Cisco Threat Grid M5 Hardware Installation Guide

First Published: 2019-12-20

Last Modified: 2021-07-16

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 SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

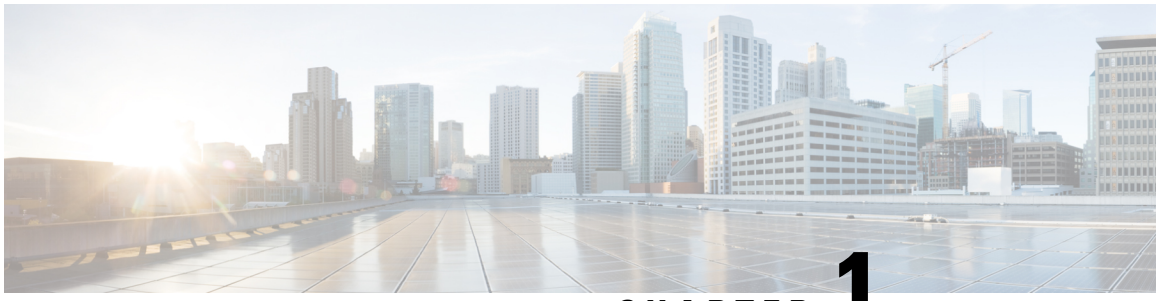
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019-2021 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Overview

Features

A Cisco Threat Grid appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. Threat Grid Appliances provide the complete Threat Grid malware analysis platform, installed on a single UCS server.

Many organizations that handle sensitive data, such as banks, health services, etc., must follow various regulatory rules and guidelines that will not allow certain types of files, such as malware artifacts, to be sent outside of the network for malware analysis. By maintaining a Cisco Threat Grid Appliance on-premises, organizations are able to send suspicious documents and files to it to be analyzed without leaving the network.

The Cisco Threat Grid M5 appliance supports Threat Grid Version 3.5.27 and later, and appliance version 2.7.2 and later.

See Product ID Numbers, on page 12 for a list of the field-replaceable product IDs (PIDs) associated with the Threat Grid M5 appliance. You can remove and replace drives and power supplies. For all other internal component failures, you must send your chassis for return material authorization (RMA).

The following table lists the features of the Threat Grid M5.

Table 1: Threat Grid M5 Features

Feature	Description
Form factor	1 RU

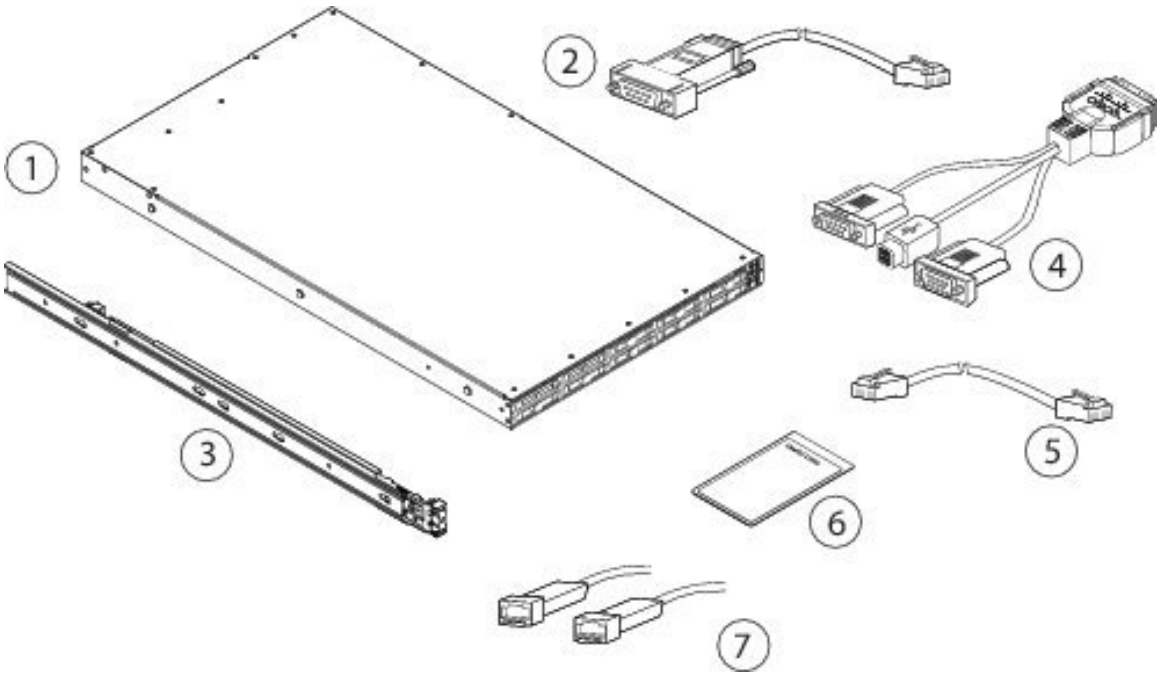
Feature	Description
Rack mount	Standard 19-inch (48.3 cm) 4-post EIA rack
Airflow	Front to rear Cold aisle to hot aisle
Pullout asset card	Displays the serial number
Grounding hole	Two threaded holes for dual-hole grounding lug Use is optional; the supported AC power supplies have internal grounding, so no additional chassis grounding is required.
Unit identification button	Yes
Power button	On front panel
Processor	Before January 2021: Two Intel Xeon 6140 After January 2021: Two Intel Xeon 6262
Memory	16 x 32 GB RAM Internal component only; not field-replaceable
RDIMMs	Before January 2021: Two 16-GB DDR4-2400-MHz RDIMMs After January 2021: Two 16-GB DDR4-2933-MHz RDIMMs Internal component only; not field-replaceable
Management ports	1 Gb built-in
Network ports	Two 1-Gb 1000Base-T Two 10-Gb SFP+
USB ports	Two Version 3.0 Type A
VGA port	One 3-row 15-pin DB-15 connector Enabled by default
SFP ports	Four fixed SFP+ ports The two left SFP+ ports are not supported.
Supported SFP+	SFP-10G-LR (10 Gb) SFP-10G-SR (10 Gb) **Note** Only these two SFPs have been qualified for use on the Threat Grid M5. Although other SFPs may work, we only support these two on the Threat Grid M5.
Serial console port	RJ45 serial port running RS-232 (RS-232D TIA-561)

Feature	Description
System power	Two 770-W AC power supplies Hot-swappable and redundant as 1+1
Power consumption	2626 BTU/hr
Fans	Six fans for front-to-rear cooling Internal component only; not field-replaceable
Storage	Two 240-GB SATA SSDs in slots 1 and 2 Six 2.4-TB SAS HDDs in slots 3 though 8 RAID 1, hot-swappable

Package Contents

The following figure shows the package contents for the Threat Grid M5. Note that the contents are subject to change and your exact contents might contain additional or fewer items.

Figure 1: Threat Grid M5 Package Contents



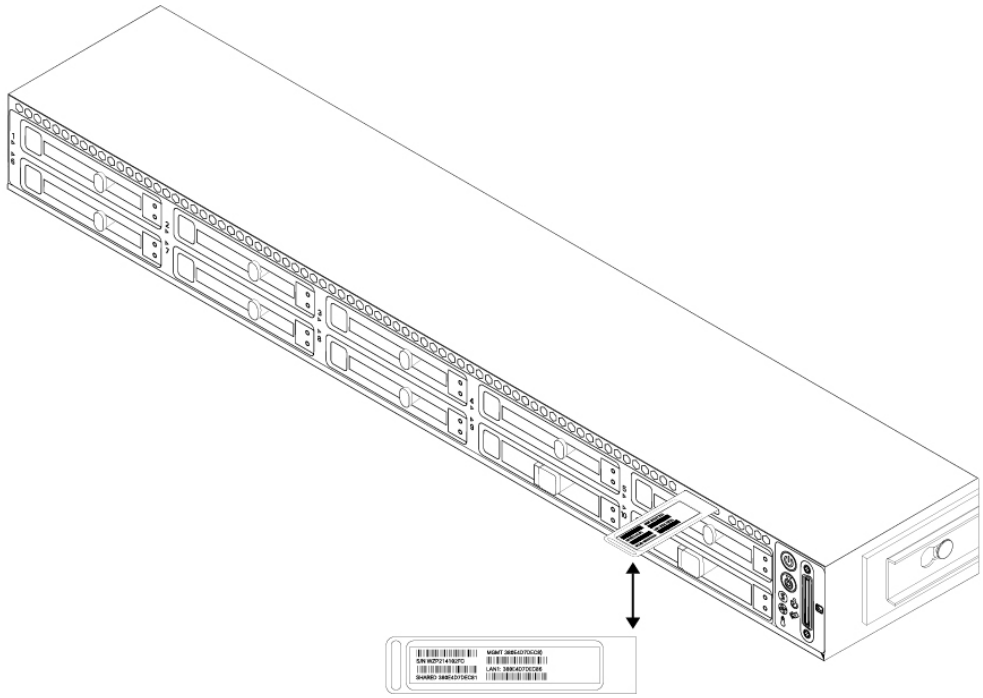
1	Chassis	**2**	RJ-45 to DP9-RS232 console cable (Cisco part number 72-3383-XX)
3	Cisco 1-RU rail kit (Cisco part number 800-43376-02)	**4**	USB dongle cable (Cisco part number 37-1016-xx)

5	RJ-45 to RJ-45 Cat 5 Ethernet cable, yellow six feet long (Cisco part number 72-1482-XX)	**6**	*Useful Links Cisco Threat Grid M5* The steps in the Useful Links document send you to the documentation you need to install, set up, and configure your Threat Grid M5.
7	Two 10-Gb transceivers with cables		

Serial Number Location

The serial number (SN) for the Threat Grid M5 is printed on the pullout asset card located on the front panel as shown in the following figure.

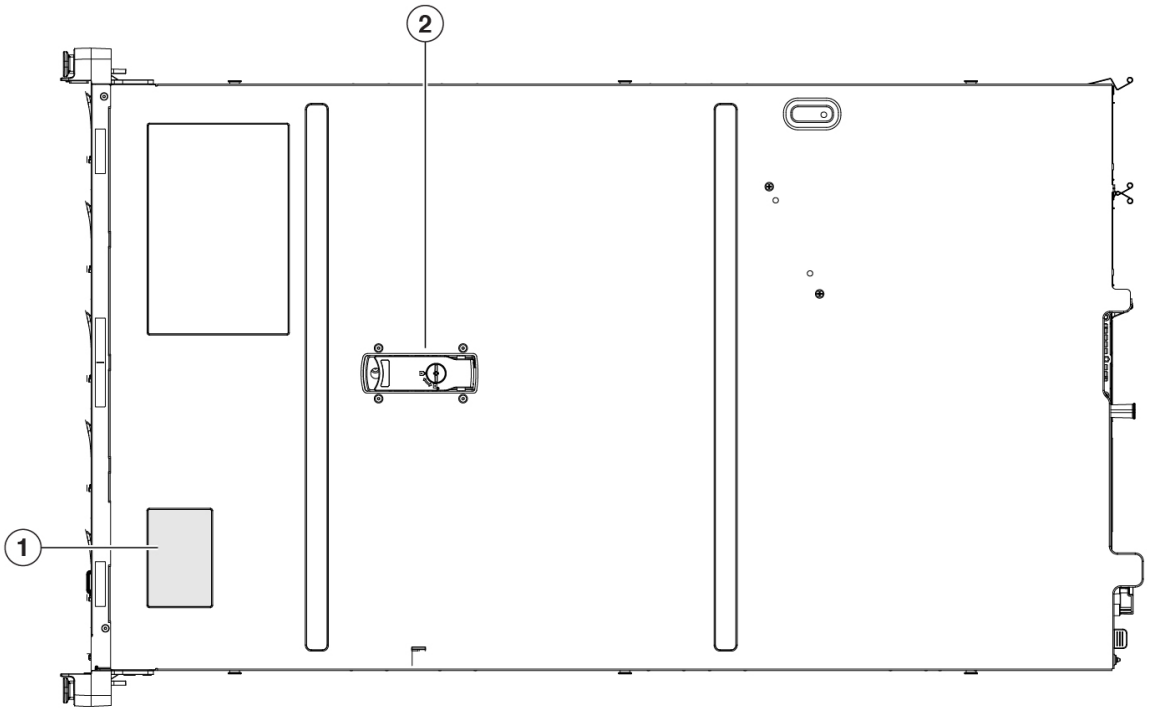
Figure 2: Serial Number on Pullout Asset Card



The serial number is also on the label on the cover of the chassis as shown in the following figure.

Caution The cover latch on the top of the chassis cover is not supported. There are no internal field-replaceable parts in the Threat Grid M5.

Figure 3: Serial Number Location on Cover

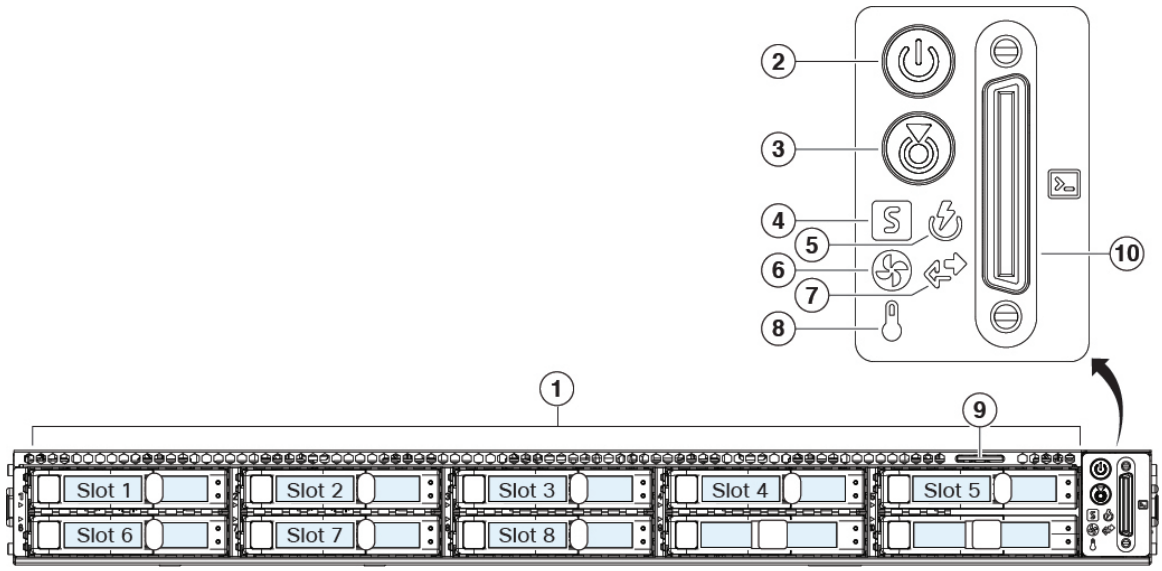


1	Serial number label	**2**	Cover latch Not supported

Front Panel

The following figure shows the front panel features and disk-drive configuration for the Threat Grid M5. See Front Panel LEDs, on page 6 for a description of the LEDs.

Figure 4: Threat Grid M5 Front Panel

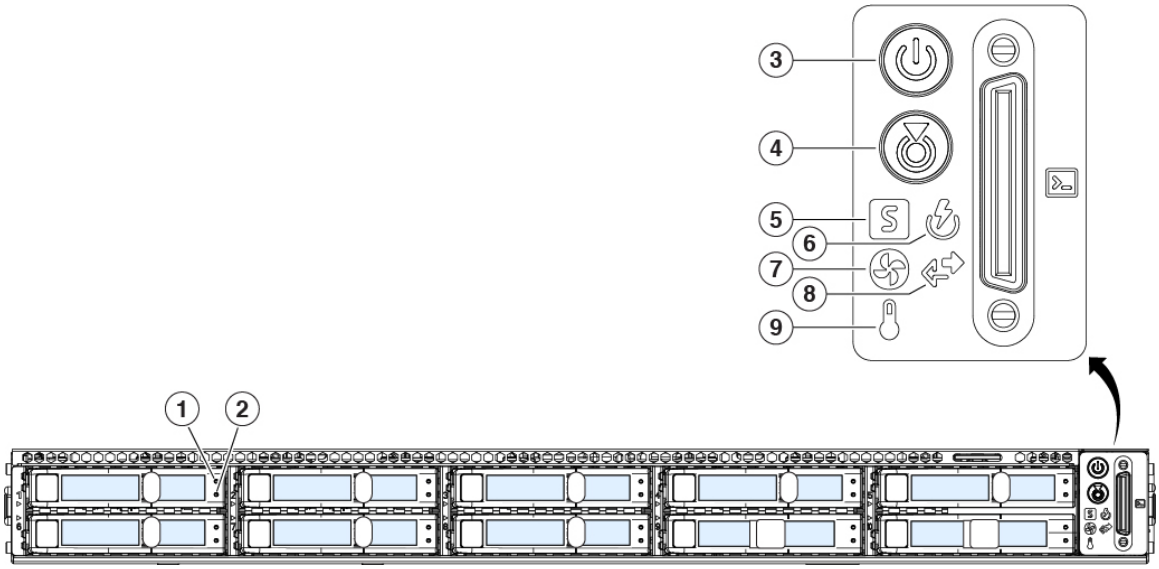


1	Drive bays Supports two SATA SSDs in slots 1 and 2 Supports six SAS HDDs in slots 3 through 8	**2**	Power button/power status LED
3	Unit identification button/LED	**4**	System status LED
5	Power supply status LED	**6**	Fan status LED
7	Network link activity LED	**8**	Temperature status LED
9	Pullout asset card	**10**	Keyboard, video, and mouse (KVM) port

Front Panel LEDs

The following figure shows the front panel LEDs and describes their states.

Figure 5: Front Panel LEDs and Their States



1	Drive fault LED: • Off—The drive is operating properly. • Amber—Drive fault detected. • Amber, flashing—The drive is rebuilding. • Amber, flashing with 1-second interval—Drive locate function activated in the software.	**2**	Drive activity LED: • Off—There is no drive in the drive tray (no access, no fault). • Green—The drive is ready. • Green, flashing—The drive is reading or writing data.
3	Power LED: • Off—There is no AC power to the chassis. • Amber—The chassis is in standby mode. • Green—The chassis is in main power mode. Power is supplied to all components.	**4**	Unit identification LED: • Off—The unit identification function is not in use. • Blue, flashing—The unit identification function is activated.

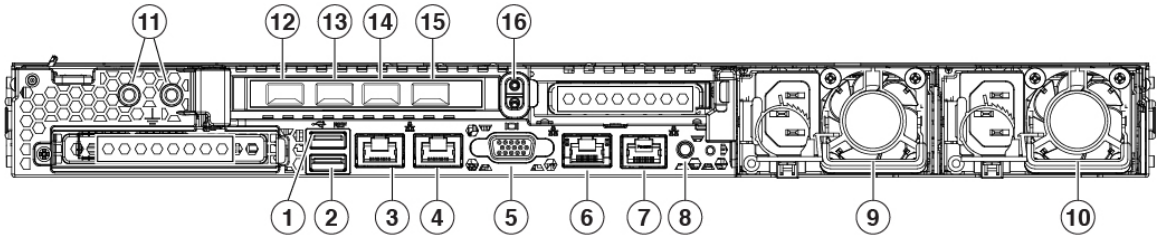
5	System status LED:
	• Green—The chassis is running in normal operating condition.
	• Green, flashing—The chassis is performing system initialization and memory check.
	• Amber—The chassis is in a degraded operational state (minor fault).
	  • Power supply redundancy is lost.
	  • CPUs are mismatched.
	  • At least one CPU is faulty.
	  • At least one DIMM is faulty.
	  • At least one drive in a RAID configuration failed.
	• Amber, two flashes—There is a major fault with the system board.
	• Amber, three flashes—There is a major fault with the DIMMs.
	• Amber, four flashes—There is a major fault with the CPUs.
		6	Power supply status LED:
			• Green—All power supplies are operating normally.
			• Amber—One or more power supplies are in a degraded operational state.
			• Amber, flashing—One or more power supplies are in a critical fault state.

7	Fan status LED: • Green—All fans are operating properly. • Amber, flashing—One or more fans breached the unrecoverable threshold.	**8**	Network link activity LED: • Off—The Ethernet port link is idle. • Green—One or more Ethernet ports are link-active, but there is no activity. • Green, flashing—One or more Ethernet ports are link-active with activity.
9	Temperature status LED: • Green—The chassis is operating at normal temperature. • Amber—One or more temperature sensors breached the critical threshold. • Amber, flashing—One or more temperature sensors breached the unrecoverable threshold.		

Rear Panel

The following figure shows the rear panel of the Threat Grid M5.

Figure 6: Threat Grid M5 Rear Panel



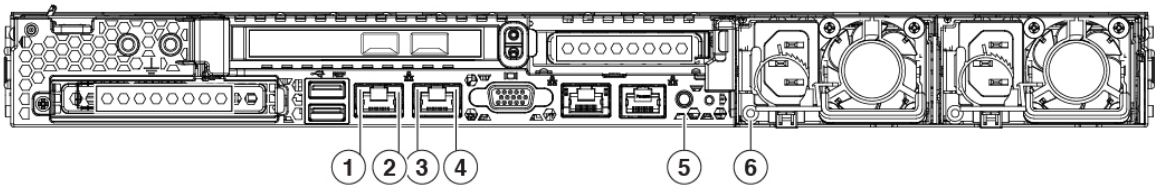
1	USB 3.0 Type A (USB 1) You can connect a keyboard, and along with a monitor on the VGA port, you can access the console.	**2**	USB 3.0 Type A (USB 2) You can connect a keyboard, and along with a monitor on the VGA port, you can access the console.
3	Data interface (Clean) Supports 100/1000/10000 Mbps depending on link partner capability.	**4**	Data interface (Dirty) Gigabit Ethernet 100/1000/10000 Mbps interface, RJ-45, LAN2
5	VGA video port (DB-15 connector)	**6**	CIMC interface (disabled in the M5) **Note** CIMC is *not* supported on any interfaces.
7	Serial console port (RJ-45 connector)	**8**	Unit identification button
9	770-W AC power supply (PSU 1) Redundant as 1 + 1	**10**	770-W AC power supply (PSU 2) Redundant as 1 + 1
11	Threaded holes for dual-hole grounding lug	**12**	SFP management interface Used for administration and NFS server connectivity (Admin) 10-Gigabit Ethernet SFP+ support SFP-10G-SR and SFP-10G-LR are qualified for use on the Threat Grid M5.
13	SFP interface Used for cluster interconnect (Clust) 10-Gigabit Ethernet SFP+ support SFP-10G-SR and SFP-10G-LR are qualified for use on the Threat Grid M5.	**14**	SFP interface Not supported

15	SFP interface Not supported	**16**	Riser handle Not supported

Rear Panel LEDs

The following figure shows the rear panel LEDs and describes their states.

Figure 7: Rear Panel LEDs and Their States



1	100-Mbps/1-Gbps/10-Gbps Ethernet link (speed on both LAN 1 and LAN 2): • Off—Link speed is 100 Mbps. • Amber—Link speed is 1 Gbps. • Green—Link speed is 10 Gbps.	**2**	100-Mbps/1-Gbps/10-Gbps Ethernet link status (speed on both LAN 1 and LAN 2): • Off—No link is present. • Green—Link is active. • Green, flashing—Traffic is present on the active link.
3	1-Gbps Ethernet dedicated management link: • Off—Link speed is 10 Mbps. • Amber—Link speed is 100 Gbps. • Green—Link speed is 1 Gbps.	**4**	1-Gbps Ethernet dedicated management link: • Off—No link is present. • Amber—Link is active. • Green, flashing—Traffic is present on the active link.
5	Rear unit identification: • Off—The unit identification function is not in use. • Blue, flashing—The unit identification function is activated.	**6**	Power supply (one LED for each power supply): • Off—No AC input (12-V main power off; 12-V standby power off) • Green, flashing—12-V main power off; 12-V standby power on. • Green—12-V main power on; 12-V standby power on. • Amber, flashing—Warning threshold detected but 12-V main power on. • Amber—Critical error detected; 12-V main power off (for example, overcurrent, overvoltage, or overtemperature failure).

Power Supply

The following table lists the specifications for each 770-W AC power supply (Cisco part number FMC-PWR-AC-770W) used in the Threat Grid M5.

Table 2: Power Supply Specifications

Description	Specification
Power consumption	1313 BTU/hr
AC input voltage range	Nominal range: 100 to 120 V AC, 200 to 240 V AC Range: 90–132 V AC, 180–264 V AC
AC input frequency	Nominal range: 50–60 Hz Range: 47–63 Hz
Maximum AC input current	9.5 A peak at 100-V AC 4.5 A peak at 208 V AC
Maximum input volt amperes	950 VA at 100 V AC
Maximum output power for each power supply	770 W
Maximum inrush current	15 A (subcycle duration)
Maximum hold-up time	12 ms at 770 W
Power supply output voltage	12 V DC
Power supply standby voltage	12 V DC
Efficiency rating	Climate Savers Platinum Efficiency (80 Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C13

Hardware Specifications

The following table contains hardware specifications for the Threat Grid M5 security appliance.

Table 3: Threat Grid M5 Hardware Specifications

Dimensions (H x W x D)	1.7 x 16.89 x 29.8 in (4.32 x 43.0 x 75.6 cm)
Weight	35.3 lb (16.01 kg)

Temperature	Operating: 50 to 95°F (10 to 35°C) Maximum temperature is derated by 1°F/547 ft (1°C/300 m) of altitude above 3117 ft (950 m). Nonoperating: –40 to 149°F (–40 to 65°C) When the appliance is stored or transported.
Humidity	Operating: 8 to 90% noncondensing Nonoperating: 5 to 95% noncondensing
Altitude	Operating: 0 to 10,000 ft Nonoperating: 0 to 40,000 ft when the appliance is stored or transported
Sound power level	5.8 Bels (measure A-weighted per ISO7779 LWAd) Operation at 73°F (23°C)
Sound pressure level	43 dBa (measure A-weighted per ISO7779 LpAM) Operation at 73°F (23°C)

Product ID Numbers

The following table lists the field-replaceable PIDs associated with the Threat Grid M5. The spare components are ones that you can order and replace yourself. If any internal components fail, you must RMA the entire chassis including the SFPs and SFP cables. Remove the drives and power supplies before you send the chassis for RMA.

Table 4: Threat Grid M5 PIDs

PID	Description
TG-M5-PWR-AC-770W	AC power supply
TG-M5-PWR-AC-770W=	AC power supply (spare)
TG-M5-HDD-2.4TB	2.4-TB HDD
TG-M5-HDD-2.4TB=	2.4-TB HDD (spare)
TG-M5-SSD-240G	240-GB SSD
TG-M5-SSD-240G=	240-GB SSD (spare)
UCSC-RAILB-M4	Rail kit

Power Cord Specifications

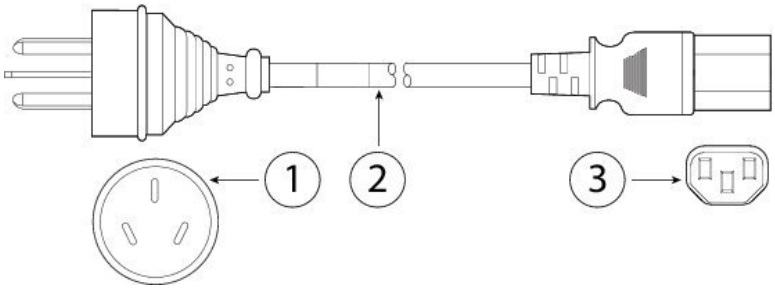
Each power supply has a separate power cord. Standard power cords or jumper power cords are available for connection to the Threat Grid M5. The jumper power cords for use in racks are available as an optional alternative to the standard power cords

If you do not order the optional power cord with the system, you are responsible for selecting the appropriate power cord for the product. Using a incompatible power cord with this product may result in electrical safety hazard. Orders delivered to Argentina, Brazil, and Japan must have the appropriate power cord ordered with the system.

Note Only the approved power cords and jumper cords provided with the Threat Grid M5 are supported.

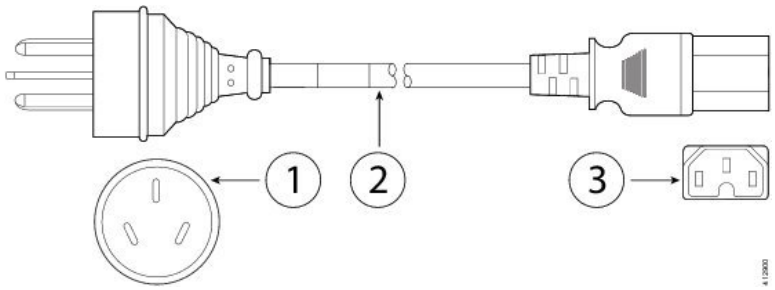
The following power cords and jumper cords are supported.

Figure 8: Argentina CAB-250V-10A-AR



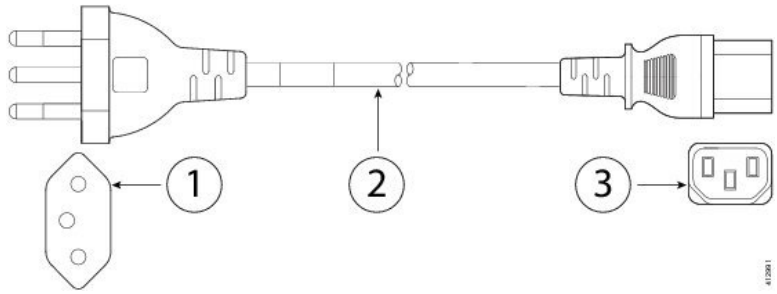
1	Plug: IRAM 2073	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		

Figure 9: Australia CAB-9K10A-AU



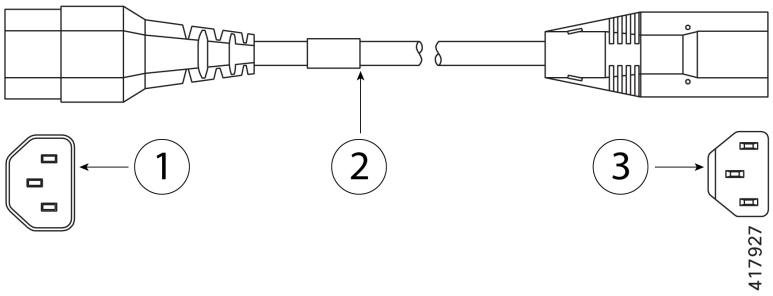
1	Plug: A.S. 3112-2000	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C15		

Figure 10: Brazil PWR-250V-10A-BZ



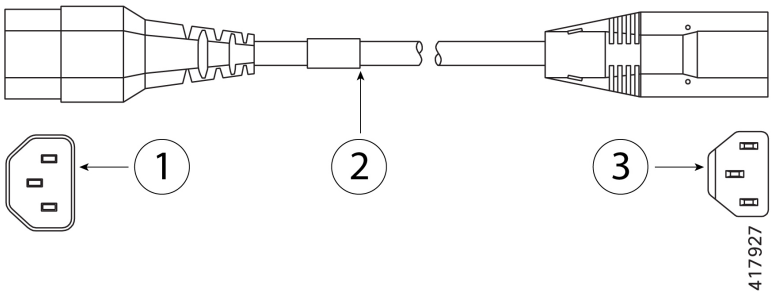
1	Plug: NBR 14136	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		

Figure 11: Cabinet Jumper CAB-C13-C14-2M



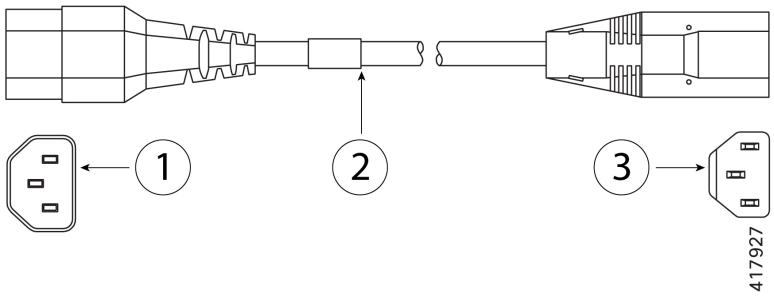
1	Plug: SS10A	**2**	Cord set rating: 10A, 250V
3	Connector: HS10S, C-13 to C-14		

Figure 12: Cabinet Jumper CAB-C13-C14-AC



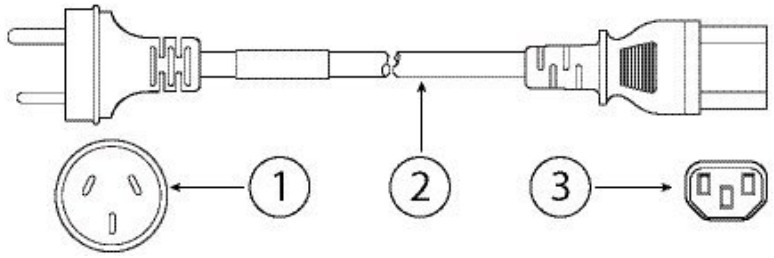
1	Plug: SS10A	**2**	Cord set rating: 10 A, 250 V
3	Connector: HS10S, C-13 to C-14 (recessed receptacle)		

Figure 13: Cabinet Jumper CAB-C13-CBN



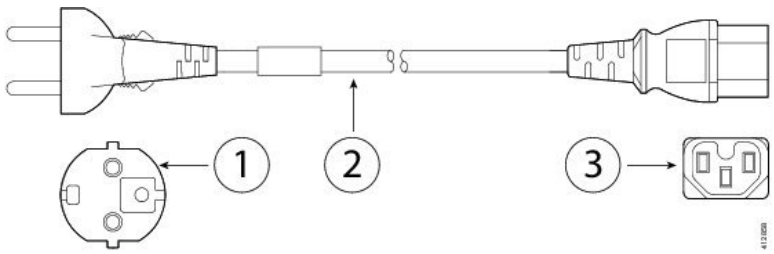
1	Plug: SS10A	**2**	Cord set rating: 10 A, 250 V
3	Connector: HS10S, C-13 to C-14		

Figure 14: China CAB-250V-10A-CH



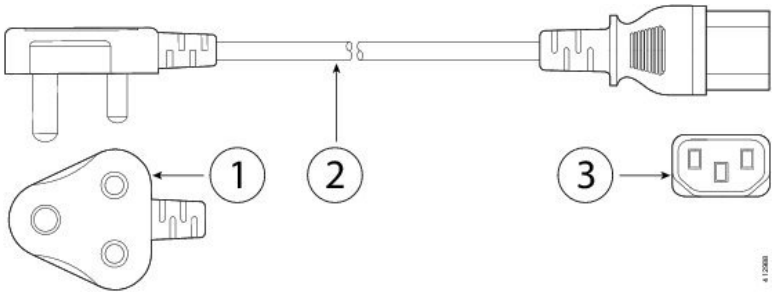
1	Plug: GB2099.1/2008	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C13		

Figure 15: Europe CAB-9K10A-EU



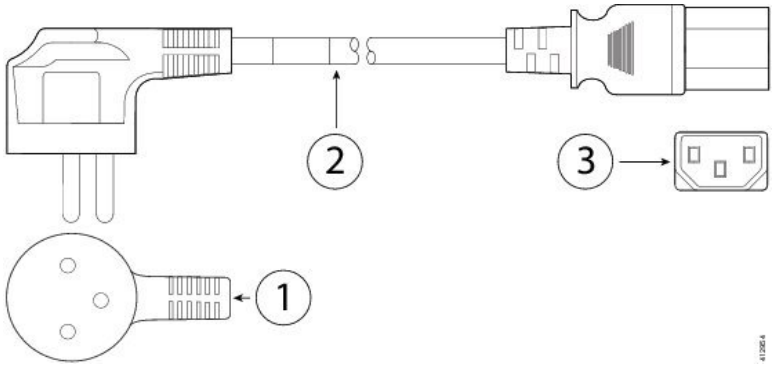
1	Plug: CEE 7/7 (M2511)	**2**	Cord set rating: 10 A/16 A, 250 V
3	Connector: IEC 60320/C15 (VSCC 15)		

Figure 16: India CAB-250V-10A-ID



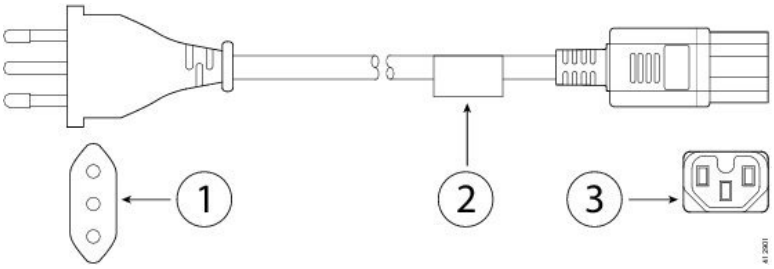
1	Plug: IS 6538-1971	**2**	Cord set rating: 16 A, 250 V
3	Connector: IEC 60320-C13		

Figure 17: Israel CAB-250V-10A-IS



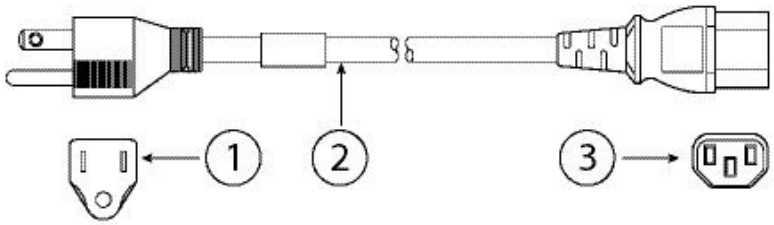
1	Plug: SI-32	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320-C13		

Figure 18: Italy CAB-9K10A-IT



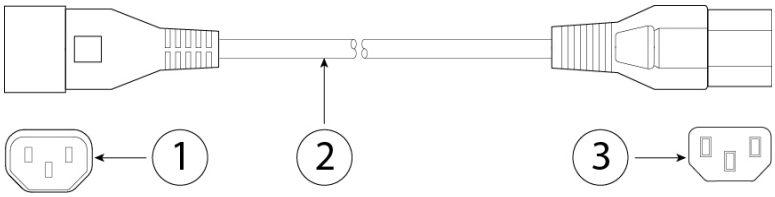
1	Plug: CEI 23-16/VII (I/3G)	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C15 (EN 60320/C15M)		

Figure 19: Japan CAB-JPN-3PIN



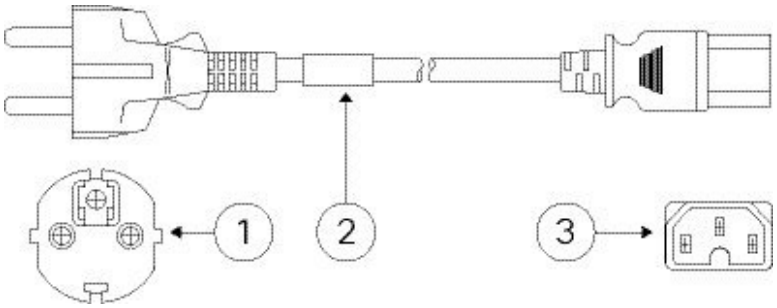
1	Plug: JIS 8303	**2**	Cord set rating: 12 A, 125 V
3	Connector: IEC 60320/C13		

Figure 20: Japan CAB-C13-C14-2M-JP



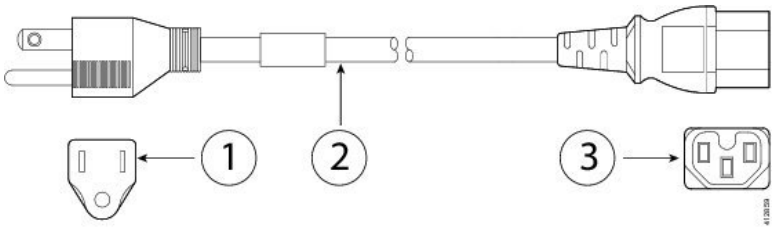
1	Plug: EN 60320-2-2/E	**2**	Cord set rating: 10 A, 250 V
3	Connector: EN 60320/C13 to C14		

Figure 21: Korea CAB-9K10S-KOR



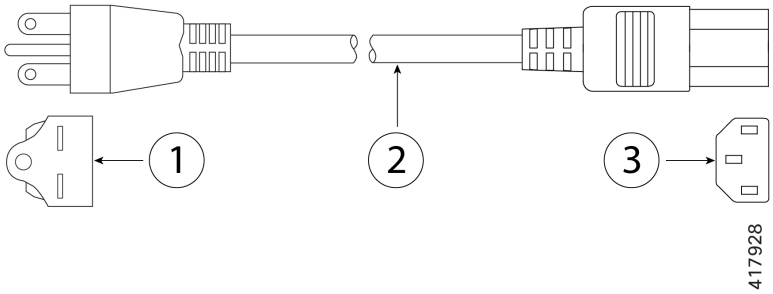
1	Plug: EL211 (KSC 8305)	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C15		

Figure 22: North America CAB-9K12A-NA



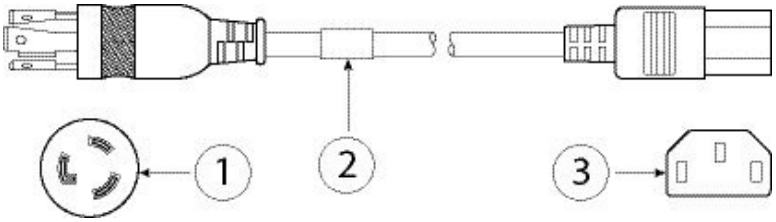
1	Plug: NEMA5-15P	**2**	Cord set rating: 13 A, 125 V
3	Connector: IEC 60320/C15		

Figure 23: North America CAB-N5K6A-NA



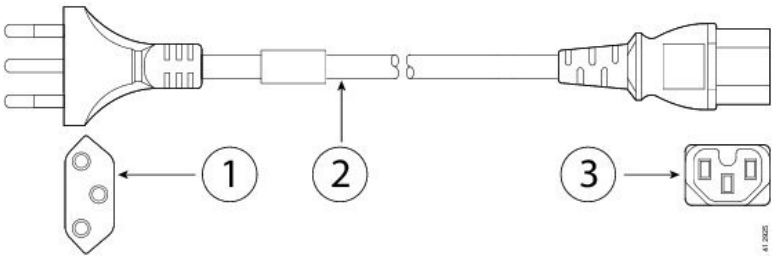
1	Plug: NEMA6-15P	**2**	Cord set rating: 10 A, 125 V
3	Connector: IEC 60320/C13		

Figure 24: North America CAB-AC-L620-C13



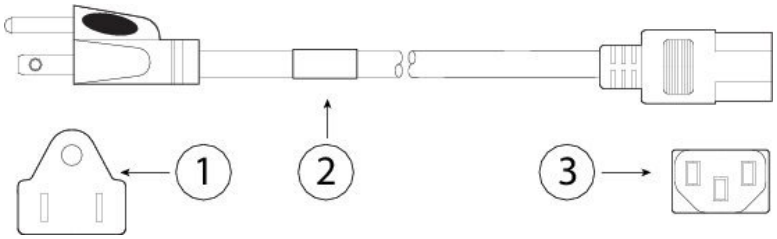
1	Plug: NEMA L6-20 (molded twist lock)	**2**	Cord set rating: 13 A, 250 V
3	Connector: IEC 60320/C13		

Figure 25: Switzerland CAB-9K10A-SW



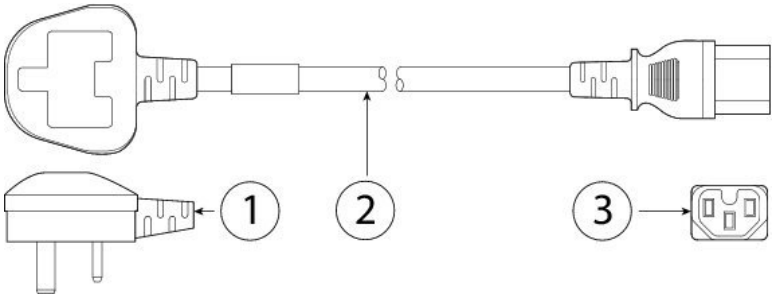
1	Plug: SEV 1011 (MP232-R)	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C15		

Figure 26: Taiwan CAB-ACTW

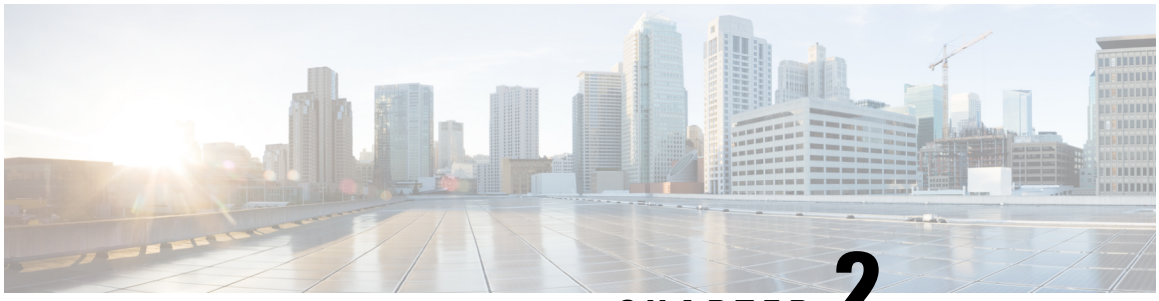


1	Plug: EL 302 (CNS10917)	**2**	Cord set rating: 10 A, 125 V
3	Connector: IEC 60320/C13		

Figure 27: United Kingdom CAB-9K10A-UK



1	Plug: BS1363A/SS145	**2**	Cord set rating: 10 A, 250 V
3	Connector: IEC 60320/C15		



CHAPTER 2

Installation Preparation

Installation Warnings

Read the Regulatory Compliance and Safety Information document before installing the Cisco Threat Grid appliance.

Caution Do *not* open the appliance except under direction from TAC.

Take note of the following warnings:

Warning

Statement 1071—Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number provided at the end of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS

Warning **Statement 12—**Power Supply Disconnection Warning

Before working on a chassis or working near power supplies, unplug the power cord on AC units. Disconnect the power at the circuit breaker on DC units.

Warning **Statement 19—**TN Power Warning

The device is designed to work with TN power systems.

Warning **Statement 43—**Jewelry Removal Warning

Before working on equipment that is connected to power lines, remove jewelry including rings, necklaces, and watches. Metal objects heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Warning **Statement 94—**Wrist Strap Warning

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Warning **Statement 1004—**Installation Instructions

Read the installation instructions before using, installing, or connecting the system to the power source.

Warning **Statement 1005**—Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: USA: 120 V, 15 A (EU: 250 V, 16 A)

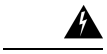
Warning **Statement 1015**—Battery Handling

To reduce risk of fire, explosion or leakage of flammable liquid or gas:

- Replace the battery only with the same or equivalent type recommended by the manufacturer.
- Do not dismantle, crush, puncture, use sharp tool to remove, short external contacts, or dispose of in fire.
- Do not use if battery is warped or swollen.
- Do not store or use battery in a temperature > 60° C.
- Do not store or use battery in low air pressure environment < 69.7 kPa.

Warning **Statement 1021—**SELV Circuit

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.



Warning **Statement 1024—**Ground Conductor

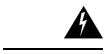
This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning **Statement 1040—**Product Disposal

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

Warning **Statement 1045—**Short-Circuit Protection

This product requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.



Warning **Statement 1053—**Class 1M Laser Radiation

Hazard level 1M invisible laser radiation is present. Do not view directly with nonattenuating optical instruments.

Warning **Statement 1074—**Comply with Local and National Electrical Codes

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Safety Recommendations

Use the information in the following sections to help ensure your safety and to protect the chassis. This information may not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

Observe these safety guidelines:

- Keep the area clear and dust free before, during, and after installation.

- Keep tools away from walkways, where you and others might trip over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, or chains that could get caught in the chassis.
- 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.
- Never attempt to lift an object that is too heavy for one person.

Maintain Safety with Electricity

Warning Before working on a chassis, be sure the power cord is unplugged.

Be sure to read the Regulatory Compliance and Safety Information document before installing the Threat Grid chassis.

Follow these guidelines when working on equipment powered by electricity:

- Before beginning procedures that require access to the interior of the chassis, locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected; always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs:
  - Use caution; do not become a victim yourself.
  - Disconnect power from the system.
  - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.
- The FMC chassis is equipped with an AC-input power supply, which is shipped with a three-wire electrical cord with a grounding-type plug that fits into a grounding-type power outlet only. Do not circumvent this safety feature. Equipment grounding should comply with local and national electrical codes.

Prevent ESD Damage

ESD occurs when electronic components are improperly handled, and it can damage equipment and impair electrical circuitry, which can result in intermittent or complete failure of your equipment.

Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to an earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground ESD voltages. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

For safety, periodically check the resistance value of the antistatic strap, which should be between one and 10 megohms.

Site Environment

See Hardware Specifications, on page 11 for information about physical specifications.

To avoid equipment failures and reduce the possibility of environmentally caused shutdowns, plan the site layout and equipment locations carefully. If you are currently experiencing shutdowns or unusually high error rates with your existing equipment, these considerations may help you isolate the cause of failures and prevent future problems.

Power Supply Considerations

See Power Supply, on page 11 for more detailed information about the power supply in the Threat Grid chassis.

When installing the chassis, consider the following:

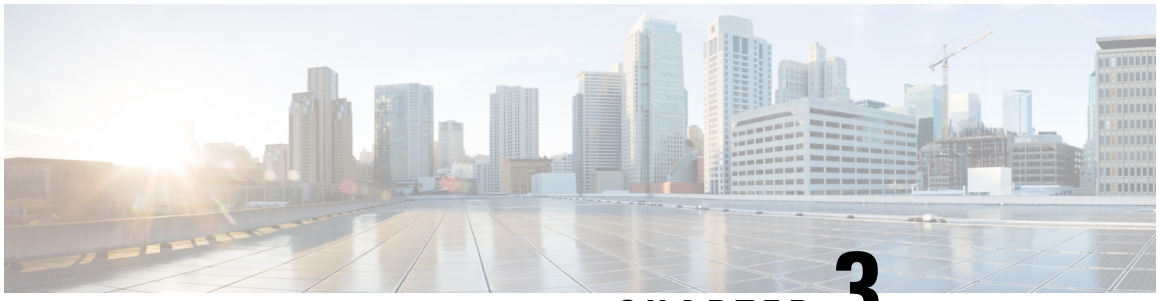
- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct appliance input-power requirement.
- Several styles of AC-input power supply cords are available for the chassis; make sure that you have the correct style for your site.
- If you are using dual redundant (1+1) power supplies, we recommend that you use independent electrical circuits for each power supply.
- Install an uninterruptible power source for your site, if possible.

Rack Configuration Considerations

See Rack-Mount the Chassis, on page 28 for rack-mount instructions.

Consider the following when planning a rack configuration:

- If you are mounting a chassis in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- Be sure enclosed racks have adequate ventilation. Make sure that the rack is not overly congested as each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- In an enclosed rack with a ventilation fan in the top, heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- 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. Experiment with different arrangements to position the baffles effectively.



CHAPTER 3

Rack-Mount the Chassis

Unpack and Inspect the Chassis

Tip Keep the shipping container in case the chassis requires shipping in the future.

Note The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

See Package Contents, on page 3 for a list of what shipped with the chassis.

Step 1 Remove the chassis from its cardboard container and save all packaging material.

Step 2 Compare the shipment to the equipment list provided by your customer service representative. Verify that you have all items.

Step 3 Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

- Invoice number of shipper (see the packing slip)
- Model and serial number of the damaged unit
- Description of damage
- Effect of damage on the installation

Rack-Mount the Chassis

You can install the chassis in a rack using the Cisco rack kit.

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, 4-post EIA rack with mounting posts that conform to English universal hole spacing per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square 0.38-in. (9.6 mm), round 0.28-in. (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per chassis must be 1 RU, equal to 1.75 in. (44.45 mm).
- The slide rails for the chassis have an adjustment range of 24 to 36 in. (610 to 914 mm).

Note The slide rails supplied by Cisco Systems for the chassis do not require tools for installation if you install them in a rack that has square 0.38-in. (9.6 mm), round 0.28-in. (7.1 mm), or #12-24 UNC threaded holes.

Before you begin

Take note of the following warnings:

Warning **Statement 1006—**Chassis Warning for Rack-Mounting and Servicing

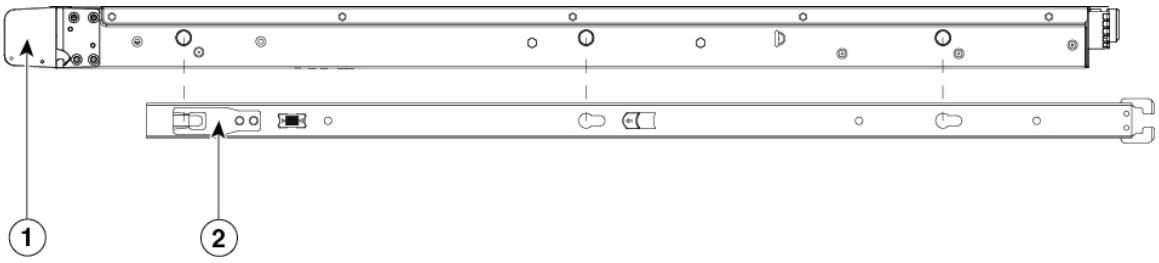
To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Step 1 Attach the inner rails to the sides of the chassis:

a) Align an inner rail with one side of the chassis so that the three keyed slots in the rail align with the three pegs on the side of the chassis.
b) Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.
c) Install the second inner rail to the opposite side of the chassis.

Figure 28: Attach the Inner Rail to the Side of Chassis

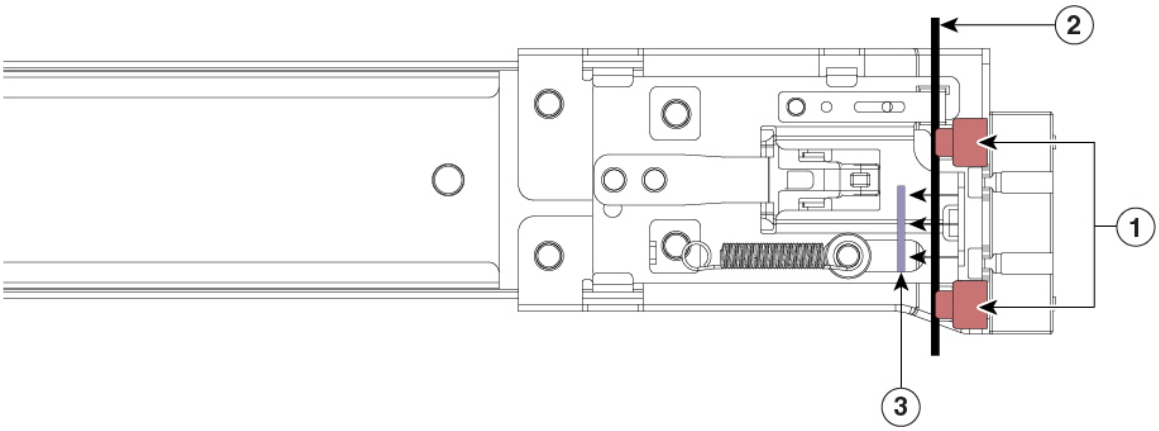


1	Front of chassis	**2**	Locking clip on inner rail

Step 2 Open the front securing plate on both slide-rail assemblies. The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes.

On the outside of the assembly, push the green arrow button toward the rear to open the securing plate.

Figure 29: Front Securing Mechanism, Inside of Front End



1	Front mounting pegs	**2**	Rack post
3	Securing plate shown pulled back to open position		

Step 3 Install the slide rails into the rack:

a) Align one slide-rail assembly front end with the front rack-post holes that you want to use.

The slide rail front end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front.

Note The rack post must be between the mounting pegs and the open securing plate.

b) Push the mounting pegs into the rack-post holes from the outside-front.
c) Press the securing plate release button, marked “PUSH.” The spring-loaded securing plate closes to lock the pegs in place.
d) Attach the second slide-rail assembly to the opposite side of the rack. Make sure that the two slide-rail assemblies are at the same height with each other and are level front-to-back.
e) Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

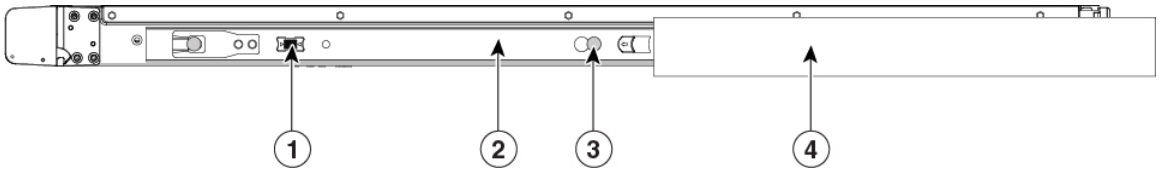
Step 4 Insert the chassis into the slide rails:

a) Align the rear of the inner rails that are attached to the chassis sides with the front ends of the empty slide rails on the rack.

b) Push the inner rails into the slide rails on the rack until they stop at the internal stops.

c) Slide the release clip toward the rear on both inner rails, and then continue pushing the chassis into the rack until its front slam latches engage with the rack posts

Figure 30: Inner Rail Release Clip



1	Inner rail release clip	**2**	Inner rail attached to the chassis and inserted into outer rail
3	Button to unlock rail Press this button to unlock the rail so you can pull out the chassis from the rack when uninstalling or performing maintenance.	**4**	Outer rail attached to rack post

Step 5 (Optional) Secure the chassis in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with chassis installed. With the chassis fully pushed into the slide rails, open a hinged slam latch lever on the front of the chassis and insert the screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the chassis from being pulled out. Repeat for the opposite slam latch.

What to do next

Continue with Connect Cables, Turn on Power, and Verify Connectivity.

Connect Cables, Turn on Power, and Verify Connectivity

After rack mounting the chassis, follow these steps to connect cables, turn on power, and verify connectivity.

Note AC power supplies have internal grounding and so no additional chassis grounding is required when the supported AC power cords are used. For more information about supported power cords, see Power Cord Specifications, on page 13.

Before you begin

Take note of the following warnings.

Warning **Statement 1009—**Laser Radiation

Laser radiation is present when the system is open.

Warning **Statement 1051—**Laser Radiation

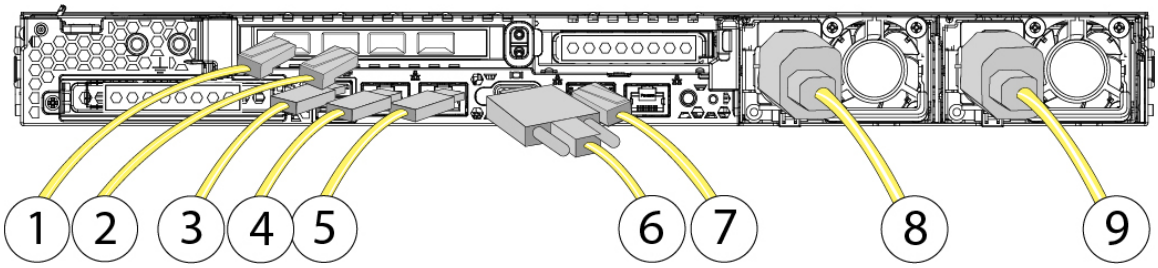
Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Step 1 Connect one Cisco-supported SFP+ transceiver and cable to the far left SFP port. This is eth0 used to manage the Threat Grid M5 through the Opadmin console and should connect to a secure management network.

Each Cisco-certified SFP+ transceiver has an internal serial EEPROM that is encoded with security information. This encoding allows us to identify and validate that the SFP transceiver meets the requirements for the Threat Grid M5 chassis.

Note Only Cisco certified SFP+ transceivers are compatible with the 10-Gb interfaces and both transceivers must be 1-Gb or 10-Gb. You cannot use one transceiver of each kind. Cisco TAC may refuse support for any interoperability problems that result from using an untested third-party SFP+ transceiver.

Figure 31: Cable Connections



1	SFP management interface (Admin) Used for administration and NFS server connectivity 10-Gigabit Ethernet SFP+ support SFP-10G-SR and SFP-10G-LR are qualified for use on the Threat Grid M5.	**2**	SFP interface (Clust) Used for cluster interconnect 10-Gigabit Ethernet SFP+ support SFP-10G-SR and SFP-10G-LR are qualified for use on the Threat Grid M5.
3	USB Ports (two)	**4**	Data interface (Clean) Supports 100/1000/10000 Mbps depending on link partner capability
5	Data interface (Dirty) Gigabit Ethernet 100/1000/10000 Mbps interface, RJ-45, LAN2	**6**	VGA video port (DB-15 connector)

7	CIMC interface (disabled in M5) **Note** CIMC is *not* supported on any interfaces.	**8**	770-W AC power supply (PSU 1) Redundant as 1 + 1
9	770-W AC power supply (PSU 1) Redundant as 1 + 1		

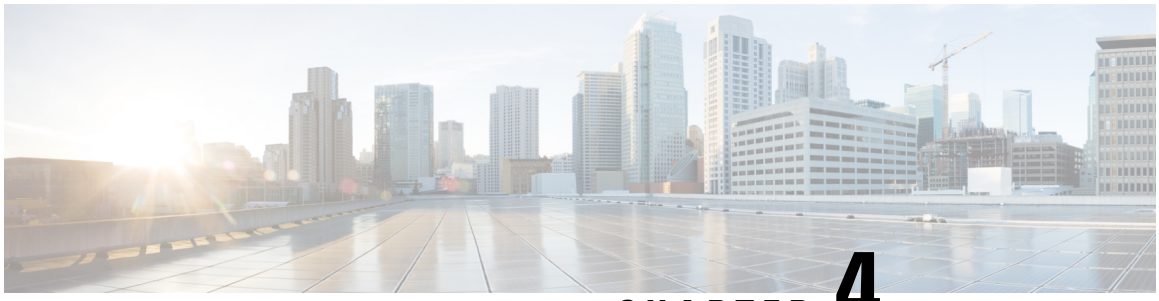
Step 2 Connect a second Cisco-supported SFP+ transceiver and cable to the SFP port to the right of the eth0 port in Step 1. This is eth1 used to access the console and allows your Threat Grid M5 to monitor traffic.

Step 3 Use the supported power cords to connect the power supplies of the chassis to your power source. For more information about supported power cords, see Power Cord Specifications, on page 13.

Step 4 Connect a keyboard to one of the USB ports and a monitor to the VGA port.

Step 5 Power on the appliance and wait for it to boot up.

Step 6 The TGSH Dialog is displayed on the console when the server has successfully booted up and connected. Complete the Initial Configuration Steps as described in the configuration guide.



CHAPTER 4

Maintenance and Upgrades

Power Button Shut Down

The Threat Grid M5 runs in two modes:

- Main power mode—Power is supplied to all Threat Grid M5 components and all operating systems can run.
- Standby power mode—Power is supplied only to the service processor and certain components. You can safely remove power cords from the Threat Grid M5 in this mode.

⚠

Caution After you shut down the Threat Grid M5 to standby power, electric current is still present in the chassis. To completely remove power as directed in some maintenance procedures, you must disconnect all power cords from all power supplies on the Threat Grid M5.

You can shut down the Threat Grid M5 using the front panel Power button or use OpAdmin to initiate a reboot or shutdown.

Step 1 Check the Power LED:

- Amber—The Threat Grid M5 is already in standby mode and you can safely remove power.
- Green—The Threat Grid M5 is in main power mode and you must shut it down before you can safely remove power.

Step 2 Perform a graceful shutdown or a hard shutdown:

Caution To avoid data loss or damage to your operating system, perform a graceful shutdown of the operating system.

- Graceful shutdown—Press and release the Power button. The operating system performs a graceful shutdown and the Threat Grid M5 goes into standby mode. The power LED is amber.
- Emergency shutdown—Press and hold the Power button for four seconds to force the main power off and immediately enter standby mode.

Step 3 If a maintenance procedure instructs you to completely remove power from the Threat Grid M5, disconnect all power cords from the power supplies.

Remove and Replace a Drive

Note The drives are hot-swappable. You do not have to shut down the Threat Grid M5 to remove or replace drives.

Note You cannot add more drives to the chassis. You can only replace the drives in the slots that shipped with your Threat Grid M5.

Before you begin

Take note of the following warnings:

Warning **Statement 1018—**Supply Circuit

To reduce risk of electric shock and fire, take care when connecting units to the supply circuit so that wiring is not overloaded.

Warning **Statement 1019—**Main Disconnecting Device

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

Warning **Statement 1024—**Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, 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.

Warning **Statement 1030—**Equipment Installation

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

Warning **Statement 1073—**No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

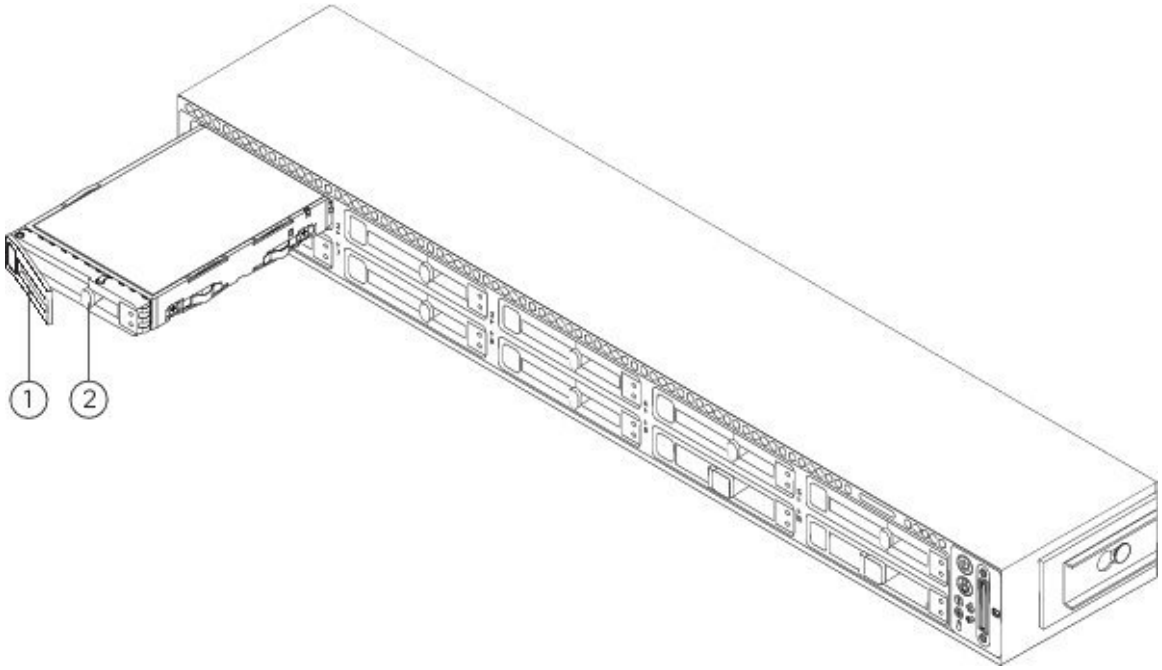
Warning **Statement 1074—**Comply with Local and National Electrical Codes

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Step 1 Remove the drive that you are replacing:

a) Press the release button on the face of the drive tray.
b) Grasp and open the ejector lever and then pull the drive tray out of the slot.

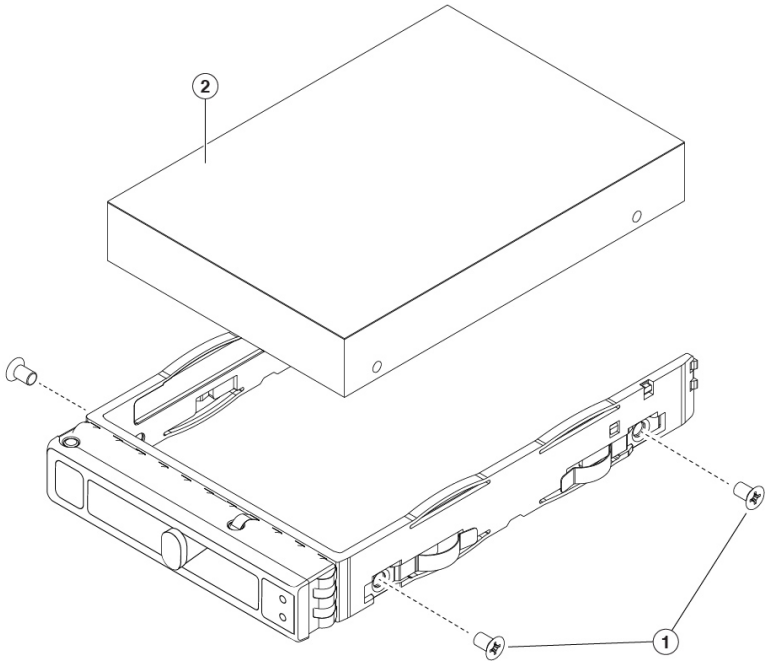
Figure 32: Remove the Drive



1	Ejector handle	**2**	Release button

Step 2 Remove the four drive-tray screws that secure the drive to the tray and then lift the drive out of the tray.

Figure 33: Remove the Drive Tray



1	Drive tray screws (two on each side)	**2**	Drive removed from drive tray

Step 3 Install a new drive:

a) Place a new drive in the empty drive tray and install the four drive-tray screws.
b) With the ejector lever on the drive tray open, insert the drive tray into the empty drive bay.
c) Push the tray into the slot until it touches the backplane, and then close the ejector lever to lock the drive in place.

Remove and Replace a Power Supply

The Threat Grid M5 ships with two power supplies, which are redundant and hot-swappable. One is the active power supply and the other is the standby power supply (1+1).

The Threat Grid M5 also supports cold redundancy. Depending on the power being drawn by the Threat Grid M5, one power supply might actively provide all power to the system while the remaining power supply is put into a standby state. For example, if the power consumption can be satisfied by power supply 1, then power supply 2 is put into a standby state.

⚠

Caution When you replace power supplies, do not mix power supply types in the Threat Grid M5. Both power supplies must be the same wattage and Cisco PID.

Trouble Power supply health monitoring notifies you if the power supply loses power or malfunctions so that redundancy is lost. Check the power supply cables to make sure they are functioning. If they are and errors are still occurring, replace the power supply.

Before you begin

Take note of the following warnings:

Warning **Statement 1018—**Supply Circuit

To reduce risk of electric shock and fire, take care when connecting units to the supply circuit so that wiring is not overloaded.

Warning **Statement 1019—**Main Disconnecting Device

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

Warning **Statement 1024—**Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, 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.

Warning **Statement 1030—**Equipment Installation

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

Warning **Statement 1073—**No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

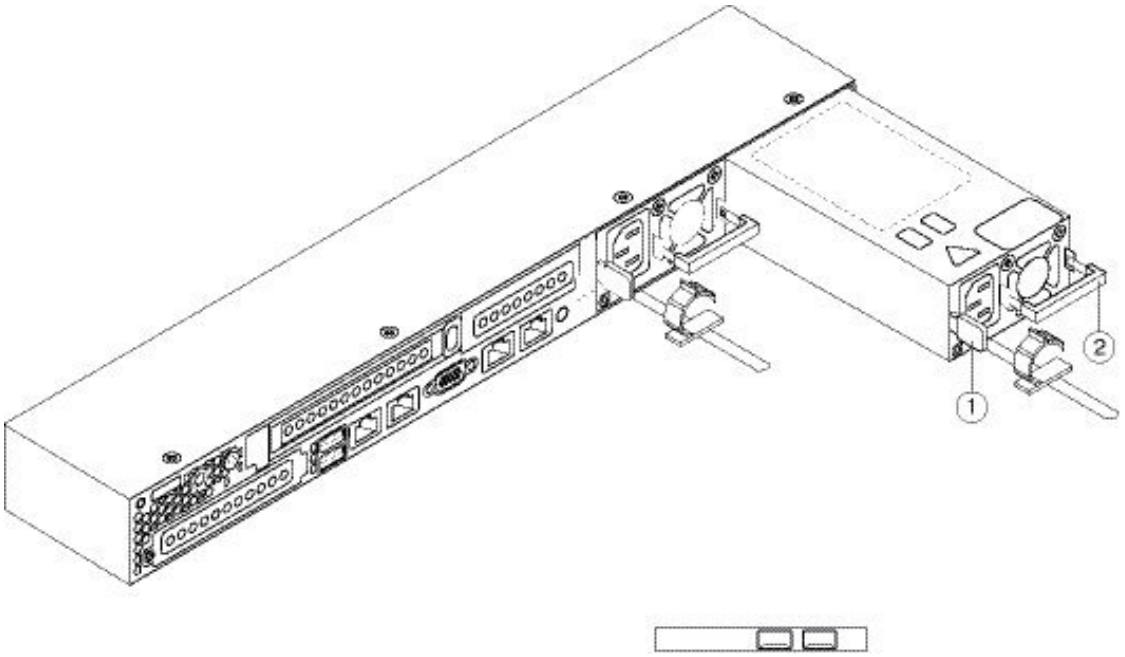
Warning **Statement 1074—**Comply with Local and National Electrical Codes

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Step 1 Remove the power supply:

a) Grasp the power supply handle while pinching the release lever toward the handle.
b) Pull the power supply out of the bay.

Figure 34: Remove and Replace the AC Power Supply



1	Release lever	**2**	Handle

Step 2 Install a new power supply:

a) Grasp the power supply handle and insert the new power supply into the empty bay.
b) Push the power supply into the bay until the release lever locks.
c) Connect the power cord to the new power supply.
d) If you shut down the Threat Grid M5, press the Power button to return it to main power mode.