Lanner

Network Appliance Platform

Hardware Platforms for Network Computing

HAN-9820C
Technical Overview

Version: 1.8

Date of Release: 18 June 2023

About this Document

This document is the overview of the various functionalities of this product, and the information you need to check before operation. It is intended for those who are:

- responsible for installing, administering and troubleshooting this system or Information Technology professionals.
- assumed to be qualified in the servicing of computer equipment, such as professional system integrators, or service personnel and technicians.

The latest version of this document can be found on Lanner's official website, available either through the product page or through the Lanner Download Center page with a login account and password.

Icon Description

The icons are used in the manual to serve as an indication of interest topics or important messages.

Icon	Usage
Note or Information	This mark indicates that there is something you should pay special attention to while using the product.
Warning or Important	This mark indicates that there is a caution or warning and it is something that could damage your property or product.

Online Resources

To obtain additional documentation resources and software updates for your system, please visit the Lanner Download Center. As certain categories of documents are only available to users who are logged in, please be registered for a Lanner Account at http://www.lannerinc.com/ to access published documents and downloadable resources.

Technical Support

In addition to contacting your distributor or sales representative, you could submit a request at our Lanner Technical Support and fill in a support ticket to our technical support department.

Documentation Feedback

Your feedback is valuable to us, as it will help us continue to provide you with more accurate and relevant documentation. To provide any feedback, comments or to report an error, please email contact@lannerinc.com. Thank you for your time.

Copyright and Trademarks

Contact Information

Taiwan Corporate Headquarters

Lanner Electronics Inc.

7F, No.173, Sec.2, Datong Rd.

Xizhi District, New Taipei City 22184,

Taiwan

立端科技股份有限公司

221 新北市汐止區

大同路二段 173 號 7 樓

T: +886-2-8692-6060

F: +886-2-8692-6101

E: contact@lannerinc.com

China

Beijing L&S Lancom Platform Tech. Co., Ltd.

Guodong LOFT 9 Layer No. 9 Huinan Road,

Huilongguan Town, Changping District, Beijing

102208 China

T: +86 010-82795600

F: +86 010-62963250

E: service@ls-china.com.cn

USA

Lanner Electronics Inc.

47790 Westinghouse Drive

Fremont, CA 94539

T: +1-855-852-6637

F: +1-510-979-0689

E: sales_us@lannerinc.com

Canada

Lanner Electronics Canada Ltd

3160A Orlando Drive

Mississauga, ON

L4V 1R5 Canada

T: +1 877-813-2132

F: +1 905-362-2369

E: sales_ca@lannerinc.com

Europe

Lanner Europe B.V.

Wilhelmina van Pruisenweg 104

2595 AN The Hague

The Netherlands

T: +31 70 701 3256

E: sales_eu@lannerinc.com

Acknowledgment

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Note

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

Important

1. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.
2. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

Safety Guidelines

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Do not wear loose clothing or jewelry that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Disconnect all power by turning off the power and unplugging the power cord before installing or removing a chassis or working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit; always check the circuit.

Consignes de sécurité

Suivez ces consignes pour assurer la sécurité générale :

- Laissez la zone du châssis propre et sans poussière pendant et après l'installation.
- Ne portez pas de vêtements amples ou de bijoux qui pourraient être pris dans le châssis. Attachez votre cravate ou écharpe et remontez vos manches.
- Portez des lunettes de sécurité pour protéger vos yeux.
- N'effectuez aucune action qui pourrait créer un danger pour d'autres ou rendre l'équipement dangereux.
- Coupez complètement l'alimentation en éteignant l'alimentation et en débranchant le cordon d'alimentation avant d'installer ou de retirer un châssis ou de travailler à proximité de sources d'alimentation.
- Ne travaillez pas seul si des conditions dangereuses sont présentes.
- Ne considérez jamais que l'alimentation est coupée d'un circuit, vérifiez toujours le circuit. Cet appareil génère, utilise et émet une énergie radiofréquence et, s'il n'est pas installé et utilisé conformément aux instructions des fournisseurs de composants sans fil, il risque de provoquer des interférences dans les communications radio.

Lithium Battery Caution

- There is risk of explosion if the battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.
- Installation should be conducted only by a trained electrician or only by an electrically trained person who knows all installation procedures and device specifications which are to be applied.
- Do not carry the handle of power supplies when moving to another place.
- Please conform to your local laws and regulations regarding safe disposal of lithium battery.
- Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery can result in an explosion.
- Leaving a battery in an extremely high temperature environment can result in an explosion or the leakage of flammable liquid or gas.
- A battery subjected to extremely low air pressure may result in an explosion or the leakage of flammable liquid or gas.

Avertissement concernant la pile au lithium

- Risque d'explosion si la pile est remplacée par une autre d'un mauvais type.
- Jetez les piles usagées conformément aux instructions.
- L'installation doit être effectuée par un électricien formé ou une personne formée à l'électricité connaissant toutes les spécifications d'installation et d'appareil du produit.
- Ne transportez pas l'unité en la tenant par le câble d'alimentation lorsque vous déplacez l'appareil.

Operating Safety

- Electrical equipment generates heat. Ambient air temperature may not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Be sure that the room in which you choose to operate your system has adequate air circulation.
- Ensure that the chassis cover is secure. The chassis design allows cooling air to circulate effectively. An open chassis permits air leaks, which may interrupt and redirect the flow of cooling air from internal components.
- Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when

electronic components are improperly handled and can result in complete or intermittent failures. Be sure to follow ESD-prevention procedures when removing and replacing components to avoid these problems.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. If no wrist strap is available, ground yourself by touching the metal part of the chassis.
- Periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

Sécurité de fonctionnement

- L'équipement électrique génère de la chaleur. La température ambiante peut ne pas être adéquate pour refroidir l'équipement à une température de fonctionnement acceptable sans circulation adaptée. Vérifiez que votre site propose une circulation d'air adéquate.
- Vérifiez que le couvercle du châssis est bien fixé. La conception du châssis permet à l'air de refroidissement de bien circuler. Un châssis ouvert laisse l'air s'échapper, ce qui peut interrompre et rediriger le flux d'air frais destiné aux composants internes.
- Les décharges électrostatiques (ESD) peuvent endommager l'équipement et gêner les circuits électriques. Des dégâts d'ESD surviennent lorsque des composants électroniques sont mal manipulés et peuvent causer des pannes totales ou intermittentes. Suivez les procédures de prévention d'ESD lors du retrait et du remplacement de composants.
- Portez un bracelet anti-ESD et veillez à ce qu'il soit bien au contact de la peau. Si aucun bracelet n'est disponible, reliez votre corps à la terre en touchant la partie métallique du châssis.
- Vérifiez régulièrement la valeur de résistance du bracelet antistatique, qui doit être comprise entre 1 et 10 mégohms (Mohms).

Mounting Installation Precautions

The following should be put into consideration for rack-mount or similar mounting installations:

- Do not install and/or operate this unit in any place that flammable objects are stored or used in.
- The installation of this product must be performed by trained specialists; otherwise, a non-specialist might create the risk of the system's falling to the ground or other damages.
- Lanner Electronics Inc. shall not be held liable for any losses resulting from insufficient strength for supporting the system or use of inappropriate installation components.
- Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Grounding - Reliable grounding of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- Instruction for the installation of the conductor to building earth by a skilled person.

Electrical Safety Instructions

Before turning on the device, ground the grounding cable of the equipment. Proper grounding (grounding) is very important to protect the equipment against the harmful effects of external noise and to reduce the risk of electrocution in the event of a lightning strike. To uninstall the equipment, disconnect the ground wire after turning off the power. A ground wire (green-and-yellow) is required and the part connecting the conductor must be greater than 6 mm2 or 8AWG.

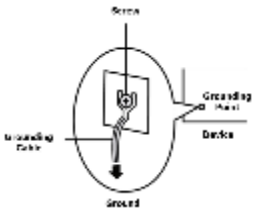
Consignes de sécurité électrique

- Avant d'allumer l'appareil, reliez le câble de mise à la terre de l'équipement à la terre.
- Une bonne mise à la terre (connexion à la terre) est très importante pour protéger l'équipement contre les effets

néfastes du bruit externe et réduire les risques d'électrocution en cas de foudre.
- Pour désinstaller l'équipement, débranchez le câble de mise à la terre après avoir éteint l'appareil.
- Un câble de mise à la terre est requis et la zone reliant les sections du conducteur doit faire plus de 6 mm2 ou 8 AWG.

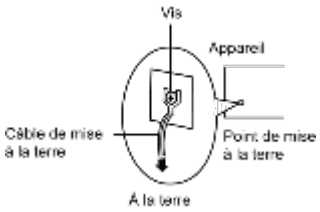
Grounding Procedure for This Device

- Connect the grounding cable to the ground.
- The protection device for the DC power source must provide 40A current.
- This protection device must be connected to the power source before DC power.



Procédure de mise à la terre l'équipement

- Branchez le câble de mise à la terre à la terre.
- L'appareil de protection pour la source d'alimentation CC doit fournir 40A de courant.
- Cet appareil de protection doit être branché à la source d'alimentation avant l'alimentation CC.



Warning

- This equipment must be grounded. The power cord for product should be connected to a socket-outlet with earthing connection.
- Product shall be used with Class 1 laser device modules.
- Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.
- The machine can only be used in a restricted access location and be installed and serviced by skilled person.

Avertissement

- Cet équipement doit être mis à la terre. La fiche d'alimentation doit être connectée à une prise de terre correctement câblée
- Le produit doit être utilisé avec des modules de dispositifs laser de classe 1.
- Peut être installé dans des salles de matériel de traitement de l'information conformément à l'article 645 du National Electrical Code et à la NFPA 75.
- Les matériels sont destinés à être installés dans des EMPLACEMENTS À ACCÈS RESTREINT.

For DC input, this unit is intended to be supplied by an UL listed power source, rated 48 to 72Vdc, 40A min, and an altitude operation 5000m min.

TABLE OF CONTENTS

CHAPTER 1: PRODUCT OVERVIEW

Thank you for choosing HAN-9820C. HAN-9820C is a 2U 19" rackmount network security appliance featuring dual 3rd Gen Intel® Xeon® Scalable Processor, higher throughputs, built-in crypto acceleration and exceptional NIC/Storage module expansion. HAN-9820C accommodates up to twenty-four 288-pin DDR4 R-DIMM/LRDIMM at 2133/2400/2666/2933/3200 MHz, providing up to 1536GB of system memory.

System Specifications

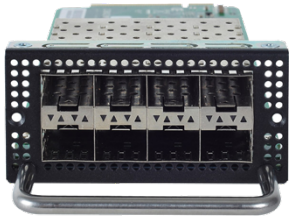
Form Factor		2U 19" Rackmount
Platform	Processor Options	3rd Gen Intel® Xeon® Processor Scalable Family (Ice Lake-SP)
	CPU Socket	2x LGA4189
	Chipset	Intel® C627A
	Security Acceleration	Intel® QuickAssist Technology
BIOS		UEFI compliant, Secure boot, IPMI, Recovery BIOS, IPv4/IPv6 remote, HTTP and HTTPS Boot
System Memory	Technology	DDR4 2133/2400/2666/2933 MHz R-DIMM / LRDIMM support advanced ECC;Scrubbing; SDDC; ADDDC
	Max. Capacity	1536GB
	Socket	24x 288-pin DIMM
Networking	Ethernet Ports	2x GbE RJ45 Intel® i350-AM2
	Bypass	Depends on NIC module specifications
	NIC Module Slot	Module up to 16 port GbE RJ45
Light Out Management	IO Interface	1 x LOM Port via BMC for Integrated Remote Access Controller (memory 1024 MB)
I/O Interface	Reset Button	1x Reset Button
	LED Indicators	Power/Status/Storage
	Power Button	1x ATX Power Switch
	Console Port	1x RJ45 Console Port
	USB Port	2x USB 3.0 Port
	LCD Module	2x20CharacterLCDw/4xKeypads for system info and debug)
	Display Port	1x VGA Port
	Power Input	AC/DC power inlet on PSU
Storage	HDD/SSD Sata Support	2x 3.5" HDD bay hot swap (optinal) 8x 2.5" HDD/SSD bay hot swap support upto 61.4TB (based on installed disk) 2x microSD/SD card support 16/32/64 GB (optinal)
	Onboard Slots	2x M.2 NVME 2280; 1x M.2 2280 SATA
Expansion	PCIe	1x PCIe x4/8/16 Gen 4 FH/FL
	Mini PCIe	N/A
Environmental Parameters	Temperature	0~40oC Operating, -40~70oC Non-Operating
	Humidity (RH)	5~90% Operating, ~95% Non-Operating
	Anti- Vibration	3 H z ~ 5 H z
Cooling	Processor	Passive CPU heat sink
	System	4 x Individual Hot-swappable Cooling Fans With Smart Fan
Security	System	Silicon root of trust, Secure Boot Secure Erase, TPM 2.0

	Remote Management	Support IPMI 2.0 Support TLS 1.3 over HTTP, HTTPS
System Dimensions	(WxDxH) Weight	438 x 720 x 88 mm 19.3 kg
Operating system	Windows Server	2012/2012R/2016/2019
	Linux kernel 4.19.x or higher	Red Hat/SUSE/Ubuntu/Debian/Centos
Power	Type/Watts	1300 W/2000 W AC 1+1 Redundant (option) Or 1600W DC 1+1 Redundant
	Input	AC 100~240V @50~60Hz
Approvals and Compliance		RoHS, CE Class A, FCC Class A, UL

Front Panel

No.	Description	
F1	Reset Button	1x Software reset button
F2	LED Indicators	 System Power System Status HDD Activity
F3	USB Port	2x USB 3.0 Ports
F4	RJ45 Port	2x RJ45 Ports w/ LED for Dual MGT (support PXE; enabled as default)
F5	LOM Port	1x LOM Port for remote management
F6	Console Port	1x RJ45 Console Port
F7	HDD Tray w/ LED Indicators	2x 2.5″/3.5″ HDD Tray  HDD Status HDD Activity
F8	NCS2 Module	8x Standard NIC/Storage/ Module Slots (each Storage module support 2x2.5 inch SATA SDD/HDD)

NCS2 Module
LCD



NCS2 Module
SFP Gbps
Network port

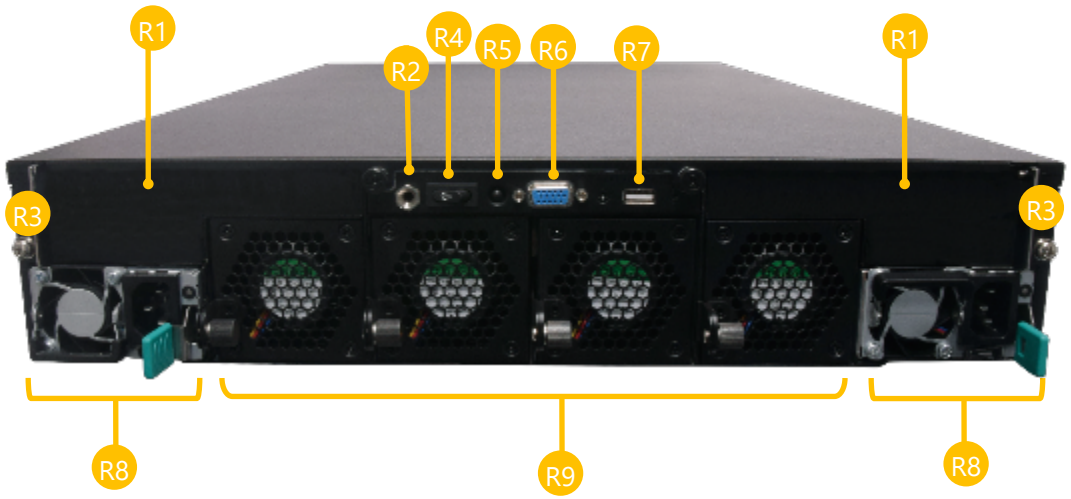
NCS2 Module
RJ-45 Gbps
Network port

NCS2 Module
2x 2.5 inch
HDD/SSD Sata

Note: Please refer to Appendix A: LED Indicator Explanations for descriptions of the LED Indicators.

Rear Panel

HAN-9820C

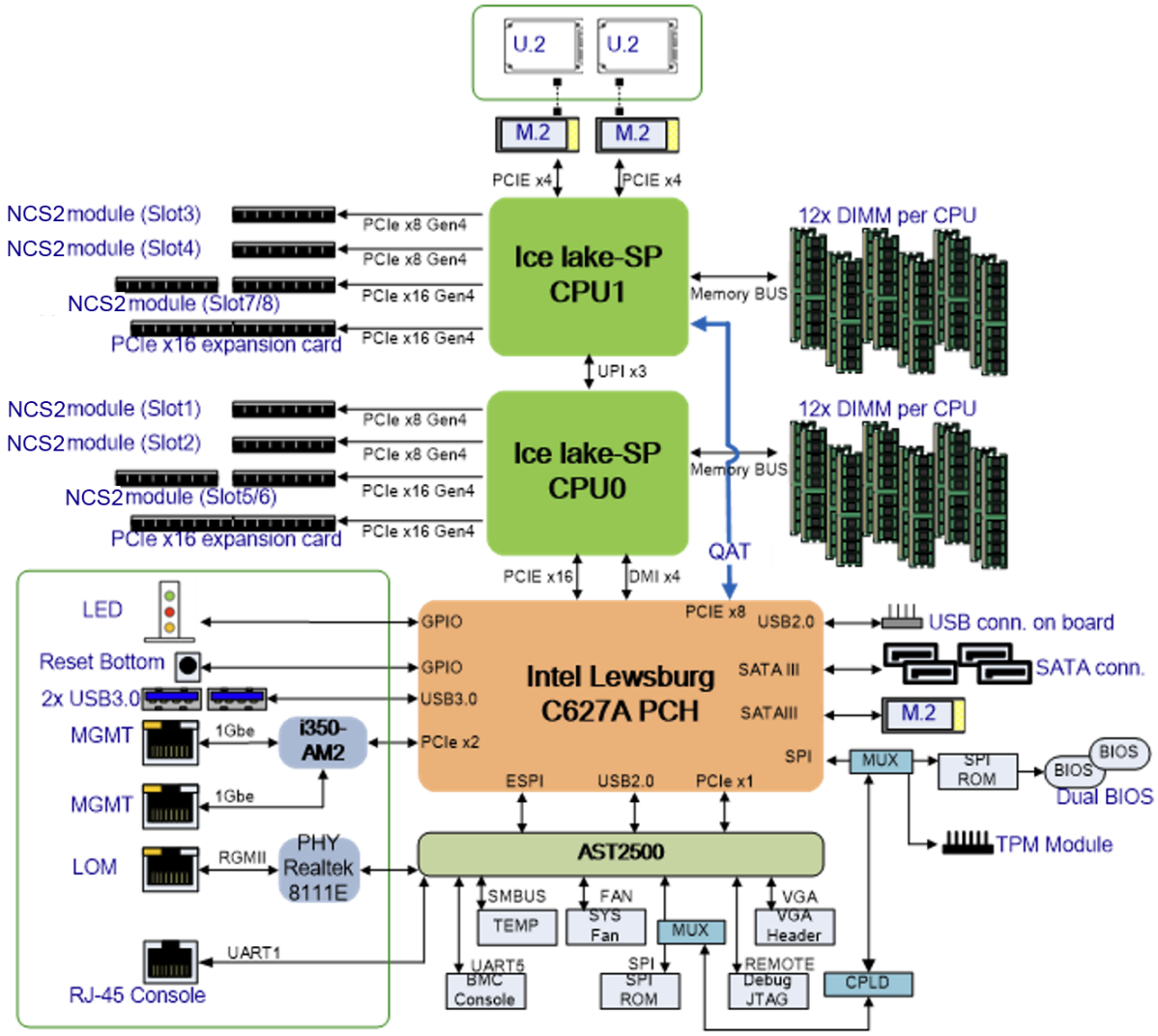


No.	Description	
R1	Rear PCIe Expansion	1x PCIE x16 FH/FL Single-slot Bracket at Left Rear Side (optional); 1x PCIE x16 FH/HL Single-slot Bracket at Right Rear Side (optional); Support up to 75W for each side
R2	ESD Jack	1x Semi-Shearing hole for ESD screws
R3	Ground Hole	2x Semi-Shearing hole for grounding screws
R4	Power Switch	1x Power Button
R5	Alarm off Button	An audible alarm will sound when the system's redundant power is missing. Press this button to turn the alarm off.
R6	VGA	1x DB15
R7	USB Port	1x Semi-Shearing hole by USB type (Optional)
R8	Power Supply	2x 1300W AC Redundant (N+1 Design); 1600W DC Redundant (Optional)
R9	Smart Fans	4x Independent Swappable Fans

CHAPTER 2: MOTHERBOARD INFORMATION

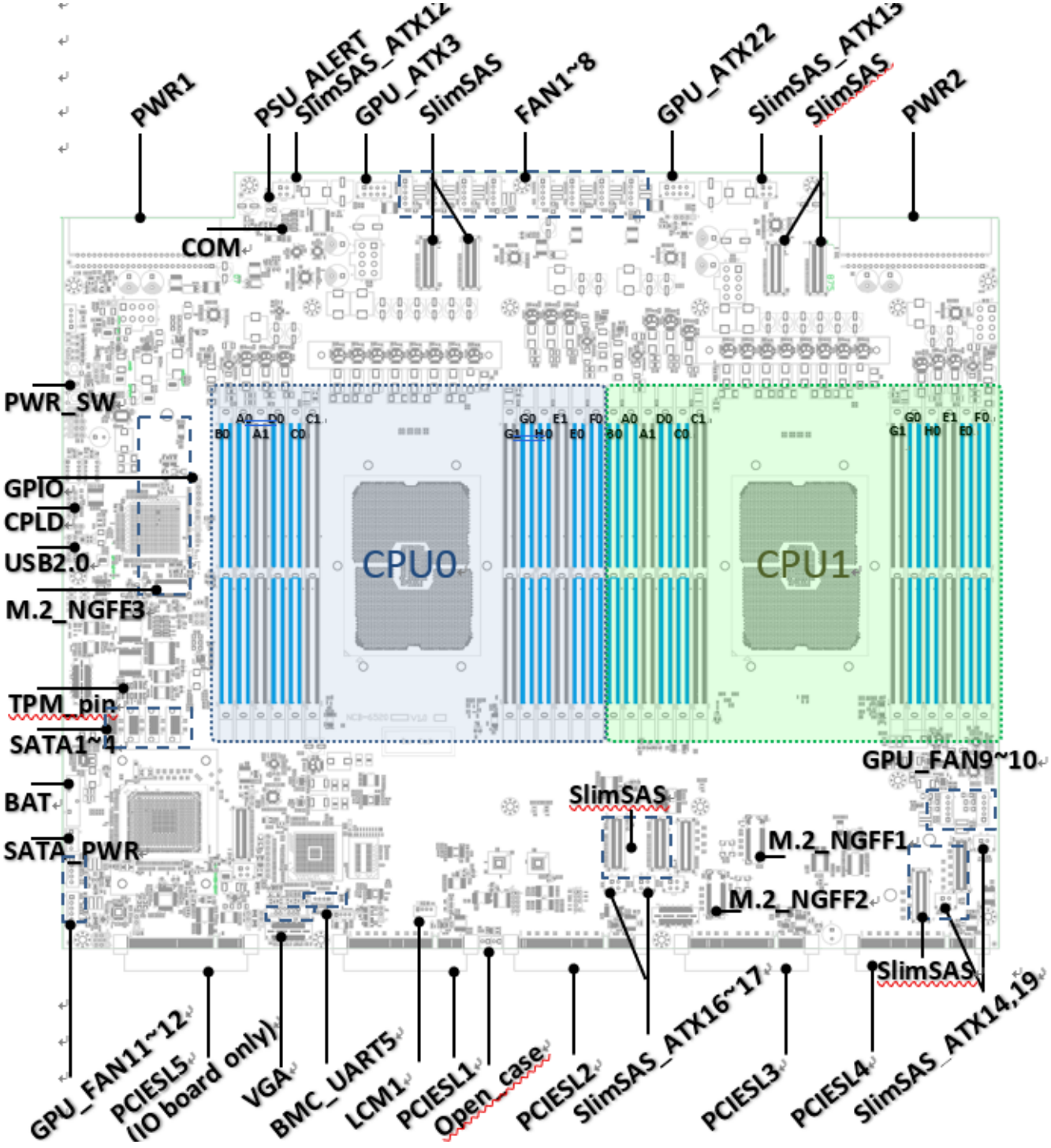
Block Diagram

The block diagram indicates how data flows among components on the motherboard. Please refer to the following figure for the motherboard layout design.



Motherboard Layout

The motherboard layout shows the connectors and jumpers on the board. Refer to the following picture as a reference of the pin assignments and the internal connectors.



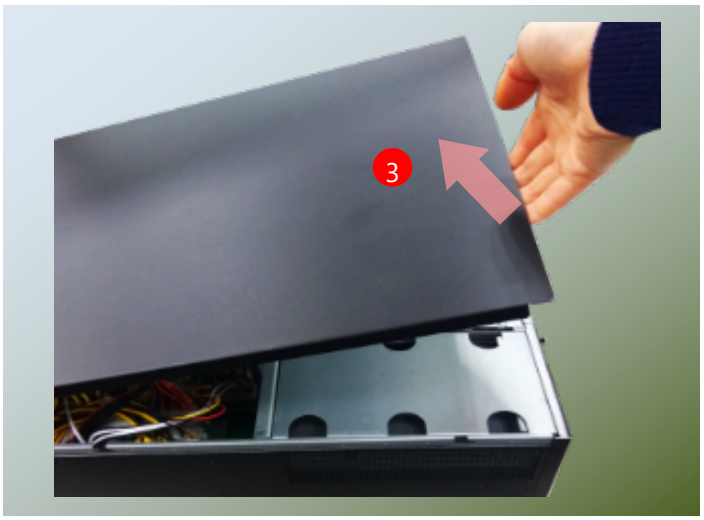
CHAPTER 3: HARDWARE COMPONENTS

System Chassis

1. Loosen the 2 thumb screws from the rear panel of HAN-9820C.

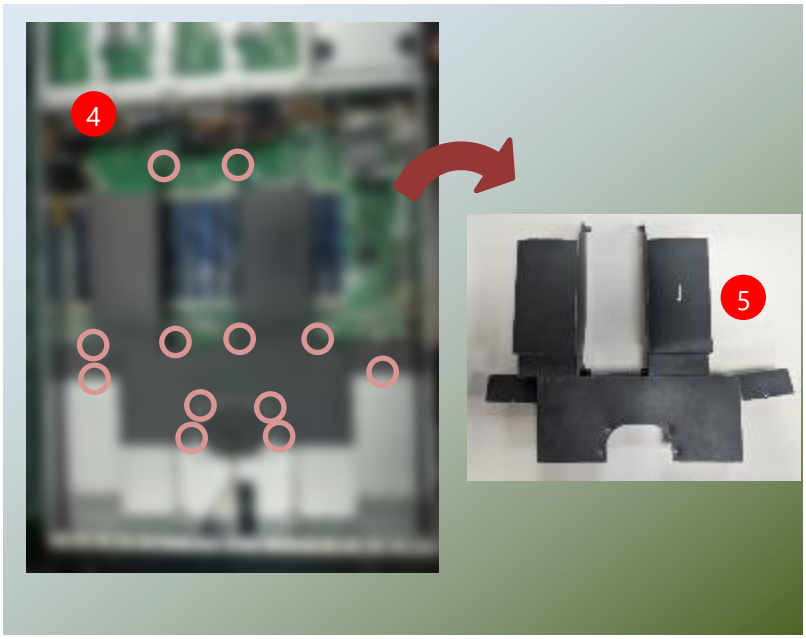
2. Gently pull the cover backward a bit.

3. Lift the cover up to remove it.



4. Unscrew the twelve (12) screws securing the cover/hood that protects the CPUs and the fans.

5. Lift up the cover/hood and place it aside. Please follow the instructions below to install the processor and heatsink module.



System the CPU

Please note that the system delivered to you includes the heatsink and processor. This processor comes with a rather sophisticated design, therefore, the assembly of which must be handled with exclusive tools and extreme care by professionals. Please read through the instructions in this section and refer to the official tutorial released by Intel® to make sure you have acquired the necessary knowledge and comply with the requirements.

Installing the processor onto the motherboard involves two stages:

1. Mount the processor onto the heat sink to make a PHM (Processor + Heat Sink Module)
2. Install the PHM onto the motherboard.

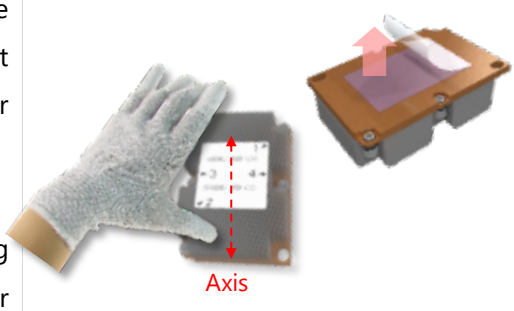
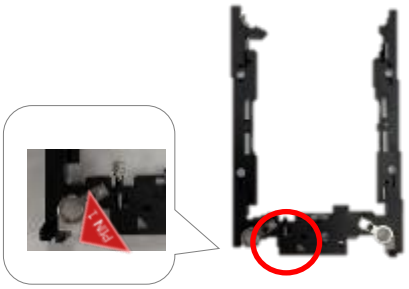
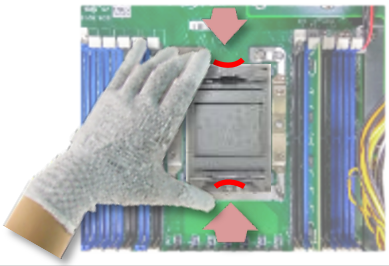
Tools Required

Tool	Description	
(T-30 Torx Bit©)	Set to 8in/lb for tightening the nuts which fasten the PHM on the bolster plate.	
ESD Protection (ESD gloves, ESD-safe work surface, ESD-safe shoes, grounded wrist strap etc.)	During the entire assembly process, at least wear a pair of ESD gloves to avoid damaging or contaminating the electronic parts while enhancing your own safety.	

Note: The images of tools shown in this document are merely for reference; the actual tools you use might differ.

Parts Explanation:

Item	Description	
Processor	Please avoid touching the gold fingers or package lands of the processor even if you are wearing ESD gloves.	 

Heat Sink	If a TIM (Thermal Interface Material) protective film is already attached to the base of the heat sink, remove it before you mount the processor on it. When holding the heatsink, please grip it along the axis of its fins with your thumb and your index finger.	
Processor Carrier	This is packed along with the processor. Before performing any assembly involving this part, please locate PIN1 on one of the corners, an important indicator used to align this carrier with the processor and the bolster plate correctly.	
Socket Cover	This cover is used to protect the package land surface of the processor from contamination. To remove it from the processor, grasp the holding features with your thumb and your index finger while pulling the cover off vertically.	
Bolster Plate	A robust bolster plate is used to assist in PHM alignment for installation, while effectively helping eliminate PCB bowing during compression. Please locate the Cutout on one of the four corners before starting PHM installation.	

CPU compatible list

This system support 3rd Gen Intel® Xeon® Processor Scalable Family (Ice Lake-SP). Below is official list of compatible CPU by Intel®

Product Name	Launch Date	Total Cores	Max Turbo Frequency	Processor Base Frequency	Cache	TDP
Intel® Xeon® Gold 5315Y Processor	Q2'21	8	3.60 GHz	3.20 GHz	12 MB	140 W
Intel® Xeon® Gold 5317 Processor	Q2'21	12	3.60 GHz	3.00 GHz	18 MB	150 W
Intel® Xeon® Gold 5318N Processor	Q2'21	24	3.40 GHz	2.10 GHz	36 MB	150 W
Intel® Xeon® Gold 5318S Processor	Q2'21	24	3.40 GHz	2.10 GHz	36 MB	165 W
Intel® Xeon® Gold 5318Y Processor	Q2'21	24	3.40 GHz	2.10 GHz	36 MB	165 W
Intel® Xeon® Gold 5320 Processor	Q2'21	26	3.40 GHz	2.20 GHz	39 MB	185 W
Intel® Xeon® Gold 5320T Processor	Q2'21	20	3.50 GHz	2.30 GHz	30 MB	150 W
Intel® Xeon® Gold 6312U Processor	Q2'21	24	3.60 GHz	2.40 GHz	36 MB	185 W
Intel® Xeon® Gold 6314U Processor	Q2'21	32	3.40 GHz	2.30 GHz	48 MB	205 W
Intel® Xeon® Gold 6326 Processor	Q2'21	16	3.50 GHz	2.90 GHz	24 MB	185 W
Intel® Xeon® Gold 6330 Processor	Q2'21	28	3.10 GHz	2.00 GHz	42 MB	205 W

Product Name	Launch Date	Total Cores	Max Turbo Frequency	Processor Base Frequency	Cache	TDP
Intel® Xeon® Gold 6330N Processor	Q2'21	28	3.40 GHz	2.20 GHz	42 MB	165 W
Intel® Xeon® Gold 6334 Processor	Q2'21	8	3.70 GHz	3.60 GHz	18 MB	165 W
Intel® Xeon® Gold 6336Y Processor	Q2'21	24	3.60 GHz	2.40 GHz	36 MB	185 W
Intel® Xeon® Gold 6338 Processor	Q2'21	32	3.20 GHz	2.00 GHz	48 MB	205 W
Intel® Xeon® Gold 6338N Processor	Q2'21	32	3.50 GHz	2.20 GHz	48 MB	185 W
Intel® Xeon® Gold 6338T Processor	Q2'21	24	3.40 GHz	2.10 GHz	36 MB	165 W
Intel® Xeon® Gold 6342 Processor	Q2'21	24	3.50 GHz	2.80 GHz	36 MB	230 W
Intel® Xeon® Gold 6346 Processor	Q2'21	16	3.60 GHz	3.10 GHz	36 MB	205 W
Intel® Xeon® Gold 6348 Processor	Q2'21	28	3.50 GHz	2.60 GHz	42 MB	235 W
Intel® Xeon® Gold 6354 Processor	Q2'21	18	3.60 GHz	3.00 GHz	39 MB	205 W
Intel® Xeon® Platinum 8351N Processor	Q2'21	36	3.50 GHz	2.40 GHz	54 MB	225 W
Intel® Xeon® Platinum 8352M	Q2'21	32	3.50 GHz	2.30 GHz	48 MB	185 W

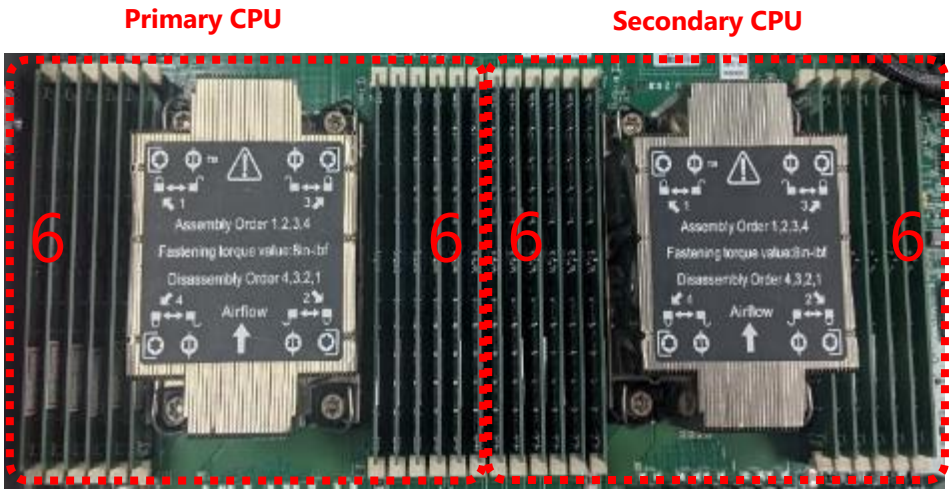
Product Name	Launch Date	Total Cores	Max Turbo Frequency	Processor Base Frequency	Cache	TDP
Processor						
Intel® Xeon® Platinum 8352S Processor	Q2'21	32	3.40 GHz	2.20 GHz	48 MB	205 W
Intel® Xeon® Platinum 8352V Processor	Q2'21	36	3.50 GHz	2.10 GHz	54 MB	195 W
Intel® Xeon® Platinum 8352Y Processor	Q2'21	32	3.40 GHz	2.20 GHz	48 MB	205 W
Intel® Xeon® Platinum 8358 Processor	Q2'21	32	3.40 GHz	2.60 GHz	48 MB	250 W
Intel® Xeon® Platinum 8358P Processor	Q2'21	32	3.40 GHz	2.60 GHz	48 MB	240 W
Intel® Xeon® Platinum 8360Y Processor	Q2'21	36	3.50 GHz	2.40 GHz	54 MB	250 W
Intel® Xeon® Platinum 8362 Processor	Q2'21	32	3.60 GHz	2.80 GHz	48 MB	265 W
Intel® Xeon® Platinum 8368 Processor	Q2'21	38	3.40 GHz	2.40 GHz	57 MB	270 W
Intel® Xeon® Platinum 8368Q Processor	Q2'21	38	3.70 GHz	2.60 GHz	57 MB	270 W
Intel® Xeon® Platinum 8380 Processor	Q2'21	40	3.40 GHz	2.30 GHz	60 MB	270 W

Product Name	Launch Date	Total Cores	Max Turbo Frequency	Processor Base Frequency	Cache	TDP
Intel® Xeon® Silver 4309Y Processor	Q2'21	8	3.60 GHz	2.80 GHz	12 MB	105 W
Intel® Xeon® Silver 4310 Processor	Q2'21	12	3.30 GHz	2.10 GHz	18 MB	120 W
Intel® Xeon® Silver 4310T Processor	Q2'21	10	3.40 GHz	2.30 GHz	15 MB	105 W
Intel® Xeon® Silver 4314 Processor	Q2'21	16	3.40 GHz	2.40 GHz	24 MB	135 W
Intel® Xeon® Silver 4316 Processor	Q2'21	20	3.40 GHz	2.30 GHz	30 MB	150 W
Intel® Xeon® Gold 6330H Processor	Q3'20	24	3.70 GHz	2.00 GHz	33 MB	150 W
Intel® Xeon® Platinum 8356H Processor	Q3'20	8	4.40 GHz	3.90 GHz	35.75 MB	190 W
Intel® Xeon® Platinum 8360H Processor	Q3'20	24	4.20 GHz	3.00 GHz	33 MB	225 W
Intel® Xeon® Platinum 8360HL Processor	Q3'20	24	4.20 GHz	3.00 GHz	33 MB	225 W
Intel® Xeon® Gold 5318H Processor	Q2'20	18	3.80 GHz	2.50 GHz	24.75 MB	150 W
Intel® Xeon® Gold 5320H Processor	Q2'20	20	4.20 GHz	2.40 GHz	27.5 MB	150 W

Product Name	Launch Date	Total Cores	Max Turbo Frequency	Processor Base Frequency	Cache	TDP
Intel® Xeon® Gold 6328H Processor	Q2'20	16	4.30 GHz	2.80 GHz	22 MB	165 W
Intel® Xeon® Gold 6328HL Processor	Q2'20	16	4.30 GHz	2.80 GHz	22 MB	165 W
Intel® Xeon® Gold 6348H Processor	Q2'20	24	4.20 GHz	2.30 GHz	33 MB	165 W
Intel® Xeon® Platinum 8353H Processor	Q2'20	18	3.80 GHz	2.50 GHz	24.75 MB	150 W
Intel® Xeon® Platinum 8354H Processor	Q2'20	18	4.30 GHz	3.10 GHz	24.75 MB	205 W
Intel® Xeon® Platinum 8376H Processor	Q2'20	28	4.30 GHz	2.60 GHz	38.5 MB	205 W
Intel® Xeon® Platinum 8376HL Processor	Q2'20	28	4.30 GHz	2.60 GHz	38.5 MB	205 W
Intel® Xeon® Platinum 8380H Processor	Q2'20	28	4.30 GHz	2.90 GHz	38.5 MB	250 W
Intel® Xeon® Platinum 8380HL Processor	Q2'20	28	4.30 GHz	2.90 GHz	38.5 MB	250 W

System Memory

The motherboard supports DDR4 with bus 2133/2400/2666/2933 MHz R-DIMM / LRDIMM support advanced ECC;Scrubbing; SDDC; ADDDC. Please follow the steps below to install the DIMM memory modules. The primary CPU and the secondary CPU both have 12 DIMM sockets (6 on each side)

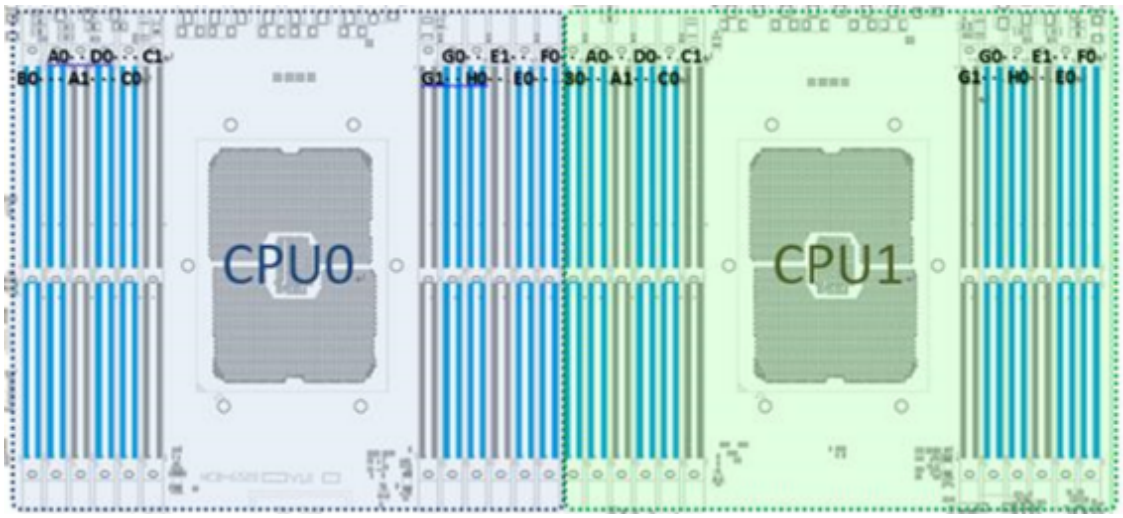


- Supported Capacities: 8/16/32/64 GB
- Maximum RAM: **1536GB** (64GB per slot)

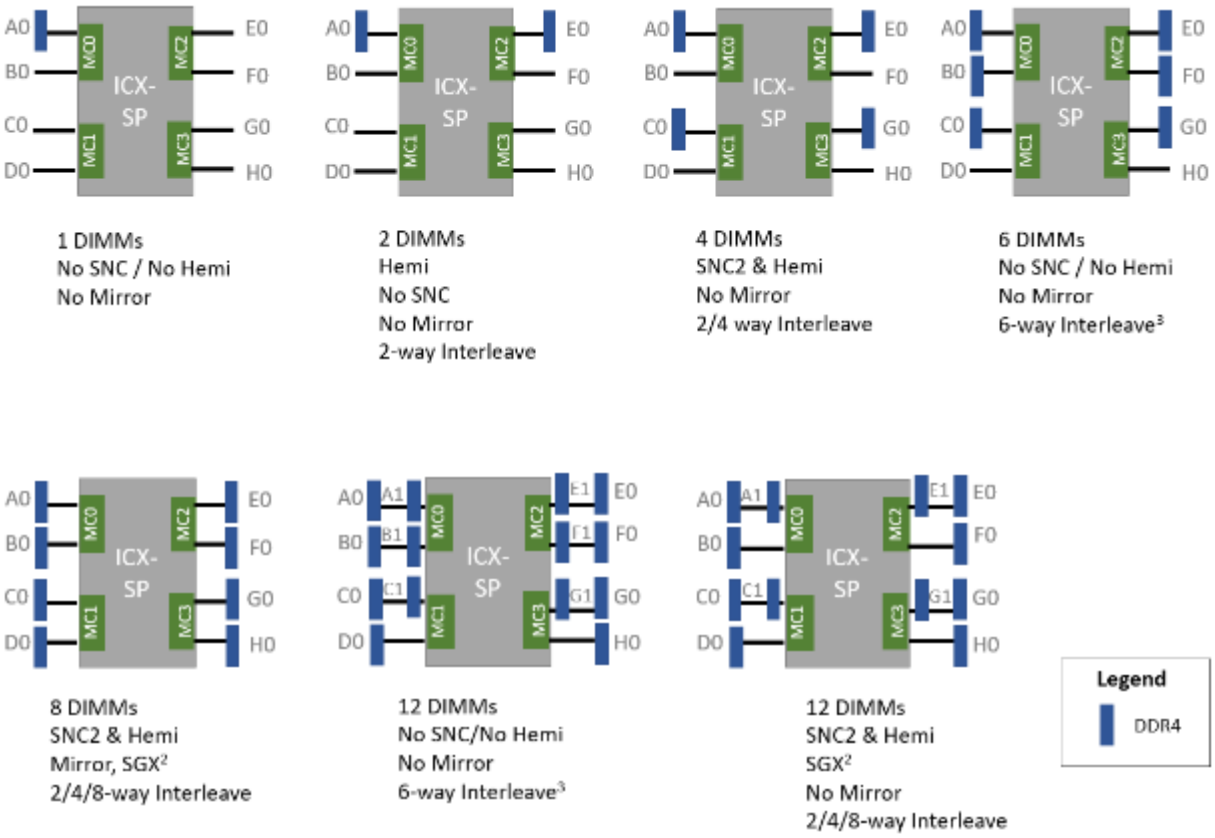
DIMM Population Guidelines:

Please do follow the memory module installation instructions to install the DIMM, and make sure the DIMM population guidelines are met:

- Each CPU requires at least 1 memory module to boot and run from.
- If you do not plan to fill up all the sockets with 24 memory modules, always start with the blue ones for optimal performance.
- Try to split the DIMMs evenly across the CPUs.
- Please use memory modules of the same capacity, speed and from the same manufacturer to avoid compatibility issues.



f



DIMM Population Notes:

- 1 DIMM: validated on any slot
- 2 DIMM: validated AE, CG, AC, EG, & AD[4]
- >2 DIMMs: Channel population can be different than shown as long as symmetric left/Right across the socket.
- >2 DIMMs: Configs with channel 0 populated before channel 1 on each MC are validated configs[4]
- A/E/C/G channels must be populated with same total capacity per channel if populate
- B/F/D/H channels must be populated with same total capacity if populated[1]
- SNC2 configuration requires full asymmetry together with LEFT/RIGHT symmetry

[1] – If capacity requirement not followed, all memory may not be mapped

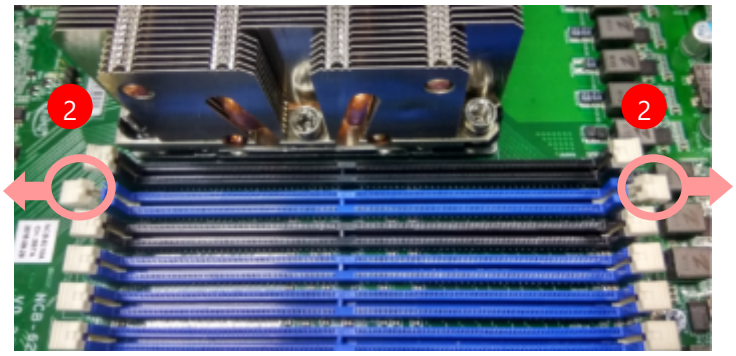
[2] – Rank sparing, ADDDC, channel mirroring, Hemi, and 2LM not supported with SGX

[3] – 6 way Interleave requires same channel capacity on all 6 channels

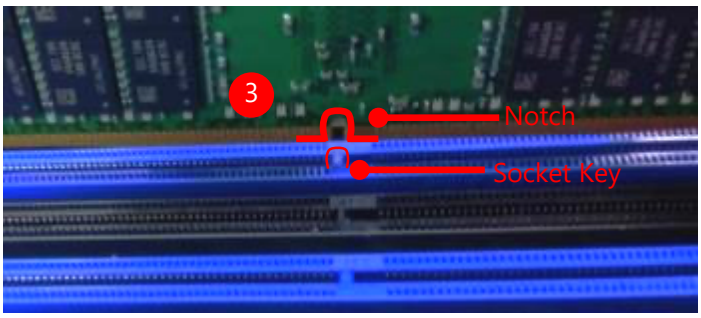
[4] – AD & ADEH additionally validated to allow for 2 different DIMM sizes in 2&4 DIMM configs

Memory Module installation

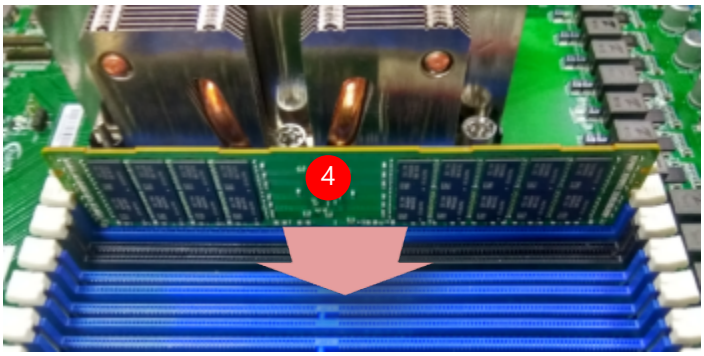
1. Power off the system.
2. Pull open the DIMM slot latches.



3. Align the notch of the DIMM module with the socket key in the slot.



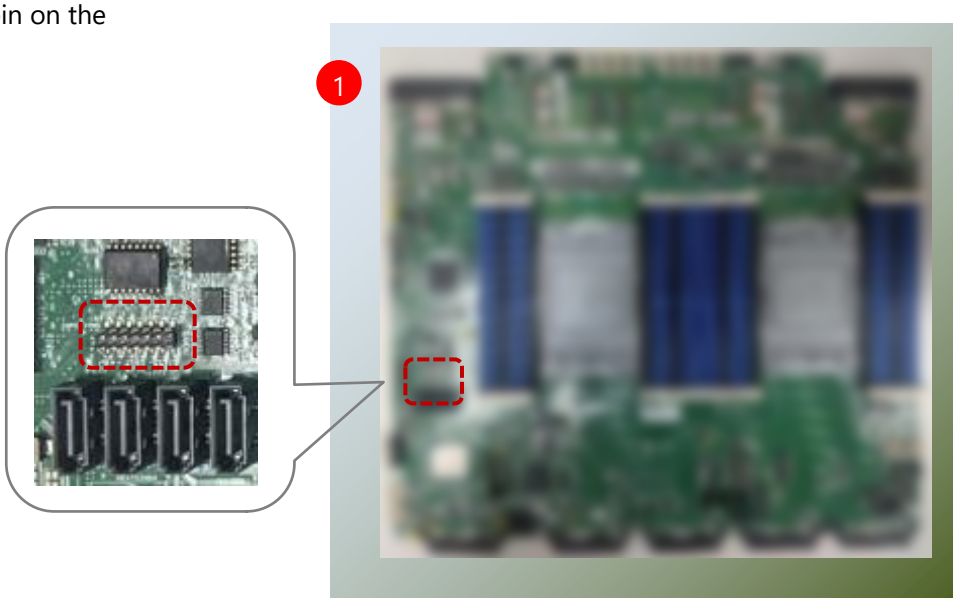
4. Insert the module into the slot until it is firmly seated. The motherboard of HAN-9820C is designed with 20 DDR DIMM sockets.



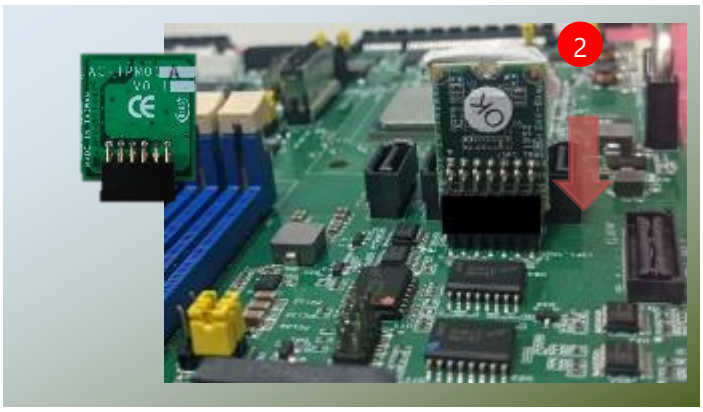
TPM Module (Optional)

The motherboard provides one TPM slot. Follow the procedures below for installing a TPM module.

1. Locate the TPM pin on the motherboard.



2. Insert the module into the TPM pins until it is fully seated.

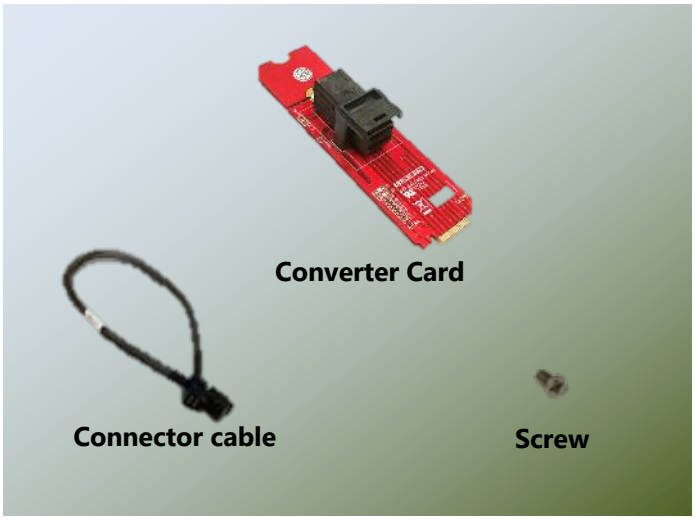


Riser Converter Card (Optional)

The motherboard provides two M.2 slots. Follow the procedures below for installing a M.2 riser converter card.

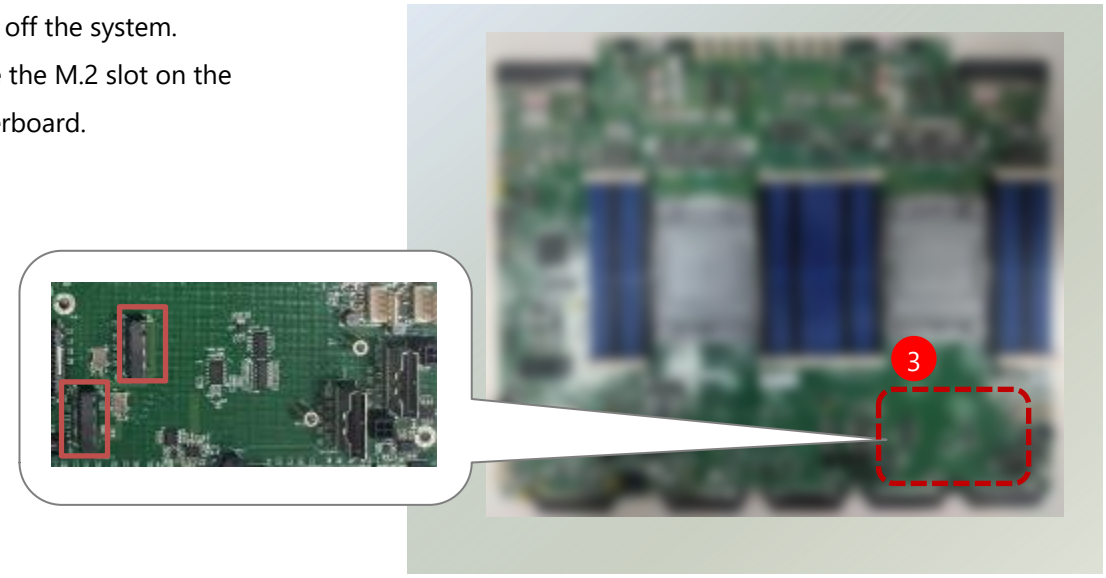
1. The Riser card kit includes:

- 1x Converter Card
- 1x Connector cable
- 1x screw

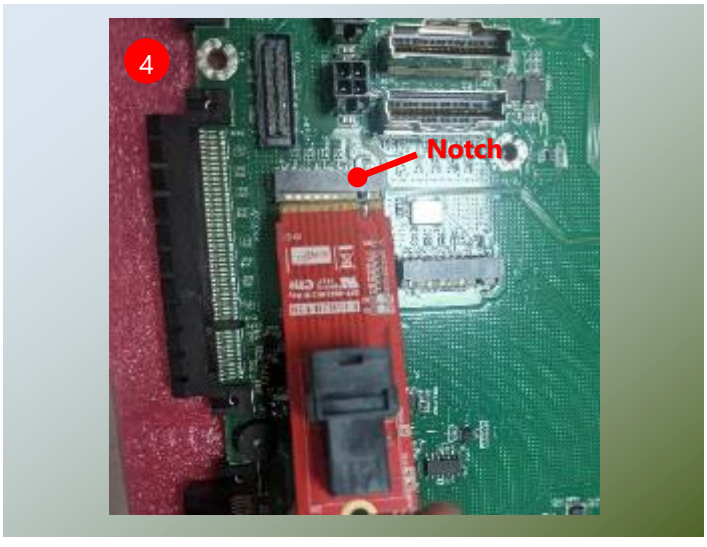


2. Power off the system.

3. Locate the M.2 slot on the motherboard.

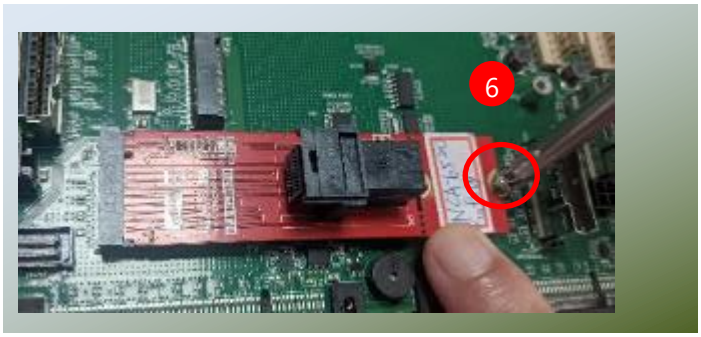


4. Align the notch of the U.2 converter card with the socket key in the pin slot.

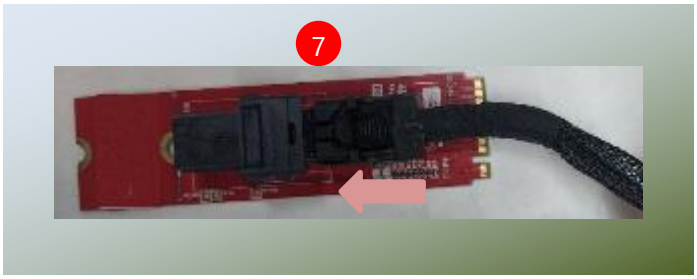


5. Insert the U.2 converter card pins at 30 degrees into the socket until it is fully seated.

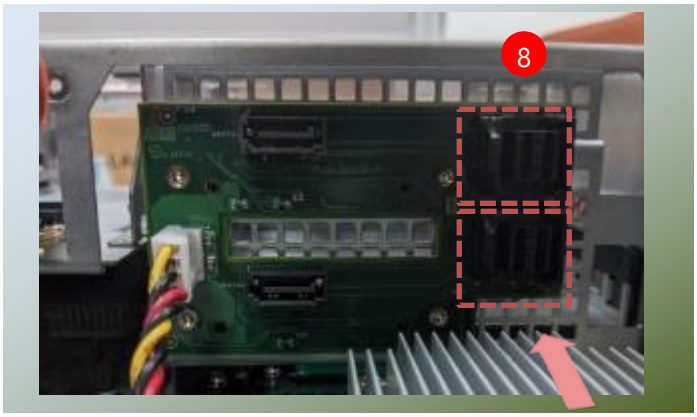
6. Push down on the module and secure it with a screw.

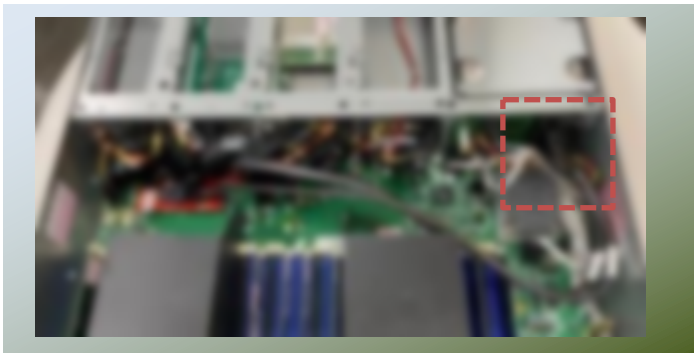


7. Insert one end of the connector cable to the converter card.



8. Connect the other end of the cable to the HDD/SSD backplane. Follow the procedures below for installing the SSD drive.



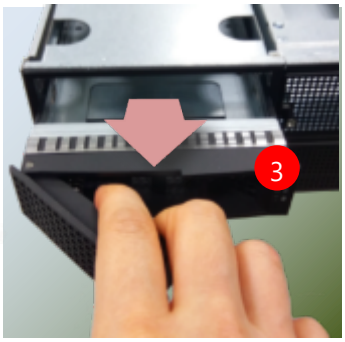


Disk Drive(s) (Optional)

HAN-9820C is built with two 3.5" HDD/SSD drive bay and NCS2 Module for 8x Standard NIC/Storage/ Module Slots (each Storage module support 2x2.5 inch SATA SDD/HDD). The following will discuss disk drive installation procedures based on their HDD/SSD designs. The total system storage based on capacity of HDD/SSD installed and can be up to 61.4 TB

1. Power off the system.
2. Locate the 3.5" disk bay on the front panel.

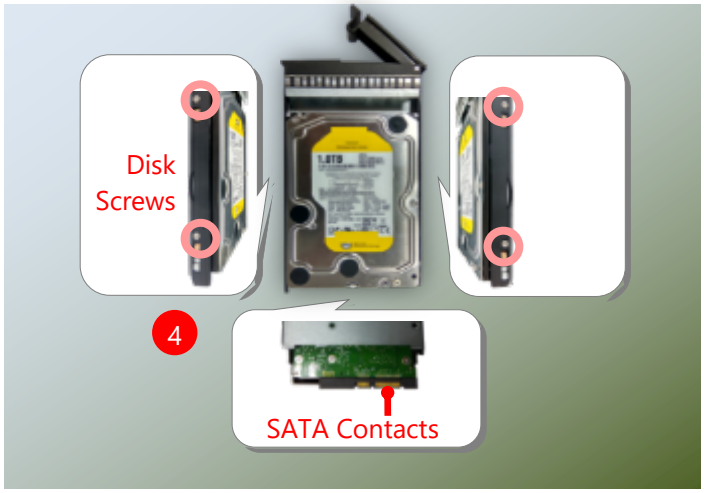
3. To remove the tray, put your finger on the tab and push it to the left to slide it open, hold the tab lever and pull out the tray.



4. The tray is designed to accommodate one 3.5" hard disk or one 2.5" hard disk.

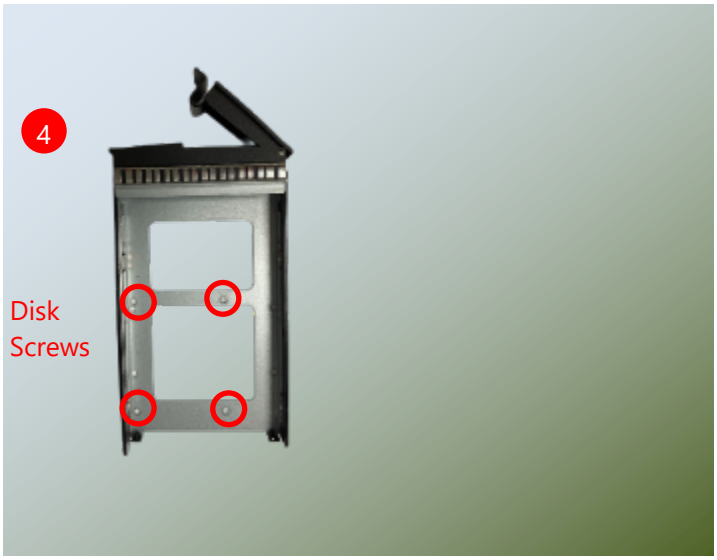
   Mounting a 3.5" hard disk

   Secure the hard disk on the tray with the provided disk screws. Make sure the disk SATA connector faces towards the SATA contacts inside the system.

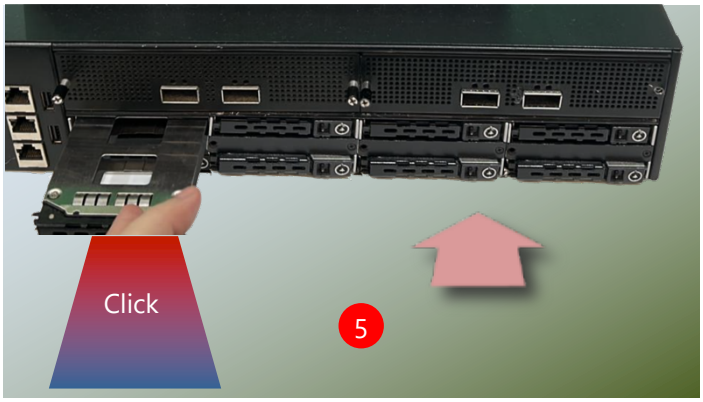


Mounting a 2.5" hard disk

Secure the hard disk on the tray with the provided disk screws. Make sure the disk SATA connector faces towards the SATA connector inside the system.



5. To install the mounted disk tray, push the tray into position in the chassis. Press the hinge tab until it clicks into place.



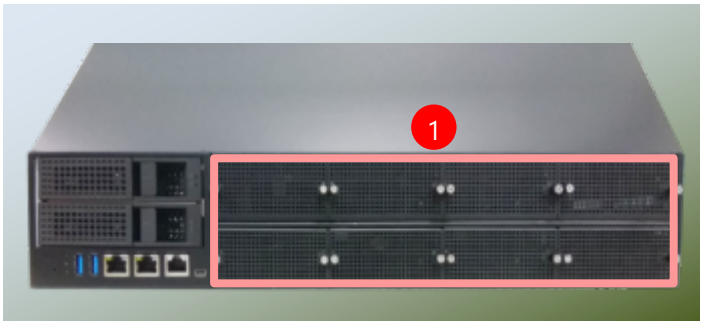
Supported Disk Drive

Form Factor	Type	Communication Speed	Disk Rotation speed	Disk Capacities
2.5 inch	SATA III	6Gb/s	SSD	240 GB, 256 GB, 480 GB, 960 GB, 1.92 TB, 3.84 TB, 7.68 TB
2.5 inch	SATA III	6Gb/s	5.4K	500 GB, 1 TB, 2 TB
3.5 inch	SATA III	6Gb/s	5.4K, 7.2K	2 TB, 4 TB, 8 TB, 12 TB, 16 TB, 20 TB
M.2	SATA III	6Gb/s	SSD	240 GB, 480 GB

NIC Modules (Optional)

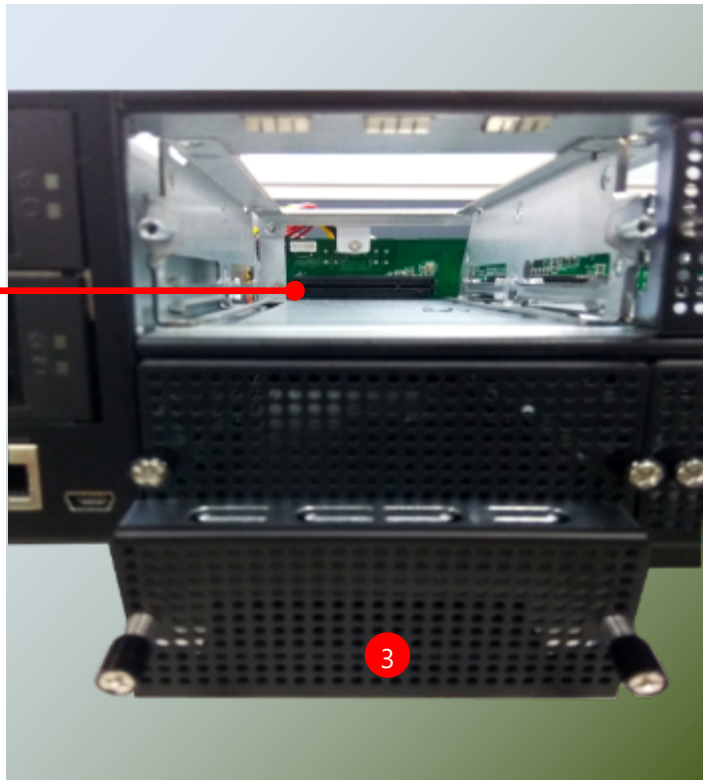
HAN-9820C comes with NCS2 Module for 8x Standard NIC/Storage/ Module Slots (each Storage module support 2x2.5 inch SATA SDD/HDD). The total network port can be up to 16 port Gbps. Please follow the steps for network bandwidth expansion.

1. On the front panel, select a NIC Ethernet module slot.

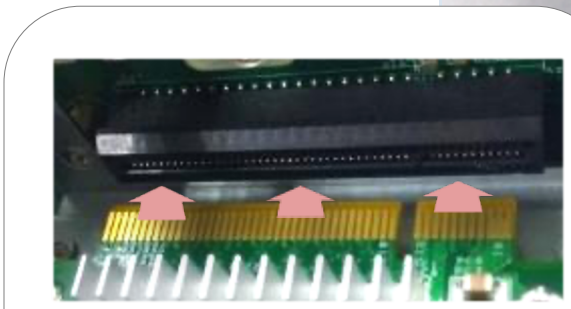


2. Rotate clockwise and loosen the two lock-screws.

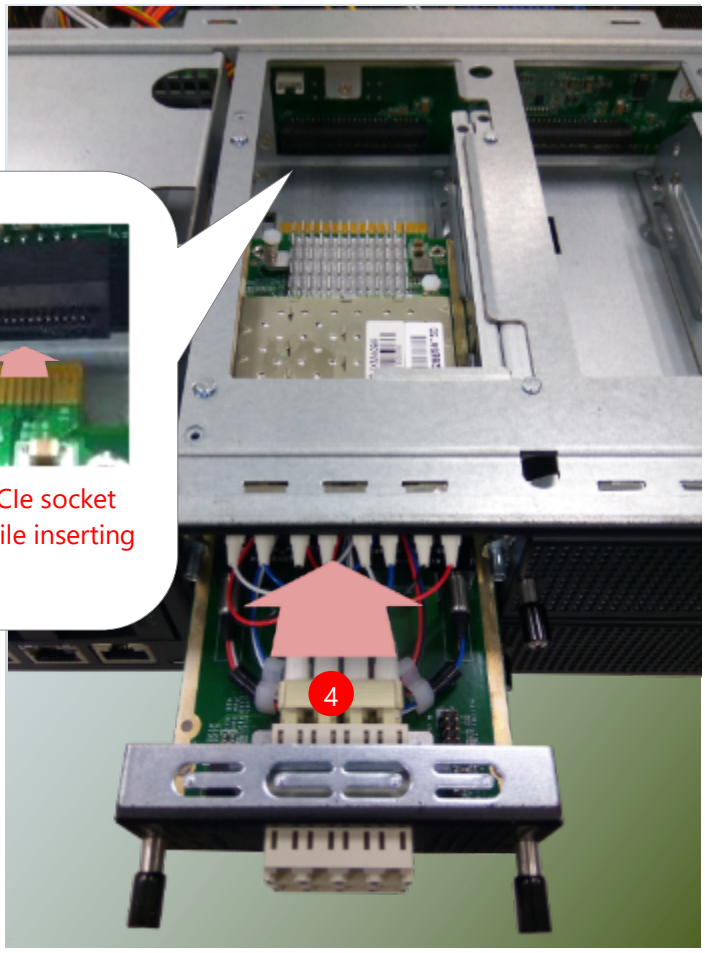
3. Remove the door and locate the PCIe socket for module insertion.



4. Insert your NIC Ethernet module. (The module shown in the image below is for reference only).



Align the golden fingers to the PCIe socket on the motherboard carefully while inserting this module.



5. Once the module is firmly seated, rotate counter-clockwise and tighten the two lock-screws.

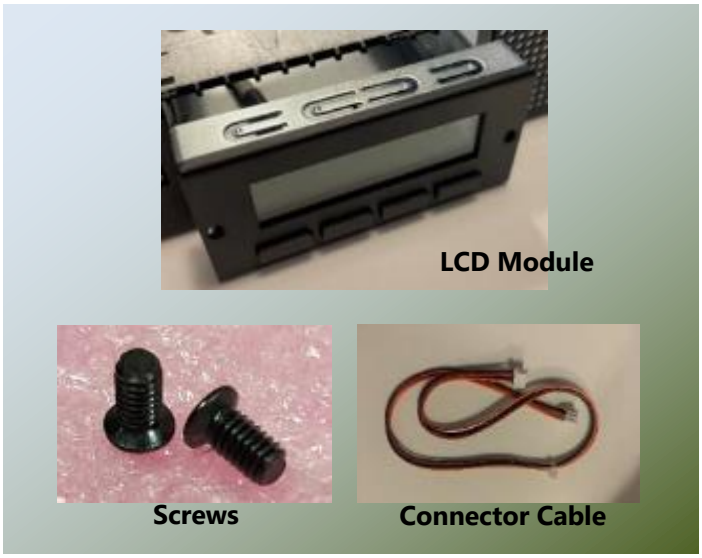
LCD Module (Optional)

HAN-9820C comes with LCD module expansion, which can install into NCS2 Module. It is a window into the health and integrity of computing systems. These modules offer users the critical ability to monitor firmware and system status, providing real-time feedback and error detection. You can programmable it to adapt with requirement purpose.

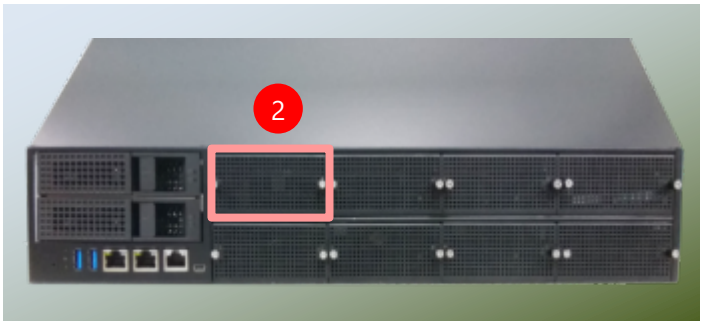
Please follow the steps for installation.

1. The LCD module package will include:

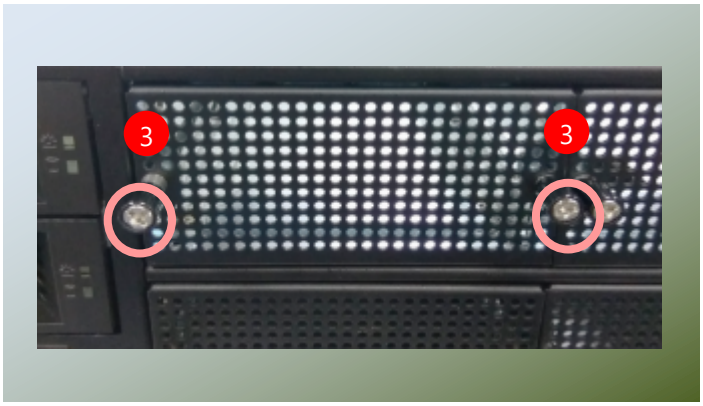
- 1x LCD Panel with 4 control key (programmable)
- 1x LCD connector cable
- 2x screws



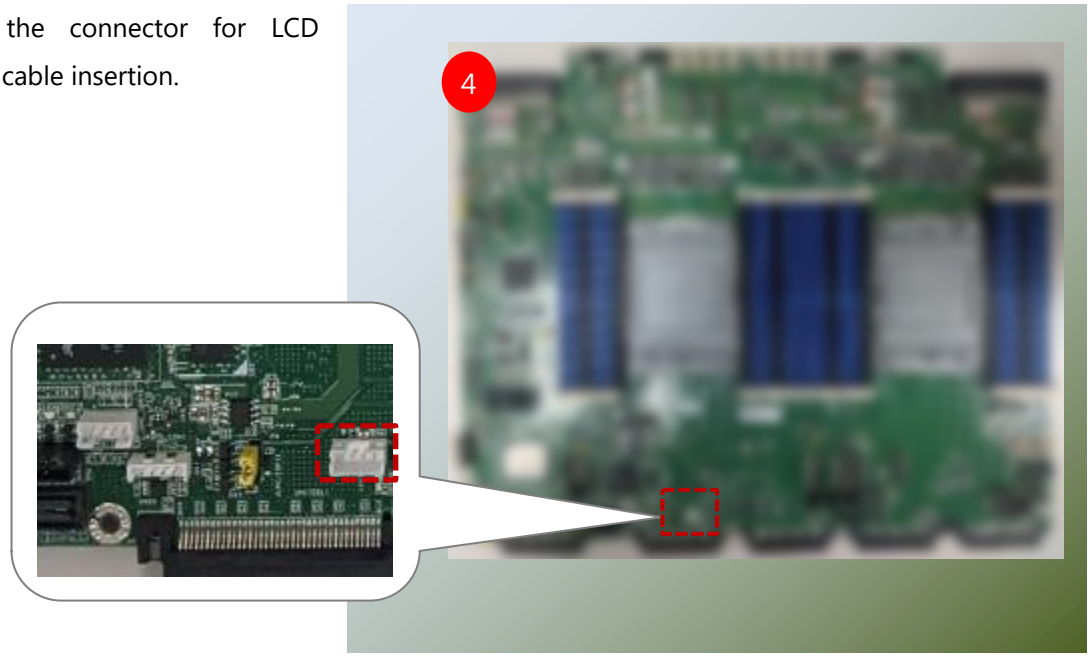
2. On the front panel of HAN-9820C, select the upper first module slot for LCD Module placement.



3. Loosen the two lock-screws and remove the door.

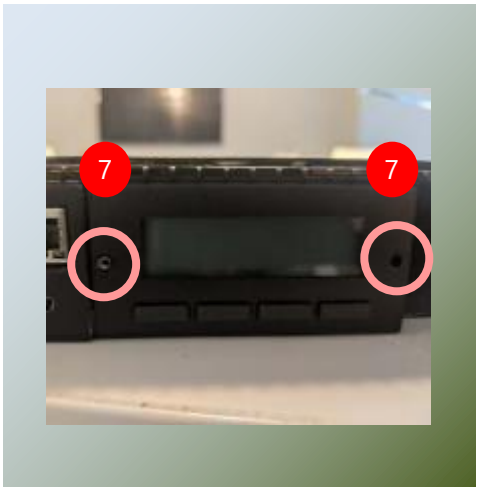


4. Locate the connector for LCD module cable insertion.



5. Install the LCD module into the module slot.

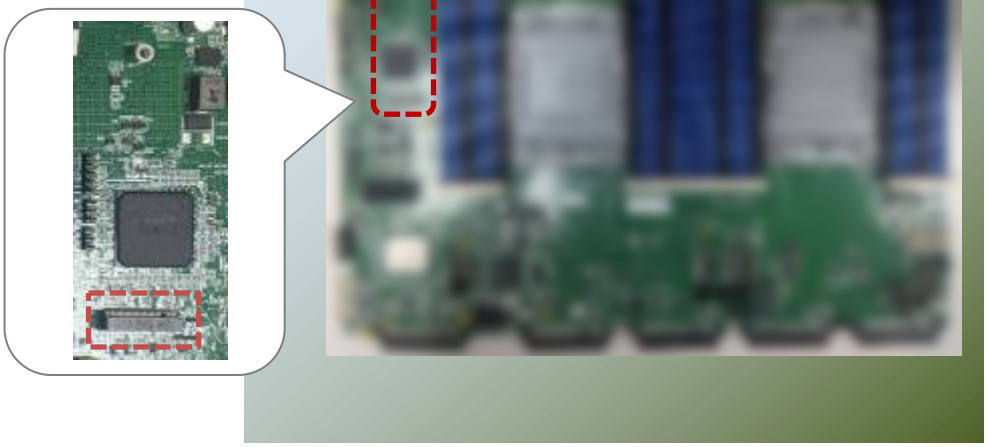
6. Insert the connector cable into the connector.
7. Rotate and screw in the two lock screws. The LCD module has been successfully installed.



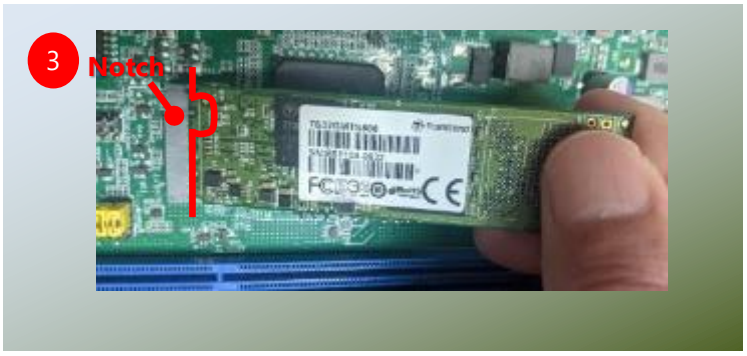
M.2 SSD memory card (Optional)

HAN-9820C comes with an additional M.2 SSD memory card slot. Please follow the steps for installation.

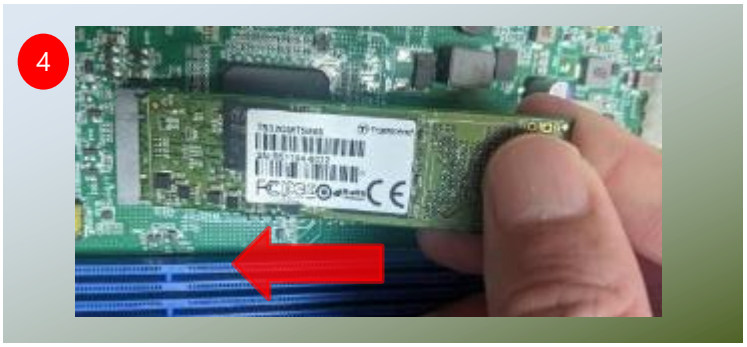
1. Power off the system.
2. Locate the M.2 slot on the motherboard.



3. Align the notch of the M.2 memory card with the socket key in the pin slot.



4. Insert the M.2 memory card pins at 30 degrees into the socket until it is fully seated.



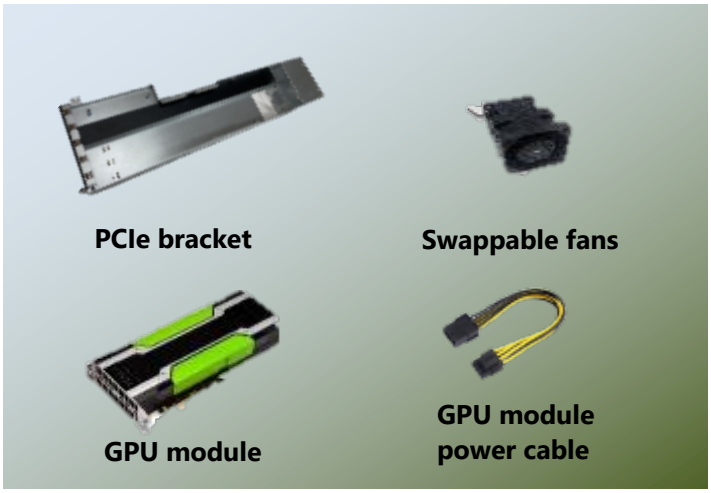
5. Push down on the module and secure it with a screw.

GPU graphic card (Optional)

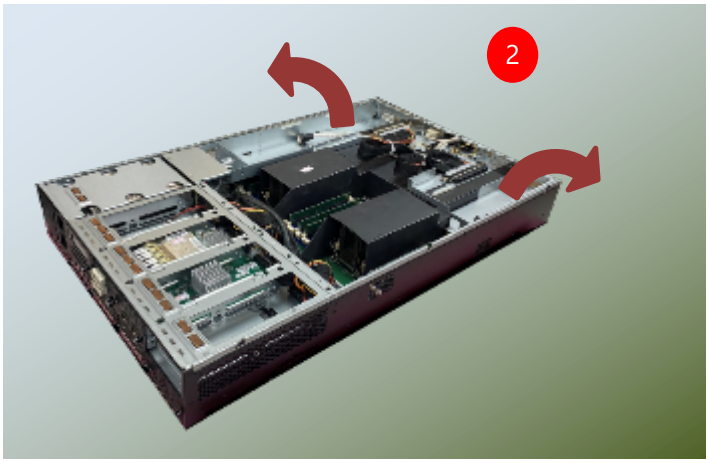
HAN-9820C comes with optional slots for GPU graphic card expansion. The GPU graphic card requires a rather complex installation process; therefore, the assembly must be handled with care. Please read through the instructions in this section to make sure you have acquired the necessary knowledge and comply with the requirements.

1. The GPU expansion kit will include:

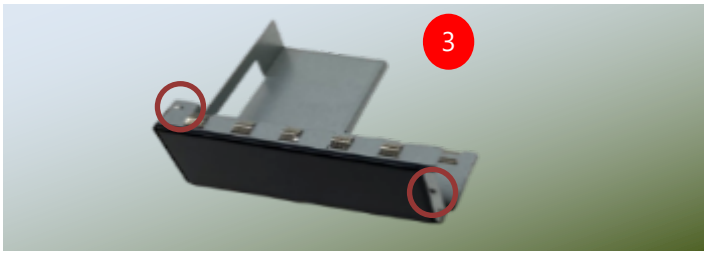
- 1x PCIe bracket (right-side or left-side)
- 1x or 2x Swappable fan(s)
- 1x GPU module
- 1x GPU power cable
- Xx screws



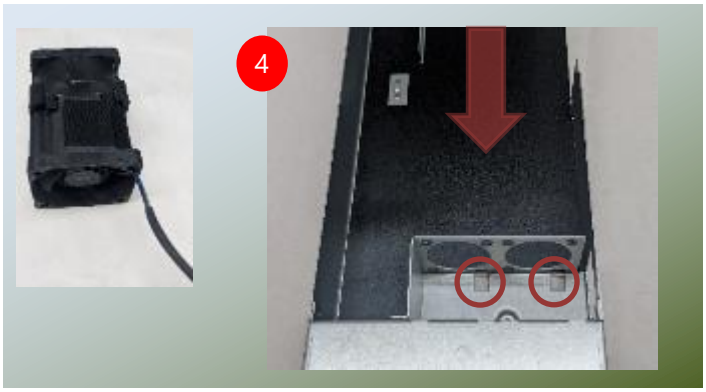
2. Power off the system and open the top cover. Unscrew and remove the black cover/hood (pls refer to p.28). Remove the Remove the original PCIe bracket (right-side or left-side).



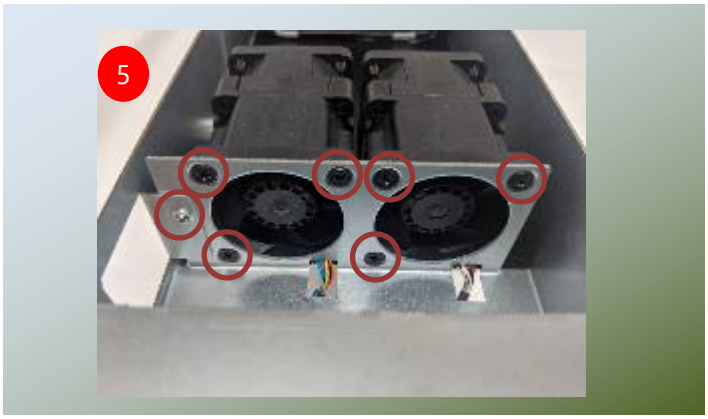
3. Unscrew two (2) screws to remove the original PCIe bracket.



4. Pick up the new PCIe bracket, and assemble the fan(s) first. Slide the fan towards the end of the bracket, and slip the fan power cable through the holes indicated.



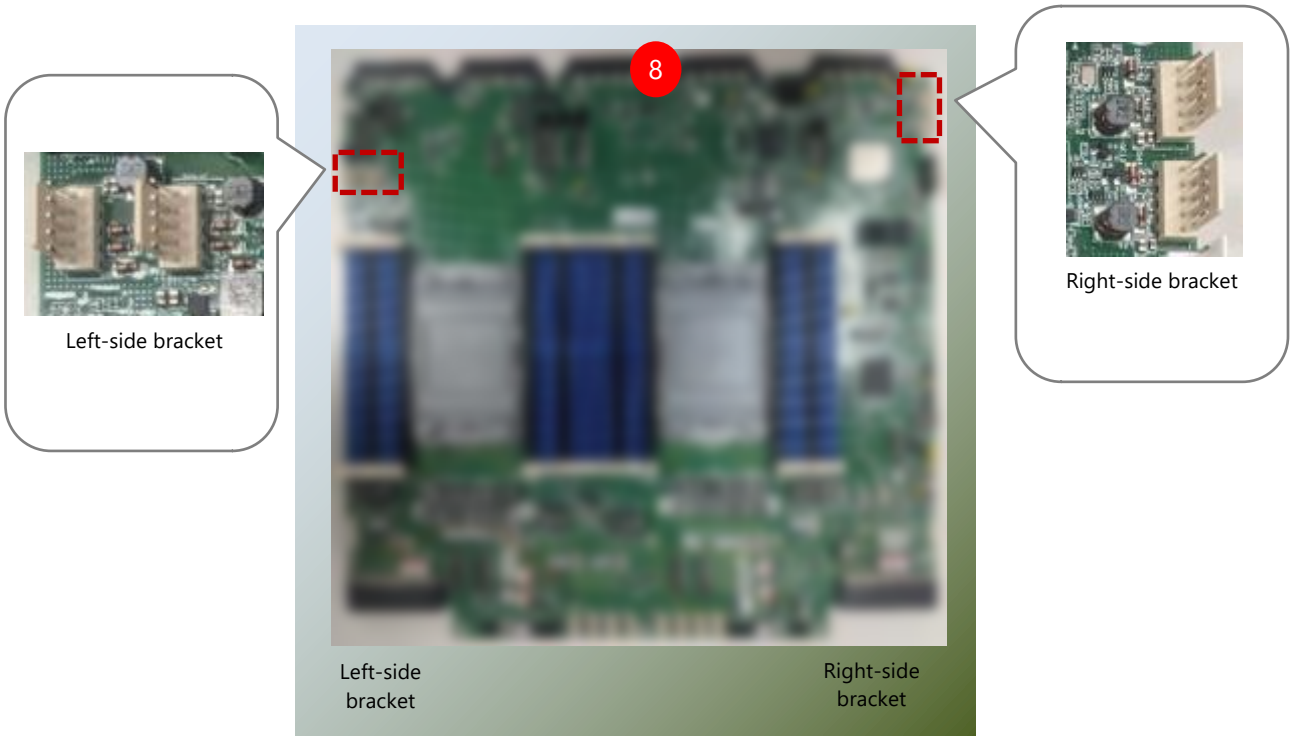
5. Secure the fan module with three (3) screws on each fan and one (1) screw on the side. Repeat the same assemble process with the second fan.



6. Turn the bracket to the other end, align the GPU card module to the PCIe bracket. Slide the GPU module into the PCIe bracket until it is completely seated and clicks.

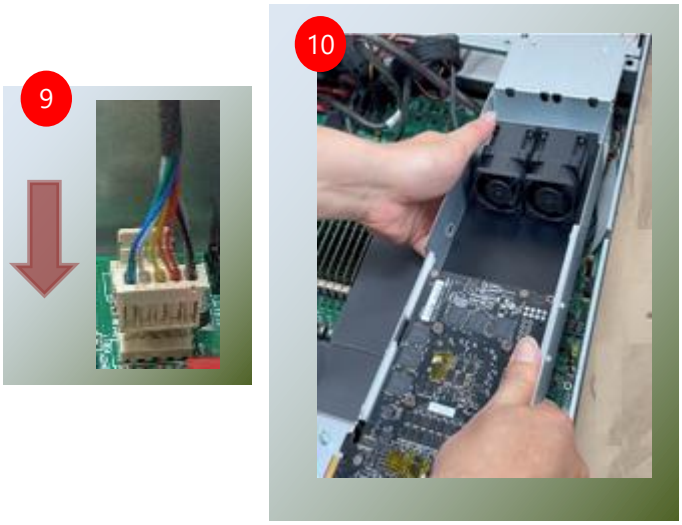
7. Place the side panel in place, and screw in four (4) screws.

8. Locate the fan cable connector.

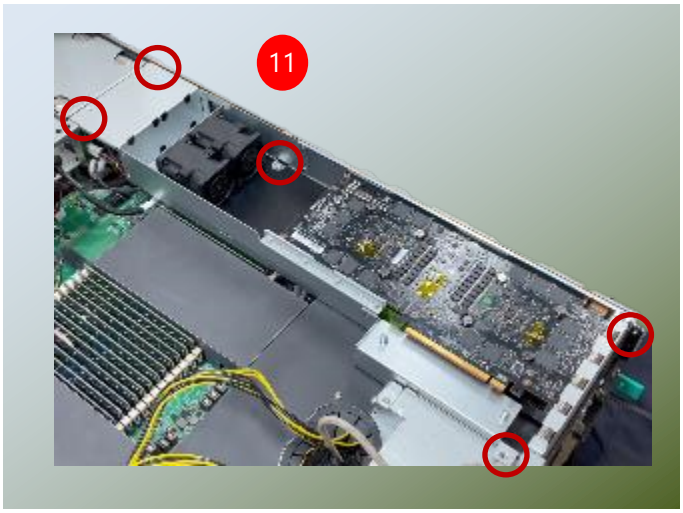


9. Insert the fan power cables into the connector.

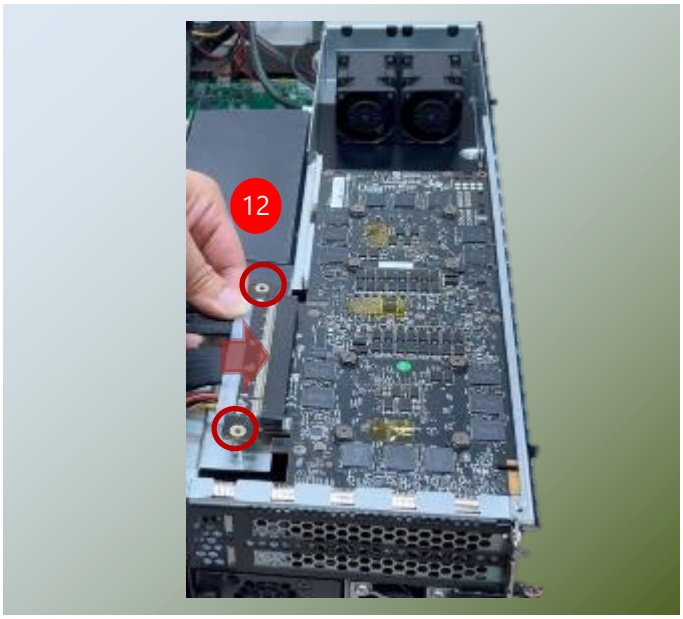
10. Then, mount the PCIe bracket with the installed GPU card module in the slot.



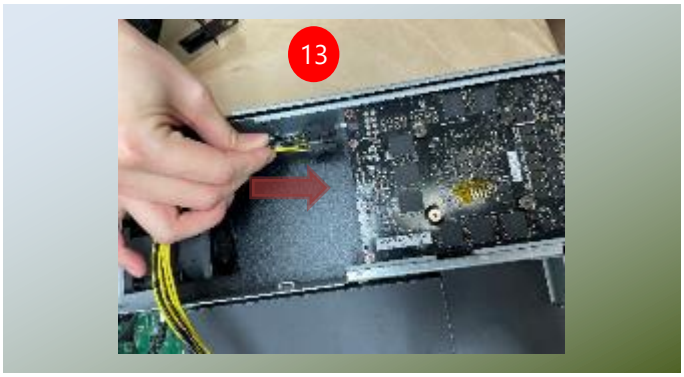
11. Secure the PCIe bracket to the system with five (5) screws.



12. Connect the PCIe cable to the golden fingers until it is fully seated and secure with two (2) screws.



13. Insert the GPU power cable to the side of the GPU module. Other end of power cable should have been pre-installed on the motherboard. The GPU module installation has been completed.



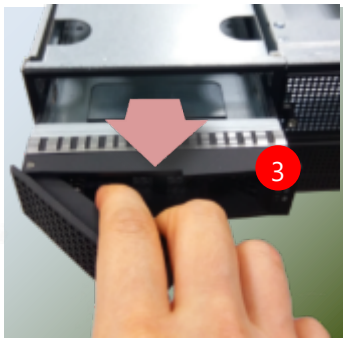
Dual SD card (Optional)

HAN-9820C is built with two 3.5" HDD/SSD drive bay which can be used for a dual SD card with capacity support 16/32/64GB. Dual SD Card Redundancy is a feature that adds a significant layer of reliability to Lanner's products, especially those deployed in industrial and mission-critical environments.

1. Power off the system.

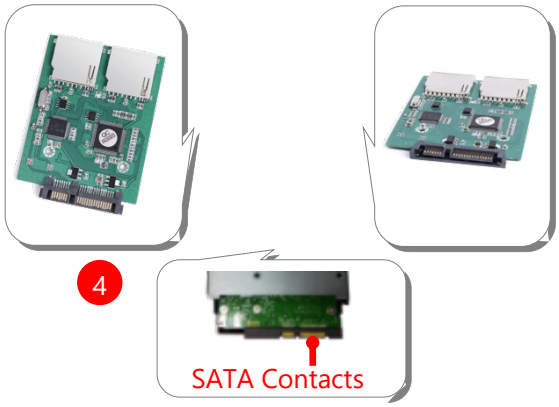
2. Locate the 3.5" disk bay on the front panel.

3. To remove the tray, put your finger on the tab and push it to the left to slide it open, hold the tab lever and pull out the tray.



4. The tray is designed to accommodate one dual SD card.

Secure board on the tray with the provided disk screws. Make sure the disk SATA connector faces towards the SATA contacts inside the system.

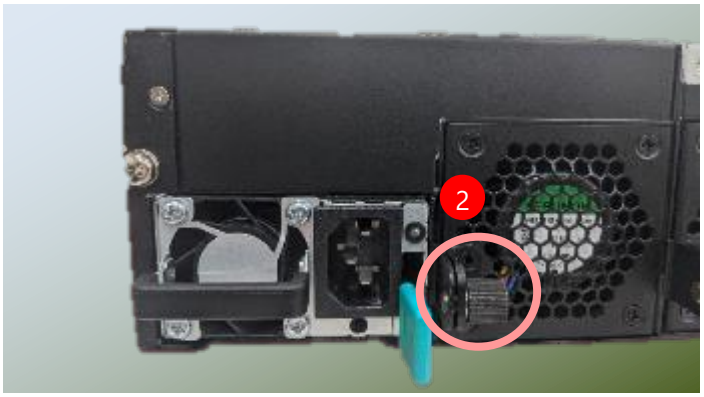


Cooling Fans

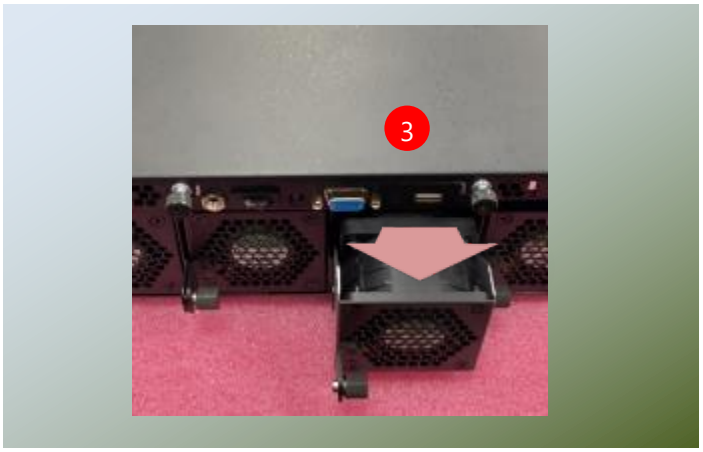
Cooling fans may wear down eventually. Please refer to the steps below for replacing cooling fans. When using a new cooling fan, simply reverse the steps to install the fan back onto the enclosure and the system.

1. Make sure to have 1x screwdriver, and 1x 5mm socket screwdriver (Hex nut screwdriver). Locate the cooling fans at the rear panel.

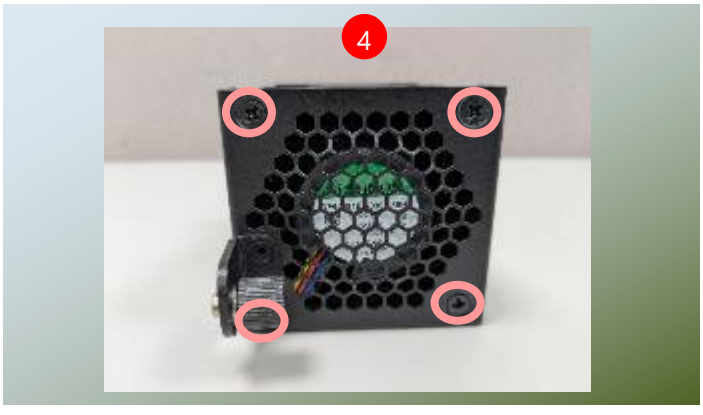
2. Loosen the (one) lock-screw of the fan you would like to replace.



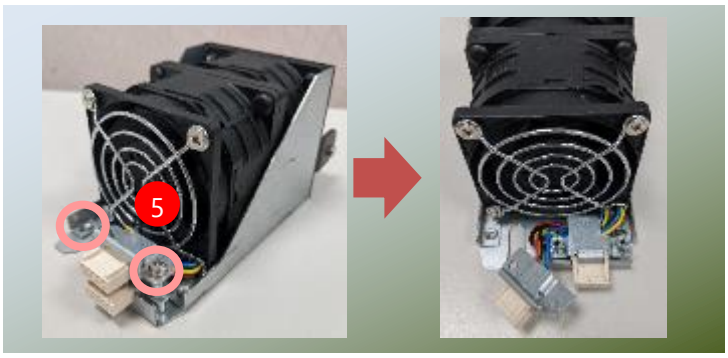
3. Hold onto the lock-screw and pull out the single fan.



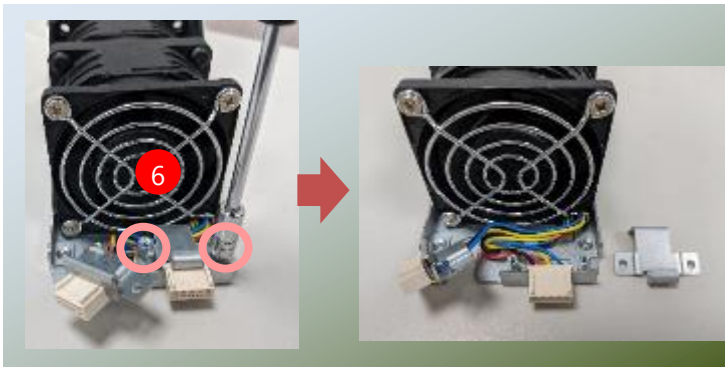
4. Remove the 4 screws that secure the fan.



5. Remove the two (2) screws securing top fan connector.



6. Use the 5mm socket screwdriver to remove the two (2) hex column screw nuts securing the bottom fan connector.



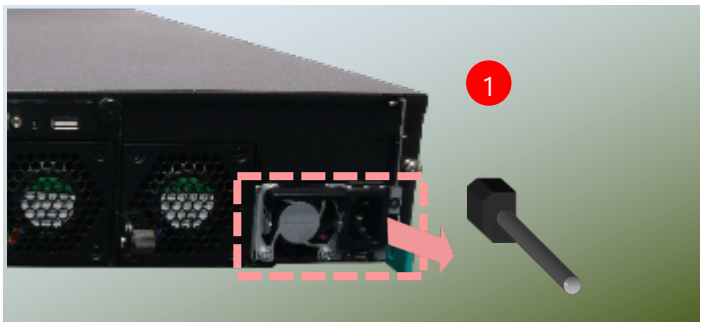
7. Take the fan and fan connectors out of the enclosure. The fan connectors will be connected to the motherboard, to remove, disconnect from the motherboard.

8. When using a new cooling fan, simply reverse the steps to install the fan back onto the enclosure and the system.

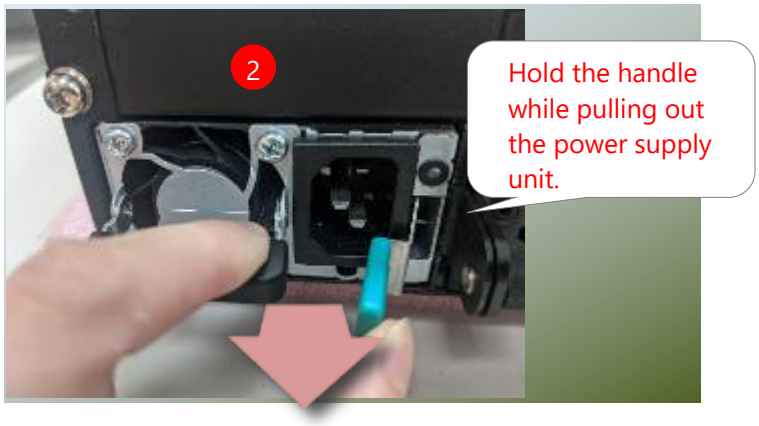
Power Supply Units

Power supply units may wear down eventually. Please be noted that HAN-9820C series supports 1300W/2000W depending on the ordering preferences. Please prepare the power supply units matching this capacity.

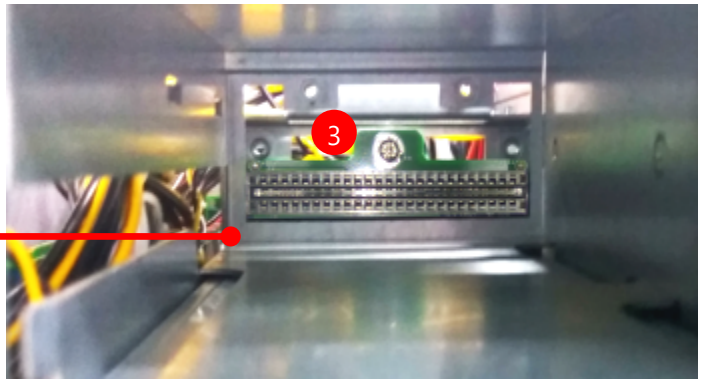
1. On the rear panel, locate the power supply unit(s) and disconnect the power cords.



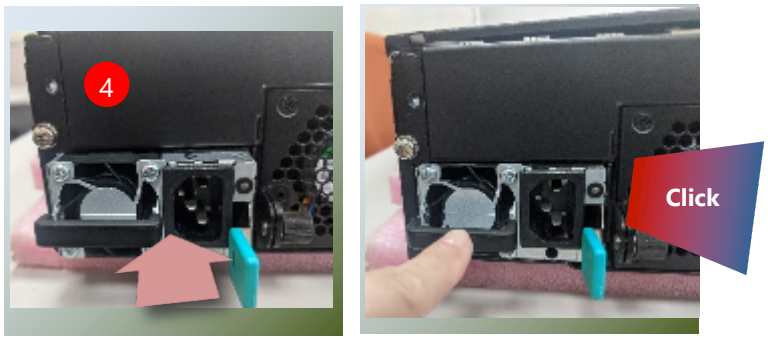
2. Pull the system out. (Pls note the images here are for reference only.)



3. Locate the internal connector of the power supply unit.

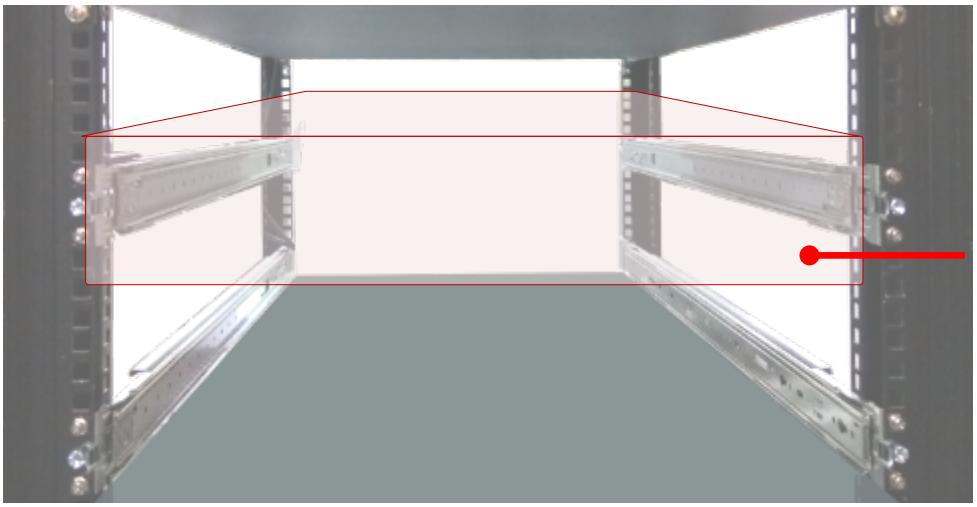


4. Insert a new power supply unit. Push the unit in until it clicks into place.



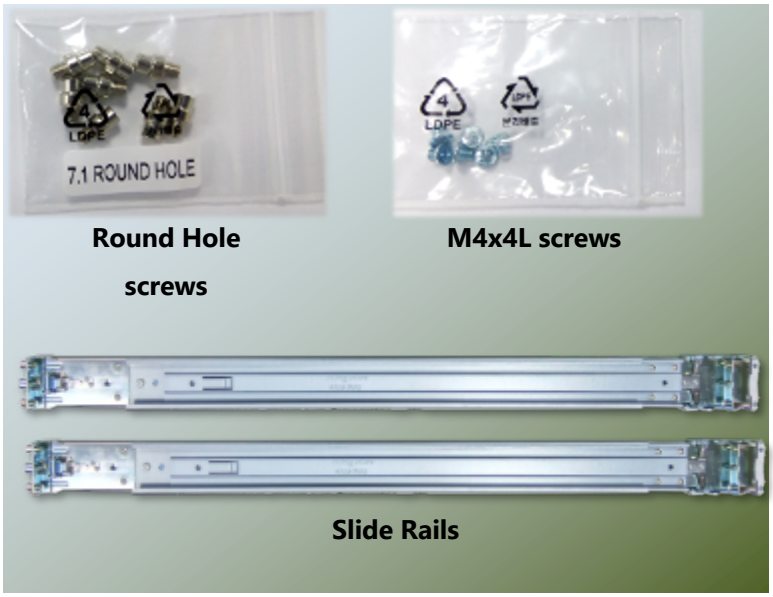
Mounting the System

The system can be installed in a rack using the Slide Rail Kit plus Short Mounting Ear brackets (optional). This method is rather complicated, but the slidable rails allow you to access the system easily while solidly securing the system in the rack. Please follow the steps below for installation.

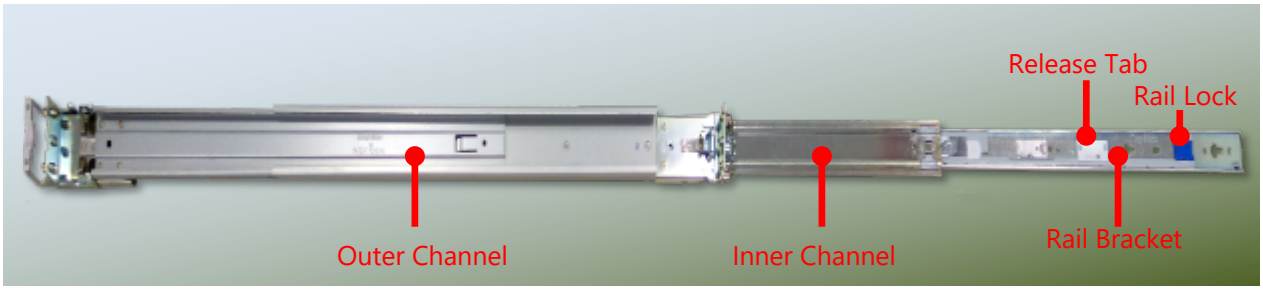


1. Check the package contents of the Slide Rail Kit. The kit shall include the following items:

- 1x pack of M4X4L screws (for securing the sliding rail on the system)
- 1x pack of 7.1mm Round Hole screws (for securing the system on the rail posts)
- 2x Slide Rails

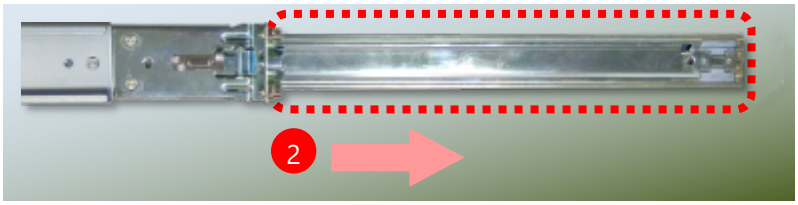


The rail consists of the following parts:

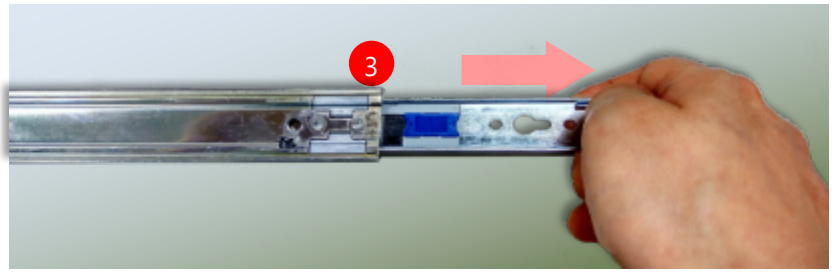


Attaching the Rail Brackets

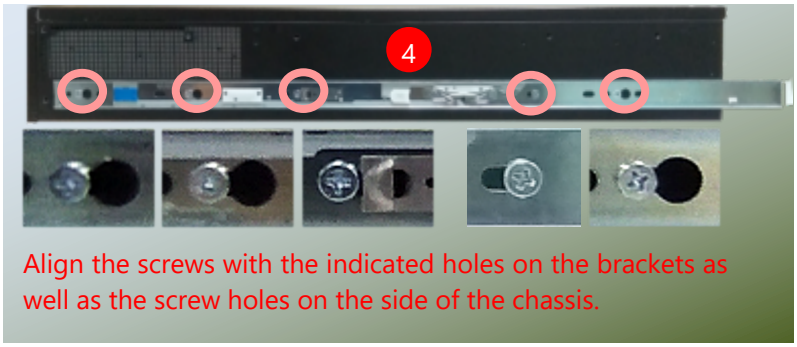
2. Unpack a slide rail and slide the inner channel all the way to the end.



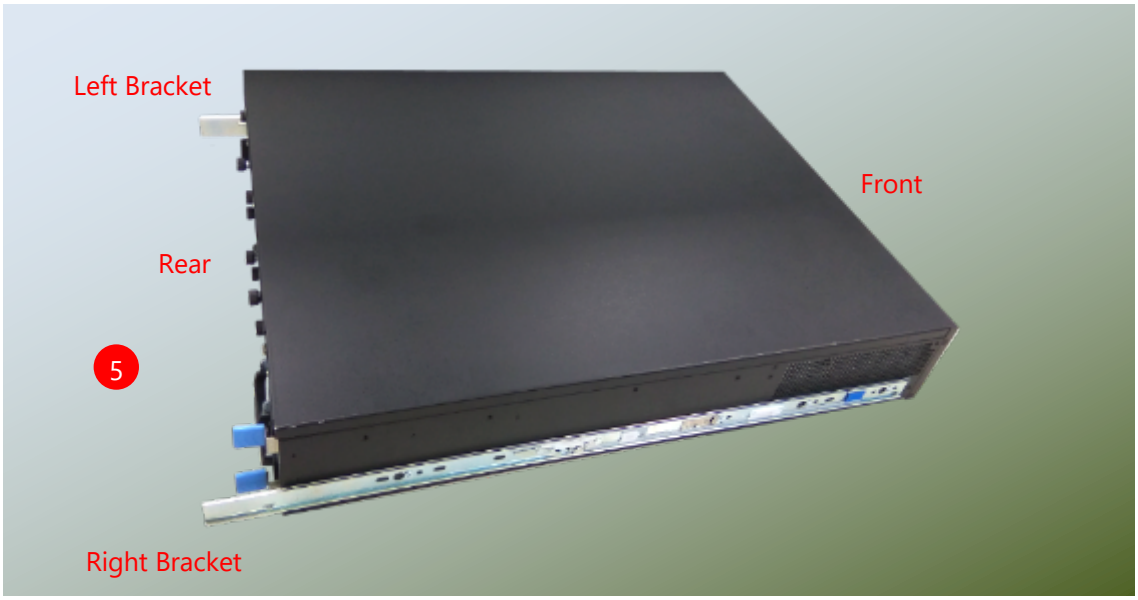
3. Remove the bracket from the Inner Rail by pushing the Release Tab on the bracket outwards while sliding it out. Stretch the bracket to the fullest.



4. Align the bracket to the side of the chassis and make sure the screw-holes are matched, and then secure the bracket onto the chassis with five provided M4X4L screws.

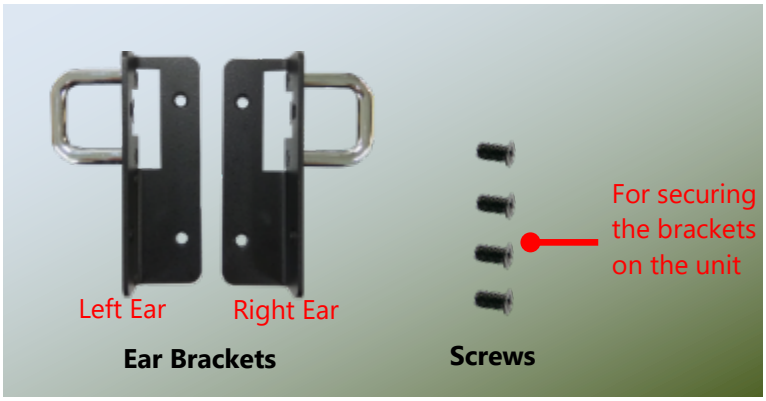


5. Repeat Steps 2~5 to attach the bracket to the other side of the chassis.

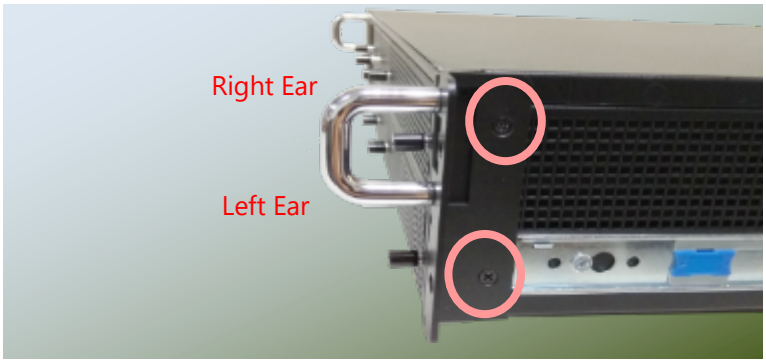


Assembling the Ear Brackets

1. Check the package contents. The supplied mounting kit shall include the items below:
   - 1x pack of screws
   - 2x Standard Ear Brackets



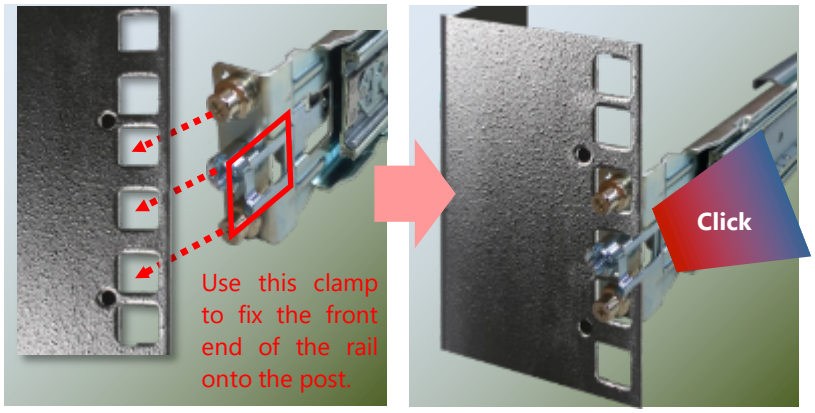
2. Install the brackets on both sides of the system using the provided screws.



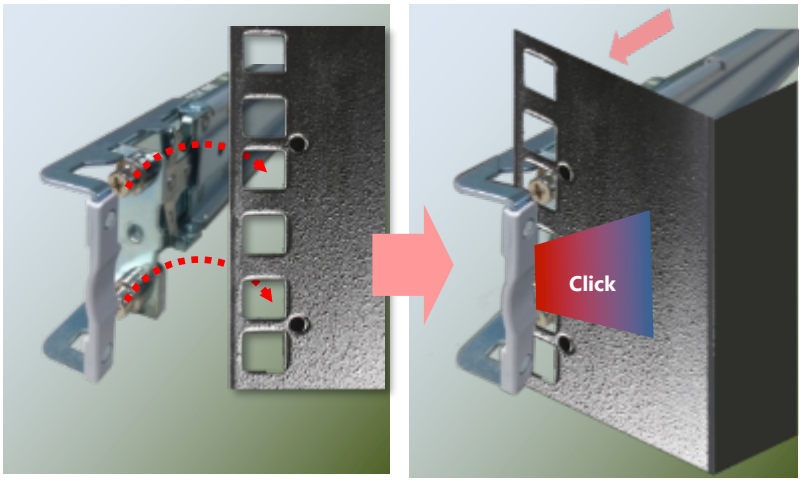
Installing the Slide Rails

Next, you shall install the slide rail assemblies onto the rack.

1. This slide-rail kit does NOT require screw-fixing. Simply aim at three (3) available screw holes on the rack front and snap the rail front into the rack post as shown in the image below. You should hear a "click" sound once it is firmly attached.

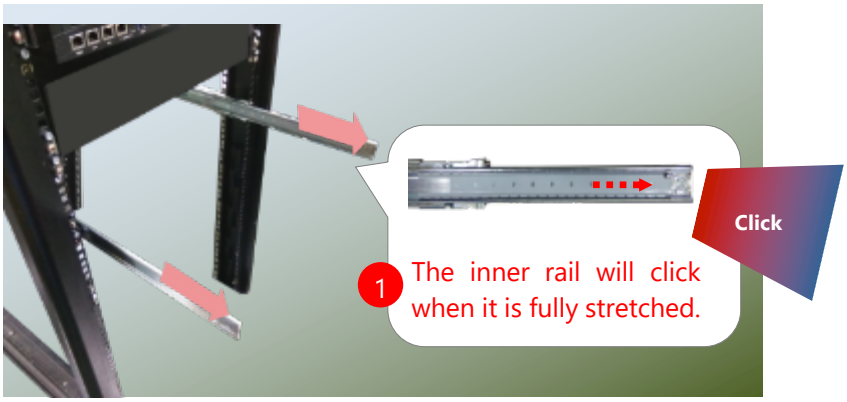


2. For the rear rack installation, slide the rail to aim and engage the bolts on the rail's rear end with the 2 available holes on the post, and the rail assembly will click into place.

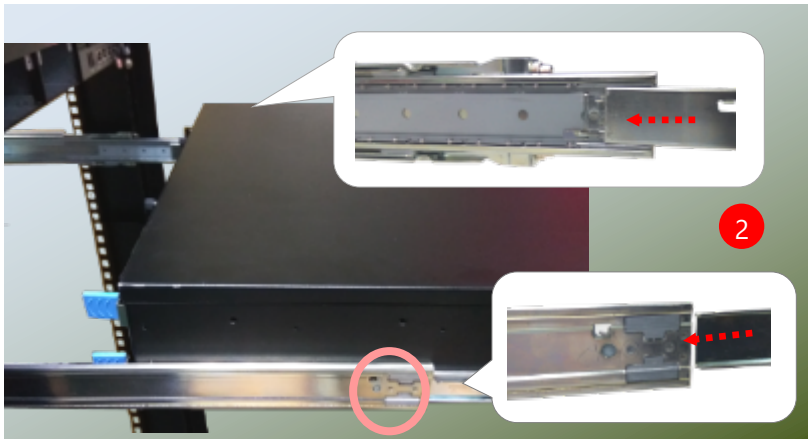


Installing the System into the Rack

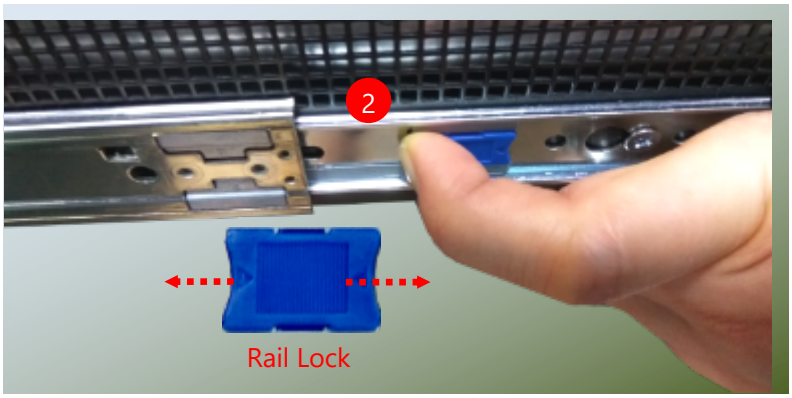
1. Stretch both of the inner rails out to their fullest extent. You will hear a click sound when they are fully stretched and locked.



2. Hold the system with its front facing you, lift the chassis and gently engage the brackets on the model while aligning them with the slide-rail assemblies as shown in the image below, and then push the system into the cabinet.



3. While pushing in the system, please also push and hold the Rail Lock tab on both brackets.



The system has completed installation in the rack.

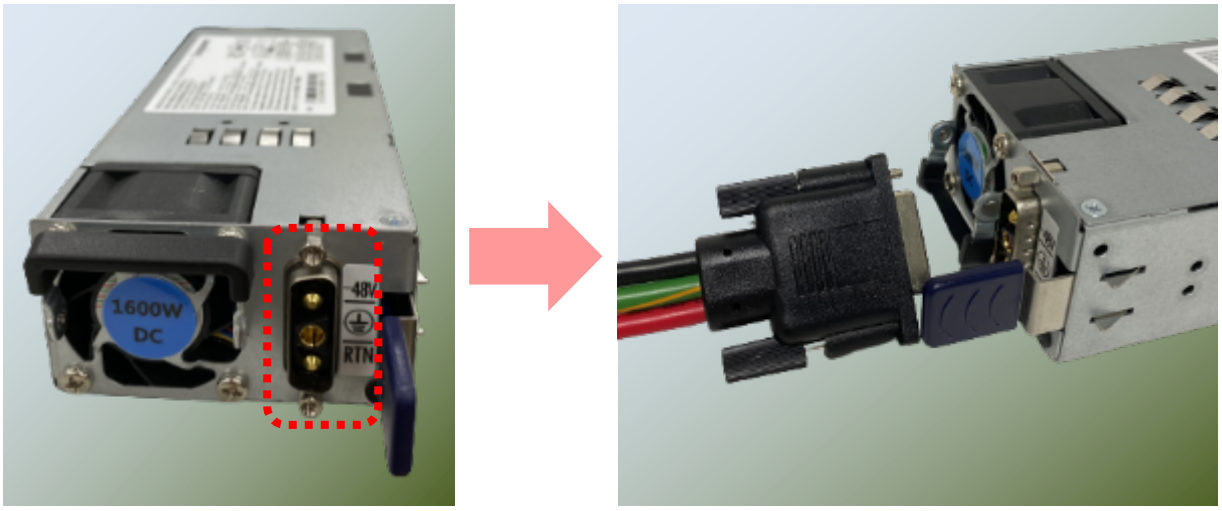
Removing the System from the Rack

1. To remove the system from the rack, gently pull it outwards towards you while pushing the Release Tab on both sides of the brackets.

DC Power Supply

The HAN-9820C series supports 1600W, depending on the ordering preferences. Please prepare the power supply units matching this capacity.

1. Connect the power cord to the connector.



- This product is intended to be supplied by a UL Listed DC power source, rated 46-72V, 40A minimum, Tma= 40 degrees C, and the altitude of operation=2000 m. If you need further assistance with purchasing the power source, please contact Lanner Electronics Inc. for further information.
- The cable should be 10AWG (20A minimum, -60V minimum).
- Use at least a 20-amp fuse for each DC breaker.
- The power supply shall not exceed 90A peak inrush current requirements for initial startup condition within the rated DC input voltage.

CHAPTER 4: REMOTE SERVER MANAGEMENT

Overview

This chapter will introduce the features of Lanner's BMC firmware and how to perform server remote management through it. Lanner has implemented IPMI 2.0 based on ASPEED service processor and support for the TLS 1.3 encryption protocol over HTTPS. The AST2500 is powered by 1024MB of RAM is a highly versatile System-on-Chip (SoC), solution designed to provide comprehensive remote access and management capabilities for servers and data center infrastructure. Its extensive feature set, coupled with integration into Lanner product, makes it an ideal choice for demanding server management scenarios. In addition, Lanner's BMC firmware runs an embedded web-server for full configuration using Web UI, which has a low learning curve.

BMC Main Features

Feature		Description
IPMI 2.0 Standard Features	System Interface support IPMI 2.0 based Management	• KCS (System Interface Support) • LAN (RMCP+) • BMC stack with an IPMI 2.0 implementation
	System Management	• Sensor monitoring • System power management • Watchdog timer • Fan speed monitor and control • FRU information
	Event Log Text Console Redirection: SOL User Management	• System Event Log (SEL) • Support in IPMI stack for SOL to remotely access BIOS and text console before OS booting • IPMI based user management • Multiple user permission level
Non-IPMI functions	Web User Interfaces User authorization Security	• BMC management via web user interface • Integrated KVM and Virtual Media • RADIUS support • LDAP support • SSL and HTTPS support • TLS 1.3 support
	Maintenance	• Auto-sync time with NTP server • Remote firmware update by Web UI or Linux tool

BMC Firmware Functional Description

System health monitoring

The BMC implements system sensor monitoring feature. It could monitor voltage, temperature, and current of critical components.

System Power Management

The BMC implements chassis power and resets functions for system administrators to control and manage the system power behavior. These functions can be activated by sending the IPMI 2.0 compatible chassis commands to the BMC over messaging interfaces. The following list summaries the supported functions.

- Chassis power on
- Chassis power off
- Chassis power cycle
- Chassis power reset
- Chassis power soft
- Server's power status report

Watchdog Timer

The BMC provides an IPMI 2.0 compatible watchdog timer which can prevent the system from system hanging.

Fan Speed Control

BMC is in charge of fan speed control. The fan speed can be modified by varying the duty cycle of PWM signal. The fan speed control algorithm mainly refers to the readings of on-board temperature sensors.

Field Replaceable Unit (FRU)

The BMC implements an interface for logical FRU inventory devices as specified in IPMI 2.0 specification. This functionality provides commands for system administrators to access and management the FRU inventory information.

System Event Log (SEL)

A non-volatile storage space is allocated to store system events for system status tracking.

Serial over LAN (SOL)

IPMI 2.0 SOL is implemented to redirect the system serial controller traffic over an IPMI session. System administrators are able to establish a SOL connection with a standard IPMI client, like IPMITOOL, to remotely interact with serial text-based interfaces such as OS command-line and serial redirected BIOS interfaces.

User Management

The BMC supports 9 IDs for IPMI user accounts. The maximum length of the username and password are 16 and 20 respectively, and the possible privilege levels are Callback, User, Operator, and Administrator. Moreover, the account creator is allowed to enable/disable the user account at any time. If not specified, the default user accounts are listed follows:

User Name	Password	User Access	Characteristics
admin	admin	Enabled	Password can be changed

Keyboard, Video, Mouse (KVM) Redirection

- The BMC provides keyboard, video, and mouse (KVM) redirection over LAN. This application is available remotely from the embedded web server.
- Support video recording, recorded videos to be downloaded & playable.

Virtual Media Redirection

- The BMC provides remote virtual CD, HD and FD redirection. CD image could be mounted directly in KVM window. HD, FD could be mounted by NFS and SAMBA.
- Efficient USB 2.0 based CD/DVD redirection with a typical speed of 20XCD.
- Completely secured transmission.

IPMI 2.0 Commands Support List

COMMANDS	NETFN	CMD
IPM Device "Global" Commands		
Get Device ID	APP (06h)	00h
Cold Reset	APP (06h)	02h
Warm Reset	APP (06h)	03h
Get Device GUID	APP (06h)	08h
BMC Watchdog Timer Commands		
Reset Watchdog Timer	APP (06h)	22h
Set Watchdog Timer	APP (06h)	24h
Get Watchdog Timer	APP (06h)	25h
BMC Device and Messaging Commands		
Get System GUID	APP (06h)	37h
Get Channel Info	APP (06h)	42h
Set User Access	APP (06h)	43h
Get User Access	APP (06h)	44h
Set User Name	APP (06h)	45h
Get User Name	APP (06h)	46h
Set User Password	APP (06h)	47h
Chassis Device Commands		
Get Chassis Capabilities	Chassis (00h)	00h
Get Chassis Status	Chassis (00h)	01h
Chassis Control	Chassis (00h)	02h
Chassis Reset	Chassis (00h)	03h
Sensor Device Commands		
Get Sensor Reading Factors	S/E (04h)	23h
Get Sensor Hysteresis	S/E (04h)	25h
Get Sensor Threshold	S/E (04h)	27h
Get Sensor Event Enable	S/E (04h)	29h
Get Sensor Event Status	S/E (04h)	2Bh
Get Sensor Reading	S/E (04h)	2Dh
Get Sensor Type	S/E (04h)	2Fh
FRU Device Commands		
Get FRU Inventory Area Info	Storage (0Ah)	10h
Read FRU Data	Storage (0Ah)	11h
Write FRU Data	Storage (0Ah)	12h
SDR Device Commands		
Get SDR Repository Info	Storage (0Ah)	20h
Get SDR Repository Allocation Info	Storage (0Ah)	21h
Get SDR	Storage (0Ah)	23h
Get SDR Repository Time	Storage (0Ah)	28h
SEL Device Commands		
Get SEL Info	Storage (0Ah)	40h
Get SEL Allocation Info	Storage (0Ah)	41h

Get SEL Entry	Storage (0Ah)	43h
Delete SEL Entry	Storage (0Ah)	46h
Clear SEL	Storage (0Ah)	47h
Get SEL Time	Storage (0Ah)	48h
Set SEL Time	Storage (0Ah)	49h
Get SEL Time UTC Offset	Storage (0Ah)	5Ch
Set SEL Time UTC Offset	Storage (0Ah)	5Dh
LAN Device Commands		
Set LAN Configuration Parameters	Transport (0Ch)	01h
Get LAN Configuration Parameters	Transport (0Ch)	02h
Serial/Modem Device Commands		
Set User Callback Options	Transport (0Ch)	1Ah
Get User Callback Options	Transport (0Ch)	1Bh
SOL Activating	Transport (0Ch)	20h
Set SOL Configuration Parameters	Transport (0Ch)	21h
Get SOL Configuration Parameters	Transport (0Ch)	22h

References

Please refer the followings document and video for more detail information

- AST 2500 & AST 2600 BMC LTC Specification Manual
  - https://www.lannerinc.com/support/download-center/software/category/31-network-appliances?download=617:ast2500-ast2600-bmc-ltc-specification-manual

- IPMI Remote Monitoring
  - https://www.youtube.com/watch?v=O2gmiYMdrb4

CHAPTER 5: BIOS FUNCTION

The system has AMI BIOS built-in, with a SETUP utility that allows users to configure required settings or to activate certain system features. Pressing the <Tab> or <DEL> key immediately allows you to enter the Setup Utility.

Enter BIOS Setup

To enter the BIOS setup utility, simply follow the steps below:

1. Boot up the system.
2. Press **<Delete>** during the boot-up if you connect a keyboard to this unit. But if you connect a PC to this unit through console USB/Serial connection, then press **<Tab>**. Your system should be running POST (Power-On-Self-Test) upon booting up.
3. Then you will be directed to the BIOS main screen.
4. Instructions of BIOS navigations:

Control Keys	Description
→←	select a setup screen, for instance, [Main], [Advanced], [Platform], [Socket], [Server Mgmt], [Security], [Boot], and [Save & Exit]
↑↓	select an item/option on a setup screen
<Enter>	select an item/option or enter a sub-menu
+/-	to adjust values for the selected setup item/option
F1	to display General Help screen
F2	to retrieve previous values, such as the parameters configured the last time you had entered BIOS.
F3	to load optimized default values
F4	to save configurations and exit BIOS
<Esc>	exit the current screen

Main Page

Setup Main Page contains BIOS information and project version information.

Item	Description
BIOS Information	BIOS Vendor: American Megatrends Core Version: AMI Kernel version, CRB code base, X64 Compliancy : UEFI version, PI version Project Version: BIOS release version Build Date and Time: MM/DD/YYYY Access Level: Administrator / User
Memory Information	Total Memory: by case
System Date	To set the Date, use **<Tab>** to switch between Date elements. Default range of Year: 2005-2099 Default range of Month: 1-12 Days: dependent on Month.
System Time	To set the Date, use **<Tab>** to switch between Date elements.

Advanced Setup

Select the Advanced menu tab from the BIOS setup screen to enter the "Advanced" setup screen. Users can select any of the items in the left frame of the screen.

Trusted Computing

This option allows you to configure parameters regarding BIOS support for security device.

Feature	Options	Description
Security Device Support	Enabled Disabled	Enables or disables BIOS support for security device. By disabling this function, OS will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

Trusted Computing (TPM1.2)

Item	Option	Description
Security Device Support	Enabled Disabled	Enables or disables BIOS support for the security device. By disabling this function, OS will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
TPM State	Enabled Disabled	Enables or disables Security Device. NOTE: Your computer will reboot during a restart in order to change State of the Device.
Pending operation	None TPM Clear	Schedules an Operation for the Security Device. NOTE: Your computer will reboot during a restart in order to change State of Security Device.
Device Select	TPM 1.2 TPM 2.0 Auto	**TPM 1.2** will restrict support to TPM 1.2 devices; while **TPM 2.0** will restrict support to TPM 2.0 devices; **Auto** will support both with the default set to TPM 2.0 devices. If not found, TPM 1.2 devices will be enumerated.

Trusted Computing (TPM 2.0)

Item	Option	Description
Security Device Support	Enabled Disabled	Enables or disables BIOS support for security device. By disabling this function, OS will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA-1 PCR Bank	Enabled Disabled	Enables or disables SHA-1 PCR Bank.
SHA256 PCR Bank	Enabled Disabled	Enables or disables SHA256 PCR Bank.
Pending operation	None TPM Clear	Schedules an Operation for the Security Device. NOTE: Your computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Enabled Disabled	Enables or disables Platform Hierarchy.
Storage Hierarchy	Enabled Disabled	Enables or disables Storage Hierarchy.
Endorsement Hierarchy	Enabled Disabled	Enables or disables Endorsement Hierarchy.
TPM2.0 UEFI Spec Version	TCG_1_2 TCG_2	Select the TCG2 Spec Version, **TCG_1_2**: Supports the Compatible mode for Win8/Win10 **TCG_2**: Supports new TCG2 protocol and event format for Win10 or later.
Physical Presence Spec Version	1.2 1.3	Select to tell OS to support PPI Spec Version 1.2 or 1.3. **NOTE**: Some HCK tests might not support 1.3.
TPM 20 Interface Type	TIS	Select **TPM 20 Device** for the Communication Interface.
Device Select	TPM 1.2 TPM 2.0 Auto	**TPM 1.2** will restrict support to TPM 1.2 devices; while **TPM 2.0** will restrict support to TPM 2.0 devices; **Auto** will support both with the default set to TPM 2.0 devices. If not found, TPM 1.2 devices will be enumerated.

Super IO Configuration

This option allows you to configure parameters about Super IO Chip.

Serial Port 1 Configuration

Select "Serial Port 1 Configuration" or "Serial Port 2 Configuration" to enter sub setting screen.

Item	Option	Description
Serial Port	Enabled Disabled	Enables or disables Serial Port 1.
Device Settings	NA	IO=3F8h; IRQ = 4

Serial Port 2 Configuration

Item	Option	Description
Serial Port	Enabled Disabled	Enables or disables Serial Port 2
Device Settings	NA	IO=2F8h; IRQ = 3

Digital IO Configuration

This option allows you to configure parameters about Digital IO pins.

Item	Option	Description
Digital I/O Output 1	Output High Output Low	Configure Digital I/O Pin5
Digital I/O Output 2	Output High Output Low	Configure Digital I/O Pin6
Digital I/O Output 3	Output High Output Low	Configure Digital I/O Pin7
Digital I/O Output 4	Output High Output Low	Configure Digital I/O Pin8

Status LED Configuration

This option allows you to change the color of status LED.

Item	Option	Description
Status LED	OFF GREEN RED	Configures Status LED color

Watch Dog Timer Configuration

This option allows you to enable or disable the watchdog timer function.

Item	Option	Description
Watch Dog Timer	Enabled Disabled	Enables or disables Watch Dog Timer function

Serial Port Console Redirection

This option allows you to configure parameters about serial port console redirection. Press <**Enter**> to access the submenu.

Item	Option	Description
COM0 Console Redirection	Enabled Disabled	Enables or disables Console Redirection

Console Redirection Settings

These settings specify how the host computer and the remote computer will exchange data. Both computers should have the same or compatible settings.

Item	Option	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	**VT100**: ASCII char set **VT100+**: Extends VT100 to support color, function keys, etc. **VT-UTF8**: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes **ANSI**: Extended ASCII char set
Bits per second	9600 19200 38400 57600 115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 8	Data Bits
Parity	None Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors.
Stop Bits	1 2	Indicates the end of a serial data packet.
Flow Control	None Hardware RTS/CTS	Flow Control can prevent data loss from buffer overflow.
VT-UTF8 Combo Key Support	Disabled Enabled	Enables VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled Enabled	With this mode enabled, only text will be sent. This is to capture Terminal data.
Resolution	Disabled	Enables or disables extended terminal resolution

100x31	Enabled	
Putty KeyPad	VT100 LINUX XTERM86 SCO ESCN VT400	Selects FunctionKey and KeyPad on Putty.

Legacy Console Redirection Settings

This option allows you to configure legacy console redirection options. Press <**Enter**> to access the submenu.

Item	Option	Description
Legacy Serial Redirection Port	COM0	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages
Legacy OS Redirection Resolution	80x24 80x25	On Legacy OS, the Number of Rows and Columns supported redirection.
Redirection After BIOS POST	Always Enable Boot Loader	When **Bootloader** is selected, legacy Console Redirection is disabled before booting to legacy OS. When **Always Enable** is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to **Always Enable**.

PCI Subsystem Settings

This option allows you to change the PCI, PCI-X and PCI Express settings.

Item	Option	Description
Above 4G Decoding	Disabled Enabled	Enables or disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64-bit PCI Decoding)
SR-IOV Support	Disabled Enabled	If the system has SR-IOV capable PCIe Devices, this option enables or disables Single Root IO Virtualization Support.

USB Configuration

This option allows you to change USB configuration parameters.

Item	Option	Description
Legacy USB Support	Enabled Disabled Auto	Enables Legacy USB support. **Auto** option disables legacy support if no USB devices are connected; **Disabled** option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled Disabled	Enables or disables USB Mass Storage Driver Support.
USB transfer time-out	1 sec 5 sec 10 sec 20 sec	The time-out value for Control, Bulk, and Interrupt transfers
Device reset time-out	1 sec 5 sec 10 sec 20 sec	USB mass storage device Start Unit command time-out
Device power-up delay	Auto Manual	Maximum time the device will take before it properly reports itself to the Host Controller. **Auto** uses default value: for a Root port, it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

Network Stack Configuration

This option enables or disables UEFI network stack.

Item	Option	Description
Network Stack	Disabled Enabled	Enables or disables UEFI Network Stack
Ipv4 PXE Support	Disabled Enabled	Enables Ipv4 PXE Boot Support. If IPV4 is disabled, PXE boot option will not be created.
Ipv4 HTTP/HTTPS Support	Disabled Enabled	Enables Ipv4 HTTP/HTTPS Boot Support. If IPV4 is disabled, HTTP boot option will not be created.
Ipv6 PXE Support	Disabled Enabled	Enables Ipv6 PXE Boot Support. If IPV6 is disabled, PXE boot option will not be created.
Ipv6 HTTP/HTTPS Support	Disabled Enabled	Enables Ipv6 HTTP/HTTPS Boot Support. If IPV6 is disabled, HTTP/HTTPS boot option will not be created.
PXE boot wait time	0	Wait time to press **<ESC>** key to abort the PXE boot
Media detect count	1	Number of times the presence of media will be checked

CSM Configuration

This option allows you to enable or disable ROM execution settings.

Item	Option	Description
CSM Support	Disabled Enabled	Enables or disables CSM Support
Network	Do Not Launch UEFI Legacy	Controls the execution of UEFI and Legacy PXE OpROM
Storage	Do Not Launch UEFI Legacy	Controls the execution of UEFI and Legacy Storage OpROM
Video	Do Not Launch UEFI Legacy	Controls the execution of UEFI and Legacy Video OpROM
Other PCI device	Do Not Launch UEFI Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video

Control Legacy PXE Boot

This option allows you to configure Legacy PXE boot settings.

Item	Option	Description
Control Legacy PXE Boot from	Disabled LAN1(i350) LAN2(i350)	Select On Board LAN# Boot

Platform Setup

Use [→] or [←] to select [Platform] setup screen. Under this screen, you may use [↑] [↓] to select an item you want to configure.

Item	Option	Description
PCH Configuration	None	Displays and provides option to change the PCH Settings
Server ME Configuration	None	Configure Server ME Technology Parameters
Runtime Error Logging	None	Press <Enter> to view or change the runtime error log configuration.

PCH Configuration

This option displays and provides options to change the PCH Settings.

Item	Option	Description
PCI Express Configuration	None	PCI Express Configuration settings
PCH sSATA Configuration	None	sSATA devices and settings
Restore AC Power Loss	Power On Power Off Last State	Select S0/S5 for ACPI state after a G3
Serial IRQ Mode	Quiet Continuous	Configure Serial IRQ Mode.

PCI Express Configuration

This option allows you to configure PCI express related options.

Item	Option	Description
PCIe Root Port Function Swapping	Disabled Enabled	Enable PCIe root port function swapping feature to dynamically assign function 0 to enabled root port.
Max Read Request Size	MRRS 128B MRRS 256B MRRS 512B MRRS 1024B MRRS 2048B MRRS 4096B	PCIE Max Read Request Size Selection.

PCH sSATA Configuration

This option allows you to configure SATA devices related options.

Item	Option	Description
SATA Controller	Disabled Enabled	Enables or disables SATA Controller
Configure SATA as	AHCI RAID	This will configure SATA as **RAID** or **AHCI**.
Support Aggressive Link Power Management	Disabled Enabled	Enables or disables SALP
Port 0/2/3/4/5	Disabled Enabled	Enable or Disable SATA Port
Hot Plug	Disabled Enabled	Designates this port as Hot Pluggable.
Configure as eSATA	Disabled Enabled	Configures port as External SATA (eSATA)
Spin Up Device	Disabled Enabled	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Unknown ISATA Direct Connect Flex M2	Identify the SATA Topology if it is Default or ISATA or Flex or Direct Connect or M2

Runtime Error Logging

This option configures runtime error logging parameters.

Item	Option	Description
System Errors	Disabled Enabled	System Error Enable/Disable setup options.

Socket Setup

Use [→] or [←] to select [Socket] setup screen. Under this screen, you may use [↑] [↓] to select an item you want to configure.

Item	Option	Description
Processor Configuration	None	Displays and provides option to change the Processor Settings
Memory Configuration	None	Displays and provides option to change the Memory Settings
IIO Configuration	None	Displays and provides option to change the IIO Settings
Advanced Power Management Configuration	None	Displays and provides option to change the Power Management Settings
Numa	Disabled Enabled	Displays and provides option to change the Power Management Settings

Processor Configuration

In Processor Configuration, you can change the processor settings and view the current parameters.

Item	Option	Description
Hyper-Threading [ALL]	Disabled Enabled	Enables Hyper Threading (Software Method to Enable/ Disable Logical Processor threads.
Machine Check	Disabled Enabled	Enable or Disable the Machine Check
Hardware Prefetcher	Disabled Enabled	= MLC Streamer Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefetcher	Disabled Enabled	= MLC Spatial Prefetcher (MSR 1A4h Bit[1])
Extended APIC	Disabled Enabled	Enables or disables extended APIC support
Enable Intel® TXT	Disabled Enabled	Enables Intel(R) TXT
VMX	Disabled Enabled	Enables the Vanderpool Technology, which takes effect after reboot.
Enable SMX	Disabled Enabled	Enables Safer Mode Extensions
AES-NI	Disabled Enabled	Enables or disables AES-NI support

Per-Socket Configuration

Enter to configure the settings related to processor socket options.

Item	Option	Description
CPU Socket0 Configuration	None	None
CPU Socket1 Configuration	None	None

CPU Socket 0 Configuration

Item	Option	Description
Core Disable Bitmap (Hex)	0	0: Enable all cores. FFFFFFFFFF: Disable all cores least one core per CPU must be enabled. Disabling all cores is an invalid configuration.

CPU Socket 1 Configuration

Item	Option	Description
Core Disable Bitmap (Hex)	0	0: Enable all cores. FFFFFFFFFF: Disable all cores least one core per CPU must be enabled. Disabling all cores is an invalid configuration.

Memory Configuration

In Memory Configuration, you can change memory settings.

Item	Option	Description
Memory Frequency	Auto 1200 1333 1400 1600 1800 1866 2000 2133 2200 2400 2600 2666 2800 2933 3000 3200 3400-OvrClk 3466-OvrClk 3600-OvrClk 3733-OvrClk 3800-OvrClk 4000-OvrClk 4200-OvrClk 4266-OvrClk 4400-OvrClk 4800-OvrClk	Maximum Memory Frequency Selections in Mhz. Do not select Reserved
Memory Topology	None	Displays memory topology with Dimm population information

IIO Configuration

In IIO Configuration, you can change socket settings and view the current parameters.

Item	Option	Description
Socket0 Configuration	None	None
Socket1 Configuration	None	None
IOAT Configuration	None	All IOAT configuration options
Intel® VT for Directed I/O (VT-d)	None	Press **<Enter>** to bring up the Intel? VT for Directed I/O (VT-d) Configuration menu.
Intel® VMD technology	None	Press <Enter> to bring up the Intel® VMD for Volume Management Device Configuration menu.
PCI-E ASPM Support (Global)	No Per-Port L1 Only	This option enables / disables the ASPM support for all downstream devices.
PCIe Extended Tag Enable	Auto No Yes	Auto/Enable - BIOS sets 8-bit Tag Field for PCIe Root Port/End Point. Disable - BIOS sets 5-bit Tag Field for PCIe Root Port/End Point
PCIe Max Read Request Size	Auto 128B 256B 512B 1024B 2048B 4096B	Set Max Read Request Size in End Points
Socket0 Configuration	None	None

Socket 0 Configuration

Enter to configure the settings related to PCI Express ports under Socket0.

Item	Option	Description
Socket 0 Port 1A	None	Settings related to PCI Express Port 1A
Socket 0 Port 2A	None	Settings related to PCI Express Port 2A
Socket 0 Port 2C	None	Settings related to PCI Express Port 2C
Socket 0 Port 4A	None	Settings related to PCI Express Port 4A
Socket 0 Port 4C	None	Settings related to PCI Express Port 4C

Socket 0 Port 5A	None	Settings related to PCI Express Port 5A

Socket 1 Configuration

Enter to configure the settings related to PCI Express ports under Socket1.

Item	Option	Description
Socket 1 Port 1A	None	Settings related to PCI Express Port 1A
Socket 1 Port 1C	None	Settings related to PCI Express Port 1C
Socket 1 Port 1D	None	Settings related to PCI Express Port 1D
Socket 1 Port 2A	None	Settings related to PCI Express Port 2A
Socket 1 Port 2C	None	Settings related to PCI Express Port 2C
Socket 1 Port 4A	None	Settings related to PCI Express Port 4A
Socket 1 Port 4C	None	Settings related to PCI Express Port 4C
Socket 1 Port 5A	None	Settings related to PCI Express Port 5A

IOAT Configuration

Item	Option	Description
Sck0 IOAT Config	None	None
Sck1 IOAT Config	None	None
Disable TPH	No Yes	TLP Processing Hint disable
Prioritize TPH	Disabled Enabled	Prioritize TPH
Relaxed Ordering	No Yes	Relaxed Ordering Enable/Disable

Intel® VT for Directed I/O (VT-d)

Item	Option	Description
Intel® VT for Directed I/O (VT-d)	No Yes	Press **<Enter>** to bring up the Intel® VT for Directed I/O (VT-d) Configuration menu.

Advanced Power Management Configuration

In Advanced Power Management Configuration, you can modify power management settings.

Item	Option	Description
CPU P State Control	None	P State Control Configuration Sub Menu, include Turbo, XE and etc.
CPU C State Control	None	CPU C State setting

CPU P State Control

Item	Option	Description
SpeedStep(Pstates)	Disabled Enabled	Enables or disables EIST (P-States)
Boot performance mode	Max Performance Max Efficient Set by Intel Node Manager	Select the performance state that the BIOS will set before OS hand off.
CPU Flex Ratio Override	Disabled Enabled	Enable/Disable CPU Flex Ratio Programming
CPU Core Flex Ratio	23	Non-Turbo Mode Processor Core Ratio Multiplier

CPU C State Control

Item	Option	Description
CPU C1 auto demotion	Disabled Enabled	Autonomous Core C-State Control
CPU C6 report	Disabled Enabled	Enables or disables CPU C6(ACPI C3) report to OS
Enhanced Halt State (C1E)	Disabled Enabled	Core C1E auto promotion Control. Takes effect after reboot.

Server Mgmt Setup

Use [→] or [←] to select [Server Mgmt] setup screen. Under this screen, you may use [↑] [↓] to select an item you want to configure.

Item	Option	Description
BMC Support	Enabled Disabled	Enable or disables interfaces to communicate with BMC.
Wait For BMC	Enabled Disabled	Wait for BMC response for specified time-out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.
FRB-2 Timer	Enabled Disabled	Enables or disables FRB-2 timer (POST timer).
FRB-2 Timer timeout	3 minutes 4 minutes 5 minutes 6 minutes	Enter value Between 3 to 6 min for FRB-2 Timer Expiration value.
FRB-2 Timer Policy	Do Nothing Reset Power Down Power Cycle	Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.
OS Watchdog Timer	Enabled Disabled	If enabled, it starts a BIOS timer which can only be shut off by Management Software after the OS loads. It also helps verify that the OS is successfully loaded or follows the OS Boot Watchdog Timer policy.
OS Wtd Timer Timeout	5 minutes 10 minutes 15 minutes 20 minutes	Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled.
OS Wtd Timer Policy	Do Nothing Reset Power Down Power Cycle	Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.
System Event Log	NA	Press **<Enter>** to change the SEL event log configuration.
BMC network configuration	NA	Configure BMC network parameters.
View System Event Log	NA	Press **<Enter>** to view the System Event Log Records.
BMC Warm Reset	NA	Press **<Enter>** to do Warm Reset BMC.

System Event Log

Use this option to change the SEL event log configuration.

Item	Option	Description
SEL Components	Disabled Enabled	Enables or disables all features of System Event Logging during boot.
Erase SEL	NO Yes, On next reset Yes, On every reset	Choose options for erasing SEL.
When SEL is Full	Do Nothing Erase Immediately Delete Oldest Record	Choose options for reactions to a full SEL.

BMC Network Configuration

This option allows you to configure BMC network parameters.

Item	Option	Description
Configuration Address source	Unspecified Static DynamicBmcDhcp	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). The **unspecified** option will not modify any BMC network parameters during BIOS phase.

View System Event Log

This option allows you to view the System Event Log Records.

Security Setup

Use [←] / [→] to select [Security] setup screen. Under this screen, you may use [↑] [↓] to select an item you would like to configure.

Item	Description
Administrator Password	If ONLY the Administrator's password is set, it only limits access to Setup and is only asked for when entering Setup.
User Password	If ONLY the User's password is set, it serves as a power-on password and must be entered to boot or enter Setup. In Setup, the User will have Administrator rights.

Secure Boot

This option allows you to customize Secure Boot settings.

Item	Option	Description
Secure Boot	Disabled Enabled	Secure Boot is activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled.
Secure Boot Mode	Standard Custom	Secure Boot mode selector: In **Custom** mode, Secure Boot Variables can be configured without authentication

Key Management

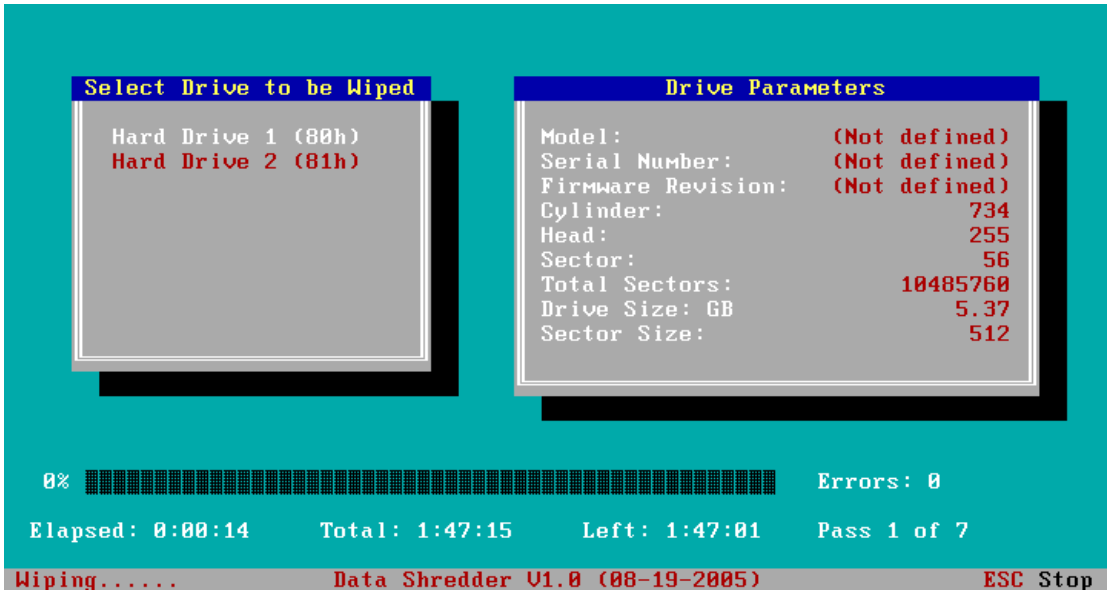
Allows you to provision advanced Secure Boot settings.

Item	Option	Description
Factory Key Provision	Disabled Enabled	Provision factory default keys on next re-boot only when System in Setup Mode.
Restore Factory keys	None	Force System to User Mode. Configure NVRAM to contain OEM-defined factory default Secure Boot keys.
Enroll Efi Image	None	Allows the image to run in Secure Boot mode. Enroll SHA256 hash of the binary into Authorized Signature Database (db)

Secure Erase

This option allows you to secure erase any or all HDD/SSD in system. Please note that all data cannot be recovered through data recovery techniques. This process is crucial in scenarios where data confidentiality and security are paramount, such as in industries like finance, healthcare, and government.

Item	Option	Description
Secure Erase	Active Back	System will kick-off an utility to allow you wipe all data in any or all HDD/SDD in system.



Boot Setup

Use [←] / [→] to select [Boot] setup screen. Under this screen, you may use [↑] [↓] to select an item you would like to configure.

Item	Option	Description
Setup Prompt Timeout	5	The Number of seconds to wait for setup activation key. 65535 means indefinite waiting.
BootupNumLock State	On Off	Select the keyboard NumLock state.
Quiet Boot	Disabled Enabled	Enables or disables Quiet Boot option.
Boot mode select	LEGACY UEFI DUAL	Select boot mode for LEGACY or UEFI.

■ Choose boot priority from boot option group.

■ Choose specific boot device priority sequence from available Group device.

Save and Exit Setup

Use [←] / [→] to select [Save & Exit] setup screen. Under this screen, you may use [↑] [↓] to select an item you would like to configure.

■Discard Changes and Exit

Select this option to quit Setup without saving any modifications to the system configuration. The following window will appear after the "Discard Changes and Exit" option is selected. Select "**Yes"** to discard changes and Exit Setup.

■Save Changes and Reset

When Users have completed the system configuration changes, select this option to save the changes and reset from BIOS Setup in order for the new system configuration parameters to take effect. The following window will appear after selecting the "**Save Changes and Reset**" option is selected. Select "**Yes**" to Save Changes and reset.

■Restore Defaults

Restore default values for all setup options. Select "**Yes"** to load Optimized defaults.

Note: The items under Boot Override may not be the same images, it would depend on devices connected on the system.

APPENDIX A: LED INDICATOR EXPLANATIONS

The status explanations of LED indicators on Front Panel are as follows:

LED indicators

System Power
System Status
HDD Activity

- **System Power**

Solid Green	*The system is powered on*
Off	*The system is powered off*

- **System Status**

  This LED indicator is programmable. You could program it to display the operating status of the behaviors described below:

Solid Green	*Defined by GPIO*
Solid Red	*Defined by GPIO*
Off	*Defined by GPIO*

- **HDD Activity**

  If this LED blinks, it indicates data access activities; otherwise, it remains off.

Blinking Amber	*Indicates HDD activity including SATA / NVME*
Off	*No data access activity OR No power on*

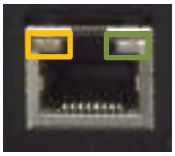
Note:

1. When cable is plug-in and network is linked. Both LED will be light up.
2. Without the Cable plug-in, the LED should be off.
3. If LAN Driver control the LED, the behavior will follow the driver.

- **RJ-45 LAN LED Indicators**

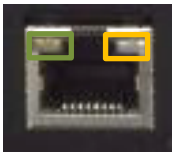
10/100/1G

Amber *Green/ Amber*



2.5G/10G

Green *Green/ Amber*



- **10M/100M/1GB RJ-45 Define:**

Speed	Amber (Active)	Green/Amber (Link)
10M	Blinking Amber – Indicates data access	OFF
100M	Blinking Amber – Indicates data access	ON (Green)
1G	Blinking Amber – Indicates data access	ON (Amber)

- **2.5G / 10G RJ-45 define:**

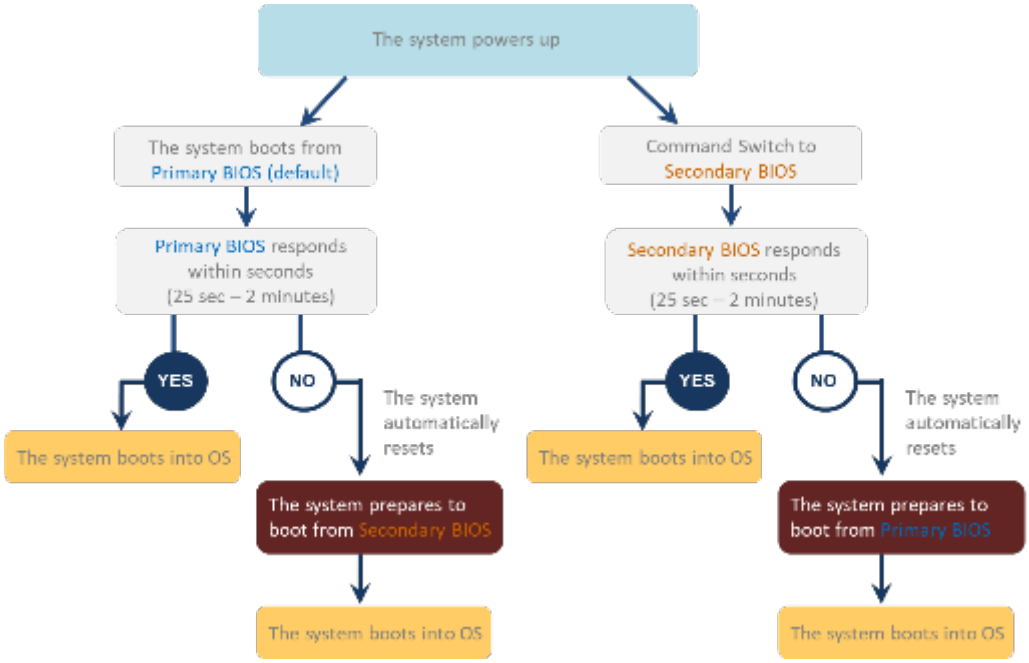
Speed	Amber (Active)	Green/Amber (Link)
2.4G	Blinking Amber – Indicates data access	ON (Green)
10G	Blinking Amber – Indicates data access	ON (Green)

APPENDIX B: DUAL BIOS FOR RECOVERY

Failure when booting up BIOS is not uncommon and can occur most often during a power failure, a mishandled BIOS update, a malware attack resulting in data corruption. When it happens, recovering procedures consume considerable time and effort. Lanner understands this pain and have empowered our products with the Dual BIOS feature.

How Dual BIOS Works

Dual BIOS features two physical BIOS ROMs soldered onto the motherboard, carrying two separate BIOS images. If the Primary BIOS (default) is not functioning correctly and fails to respond within seconds (~25 seconds to 2 minutes, depend upon appliance), the system will invoke a bootup from the Secondary BIOS, automatically restarting the system and launch the operating system.



2nd Gen Dual BIOS

To provide increased flexibility and usage protection, Lanner has released the 2nd Gen Dual BIOS function on Lanner appliances. With 2nd Gen Dual BIOS, both the primary BIOS and secondary BIOS can be updated and flashed using the BIOS Tool to run different versions of BIOS ROMS independently for maximum compatibility. This additionally allow users to switch BIOS ROMS for booting up, toggling between primary BIOS and secondary BIOS.

- **Flexible recovery timer control**

Users can designate the amount of time before recovery BIOS launch. The amount of time is no longer fixed to 7 minutes.

- **Flexible Dual BIOS ROMs control.**

Users can flash both the Primary BIOS and Secondary BIOS, thus run different versions of BIOS ROMS independently for maximum compatibility.

- **Flexible Dual BIOS ROMs switch**

The 2nd Gen Dual BIOS allow users to choose one of the BIOS ROMS (Primary BIOS/Secondary BIOS) for booting up. Use software command prompt to toggle between Primary BIOS and Secondary BIOS.

	Gen1 Dual BIOS	Gen2 Dual BIOS
Function	Primary / Recovery 2ND BIOS for recovery purpose	Primary / Secondary (Peer to Peer) Both BIOS can let the system work
Detection Time	7 min	Seconds (By platform design)
2nd BIOS updated	Only using the SPI facility	By BIOS tool command or SPI facility
MAC/DMI	Only for BIOS1	For both BIOS
CPLD Interface	GPIO	LPC or eSPI (By Platform)

Figure 1. Gen 1 vs Gen 2 Dual BIOS comparison chart

Few things can shut down a computer as completely as a corrupted BIOS. With Dual BIOS feature, you will be guaranteed to enter a healthy OS to perform thorough troubleshooting before the situation is irreparable.

Get Ready for BIOS Update

Flashing a BIOS needs to be carefully completed, especially pertaining to a corrupted BIOS, which can lead to an unusable system if done incorrectly. To get ready for a BIOS update, acquire the following BIOS resources from Lanner technical support:

- Firmware and Flash Tool
- BIOS Engineering Spec

Before you start, make sure you select the correct firmware version, correct BIOS (Primary or Secondary) and go through the instructions for BIOS update in *BIOS Engineering Spec* thoroughly. If you cannot be certain if this version is correct for your system, please contact Lanner Technical Support.

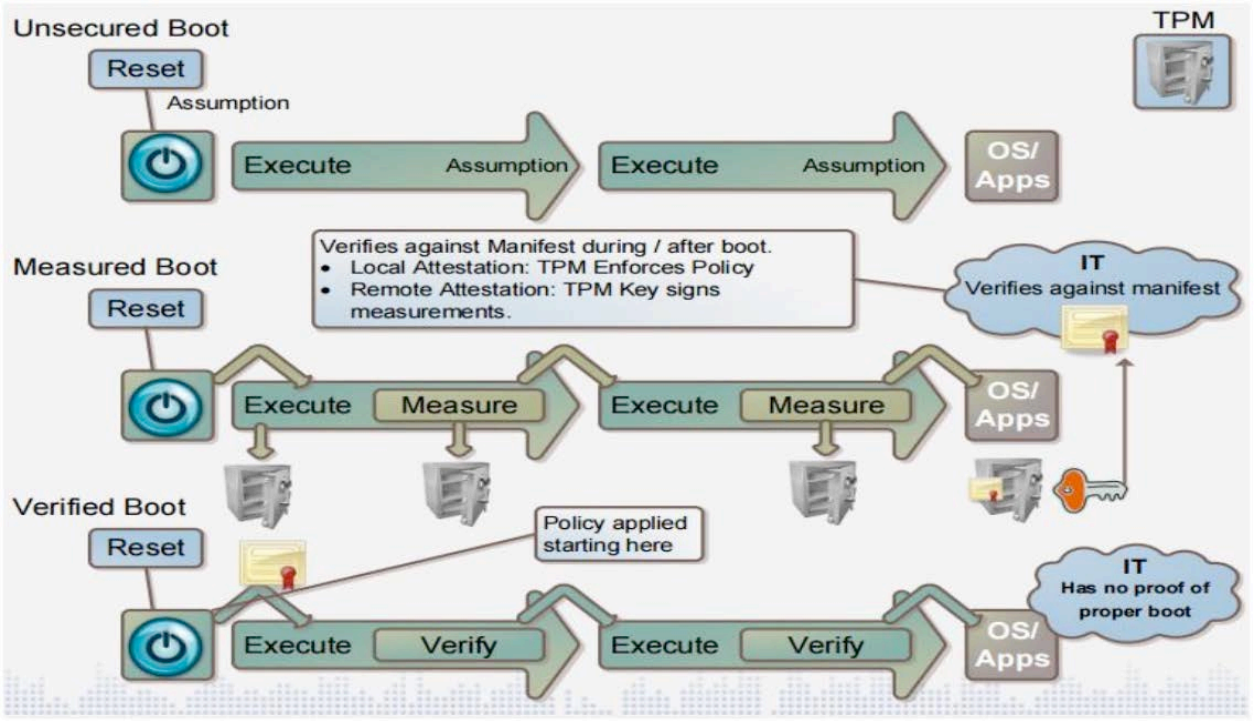
Note:
1. Dual BIOS feature cannot work with BIOS Boot Guard function
2. To update BIOS, it is mandatory to have both BIOS updated first. This is to avoid both BIOS having ME code variations, which could lead to unexpected risk and errors.
3. When the system enters BIOS menu or Option ROM, the system will not reboot automatically.

Warning
DO NOT power off or reset the system during BIOS updating process.

Disclaimer
Under no circumstances will Lanner accept responsibility or liability for damages of any kind whatsoever resulting or arising directly or indirectly from a BIOS update.

APPENDIX C: SILICON ROOT OF TRUST

Security is paramount in the digital age, and the Silicon Root of Trust stands as an unwavering guardian. This concept revolves around the notion of embedding a hardware-based trust anchor into a device's silicon infrastructure. The SRT serves as the cornerstone of security by ensuring the integrity of the device's boot process, key management, and overall security posture.



How Lanner's Silicon Root of Trust Works

Lanner has made significant strides in enhancing security by embedding the Silicon Root of Trust into their products. Here's how this pivotal feature operates:

Boot Process Security:

The security journey begins at the device's boot process, where Lanner's Silicon Root of Trust plays a pivotal role. It verifies the integrity of the firmware, ensuring that it is unaltered and originates from a trusted source.

Chain of Trust:

The Silicon Root of Trust establishes a chain of trust, where each subsequent component in the boot process is verified. This includes the bootloader, the operating system kernel, and other critical components. Any inconsistency or unauthorized alteration halts the boot process, safeguarding the device from potential threats.

Secure Key Management:

Lanner's Silicon Root of Trust often includes secure key management. Cryptographic keys are generated, stored, and managed within the secure enclave. These keys serve a wide range of security functions, such as encryption, authentication, and digital signatures, ensuring data protection and secure communication.

Remote Attestation:

Lanner's SRT can also provide remote attestation capabilities. This involves generating a secure report about the device's configuration and security state. Remote parties can use this report to ensure that the device is in a trusted and secure condition, even in distributed and cloud-based environments.

Hardware-Backed Security:

The hardware-based security of Lanner's Silicon Root of Trust is a crucial asset. It provides robust resilience against software-based attacks and vulnerabilities, guaranteeing the highest level of trustworthiness.

Advantages of Lanner's Silicon Root of Trust

The integration of the Silicon Root of Trust into Lanner's products yields several critical advantages:

Security Assurance: Lanner's SRT establishes trust from the very core, ensuring that every aspect of a device's operation remains secure.

Protection Against Tampering: Unauthorized alterations to the boot process or critical components are thwarted, mitigating risks of cyberattacks.

Confidence in Key Management: Secure key management safeguards cryptographic keys, which are essential for data protection, privacy, and secure communication.

Remote Attestation for Trust: Remote attestation facilitates trust verification in distributed and cloud-based settings, assuring the device's security.

Resilience to Cyber Threats: Hardware-backed security provided by the SRT makes Lanner's products highly resilient to software-based attacks.

APPENDIX D: REDUNDANT POWER MODULE BEHAVIOR

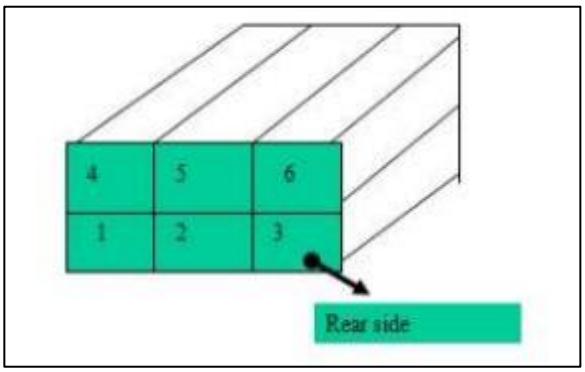
Define the Alarm and Mute behavior

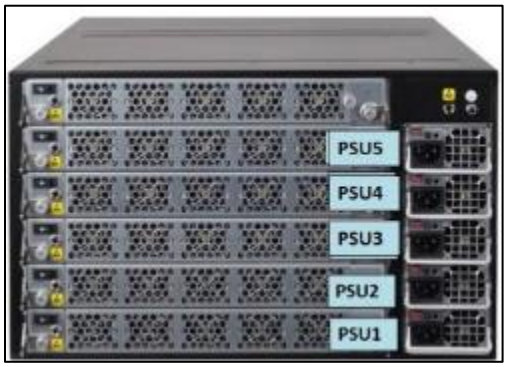
	Power Module Fail	Power Module Remove	Power Cord Remove
Buzzer	**Alarm**	**Alarm**	**Alarm**
Mute	Change back the Good PSU Module or Press the Mute Button	Put back the PSU Module or Press the Mute Button	Plug-in the Power cord or Press the Mute Button

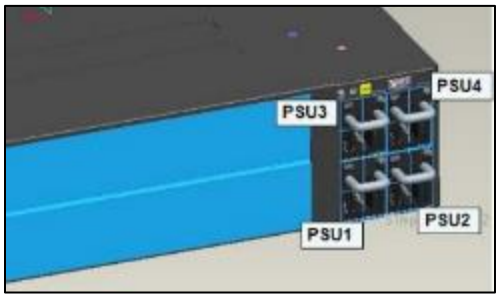
Define the sequence of the Power Module

PSU Sequence	The detection is from the left to the right side , from the bottom to the top side

Example :





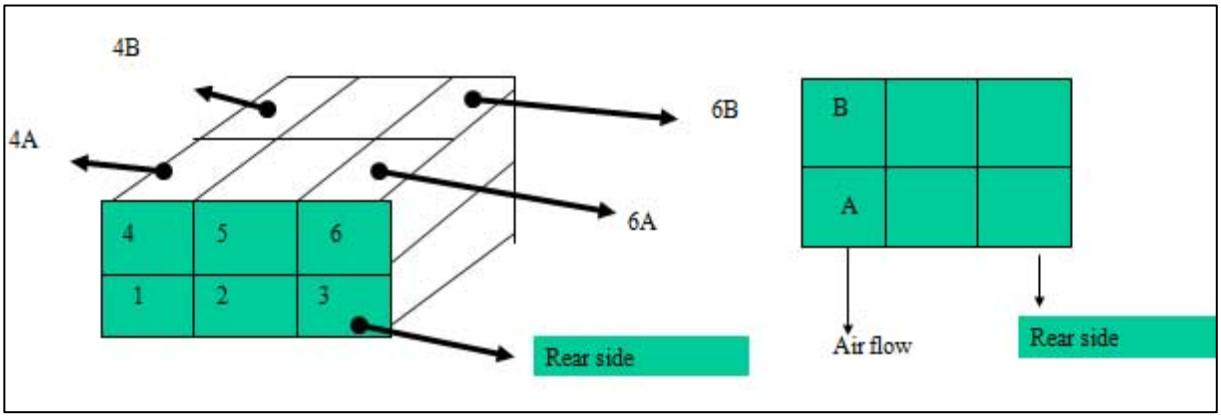


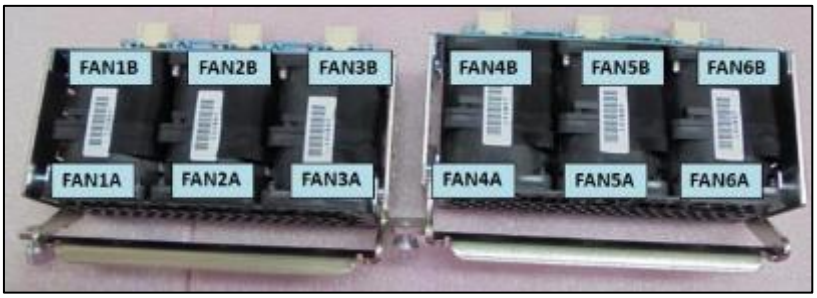
APPENDIX E: FAN SEQUENCE

Define the sequence of the FAN

FAN Sequence	The detection is from the left to the right side , from the bottom to the top side

Example:





APPENDIX F: SMART POWER & RESET BUTTON

Smart Power and Reset Button – Control by CPLD

APPENDIX G: ESD/SURGE ENHANCEMENT

Electrostatic Discharge (ESD): IEC-61000-4-2	Contact discharge	Air discharge	STD
Level 1	±2 kV	±2 kV	
Level 2	±4 kV	±4 kV	4K Contact
Level 3	±6 kV	±8 kV	8K Air
Level 4 (TBD)	±8 kV	±15 kV	New Requirement
			STD
Surge Immunity (LAN) IEC-61000-4-5	Test Level		
Level 0	25V		
Level 1	500V		
Level 2	1kV		V (Current)
Level 3 (TBD)	2kV		New Requirement
Level 4	4kV		
			STD
Electrical Fast Transient (EFT): IEC-61000-4-4			
Level 1	0.5kV		
Level 2	1kV		V (Current)
Level 3 (TBD)	2kV		New Requirement
Level 4	4kV		

APPENDIX H: TERMS AND CONDITIONS

Warranty Policy

1. All products are under warranty against defects in materials and workmanship for a period of one year from the date of purchase.
2. The buyer will bear the return freight charges for goods returned for repair within the warranty period; whereas the manufacturer will bear the after-service freight charges for goods returned to the user.
3. The buyer will pay for repair (for replaced components plus service time) and transportation charges (both ways) for items after the expiration of the warranty period.
4. If the RMA Service Request Form does not meet the stated requirement as listed on "RMA Service, "RMA goods will be returned at customer's expense.
5. The following conditions are excluded from this warranty:
   - Improper or inadequate maintenance by the customer
   - Unauthorized modification, misuse, or reversed engineering of the product
   - Operation outside of the environmental specifications for the product.

RMA Service

Requesting an RMA#

1. To obtain an RMA number, simply fill out and fax the "RMA Request Form" to your supplier.
2. The customer is required to fill out the problem code as listed. If your problem is not among the codes listed, please write the symptom description in the remarks box.
3. Ship the defective unit(s) on freight prepaid terms. Use the original packing materials when possible.
4. Mark the RMA# clearly on the box.

Note: Customer is responsible for shipping damage(s) resulting from inadequate/loose packing of the defective unit(s). All RMA# are valid for 30 days only; RMA goods received after the effective RMA# period will be rejected.

RMA Service Request Form

When requesting RMA service, please fill out the following form. Without this form enclosed, your RMA cannot be processed.

RMA No:	Reasons to Return: ▫ Repair(Please include failure details) ▫ Testing Purpose
Company:	Contact Person:
Phone No.	Purchased Date:
Fax No.:	Applied Date:
Return Shipping Address: _____ Shipping by: ▫ Air Freight ▫ Sea ▫ Express_____ ▫ Others:_____	

Item	Model Name	Serial Number	Configuration

Item	Problem Code	Failure Status

*Problem Code:

01:D.O.A.	07: BIOS Problem	13: SCSI	19: DIO
02: Second Time R.M.A.	08: Keyboard Controller Fail	14: LPT Port	20: Buzzer
	09: Cache RMA Problem	15: PS2	21: Shut Down
03: CMOS Data Lost	10: Memory Socket Bad	16: LAN	22: Panel Fail
04: FDC Fail	11: Hang Up Software	17: COM Port	23: CRT Fail
05: HDC Fail	12: Out Look Damage	18: Watchdog Timer	24: Others (Pls specify)
06: Bad Slot			

Request Party

Authorized Signature / Date

Confirmed By Supplier

Authorized Signature / Date