:08 PM

Timezone :
GMT+00:00

Primary NTP Server :
pool.ntp.org

Secondary NTP Server :
time.nist.gov

Daylight Saving Time

Automatic Date & Time

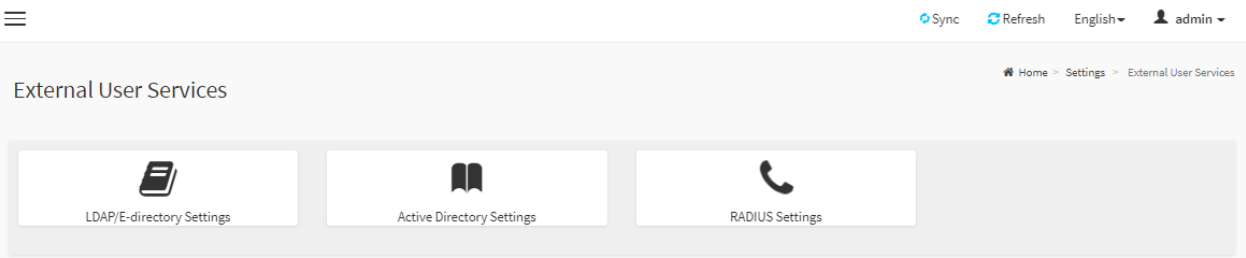
Save

Date & Time Page

- Date & Time:** To specify the current date and time of the device.
- Timezone:** Timezone list contains the UTC offset along with the locations and Manual UTC offset for NTP server, which can be used to display the exact local time.
- Primary NTP Server:** To configure a primary NTP server to use when automatically setting the date and time.
- Secondary NTP Server:** To configure a secondary NTP server to use when automatically setting the date and time.
- Daylight Saving Time:** Enable daylight saving time for the device.
- Automatic Date & Time:** To automatically synchronize Date and Time with the NTP Server.

28.7.2 External User Services

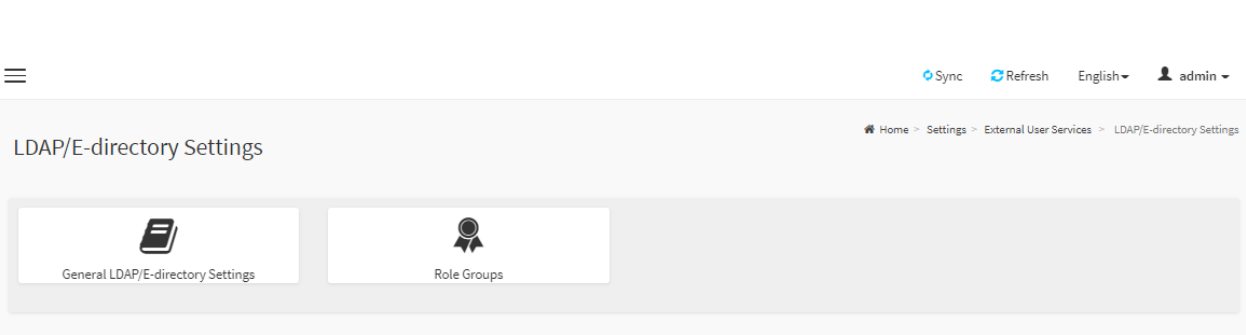
This page is used to configure the external service.



External User Services Page

28.7.2.1 LDAP/E-directory Settings

LDAP is an Internet protocol that BMC 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 web users. This is done by passing login requests to your LDAP Server.



LDAP/E-directory Settings Page

General Settings: This page is used to configure LDAP/E-Directory settings.

General LDAP/E-directory Settings

Home > Settings > External User Services > LDAP/E-directory Settings > General LDAP/E-directory Settings

Enable LDAP/E-directory Authentication

Encryption Type

Common Name Type

Server Address

Port

Bind DN

Password

Search Base

Attribute of User Login

Save

☐

No Encryption

SSL

StartTLS

IP Address

389

E.g., cn=admin,ou=login,dc=domain,dc=com

Whitespace not allowed

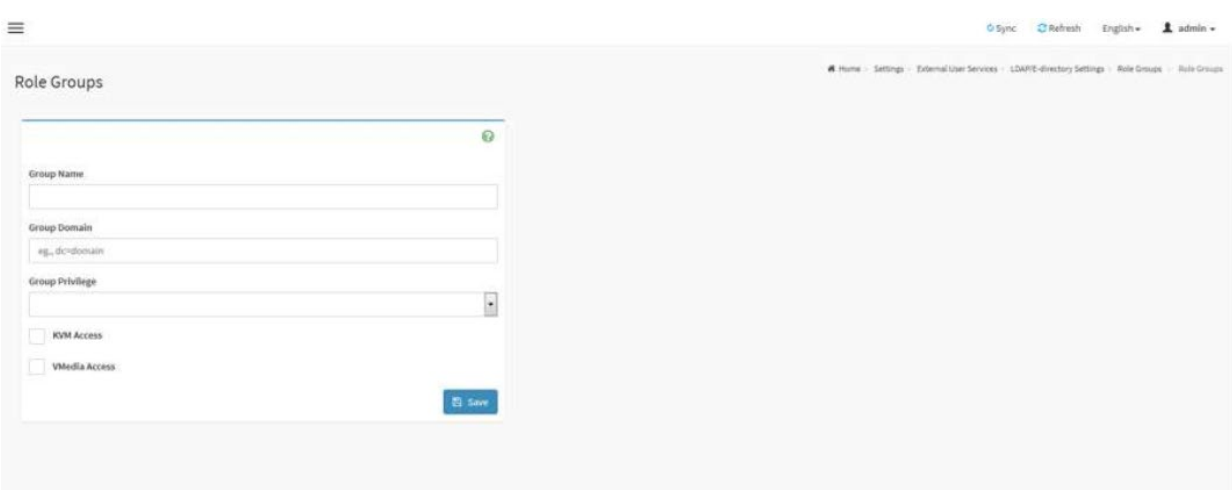
E.g., ou=login,dc=domain,dc=com

cn

General Settings Page

- Enable LDAP/E-Directory Authentication:** Check the box to enable LDAP/E-Directory authentication.
- Encryption Type:** Select the encryption type for LDAP/E-Directory.
- Common Name Type:** Select the Common Name Type for LDAP/E-Directory.
- Server Address:** The IP address (IPv4 or IPv6) of LDAP/E-Directory server.
- Port:** The port of LDA/E-Directory server.
- Bind DN:** The **Bind DN** is used during bind operation, which authenticates the client to the server.
- Password:** The password of LDA/E-Directory server.
- Search Base:** The Search base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group of external directory.
- Attribute of User Login:** To find the LDAP/E-Directory server which attribute should be used to identify the user.
- CA Certificate File:** To identify the certificate of the trusted CA certs.
- Certificate File:** To find the client certificate filename.
- Private Key:** To find the client private key filename.

Role Groups: This page is used to add a new role group to the device. Alternatively, double click on a free slot to add a role group.

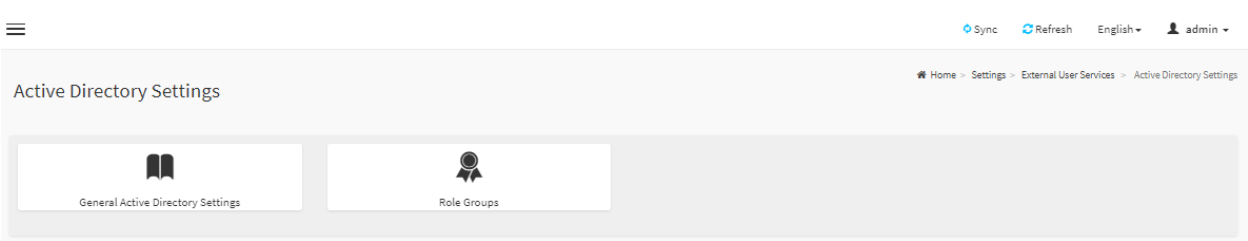


Role Groups Page

- Group Name:** Enter the name that identifies the role group.
- Group Domain:** Enter the Role Group Domain where the role group is located.
- Group Privilege:** Enter the level of privilege (User, Administrator, Operator, OEM, None) to assign to this role group.
- KVM Access:** Check the box to enable KVM access for the group.
- VMedia Access:** Check the box to enable VMedia access for the group.

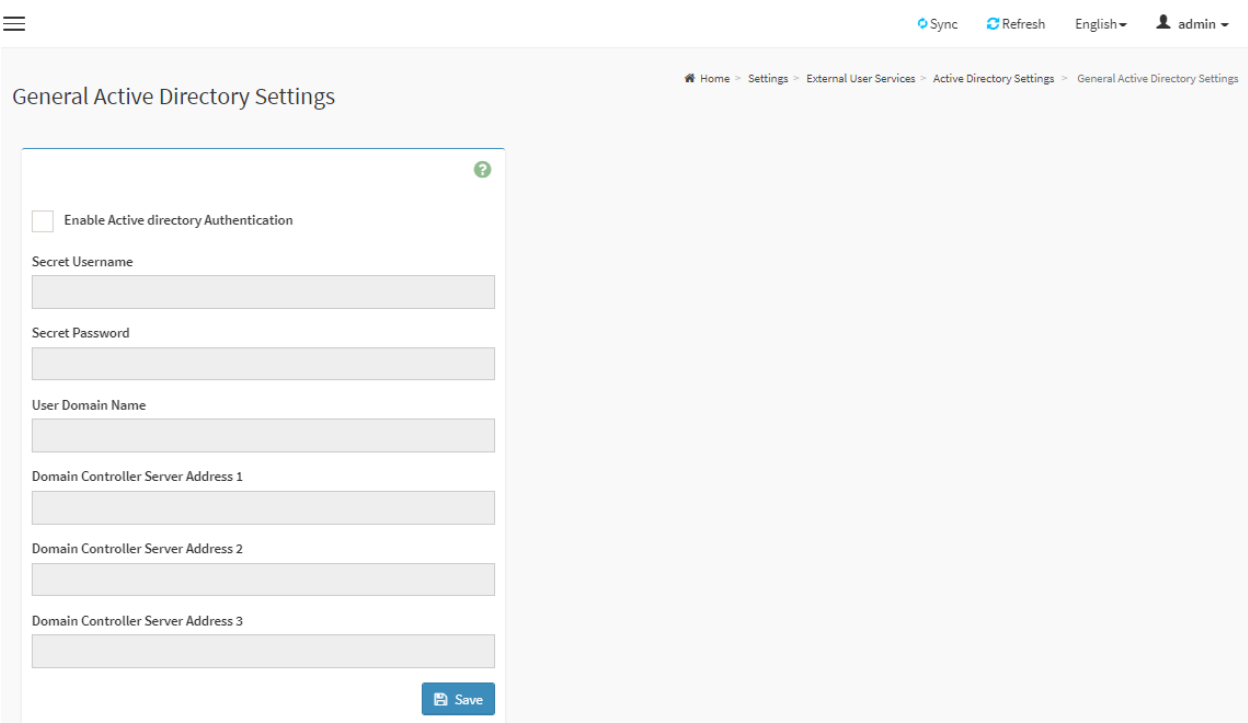
28.7.2.2. Active Directory Settings

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. 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.



Active directory Settings Page

General Settings: This page is used to configure Active Directory general settings.



General Settings Page

- Enable Active directory Authentication:** Check box to enable Active Directory Authentication.
- Secret User Name:** The Username of the Active Directory Server.
- Secret Password:** The Password of the Active Directory Server.
- User Domain Name:** The Domain Name for the user. E.g. MyDomain.com
- Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address3:** The IP address of Active Directory server.

Role Groups: This page is used to add a new role group to the device. Alternatively, double click on a free slot to add a role group.

SyncRefreshEnglishadmin

Role Groups

HomeSettingsExternal User ServicesActive Directory SettingsRole GroupsRole Groups

Group Name

Group Domain

eg., dc=domain

Group Privilege

None

☐ KVM Access

☐ VMedia Access

Save

Role Groups Page

- Group Name:** Enter the name that identifies the role group.
- Group Domain:** Enter the Role Group Domain where the role group is located.
- Group Privilege:** Enter the level of privilege (User, Administrator, Operator, OEM, None) to assign to this role group.
- KVM Access:** Check the box to enable KVM access for the group.
- VMedia Access:** Check the box to enable VMedia access for the group.

28.7.2.3. RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities. You can set the RADIUS Authentication from here.

SyncRefreshEnglishadmin

RADIUS Settings

Home>Settings>External User Services>RADIUS Settings

General RADIUS Settings

Advanced RADIUS Settings

RADIUS Settings Page

General RADIUS Settings: This page is used to configure Radius general settings.

Sync

Refresh

English

admin

Home

Settings

External User Services

RADIUS Settings

General RADIUS Settings

General RADIUS Settings

?

☐

Enable RADIUS Authentication

Server Address

Port

1812

Secret

☐

Enable KVM Access

☐

Enable VMedia Access

Save

General RADIUS Settings Page

- Enable RADIUS Authentication:** Check the box to enable Radius authentication.
- Server Address:** The IP address of Radius server.
- Port:** The port number of Radius server.
- Secret:** The authentication secret of Radius server.
- KVM Access:** Check the box to enable KVM access for Radius authenticated users.
- VMedia Access:** Check the box to enable VMedia access for Radius authenticated users.

Advanced RADIUS Settings: This page is used to configure Advanced Radius authorization setting.

SyncRefreshEnglishadmin

Advanced RADIUS Settings

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

RADIUS Authorization?

Radius configuration is not enabled.

Administrator

Operator

User

OEM Proprietary

No Access

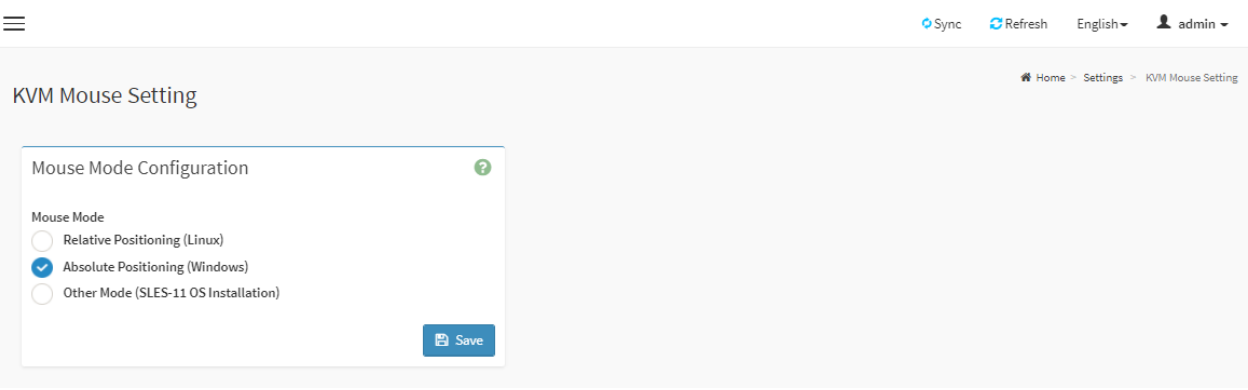
Save

Advanced RADIUS Settings Page

- Administrator:** Configure Administrator with Vendor Specific Attribute in Server side.
- Operator:** Configure Operator with Vendor Specific Attribute in Server side.
- User:** Configure User with Vendor Specific Attribute in Server side.
- OEM Proprietary:** Configure OEM Proprietary with Vendor Specific Attribute in Server side.
- No Access:** Configure No Access with Vendor Specific Attribute in Server side.

28.7.3 KVM Mouse Settings

The Redirection Console handles mouse emulation from local window to remote screen in either of three methods.

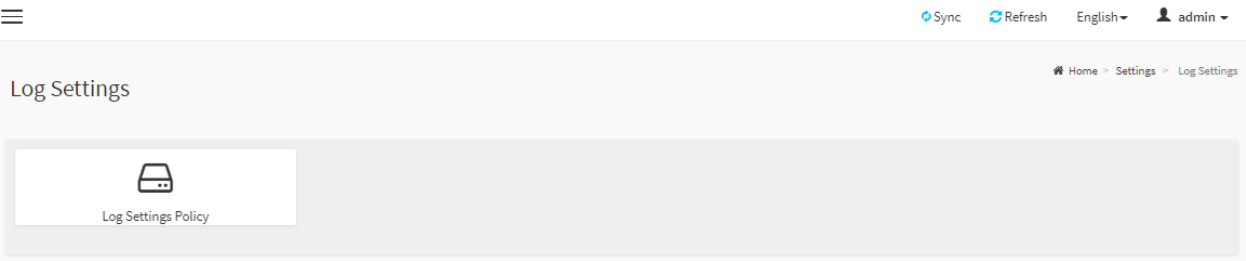


KVM Mouse Setting Page

- Relative Positioning (Linux):** Relative mode sends the calculated relative mouse position displacement to the server.
- Absolute Positioning (Windows):** The absolute position of the local mouse is sent to the server.
- Other Mode (SLES-11 OS Installation):** To have the calculated displacement from the local mouse in the center position sent to the server.

28.7.4. Log Settings

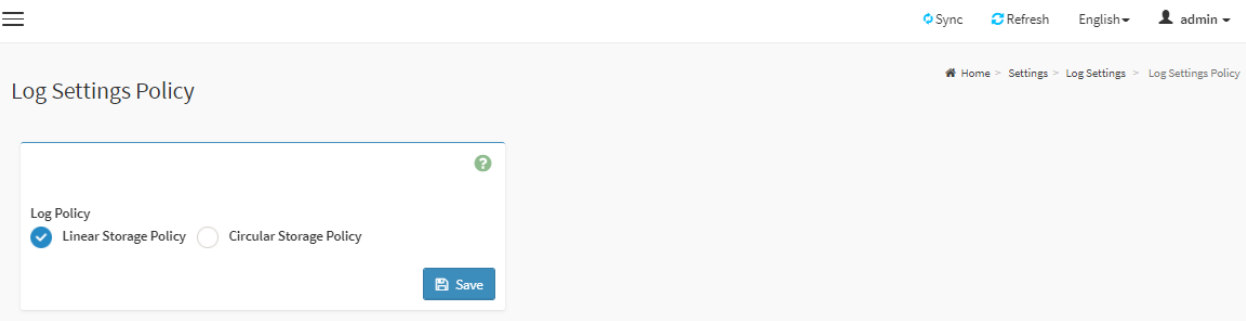
This page is used to configure the log settings.



Log Settings Page

28.7.4.1. Log Settings Policy

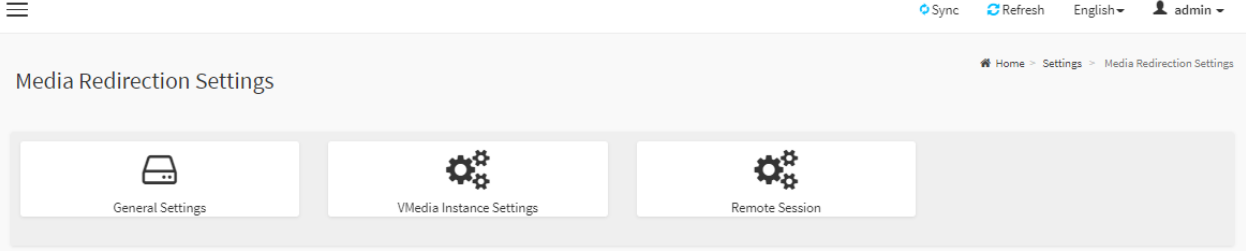
This page is used to configure the log policy for the event log.



Linear Storage Policy: Check the option to enable linear storage policy for the event log.
Circular Storage Policy: Check the option to enable circular storage policy for the event log

28.7.5. Media Redirection Settings

This page is used to configure the media into BMC for redirection.



Media Redirection Settings Page

28.7.5.1 General Settings

This page is used to configure general media settings.

Home

Settings

Media Redirection Settings

General Settings

General Settings

Remote Media Support

Mount CD/DVD

Server Address for CD/DVD Images

Server IP or Host name

Path In server

eg. /opt/bmc/nfs

Share Type for CD/DVD

nfs

cifs

Domain Name

Username

Password

Same settings for Floppy/Harddisk Images

Mount Floppy

Server Address for Floppy Images

Server IP or Host name

Path In server

eg. /opt/bmc/nfs

Share Type for Floppy

nfs

cifs

Domain Name

Username

Password

Mount Harddisk

Server Address for Harddisk Images

Server IP or Host name

Path in server

eg. /opt/bmc/nfs

Share Type for Harddisk

nfs

cifs

Domain Name

Username

Password

Save

General Settings Page

Remote Media Support: Check the box to enable Remote Media support.

Mount CD/DVD: Check the box to enable Mount CD/DVD support.

Server Address for CD/DVD Images: Displays the address of the server where the remote media images are stored.

Path in server: Displays the Source path to the remote media images.

Path in server: Displays the Share Type of the remote media server either NFS or CIFS.

Domain Name: If share Type is Samba(CIFS), then enter domain name to authenticate on the server.

Username: If share Type is Samba(CIFS), then enter username to authenticate on the server.

Password: If share Type is Samba(CIFS), then enter password to authenticate on the server.

Same settings for Floppy/Harddisk Images: Enable/Disable to select same media type data configurations for all the remote media types.

Mount Floppy: Check the box to enable Mount Floppy support.

Server Address for Floppy Images: Displays the address of the server where the remote media images are stored.

Path in server: Displays the Source path to the remote media images.

Share Type for Floppy: Displays the Share Type of the remote media server either NFS or CIFS.

Mount Harddisk: Check the box to enable Mount Harddisk support.

Server Address for Harddisk Images: Displays the address of the server where the remote media images are stored.

Path in server: Displays the Source path to the remote media images.

Share Type for Harddisk: Displays the Share Type of the remote media server either NFS or CIFS.

28.7.5.2. VMedia Instance Settings

This page is used to configure virtual media device settings.

Sync

Refresh

English

admin

Home

Settings

Media Redirection Settings

VMedia Instance Settings

VMedia Instance Settings

Floppy device instances

1

CD/DVD device instances

1

Hard disk instances

1

Save

VMedia Instance Settings Page

- Floppy device instances:** The number of floppy devices supported for Virtual Media redirection.
- CD/DVD device instances:** The number of CD/DVD devices supported for Virtual Media redirection.
- Hard disk instances:** The number of hard disk devices supported for Virtual Media redirection.
- Encrypt Media Redirection Packets:** Check the box to enable Media Encryption support.
- Power Save Mode:** To enable or disable the virtual USB devices visibility in the host. If this option is enabled, Virtual media devices will be connected to the Host machine only at the instance launching KVM session. If this option is disabled, Virtual media devices will remain connected to the host machine all the time irrespective of KVM session status.

28.7.5.3. Remote Session

This page is used to configure remote session configuration settings.

Sync

Refresh

English

admin

Home

Settings

Media Redirection Settings

Remote Session

Remote Session

☒ KVM Single Port Application

Keyboard Language

Auto Detect (AD)

Virtual Media Attach Mode

Attach

Retry Count

3

Retry Time Interval(Seconds)

10

☐ Automatically OFF Server Monitor, When KVM Launches

Save

Remote Session Page

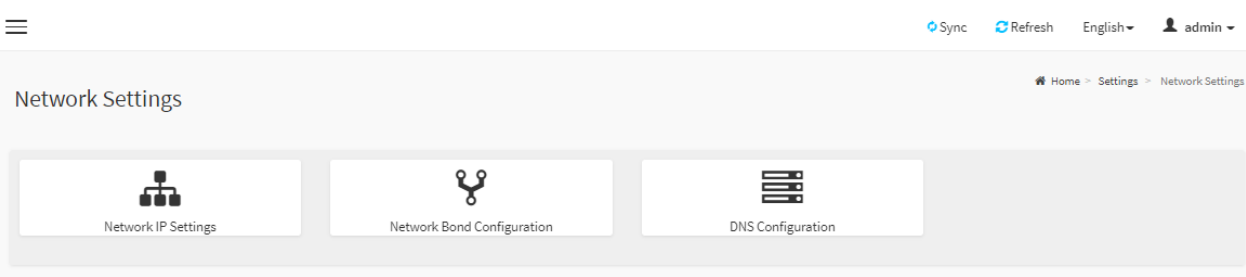
- KVM Single Port Application:** Check the box to enable single port support when using JViewer(Java KVM). On changing this configuration, KVM and VMedia Sessions will be restarted. If this support is enabled, KVM session will not use its dedicated port whereas both Web and KVM sessions will be established only via Web Port. If this support is disabled, KVM and Web sessions will use their own dedicated ports respectively.
- Enable KVM Encryption:** Check the box to enable KVM Encryption for the next redirection session when using JViewer(Java KVM). If KVM Encryption is enabled, the KVM session will use the Secure port.
- Keyboard Language:** This option is used to select the keyboard supported languages for both H5Viewer(HTML5 KVM) and JViewer(Java KVM).
- Retry Count:** This option is used to retry the redirection session for certain number of attempts.
- Retry Time Interval(Seconds):** This option is used to give time interval for each attempts.
- Automatically OFF Server Monitor, When KVM Launches:** Check the box to enable Automatically OFF Server Monitor, When KVM Launches.

Note: It will automatically close the existing remote redirection either KVM or Virtual media sessions on Single Port enable/Disable or KVM Encryption Enable/Disable.

82

28.7.6. Network Settings

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



Network Settings Page

28.7.6.1 Network IP Settings

This page is used to configure the network IP settings.

Network IP Settings

?

☒

Enable LAN

LAN Interface

bond0

MAC Address

D0:50:99:F2:52:A5

☒

Enable IPv4

☒

Enable IPv4 DHCP

IPv4 Address

172.29.2.11

IPv4 Subnet

255.255.0.0

IPv4 Gateway

172.29.0.2

☒

Enable IPv6

☒

Enable IPv6 DHCP

IPv6 Index

IPv6 Address

::

Subnet Prefix Length

0

☐

Enable VLAN

VLAN ID

0

VLAN Priority

0

Save

Network IP Settings

- Enable LAN:** Check the box to enable the selected channel.
- LAN Interface:** Lists the available LAN interfaces.
- MAC Address:** Displays the MAC Address of the device. This is a read-only field.
- Enable IPv4:** Check the box to enable the IPv4 for the selected channel.
- Enable IPv4 DHCP:** Check the box to enable IPv4 DHCP support for the selected channel.
- IPv4 Address:** Specify the static IPv4 address for the selected channel.
- IPv4 Subnet Mask:** Specify the static IPv4 subnet mask for the selected channel.

IPv4 Default Gateway: Specify the static IPv4 default gateway for the selected channel.

Enable IPv6: Check the box to enable the IPv6 for the selected channel.

Enable IPv6 DHCP: Check the box to enable IPv6 DHCP support for the selected channel.

IPv6 Index: Specify a static IPv6 Index to be configured for the selected channel. E.g.: 0

IPv6 Address: Specify a static IPv6 address to be configured to the device for the selected channel. E.g.: 2004::2010

Subnet Prefix length: Specify the subnet prefix length for the IPv6 settings.

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

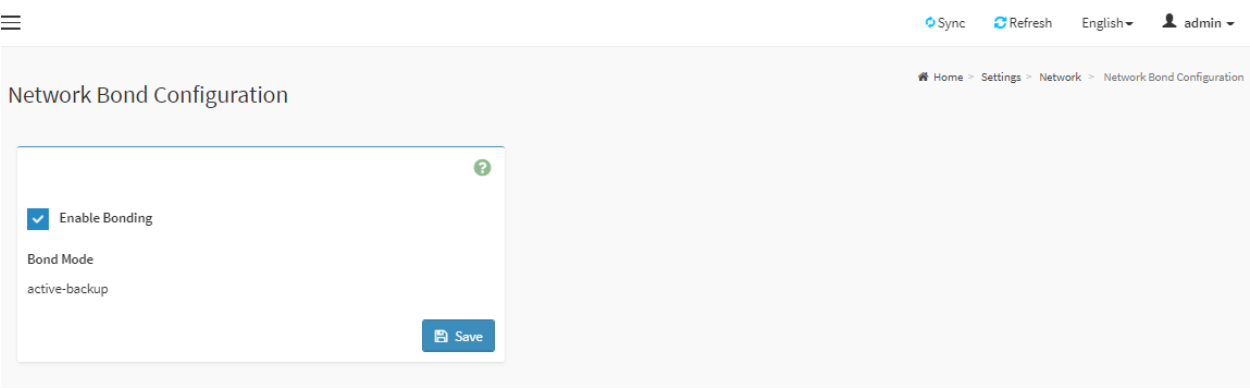
Enable VLAN: Check the box to enable the VLAN support for selected interface.

VLAN ID: The Identification for VLAN configuration.

VLAN Priority: The priority for VLAN configuration.

28.7.6.2. Network Bond Configuration

This page is used to configure the network bond configurations.

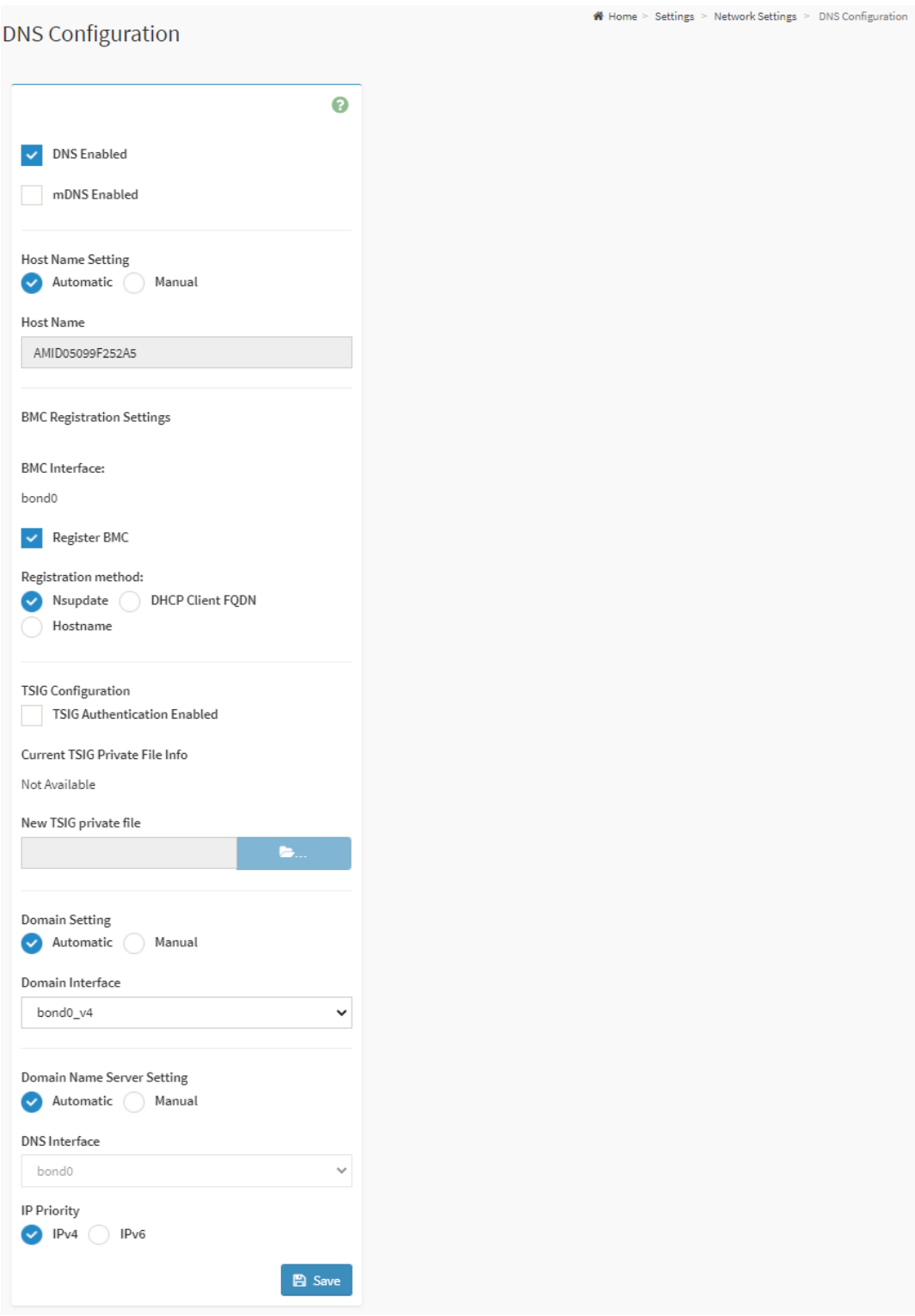


Network Bond Page

- Enable Bonding:** Check this option to enable network bonding for network interface.
- Bond Mode:** This field displays the Network bonding mode. Note: this field is not configurable.

28.7.6.3. DNS Configuration

This page is used to manage the DNS settings.



DNS Configuration Page

DNS Enabled: Check the box to enable the DNS support.

mDNS Enable: Check the box to enable the mDNS support.

Host Name Settings: Choose either Automatic or Manual settings.

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

BMC Interface: To register the BMC through the Interfaces.

Register BMC: To register BMC through registration method.

Registration Method: To register the BMC are through **NS Update** or **DHCP Client FQDN** or **Hostname**.

TSIG Authentication Enabled: Check this box to enable TSIG authentication while registering DNS via Nsupdate. Separate TSIG files can be uploaded for each LAN interface.

Current TSIG Private File: The information of Current TSIG private file along with its uploaded date/time will be displayed (read only).

New TSIG Private File: Browse and navigate to the TSIG private file, the file should be of private type.

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

Domain Interface: This field will be present if specify **Domain Setting to Automatic**, the field is used to display the domain interface of the device.

Domain Name: This field will be present if specify **Domain Setting to Manual**, the field is used to specify the domain name of the device.

Domain Name Server Setting: Select whether the DNS interface will be configured manually or automatically.

DNS Interface: This field will be present if specify **Domain Name Server Setting to Automatic**, the field is used to specify the interface to be used.

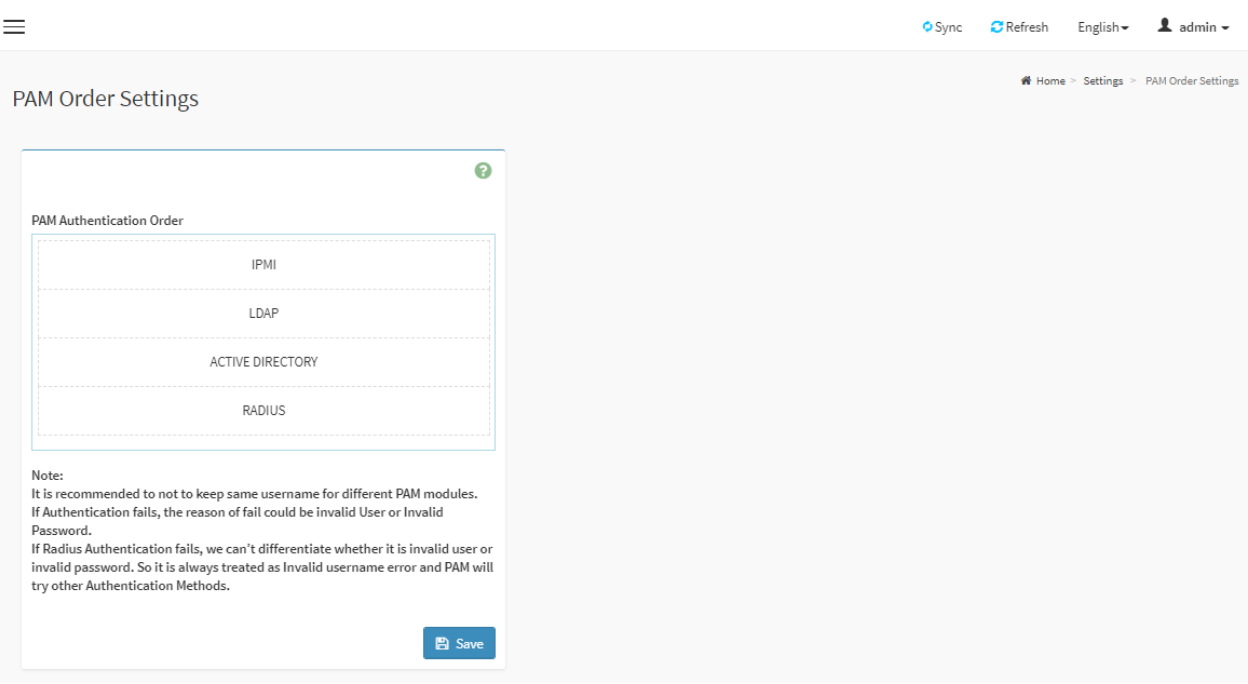
IP Priority: This field will be present if specify **Domain Name Server Setting to**

Automatic, the field is used to select the IP Priority. If IP priority is IPv4, 2 IPv4 and 1 IPv6 DNS servers are used. If IP priority is IPv6, 1 IPv4 and 2 IPv6 DNS servers are used.

DNS Server 1, 2 & 3: This field will be present if specify **Domain Name Server Setting to Manual**, the field is used to specify the DNS (Domain Name System) server address to be configured for the BMC.

28.7.7 PAM Order Settings

This page is used to configure the PAM ordering for user authentication.



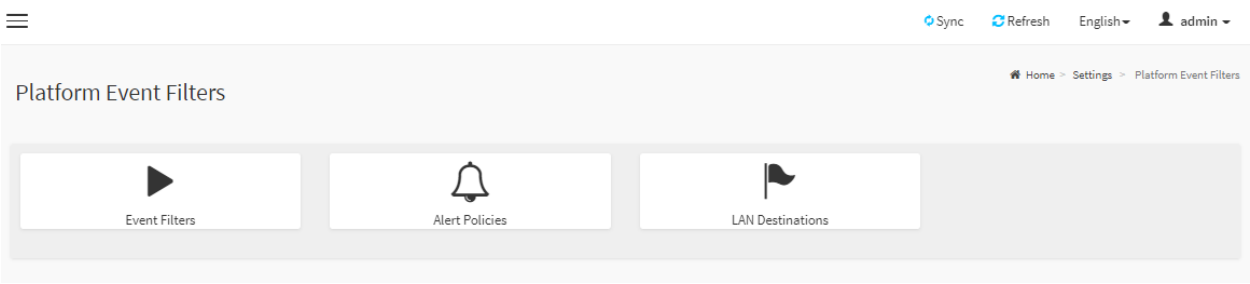
PAM Order Settings Page

PAM Authentication Order: It shows the list of available PAM modules supported in BMC. Click and Drag the required PAM module to change its order.

- Note:**
1. It is recommended not keeping the same username for different PAM modules.
 2. If Authentication fails, the reason for failure could be invalid user or invalid password.
 3. If Radius Authentication fails, we can't differentiate whether it is invalid user or invalid password. So it is always treated as Invalid username error and PAM will try other Authentication Methods.
 4. If AD contains secret username & password as empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods. So it is recommended keeping AD in the last location in PAM order.

28.7.8. Platform Event Filter

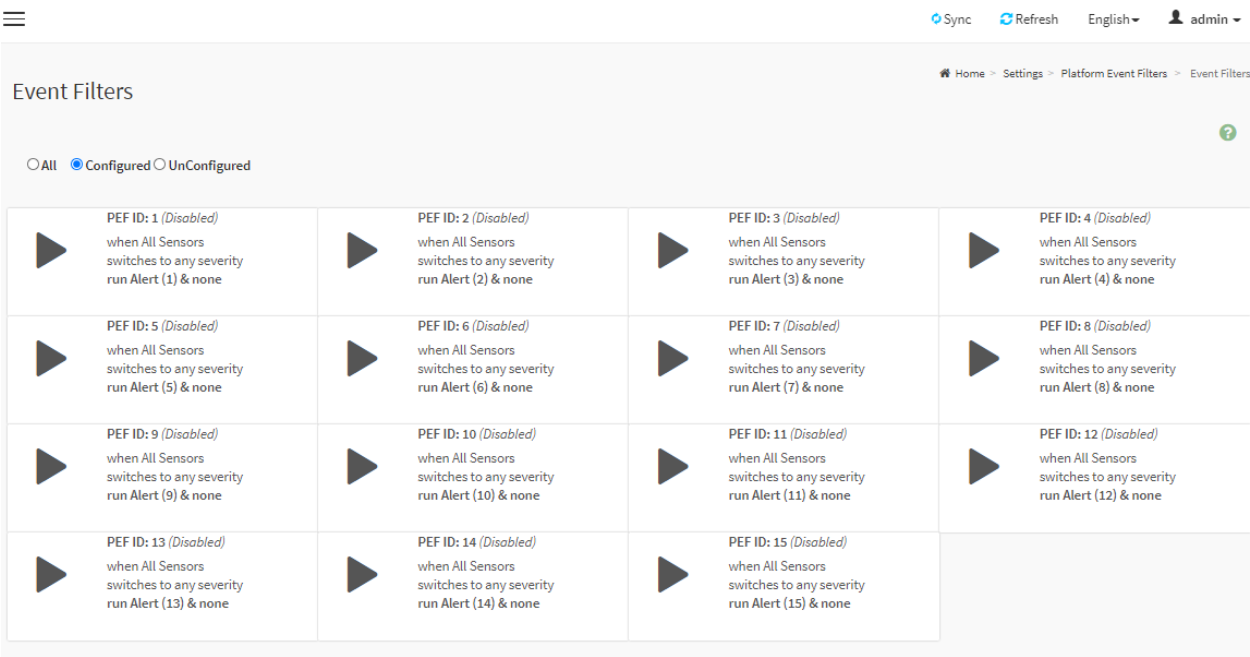
Platform Event Filter (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.



Platform Event Filter Page

28.7.8.1. Event Filters

This page is used to configure Event filters. You can modify or add new event filter entry from here. By default, 15 event filter entries are configured among the 40 available slots.



Event Filters Page

Event Filter Configuration: Click the **Event Filters** section to configure the event filters in the available slots.

Event Filter Configuration

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

?

☐ Enable this filter

Event severity to trigger

Any severity

Power Action

None

Alert Policy Group Number

1

☒ Raw Data

Generator ID 1

255

Generator ID 2

255

Generator Type

☐ Slave ☐ Software

Slave Address/Software ID

Channel Number

0

IPMB Device LUN

0

Sensor type

All Sensors

Sensor name

All Sensors

Event Options

All Events

Event trigger

255

Event Data 1 AND Mask

0

Event Data 1 Compare 1

0

Event Data 1 Compare 2

0

Event Data 2 AND Mask

0

Event Data 2 Compare 1

0

Event Data 2 Compare 2

0

Event Data 3 AND Mask

0

Event Data 3 Compare 1

0

Event Data 3 Compare 2

0

Delete

Save

Event Filters Configuration Page

Enable this filter: Check the box to enable the PEF settings.

Event Severity to trigger: Select any one of the Event severity from the list.

Power Action: Select any one of the power action either Power down, Power reset or Power cycle from the drop-down list

Alert Policy Group Number: Select any one of the alert policy group number from the drop-down list.

Raw Data: Check the box to fill the Generator ID with raw data.

Generator ID 1: Enter the raw generator ID1 data value.

Generator ID 2: Enter the raw generator ID2 data value.

Generator Type: Choose the event generator as slave address - if event is generated from IPMB.

Slave Address/Software ID: Specify corresponding I2C slave address or system software ID.

Channel Number: Choose the particular channel number through which the event message is received over. Choose “0” if the event message is received via the system interface, primary IPMB, or internally generated by the BMC.

IPMB Device LUN: Choose the corresponding IPMB device LUN if event is generated by IPMB.

Sensor type: Select the type of sensor that will trigger the event filter action.

Sensor name: Choose the particular sensor from the sensor list.

Event Options: Choose event option to be either all events or sensor specific events.

Event Trigger: Enter the raw event/reading type value.

Event Data 1 AND Mask: Indicate wildcarded or compared bits.

Event Data 1 Compare 1 & Event Data 1 Compare 2: Indicate whether each bit position’s comparison is an exact comparison or not.

Event Data 2 AND Mask: Similar to Event Data 1 AND Mask.

Event Data 2 Compare 1 & Event Data 2 Compare 2: Similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

Event Data 3 AND Mask: Similar to Event Data 1 AND Mask.

Event Data 3 Compare 1 & Event Data 3 Compare 2: Similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

89

28.7.8.2 Alert Policies

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

Sync

Refresh

English

admin

Alert Policies

Home > Settings > Platform Event Filters > Alert Policies

Group: 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 2 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group: 5 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 6 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 7 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 8 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group: 9 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 12 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
Group: 13 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Group: 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0

Alert Policies Page

Alert Policies: Click the **Alert Policies** section to configure the alert policies in the available slots.

SyncRefreshEnglishadmin

Alert Policies

Home>Settings>Platform Event Filters>Alert Policies>Alert Policies

Alert Policies

Policy Group Number

1

Enable this alert

Policy Action

Always send alert to this destination

LAN Channel

1

Destination Selector

Event Specific Alert String

Alert String Key

DeleteSave

Alert Policies Page

- Policy Group Number:** Displays the Policy number of the configuration.
- Enable this alert:** Check the box to enable the policy settings.
- Policy Action:** Choose any one of the Policy set values from the list.
- LAN Channel:** Choose a particular channel from the available channel list.
- Destination Selector:** Choose a particular destination from the configured destination list.
- Event Specific Alert String:** Check the box to specify event-specific Alert String.
- Alert String Key:** Specify which string is to be sent for this Alert Policy entry.

28.7.8.3. LAN Destinations

This page is used to configure the LAN destination of PEF configuration.

SyncRefreshEnglishadmin

LAN Destinations

Home>Settings>Platform Event Filters>LAN Destinations

Select the LAN Channel

1

LAN Channel: 1 LAN Destination: 1 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 2 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 3 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 4 SNMP Trap Sent To: Send Test Alert
LAN Channel: 1 LAN Destination: 5 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 6 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 7 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 8 SNMP Trap Sent To: Send Test Alert
LAN Channel: 1 LAN Destination: 9 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 10 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 11 SNMP Trap Sent To: Send Test Alert	LAN Channel: 1 LAN Destination: 12 SNMP Trap Sent To: Send Test Alert

LAN Destinations Page

Select the LAN Channel: Select the LAN Channel number.

LAN Destination Configuration: Select any empty slot to configure LAN Destinations.

LAN Destination Configuration

Home > Settings > Platform Event Filters > LAN Destinations > LAN Destination Configuration

LAN Channel

1

LAN Destination

1

Destination Type

☒ SNMP Trap

☐ E-Mail

SNMP Destination Address

BMC Username

Email Subject

Email Message

Delete

Save

LAN Destination Configuration Page

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

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

SNMP Destination Address: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the four fields - SNMP Destination Address, BMC User Name, Email subject and Email message needs to be filled. For SNMP Trap, only the SNMP Destination Address has to be filled.

BMC User Name: If Destination type is Email Alert, then choose the user to whom the email alert has to be sent.

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

28.7.9. Services

This page is used to displays the basic information about services running in the BMC.

SyncRefreshEnglishadmin

Services

Home>Settings>Services

Service	Status	Interfaces	Non Secure Port	Secure Port	Timeout	Maximum Sessions		
web	Active	bond0	80	443	1800	20		
kvm	Active	bond0	7578	7582	1800	2		
cd-media	Active	bond0	5120	5124	N/A	4		
fd-media	Active	bond0	5122	5126	N/A	4		
hd-media	Active	bond0	5123	5127	N/A	4		
ssh	Active	NA	N/A	22	600	N/A		
solssh	Inactive	bond0	52123	N/A	60	N/A		

Services Page

- Services:** Displays service name of the selected slot (read only).
- Status:** Displays the current status of the service, either active or inactive state.
- Interfaces:** It shows the interface in which service is running.
- Nonsecure Port:** Displays non secure port number of the service.
- Secure Port:** Displays secure port number of the service.
- Timeout:** Displays the session timeout value of the service.
- Maximum Sessions:** Displays the maximum number of allowed sessions for the service.

View the active sessions: Click **View** icon  to view the details about the active sessions for the service.

Sync

Refresh

English

admin

Home > Settings > Services > Service Sessions

Service Sessions

Active Session - Web

Session ID	Session Type	User ID	User Name	Client IP	Privilege	
4*	Web HTTPS	2	admin	172.29.2.5	Administrator	

Service Session Page

- Session ID:** Displays the ID of the active sessions.
- Session Type:** Displays the type of the active sessions.
- User ID:** Displays the ID of the user.
- User Name:** Displays the name of the user.
- Client IP:** Displays the IP addresses that are already configured for the active sessions
- Privilege:** Displays the access privilege of the user.
- Terminate Session:** Click **Terminate** icon  to terminate the particular session of the service.

Edit the existing service: Click **Edit** icon  to modify the configuration of the service.

Home > Settings > Services > Service Configuration

Service Configuration

Service Name

web

Active

☒

Interface Name

bond0

Non-secure port

80

Secure port

443

Mutual port

4433

Enable Timeout

☒

Timeout

1800

Maximum Sessions

20

Save

Service Configuration Page

- Service Name:** Displays service name of the selected slot (read only).
- Active:** Check the box to enable the service.
- Interface Name:** Choose any one of the available interfaces from the drop-down list.
- Non-secure Port:** Configure non secure port number for the service.
- Secure Port:** Configure secure port number for the service.
- Mutual Port:** Configure mutual port number for the service.
- Enable Timeout:** Check the box to enable the timeout function.
- Timeout:** Configure the session timeout for the service.
- Maximum Sessions:** Displays the maximum number of allowed sessions for the service.

28.7.10. SMTP Settings

This is used to configure the SMTP settings of the device.

SMTP Settings

Home > Settings > SMTP Settings

?

☐ Default Setting

LAN Interface

bond0

Sender Email ID

☒ Primary SMTP Support

Primary Server Name / Domain

Primary Server IP

Primary SMTP port

25

Primary Secure SMTP port

465

☐ Primary SMTP Authentication

Primary Username

Primary Password

☐ Primary SMTP SSLTLS Enable

☐ Primary SMTP STARTTLS Enable

☐ Secondary SMTP Support

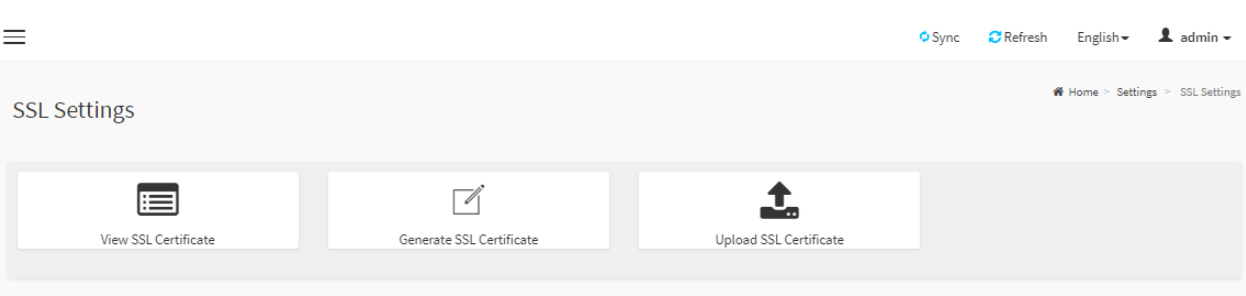
Save

SMTP Settings Page

- LAN Interface:** Displays the list of LAN channels available.
- Sender Email ID:** Enter the valid Sender Email ID on the SMTP Server.
- Primary SMTP Support:** Check the box to enable SMTP support for the BMC.
- Primary Server Name:** Enter the Machine Name of the SMTP Server.
- Primary SMTP IP:** Enter the IP address of the SMTP Server
- Primary SMTP Port:** Specify the SMTP Port.
- Primary Secure SMTP Port:** Specify the SMTP Secure Port.
- Primary SMTP Authentication:** Check the box to enable SMTP Authentication.
- Primary Username:** Enter the username to access SMTP Accounts.
- Primary Password:** Enter the password for the SMTP User Account.
- Primary SMTP SSLTLS Enable:** Check the box to enable SMTP SSLTLS protocol
- Primary SMTP STARTTLS Enable:** Check the box to enable SMTP STARTTLS protocol.
- Upload SMTP CA Certificate File:** This field will be present if enable **SMTP SSLTLS Enable** or **STARTTLS Enable**, the field is used to upload CACERT key file.
- Upload SMTP Certificate File:** This field will be present if enable **SMTP SSLTLS Enable** or **STARTTLS Enable**, the field is used to upload CERT key file.
- Upload SMTP Private Key:** This field will be present if enable **SMTP SSLTLS Enable** or **STARTTLS Enable**, the field is used to upload SMTP key file.
- Secondary SMTP Support:** Check the box to enable secondary SMTP support for the BMC.

28.7.11. SSL Settings

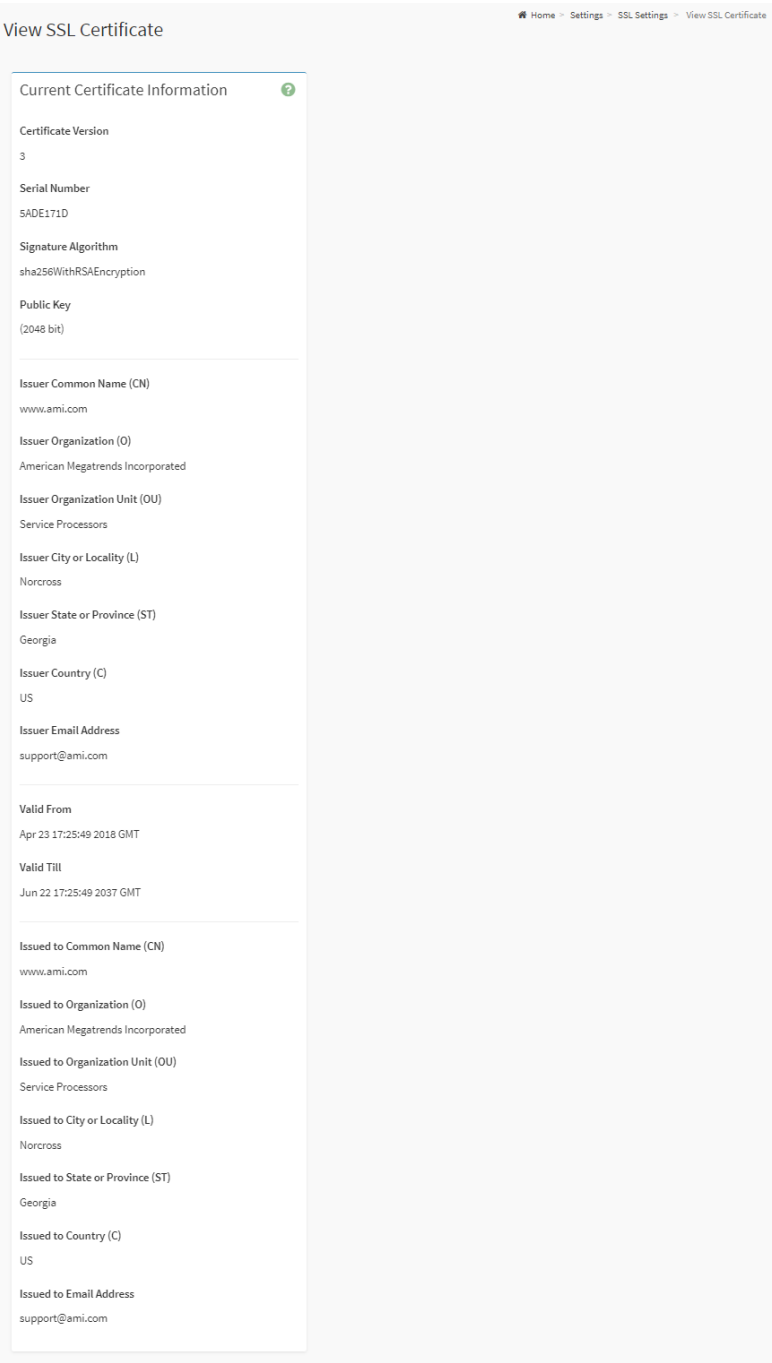
This page is used to configure SSL certificate for the BMC.



SSL Settings Page

28.7.11.1. View SSL Certificate

This page is used to view the uploaded SSL certificate in readable format.



View SSL certificate Page

Note: This page provides a simple method to generate SSL certificate and it is not issued by a trusted Certificate Authority, you can upload a trusted certificate by yourself, if necessary.

28.7.11.2. Generate SSL Certificate

This page is used to generate the SSL certificate based on configuration details.

Generate SSL Certificate

Home > Settings > SSL Settings > Generate SSL Certificate

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

Valid for

in days

Key Length

2048 bits

Save

Generate SSL certificate Page

- Common Name(CN):** Common name for which certificate is to be generated.
- Organization(O):** Organization name for which the certificate is to be generated.
- Organization Unit(OU):** Over all organization section unit name for which certificate is to be generated.
- City or Locality(L):** City or Locality of the organization.
- State or Province(ST):** State or Province of the organization.
- Country(C):** Country code of the organization.
- Email Address:** E-mail Address of the organization.
- Valid for:** Validity of the certificate.
- Key Length:** The key length bit value of the certificate.

28.7.11.3. Upload SSL Certificate

This page is used to upload the certificate and private key file into the BMC.

Upload SSL Certificate

Home > Settings > SSL Settings > Upload SSL Certificate

Current Certificate

Tue Sep 29 08:11:40 2020

New Certificate

Current Private Key

New Private Key

☐ Upload CA Certificate

Upload

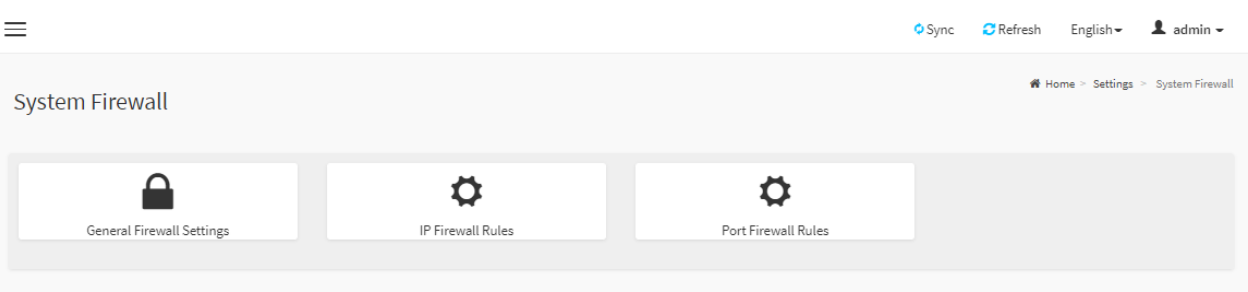
Upload SSL certificate Page

- Current Certificate:** Displays current certificate and uploaded date/time (read only).
- New Certificate:** Browse and navigate to the certificate file, the file should be of pem type
- Current Private Key:** Displays current Private key information (read only).
- New Private Key:** Browse and navigate to the private key file, the file should be of the type pem.
- Upload CA Certificate:** Check this option to upload CA Certificate file.
- New CA Certificate:** Browse and navigate to the CA certificate file.

97

28.7.12. System Firewall

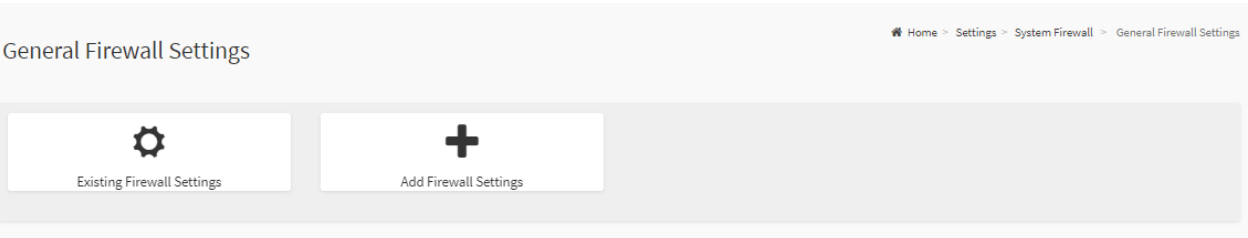
This page is used to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers.



System Firewall Page

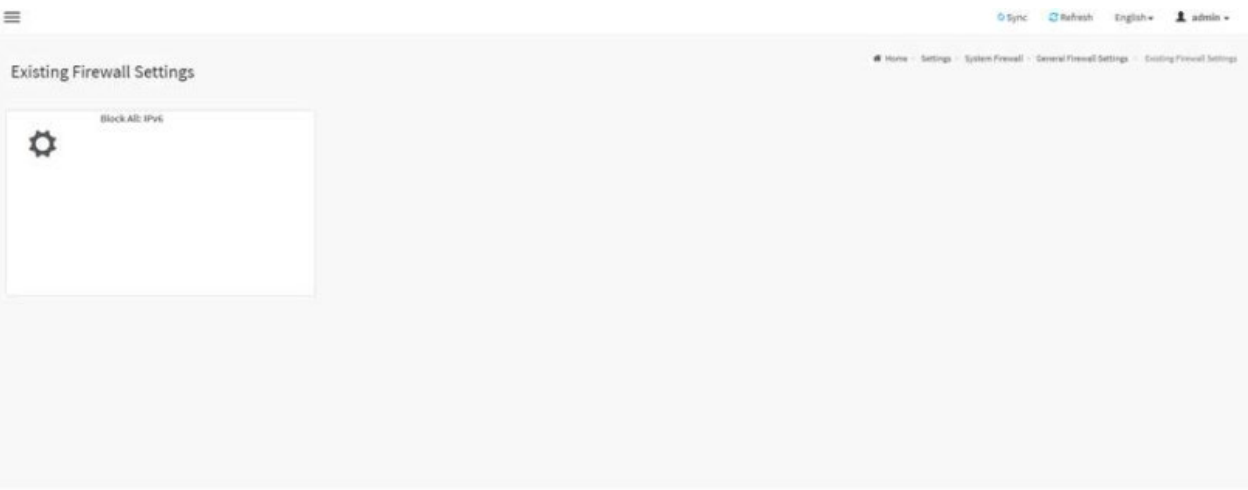
28.7.12.1. General Firewall Settings

This page is used to configure general firewall settings.



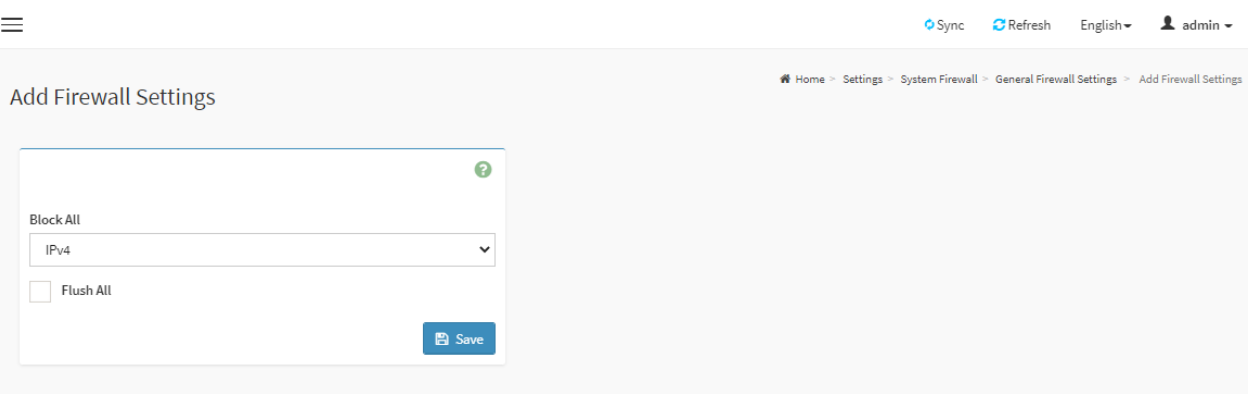
General Firewall Settings Page

Existing Firewall Settings: This page is used to displays existing firewall settings.



Existing Firewall Settings Page

Add Firewall Settings: This page is used to displays add firewall settings.

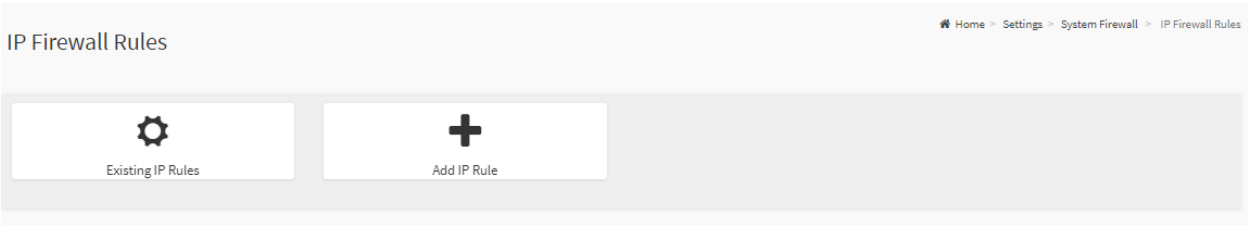


Add Firewall Settings Page

Block All: This option will block all incoming IPs and Ports.
Flush All: This option is used to flush all the system firewall rules.

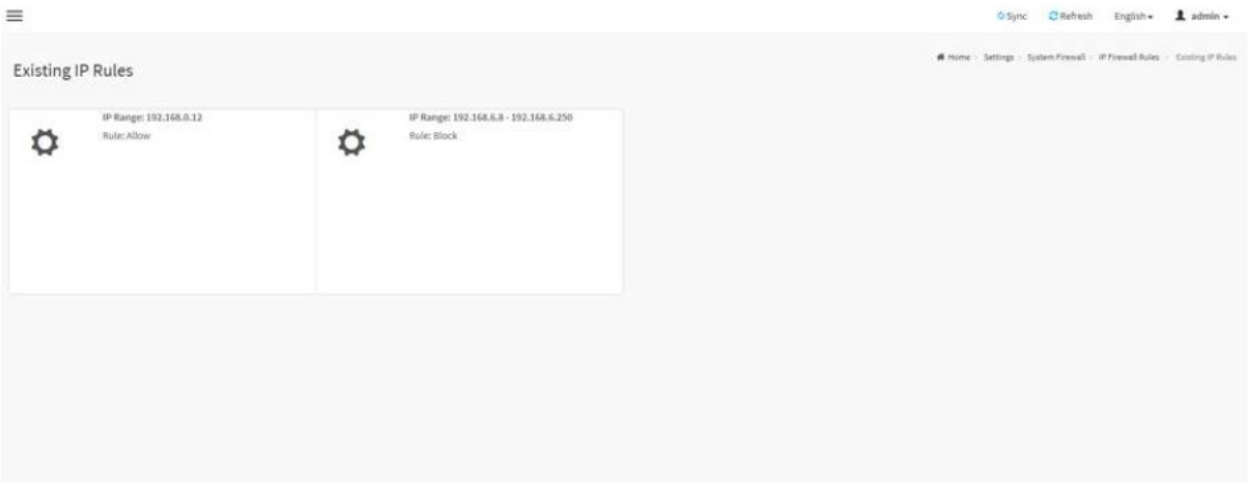
28.7.12.2. General Firewall Settings

This page is used to add a new IP Address or Range to firewall settings.



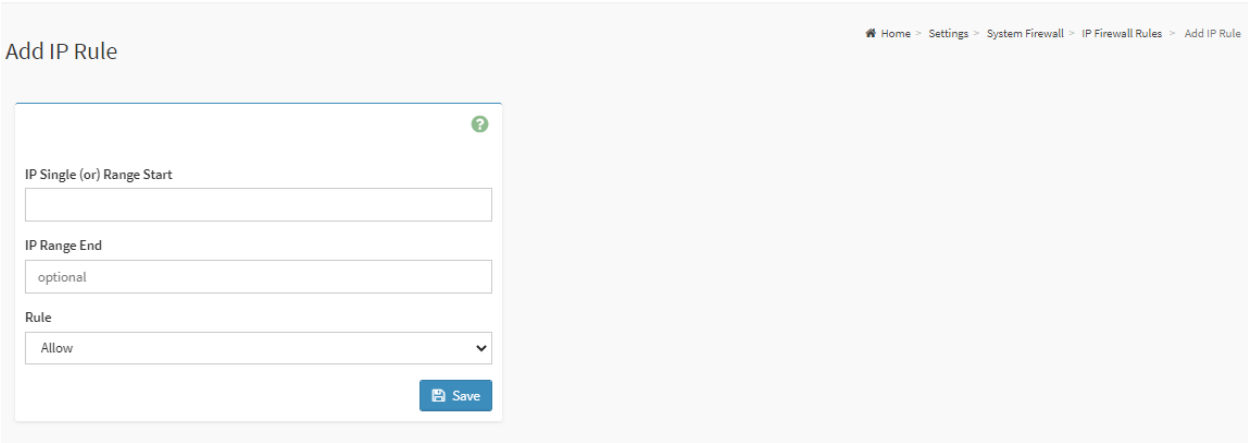
IP Firewall Rules Page

Existing IP Rules: This page is used to displays existing IP rules.



Existing IP Rules Page

Add IP Rule: This page is used to displays add IP rule settings.



Add IP Rule Page

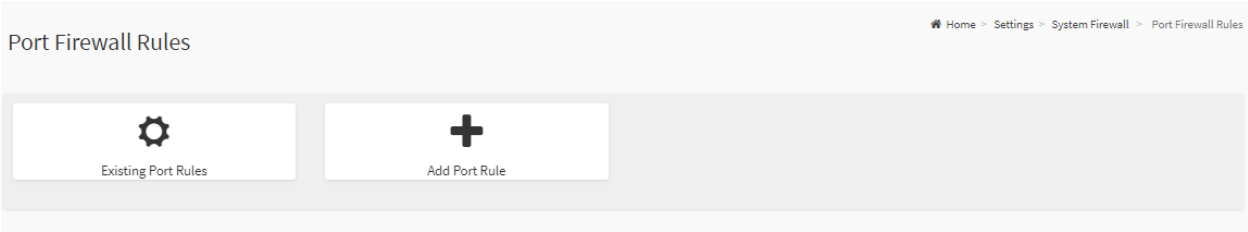
IP Single (or) Range Start: This field is used to configure the IP address or range of IP addresses.

IP Range End: This field is used to configure the IP range end of IP addresses.

Rules: This field is used to determine the rule to **Allow** or **Block**.

28.7.12.3. Port Firewall Rules

This page is used to add a new Port or Range to firewall settings.



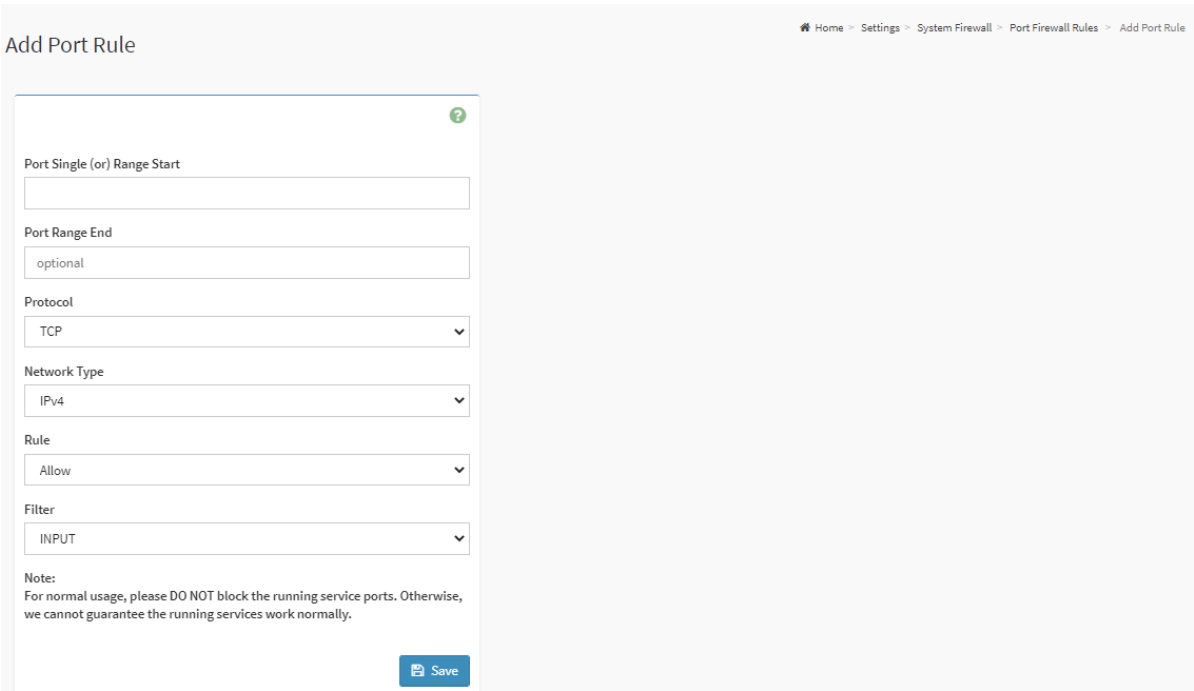
Port Firewall Rules Page

Existing Port Rules: This page is used to displays existing port rules.



Existing Port Rules Page

Add Port Rule: This page is used to displays add port rule settings.



Add Port Rule Page

Port Single (or) Range Start: This field is used to configure the port number or range of port numbers.

Port Range End: This field is used to configure the port range end of port numbers.

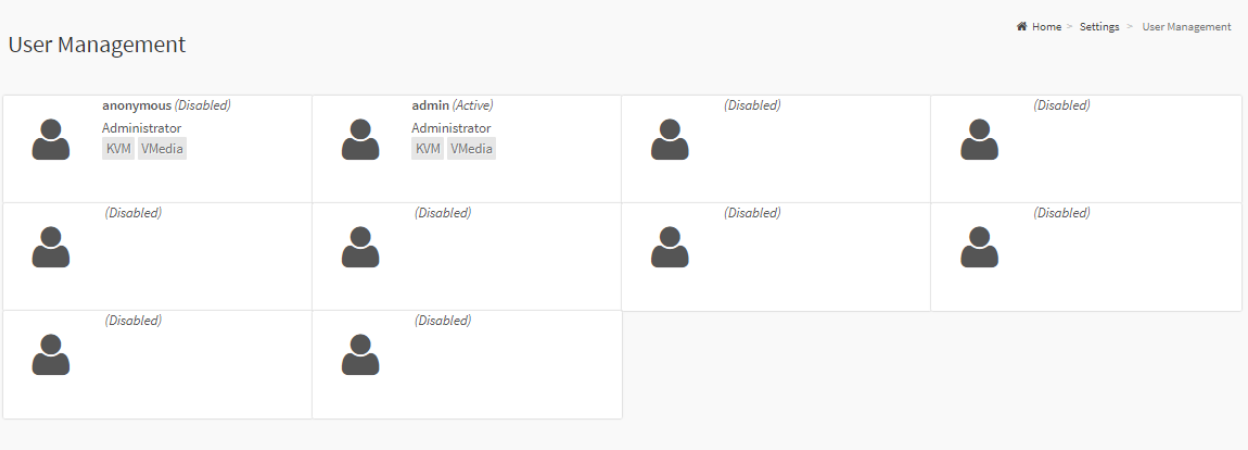
Protocol: This field is used to configure the protocol.

Network Type: This field is used to configure the network type.

Rule: This field is used to determine the rule to **Allow** or **Block**.

28.7.13 User Management

This page displays the current list of user slots for the server. You can add a new user and modify or delete the existing users.



User Management Page

Add a new user: To add a new user, select a free section and click on the empty section.

The screenshot shows the 'User Management Configuration' page. It features a form with the following fields and options:

- Username:** A text input field.
- Password Size:** A dropdown menu currently set to '16 bytes'.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Enable User Access:** A checkbox.
- Network Privilege:** A dropdown menu.
- Serial Privilege:** A dropdown menu.
- KVM Access:** A checkbox.
- VMedia Access:** A checkbox.
- SNMP Access:** A checkbox.
- SNMP Access level:** A dropdown menu.
- SNMP Authentication Protocol:** A dropdown menu.
- SNMP Privacy Protocol:** A dropdown menu.
- Email Format:** A dropdown menu.
- Email ID:** A text input field.
- Existing SSH Key:** A text input field with the value 'Not Available'.
- Upload SSH Key:** A text input field with a file upload button.
- Save:** A blue button at the bottom right of the form.

Add User Page

- Username:** Enter the name of the user.
- Password Size:** Either 16 Bytes or 20 Bytes password size can be chosen.
- Password:** Enter the password of the user.
- Confirm Password:** Confirm the password.
- Enable User Access:** Enabling user access will intern assign the IPMI messaging privilege to user.
- Network Privilege:** Select the network privileges assigned to the user.

Serial Privilege: Select the serial privileges assigned to the user.

KVM Access: Assign the KVM privilege for the user.

VMedia Access: Assign the VMedia privilege for the user.

Note: Both KVM and VMedia privilege will enable(disable) automatic when Network Privilege is administrator(other).

Email Format: Specify the format for the email. Two types of formats are available.

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

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

Email ID: Enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

Existing SSH Key: Displays the uploaded SSH key information(read only).

Upload SSH Key: Upload the public SSH key file.

Modify user: To modify the existing user, click on the active user tab.

User Management Configuration

Home > Settings > User Management > User Management Configuration

?

Username

anonymous

☐

Change Password

Password Size

16 bytes

Password

Confirm Password

☐

Enable User Access

Network Privilege

Administrator

Serial Privilege

None

☒KVM Access

☒VMedia Access

☐SNMP Access

SNMP Access level

SNMP Authentication Protocol

SNMP Privacy Protocol

Email Format

AMI-Format

Email ID

Existing SSH Key

Not Available

Upload SSH Key

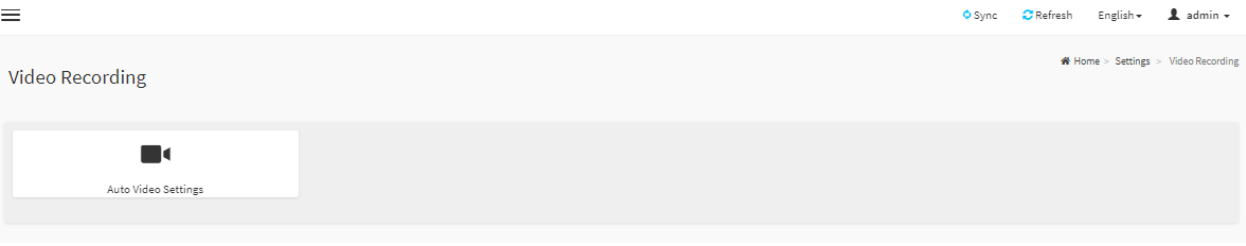
Delete

Save

Modify User Page

28.7.14. Video Recording

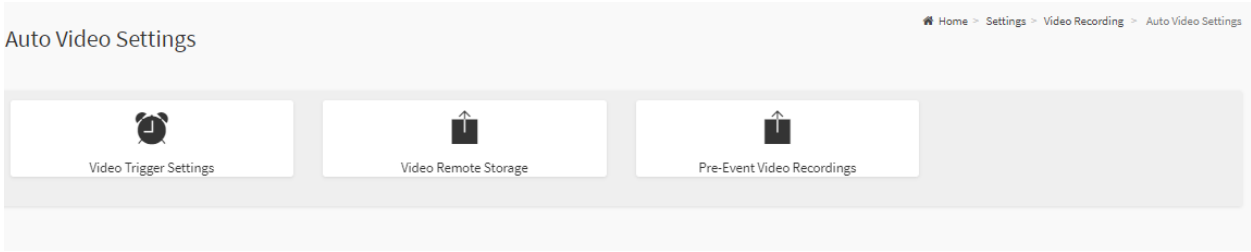
This page is used to configure video recording settings.



Video Recording Page

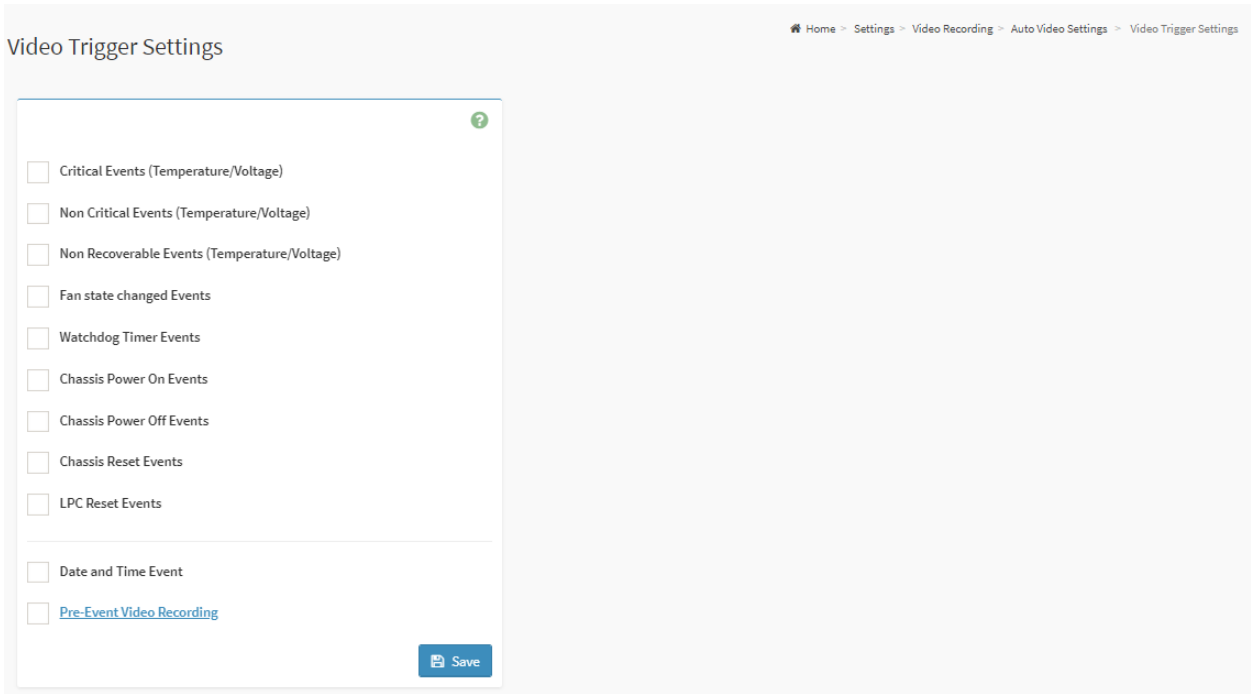
28.7.14.1. Port Firewall Rules

This page is used to configure auto video recording settings.



Auto Video Settings Page

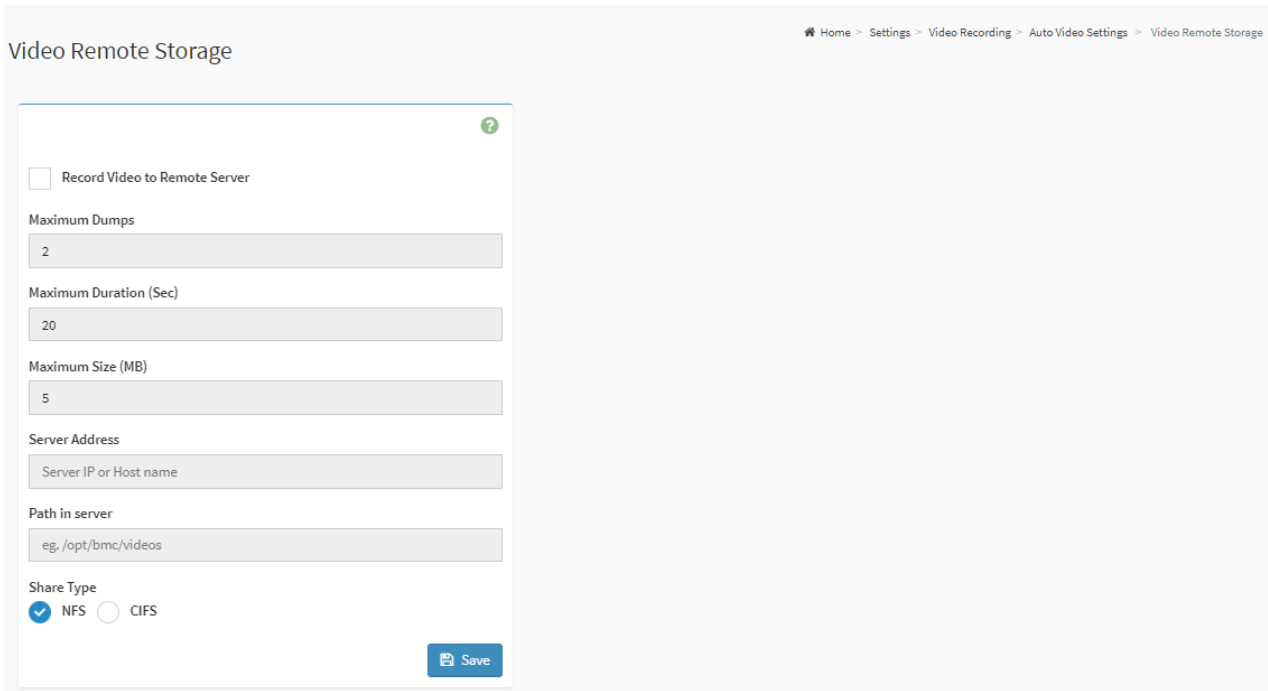
Video Trigger Settings: This page is used to configure the events that will trigger auto video recording function of the KVM server.



Video Trigger Settings Page

- Critical Events (Temperature/Voltage):** Trigger the recording by the critical events for Temperature/Voltage sensor.
- Non Critical Events (Temperature/Voltage):** Trigger the recording by the non-critical events for Temperature/Voltage sensor.
- Non Recoverable Events (Temperature/Voltage):** Trigger the recording by the non-recoverable events for Temperature/Voltage sensor.
- Fan state changed Events:** Trigger the recording by all fan sensor events
- Watchdog Timer Events:** Trigger the recording when watchdog timer be triggered.
- Chassis Power On Events:** Trigger the recording by system power on events (DC on).
- Chassis Power Off Events:** Trigger the recording by system power off events (DC off).
- Chassis Reset Events:** Trigger the recording by system reset events.
- LPC Reset Events:** Trigger the recording by Host LPCRESET event.
- Date and Time Event:** Trigger the recording by specific date and time.
- Pre-Event Video Recording:** Select Crash Reset either **Pre-crash** or **Pre-reset**.

Video Remote Storage: This page is used to configure the remote storage path.



Video Remote Storage Page

Record Video to Remote Server: Check the box to enable remote video support. If remote video support is enabled, then the video files will be stored in remote path.

Maximum Dumps: Enter maximum dumps of the video.

Maximum Duration(Sec): Enter maximum duration of the video.

Maximum Size(MB): Enter maximum size of the video.

Server Address: Specify server address of the server.

Path in Server: Select the **Share Type** (NFS/CIFS). If the selected share type is (CIFS), enter the **User Name**, **Password** and **Domain Name** in the respective fields.

Pre-Event Video Recordings: This page used to configure the Pre-Event video recording configurations.

Pre-Event Video Recordings

Home > Settings > Video Recording > Auto Video Settings > Pre-Event Video Recordings

?

This page used to configure the Pre-Event video recording configurations.Pre-Event video recording is currently disabled.To enable the Pre-Event video recording in [Triggers Configuration](#) page and trigger the video.

Video Quality

Very Low

Compression Mode

High

Frames Per Second

1

Video Duration

10

Save

Pre-Event Video Recording Page

Video Quality: To set video quality, select ranges from the drop-down list.

Compression Mode: To set compression mode, select modes from the drop-down list.

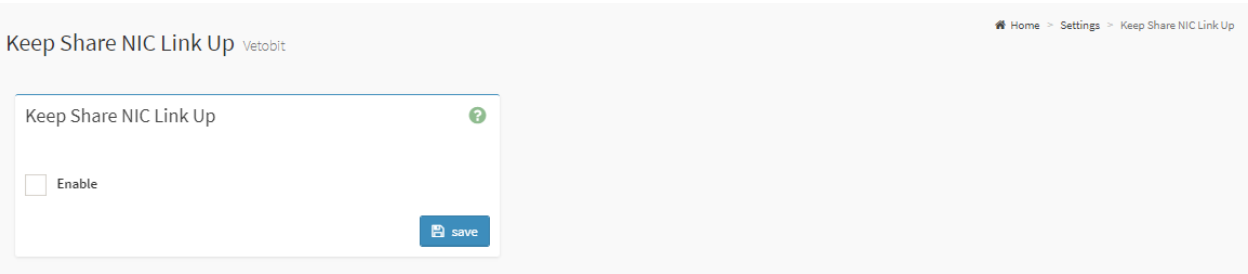
Frames Per Second: To set number of frames per second, select frames/sec (1-4) from the drop-down list.

Video Duration: To set duration of video, select second (10-60) from the drop-down list.

105

28.7.15. Keep Share NIC Link Up

This page is used to configure share NIC (NCSI) PHY link up setting.

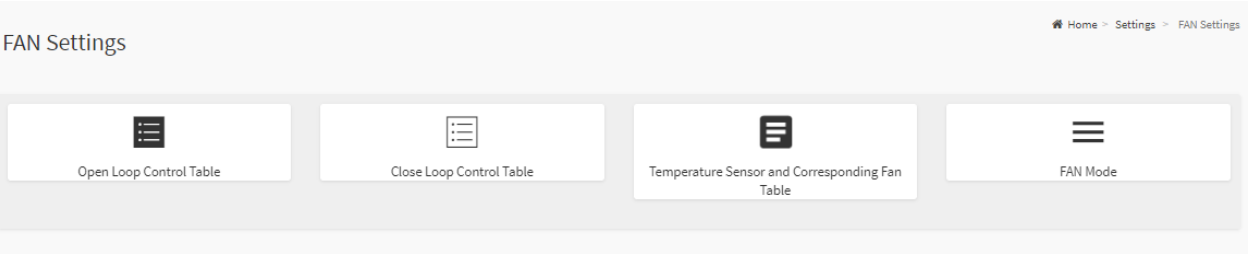


Keep Share NIC Link Up Page

Enable: Check the box to enable Keep Share NIC Link Up, share NIC PHY will keep link up, and it could avoid share NIC disconnection while system reset.

28.7.16. FAN Settings

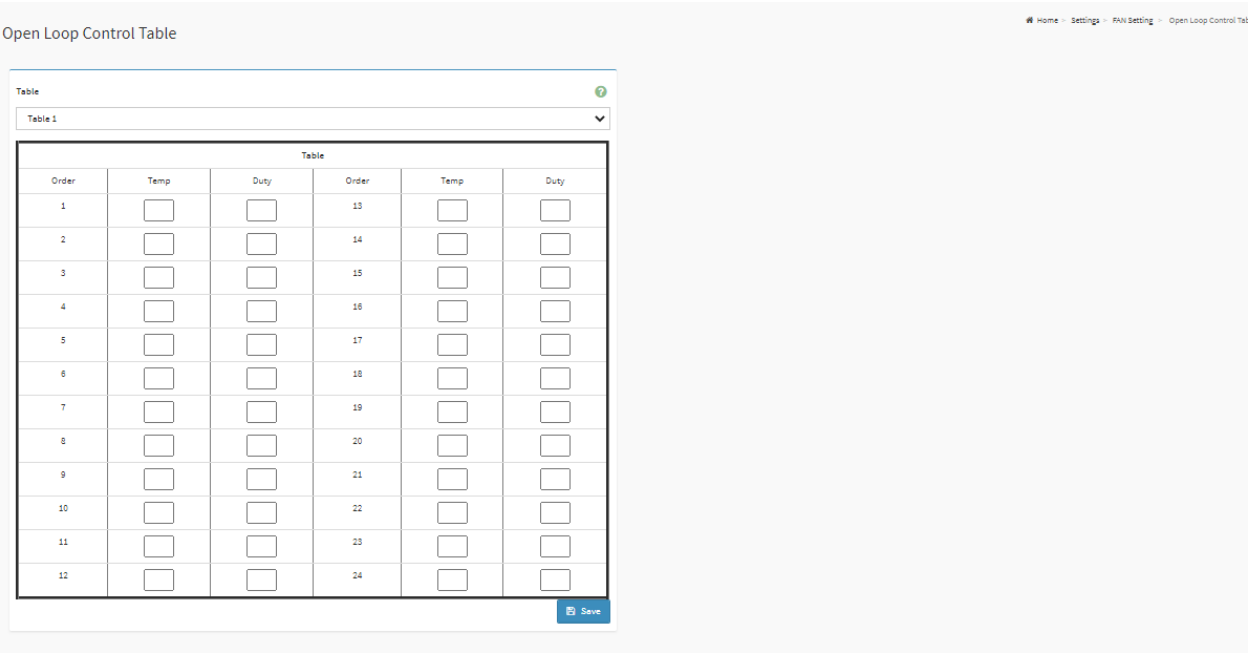
This page is used to configure the Fan Settings.



Fan Settings Page

28.7.16.1 Open Loop Control Table

This page is used to configure the Open Loop Control Table.

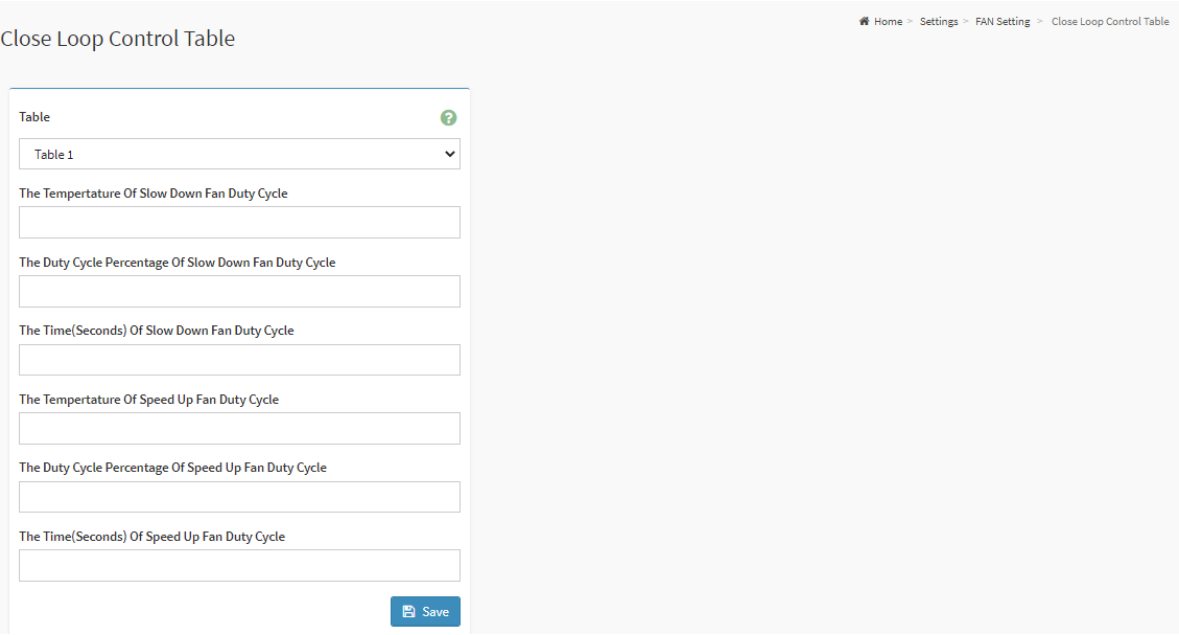


Open Loop Control Table

- Temp:** Select to set the values from 0 to 120 degree Celsius.
- Duty:** Select to set the values from 20 to 100.

28.7.16.2 Close Loop Control Table

This page is used to configure the Close Loop Control Table.



Close Loop Control Table

Table: To select the table from the list.

- The Temperature of Slow Down Fan Duty Cycle:** To select the condition for temperature of slow down fan duty cycle.
- The Duty Cycle Percentage of Slow Down Fan Duty Cycle:** To select the condition for duty cycle percentage of slow down fan duty cycle.
- The Time (Seconds) of Slow Down Fan Duty Cycle:** To select the condition for time of slow down fan duty cycle.
- The Temperature of Speed Up Fan Duty Cycle:** To select the condition for temperature of speed up fan duty cycle.
- The Duty Cycle Percentage of Speed Up Fan Duty Cycle:** To select the condition for duty cycle percentage of speed up fan duty cycle.
- The Time (Seconds) Of Speed Up Fan Duty Cycle:** To select the condition for time of speed up fan duty cycle.

28.7.16.3 Temperature Sensor and Corresponding Fan Table

This page is used to configure the Temperature Sensor and Corresponding Fan Table.

Temperature Sensor and Corresponding Fan Table

Home > Settings > FAN Setting > Temperature Sensor and Corresponding Fan Table

ALL Sensor

MB TempCard Side TempTR1 TempCPU Temp

Sensor Number

Select Open Loop Control Table

Disable

Select Close Loop Control Table

Disable

Select Fan

Fan1	☐
Fan2	☐
Fan3	☐
Fan4	☐
Fan5	☐
Fan6	☐
Fan7	☐

Set

Temperature Sensor and Corresponding Fan Table

- All Sensors:** To select the Motherboard, Card Side, TR1 and CPU temperatures.
- Sensor Number:** To select the Sensor Number which corresponds to the Motherboard, Card Side, TR1 and CPU temperatures.
- Select Open Loop Control Table:** To select the Open Loop Control Table which links to the Open Control Table Page.
- Select Close Loop Control Table:** To select the Close Loop Control Table which links to the Close Loop Control Table.
- Select Fan:** Check the box to enable the Fans.

28.7.16.4 FAN Mode

This page is to set the FAN Mode settings.

FAN Mode

Home > Settings > FAN Setting > FAN Mode

Set Fan Duty For Manual Mode

FAN	Duty
1	0
2	0
3	0
4	0
5	0
6	0
7	0

Save manual mode

Set Fan Control Mode

Mode	Default	Manual	Customized
Fan1	☒	☐	☐
Fan2	☒	☐	☐
Fan3	☒	☐	☐
Fan4	☒	☐	☐
Fan5	☒	☐	☐
Fan6	☒	☐	☐
Fan7	☒	☐	☐

Save control mode

Clean All Fan Setting

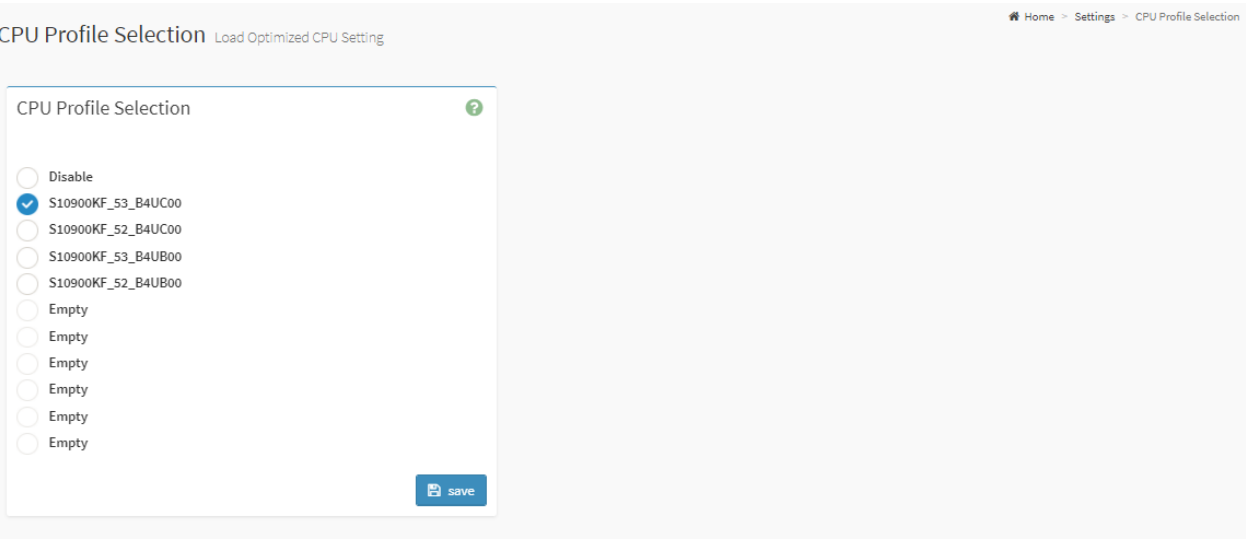
Clean All Fan Setting

Fan Mode Page

- Set Fan Duty For Manual Mode:** To set the Fan Duty values for Manual Fans.
- Set Fan Control Mode:** To set Fan Control Mode to be Default, either Manual or Customized.

28.7.17. CPU Profile Selection

This page is to set the CPU Profiles settings. You can select the overclock profiles and you must reboot the machine for the settings to take effect.



CPU Profile Selection

28.8 Remote Control

This page is used to launch the remote console redirection.



Remote Control Page

Launch KVM: Click the button to open remote control KVM page.

Launch Java KVM: Click the button to open Java KVM application.

28.9 Image Redirection

This page is used to configure the images into BMC for redirection

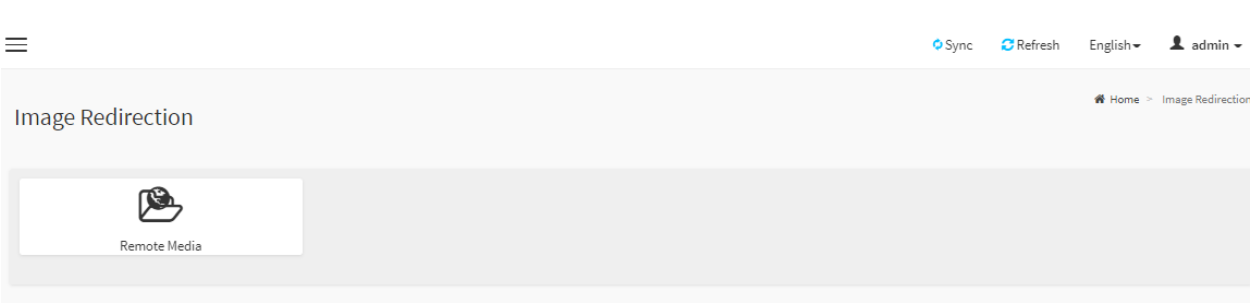
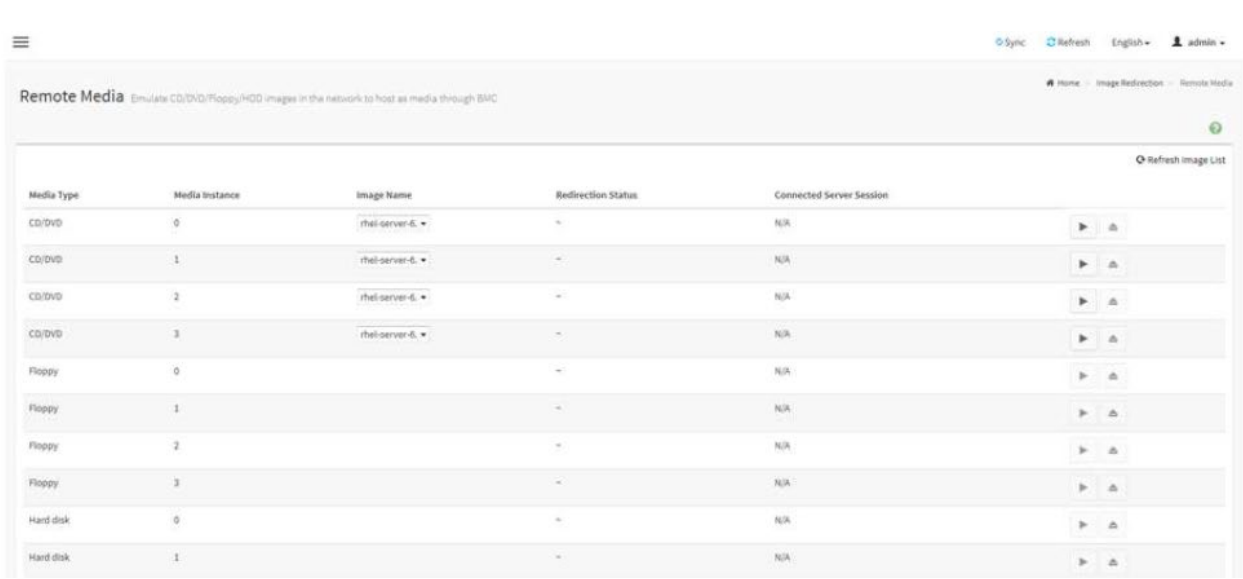


Image Redirection Page

28.9.1. Remote Media

This page is used to configure the remote images into BMC for redirection.

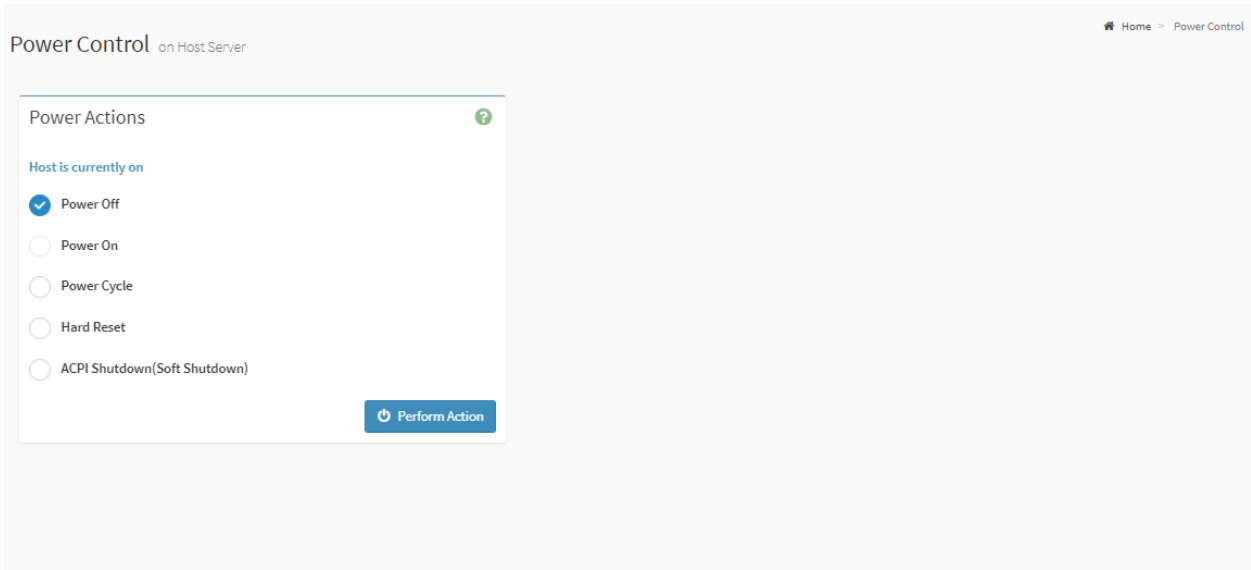


Remote Media Page

- Media Type:** Displays type of Media such as CD/DVD, Floppy and Hard disk.
- Media Instance:** Displays total media instance count.
- Image Name:** Displays the default recovery image name on the server.
- Status:** Displays the status of the media.
- Session Index:** Displays Media Server Session Index.
- Start/Stop Redirection:** To start or stop media redirection.
- Pause:** To pause the media redirection.
- Refresh Image List:** To get latest Image lists from the Remote Storage.
- Note:** To configure the image, you need to enable Remote Media support first.

28.10 Power Control

This page is used to view and control the power of the server.



Power Control Page

Power Off: Select this option to immediately power off the server.

Power On: Select this option to power on the server.

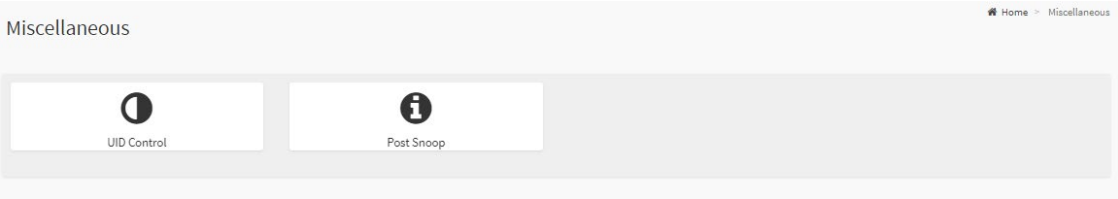
Power Cycle: Select this option to first power off, and then reboot the system (cold boot).

Hard Reset: Select this option to reboot the system without powering off (warm boot).

ACPI Shutdown (Soft Shutdown): Select this option to initiate operating system shutdown prior to the shutdown.

28.11 Miscellaneous

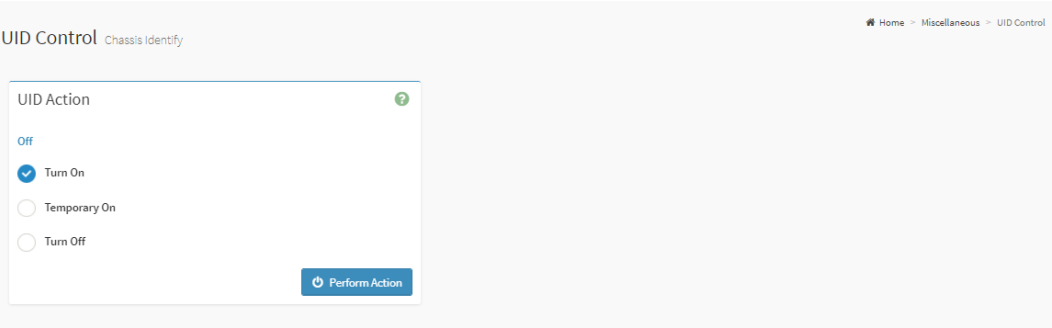
This page is used to configure miscellaneous settings.



Miscellaneous Page

28.11.1 UID Control

This page is used to control the UID of the chassis.

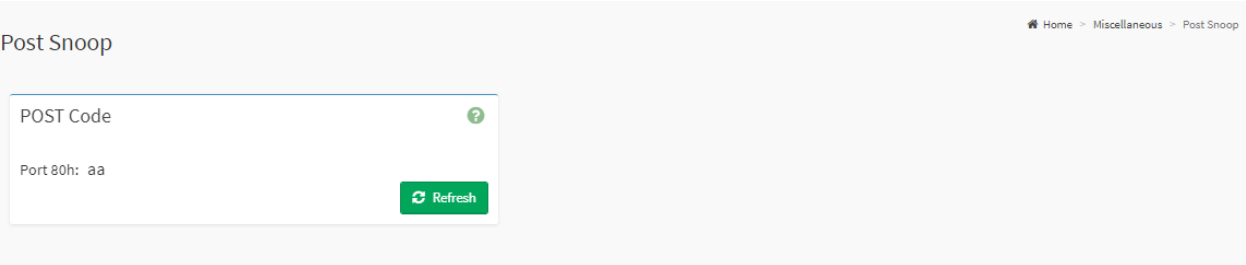


UID Control Page

- Turn On:** Select this option to turn on UID.
- Temporary On:** Select this option to temporary turn on UID. (15 sec blink)
- Turn Off:** Select this option to turn off UID.

28.11.2 Post Snoop

This page is used to display the last POST code of BIOS.

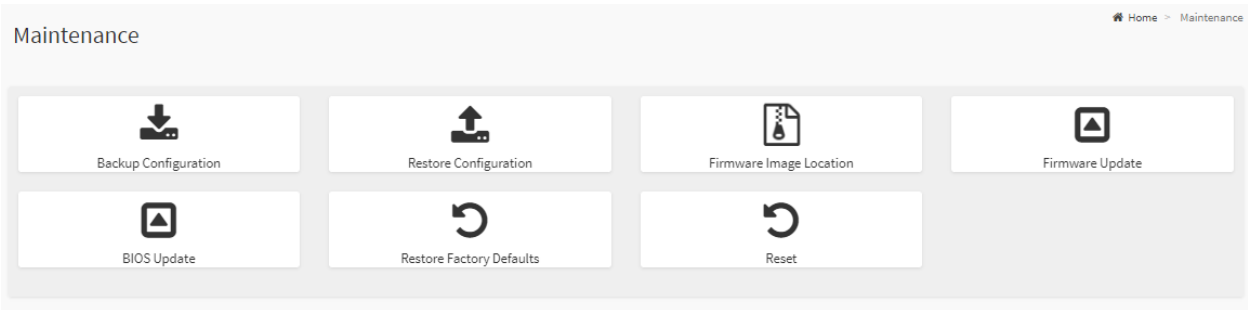


Post Snoop Page

Post 80h: Click **Refresh** button to get the last POSTcode of BIOS. (Read only).

28.12 Maintenance

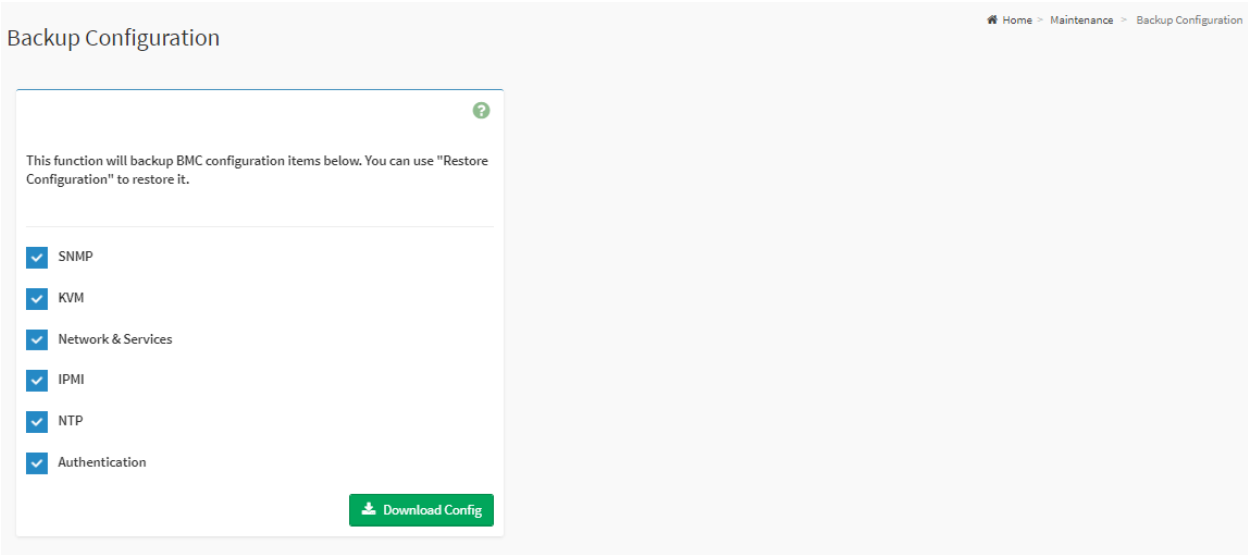
This page is used to do maintenance tasks on the device.



Maintenance Page

28.12.1 Backup Configuration

This page is used to back up the configuration.

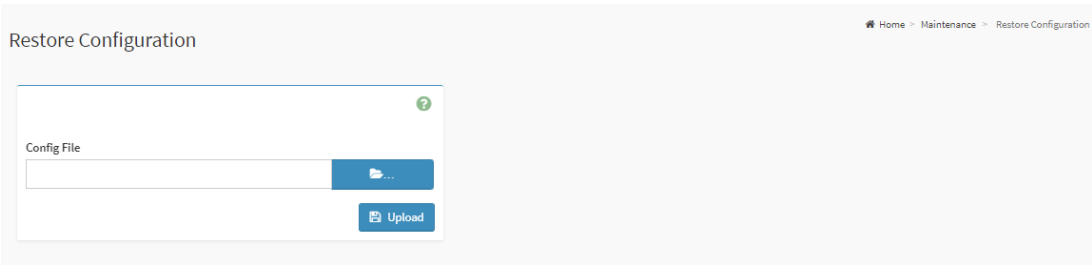


Backup Configuration Page

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

28.12.2 Restore Configuration

This page is used to restore the configuration files from the client system to the BMC.



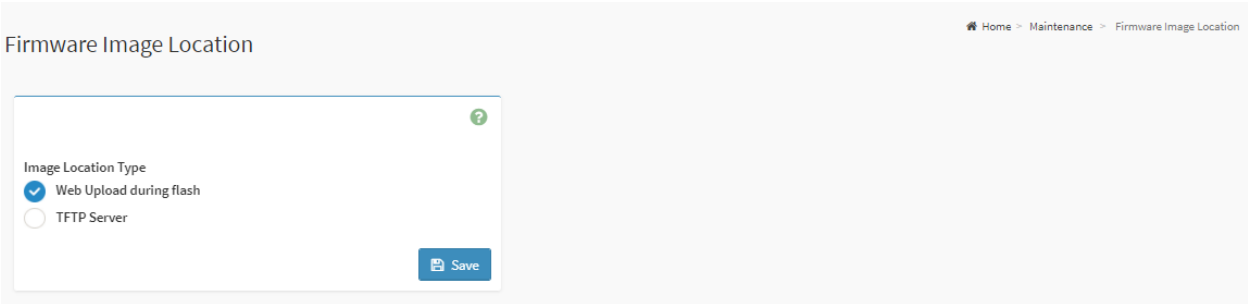
Restore Configuration Page

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

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

28.12.3 Firmware Image Location

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



Firmware Image Location Page

Web Upload during flash: Select the option to transfer the firmware image into the BMC via HTTP/HTTPS.

TFTP Server: Select the option to transfer the firmware image into the BMC via TFTP.

TFTP Server Address: This field will be present if enable **TFTP Server**, the field is used to configure the address of TFTP server.

TFTP Image Name: This field will be present if enable **TFTP Server**, the field is used to configure full source path with filename of TFTP server.

TFTP Retry Count: This field will be present if enable **TFTP Server**, the field is used to configure the number of times to be retried in case a transfer failure occurs.

28.12.4 Firmware Update

This page is used to update BMC firmware.

Firmware Update

The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose 'Firmware Image Location' under Maintenance.

Protocol Type: HTTP/HTTPS

☐ Preserve all Configuration

☐ Preserve Network Settings

☐ Preserve User Account

Select Firmware Image

Choose File

No file chosen

Start firmware update

Firmware Update Page

- Preserve all Configuration:** To preserve all configuration.
- Preserve Network Settings:** To preserve network settings.
- Preserve User Account:** To preserve user accounts.
- Select Firmware Image:** To Select the firmware image to be uploaded.
- Start Firmware Update:** To Start the firmware update.

28.12.5 BIOS Update

This page is used to update BIOS firmware.

BIOS Update

Upgrade BIOS of the host.
Please select BIOS image and press 'Start BIOS update' to start the BIOS update procedure.

Configuration

☐ Preserve BIOS configuration

Option

☒ Immediately shutdown server to flash BIOS

Select BIOS Image

Choose File

No file chosen

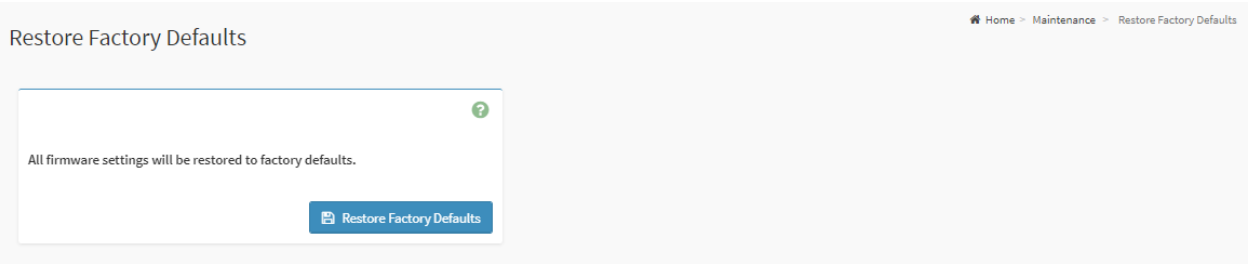
Start BIOS update

BIOS Update Page

- Preserve BIOS configuration:** To preserve BIOS configuration.
- Immediately shutdown server to flash BIOS:** To shutdown server immediately to flash BIOS.
- Start Firmware Update:** To Start the BIOS update.

28.12.6 Restore Factory Defaults

This page is used to restore the factory defaults of the device firmware.



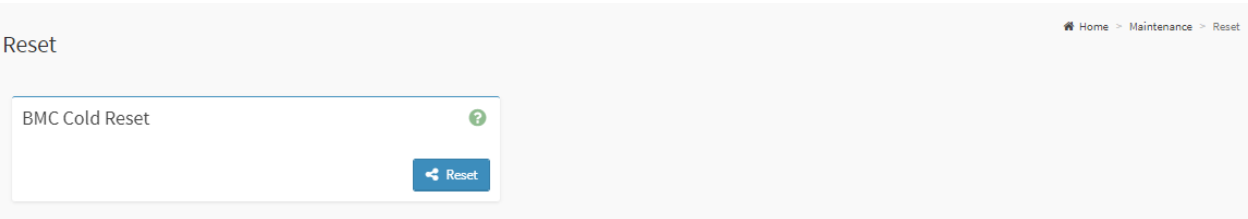
Restore Factory Defaults Page

Restore Factory Defaults: Click the button to restore configuration to **factory default settings**, the following settings will be restored.

- SDR
- SEL
- IPMI
- Network
- NTP
- SSH
- KVM
- Authentication
- Syslog
- Web

28.12.7 Reset

This page is used to reset BMC device.

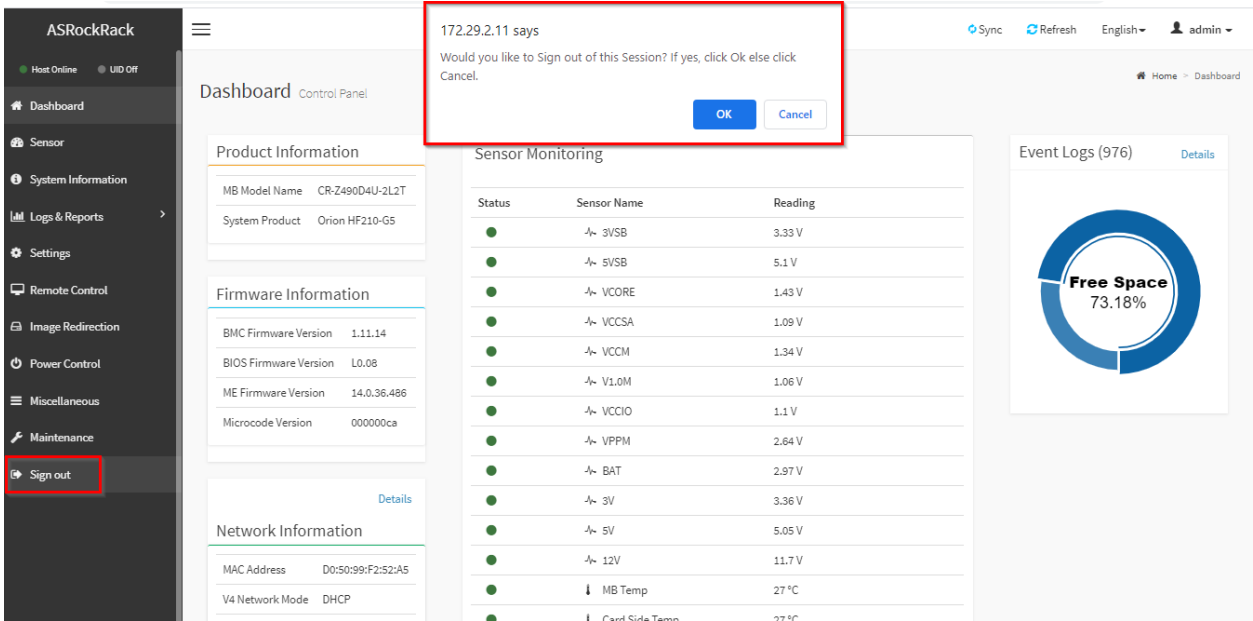


Reset Page

Reset: Click the button to reset the device.

28.13 Sign Out

Click **Sign Out** to perform log out from the Web GUI. A Warning message will be prompted you to proceed further, click **OK** to log out else **Cancel** to retain the Web GUI.

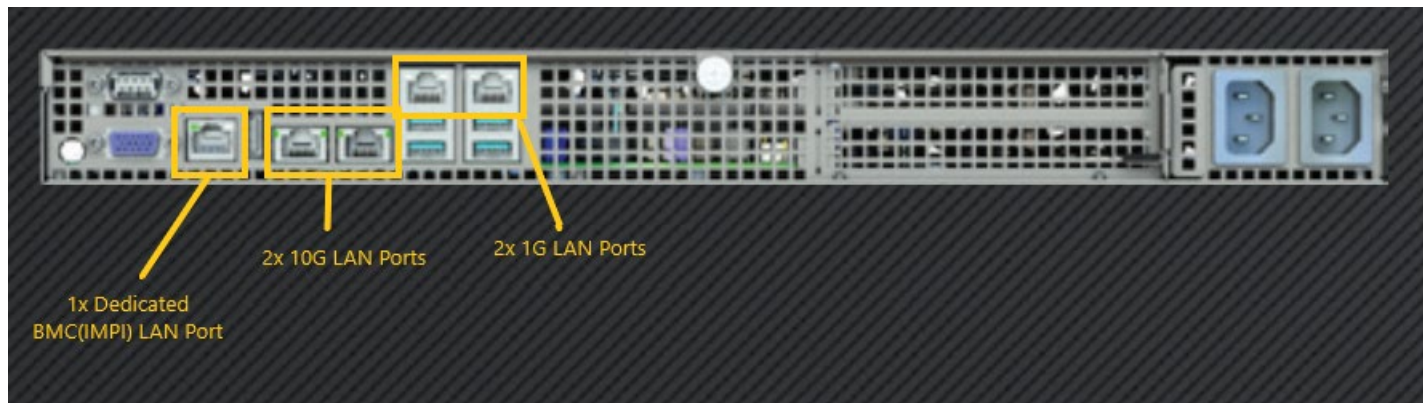


Sign Out Button and Prompt

29. Updating Bios and ME

This section contains information on how to update the BIOS and ME through the BMC port.

Step 1: Insert the network cable in the dedicated BMC/IPMI Lan port.



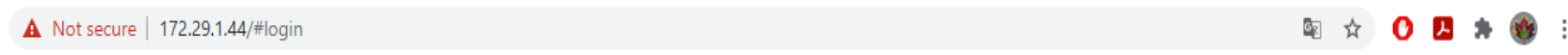
Step 2: Turn ON the machine.

Step 3: Note down the **BMC IP** address detected as shown in the screenshot



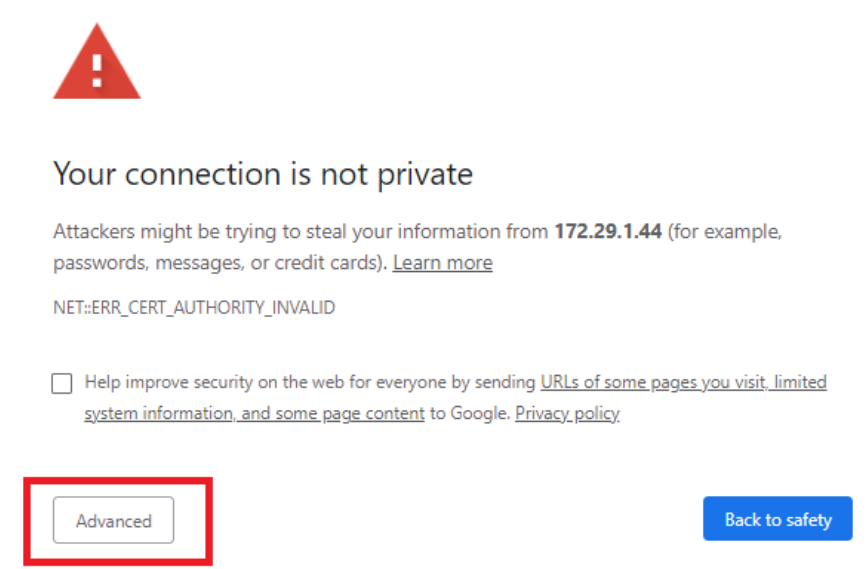
Step 4: Turn off the machine.

Step 5: Go to you computer and open a browser IE or Chrome and then put the BMC IP address on the address bar (ex: [*https://172.29.1.44*]) and press enter.

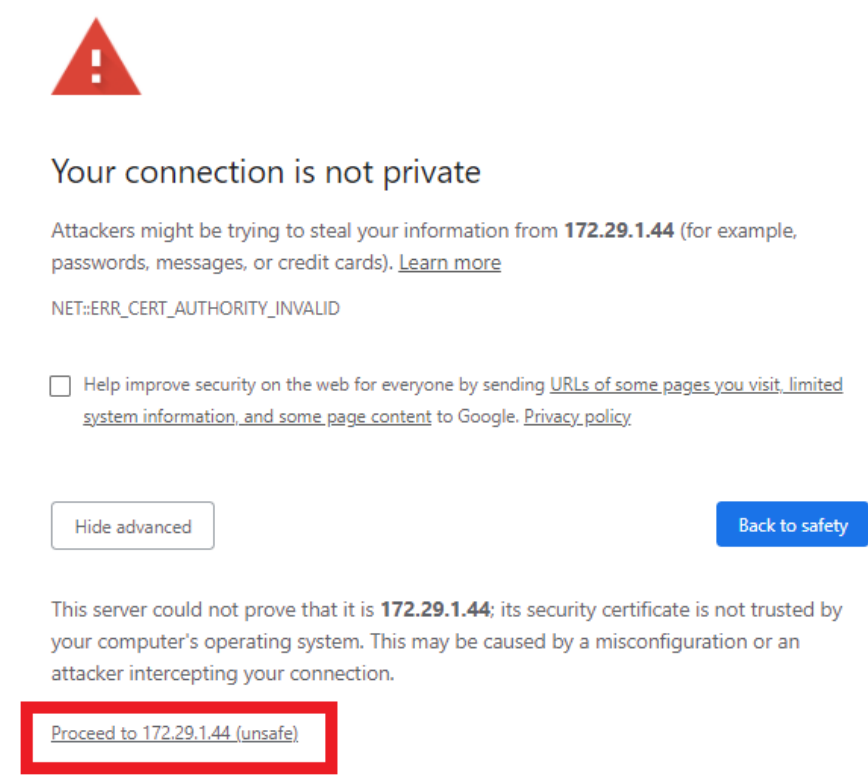


Step 6: If the web page does not open then modify the Browser's **Privacy and Security settings**.

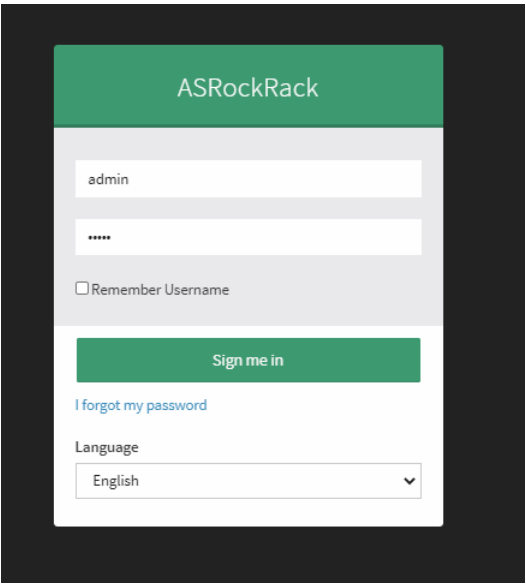
Step 7: Click on ADVANCED



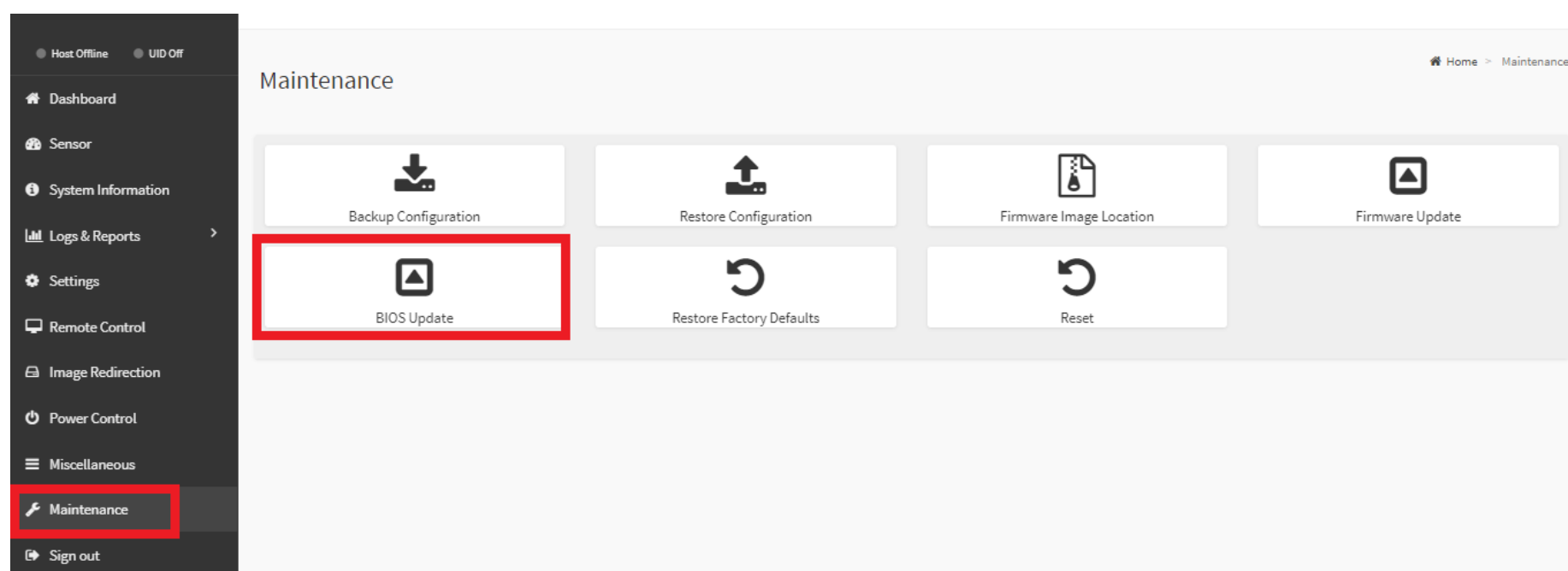
Step 8: Click on Proceed to (...) unsafe



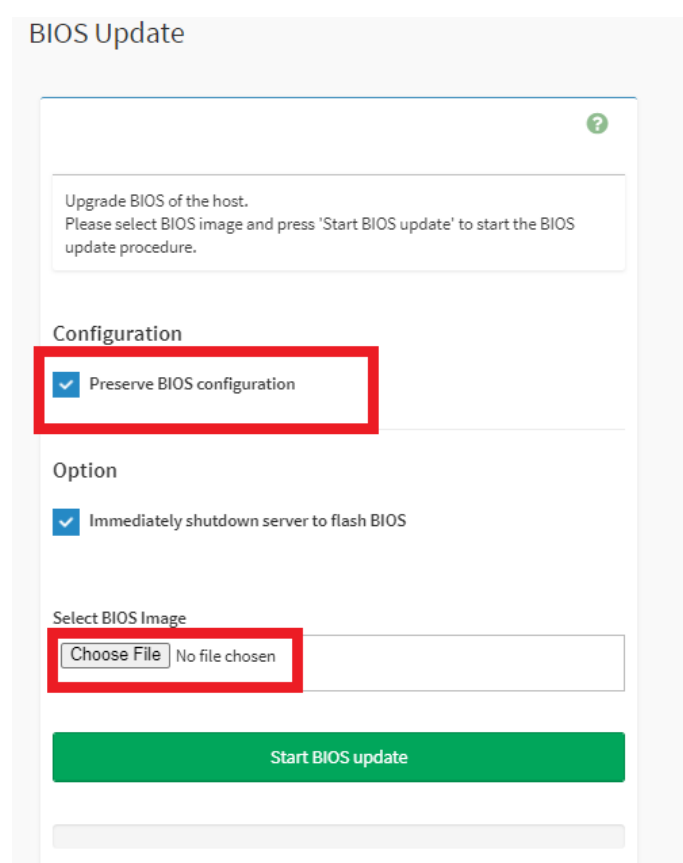
Step 9: Enter a Username: admin and Password: admin



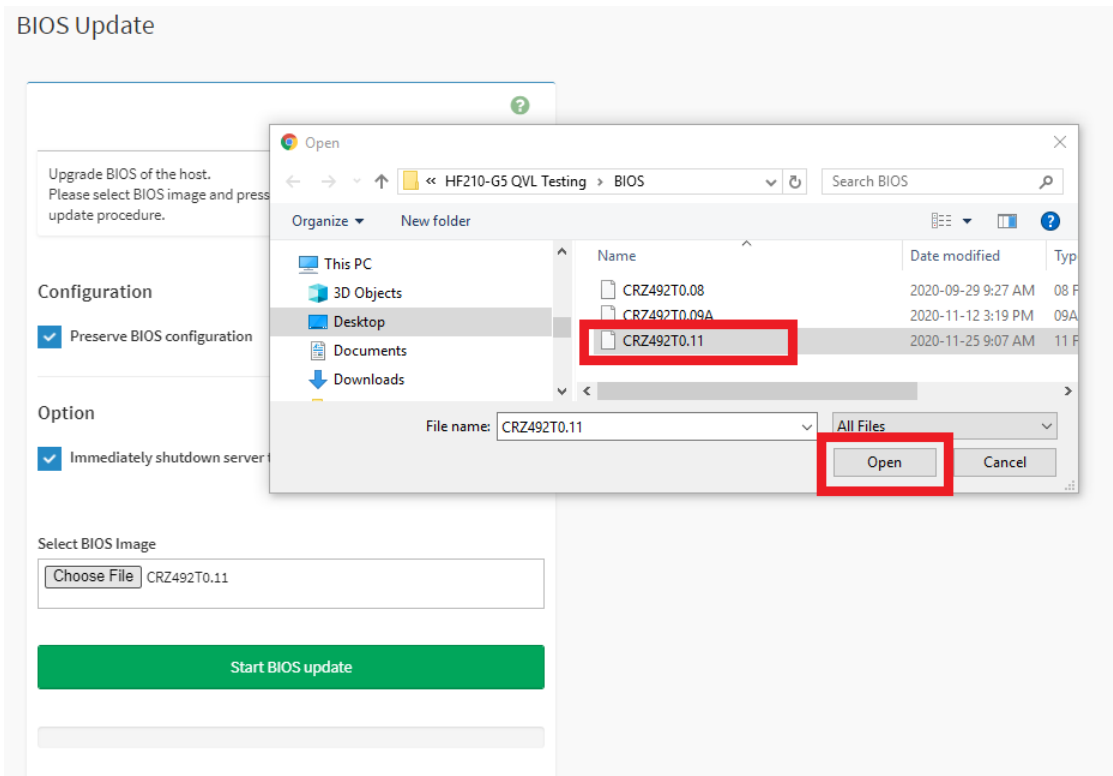
Step 10: Click on Maintenance and then click on BIOS Update



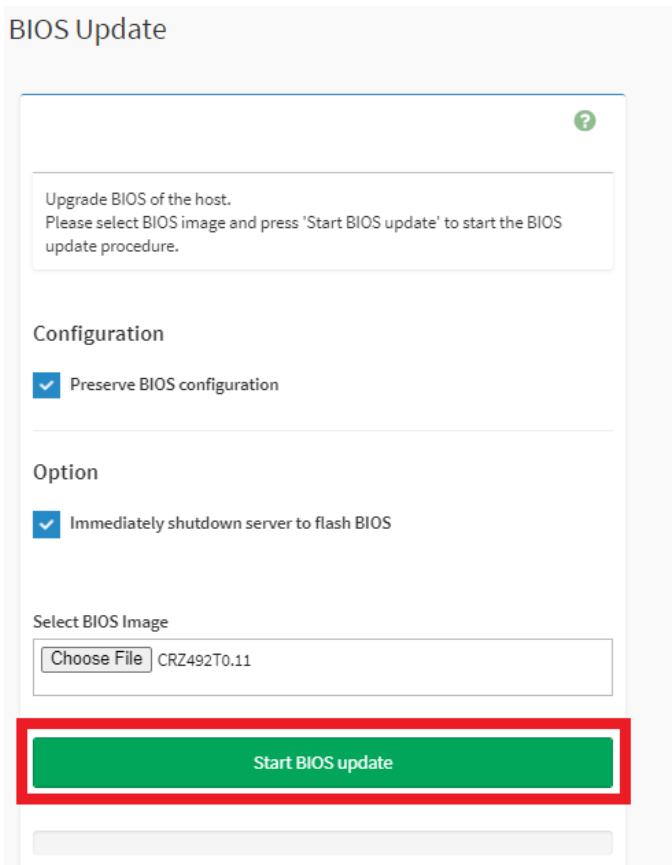
Step 11: Select the Preserve BIOS configuration and then click on Choose File



Step 12: Navigate the folder containing a BIOS then Select the BIOS and click on **Open**



Step 13: Click on **Start BIOS update**



Step 14: Click on OK

BIOS Update

172.29.1.44 says

We will start the BIOS update now. You will not be able to access BIOS until it flashes and restarts. Do you want to continue?

OK

Cancel

Upgrade BIOS of the host.
Please select BIOS image and press 'Start
update procedure.'

Configuration

☒

 Preserve BIOS configuration

Option

☒

 Immediately shutdown server to flash BIOS

Select BIOS Image

Choose File

 CRZ492T0.11

Start BIOS update

Step 15: Wait until the **Processing** Window completes.

BIOS Update

Upgrade BIOS of the host.
Please select BIOS image and press 'Start BIOS update' to start the BIOS
update procedure.

Configuration

☒

 Preserve BIOS configuration

Option

☒

 Immediately shutdown server to flash BIOS

Select BIOS Image

Choose File

 CRZ492T0.11

Processing...

Uploading... 34%

Step 16: Click on **Proceed**

BIOS Update

Upgrade BIOS of the host.
Please select BIOS image and press 'Start BIOS update' to start the BIOS update procedure.

Configuration

☒ Preserve BIOS configuration

Option

☒ Immediately shutdown server to flash BIOS

Select BIOS Image

CRZ492T0.11

BIOS Update

Do you want to continue the update?

Uploading... 100%

Step 17: Click on **OK** to proceed the BIOS update.

BIOS Update

Upgrade BIOS of the host.
Please select BIOS image and press 'Start BIOS update' to start the BIOS update procedure.

Configuration

☒ Preserve BIOS configuration

Option

☒ Immediately shutdown server to flash BIOS

Select BIOS Image

CRZ492T0.11

BIOS Update

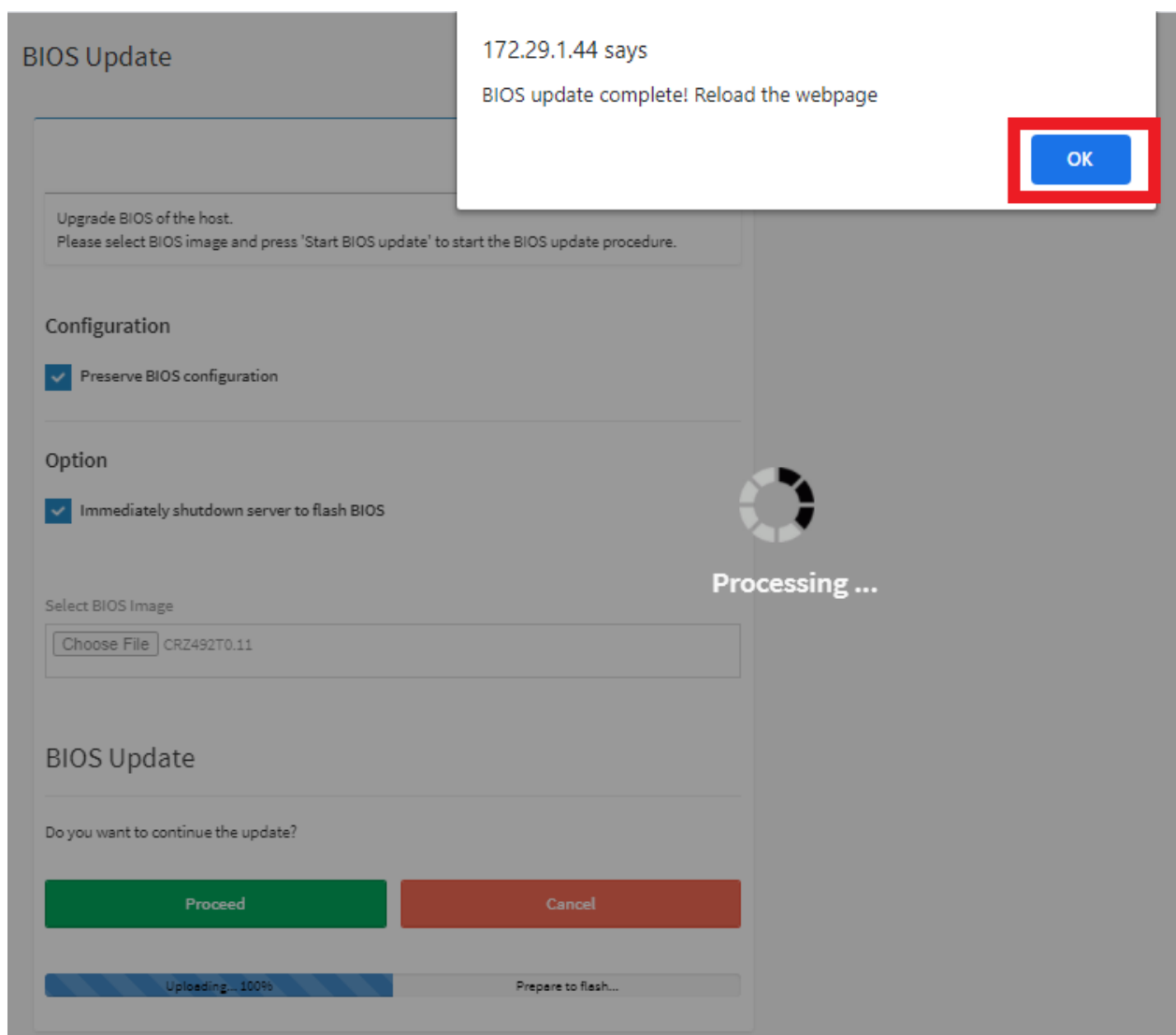
Do you want to continue the update?

Uploading... 100%

172.29.1.44 says

Clicking 'OK' will start the actual upgrade operation, where the storage is written with the new firmware image. It is essential that the upgrade operation is not interrupted once it starts. Do you wish to proceed?

Step 18: Wait until the BIOS update completes and then click on **OK**

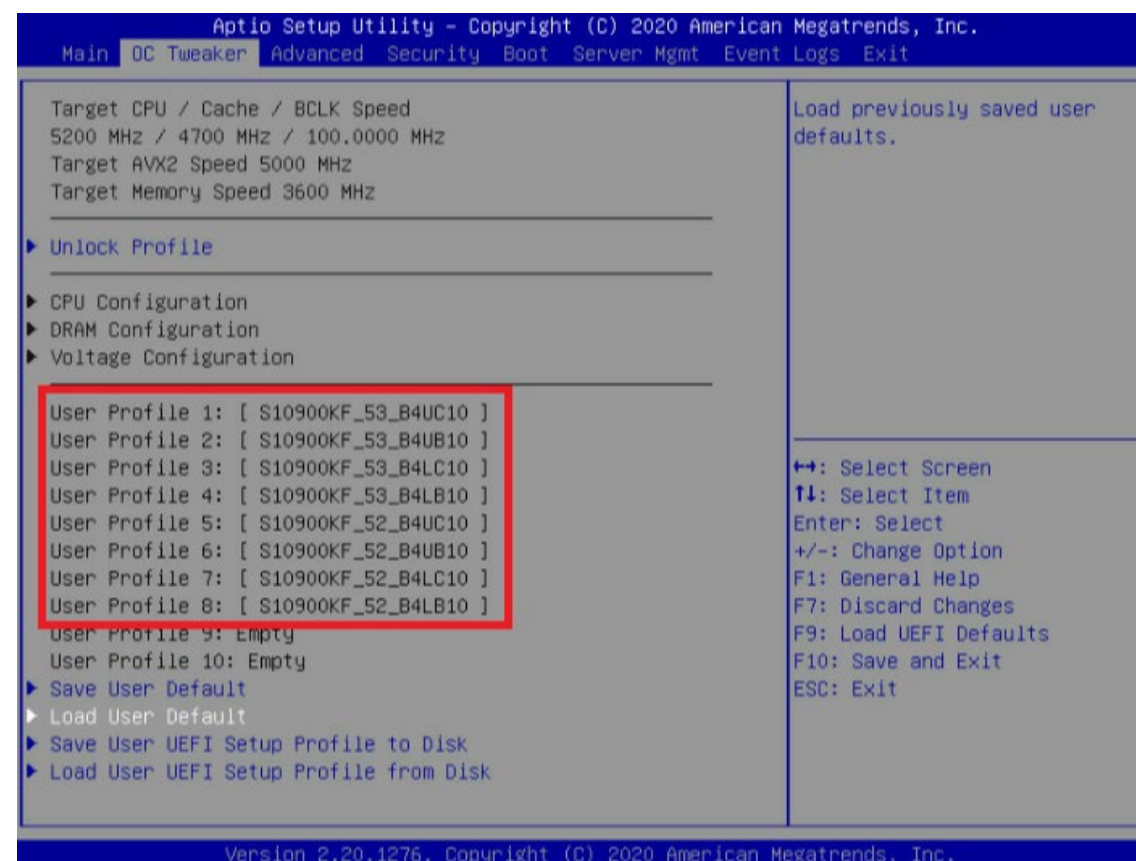


30. Profile Loading in BIOS

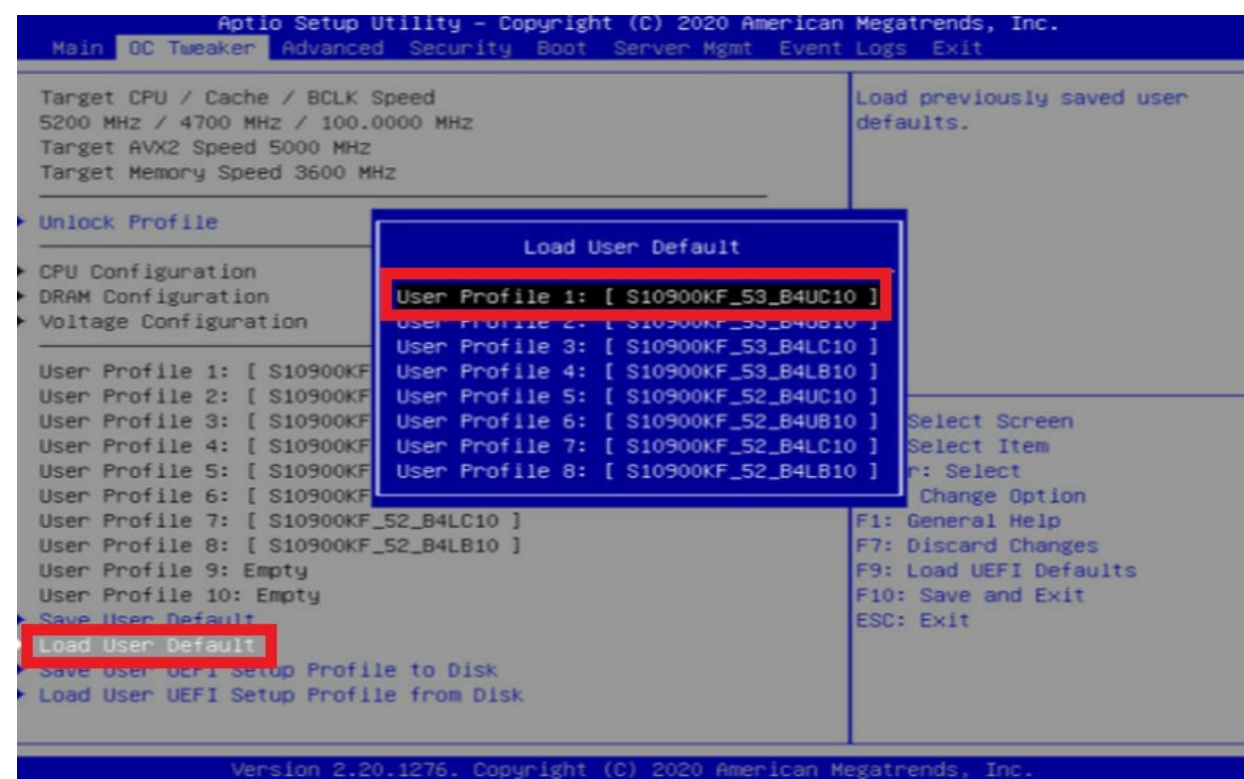
This section contains step-by-step instructions on how to upload the overclocking profile in the BIOS.

Step 1: Turn ON the machine.

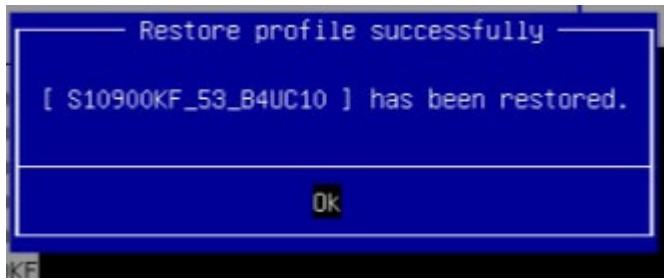
Step 2: Press **DEL** or **F2** continuously while the system is booting in order to get in to the BIOS. Once in the BIOS navigate in to the **OC Tweaker** menu and verify the **User profiles** to be the uploaded.



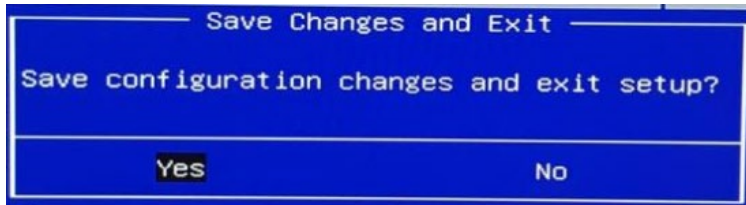
Step 3: Select the **Load User Default**, then select the desired overclocking profiles and press **Enter**



Step 4- Enter **Ok** to restore the profile.



Step 5- Press **F10** and enter **Yes** to save the settings and then reboot the system.



31. Downloading and Uploading a Profile in Linux

This sections contains step-by-step instructions to download and upload the overclocking Profiles with Linux OS in the Orion HF210-G5 systems. The overclocking profiles can be downloaded or uploaded through remote or local system with Linux OS with the OCProfile utility.

31.1 Downloading an existing Overclocking Profile

Step 1: Login in to the Remote or local Linux system with the OCProfile utility.

Step 2: Go in to the OCProfile directory.

```
root@localhost Downloads1# cd OCProfile\ v1.04
```

Step 3: Go under the linux directory and verify the existence of OCProfile utility.

```
root@localhost OCProfile v1.041# dir
los linux win64
root@localhost OCProfile v1.041# cd linux
root@localhost linux1# dir
OCProfile
```

Step 4: Enter the **chmod 777 *** command to modify the file permissions for the OCProfile utility.

```
root@localhost linux1# chmod 777 *
```

Step 5: Execute the following OCProfile command to download the overclocking profile.

To download a single overclocking profile:

```
./OCProfile -H {IP address} -U {username} -P {password} -p 1 -g OCProfileTest1.bin
```

To download the multiple profiles:

```
./OCProfile -H {IP address} -U {username} -P {password} -p 1,2 -g OCProfileTest1.bin,OCProfileTest2.bin
```



The **{IP address}** is the BMC/IPMI ip address of the source system.

The **{username}** and **{password}** is the username and password of BMC/IPMI on the source system.

The **-p** parameter indicates the position of the overclocking profiles in the BIOS of the target system.

The **-g** parameter in the commands indicates to download the profiles.

The Return code shows if the command is successfully pass or fail.

0 = pass.

1 = fail.

Example:

In this example, there are eight multiple profiles being downloaded from the source overclocking profiles system either through a remote or local system with linux OS having OCProfile utility.

```
[root@localhost linux]# ./OCProfile -H 172.29.2.11 -U admin -P admin -p 1,2,3,4,5,6,7,8 -g S10900KF_53_B4UC10.bin,S10900KF_53_B4UB10.bin,S10900KF_53_B4LC10.bin,S10900KF_53_B4LB10.bin,S10900KF_52_B4UC10.bin,S10900KF_52_B4UB10.bin,S10900KF_52_B4LC10.bin,S10900KF_52_B4LB10.bin
ASRockBack OCProfile tool - V1.04
=====
OCM Revision = 0.0.0

Downloading OCProfile1.
Download completed.

Downloading OCProfile2.
Download completed.

Downloading OCProfile3.
Download completed.

Downloading OCProfile4.
Download completed.

Downloading OCProfile5.
Download completed.

Downloading OCProfile6.
Download completed.

Downloading OCProfile7.
Download completed.

Downloading OCProfile8.
Download completed.

Return code = 0.
```

Step 6: Type **ls-l** to verify that the downloaded overclocking profiles under the OCProfile directory.

```
[root@localhost linux]# ls -l
total 3468
-rwxrwxrwx. 1 root root 3452688 Dec  3 15:32 OCProfile
-rw-r--r--. 1 root root  8309 Dec  9 16:13 S10900KF_52_B4LB10.bin
-rw-r--r--. 1 root root  8309 Dec  9 16:12 S10900KF_52_B4LC10.bin
-rw-r--r--. 1 root root  8309 Dec  9 16:12 S10900KF_52_B4UB10.bin
-rw-r--r--. 1 root root  8309 Dec  9 16:11 S10900KF_52_B4UC10.bin
-rw-r--r--. 1 root root  8309 Dec  9 16:11 S10900KF_53_B4LB10.bin
-rw-r--r--. 1 root root  8309 Dec  9 16:10 S10900KF_53_B4LC10.bin
-rw-r--r--. 1 root root  8309 Dec  9 16:10 S10900KF_53_B4UB10.bin
-rw-r--r--. 1 root root  8309 Dec  9 16:09 S10900KF_53_B4UC10.bin
[root@localhost linux]#
```

31.2 Uploading a Overclocking Profile

Step 1: Login in to the Remote or local Linux system with the OCProfile utility.

Step 2: Go in to the OCProfile directory.

```
root@localhost Downloads1# cd OCProfile\ v1.04
```

Step 3: Go under the linux directory and verify the existence of OCProfile utility.

```
root@localhost OCProfile v1.041# dir
dos  linux  win64
root@localhost OCProfile v1.041# cd linux
root@localhost linux1# dir
OCProfile
```

Step 4: Enter the **chmod 777 *** command to modify the file permissions for the OCProfile utility.

```
root@localhost linux1# chmod 777 *
```

Step 5: Execute the following OCProfile command to upload the overclocking profile to a target system.

To download a single overclocking profile:

```
./OCProfile -H {IP address} -U {username} -P {password} -p 1 -s OCProfileTest1.bin
```

To download the multiple profiles:

```
./OCProfile -H {IP address} -U {username} -P {password} -p 1,2 -s OCProfileTest1.bin,OCProfileTest2.bin
```



The **{IP address}** is the BMC/IPMI ip address of the source system.

The **{username}** and **{password}** is the username and password of BMC/IPMI on the target system.

The **-p** parameter indicates the position of the overclocking profiles in the BIOS of the target system.

The **-s** parameter in the commands indicates to upload the profiles.

The Return code shows if the command is successfully pass or fail.

0 = pass.

1 = fail.

Example:

In this example, there are eight multiple profiles being uploaded to target system either through a remote system or local system with linux OS having OCProfile utility.

```
[root@localhost linux]# ./OCProfile -H 172.29.1.44 -U admin -P admin -p 1,2,3,4,5,6,7,8 -s S10900KF_S3_B4UC10.bin,S10900KF_S3_B4UB10.bin,S10900KF_S3_B4LC10.bin,S10900KF_S3_B4LB10.bin,S10900KF_S2_B4UC10.bin,S10900KF_S2_B4UB10.bin,S10900KF_S2_B4LC10.bin,S10900KF_S2_B4LB10.bin
ASRockBack OCProfile tool - V1.04
*****
IPC Revision = 1.11.14

Uploading OCProfile1.
Check file CRC..
The local and remote files are the same.
Upload success.

Uploading OCProfile2.
Check file CRC..
The local and remote files are the same.
Upload success.

Uploading OCProfile3.
Check file CRC..
The local and remote files are the same.
Upload success.

Uploading OCProfile4.
Check file CRC..
The local and remote files are the same.
Upload success.

Uploading OCProfile5.
Check file CRC..
The local and remote files are the same.
Upload success.

Uploading OCProfile6.
Check file CRC..
The local and remote files are the same.
Upload success.

Uploading OCProfile7.
Check file CRC..
The local and remote files are the same.
Upload success.

Uploading OCProfile8.
Check file CRC..
The local and remote files are the same.
Upload success.

Return code = 0.
```

Step 6: To load and activate a profile in BIOS refer to the instructions in shown in the section **32- Loading a Profile in BIOS**

32. Drivers & Tools

This section contains information about the drivers downloading and running common monitoring tools under Linux & windows on the Orion HF210-G5 systems.

32.1 Drivers Downloading

The drivers are available on the Ciara's website: <https://ciartech.com/support-center/> and you can search them either through a Filter or Search.

The screenshot displays the Ciara Support Center website. The header includes the Ciara logo, navigation links (PRODUCTS, SOLUTIONS, SERVICES, INDUSTRIES, COMPANY, CONTACT US), and a SUPPORT button. Below the header, there are three main service options: Customer Support, Knowledge Base, and My Account. The main content area is titled "Product Drivers and Documentation" and features a filterable table. The filter bar includes dropdowns for Product, Driver, and OS Compatibility, along with a Reset button and a search field. The table below has columns for Product, Title, File Type, OS Compatibility, Version, Release Date, File, and File Size.

How Can We Help You?

Customer Support
Technical support for your challenges.

Knowledge Base
Find answers to common questions.

My Account
Log into your user portal.

Product Drivers and Documentation

Filter: Product Driver OS Compatibility Reset Search:

Product	Title	File Type	OS Compatibility	Version	Release Date	File	File Size
---------	-------	-----------	------------------	---------	--------------	------	-----------

32.2 Monitoring CPU Frequency in Linux

This sections contains the information on how to monitor CPU frequencies in the linux through **i7z** and **turbostat** utility.

32.2.1 i7z

The **i7z** is a small open source utility that reports CPU frequency information. The information displayed covers Turbo Boost, frequencies, multipliers, temperature, and times spent in the C0/C1/C3/C6/C7 states.

For **RHEL 7.x**; download using this link: <https://mtlbpccloud2.hypertec-group.com/index.php/s/DLiBeL9FzfCbBXE>

For **RHEL 8.3 or later**; download using this link: <https://mtlbpccloud2.hypertec-group.com/index.php/s/DPchQUsCEV1DKte>

 This needs to be unzipped in the Linux.

For **Ubuntu 18.04, 20.04 or later**; enter the command **apt install i7z** to install and then go to step 3.

 For Ubuntu 18.04 make sure the security fix for **apt upgrade** has installed and **systemd** is updated.

Step 1: In the Terminal, go to the directory where i7z was downloaded.

Step 2: Run the following command to make the file executable:

RHEL 7.x: `chmod +x i7z_64bit`

RHEL 8.x: `chmod +x i7z`

Step 3: Run **i7z** to monitor the CPU frequency:

For **RHEL 7**: Enter the following command If logged in as root: `./i7z_64bit` or If logged in as a standard user: `sudo ./i7z_64bit`

For **RHEL 8, Ubuntu 18.04 and Ubuntu 20.04**: enter the following command If logged in as root: `./i7z` or If logged in as a standard user: `sudo ./i7z`

```
Cpu speed from cpufreq 3311.00MHz
cpufreq might be wrong if cpufreq is enabled. To guess correctly try estimating via tsc
Linux's inbuilt cpu khz code emulated now
True Frequency (without accounting Turbo) 3312 MHz
CPU Multiplier 33x || Bus clock frequency (BCLK) 100.36 MHz

Socket [0] - [physical cores=10, logical cores=10, max online cores ever=10]
TURBO ENABLED on 10 Cores, Hyper Threading OFF
Max Frequency without considering Turbo 3412.36 MHz (100.36 x [341])
Max TURBO Multiplier (if Enabled) with 1/2/3/4/5/6 Cores is 46x/46x/46x/46x/46x/46x
Real Current Frequency 4619.69 MHz [100.36 x 46.03] (Max of below)
Core [core-id] : Actual Freq (Mult.) C0% Halt(C1)% C3 % C6 % Temp
Core 1 [0]: 4611.37 (45.95x) 0 100 0 0 27
Core 2 [1]: 4600.46 (45.84x) 1 99.7 0 0 27
Core 3 [2]: 4600.19 (45.84x) 1 99.6 0 0 25
Core 4 [3]: 4602.66 (45.86x) 1 100 0 0 25
Core 5 [4]: 4619.69 (46.03x) 1 100 0 0 25
Core 6 [5]: 4603.23 (45.87x) 1 99.9 0 0 27
Core 7 [6]: 4602.63 (45.86x) 0 100 0 0 26
Core 8 [7]: 4603.48 (45.87x) 1 100 0 0 25
Core 9 [8]: 4604.17 (45.87x) 0 100 0 0 24
Core 10 [9]: 4599.84 (45.83x) 1 99.9 0 0 24
```

Frequency → RED --- Turbo Multiplier (confirms if overclock is set) → BLUE

32.2.2 Turbostat

The **turbostat** is the base install utility in the linux and in case it is not possible to install or use **i7z** then run you can run **turbostat** and verify **Bzy_Mhz** for an actual frequency.

```
[root@localhost ~]# turbostat
cpu0: Guessing tjMax 100 C, Please use -T to specify
Core CPU Avg_MHz Busy% Bzy_MHz TSC_MHz IRQ CoreTmp PkgTmp CPU%LPI SYS%LPI
- - - - -
0 0 0 0.01 5294 3696 763 15 15 0.00 0.00
1 1 0 0.00 5295 3696 524 13 15 0.00 0.00
2 2 0 0.00 5292 3696 14 13
3 3 0 0.00 5290 3696 5 14
4 4 1 0.01 5295 3696 40 15
5 5 1 0.02 5294 3696 123 13
6 6 0 0.00 5294 3696 12 13
7 7 0 0.00 5289 3696 17 15
8 8 0 0.00 5302 3696 10 15
9 9 0 0.00 5294 3696 6 14
0 0 0 0.00 5294 3696 12 12
```

32.3 Verifying CPU Frequency for Windows

This sections contains the information how to download and monitor CPU frequencies in the Windows through **HWiNFO64** utility.

The Hwinfo64 utility for Windows available on website: <https://www.hwinfo.com/download/>

Run the **HWiNFO64**, verify the appropriate **Core # Clock** and **Core # Ratio** (depending on overclocking profiles).

Core 0 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,298.3 MHz
Core 1 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,298.3 MHz
Core 2 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,298.3 MHz
Core 3 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,298.3 MHz
Core 4 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,298.3 MHz
Core 5 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,298.3 MHz
Core 6 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,297.0 MHz
Core 7 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,297.0 MHz
Core 8 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,297.0 MHz
Core 9 Clock	5,300.0 MHz	5,098.8 MHz	5,302.6 MHz	5,297.0 MHz
Bus Clock	100.0 MHz	99.9 MHz	100.0 MHz	100.0 MHz
Ring/LLC Clock	4,800.0 MHz	4,796.5 MHz	4,802.4 MHz	4,799.6 MHz

Core 0 Ratio	53.0 x	51.0 x	53.0 x
Core 1 Ratio	53.0 x	51.0 x	53.0 x
Core 2 Ratio	53.0 x	51.0 x	53.0 x
Core 3 Ratio	53.0 x	51.0 x	53.0 x
Core 4 Ratio	53.0 x	51.0 x	53.0 x
Core 5 Ratio	53.0 x	51.0 x	53.0 x
Core 6 Ratio	53.0 x	51.0 x	53.0 x
Core 7 Ratio	53.0 x	51.0 x	53.0 x
Core 8 Ratio	53.0 x	51.0 x	53.0 x
Core 9 Ratio	53.0 x	51.0 x	53.0 x
Uncore Ratio	48.0 x	48.0 x	48.0 x