Cisco 5400 Enterprise Network Compute System Hardware Installation Guide

First Published: 2017-03-02

Last Modified: 2021-11-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using 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.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

Preface

This preface describes the audience, and provides information about how to obtain related documentation.

Audience

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

This guide is intended for Cisco equipment providers and service persons who are technically knowledgeable and familiar with Cisco hardware devices. This guide identifies certain procedures that should be performed only by trained and qualified personnel.

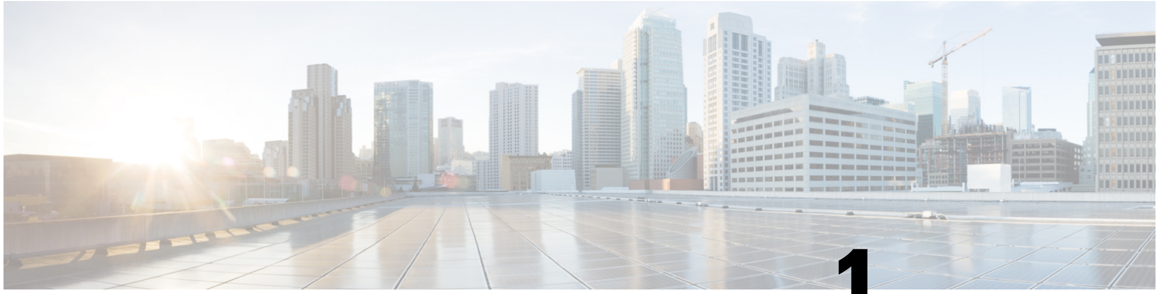
Related Documentation

- Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) Configuration Guide
- API Reference for Cisco Enterprise Network Function Virtualization Infrastructure Software

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

Overview of the Cisco 5400 Enterprise Network Compute System

About the Cisco 5400 Enterprise Network Compute System

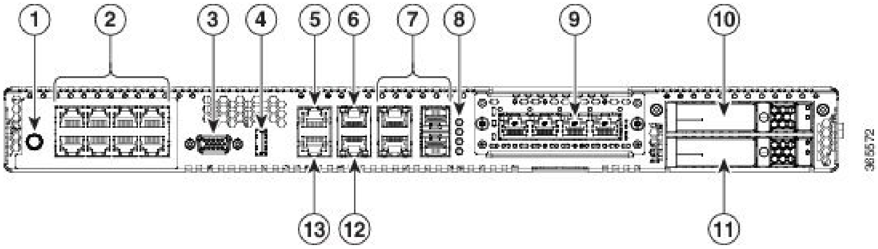
Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

The Cisco 5400 Enterprise Network Compute System (ENCS) combines routing, switching, storage, processing, and a host of other computing and networking activities into a compact one Rack Unit (RU) box. This high-performance unit achieves this goal by providing the infrastructure to deploy virtualized network functions while at the same time acting as a server that addresses processing, workload, and storage challenges.

Cisco 5400 Series Enterprise Network Compute System Chassis

Chassis - Front Panel

Figure 1: Front Panel of the Cisco 5400 ENCS

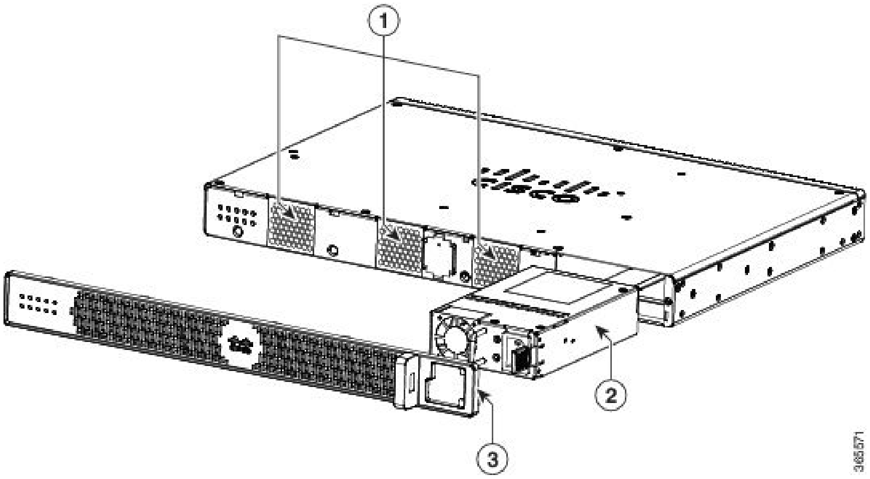


1.	Power on/off switch	2	Integrated LAN ports - optional PoE support is available for some models
3	VGA connector	4	USB port
5	Serial console port for CPU	6	Ethernet management port for CPU
7	Front panel Gigabit Ethernet WAN ports	8	LEDs for front panel Gigabit Ethernet WAN ports
9	Network Interface Module (NIM)	10	Drive bay 0
11	Drive bay 1	12	Ethernet management port for CIMC
13	Serial console port for CIMC		

Note WAN ports must only be used for WAN functions, and LAN ports must only be used for LAN functions. If you require any additional LAN or WAN connectivity with Cisco ISRv or Catalyst 8000v, install the Cisco Network Interface Modules (NIMs).

Chassis - Bezel Side

Figure 2: Bezel View of the Cisco 5400 ENCS



1	Fan vents	2	Modular power supply
3	Removable bezel		

Chassis - Internal View

Figure 3: Internal View of the Cisco 5400 ENCS

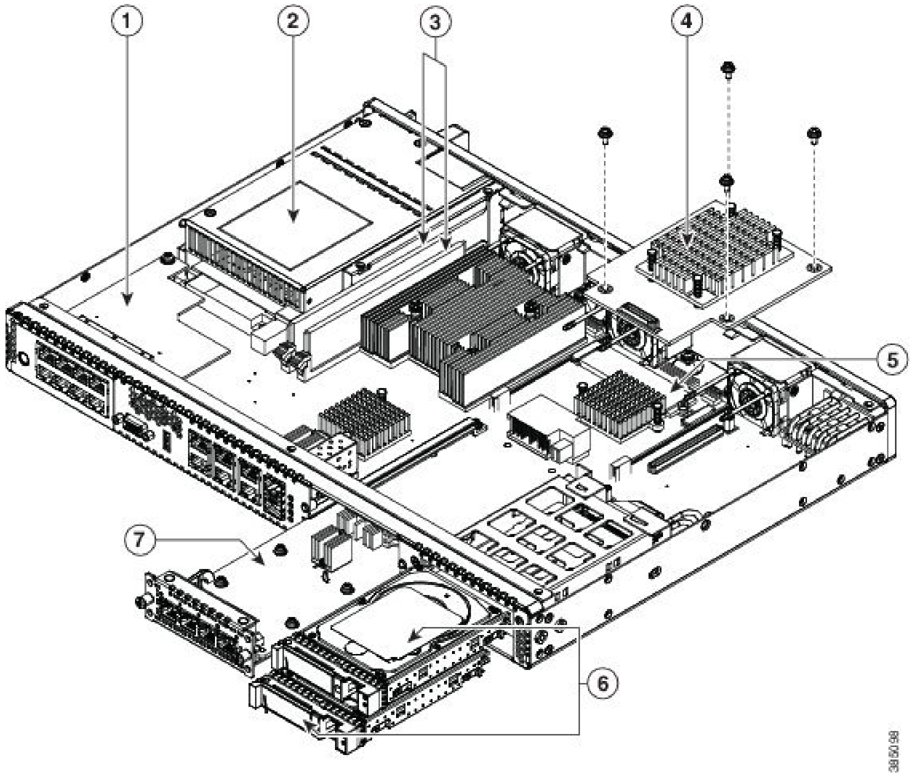


Table 1:

1	PoE daughter card	2	Modular power supply
3	DDR4 DIMM slots on motherboard - 2	4	RAID card
5	M.2 storage module on motherboard	6	Drive bays for hard drives and solid-state drives (SSDs).
7	Network Interface Module		

Safety Warnings

Danger IMPORTANT SAFETY INSTRUCTIONSThis warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071SAVE THESE INSTRUCTIONS

Danger Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

Danger Only trained and **qualified personnel should be allowed** to install, replace, or service this equipment. Statement 1030

Warning Read the installation instructions before you connect the system to its power source. Statement 1004

Warning Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

Warning Installation of the equipment must comply with local and national electrical codes. Statement 1074

Warning To comply with the Class A emissions requirements shielded twisted pair T1/E1 cables must be used for SPA-8-Port Channelized T1/E1 SPA (SPA-8XCHT1/E1) on the router. EN55022/CISPR22 Statement

Warning To comply with Class A emissions requirements- shielded management Ethernet, CON, and AUX cables on the router must be used.

Warning Power cable and AC adapter - When installing the product, please use the provided or designated connection cables/power cables/AC adaptors. Using any other cables or adapters could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of certified cables (that have the 'UL' shown on the code) for any other electrical devices than products designated by Cisco. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have 'PSE' shown on the code) is not limited to Cisco-designated products. Statement 371

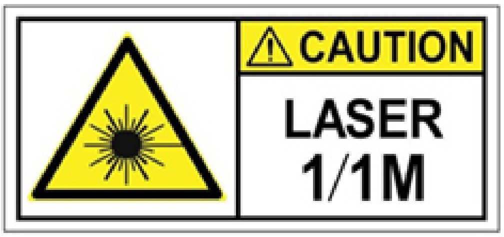
Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: AC power supplies for the Cisco 4451-X ISR. Statement 1005

Warning This unit may have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

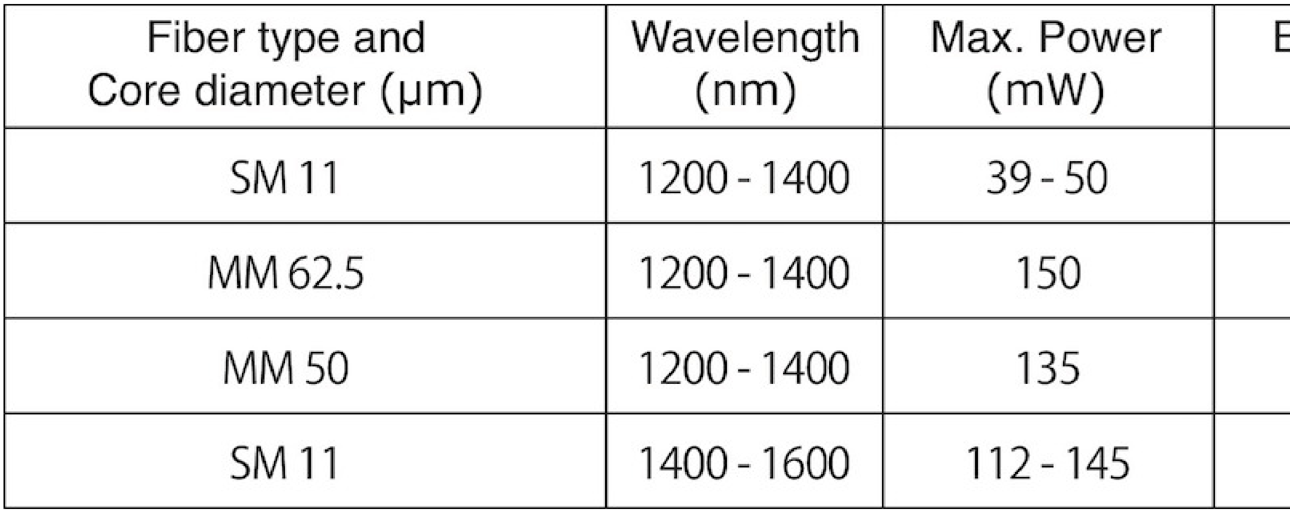
Warning This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

Warning Class 1 LED product. Statement 1027

Warning Class I(CDRH) and Class 1M (IEC) laser products. Statement 1055



Warning Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Statement 1056



Fiber type and Core diameter (µm)	Wavelength (nm)	Max. Power (mW)	E
SM 11	1200 - 1400	39 - 50	
MM 62.5	1200 - 1400	150	
MM 50	1200 - 1400	135	
SM 11	1400 - 1600	112 - 145	

Warning There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Statement 1015

Warning To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40 degrees C. Statement 1047

Warning Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029

Warning This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

Warning Hazardous network voltages are present in WAN ports regardless of whether power to the unit is OFF or ON. To avoid electric shock, use caution when working near WAN ports. When detaching cables, detach the end away from the unit first. Statement 1026

Warning Before opening the unit, disconnect the telephone-network cables to avoid contact with telephone-network voltages. Statement 1041

Warning Do not use this product near water; for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool. Statement 1035

Warning Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations. Statement 1036

Warning No user-serviceable parts inside. Do not open. Statement 1073

Warning Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface. Statement 1037

Warning Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning. Statement 1038

Warning To report a gas leak, do not use a telephone in the vicinity of the leak. Statement 1039

Hardware Features - Standard

- **Integrated LAN ports:** There are eight integrated LAN ports. These ports can provide Power over Ethernet (PoE) if you have purchased a model that supports PoE power supply. These ports must only be used for LAN functions.
- **Integrated WAN ports:** There are 2 to 4 Gigabit Ethernet (GE) WAN ports (dual-mode RJ-45 and SFP). These ports must only be used for WAN functions.
- **USB 3.0 port:** You can use this port to connect a mouse, keyboard, or any other USB device. Using a USB hub, you can connect more than one USB device to this port. Because this port is backward compatible, you can also use an older version of USB devices on this port.

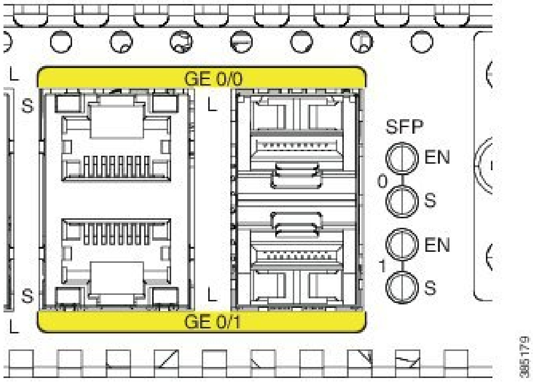
- **VGA connector:** You can use this port to connect a monitor to the device. It supports a display resolution of up to 1600 x 1200 16bpp @ 60Hz.
- **Ethernet management port for CIMC:** Cisco Integrated Management Controller (CIMC) is the component in the device that monitors the health of the entire system.
- **Ethernet management port for CPU:** Use this port to connect to the CPU in your device.
- **Front panel Gigabit Ethernet ports:** This is a set of two dual ports. For each RJ45 port, there is a corresponding fiber optic port. At a given time, the user can use either the RJ45 connection or the corresponding fiber optic port.
- **Serial console port for CPU:** This serial port provides a connection to initially configure the main system's CPU, including the NFVIS software that runs there, using a traditional serial terminal. The terminal should be configured for 9600 8-N-1.
- **Serial Console port for CIMC:** This serial port provides a connection to initially configure the CIMC using a traditional serial terminal. The terminal should be configured for 9600 8-N-1.

Note The speed and duplex configurations are dependent on the peer configuration. If the peer is set at a certain speed and duplex, NFVIS port is set to match that speed. Not all ports on ENCS 5000 series hardware devices support Automatic medium-dependent interface crossover (auto-MDIX) feature. Based on the port connected to the ENCS device, the cable type used to connect to the peer and the speed or duplex settings on the peer, you can try straight through and cross over cable.

LEDs for Gigabit Ethernet WAN Ports

The front panel Gigabit Ethernet WAN ports GE0-0 and GE0-1 (numbered 7 in Figure 1) are a set of two dual ports: for every RJ45 port, there is a corresponding fiber optic port. There are four LEDs for the front panel Gigabit Ethernet ports (numbered 8 in Figure 1). The first two LEDs are for the first set of ports and the last two LEDs are for the second set of ports. If both RJ45 and fiber optic ports are enabled when the system boots, the fiber optic port is used and the RJ45 port is disabled.

Figure 4: LEDs for Gigabit Ethernet WAN Ports



The LEDs labeled **EN** indicates whether the corresponding ports are enabled.

The frequency of the blinks of the LEDs labeled **S** shows the speed of the corresponding ports. This table maps the blink frequency of a LED to the speed of the corresponding port.

Blink Frequency	Speed
No blink	No link
1 blink	10Mbps
2 blinks	100Mbps
3 blinks	1000Mbps

Front Panel LED Status

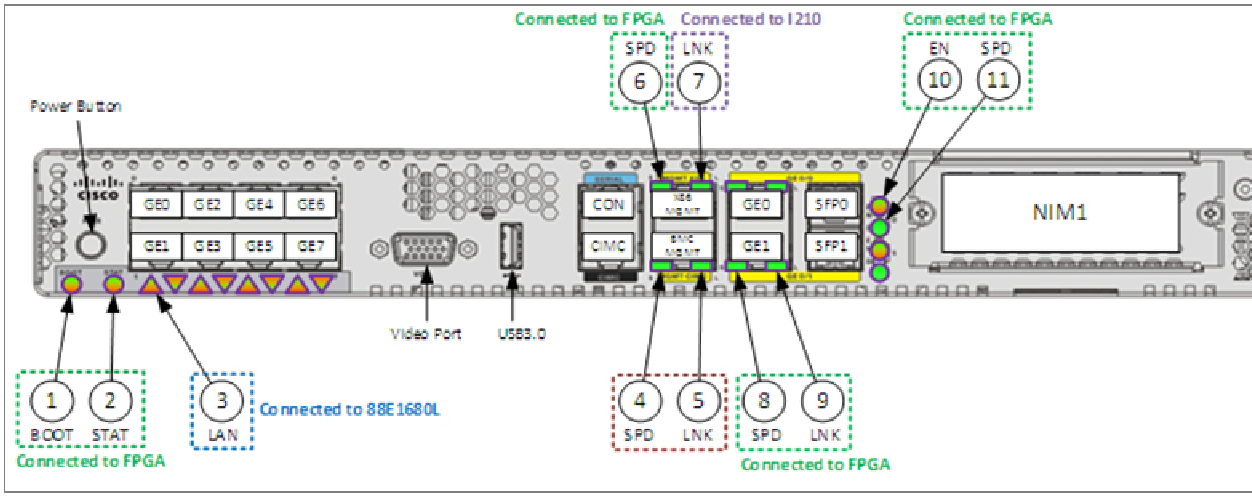


Table 2: Front Panel LED Status

No.	LED Label	Color	Behavior
1	System boot LED	Amber	BMC boot complete, Intel powered down
		Blinking amber	BMC booting, Intel powered down
		Green	BMC boot complete, Intel powered up
		Blinking green	BMC rebooting, Intel powered up
2	System status LED	Amber	A fault is detected in the system.
		Green	Normal system operation.

No.	LED Label	Color	Behavior
3	LAN port	Blinking green	TXD/RXD data.
		Amber	POE fault, implies no link.
4	BMC management port speed LED	Blinking green	Blink frequency indicates port speed: 1 blink - 10 Mbps link speed 2 blink - 100 Mbps link speed 3 blink - 1000 Mbps link speed
5	BMC management port link LED	Green	Ethernet cable present and link established
6	Management port speed LED	Blinking green	Blink frequency indicates port speed: 1 blink - 10 Mbps link speed 2 blink - 100 Mbps link speed 3 blink - 1000 Mbps link speed
7	Management port link LED	Green	Ethernet cable present and link established
8	WAN port speed LED	Blinking green	Blink frequency indicates port speed: 1 blink - 10 Mbps link speed 2 blink - 100 Mbps link speed 3 blink - 1000 Mbps link speed
9	WAN port link LED	Green	Ethernet cable present and link established
10	WAN port SFP enable LED	Green	Indicates SFP module detected
		Amber	Indicates SFP is not detected or at fault

No.	LED Label	Color	Behavior
11	WAN port SFP speed LED	Blinking green	Blink frequency indicates port speed: 3 blink - 1000 Mbps link speed
12	HDD status LED	Green	HDD present
		Blinking green	HDD is in rebuilt state.
		Amber	HDD is in a fault state
		Blinking amber	HDD is in a PFA alert state
13	HDD activity LED	Blinking green	The hard drive is reading or writing data.

Bazel Side LED Status

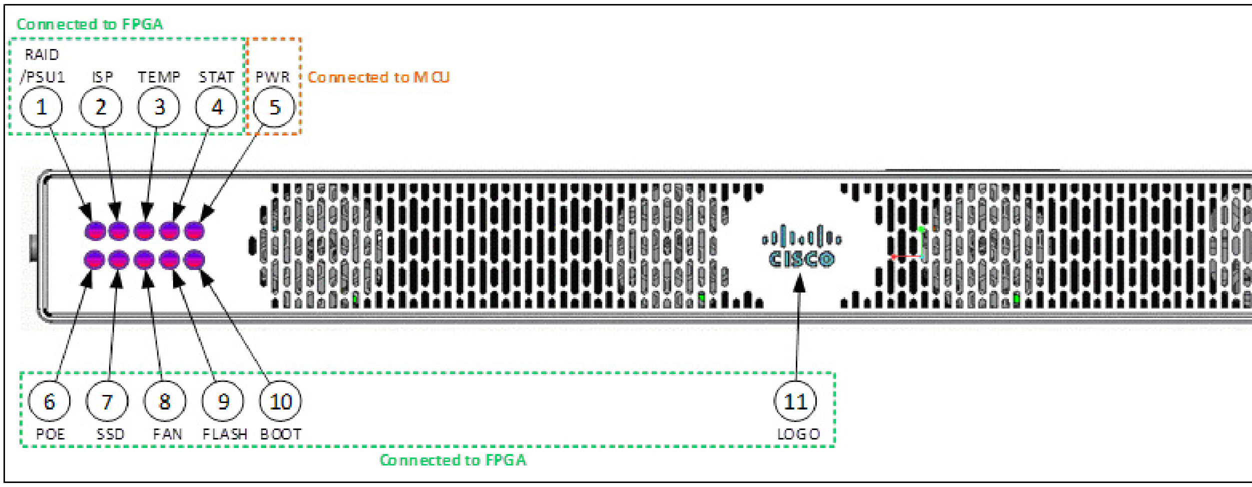


Table 3: Bazel Side LED Status

No.	LED Label	Color	Behavior
1	RAID status	Blue	RAID card is present and working
		Amber	RAID card is present and not operating
2	Integrated services processor status	Blue	Present and functioning
		Amber	Present and not functioning or faulted

No.	LED Label	Color	Behavior
3	Temperature status	Blue	All temperature sensors in the system are working
		Amber	One or two temperature sensors are not working
4	System status	Blue	Normal system operations
		Amber	A fault has been detected in the system.
5	System power	Blue	System power is ok.
		Blinking amber	System is powering up.
6	Power supply with PoE status	Blue	PSU on and providing power.
		Amber	PSU is on but in power failure condition
7	SSD slot status	Blue	Present.
		Amber	Present with failure.
8	Fan status	Blue	All fans are operating.
		Amber	One fan has stopped working.
		Blinking amber	Two or more fans have stopped.
9	eMMC/SD flash status	Blinking blue	Present and currently being used
		Amber	Fault detected
10	eMMC/SD flash status	Blue	BMC boot is complete, intel is powered up
		Blinking Blue	BMC is rebooting, intel is powered up
		Amber	BMC boot is complete, intel powered down.
		Blinking amber	BMC is booting, intel powered down.
11	Cisco logo	Blue	System is powered on.
12	PSU failure	Amber	PSU in failure mode.

Hardware Features - Replaceable and Upgradable Units

The replaceable and upgradable units of the Cisco 5400 ENCS are:

- **Power supply:** The power supply provides AC power. The ENCS5406/K9 device supports only the non-PoE power supply option. This means the LAN ports of this device cannot provide Power over Ethernet (PoE). The ENCS5408/K9 and ENCS5412/K9 devices support both the PoE and non-PoE power supply options. If you want to upgrade from a non-POE power supply to a POE power supply, you can do that by replacing the power supply unit. The reverse is also possible - replacing a POE power supply with a non-POE power supply. The power supply can supply a total of 250 watts of inline power across the 8 PoE capable ports in the system; a maximum of 30 watts of PoE power per port and 60 watts of UPoE power per port.
- **Network Interface Module (NIM):** You can install a NIM in the NIM slot. Similarly when not needed, you can remove the NIM from the NIM module. The device supports only one NIM at a time. The following NIMs are currently supported:

Table 4: Supported NIMs

NIM	Product Module	Minimum Software
LTE	NIM-4G-LTE-VZ	NFVIS 3.6.1 ISRv 16.6.1
	NIM-4G-LTE-ST	
	NIM-4G-LTE-NA	
	NIM-4G-LTE-GA	
	NIM-4G-LTE-LA	
	NIM-LTEA-EA	
	NIM-LTEA-LA	
T1/E1 Data	NIM-1MFT-T1/E1	NFVIS 3.6.1 ISRv 16.6.1
	NIM-2MFT-T1/E1	
	NIM-4MFT-T1/E1	
	NIM-8MFT-T1/E1	
	NIM-1CE1T1-PRI	
	NIM-2CE1T1-PRI	
	NIM-8CE1T1-PRI	
Asynchronous	NIM-16A	NFVIS 3.8.1 ISRv 16.8.1
	NIM-24A	

NIM	Product Module	Minimum Software
T1/E1 Voice	Same as T1/E1 Data PID List	NFVIS 3.9.1 ISRv 16.9.1
DSL	NIM-VA-B	NFVIS 3.9.1 ISRv 16.10.1
	NIM-VAB-A	
	NIM-VAB-M	
GE	NIM-1GE-CU-SFP	NFVIS 3.9.1 ISRv 16.9.1
	NIM-2GE-CU-SFP	

For more information on how to configure the voice module NIMs, refer Configuring the Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module

- **Drive bays:** There are two drive bays. You can choose to use one of them, both of them, or none of them. The types of storage modules that each of these bays can currently hold are:
  - 480GB 2.5" SATA SSD
  - 960GB 2.5" SATA SSD
  - 1TB 2.5" SATA HDD
  - 2TB 2.5" SATA HDD

  Note This list shows the storage modules that are currently supported. More types of storage modules may be supported in the future.

- **M.2 storage module:** This is a high capacity storage component on the motherboard. The OS is installable in this module. The storage capacity of this module is upgradeable. The different storage capacities that are currently available for this module are 64GB, 100GB, 200GB, and 400GB. Other storage capacities might be made available in the future.
- **DDR4 DIMM Slots:** There are two DDR4 dual in-line memory module (DIMM) slots on the motherboard. Each slot can hold 8 GB, 16 GB, or 32 GB memory module. The memory module in each of the slots can be upgraded to a maximum of 32 GB. As a result, you can have a maximum capacity of 64 GB DIMM.
- **RAID Card:** The RAID card improves the performance of the hard drive. The RAID card is installed in the Internal Service Processor (ISP) module of the motherboard.
- **RMA:** Return Material Authorization (RMA) Support allows you to move M.2 SSD, memory, disk drives, RAID card, NIM, and power supply from one system to another system while keeping the configuration and data. This feature is supported of like-to-like systems and the two systems must have the same versions of firmware. In case the two systems do not have the same versions of firmware, you can upgrade the firmware after swapping the hardware components. The following firmware versions are supported in RMA:

Table 5:

	firmware compatible case		**firmware incompatible case**	
	original system	new system	original system	new system
FPGA	1.6	1.6	1.6	1.4
BIOS	2.4	2.4	2.4	1.2
CIMC	3.2.3	3.2.3	3.2.3	3.1.4

Models

The Cisco 5400 ENCS is available in these models:

Product ID	**Description**
ENCS5406/K9	This device has a 6 core CPU. This system does not support a PoE power supply.
ENCS5408/K9	This device has an 8 core CPU.
ENCS5412/K9	This device has a 12 core CPU.

Note With the exception of the CPU capacity and the power supply unit, all other hardware features (standard, replaceable and upgradable) are common across all models.

Table 6: Service Spares

Product ID
ENCS5406P/K9
ENCS5408P/K9
ENCS5412P/K9

Note Service spares are chassis with no memory or disk.

SFP Modules

This section provides information on Cisco Small Form-Factor Pluggable (SFP) Modules in Cisco ENCS 5400. The switch Gigabit Ethernet SFP and SFP+ modules provide copper or optical connections to other devices. These modules are hot-swappable and provide the uplink interfaces. The SFP modules have fiber-optic LC connectors or RJ-45 copper connectors.

Use only supported SFP modules on the switch. Each module has an internal serial EEPROM that is encoded with security information.

Note If non-supported SFP is plugged into the system, you need to reboot the system after removing the non-supported SFP for other SFPs to work normally.

Caution Pluggable optical modules comply with IEC 60825-1 Ed. 3 and 21 CFR 1040.10 and 1040.11 with or without exception for conformance with IEC 60825-1 Ed. 3 as described in Laser Notice No. 56, dated May 8, 2019. Statement 1255

The Cisco ENCS 5400 supports the following SFP modules:

Part Number	Description
GLC-LH-SMD	Cisco 1000BASE-LX/LH SFP module for MMF [1] and SMF, 1300-nm wavelength, commercial operating temperature range.
GLC-SX-MMD	Cisco 1000BASE-SX SFP module for MMF, 850-nm wavelength, extended operating temperature range.
SFP-GE-S	Cisco 1000BASE-SX SFP module for MMF, 850-nm wavelength, extended operating temperature range.

[1] A mode-conditioning patch cord, as specified by the IEEE standard, is required. Using an ordinary patch cord with MMF, 1000BASE-LX/LH SFP transceivers, and a short link distance can cause transceiver saturation, resulting in an elevated bit error rate (BER). When using the LX/LH SFP transceiver with 62.5-micron diameter MMF, you must also install a mode-conditioning patch cord between the SFP transceiver and the MMF cable on both the sending and receiving ends of the link. The mode-conditioning patch cord is required for link distances greater than 984 feet (300 m).

CHAPTER 2

Preparing for Installation

Safety Recommendations and Warnings

Please read the following safety guidelines before you install this product:

- Review the safety warnings listed in Regulatory Compliance and Safety Information for the Cisco 5400 Enterprise Network Compute System before installing, configuring, or maintaining the device.
- Keep the chassis area clean and dust-free during and after installation.
- Keep the chassis in a safe place when you remove the chassis cover.
- Do not wear loose clothing that could get caught in the chassis.
- Wear safety glasses when working under conditions that might be hazardous to your eyes.
- Do not perform any action that creates a hazard to people or makes the equipment unsafe.

Safety with Electricity

Follow these general guidelines when working on equipment that is powered by electricity:

- Locate the emergency power-off switch in the room in which you are working. If an electrical accident occurs, you can quickly turn off the power.
- Disconnect all power before doing the following:
  - Installing or removing a chassis.
  - Working near power supplies.

- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- Do not work alone if hazardous conditions exist.
- Never assume that power is disconnected from a circuit. Always check.
- Never open the enclosure of the internal power supply.
- If an electrical accident occurs, proceed as follows:
    - Turn off power to the device.
    - Call for help.
    - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

Follow these guidelines when working with any equipment that is disconnected from a power source but is still connected to telephone wiring or other network cabling:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for it.
- Never touch uninsulated telephone wires or terminals unless the telephone line is disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Remove power cables from all installed power supplies before opening the chassis.

Always follow these electrostatic discharge (ESD) prevention procedures when removing and replacing modules:

- Ensure that the router chassis is electrically connected to ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.
- If no wrist strap is available, ground yourself by touching a metal part of the chassis.

Caution For the safety of your equipment, periodically check the resistance value of the anti-static strap. It should be between 1 and 10 megohms (Mohm).

Site Requirements

Follow the general precautions listed below when installing or working with your device:

- Keep your system components away from radiators and heat sources.
- Do not block cooling vents.

- Ensure that the chassis cover and module rear panels are secure. All empty network module slots, interface card slots, and power supply bays must have filler panels installed. The chassis is designed to allow cooling air to flow within it, through specially designed cooling slots. A chassis with uncovered openings permits air leaks, which, in turn, may interrupt and reduce the flow of air across internal components.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which can be found by experimenting with different configurations.
- Do not spill food or liquid on any system components and do no operate in a wet environment.
- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components.
- Route system cables, and the power supply cable and plug so that they cannot be stepped on or tripped over. Be sure that nothing else rests on your system component cables or power cable.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local and national wiring rules.
- If you turn off your system, wait at least 30 seconds before turning it on again to avoid system component damage.

Temperature, humidity, altitude, and vibration can affect the performance and reliability of the router. After installation, ensure that the site maintains the environmental characteristics shown in this table:

Environmental Characteristic	**Minimum**	**Maximum**
Steady State Operating	0 degree C	40 degree C (40 degrees C at 10,000 feet)
Storage	-20 degrees C	+70 degrees C
Humidity operating (noncondensing)	10%	90%
Humidity nonoperating (noncondensing)	5%	95%
Altitude operating: over allowable temperature range (0 to 40 degrees C)	-500 feet	10,000 feet
Altitude, nonoperating: over allowable temperature range	-1000 feet	50,000 feet
Thermal shock non-operating with change over time of 3 minute	-25 degrees C	+70 degrees C
Thermal Shock - Operating at 2.5 degree C per minute	0 degrees C	+40 degrees C

Note When an equipment that is installed in a rack (particularly in an enclosed rack) fails, try, if possible, to operate the equipment in isolation. Power off other equipment in the rack (and in adjacent racks) to allow the equipment to be tested in a condition that has maximum cool air and clean power.

Mounting Requirements

The height, width, depth and weight of the chassis are displayed in this table:

Characteristic	Measurement
Height	1.73 inches (4.39 cm) — 1RU rack-mount
Width	17.25 inches (43.815 cm) — 19 inch rack-mount
Depth	13.8 inches (35.052 cm) (including card handles and power supply handles)
Weight	13 lbs. (5.9 kg)

To place the system in a proper location, it is necessary to know the dimensions of the device's chassis.

The Cisco 5400 ENCS can be placed on a desktop or installed in a rack. The mounting ears for the device are designed for #12-24 UNC screws.

The location of your device and the layout of your equipment rack or wiring room are extremely important considerations for proper operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause malfunctions and shutdowns, and can make maintenance difficult. Plan for access to both front and rear panels of the device.

This information can help you plan the rack configuration for your equipment:

- Allow clearance around the rack for maintenance.
- Allow at least one rack unit of vertical space between devices.
- Enclosed racks must have adequate ventilation. Ensure that the rack is not congested, because each device generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air. Heat generated by equipment near the bottom of the rack can be drawn upward into the intake ports of the equipment above it.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated in the rack.

Power Guidelines and Requirements

Check the power at your site to ensure that you are receiving "clean" power (free of spikes and noise). Install a power conditioner if necessary.

The AC power supply supports either 110V or 220V operation. All units include a 6-foot (1.8-meter) electrical power cord. (A label near the power inlet indicates the correct voltage, frequency [AC-powered systems only], current draw, and power dissipation for the unit.)

Network Cabling Specification

- Ethernet cables for RJ45 ports
- Serial or console cables used to connect devices like routers
- Shielded USB cables with properly terminated shields for the USB port
- Standard Shielded Cable with 15-Pin VGA Male Connector

Required Tools and Equipment

You will need the following equipment to install the device and its equipment:

- ESD-preventive cord and wrist strap
- Phillips screwdrivers: small, 3/16-in. (4 to 5 mm), and medium, 1/4-in. (6 to 7 mm)
- Screws that fit your rack
- Wire crimper for chassis grounding - to be used along with the ground lug kit
- One AWG 6 cable for the ground lug kit

Note The ground lug is for chassis grounding and is NEBS compliant.

In addition, depending on the type of modules you plan to use, you might need the following equipment to connect a port to an external network

- Cables for connection to the WAN and LAN ports (dependent on the configuration)

Note If you order the required cables when you purchase the device, the cables ship along with the product.

CHAPTER 3

Installing the Device

Unpacking the Device

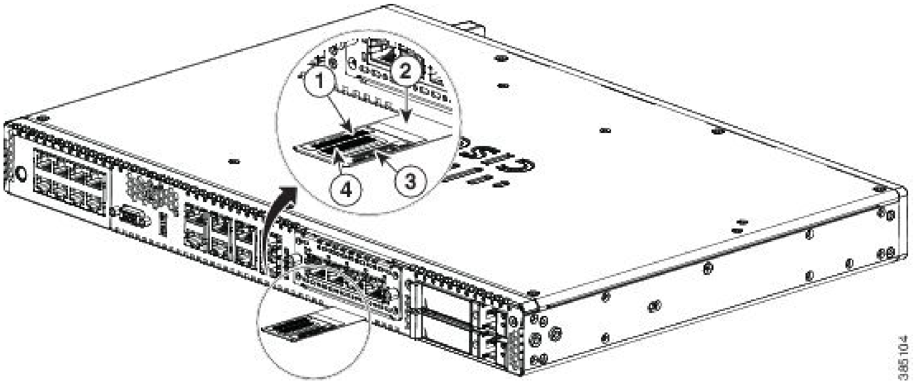
The device, accessory kit, publications, and any optional units may be shipped in more than one container. When you unpack the containers, check the packing list to ensure that you have received all the items on the list.

Only unpack the product when you are ready to install it. This will help prevent accidental damage.

Locating the Product ID, Serial Number, Version ID and Common Language Equipment Identifies (CLEI)

The serial number (SN), product ID (PID), version ID (VID), and Common Language Equipment Identifier (CLEI) are printed on a label on the label tray located on the server chassis or motherboard.

Figure 5: Label Tray



1	Product ID	2	Serial Number
3	PID/VID	4	CLEI

Installing the Cisco 5400 ENCS

If it is not already installed, the DIMMs, M.2 storage module and RAID card must be installed before rack-mounting or wall-mounting the chassis. We recommend that you install the power supply when you have the best access to the back panel of the device; this could be before or after you mount the device. You can install the NIM and HDDs either before or after you mount the chassis.

Rack-Mounting the Chassis

The Cisco 5400 ENCS can be installed in 19-inch (48.26-cm) racks. Use the standard brackets shipped with the router for mounting the chassis in a 19-inch EIA rack.

You can mount the device in the following ways:

- Front mounting—Brackets attached at the front of the chassis with the front panel facing forward
- Back mounting—Brackets attached at the back of the chassis with the back panel facing forward
- Center-front mounting—Brackets attached in the center front of the chassis with the front panel facing forward
- Center-back mounting—Brackets attached in the center back of the chassis with the back panel facing forward

Attaching Brackets to the Chassis

Attach one mounting bracket to each side of the device as shown in Figures 6 and 7. You will need four screws to attach each bracket to the device; so, you will need eight screws in total to attach both the brackets to the device. Use the screws provided along with the mounting kit to attach the screws to the device.

Figure 6: Bracket Installation for Front Mounting

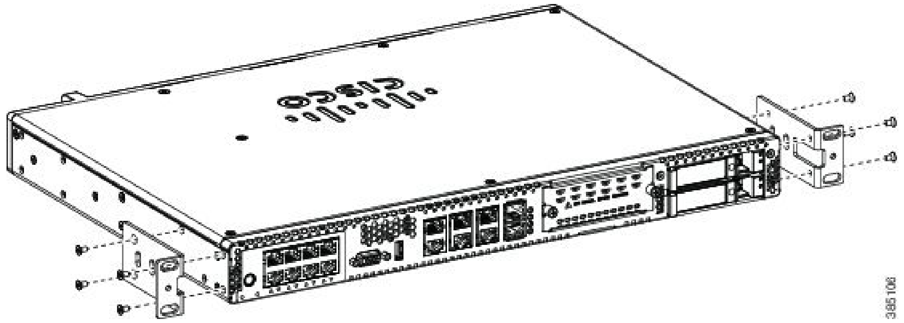
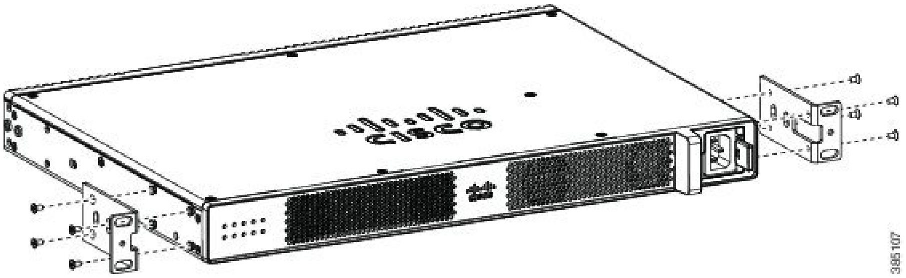


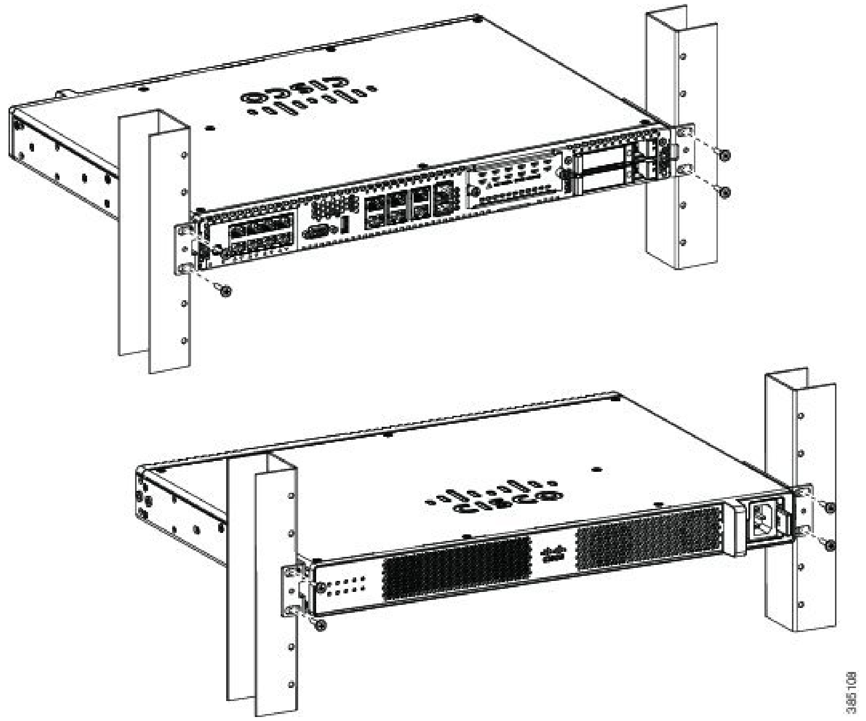
Figure 7: Bracket Installation for Back Mounting



Mounting the device in a Rack

After you attach the brackets to the device, install the chassis on the rack as shown in Figure 8. You will need two screws to attach each bracket to the rack; so, you will need four screws in total to attach the device to the rack. The screws for attaching the device to the rack are not provided with the kit.

Figure 8: Mounting the Chassis on the Rack - Front and Back



Tip The screw slots in the brackets are spaced to line up with every *second* pair of screw holes in the rack. When the correct screw holes are used, the small threaded holes in the brackets line up with unused screw holes in the rack. If the small holes do not line up with the rack holes, you must raise or lower the brackets to the next rack hole.

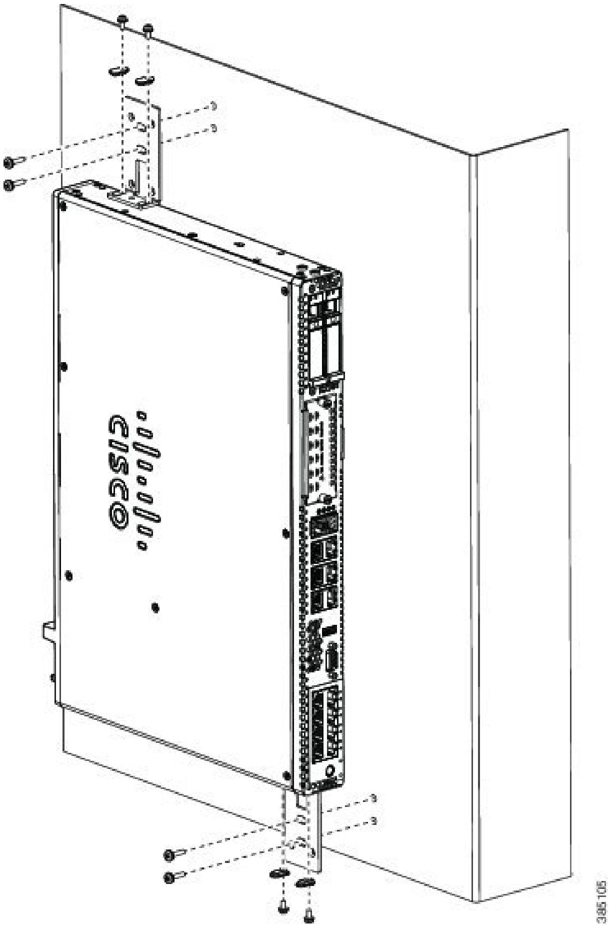
Wall-Mounting the Chassis

These are the steps to wall mount the chassis:

1. Attach the brackets to the device using the screws and plastic spacers provided with the mounting kit. As shown in Figure 9, two screws and two plastic spaces should be used to attach each bracket to the chassis.
2. Fix the router to the wall using the brackets that you attached to the device. The screws for attaching the device to the wall are not provided with the kit. Depending on the type of wall (wood, brick, stone etc), use appropriate screws to fix the device to the wall.

Note Route the cables so that they do not put a strain on the connectors or mounting hardware.

Figure 9: Wall Mounting the Server



Powering On the Server

Note When the power cord is connected to the system, both the management controller (CIMC) and the server is automatically powered on. When the system is powered on, do not press the front-panel power button. If you press the front-panel power button, it will power off the server, but the management controller (CIMC) continues to be operational. You must press this button again to power on the server.

1. Attach the power cord to the power supply unit in the server and then attach the other end of the power chord to the grounded power outlet.
2. Wait for approximately three minutes.
3. Verify the power status of the system by looking at the system power status LED. The power status LED blinks in amber color during initial boot up and in solid amber when the system reaches the standby power mode.

Initial Server Setup

Local Connection Procedure

1. Ensure that the device is powered on.
2. Connect a keyboard and a monitor to the corresponding ports on the front panel of the device.
3. When you see the prompt, you can do the following:
   - Press F2 to get into the setup (BIOS) to change some settings.
   - Press F8 to configure the IP address of the CIMC.
4. After you have performed the required configuration, save the setup and continue to boot.

Remote Connection Procedure

1. Plug in your terminal server to the Serial CIMC port (Refer to Front panel of Chassis)
2. Telnet into the console and perform the necessary configuration using corresponding commands. You can also configure the IP address for the Ethernet CIMC port.

Use CIMC to configure the box. For more details, see Initial Setup for UCS C-Series Servers.

CHAPTER 4

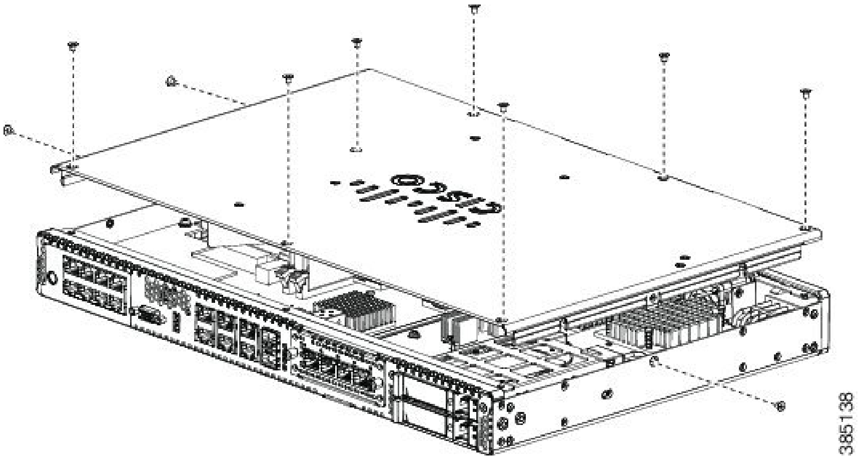
Installing and Upgrading FRUs

Removing and Replacing the Chassis Cover

These are the steps to remove the chassis cover:

1. Confirm the router is turned off and disconnected from the power supply or power supplies.
2. Place the chassis on a flat surface.
3. Remove the screws at top of the chassis cover.
4. Remove the screws at the sides of the device (See Figure 11).
5. Lift the chassis cover once you have removed all the screws.

Figure 10: Removing the Chassis Cover



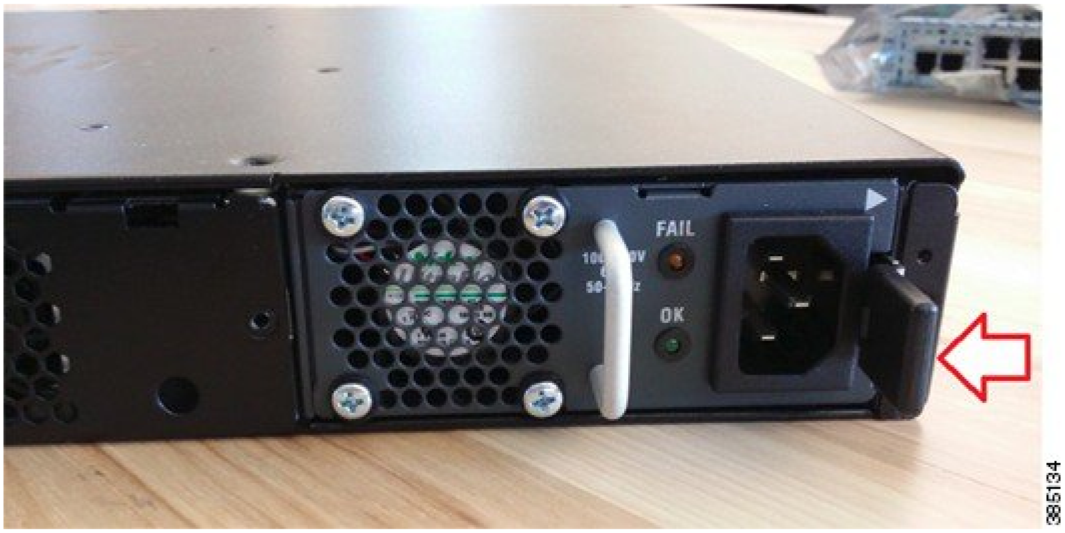
Note To replace the chassis cover, place the cover evenly on the top of the device and use the screws to secure it to the device.

Replacing the Power Supply

These are the steps to replace the power supply:

1. Disconnect the power cord from the power supply.
2. Remove the bezel. The bezel is secured with snap latches. To remove the bezel, hold the top and bottom, and pull the bezel.
3. The latch that secures the power supply to the device is on the right. Press the latch to the left and pull out the power supply using the handle.

Figure 11: Power Supply Latch and Handle



4. Insert the replacement power supply.
5. Replace the bezel.

Installing Drive Bays

There are two drive bays. You can use one of them, both of them, or none. Refer to Hardware Features - Replaceable and Upgradable Units, on page 13 to know the types of storage module that each of this bay can hold. If you had not ordered drives, the slots are closed with a blank cover as shown in the image.

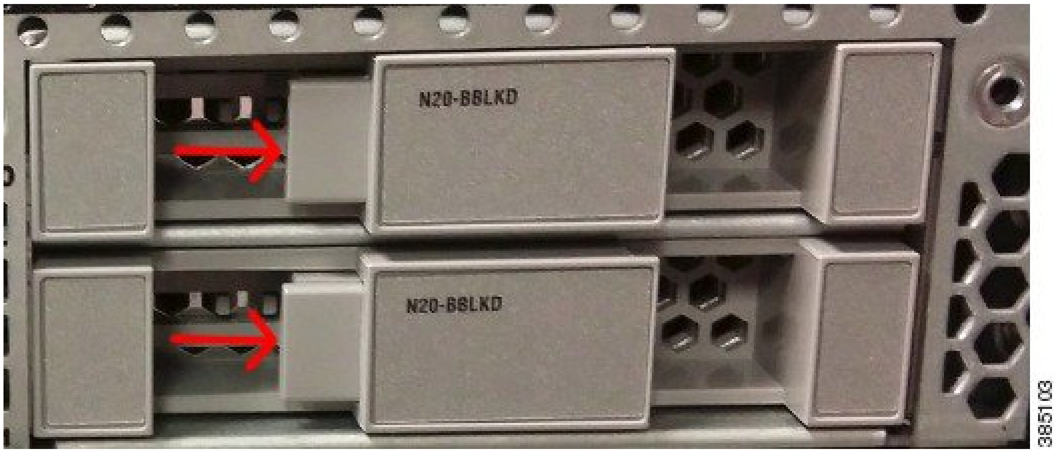
These are the steps to install a drive in a drive bay:

1. The drive bays are in the front panel of the device. The bays are closed with a cover if there are no drives in the slots.

2. Press the push button on the center of the cover and pull the cover out of the system to expose the slot.
3. Slide the drive into the slot.

Note Keep the drive bays covered when there are no drives installed in the slot.

Figure 12: Covers of Hard Disk Drive Slots



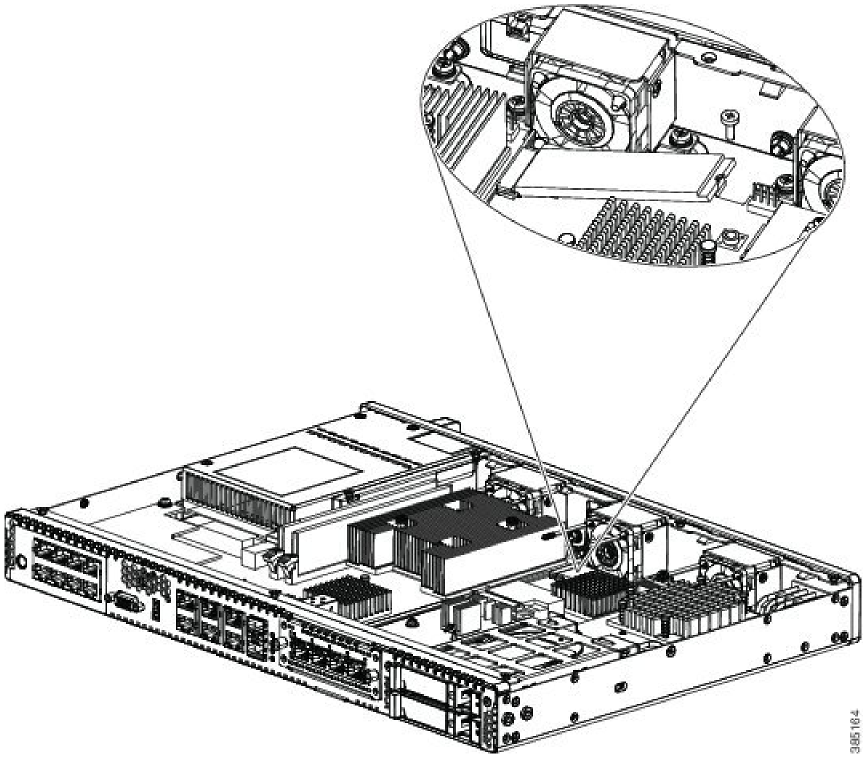
Upgrading the M.2 Storage Module

The M.2 storage module is a hardware that is 22mm wide and 80mm long. This hardware comes with different storage capacities.

These are the steps to upgrade the M.2 memory module:

1. Remove the chassis cover.
2. Locate the M.2 storage module. Refer to the Chassis - Internal View, on page 3 section to identify and locate the module.
3. Remove the old storage module by unscrewing the screw that secures the hardware and removing out the storage module.
4. Plug in the new storage module in the same location and secure it with the screw.

Figure 13: Upgrading the M.2 Storage Module

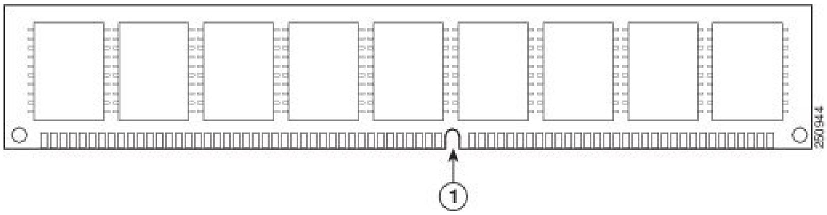


5. Replace the chassis cover.

Installing and Removing a DIMM

There are two DDR4 DIMM slots. DIMMs have a polarization notch on the connecting edge to prevent incorrect insertion.

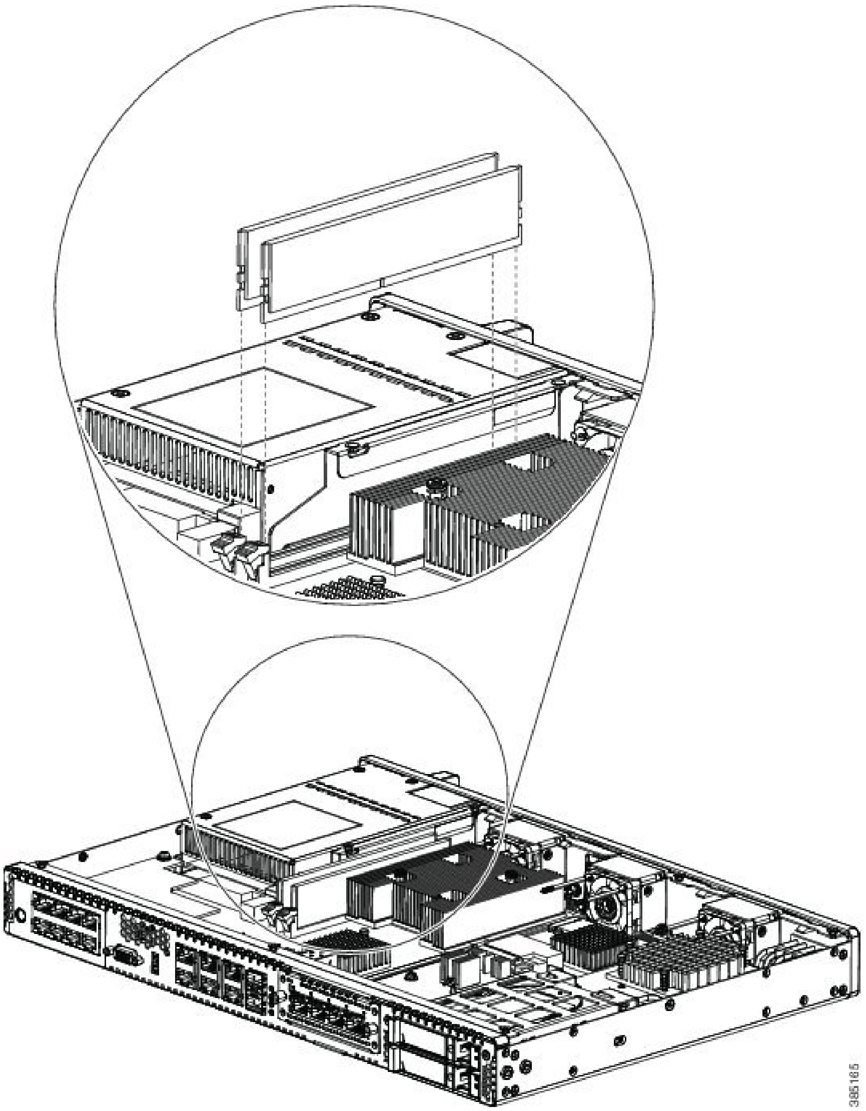
Figure 14: DIMM Showing Polarization Notch



These are the steps to install a DIMM:

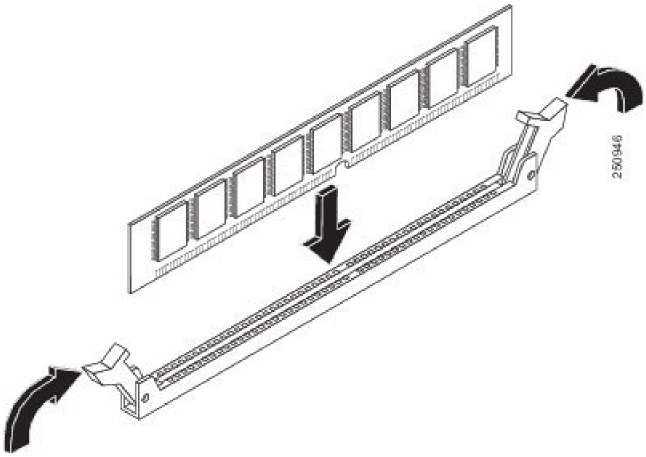
1. Remove the chassis cover.
2. Locate the DIMM module on the device.

Figure 15: DIMM Module



3. Make sure that both latches on the DIMM connector are in the open position.
4. Orient the DIMM so that the polarization notch lines up with the polarization key on the connector.
5. Insert the DIMM into the connector.

Figure 16: Inserting a DIMM

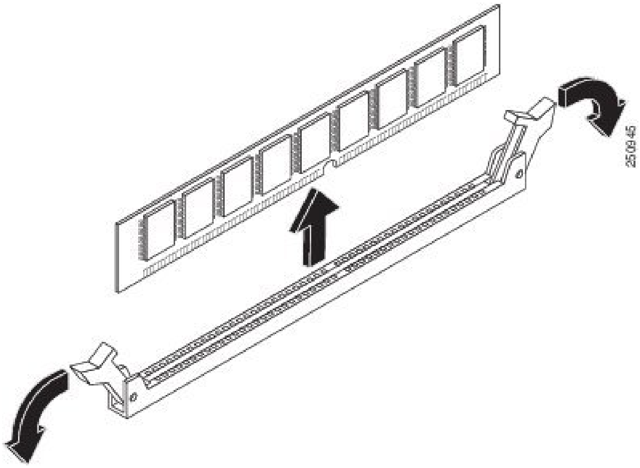


6. Replace the chassis cover.

These are the steps to remove a DIMM:

1. Remove the chassis cover.
2. Locate the DIMM module on the device. Refer to the Chassis - Internal View, on page 3 section to identify and locate the DIMM module.
3. Pull the latches away from the DIMM at both ends to lift the DIMM slightly. Pull the DIMM out of the socket.

Figure 17: Removing a DIMM



4. Place the DIMM in an antistatic bag to protect it from ESD damage.
5. Replace the chassis cover.

Installing and Removing a NIM

These are the steps to install a NIM:

- Locate the NIM slot on the front panel.
- Loosen the screws to open the slot cover.
- Insert the NIM into the slot.
- Tighten the screws to secure the NIM in the slot.

These are the steps to remove a NIM:

- If the NIM is up and running, issue the following command to shut down the NIM gracefully before removing it:

  hw-module subslot slot 0/2 stop

  > **Caution** If you do not shut down the NIM gracefully before removing it, the NIM card could get damaged.

- Locate the NIM slot on the front panel.
- Loosen the screws that secure the NIM.
- Gently pull out the NIM from the slot.

ENCS supports hot swap or OIR (Online Insertion and Removal) for NIM. So, you can insert and remove the NIM when ENCS is running; however, before removing the NIM, ensure that the NIM is shut down gracefully.

Code extract that shows the graceful shutdown of a NIM:

```
CSR-8#hw-module subslot 0/2 stop
Proceed with stop of module? [confirm]
CSR-8#
CSR-8#
CSR-8#sh platform
Chassis type: ISRV

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISRV                ok                    16:41:27
0/2       NIM-4G-LTE-NA       stopped               00:00:05
R0        ISRV                ok, active            16:42:19
F0        ISRV                ok, active            16:42:19
```

CHAPTER 5

Supported RAID Controllers and Required Cables

Table 7:

Controller	Style	Maximum Front-Facing Drives Controlled	RAID Levels	Required Cables	SCPM [1]	Full Disk Encryption
ENCS-MRAID Controller **Note** This controller cannot be ordered with FBWC. [2]	PCIe	SFF drives: 2 internal drives	0, 1, JBOD	Not required	Not Available	Yes [3]

[1] SCPM = SuperCap power module (RAID backup unit).

[2] FBWC: modular flash-based write cache.

[3] When using SED drive.

RAID Cabling

Cisco ENCS-MRAID card does not require additional cable to connect hard drives and RAID card. The flex cable connected to the mainboard can be used to connect to RAID card.

RAID Card LED Indicator

When RAID card is installed, the LED indicator in the front bezel should turn in solid green.

RAID Card Firmware Compatibility

The firmware on the RAID controller must be verified for compatibility with the current Cisco IMC (3.1.5) and BIOS (2.3) versions that are installed on the server. If not compatible, upgrade or downgrade the RAID controller firmware accordingly using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: HUU Guides

ENCS-MRAID Controller Considerations

Stripe-Size Limitation When No Flash-Backed Write Cache is Present

This controller does not have a FBWC, the only stripe size available is 64 KB.

Write-Cache Policy for ENCS-MRAID Controller

This controller does not have SCPM, the default write-cache policy for the ENCS-MRAID controller is *Write Through*.

Support Matrix For ENCS-MRAID Controller

the following table lists the support for the available controllers by server version.

Table 8:

ENCS Version	Boot SSD (Internal M.2) Supported?	ENCS-MRAID Controller Control Front-Facing Drives?
ENCS 5406 ENCS 5408 ENCS 5412	No	Yes

Drive Types and Sizes Supported

- 480GB 2.5" SATA SSD (ENCS-SSD-480G)
- 960GB 2.5" SATA SSD (ENCS-SSD-960G)
- 1TB 2.5" SATA HDD (ENCS-SATA-1T)
- 2TB 2.5" SATA HDD (ENCS-SATA-2T)
- 1.2TB SAS HDD (ENCS-SAS-12T)
- 1.8TB SAS HDD (ENCS-SAS-18T)
- 1.2TB SED SAS HDD (ENCS-SED-12T)

ENCS-MRAID Drive and Predictive Failure Behavior

- Good drive handling:
  - The physical drive is marked GOOD in the GUI/CLI interfaces and fault LED on the drive is off.
  - The virtual drive (RAID volume group) is marked GOOD in GUI/CLI interface. There is no LED for this.
- Bad/invalid/0MB drive handling:
  - The bad drive is marked BAD in the GUI/CLI interfaces and the fault LED on the drive is solid amber.
- Drive predictive failure:
  - If the drive is part of a RAID volume with a spare, the software performs an auto-copy backup and then marks the drive failed/BAD with the fault LED on the drive solid amber.

Setting the Preferred Boot Device Order for ENCS-MRAID

The default boot device is internal SSD, disks connected to RAID card are only used as external datastores for VM images.

Refer to BIOS Boot order procedures to select the right boot device and make order of RAID adapter as low as possible.

Mixing Drive Types in RAID Groups

The following table lists the technical capabilities for mixing hard disk drive (HDD) and solid state drive (SSD) types in a RAID group. However, see the recommendations that follow for the best performance.

Table 9: Drive Type Mixing

Mix of Drive Types in RAID Group	JBOD	RAID-1	RAID-0 (not in 3.6.1)
SATA HDD + SATA HDD	Yes	Yes	Yes
SATA SSD + SATA SSD	Yes	Yes	Yes
SAS HDD + SAS HDD	Yes	Yes	Yes
SAS SED HDD + SAS SED HDD	Yes [1]	Yes [1]	Yes [1]
SAS HDD + SATA HDD	Yes	Yes	Yes
SAS HDD + SAS SED HDD	Yes	Yes [2]	Yes [2]
HDD + SSD	Yes	No	No

[1] With or without encryption enabled.

[2] Virtual disk encryption cannot be enabled.

Mixing Drive Types in RAID Groups

For the best performance, follow these guidelines:

- Use either all SAS or all SATA drives in a RAID group.
- Use the same capacity for each drive in the RAID group.
- Never mix HDDs and SSDs in the same RAID group.
- Never mix SAS and SED SAS.

Disks Replacement Considerations

For the best compatibility with NFVIS, follow these guidelines:

- When replace a faulty unit, make sure the replacement unit does not have existing partitions.
- Do not swap the drives between Slot-0 and Slot-1.
- Do not swap or replace drives used by other ENCS system without reformatting it beforehand.
- OIR (Online Insertion/ Removal) is not supported in ENCS system.
- Do not attempt to swap or replace drives used by other ENCS systems.

RAID Backup Units

ENCS-MRAID does not support RAID backup units.

Installing ENCS-MRAID Drivers for NFVIS

NFVIS 3.6.1 already includes the required drivers and there is no need to install additional driver for this RAID controller.

RAID Configuration

RAID configuration is done through CIMC Web GUI unless specified otherwise. Though ENCS-MRAID controller can support multiple RAID modes, the physical limitation of ENCS chassis (two physical drives) restrict ENCS-MRAID controller only supporting JBOD and RAID-1 modes under NFVIS 3.6.1.

JBOD Mode

When a brand new drive is inserted, the drive's status is either **Unconfigured Good** or **JBOD**. If drive is in **Unconfigured Good** status, use the following steps to enable JBOD mode:

Procedure

	Command or Action	Purpose
Step 1	Log into CIMC.	
Step 2	choose **Storage** tab on the left pane.	
Step 3	Choose **Physical Drive Info** tab in middle pane.	
Step 4	Highlight the drive which is in **Unconfigured Good** status.	
Step 5	Click **Set State as JBOD** in the **Actions** field.	
Step 6	Reboot NFVIS to use the new installed drive.	

For existing ENCS with external drives inserted but no RAID card installed, the drives will be set to JBOD mode without further configuration after RAID card installed..

RAID-1 Mode

After both drives are in **Unconfigured Good** state, use the following steps to create virtual disk (under WebGUI):

Before you begin

To enable RAID-1 virtual disk on ENCS, refer to **Mixing Drives Types in RAID Groups** for hard drive compatibility and best practice for performance. Before creating virtual disk, both drives must be in **Unconfigured Good** status. If drive is on other status, use CIMC Web GUI/CLI and do the following:

- If disk is in JBOD state: go to **Storage** tab > **Physical Drive Info** tab, choose **Set State as Unconfigured Good** link for this drive.
- If disk is in **Foreign Config** state, go to **Storage** tab > **Controller Info** tab, choose **Clear Foreign Config** in **Action** field.

Procedure

	Command or Action	Purpose
Step 1	Click on **Storage** tab in left-pane.	
Step 2	Click on **Controller Info** tab in mid-pane.	
Step 3	Click on **Create Virtual Drive** from **Unused Physical Drives** in **Action** field. Wait for a new pop-up window to open.	
Step 4	In the **Create Virtual Drive** from **Unused Physical Drives** pop-up, choose the following: • **RAID Level**: 1 • **Enable Full Disk Encryption**: un-checked • **Create Drive Groups**: select the physical drives, and click >> to add both disks into Drive Groups. • Fill the following **Virtual Drive Properties** and click **Create Virtual Drive** button: • **Virtual Drive Name**: RAID1_12 (auto-assign by GUI) • **Strip Size**: 64k (default) • **Write Policy**: Write Through (default) • **Access Policy**: Read Write (default) • **Read Policy**: No Read Ahead (default) • **Cache Policy**: Direct IO (default) • **Disk Cache Policy**: Unchanged (default) • **Size**: xxxxxxx (auto-filled by GUI)	
Step 5	Click on **Virtual Drive Info** tab in mid-pane to verify virtual drive is in **Optimal** state and health is **Good**.	

Secured RAID Group Configuration

ENCS-MRAID controller support Full Disk Encryption (FDE) feature in hardware level when using supported Self-Encryption Drive (SED). To use secured RAID group feature, first you must enable security on RAID controller before you enable security on drives. Use CIMC CLI to enable security with following steps:

SUMMARY STEPS

1. Log into CIMC.
2. Under CIMC CLI shell, issues the following CLI:
3. Verify that controller's security is enabled.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Log into CIMC.	

Step 2	Under CIMC CLI shell, issues the following CLI:	`ENCS5408-FGL210310KJ#`
		`ENCS5408-FGL210310KJ# scope chassis`
		`ENCS5408-FGL210310KJ /chassis # scope`
		`storageadapter SLOT-5`
		`ENCS5408-FGL210310KJ /chassis/storageadapter #`
		`ENCS5408-FGL210310KJ /chassis/storageadapter #`
		`ENCS5408-FGL210310KJ /chassis/storageadapter #`
		`enable-controller-security`
		`Use generated key-id 'UCSC-MRAIDC460__21313526'?`
		` (y or n)--> y`
		`Use suggested security-key`
		`'i7mbSmYjqbXicAFOOb44yeKCGLldoFlB'?  (y or n)-->`
		`y`
		`ENCS5408-FGL210310KJ /chassis/storageadapter #`

Step 3	Verify that controller's security is enabled.	`ENCS5408-FGL210310KJ /chassis/storageadapter # show`
		` detail`
		`PCI Slot SLOT-5:`
		`    Health: Good`
		`    Controller Status: Optimal`
		`    ROC Temperature: 60 degrees C`
		`    Product Name: MegaRAID SAS 3108 R`
		`    Serial Number:`
		`    Firmware Package Build: 24.12.1-0039`
		`    Product ID: LSI Logic`
		`    Battery Status: BBU Not Supported`
		`    NVRAM Size: 32 KB`
		`    Memory Size: 0 MB`
		`    Flash Memory Size: 16 MB`
		`    Cache Memory Size: 0 MB`
		`    Boot Drive: 0`
		`    Boot Drive is PD: false`
		`    TTY Log Status: Not Downloaded`
		`    Controller is Secured: 1`

JBOD Secured Mode

When controller security feature is enabled, we can verify and configure SED drive. To verify drive is security (FDE) capable, use the following:

- From CIMC web GUI, go to **Storage tab** > **Physical Drive Info** tab, select the drive, check **General field** in the mid-pane, you should see **Security Capable: Yes**.
- From CIMC CLI, issue the following CLI:

```
ENCS5408-FGL210310KJ /chassis/storageadapter # show physical-drive 1 detail
Physical Drive Number 1:
    Controller: SLOT-5
    Health: Good
    Status: JBOD
    Boot Drive: false
    Manufacturer: HGST
    Model: HUC101812CSS205
    Predictive Failure Count: 0
    Drive Firmware: D703
    Coerced Size: 1143455 MB
    Type: HDD
    Block Size: 512
    Link Speed: 12.0 Gb/s
    Locator LED: false
    FDE Capable: 1
    FDE Enabled: 0
    FDE Secured: 0
    FDE Locked: 0
FDE Locked Foreign Config: 0
```

To enable FDE feature, do the following:

1. From CIMC web GUI, go to **Storage tab** > **Physical Drive Info** tab, select the drive, check **General field** in the mid-pane, click on **Enable Secure Drive** from **Actions** field.
2. To verify, similar action is taken
    - From CIMC Web, check **Security Enabled: Yes** string.
    - From CIMC CLI, check the following:

```
ENCS5408-FGL210310KJ /chassis/storageadapter # show physical-drive 1 detail
Physical Drive Number 1:
    Controller: SLOT-5
    Health: Good
    Status: JBOD
    Boot Drive: false
    Manufacturer: HGST
    Model: HUC101812CSS205
    Predictive Failure Count: 0
    Drive Firmware: D703
    Coerced Size: 1143455 MB
    Type: HDD
    Block Size: 512
    Link Speed: 12.0 Gb/s
    Locator LED: false
    FDE Capable: 1
    FDE Enabled: 1
    FDE Secured: 1
FDE Locked: 0
FDE Locked Foreign Config: 0
```

RAID-1 Secured Mode

To enable FDE on RAID-1 virtual disk, the steps are similar to previous RAID-1 virtual disk creation, the only difference is on Step 4 when **Create Virtual Drive** from **Unused Physical Drives** pop-up appeares, check **Enable Full Disk Encryption** option to enable FDE on virtual disk level.

Component Replacement Consideration

Unlike the security-disabled configuration, different controller has different encryption key, please advise your system administrator with the following conditions:

- Replacing ENCS-MRAID controller will render FDE-enabled disks data un-retrievable on same host.
- FDE-enabled disks cannot be swapped between systems.
- FDE-enabled disks can be re-used by clear its foreign config and set its state to **Unconfigured Good**.

RAID Disk Group Rebuild

RAID-1 Disk Group is the only mode can be rebuilt under ENCS-MRAID controller. To rebuild the disk group, you must provide the disk with same type, equal or larger size than virtual disk.

For More Information

The LSI utilities have help documentation for more information about using the utilities.

For basic information about RAID and for using the utilities for the RAID controller cards that are supported in Cisco servers, see the Cisco UCS Servers RAID Guide.

Full Avago Technologies/LSI documentation is also available:

- • For hardware SAS MegaRAID - Avago Technologies/LSI 12 Gb/s MegaRAID SAS Software User’s Guide, Rev. F
- • For embedded software MegaRAID - LSI Embedded MegaRAID Software User Guide