



## **Cisco Security Packet Analyzer 2400 Series Appliances Installation and Configuration Guide**

September 2016

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Text Part Number:

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.

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: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1110R)

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.

*Cisco Security Packet Analyzer 2400 Series Appliances Installation and Configuration Guide*  
© 2016 Cisco Systems, Inc. All rights reserved.



# Contents

---

## CHAPTER 1

About the Cisco Security Packet Analyzer 2400 Series Appliance	1-1
Cisco Security Packet Analyzer 2400 Appliance Views and LEDs	1-2
Input/Output Ports and Connectors	1-4
Packet Analyzer Management Port (LAN 1)	1-4
Serial (Console) Port Connector and Cable	1-5
Small Form-Factor Pluggable (SFP) Modules	1-5
KVM Console	1-6
AC Power Supplies	1-6
Summary of Appliance Features	1-7
Cisco Security Packet Analyzer 2400 Feature	1-7

---

## CHAPTER 2

Requirements and Restrictions	2-2
Installation Process Summary	2-2
Unpack and Inspect the Appliance	2-4
Cisco Cisco Security Packet Analyzer 2400 Appliance Packing List	2-5
Install the Appliance in a Rack	2-5
Install the Transceiver Modules	2-6
Connect the Power	2-7
Connect the Appliance Cables	2-8
Connect the Management Port	2-8
Connect the Monitoring Ports	2-9
Direct Connections	2-9
Optical Tap Connections	2-9
Connect a Console Terminal	2-11
Connect a Monitor to the Appliance	2-12
Power Up the Appliance	2-12

---

## CHAPTER 3

Logging In For the First Time	3-1
Changing the Root Password	3-2
Examples	3-3
Changing the Packet Analyzer Root Password: Example	3-3
Verifying the Packet Analyzer Root Password: Example	3-3

- Resetting the Packet Analyzer Root Password to the Default Value 3-3
- Establishing Network Connectivity 3-4
- Checking Your Configuration 3-5
- Enabling the Cisco Security Packet Analyzer Web Server 3-6
- Verifying System Status 3-8
- Configuring a Monitored Device 3-10
  - Configuring a Monitored Device Interface 3-10
  - Creating a SPAN Session 3-10
- Opening and Closing a Telnet or SSH Session to the Packet Analyzer 3-11
  - Examples 3-12
- Setting up the CIMC 3-13
  - Setting up Serial Console Connection 3-14
    - Setting up Serial Console Access through External RJ-45 Port 3-14
- Shutting Down and Starting Up the Appliance 3-14

---

**CHAPTER 4**

- Configuring the iSCSI Array 4-1
- Locating the Packet Analyzer IQN 4-2
- Connecting the Storage Array 4-2

---

**CHAPTER 5**

- General Maintenance Guidelines 5-1
- Reading the LEDs 5-1
  - Cisco Packet Analyzer 2400 LEDs 5-2
    - Cisco Security Packet Analyzer 2400 5-2
      - Reading the Cisco Cisco Security Packet Analyzer 2400 Rear-Panel LEDs 5-4
  - Reading the NIC LEDs 5-5
  - Reading the AC Power Supply LED 5-6
- Replacing Appliance Components 5-7
  - Installing or Removing a UCS PCIe NIC Card 5-7
  - Replacing Transceiver Modules 5-7
  - Removing and Replacing a Hard Disk Drive 5-8
  - Installing or Replacing a Power Supply. 5-8
- Removing or Replacing the Cisco Security Packet Analyzer 2400 Series Appliances 5-8

---

**CHAPTER 6**

- Backing Up Your Configuration 6-1
- Restoring Your Configuration 6-2
- Upgrading Your Software 6-2
- Recovery Installation 6-3

**APPENDIX A****Troubleshooting A-1**

- Troubleshooting Guidelines A-1
- Troubleshooting Appliance Problems A-2
- Serial Number Locations A-5

**APPENDIX B****Safety Guidelines B-1**

- General Precautions B-1
- Safety with Equipment B-2
- Safety with Electricity B-3
- Preventing Electrostatic Discharge Damage B-4
- Lifting Guidelines B-5

**APPENDIX C****Technical Specifications C-1**

- Cisco Security Packet Analyzer2400 Technical Specifications C-1
- SFP Port Cable Specifications C-1
- Optical Tap Devices C-1

**APPENDIX D****Sample Site Log and Preinstallation Task Checklist D-1**

- Sample Site Log D-1
- Sample Preinstallation Task Checklist D-3

**APPENDIX E****Helper Utility E-1**

- Helper Utility Menu Summary E-2
- Option n - Configure Network E-2
- Option 1 - Download Application Image and Write to HDD E-3
- Option 2 - Download Application Image and Reformat HDD E-4
- Option 3 - Install Application Image from CD E-4
- Option 4 - Display Software Versions E-4
- Option 5 - Reset Application Image CLI Passwords to Default E-5
- Option 6- Send Ping E-5
- Option 7 - Configure Capture RAID Settings E-5
- Option 8 - Install Application Image From Flash and Reformat HDD E-6
- Option f - Check For and Fix Filesystem Errors on Local Disk E-6
- Option s - Show Upgrade Log E-6
- Option r - Exit and Reset Services Engine E-6
- Option h - Exit and Shutdown Services Engine E-6





# Introducing the Cisco Security Packet Analyzer 2400 Series Appliance

---

Cisco Packet Analyzer 2400 appliance which is based on UCS C240 server. The Cisco Security Packet Analyzer 2400 appliance has the option for one of three capture interface card types according to your requirement.

- 4x1GE optical
- 4x 1GE RJ45
- 2x 10GE Optical

This chapter contains the following sections:

- [About the Cisco Security Packet Analyzer 2400 Series Appliance, page 1-1](#)
- [Summary of Appliance Features, page 1-7](#)

## About the Cisco Security Packet Analyzer 2400 Series Appliance

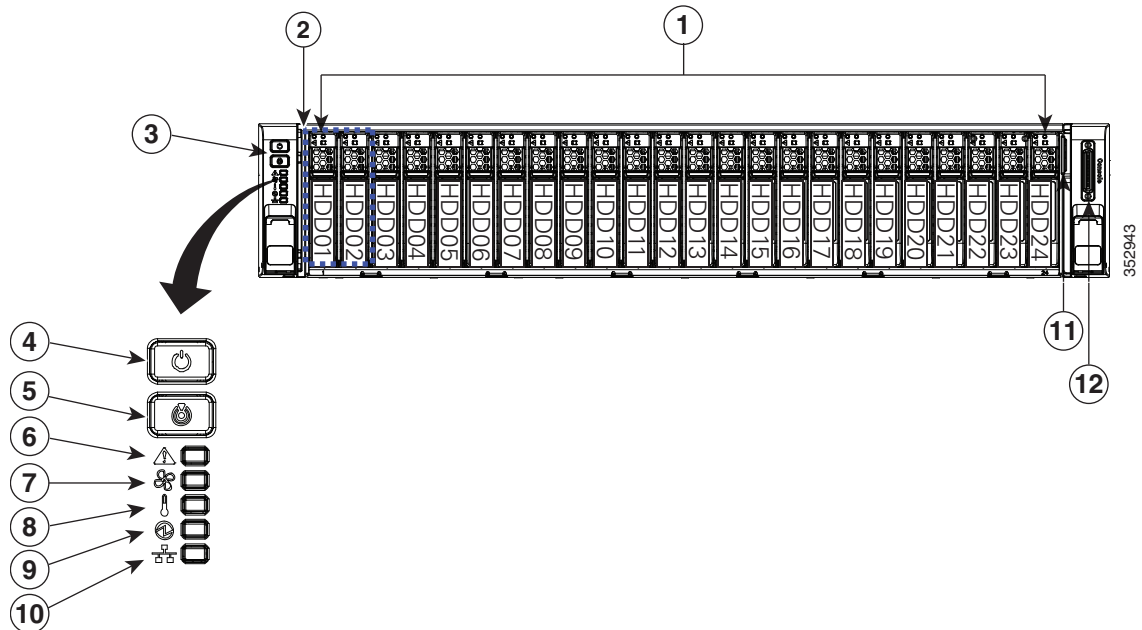
Cisco Security Packet Analyzer 2400—This model has three monitoring interfaces card types with an option to select one according to your requirement. This model receives collected data over up to four 1 GbE ports at a data rate of 1 Gb/s each or two 10 GbE ports at a data rate of 10 Gb/s each, uses fiber-optic or copper cables, and connects to the data collection devices with SFP, SFP+ or RJ-45 connectors. The data ports also support 1GbE SFP modules. The Cisco Security Packet Analyzer come preloaded with Cisco Prime Network Analysis Module software and are contained in a standard shelf-rack enclosure.

The following sections describe:

- [Cisco Security Packet Analyzer 2400 Appliance Views and LEDs](#)
- [Input/Output Ports and Connectors](#)
- [KVM Console](#)
- [AC Power Supplies](#)

## Cisco Security Packet Analyzer 2400 Appliance Views and LEDs

Figure 1-1 Cisco Security Packet Analyzer 2400 Appliance Front View

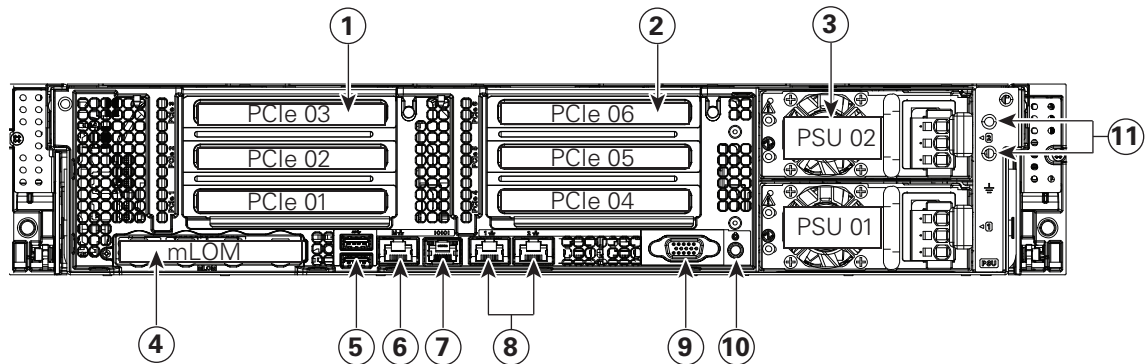


1	Drive bays 1–24 (up to 24 2.5-inch drives)	7	Temperature status LED
2	Operations panel buttons and LEDs	8	Power supply status LED
3	Power button/LED	9	Network link activity LED
4	Unit Identification button/LED	10	Pull-out asset tag
5	System status LED	11	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
6	Fan status LED		

For a description of the Cisco Packet Analyzer 2400 appliance front panel LEDs and their state definitions, see [“Reading the LEDs”](#) section on page 5-1.



Figure 1-2 Cisco Security Packet Analyzer 2400 Appliance Rear View



352947

1	PCIe riser 1 (slots 1, 2, 3*) *Slot 3 not present in all versions.	7	Serial connector (RJ-45)
2	PCIe riser 2 (slots 4, 5, 6)	8	Two embedded (on the motherboard) Intel i350 GbE Ethernet controller ports (LAN1, LAN2)
3	Power supplies (DC power supplies shown)	9	VGA video port (DB-15 connector)
4	Modular LAN-on-motherboard (mLOM) card slot	10	Rear Unit Identification button/LED
5	USB 3.0 ports (two)	11	Grounding-lug holes (for DC power supplies)
6	1-Gbps dedicated management port		

### Related Topics

For Information About...	See...
Cisco Packet Analyzer 2400 rear panel LEDs and their state definitions	, page 5-4
NIC LEDs and their state descriptions	<a href="#">Reading the NIC LEDs, page 5-5</a>
AC power supply LED and its state descriptions	<a href="#">Reading the AC Power Supply LED, page 5-6</a>

## Input/Output Ports and Connectors

The Cisco Packet Analyzer 2400 appliance support the following ports on the rear of the appliance:

- Packet Analyzer management port (LAN1, marked “1”)

Additional ports include:

- The video connector is not required for normal day-to-day operation of the Packet Analyzer appliances.
- The built-in port labeled “M” is the Cisco Integrated Management Controller (CIMC) port.



**Note** You can either use a single connection on port "1" for both Packet Analyzer management and CIMC or use port "1" for Packet Analyzer management and port "M" for CIMC to connect them to different switches.

The Cisco Packet Analyzer 2400 series appliances use the following connector types:

**Table 1-1 Packet Analyzer Series Connector Types**

Appliance Model	Number of Ports	Connector	Required Cable Type
CISCO SECURITY PACKET ANALYZER2400-K9	4 or 2	<ul style="list-style-type: none"> <li>• 1G SFP/RJ-45</li> <li>• 1G SFP/10G SFP+ The data ports on the 2400 also support 1G SFP.</li> </ul>	<ul style="list-style-type: none"> <li>• Fiber optic or copper cables.</li> <li>• Single-mode fiber or multi-mode fiber. For SFP cabling specifications, see <i>Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco CPT and Cisco ONS Platforms</i>, <a href="#">SFP and SFP+ Description and Specifications</a>.</li> </ul>

### Packet Analyzer Management Port (LAN 1)

The Cisco Security Packet Analyzer 2400 series appliances use the LAN 1 port, an integrated Ethernet controller (10/100/1000 Mb/s), as the management port. When you connect this port to a gateway, you enable management and Packet Analyzer application access to the Cisco Security Packet Analyzer 2400 series appliances.



**Note** Do not use the built-in port labeled “M”, which is the Cisco Integrated Management Controller (CIMC) port, as the management port; the LAN 1 port provides additional functionality.



**Note** We recommend that you use no less than a Category 5e (or better) unshielded twisted-pair (UTP) cable for the management port connection.

To access the Ethernet port, connect a Category 5e (or better) unshielded twisted-pair (UTP) cable to the RJ-45 connector on the back of the appliance. (See [Table 1-2](#)). The appliance comes with an Ethernet RJ-45-to-RJ-45 yellow cable.

**Table 1-2 Ethernet Cabling Guidelines**

Type	Description
10BASE-T	EIA Categories 3, 4, or 5 UTP (2 or 4 pairs) up to 328 ft. (100 m)
100BASE-TX	EIA Category 5e (or better) UTP (2 pairs) up to 328 ft. (100 m)
1000BASE-T	EIA Category 6 (recommended), Category 5E or 5 UTP (or better) (2 pairs) up to 328 ft. (100 m)

## Serial (Console) Port Connector and Cable

The Cisco Security Packet Analyzer 2400 series appliances use the RJ-45 serial port connector, which is located on the back of the appliance, to connect a console terminal (an ASCII terminal or PC running terminal-emulation software).

Use the thin, flat, RJ-45-to-RJ-45 rollover cable that comes with the appliance to connect the console port to an ASCII terminal or a PC running terminal-emulation software.

If you do not want to use the serial RJ-45 in the back, the Packet Analyzer appliance comes with a KVM connector that hooks to the front (see [Figure 1-1](#)). This connector splits off into two USB ports: a DB-9-male port and a DB15-female port. The Cisco Security Packet Analyzer 2400 series appliances is equipped with a DC power supply.

## Small Form-Factor Pluggable (SFP) Modules

The Cisco small form-factor pluggable (SFP) and SFP+ transceiver modules are hot-swappable input/output (I/O) devices that plug into module sockets. The transceiver connects the electrical circuitry of the module with the optical or copper network.

### Related Topics

For Information About...	See...
The transceiver types used by the SFP-based Cisco Security Packet Analyzer 2400 series appliances and their cable requirements	<a href="#">Table 1-2 on page 1-5</a>
SFP transceivers	<a href="#">Cisco SFP Optics for Packet-Over-Sonet/SDH and ATM Applications</a>
SFP+ transceivers	<a href="#">Cisco Small Form-Factor Pluggable Modules for Gigabit Ethernet Applications Data Sheet</a>

## KVM Console

The KVM console is an interface accessible from the Cisco UCS Manager GUI or the KVM Launch Manager that emulates a direct KVM connection. The KVM console allows you to view the serial console remotely without any connection to a terminal server. It also provides the “Virtual Media” feature used for recovery/ISO install.

If you want to use the KVM console to access the Packet Analyzer appliance, you must ensure that either the appliance or the service profile associated with the appliance is configured with a CIMC IP address. The KVM console uses the CIMC IP address assigned to an appliance or a service profile to identify and connect with the correct Packet Analyzer appliance.

- If the management subnet you are connected to has a DHCP server deployed, the CIMC will automatically receive an IP address. This address will be displayed during initial bootup and can be seen from a serial console connection or a VGA screen.
- If the management subnet you are connected to does *not* have a DHCP server, you must enter a static IP address by entering the CIMC configuration setup during bootup. To do this, press <F8> during initial bootup. After the address is set, the CIMC GUI and ssh connections will be available.

For more information about the KVM console, see the [Starting the KVM Console](#) section in the *Cisco UCS Manager GUI Configuration Guide*.

## AC Power Supplies

The Cisco Security Packet Analyzer 2400 series appliances are equipped with a wide input range AC power supply that supports both 110-V and 220-V.

For more information about the power supplies shipped with the Cisco Security Packet Analyzer 2400 series appliances see the [Power Specifications](#) section in the Cisco UCS C240 Server Installation and Service Guide for Packet Analyzer 2400 appliance.



### 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

---

There will not be any blanking panels for the power supplies but there will be blanking panels for the 16 disk configuration. The server has 24 disk slots, so with the 16 disk configuration, there will be 8 blanking panels.

# Summary of Appliance Features

## Cisco Security Packet Analyzer 2400 Feature

The Cisco Security Packet Analyzer 2400 appliance, which is based on UCS C220 M4 server, includes these features:

CPU	One Intel E5-2660 v3 (Haswell) 2.60 GHz 105W 10C/25MB Cache/DDR4 2133MHZ.
Memory	Two 32GB DDR4-2133-MHz LRDIMM/PC4-17000/quad rank/x4/1.2v.
Storage	24 2TB 2.5" enterprise class SAS 7.2K RPM HDD - two in RAID 1 for system and CDB files; the other six are in RAID 5 for capture.
Network and Management I/O	Cisco Security Packet Analyzer 2400 - 4x1G Napatech NT4E-4T-STD or NT4E-4-STD - Supports RJ-45 or 1G SFP modules. See section <a href="#">Small Form-Factor Pluggable (SFP) Modules, page 1-5..</a>
Disk Management	Cisco 12G SAS Modular Raid Controller with 4G flash-backed write cache module.
Optical Drive	None
Hardware Filters	None





# Installing the Cisco Security Packet Analyzer 2400 Series Appliances

---

This chapter provides the information you need to install your Cisco Security Packet Analyzer 2400 series appliances, including how to install hardware options, how to mount the Packet Analyzer appliance in a rack, cabling, and how to connect it to the network.

These instructions are intended for technicians who are experienced with installing, replacing, and removing the hardware components from electronic devices and are familiar with the Cisco Security Packet Analyzer 2400 series appliance. Additionally, site planners, network administrators, and facility maintenance personnel might also find this information helpful.

The installation and replacement of the hardware components of the Cisco Security Packet Analyzer 2400 series appliance involve many steps, most of which must be done in the order in which they are presented here. Each section explains one associated group of tasks upon which the next section's tasks are built.

This chapter contains the following sections:

- [Requirements and Restrictions, page 2-2](#)
- [Installation Process Summary, page 2-2](#)
- [Unpack and Inspect the Appliance, page 2-4](#)
- [Install the Appliance in a Rack, page 2-5](#)
- [Install the Transceiver Modules, page 2-6](#)
- [Connect the Power, page 2-7](#)
- [Connect the Appliance Cables, page 2-8](#)
- [Power Up the Appliance, page 2-12](#)

# Requirements and Restrictions

This section contains the requirements that are necessary for the product to run successfully:

- Plan your site configuration and prepare the site before installing the appliance. Cisco Security Packet Analyzer 2400 Series Appliances come preinstalled on a Cisco UCS C240 server, so for the recommended site planning tasks, see the [Cisco UCS Site Preparation Guide](#).
- For physical, environmental, and power requirements, including thermal (air conditioning), space, and power requirements, see [Appendix C, “Technical Specifications”](#). If available, you can use an uninterruptible power supply (UPS) to protect against power failures.
- Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current draw fluctuations from fluctuating data traffic patterns. Ensure that the cabinet or rack meets the requirements listed in the section, see [Install the Appliance in a Rack, page 2-5](#).

## Installation Process Summary

This section provides a summary of how to prepare and install the Cisco Security Packet Analyzer 2400 series appliances.



Warning

**Read the installation instructions before connecting the system to the power source.** Statement 1004



Warning

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



Warning

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



Warning

**This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017



Warning

**Power off the unit before you begin.** Statement 237



Warning

**To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules (such as power supplies, fans, or cards); these types of handles are not designed to support the weight of the unit.** Statement 1032



**Warning**

**Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.** Statement 4

**Warning**

**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.** Statement 1006

- 
- Step 1** Review the following:
- [Regulatory Compliance and Safety Information for the Cisco UCS C-Series Servers](#)
  - [Appendix B, “Safety Guidelines”](#)
- Step 2** Unpack and inspect each of the components for possible damage that might have occurred during shipping. Ensure that you have all required components.  
See [Unpack and Inspect the Appliance, page 2-4](#).
- Step 3** Install the Cisco Packet Analyzer 2400 appliance in a rack.  
See [Install the Appliance in a Rack, page 2-5](#).
- Step 4** Install the transceiver modules.  
See [Install the Transceiver Modules, page 2-6](#).
- Step 5** Connect the appliance to a power source.  
See [Connect the Power, page 2-7](#).
- Step 6** Connect the appliance cables.  
See [Connect the Appliance Cables, page 2-8](#)
- Step 7** Turn on the power.  
See [Power Up the Appliance, page 2-12](#)
- 

After completing the hardware installation, configure the appliance. See [Chapter 3, “Configuring the Cisco Security Packet Analyzer 2400 Series Appliances.”](#)

# Unpack and Inspect the Appliance

**Caution**

When handling internal appliance components, wear an ESD strap and handle modules by the carrier edges only.

**Tip**

Do not remove the appliance from its shipping container until you are ready to install it.

**Tip**

Do not discard the packaging materials used in shipping your Cisco Packet Analyzer 2400 appliance. You will need the packaging materials in the future if you move or ship your appliance.

**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.

To unpack and inspect the shipment:

---

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

**Step 2** Compare the shipment to the equipment list. Verify that you have all items.

The appliance, cables, and any optional equipment you ordered might be shipped in more than one container. When you unpack the containers, check the items against the packing list (see [Table 2-1](#)) to verify that you received all the parts.

**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 (see [Serial Number Locations, page A-5](#)) of the damaged unit
  - Description of damage
  - Effect of damage on the installation
-

## Cisco Cisco Security Packet Analyzer 2400 Appliance Packing List

The following table lists the items that ship with the Cisco Cisco Security Packet Analyzer 2400. A *Notes* section has been provided to record damaged or missing items.

**Table 2-1** Cisco Cisco Security Packet Analyzer 2400 Appliance Packing List

✓	Item
<input type="checkbox"/>	Cisco Cisco Security Packet Analyzer 2400 is pre-installed on a Cisco UCS C240 server
<input type="checkbox"/>	Power cable (customer chosen)
<input type="checkbox"/>	Cable assembly, Ethernet, RJ45-RJ45, Yellow, 6 ft.
<input type="checkbox"/>	CABASY, Console, RJ45/DB9
<input type="checkbox"/>	CABASY, RF, MICRO MINITURE, FOX 36P, 9P DSUB, USB, DONGLE CABLE
<input type="checkbox"/>	ASY, MECH, RAIL KIT, 1RU, SAVBU
<input type="checkbox"/>	<i>Cisco Prime Packet Analyzer Documentation Roadmap</i>

## Install the Appliance in a Rack

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-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 .38-inch (9.6 mm), round .28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per appliance must be two RUs, equal to 3.5 in. (88.9 mm).

The slide rails supplied by Cisco Systems for this appliance do not require tools for installation. The inner rails (mounting brackets) are pre-attached to the sides of the appliance.

Because the Cisco Security Packet Analyzer 2400 series appliances come pre-installed on a Cisco UCS C240 server, see The [Installing the Server In a Rack](#) section in the Cisco UCS C240 Server Installation and Service Guide for the recommended rack mounting tasks for Cisco Cisco Security Packet Analyzer 2400 Appliance.

# Install the Transceiver Modules

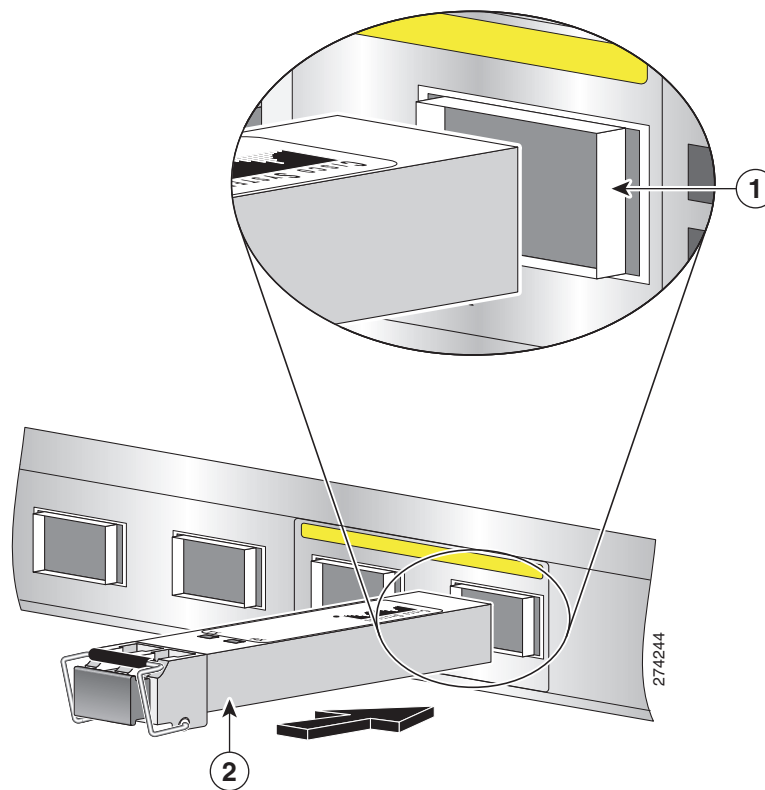
You can order SFP or SFP+ transceiver modules as hardware options or you can use modules you might already own as long as they meet the specifications described in the [data sheets](#) on Cisco.com. Because these modules are delicate devices, they are packaged separately and are not installed in the appliance prior to shipping.


**Caution**

Do not add labels or markings to the modules.

Figure 2-1 shows a detailed view of an SFP+ module installation.

**Figure 2-1** Installing an SFP+SFP Module



<b>1</b>	SFP+ slot in back panel	<b>2</b>	SFP+ positioned for back panel slot
----------	-------------------------	----------	-------------------------------------

To install an SFP or SFP+ module in a Cisco Security Packet Analyzer 2400 series appliance:

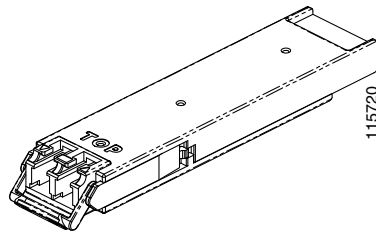
- Step 1** Locate the transceiver module you plan to install and remove any protective packaging.
- Step 2** Determine into which of the two slots on the rear panel of the Packet Analyzer appliance you will install the module.

The SFP and SFP+ modules use the bail clasp latching mechanism as shown unlatched in [Figure 2-2](#) and latched in [Figure 2-3](#).

- Step 3** With its latch open, slide the module into the slot until you feel resistance, then push it harder until you feel (or hear) it click into its socket.

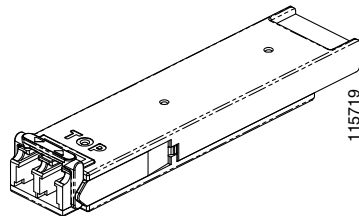
Figure 2-2 shows an example of a transceiver module with its latch open.

**Figure 2-2** Transceiver Module (unlatched)



- Step 4** With your finger, pull the latch upwards to lock the module into its slot.

**Figure 2-3** Transceiver Module (latched)



- Step 5** Plug in the fiber optical cable.

- Step 6** Observe the front-panel LEDs to verify that the connection is operating properly. (See “[Reading the LEDs](#)” section on page 5-1.)

---

To replace a transceiver module, see [Replacing Transceiver Modules](#), page 5-7.



---

**Note** If you use NIC card with RJ45 ports, do not install the transceiver modules.

---

## Connect the Power

When installing the Cisco Security Packet Analyzer appliance, use the AC power cord that was shipped with the Cisco Security Packet Analyzer 2400 series appliance.

The AC power cord is considered the primary disconnect for the appliance and must be readily accessible when installed. If the appliance power cord is not readily accessible to be disconnected, you must install an AC power disconnect for the entire rack. This disconnect must be readily accessible, and it must be properly labeled as the controlling power to the entire rack, not just to the appliance.

To connect the AC power to the Cisco Security Packet Analyzer 2400 series appliance:

- 
- Step 1** Review the [Safety with Electricity](#) information in the [Safety Guidelines](#) appendix.

**Step 2** Ground the rack.

To avoid the potential for an electrical shock, you must include a third wire safety ground conductor with the rack installation. If the appliance power cord is plugged into an AC outlet that is part of the rack, you must provide proper grounding for the rack itself. If the appliance power cord is plugged into a wall outlet, the safety ground conductor in the power cord provides proper grounding only for the appliance. You must provide additional, proper grounding for the rack.

**Step 3** Plug the AC power cord into the AC power input connector at the rear of the appliance (see [Figure 1-2](#)), and the other end of the power cord to a power source at your site.

The AC power cord is considered the primary disconnect for the appliance and must be readily accessible when installed. If the appliance power cord is not readily accessible to be disconnected, you must install an AC power disconnect for the entire rack. This disconnect must be readily accessible, and it must be properly labeled as the controlling power to the entire rack, not just to the appliance.

**Caution**

*Do not power on the unit yet.*

## Connect the Appliance Cables

This section describes how to connect cables to your Cisco Security Packet Analyzer 2400 series appliance. It includes the following topics:

- [Connect the Management Port](#)
- [Connect the Monitoring Ports](#)
- [Connect a Console Terminal](#)
- [Connect a Monitor to the Appliance](#)

## Connect the Management Port

The Cisco Security Packet Analyzer 2400 series appliance management port is the LAN 1 port, an RJ-45 10BASE-T/100BASE-TX/1000BASE-T network interface connector.

To connect the Cisco Security Packet Analyzer 2400 appliance management port:

**Step 1** Connect one end of a Cat5e (or better) UTP cable to the LAN 1 port on the appliance.**Step 2** Connect the other end of the cable to a hub or switch (a gateway) in your network.**Step 3** After connecting the management port, observe the front-panel LEDs to verify that the connection is operating properly. (See [Status LEDs and Buttons Section](#) [Status LEDs and Buttons Section](#) in the Cisco UCS C220C240 M4 Server Installation and Service Guide.)

## Connect the Monitoring Ports

You can connect the Cisco Security Packet Analyzer 2400 series appliance directly to a device to monitor, such as a switch or router, or you can connect a Packet Analyzer appliance between two devices using an optical tap device. The following topics describe these connection methods:

- [Direct Connections](#)
- [Optical Tap Connections](#)

### Direct Connections

In a typical Packet Analyzer installation, the Cisco Security Packet Analyzer 2400 series appliance receives switch or router traffic from the SPAN ports of the remote device.

To connect the Cisco Security Packet Analyzer 2400 series appliance directly to a device you want to monitor, such as a switch or router:

- 
- Step 1** Run a fiber optical cable from the port on the remote device to the transceiver module in the back panel of the Cisco Security Packet Analyzer 2400 series appliance.
- Step 2** Cisco Security Packet Analyzer 2400 has 10G ports. They support 1GbE SFP and 10GbE SFP+ modules. Be sure that the modules on both ends of a connection match. After connecting the appliance, observe the front-panel LEDs to verify that the connection is operating properly. (See [“Reading the LEDs” section on page 5-1.](#))

**Note**

You can only use the Ethernet cables, if you are using NIC with RJ45 / copper ports.

### Optical Tap Connections

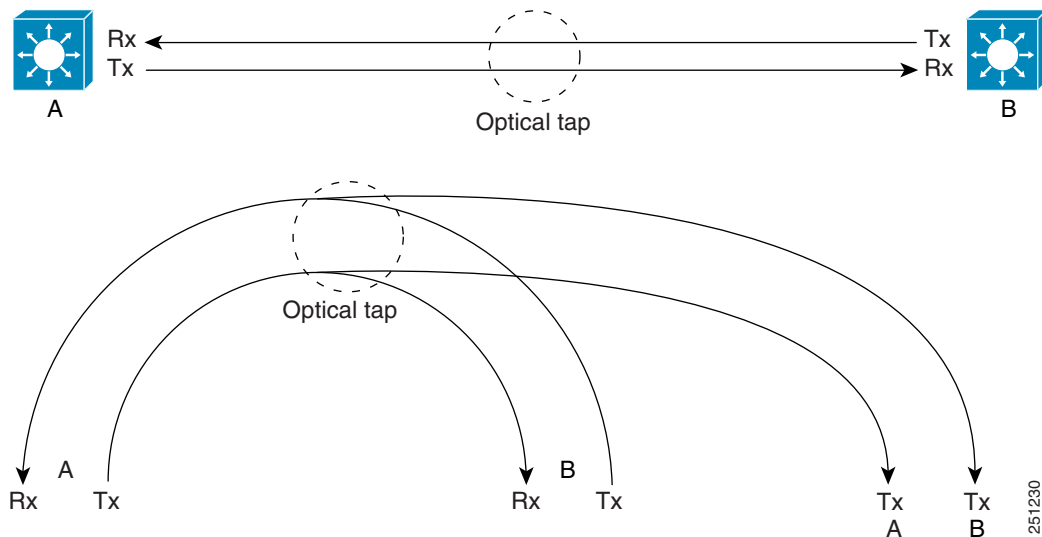
Another possible Packet Analyzer installation enables you to monitor traffic between two devices by locating the Cisco Security Packet Analyzer 2400 series appliance between the two devices. Using traffic tapping, the network tap passes the traffic between the two devices while mirroring each direction of traffic to one of the Packet Analyzer data ports.

You can connect the Cisco Security Packet Analyzer 2400 series appliance between two remote devices using an optical tap device. The optical tap mirrors the transmit sides of the cable that connects two remote devices as shown in [Figure 2-4](#).

**Note**

The optical tap connection requires two additional fiber optical cables.

Figure 2-4 Optical Tap Connection

**Note**

You can find optical tap and cable specifications in [Appendix C, “Technical Specifications.”](#)

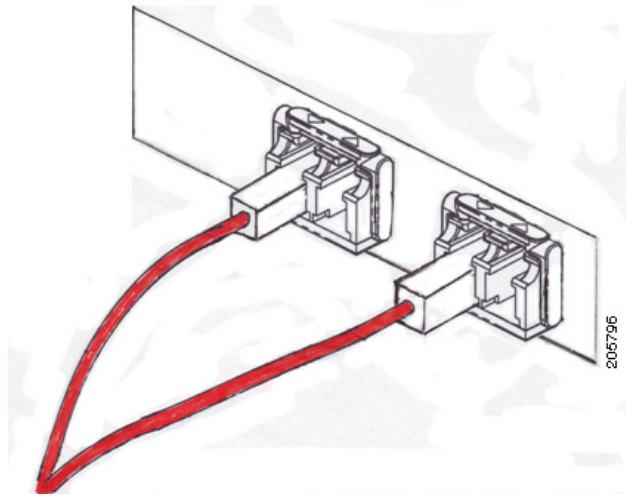
To use an optical tap to connect the Tx signals of two devices to the Cisco Security Packet Analyzer 2400 series appliance monitoring ports:

- Step 1** Disconnect the 10 GbE fiber optical cable that connects the two devices and plug the disconnected end of the cable into the appropriate ports on the optical tap for Device A.
- Step 2** Plug another 10 GbE fiber optical cable into the output port for Device B, then plug the other end into the appropriate ports on the optical tap for Device B.
- Step 3** Run a third 10 GbE fiber optical cable from the Tx A/Tx B ports on the optical tap device to the Cisco Security Packet Analyzer 2400 series appliance.
- Step 4** At the Cisco Security Packet Analyzer 2400 series appliance, separate the connectors at the end of the 10 GbE fiber optical cable.

The two connectors of the 10 GbE fiber optical cable plug into different SFPs enabling the appliance to monitor all traffic between the two devices. See [Figure 2-5](#) for an illustration of the fiber optical cable inputs to the SFPs for an optical tap configuration.



**Figure 2-5** Fiber Optical Cable Inputs for Optical Tap Configuration



- Step 5** Plug Device A's Tx connector into the left side of the SFP on the right (logical DataPort1).
- Step 6** Plug the Device B Tx connector into the left side of the SFP on the left (logical DataPort2).

To use breakout mode configuration, use an optical tap to split the Tx and Rx signals of two connected devices so the Packet Analyzer appliance receives the Tx of both devices to observe the transmitted output of each device.

There are two breakout mode configurations:

- Tx of one direction of the monitored data traffic is replicated on Tx of one breakout port and Tx of the other direction of the monitored data traffic is replicated on Tx of the other breakout port.

This case provides two output replicated ports: one for Tx in one direction and one for Tx of the other direction. Each replicated port is an input to a different monitoring port of the appliance to monitor both directions of traffic.

- Tx of one direction of the monitored data traffic is replicated in one Tx connection of the breakout port and Tx of the other direction of the monitored data traffic is replicated on the other Tx connection of the same breakout port.

This case provides only one replicated port which has Tx of both directions. This case requires you to split the connectors of one fiber optical cable and put one connector into one appliance monitoring port and put the other connector into a different appliance monitoring port.

## Connect a Console Terminal

You can connect a console terminal using a PC running terminal-emulation software to the console port on the Cisco Security Packet Analyzer 2400 series appliance in either of two ways:

- Connect the terminal using a rollover cable to the appliance console port (see [Figure 1-2](#)).  
The rollover cable is provided in the cables shipped with your appliance.
- Connect a terminal server to the appliance console port.

After connecting the console terminal, observe the front-panel LEDs to verify that the connection is operating properly. (See [“Reading the LEDs” section on page 5-1.](#))

Configure your terminal or terminal-emulation software as shown in [Table 2-2.](#)

**Table 2-2 Terminal Configuration**

Baud rate	9600
Data bits	8
Parity	No
Stop bit	1
Hardware flow control	Off

## Connect a Monitor to the Appliance

You might want to connect a monitor to the Cisco Security Packet Analyzer 2400 series appliance, but it is not required; you can establish a console connection to the Packet Analyzer appliance in other ways. The Cisco Security Packet Analyzer 2400 series appliance supports a VGA monitor.

The VGA monitor connector is located on the back panel of the appliance (see [Figure 1-2.](#))

After connecting the monitor cable, observe the front-panel LEDs to verify that the connection is operating properly. (See [“Reading the LEDs” section on page 5-1.](#))

## Power Up the Appliance

After you have completed all connections for the Cisco Security Packet Analyzer 2400 series appliance, you can turn on AC power. The power switch is located on the front panel (see [Figure 1-1.](#))

After the operating system boots up, observe the front-panel LEDs to verify that your system is operating properly. (See [“Reading the LEDs” section on page 5-1.](#))



# Configuring the Cisco Security Packet Analyzer 2400 Series Appliances

---

This chapter describes how to configure the Cisco Security Packet Analyzer 2400 series appliances to establish network connectivity, configure IP parameters, and how to perform other required administrative tasks using the Packet Analyzer command line interface (CLI). This chapter also provides information about how to get started with the Packet Analyzer graphical user interface (GUI) and how to perform various system management tasks.

This chapter contains the following sections:

- [Logging In For the First Time](#)
- [Changing the Root Password](#)
- [Resetting the Packet Analyzer Root Password to the Default Value](#)
- [Establishing Network Connectivity](#)
- [Checking Your Configuration](#)
- [Enabling the Cisco Security Packet Analyzer Web Server](#)
- [Enabling the Cisco Security Packet Analyzer Web Server](#)
- [Configuring a Monitored Device](#)
- [Opening and Closing a Telnet or SSH Session to the Packet Analyzer](#)
- [Setting up the CIMC](#)
- [Shutting Down and Starting Up the Appliance](#)

For more advanced Packet Analyzer configuration information, use the Packet Analyzer web server interface or see the [Network Analysis Module Command Reference](#).

## Logging In For the First Time

After you turn power on and boot the Cisco Security Packet Analyzer 2400 series appliance for the first time, the login prompt displays on the attached console. When shipped from the factory, the root user is preconfigured on the Cisco Security Packet Analyzer 2400 series appliance. The default password for the root user is *root*.



**Note**

---

You must change the user root password during the first login session.

---

The root user has access to the root (read/write) level of Packet Analyzer and can enter Packet Analyzer command-line interface (CLI) commands.

To log in to the Cisco Security Packet Analyzer 2400 series appliance for the first time, open a console session or a serial session with the Cisco Security Packet Analyzer appliance.

**Note**

After your initial login, you can enable **telnet** and **ssh** connections to the Packet Analyzer appliance.

**Step 1** When the Packet Analyzer login prompt appears, type **root** and press **Enter**.

```
secpa.localdomain login: root
```

**Step 2** When the password prompt appears, type **root** and press **Enter**.

After you enter the ID and password, you will be prompted to change the root password.

```
secpa2400-209.localdomain login: root
Password: <secpa1>
Last login: Mon Aug 20 08:28:34 2012 from sjc-vpn2-1516.cisco.com on pts/1
```

```
Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.
```

```
System_Alert! Default password has not been changed!
Please enter a new root user password.
Enter new password:
```

**Step 3** Enter the new password for the root user, then enter it a second time.

```
Confirm new password:
Successfully changed password for user 'root'
```

We recommend that you make a record of the password, and store this information in a secure location. You should change this password regularly in accordance with your site's password security policies. See [Changing the Root Password, page 3-2](#).

## Changing the Root Password

This section describes how to change the root user password after the initial login session. To change the root password:

**Step 1** Open a console session or serial session with the Cisco Security Packet Analyzer appliance.

**Step 2** When prompted for a username, enter **root**.

The Cisco Security Packet Analyzer 2400 appliance ships from the factory with default settings for user **root** with a password of **root**.

**Step 3** When prompted, enter the password for user root.

After you log in as the root user, you have read and write access to the root level of the Cisco Security Packet Analyzer appliance, and you can enter and perform CLI commands.

```
root@hostname#
```

**Step 4** Enter the following command to change the root user password.

```
password root

New password:
Confirm password:
```

**Step 5** Enter the new password for user root and confirm it.

We recommend that you make a record of the password and store this information in a secure location. You should change this password regularly in accordance with your site's password security policies.

**Step 6** Type **exit** to end the session and log out.

---

## Examples

This section provides the following examples:

- [Changing the Packet Analyzer Root Password: Example, page 3-3](#)
- [Verifying the Packet Analyzer Root Password: Example, page 3-3](#)

### Changing the Packet Analyzer Root Password: Example

```
root@secpa2400-209.localdomain# password root
Enter new password:
Confirm new password:
Successfully changed password for user 'root'
```

### Verifying the Packet Analyzer Root Password: Example

```
nam1.company.com login: root
Password: <secpa1>
Terminal type: vt100

Cisco Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

root@nam1.company.com#
root@nam1.company.com# exit
```

## Resetting the Packet Analyzer Root Password to the Default Value

For information about how to reset the Packet Analyzer root password to the default value, see the [Cisco Prime Network Analysis Module Software User Guide](#).

# Establishing Network Connectivity

This section describes how to configure a Cisco Security Packet Analyzer 2400 appliance to configure IP parameters in IPv4 environment to establish network connectivity.

Log in to a Cisco Security Packet Analyzer 2400 appliance from the management console and enter the following CLI commands with the appropriate information for your site:

- Step 1** Use the **ip address** command to configure the Cisco Security Packet Analyzer appliance IP address. The syntax for this command is as follows:

```
ip address ip-address subnet-mask
```

### Example

```
root@localhost# ip address 172.20.104.126 255.255.255.248
```

- Step 2** Use the **ip gateway** command to configure the Cisco Security Packet Analyzer appliance default gateway address. The syntax for this command is as follows:

```
ip gateway ip-address
```

### Example

```
root@localhost# ip gateway 172.20.104.123
```

- Step 3** You can use the **exsession** command to enable remote login to the Cisco Security Packet Analyzer appliance using either Telnet or SSH. The syntax for this (optional) command is as follows:

```
exsession on (for Telnet)
```

or

```
exsession on ssh (for SSH)
```

### Examples

To configure the Cisco Security Packet Analyzer appliance to enable Telnet access:

```
root@localhost# exsession on
```

To configure the Cisco Security Packet Analyzer appliance to enable SSH access:

```
root@localhost# exsession on ssh
```

- Step 4** You can use the **ip domain** command to configure the Cisco Security Packet Analyzer appliance system domain name. The syntax for this (optional) command is as follows:

```
ip domain name
```

### Example

```
root@localhost# ip domain your_company.com
```

**Step 5** You can use the **ip host** command to configure the Cisco Security Packet Analyzer appliance system hostname.

The syntax for this command is as follows:

```
ip host name
```

#### Example

```
root@localhost# ip host secpa_machine
```

**Step 6** You might (optionally) want to use the **ip nameserver** command to configure one or more name servers for the Cisco Security Packet Analyzer appliance.

The syntax for this command is as follows:

```
ip nameserver ip-address [ip-address] [ip-address]
```

#### Examples

```
root@localhost# ip nameserver 172.20.104.10
```

```
root@localhost# ip nameserver 172.20.104.10 172.20.104.20 172.20.104.30
```

## Checking Your Configuration

After you finish configuring the Cisco Security Packet Analyzer appliance for network connectivity, it is a good idea to check your connectivity and verify the IP parameters you have just configured for the Cisco Security Packet Analyzer appliance.

**Step 1** Use the **ping** command to check connectivity between the Cisco Security Packet Analyzer appliance and a network device.

The syntax for this command is as follows:

```
ping {hostname | ip-address}
```

#### Examples

```
root@localhost# ping secpa_machine.your_company.com
```

```
root@localhost# ping 172.20.104.10
```

The following is an example of the **ping** command showing successful connectivity:

```
root@secpa_machine.your_company.com# ping 172.20.104.10
PING 172.20.104.10 (172.20.104.10) 56(84) bytes of data.
 64 bytes from 172.20.104.10: icmp_seq=1 ttl=254 time=1.27 ms
 64 bytes from 172.20.104.10: icmp_seq=2 ttl=254 time=1.13 ms
 64 bytes from 172.20.104.10: icmp_seq=3 ttl=254 time=1.04 ms
 64 bytes from 172.20.104.10: icmp_seq=4 ttl=254 time=1.08 ms
 64 bytes from 172.20.104.10: icmp_seq=5 ttl=254 time=1.11 ms

--- 172.20.104.10 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4003ms
 rtt min/avg/max/mdev = 1.043/1.129/1.278/0.090 ms
root@secpa_machine.your_company.com#
```

**Step 2** Use the **show ip** command to verify that you have configured the Cisco Security Packet Analyzer appliance IP parameters the way you want them.

The syntax for this command is as follows:

**show ip**

```
root@localhost# show ip root@nam1.company.com# show ip
```

The following is an example of the **show ip** command output that shows a configured Cisco Security Packet Analyzer appliance:

```
root@secpa-2400-96.cisco.com# show ip

==== IP/DNS Configuration ====
IPv4 Address/Netmask: 172.20.124.96 / 255.255.255.0
IPv4 Default Gateway: 172.20.124.47
IPv4 Broadcast:      172.20.124.255
IPv6 Address:        2001:20:1:100::96/64
IPv6 Default Gateway: 2001:20:1:100::1
Host Name:           appliance-2404-96.cisco.com
Nameserver(s):      171.70.168.183

==== Remote Access & Authentication ====
HTTP:                Enabled (on port 80)
HTTPS:               Disabled
SSH:                 Enabled (on port 22)
Telnet:              Enabled (on port 23)
TACACS+:             Disabled

==== File Sharing Services ====
SMB:                 Disabled
SFTP:                Disabled
```

## Enabling the Cisco Security Packet Analyzer Web Server

This section describes how to enable the Cisco Security Packet Analyzer web server and browser-based access to the Packet Analyzer graphical user interface (GUI).



**Note**

You can enable the Packet Analyzer to function as an HTTP server or an HTTPS secure server, but not as both simultaneously.

To enable the Packet Analyzer web server and provide browser-based access, confirm that your web browser supports your Packet Analyzer software release.



**Note**

For a list of supported browsers, see the [Cisco Security Packet Analyzer software release notes](#).



To enable the Packet Analyzer web server:

- Step 1** Open a Telnet or SSH session to the Cisco Security Packet Analyzer appliance and at the password prompt, enter your password.

```
telnet {ip-address | hostname}
```

or

```
ssh {ip-address | hostname}
```

- Step 2** Enter one of the following commands to enable either an HTTP server or an HTTPS secure server:  
To enable the Packet Analyzer HTTP web server:

```
ip http server enable
```

To enable the Packet Analyzer HTTPS secure web server:

```
ip http secure server enable
```

The Packet Analyzer requests a web administrator user name.

```
Enabling HTTP server...
```

```
No web users are configured.
```

```
Please enter a web administrator user name [admin]: <CR>
```

The Packet Analyzer web server requires at least one properly-configured web administrator. If the Packet Analyzer does not prompt you for a web username and password, then at least one web administrator was previously configured.

- Step 3** Enter the username of the web administrator. Otherwise, press **Enter** to use the default web administrator username *admin*.

The Packet Analyzer requests a password for the web administrator, then requests the password to be entered again to ensure accuracy.

```
New password: <adminpswd>
```

```
Confirm password: <adminpswd>
```

- Step 4** Enter the password for the web administrator and confirm it.



**Note**

Because this document is available to the public by way of Cisco.com, it is a good idea to change this and all default passwords as soon as possible.

- Step 5** To check the Packet Analyzer web server functionality, launch an approved internet browser and enter the IP address or host and domain name in the browser address field.



**Note**

For a list of supported browsers, see the [Cisco Security Packet Analyzer software release notes](#).

If the Cisco Security Packet Analyzer 2400 series appliance web server is properly configured, you should access the Packet Analyzer login window.

At this point, the only user able to log in to the Packet Analyzer web server is the administrative user you configured when you enabled the web server.

## Verifying System Status

To verify the status of an installation, upgrade, or downgrade or to troubleshoot problems, use commands from those listed in [Table 3-1, Common Diagnostic and Show Commands](#).



### Note

- The tables in these sections show only common managed device and network module commands.
  - To view a complete list of available commands, type `?` at the prompt (Example: `user@secpa_host.domain# ?`).
  - To view a complete list of command keyword options, type `?` at the end of the command (Example: `secpa_host.domain# ip ?`).
- The tables group commands by the configuration mode in which they are available. If the same command is available in more than one mode, it might act differently in each mode.



### Note

Many **show** commands include the keyword option to display diagnostic output on your screen or to pipe it to a file or a URL.

**Table 3-1 Common Diagnostic and Show Commands**

Command	Purpose
<b>clear access-log</b>	Clear web access log.
<b>clear captured-data-files</b>	Delete all captured files in Packet Analyzer local drive.
<b>clear monitoring-data</b>	Delete all monitoring data on Packet Analyzer.
<b>clear system-alerts</b>	Clear system alerts.
<b>clear system-passwords</b>	Restore default CLI passwords of application image.
<b>ping</b>	Pings a specified IP address or hostname to check network connectivity.
<b>show access-log</b>	Displays the web access log.
<b>show application</b>	Displays the protocol grouping information.
<b>show audit-trail</b>	Displays the web GUI logins and CLI access settings.
<b>show autocreate-data-source</b>	Displays the data source autocreation settings.
<b>show cdb</b>	Displays information about a CDB file.
<b>show cdp settings</b>	Displays the CDP settings.
<b>show certificate</b>	Displays installed certificate.
<b>show certificate-request</b>	Displays certificate signing request.
<b>show clock</b>	Displays the current date and time.

**Table 3-1 Common Diagnostic and Show Commands (continued)**

<b>Command</b>	<b>Purpose</b>
<b>show configuration</b>	Displays the current bootloader configuration as entered using the <b>configure</b> command.
<b>show data-source</b>	Displays the data sources.
<b>show date</b>	Displays the current date and time.
<b>show debug</b>	Displays the debug information.
<b>show device</b>	Displays the remote devices.
<b>show email</b>	Displays EMail settings.
<b>show entity</b>	Displays the entity MIB information.
<b>show flow-cache-sizes</b>	Displays the Packet Analyzer internal cache sizes.
<b>show ftp</b>	Displays the FTP settings for schedule reports.
<b>show hosts</b>	Displays the hosts entries.
<b>show inventory</b>	Displays the system inventory information.
<b>show ip</b>	Displays the IP parameters.
<b>show local-storage all</b>	Displays all physical disks and virtual drives.
<b>show local-storage physical</b>	Displays all physical disks.
<b>show local-storage progress</b>	Displays progress of drive rebuilds.
<b>show local-storage virtual</b>	Displays all virtual drives.
<b>show log</b>	Displays the Packet Analyzer config, patch, report, and upgrade logs
<b>show memory</b>	Displays the amount of installed memory, amount available, and the amount currently used by the system.
<b>show monitor</b>	Displays the configured collections.
<b>show patches</b>	Displays any installed patches.
<b>show preferences</b>	Displays the Packet Analyzer web interface preferences.
<b>show protocol-feature</b>	Displays the parsing protocol feature settings.
<b>show remote-storage</b>	Displays the remote storage settings for storing capture data.
<b>show snmp</b>	Displays the SNMP parameters.
<b>show syslog-settings</b>	Displays the Packet Analyzer syslog settings.
<b>show system-alerts</b>	Displays Packet Analyzer failures and problems.
<b>show tech-support</b>	Displays general information about the host router that is useful to Cisco technical support for problem diagnosis.
<b>show time</b>	Displays the Packet Analyzer system time settings.
<b>show trap-dest</b>	Displays the Packet Analyzer trap destination.
<b>show version</b>	Displays information about the loaded router, software or network module bootloader version, and also hardware and device information.
<b>show waas</b>	Displays WAAS devices and data sources.

**Table 3-1 Common Diagnostic and Show Commands (continued)**

Command	Purpose
<code>show web-publication</code>	Displays web publication settings.
<code>show web-users</code>	Displays a list of current local web users.

## Configuring a Monitored Device

After you connect an output interface of a monitored (or managed) device to the monitoring ports of the Cisco Security Packet Analyzer 2400 series appliance, you must also configure the monitored device to send data to that interface. You do this in two steps:

- [Configuring a Monitored Device Interface](#)
- Span the port of the monitored device to use the Cisco Security Packet Analyzer 2400 series appliance as a destination port

## Configuring a Monitored Device Interface

At the monitored device, configure the connection to the Cisco Security Packet Analyzer 2400 series appliance as a trunk port, but use the `no negotiate` option. Using the `no negotiate` option on the monitored device, precludes the switch or router from performing dynamic trunk protocol (DTP) with the appliance monitoring port.

The following example shows how to configure a switch port connected to the appliance monitoring port as Te 7/29.

From the monitored device command line, enter a CLI command like the following:

```
show run interface ethernet 4/37
```

```
n7k-4# show run int ethernet 4/37
!Command: show running-config interface Ethernet4/37
!Time: Mon Apr 27 09:49:03 2015

version 7.2(0)D1(1)

interface Ethernet4/37
  description "Connected to secpa data port"
  switchport
  switchport monitor
  mtu 9216
```

## Creating a SPAN Session

A SPAN session is required to SPAN the monitored device's traffic to the port connected to the monitoring port of the appliance. You can create a SPAN session using the monitored device's CLI or using the Packet Analyzer appliance GUI.

For information about how to use the Packet Analyzer GUI to set up the SPAN session, see the [Cisco Security Packet Analyzer User Guide](#).

# Opening and Closing a Telnet or SSH Session to the Packet Analyzer

This procedure opens and closes a Telnet or SSH session to the Packet Analyzer. This procedure is not commonly performed, because you would typically use the Packet Analyzer GUI to monitor and maintain the Packet Analyzer. If, however, you cannot access the Packet Analyzer GUI, you might want to use Telnet or SSH to troubleshoot from the Packet Analyzer CLI.

If your Cisco Security Packet Analyzer 2400 series appliance is not properly configured for Telnet or SSH access (see the following [Prerequisites](#), page 3-11 section), you can open a Telnet session to the managed device to which the Cisco Security Packet Analyzer 2400 series appliance is connected, then open a Packet Analyzer console session from the managed device.

## Prerequisites

- Configure the Packet Analyzer system IP address. Optionally, set the Packet Analyzer system hostname.
- Verify Packet Analyzer network connectivity by performing one of the following ping tests:
  - From a host beyond the gateway, ping the Packet Analyzer system IP address.
  - From the Packet Analyzer CLI, ping the Packet Analyzer system default gateway.

## Telnet Prerequisites

- Enter the **exsession on** Packet Analyzer CLI command.

## SSH Prerequisites

- Enter the **exsession on ssh** Packet Analyzer CLI command.

## Summary Steps

1. **telnet** {*ip-address* | *hostname* }  
or  
**ssh** {*ip-address* | *hostname* }
2. At the login prompt, enter **root**.
3. At the password prompt, enter your password.  
or  
If you have not changed the password from the factory-set default, enter **root** as the root password.
4. Perform the tasks that you need to perform in the Packet Analyzer CLI. When you want to end the Telnet or SSH session to the Packet Analyzer and return to the Cisco IOS CLI, complete [Step 5](#) and [Step 6](#).
5. **exit**
6. **logout**

## Detailed Steps

	Command or Action	Purpose
Step 1	<p><b>telnet</b> {ip-address   hostname} or <b>ssh</b> {ip-address   hostname}</p> <p><b>Example:</b> host.domain# telnet 10.20.30.40</p> <p><b>Example:</b> host.domain# ssh 10.20.30.40</p>	<p>Logs in to a host that supports Telnet.</p> <p>or</p> <p>Starts an encrypted session with a remote networking device.</p> <ul style="list-style-type: none"> <li>Use the Packet Analyzer system IP address or Packet Analyzer system hostname.</li> </ul>
Step 2	<p>At the login prompt, enter <b>root</b>.</p> <p><b>Example:</b> login: root</p>	Accesses the root (read/write) level of Packet Analyzer.
Step 3	<p>At the password prompt, enter your password.</p> <p>or</p> <p>If you have not changed the password from the factory-set default, enter <b>root</b> as the root password.</p> <p><b>Example:</b> Password: root</p>	
Step 4	<p>Perform the tasks that you need to perform in the Packet Analyzer CLI. When you want to end the Telnet or SSH session to the Packet Analyzer and return to the Cisco IOS CLI, complete <a href="#">Step 5</a> and <a href="#">Step 6</a>.</p>	For help using Packet Analyzer CLI commands.
Step 5	<p><b>exit</b></p> <p><b>Example:</b> root@localhost(sub-custom-filter-capture)# exit root@localhost#</p>	<p>Leaves a subcommand mode.</p> <ul style="list-style-type: none"> <li>Return to command mode.</li> </ul>
Step 6	<p><b>logout</b></p> <p><b>Example:</b> root@localhost# logout</p> <p>Connection closed by foreign host.</p>	Logs out of the Packet Analyzer system.

## Examples

## Opening and Closing a Telnet Session to the Packet Analyzer Using the Packet Analyzer System IP Address

```
secpa_host> telnet 172.20.105.215
Trying 172.20.105.215 ... Open
```

```
Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
```

```

Copyright (c) 2012-2016 by Cisco Systems, Inc.

login: root
Password: <password>
Terminal type: vt100

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

WARNING! Default password has not been changed!
root@secpa.company.com#
root@secpa.company.com# logout

[Connection to 172.20.105.215 closed by foreign host]
secpa_host>

```

### Opening and Closing an SSH Session to the Packet Analyzer Using the Packet Analyzer System Hostname

```

host [/home/user] ssh -l root@namappl
root@namappl's password: <password>
Terminal type: vt100

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

WARNING! Default password has not been changed!
root@secpa.company.com#
root@secpa.company.com# logout

Connection to secpa closed.
host [/home/user]

```

## Setting up the CIMC

The Cisco Integrated Management Controller (CIMC) is a built-in feature of Cisco UCS servers that provides a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server remotely. The Cisco Security Packet Analyzer 2400 series appliances are based on the Cisco UCS server platform, and thus include the CIMC functionality.

While setting up the CIMC is not strictly necessary to use the Packet Analyzer, certain administrative and troubleshooting tasks can only be performed via the CIMC. Therefore, it is highly recommended to configure the CIMC with an IP address so that it can be accessed if needed.

To configure an IP address for the CIMC, reboot the Cisco Security Packet Analyzer appliance and press F8 when prompted to enter the “Cisco IMC Configuration Utility”. Set the “NIC mode” to “Shared LOM”, and configure the IP and VLAN parameters as appropriate. For more details on the CIMC configuration process, see the [Cisco UCS C240 M3 Server Installation and Service Guide](#).

You can also setup a dedicated CIMC connection using the UCS management port labeled M.



#### Note

The UCS management port labeled M is different from Packet Analyzer management port LAN1.

## Setting up Serial Console Connection

There are two ways to connect to the Packet Analyzer serial console:

- Serial over LAN (SoL)—Allows access to the Packet Analyzer serial console through the web-based GUI or SSH-based CLI of CIMC. This access method is configured by default.
- Physical external serial console connector (RJ-45)—Allows access to the Packet Analyzer serial console through a direct serial cable or terminal server. See section [Setting up Serial Console Access through External RJ-45 Port](#), page 3-14 for details.

Packet Analyzer supports two serial console ports: com0 and com1. The Packet Analyzer CLI can be accessed through either of these ports. However, only the com0 port provides full output and interactivity during the bootup process. The two serial console options (SoL or RJ-45 connector) cannot use com0 at the same time, so you should assign com0 to the option you would customarily use within your environment. By default, the Packet Analyzer is configured with SoL on com0, so if SoL is your preferred method of access, then you need not do anything more. If you prefer to assign com0 to the RJ-45 serial port, then follow the steps in section [Setting up Serial Console Access through External RJ-45 Port](#).

### Setting up Serial Console Access through External RJ-45 Port

See [Figure 5-2](#) for Serial connector (RJ-45) location.

To setup serial console access through the external RJ-45 port:

- 
- Step 1** Log into the CIMC GUI.
  - Step 2** Click the **Server** tab and then click **Remote Presence**.
  - Step 3** Click the **Serial over LAN** tab.
  - Step 4** If you do not want to use Serial over LAN, uncheck the **Enabled** check box. This will make the serial console accessible on com0 through the RJ-45 port. Alternatively, if you prefer to use the RJ-45 serial console primarily, but maintain Serial over LAN as a secondary method for access to the Packet Analyzer CLI, then keep Serial over LAN enabled, but change **Com Port** to com1.
  - Step 5** Click the **Save Changes** button.

Console access through the RJ-45 console port will be enabled. Configure your terminal emulator or terminal server to use 9600 baud/bps, 8-N-1 when connecting to the console.

In some cases, it may be necessary to power cycle the Packet Analyzer appliance before the serial console works. From the CIMC GUI, click the **Server** tab and click **Summary**, and then click **Power Cycle Server**.

---

## Shutting Down and Starting Up the Appliance

To shut down a Cisco Security Packet Analyzer 2400 series appliance, issue the Packet Analyzer CLI **shutdown** command.

The Cisco Security Packet Analyzer 2400 series appliance reboots after you press the Power button. You can also switch on the server through the CIMC web interface.





## Installing and Configuring External Storage

---

This section describes how to manually prepare your external iSCSI storage information to work with Packet Analyzer. It contains the following topics:

- [Configuring the iSCSI Array](#)
- [Locating the Packet Analyzer IQN](#)
- [Connecting the Storage Array](#)

### Configuring the iSCSI Array

Use your vendor's user guide to ensure you have properly configured the iSCSI array. The Packet Analyzer is independent of most array settings, but some are important for accessibility and performance.

- 
- Step 1** To configure the Logical Unit Numbers (LUNs) on the array, there is often a Segment Size setting. Larger segment sizes can improve write speeds. Configure the Segment Size setting to use the largest possible segment size (up to 512KB).
- Multiple LUNs can be configured on a single array.
- Step 2** Map the LUNs to iSCSI Qualified Names (IQNs) on the array. Each IQN represents a different list of LUNs for hosts (such as the Packet Analyzer) to access.
- Step 3** The Packet Analyzer supports up to 32 LUNs between all protocols. Multiple LUNs can be mapped to one IQN.
- Step 4** The Packet Analyzer also has an IQN, which represents the host side of an iSCSI session. Be sure you map each Packet Analyzer's IQN to the LUNs for host read-write access. Most storage arrays require this for security reasons, to ensure that only certain hosts can access the LUNs. Each Packet Analyzer has a unique IQN, so perform this step for each Packet Analyzer that requires access and for each target LUN that is to be accessed. For more details about which CLI command to use, see [Locating the Packet Analyzer IQN, page 4-2](#).
- Step 5** Set the IP path to the Packet Analyzer management port. For details, see [Connecting the Storage Array, page 4-2](#).
-

## Locating the Packet Analyzer IQN

To find the Packet Analyzer IQN, use the **remote-storage iscsi local-iqn** CLI command:

```
root@secpa.domain# remote-storage iscsi local-iqn
```

```
Local iSCSI Qualified Name: iqn.1967-04.com.cisco:SEC-PA-2400-K9.00:19:55:07:15:9A
```

## Connecting the Storage Array

After you configure the iSCSI storage arrays, be sure that it has an IP path to the Packet Analyzer management port. The array can be connected while the Packet Analyzer is running.

Some arrays come with multiple storage controller modules. As a security feature, module ownership must often be mapped to each LUN.

The Packet Analyzer logs into the storage to start an iSCSI session using the IP address and IQN(s) of the storage array. To connect the storage array using the user interface, follow these steps:

---

**Step 1** Log into the Packet Analyzer web interface. To access the Data Storage page, select **Capture > Packet Capture/Decode > Data Storage**.

**Step 2** Click the **iSCSI Login** button and enter the target IP and IQN.

The storage table refreshes with the newly discovered LUNs.

If the LUNs do not appear:

- a. Check **remote-storage iscsi list** to verify the iSCSI session was properly started.

The follow example shows how to verify the iSCSI session.

```
root@secpa.domain# remote-storage iscsi list
Storage ID: 16
Label:
Status: Ready
  Protocol: iSCSI
  Target IP: 172.20.10.82
Target IQN: iqn.2015-04:celermas.target18
Type: LUN
Model: IET VIRTUAL-DISK
LUN: 4
  Capacity: 24.98GB
  Available: 24.98GB
Active iSCSI Sessions:
tcp: [8] 172.20.10.82:3260,1 iqn.2015-04:celermas.target18
```

The LUN number (in the above example, LUN 4) can help you identify one LUN from others of the same IQN. This number is unique to each IQN, meaning two LUNs from different IQNs can have the same number.

- b. If the iSCSI session was properly started, check the storage array configuration to verify that:
  - The LUNs are mapped to the target IQN, and
  - The Packet Analyzer IQN has been given Read/Write access to the LUNs.
- c. If you make any configuration changes, logout of the iSCSI session and login again. To logout, use the CLI **remote-storage iscsi logout**. If the LUNs appear on the user interface, you can select one of them and click **iSCSI Logout**. All LUNs mapped to that target IQN will be disconnected.

You can now use the iSCSI external storage from within the Packet Analyzer. For more information, see the [Cisco Security Packet Analyzer Software User Guide](#).

---





# Maintaining the Cisco Security Packet Analyzer 2400 Series Appliances

This chapter provides instructions for maintaining your Cisco Security Packet Analyzer 2400 series appliance.

These instructions are intended for technicians who are experienced with installing, replacing, and removing the hardware components from electronic devices and are familiar with the Cisco Security Packet Analyzer 2400 series appliances. Additionally, site planners, network administrators, and facility maintenance personnel might also find this chapter helpful.

This chapter contains the following sections:

- [General Maintenance Guidelines](#)
- [Reading the LEDs](#)
- [Replacing Appliance Components](#)
- [Removing or Replacing the Cisco Security Packet Analyzer 2400 Series Appliances](#)

## General Maintenance Guidelines

For information about general maintenance tasks, see the *Preparing the Site* section in the *Cisco UCS Site Preparation Guide*.

## Reading the LEDs

There are several LEDs on a Cisco Security Packet Analyzer 2400 series appliance. LEDs serve the following purposes:

- Indicate that basic power is available to the appliance
- Guide you to a broken adapter card, or to one that has failed its diagnostics
- Give an indication that traffic is flowing through the adapter card to the appliance

The LEDs on the front panel of the Cisco Security Packet Analyzer 2400 series appliance and corresponding adapter card are aids for determining appliance and adapter performance and operation.

This section describes the location and meaning of LEDs and buttons and includes the following topics:

- [Cisco Packet Analyzer 2400 LEDs](#)

- Reading the NIC LEDs
- Reading the AC Power Supply LED

## Cisco Packet Analyzer 2400 LEDs

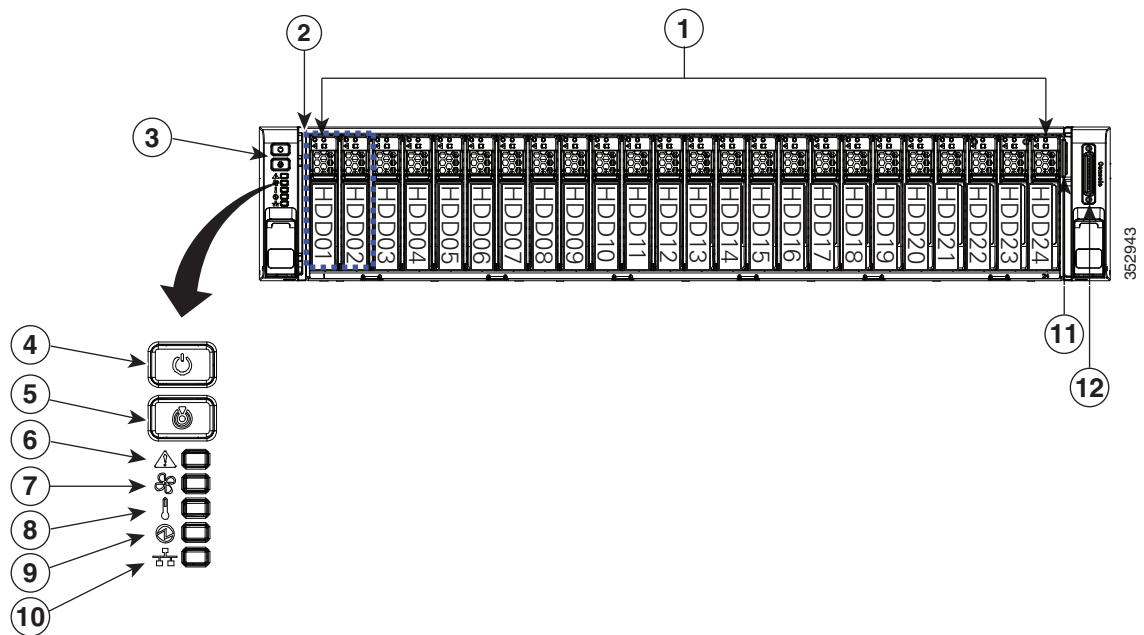
These sections describe the location and meaning of the LEDs for the Cisco Security Packet Analyzer 2400 appliance.

### Cisco Security Packet Analyzer 2400

Packet Analyzer 2400

Figure 5-1 shows the front-panel LEDs for the Cisco Packet Analyzer 2400. Table below defines the LED states

**Figure 5-1 Cisco Security Packet Analyzer 2400 Front-Panel LEDs**



1	Drive bays 1–24 (up to 24 2.5-inch drives)	7	Temperature status LED
2	Operations panel buttons and LEDs	8	Power supply status LED
3	Power button/LED	9	Network link activity LED
4	Unit Identification button/LED	10	Pull-out asset tag
5	System status LED	11	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
6	Fan status LED		

**Table 5-1 Cisco Security Packet Analyzer 2400 Front-Panel LEDs**

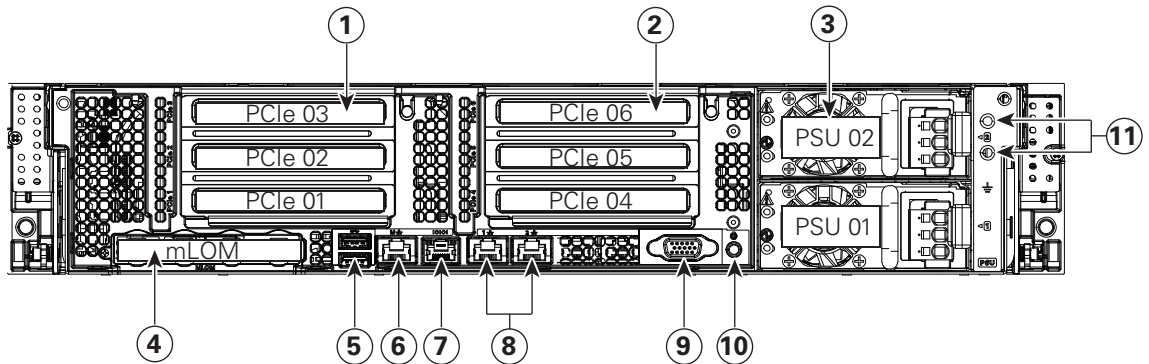
LED Name	State
Power button/Power status LED	<ul style="list-style-type: none"> <li>• Off—There is no AC power to the appliance.</li> <li>• Amber—The appliance is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.</li> <li>• Green—The appliance is in main power mode. Power is supplied to all appliance components.</li> </ul>
Identification	<ul style="list-style-type: none"> <li>• Off—The Identification LED is not in use.</li> <li>• Blue—The Identification LED is activated.</li> </ul>
Cisco Security Packet Analyzer status	<ul style="list-style-type: none"> <li>• Green—The appliance is running in normal operating condition.</li> <li>• Green, blinking—The appliance is performing system initialization and memory check.</li> <li>• Amber, steady—The appliance is in a degraded operational state. For example: <ul style="list-style-type: none"> <li>– Power supply redundancy is lost.</li> <li>– CPUs are mismatched.</li> <li>– At least one CPU is faulty.</li> <li>– At least one DIMM is faulty.</li> <li>– At least one drive in a RAID configuration failed.</li> </ul> </li> <li>• Amber, blinking—The appliance is in a critical fault state. For example: <ul style="list-style-type: none"> <li>– Boot failed.</li> <li>– Fatal CPU and/or bus error is detected.</li> <li>– The appliance is in over-temperature condition.</li> </ul> </li> </ul>
Fan status	<ul style="list-style-type: none"> <li>• Green—All fan modules are operating properly.</li> <li>• Amber, steady—One fan module has failed.</li> <li>• Amber, blinking—Critical fault, two or more fan modules have failed.</li> </ul>
Temperature status	<ul style="list-style-type: none"> <li>• Green—The appliance is operating at normal temperature.</li> <li>• Amber, steady—One or more temperature sensors have exceeded a warning threshold.</li> <li>• Amber, blinking—One or more temperature sensors have exceeded a critical threshold.</li> </ul>
Power supply status	<ul style="list-style-type: none"> <li>• Green—All power supplies are operating normally.</li> <li>• Amber, steady—One or more power supplies are in a degraded operational state.</li> <li>• Amber, blinking—One or more power supplies are in a critical fault state.</li> </ul>

**Table 5-1** Cisco Security Packet Analyzer 2400 Front-Panel LEDs (continued)

LED Name	State
Network link activity	<ul style="list-style-type: none"> <li>Off—The Ethernet link is idle.</li> <li>Green—One or more Ethernet LOM ports are link-active, but there is no activity.</li> <li>Green, blinking—One or more Ethernet LOM ports are link-active, with activity.</li> </ul>
Hard drive fault	<ul style="list-style-type: none"> <li>Off—The hard drive is operating properly.</li> <li>Amber—This hard drive has failed.</li> <li>Amber, blinking—The device is rebuilding.</li> </ul>
Hard drive activity	<ul style="list-style-type: none"> <li>Off—There is no hard drive in the hard drive sled (no access, no fault).</li> <li>Green—The hard drive is ready.</li> <li>Green, blinking—The hard drive is reading or writing data.</li> </ul>

## Reading the Cisco Cisco Security Packet Analyzer 2400 Rear-Panel LEDs

Figure 5-2 shows the rear-panel LEDs for the Cisco Cisco Security Packet Analyzer 2400.

**Figure 5-2** Cisco Security Packet Analyzer 2400 Rear-Panel LEDs

1	PCIe riser 1 (slots 1, 2, 3*) *Slot 3 not present in all versions.	7	Serial connector (RJ-45)
2	PCIe riser 2 (slots 4, 5, 6)	8	Two embedded (on the motherboard) Intel i350 GbE Ethernet controller ports (LAN1, LAN2)



3	Power supplies (DC power supplies shown)	9	VGA video port (DB-15 connector)
4	Modular LAN-on-motherboard (mLOM) card slot	10	Rear Unit Identification button/LED
5	USB 3.0 ports (two)	11	Grounding-lug holes (for DC power supplies)
6	1-Gbps dedicated management port		

**Table 5-3 Cisco Security Packet Analyzer 2400 Rear-Panel LEDs**

LED Name	State
Power supply fault	<ul style="list-style-type: none"> <li>Off—The power supply is operating normally.</li> <li>Amber, blinking—An event warning threshold has been reached, but the power supply continues to operate.</li> <li>Amber, solid—A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).</li> </ul>
Power supply AC OK	<ul style="list-style-type: none"> <li>Off—There is no AC power to the power supply.</li> <li>Green, blinking—AC power OK, DC output not enabled.</li> <li>Green, solid—AC power OK, DC outputs OK.</li> </ul>
1-Gb Ethernet dedicated management link speed	<ul style="list-style-type: none"> <li>Off—link speed is 10 Mbps.</li> <li>Amber—link speed is 100 Mbps.</li> <li>Green—link speed is 1 Gbps.</li> </ul>
1-Gb Ethernet dedicated management link status	<ul style="list-style-type: none"> <li>Off—No link is present.</li> <li>Green—Link is active.</li> <li>Green, blinking—Traffic is present on the active link.</li> </ul>
1-Gb Ethernet link speed	<ul style="list-style-type: none"> <li>Off—Link speed is 10 Mbps.</li> <li>Amber—Link speed is 100 Mbps.</li> <li>Green—Link speed is 1 Gbps.</li> </ul>
1-Gb Ethernet link status	<ul style="list-style-type: none"> <li>Off—No link is present.</li> <li>Green—Link is active.</li> <li>Green, blinking—Traffic is present on the active link.</li> </ul>
Identification	<ul style="list-style-type: none"> <li>Off—The Identification LED is not in use.</li> <li>Blue—The Identification LED is activated.</li> </ul>

## Reading the NIC LEDs

Figure 5-3 shows the NIC 1 LEDs located on the rear of the Cisco Security Packet Analyzer appliance. These LEDs indicate the connection activity and speed of the NIC ports. Table 5-4 describes the activity and connection speed associated with each LED state.

Figure 5-3 NIC 1 LEDs

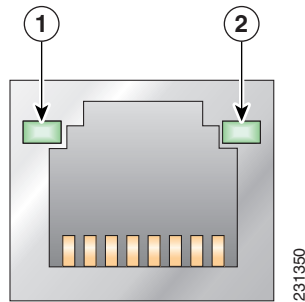


Table 5-4 NIC 1 LED Descriptions

Location	LED	Color	State	Description
1	Left		Off	No network connection
		Green	Solid	Network connection
		Green	Blinking	Transmit/receive activity
2	Right		Off	10-Mb/s connection (if left LED is on or blinking)
		Green	Solid	100-Mb/s connection
		Amber	Solid	1000-Mb/s (or 1-Gb/s) connection

## Reading the AC Power Supply LED

The rear of Cisco Security Packet Analyzer 2400 series appliances include LEDs that indicate the power status of the AC power supply. (See location 2 in [Figure 5-2](#).) [Table 5-5](#) describes the power status associated with the AC power supply LED.

Table 5-5 AC Power Supply LED

LED	Color	State	Description
Below AC power supply input connector		Off	No AC input power to power supply
	Green	Blinking	AC power applied to power supply and standby voltages are available
	Green	Solid	All power available
	Amber	Blinking	AC power supply warning due to overcurrent or overtemperature condition or slow fan
	Amber	Solid	AC power supply failed or shut down due to blown fuse, high overcurrent or overtemperature condition, or fan failure

# Replacing Appliance Components

Table 5-6 lists the Field Replaceable Units (FRUs) of the Cisco Security Packet Analyzer 2400 series appliances.

**Table 5-6 Cisco Cisco Security Packet Analyzer 2400 Appliances FRUs**

Description	Notes
SFP, SFP+	See <a href="#">Replacing Transceiver Modules</a> , page 5-7.
Hard Disk Drive, 1 TB	See <a href="#">Removing and Replacing a Hard Disk Drive</a> , page 5-8.
AC Redundant Power Supply	See <a href="#">Installing or Replacing a Power Supply.</a> , page 5-8.
Hard Disk, 2 TB for 2400	See <a href="#">Installing or Replacing a Power Supply.</a> , page 5-8.
UCS PCIe NIC Card	See <a href="#">Installing or Removing a UCS PCIe NIC Card</a> , page 5-7

## Installing or Removing a UCS PCIe NIC Card

For information about installing or removing a UCS PCIe NIC Card in Cisco Security Packet Analyzer 2400 series appliances, see the [Replacing a PCIe Card](#) section in the *Cisco UCS C240 Server Installation and Service Guide* for Cisco Security Packet Analyzer 2400 appliance.

## Replacing Transceiver Modules

To replace an SFP or an SFP+ transceiver module in a Cisco Security Packet Analyzer 2400 series appliance:

- Step 1** Locate the new transceiver module you plan to install, remove any protective packaging, and examine it for any signs of damage.
- Step 2** Determine which module you want to replace on the Cisco Security Packet Analyzer rear panel.
- Step 3** Remove the fiber optical cable from the module to be replaced.
- Step 4** With your finger, pull the latch down to release the module from its latched position (see [Figure 2-2](#)).
- Step 5** Using the latch, pull the SFP+ out of the appliance and place it in a safe location.
- Step 6** Insert the new SFP+ into the slot and slide it in until you feel resistance, then push the SFP+ harder until you feel (or hear) it click into its socket.
- Step 7** With your finger, pull the latch upwards to lock the SFP+ into its slot (see [Figure 2-3](#)).
- Step 8** Replace the fiber optical cable.



**Note**

If you use NIC card with RJ45 ports, do not install the transceiver modules.

## Removing and Replacing a Hard Disk Drive

For information about replacing hard disk drives in Cisco Security Packet Analyzer 2400 series appliances, see the *Replacing Hard Drives or Solid State Drives* section in the *Cisco UCS C240 Server Installation and Service Guide* for Cisco Security Packet Analyzer 2400 appliance.

Customer should not swap any disk with another disk inside the same Packet Analyzer appliance. This will make the RAID unrecoverable and all data on the RAID will be lost.



### Note

A single disk failure per RAID can be fixed in the field by replacing the failed disk with an exactly matching disk. You should not swap any disk with another disk inside the same Packet Analyzer appliance. It makes the RAID unrecoverable and all data on the RAID is lost.

## Installing or Replacing a Power Supply.

For information about replacing power supplies in Cisco Security Packet Analyzer 2400 series appliances, see the *Replacing Power Suppliers* section in the *Cisco UCS C240 Server Installation and Service Guide* for Cisco Security Packet Analyzer 2400 appliance.

# Removing or Replacing the Cisco Security Packet Analyzer 2400 Series Appliances

Always use the Packet Analyzer CLI command **shutdown** to shut down the Packet Analyzer application.



### Warning

**Power off the unit before you begin.** Statement 237



### Warning

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

To remove a Cisco Security Packet Analyzer 2400 series appliance from your network, use the Packet Analyzer CLI command **shutdown** to shut down the Packet Analyzer application.

The appliance is in constant communication on your network, which means that when the network notices that the appliance is no longer responding to it, the network stops sending requests to the appliance. This change is transparent to users. If other appliances are attached to the network, the network continues sending requests to the other appliances.

To replace an appliance, remove it from the network. Then, install a new appliance and configure it using the same configuration parameters that you used for the removed appliance.



## Upgrade and Recovery Procedures

---

Cisco occasionally provides upgrades to Packet Analyzer software you can download and install on your Cisco Security Packet Analyzer 2400 series appliance. You might also use the downloadable software to restore your appliance software in the case of a catastrophic failure.

After you upgrade or restore your appliance software, if you have backed up your Cisco Security Packet Analyzer appliance configuration, you can restore that configuration and resume network monitoring without undue delay.

This chapter contains the following sections:

- [Backing Up Your Configuration](#)  
After you complete any changes to your Cisco Security Packet Analyzer appliance configuration, use the command line interface to upload your Packet Analyzer configuration to an archive server.
- [Restoring Your Configuration](#)  
Use the command line interface to restore your previous Packet Analyzer configuration.
- [Upgrading Your Software](#)  
Download a version of the current Packet Analyzer software and use a single CLI command to perform the software upgrade.
- [Recovery Installation](#)  
Use the helper utility to perform a recovery installation.

### Backing Up Your Configuration

Before you begin the upgrade process, we recommend that you perform a complete backup of your current Packet Analyzer configuration.



#### Note

Having a backup configuration file can save you time and frustration if your Packet Analyzer appliance should suffer a hard disk failure that requires you to reformat or repartition your hard disk drives. This procedure does not back up the capture files and the monitoring data.

To back up your current configuration, use the Packet Analyzer CLI **config upload** command like the following:

```
config upload ftp://user:password@server/path backup_file_name
```

For example:

```
config upload ftp://admin:secret@172.20.104.11//archive/secpa_config
```

The **config upload** command sends a copy of the Packet Analyzer running configuration to the destination you specify. The copy of your configuration is stored in a back-up configuration file with an ending suffix of **.config** as in **Packet Analyzer\_host-secpa2400-6.2-1.config**. The destination address should be a valid server name and directory path where you have read and write permissions.

## Restoring Your Configuration

If you have stored your Packet Analyzer configuration file at a remote server location that you can access using FTP or HTTP (see [Backing Up Your Configuration, page 6-1](#)), you can restore your Packet Analyzer configuration file after a system recovery or upgrade. This, however, is optional.

Use the **config network** command to restore your previous Packet Analyzer configuration, as in the following:

```
config network ftp://user:password@server//path backup_file_name
```

For example:


```
config network ftp://admin:secret@172.20.104.11//archive/secpa_config/Packet
Analyzer_host-secpa2400-6.2-1.config or Packet
Analyzer_host-nam2400.6.0.2.secpaconf.tar
```

## Upgrading Your Software

To upgrade the software for a Cisco Security Packet Analyzer 2400 series appliance:

- 
- Step 1** Download the Cisco Security Packet Analyzer application software for the Cisco Security Packet Analyzer 2400 series appliance from the Cisco.com at the following URL:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/nam-appl>
  - Step 2** Look for a file that begins with **secpa-app-x86\_64**, as in **secpa-app-x86\_64.x-x-x.SPA.bin.gz** (where **x-x-x** is the Packet Analyzer software release number). The file will be described as the Packet Analyzer2400 Application Image.
  - Step 3** Store the Cisco Security Packet Analyzer application software on the same server where you archived your Packet Analyzer configuration.
  - Step 4** Use the commands as needed from the list of upgrade commands shown in [Table 6-1](#).

**Table 6-1 Common Upgrade Commands**

Configuration Mode	Command <sup>1</sup>	Purpose
host.domain#	<b>upgrade ftp://user:password@server//path/ filename</b>	Enter the command with the path to the location of the upgrade application image.
	<b>upgrade ftp://user:password@server//path/file name reformat</b>	Reformats the existing installation.   <b>Caution</b> All configuration and data will be lost.

1. You may also use HTTP instead of FTP.

## Recovery Installation

You can use the helper utility to reinstall Cisco Security Packet Analyzer application software on your Cisco Security Packet Analyzer 2400 series appliance if your appliance should suffer a catastrophic event, such as a hard disk crash, and you can no longer boot the Cisco Security Packet Analyzer application.

To access the helper utility, use the Cisco Image Management Controller (the CIMC, not the Packet Analyzer management port) to map the Packet Analyzer recovery ISO file to the virtual media CD.

We highly recommend you to configure and test the CIMC interface because CIMC interface will be the only way for Packet Analyzer image recovery, as the Packet Analyzer appliance no longer has CD/DVD drive installed. CIMC interface can also be used for many Packet Analyzer management tasks such as remote power on, power off, and hardware health monitoring.



### Note

You must log in with user or admin privileges to perform this task.

**Step 1** Download the ISO file from CCO (where all of the other Packet Analyzer images are).

**Step 2** Log in to the CIMC web interface (default: **admin/password**) using your web browser.

For more information about configuring the CIMC, see the [Cisco UCS C-Series Servers Integrated Management Controller Configuration Guide](#).

**Step 3** Click **Launch KVM Console** (requires Java).

A Java Launcher file (.jnlp) will be download.

**Step 4** Open the Java Launcher file using Java Web Start Launcher.

**Step 5** In the Java applet, click the **Virtual Media** tab.

**Step 6** Click **Accept this session** to accept the unencrypted session for Virtual Media to server.

**Step 7** Click **Apply**.

The Virtual Media menu will show the virtual devices.

- Step 8** Choose **Virtual Media > Map CD/DVD**.
- Step 9** Click **Browse** and select the ISO file.
- Step 10** Check **Map**.
- Step 11** In the CIMC web interface, click **Power Cycle Server**.
- Step 12** The appliance will boot up from the mapped ISO image and will stop at the Helper Utility menu.
- Step 13** Choose one of these options:
- a. **Option 3** to install the image bundled in the ISO.
  - b. **Option 1** to pull a new image down from the network.
- 

For information about the helper utility options, see [Appendix E, “Helper Utility.”](#)





# Troubleshooting

The Cisco Security Packet Analyzer 2400 series appliances undergo extensive testing before they leave the factory. If you encounter problems, use the information in this appendix to help isolate problems or to eliminate the appliance as the source of the problem.



## Note

The procedures in this appendix assume that you are troubleshooting the initial Cisco Security Packet Analyzer 2400 series appliance startup, and that the appliance is in the original factory configuration. If you have removed or replaced components or changed any default settings, the recommendations in this appendix might not apply.

This appendix does not cover every possible trouble event that might occur on an appliance, but instead focuses on those events that are frequently seen by the customer.

This appendix contains the following sections:

- [Troubleshooting Guidelines](#)
- [Troubleshooting Appliance Problems](#)

## Troubleshooting Guidelines

Before and at initial system boot, you should verify the following:

- External power cable is connected, and the proper power source is being applied.
- The appliance fan and blower are operating.
- The appliance software boots successfully.
- The adapter cards (if installed) are properly installed in their slots, and each initializes (is enabled by the appliance software) without problems.

When each of these conditions is met, the hardware installation is complete, and you should proceed to perform a basic configuration (see the software installation guide or user guide that shipped with your appliance for proper configuration procedures).

If you cannot locate the source of the problem, contact a customer service representative for information on how to proceed. For technical support information, see the *Cisco Information Packet* publication that shipped with your appliance. Before you call, have the following information ready:

- Appliance chassis type (see the *Cisco Product Identification Tool*) and serial number (see [Serial Number Locations](#), page A-5)
- Maintenance agreement or warranty information (see the *Cisco Information Packet*)

- Type of software and version number (if applicable)
- Date you received the new appliance
- Brief description of the problem you are having and the steps you have taken to isolate and resolve the problem

**Note**

---

Ensure you provide the customer service representative with any upgrade or maintenance information that was performed on the Cisco Security Packet Analyzer 2400 series appliance after your initial installation. (For Site Log information, see [Appendix D, “Sample Site Log and Preinstallation Task Checklist”](#).)

---

## Troubleshooting Appliance Problems

The key to problem solving is to isolate the problem to a specific location by comparing what the Cisco Security Packet Analyzer 2400 series appliance is doing to what it should be doing.

In other words, when troubleshooting, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

**Note**

---

The LEDs on the front panel of the appliance enable you to determine appliance performance and operation. For a description of these LEDs, see the [“Reading the LEDs” section on page 5-1](#).

---

When problem solving, check the following appliance subsystems first:

- Power and cooling systems—External power source, AC power cable or DC power wires, and appliance fans. Also check for inadequate ventilation, air circulation, or environmental conditions.
- Adapter cards—Checking the LEDs on the adapter card can help you to identify a failure.
- Cables—Ensure that the external cables connecting the appliance to the network are all secure.

Table A-1 provides troubleshooting tips for possible appliance subsystem problems.

**Table A-1 Troubleshooting Tips**

Problem Description	What to Check?	What Should You Do?
The power LED on the front panel is not on.	Is the AC power cord connected properly?	If the power LED is still off, the problem might be a power supply failure.
The appliance shuts down after being on for only a short time.	<ul style="list-style-type: none"> <li>Check for an environmentally induced shutdown (see the <a href="#">“Reading the LEDs” section on page 5-1</a>).</li> <li>Check the fans. If the fans are not working, the appliance will overheat and shut itself down.</li> <li>Ensure that the appliance intake and exhaust vents are clear.</li> </ul>	<ul style="list-style-type: none"> <li>If the fans are not working, you might need to check the power supply connections to the fans.</li> <li>Check the environmental site requirements in <a href="#">Appendix C, “Technical Specifications.”</a></li> </ul>
The appliance partially boots, but the LEDs do not light.	Check for a power supply failure by inspecting the power LED on the front panel of the appliance. If the LED is on, the power supply is functional.	If the LED is off, refer to the <a href="#">Cisco Information Packet</a> for warranty information or contact your customer service representative.
Power supply shuts down or latches off.	Check to see if the fan has failed, the air conditioning in the room has failed or airflow is blocked to cooling vents.	Take steps to correct the problem. For information about environmental operating conditions, see the User Guide.
Adapter card is not recognized by the appliance.	<ul style="list-style-type: none"> <li>Make sure that the adapter card is firmly seated in its slot.</li> <li>Check the LEDs on the adapter card. Each adapter card has its own set of LEDs. For information on these LEDs, see the <a href="#">“Reading the LEDs” section on page 5-1</a>.</li> <li>Make sure that you have a version of software that supports the adapter card.</li> </ul>	For information, see the documentation that was included with your adapter card.

**Table A-1** Troubleshooting Tips (continued)

Problem Description	What to Check?	What Should You Do?
Adapter card is recognized, but interface ports do not initialize.	<ul style="list-style-type: none"> <li>• Make sure that the adapter card is firmly seated in its slot.</li> <li>• Check external cable connections.</li> <li>• Make sure that you have a version of software that supports the adapter card. Refer to the documentation that was included with your adapter card.</li> </ul>	For information, see the documentation that was included with your adapter card.
The appliance does not boot properly, or it constantly or intermittently reboots.	<ul style="list-style-type: none"> <li>• Make sure that the adapter card is firmly seated in its slot.</li> <li>• Check the appliance chassis or the application software.</li> </ul>	<ul style="list-style-type: none"> <li>• For information, see the documentation that was included with your adapter card.</li> <li>• For warranty information, see the <i>Cisco Information Packet</i> publication that shipped with your appliance or contact your customer service representative.</li> </ul>
If you are using the console port with a terminal, and the appliance boots but the console screen is frozen.	<ul style="list-style-type: none"> <li>• Check the external console connection.</li> <li>• Verify that the parameters for your terminal are set as follows:               <ul style="list-style-type: none"> <li>(a) The terminal should have the same data rate that the appliance has (9600 bps is the default).</li> <li>(b) 8 data bits.</li> <li>(c) No parity generated or checked.</li> <li>(d) 1 stop bit.</li> </ul> </li> </ul>	
The appliance powers up and boots only when an adapter card is removed.	Check the adapter card. There might be a problem with the adapter card. Refer to the documentation that was included with your adapter card.	For warranty information, refer to the <i>Cisco Information Packet</i> publication that shipped with your appliance or contact your customer service representative.

**Table A-1** Troubleshooting Tips (continued)

Problem Description	What to Check?	What Should You Do?
The Cisco Security Packet Analyzer 2400 series appliance powers up and boots only when a particular cable is disconnected.	There might be a problem with the cable.	For warranty information, see the <i>Cisco Information Packet</i> publication that shipped with your appliance or contact your customer service representative.
Cannot locate the product serial ID on the Cisco Security Packet Analyzer.	<p>Before you submit a request for service online or by phone, use the <a href="#">Cisco Product Identification tool</a> to locate your product serial number.</p> <p>This tool offers three search options:</p> <ul style="list-style-type: none"> <li>• Search by product ID or model name</li> <li>• Browse for Cisco model</li> <li>• Copy and paste the output of the <b>show</b> command to identify the product</li> </ul>	For the location of the Cisco Security Packet Analyzer 2400 series appliance serial number, see <a href="#">Serial Number Locations, page A-5</a> .

## Serial Number Locations

The serial number for the appliance is printed on a pull-out asset tag inside the front panel. See [Figure 1-1](#).





## Safety Guidelines

---

Before you install your appliance, review the safety guidelines in this appendix to avoid injuring yourself or damaging the equipment.

In addition, before replacing, configuring, or maintaining the appliance, review the safety warnings listed in the *Regulatory Compliance and Safety Information* document.

- [General Precautions, page B-1](#)
- [Safety with Equipment, page B-2](#)
- [Safety with Electricity, page B-3](#)
- [Preventing Electrostatic Discharge Damage, page B-4](#)
- [Lifting Guidelines, page B-5](#)

## General Precautions

Observe the following general precautions for using and working with your appliance:

- Observe and follow service markings. Do not service any Cisco product except as explained in your appliance documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt might expose you to electrical shock. Components inside these compartments should be serviced only by an authorized service technician.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your authorized service provider:
  - The power cable, extension cord, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your appliance away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your appliance, and never operate the product in a wet environment.
- Do not push any objects into the openings of your appliance. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with other equipment approved by Cisco.
- Allow the product to cool before removing covers or touching internal components.

- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service representative or local power company.
- Use only approved power cables. If you have not been provided with a power cable for your appliance or for any AC-powered option intended for your appliance, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the appliance and power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cord, use a three-wire cord with properly grounded plugs.
- Observe extension cord and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cord or power strip does not exceed 80 percent of the extension cord or power strip ampere ratings limit.
- Do not use appliance or voltage converters or kits sold for appliances with your product.
- To help protect your appliance from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position cables and power cords carefully; route cables and the power cord and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your appliance cables or power cord.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local or national wiring rules.

## Safety with Equipment

The following guidelines will help ensure your safety and protect the equipment. However, this list does not include all potentially hazardous situations, so be *alert*.



### Warning

---

**Read the installation instructions before connecting the system to the power source.** Statement 1004

---

- Always disconnect all power cords and interface cables before moving the appliance.
- Never assume that power is disconnected from a circuit; *always* check.
- Keep the appliance chassis area clear and dust-free before and after installation.
- Keep tools and assembly components away from walk areas where you or others could fall over them.
- Do not work alone if potentially hazardous conditions exist.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not wear loose clothing that might get caught in the appliance chassis.
- Wear safety glasses when working under conditions that might be hazardous to your eyes.



# Safety with Electricity



Warning

**This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Statement 1017



Warning

**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.** Statement 1021



Warning

**Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.** Statement 4



Warning

**Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43



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.** Statement 12



Warning

**Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001



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

**When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 1046

Follow these guidelines when working on equipment powered by electricity:

- Locate the room's emergency power-off switch. Then, if an electrical accident occurs, you can quickly turn off the power.
- Disconnect all power before doing the following:
  - Working on or near power supplies
  - Installing or removing an appliance

- Performing most hardware upgrades
- Never install equipment that appears damaged.
- Carefully examine your work area for possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Never assume that power is disconnected from a circuit; *always* check.
- Never perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never work alone when potentially hazardous conditions exist.
- If an electrical accident occurs, proceed as follows:
  - Use caution, and do not become a victim yourself.
  - Turn off power to the appliance.
  - If possible, send another person to get medical aid. Otherwise, determine the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing, external cardiac compressions, or other medical attention; then take appropriate action.

In addition, use the following guidelines when working with any equipment that is disconnected from a power source but still connected to telephone wiring or 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.

## Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD can occur when electronic printed circuit cards are improperly handled and can cause complete or intermittent failures. Always follow ESD-prevention procedures when removing and replacing modules:

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your appliance. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.
- Ensure that the appliance is electrically connected to earth ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the appliance 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 appliance.

**Caution**

For the safety of your equipment, periodically check the resistance value of the antistatic wrist strap. It should be between 1 and 10 Mohm.

## Lifting Guidelines

The appliance weighs approximately 33 pounds. The appliance is not intended to be moved frequently. Before you install the appliance, ensure that your site is properly prepared so you can avoid having to move the appliance later to accommodate power sources and network connections.

Whenever you lift the appliance or any heavy object, follow these guidelines:

- Always disconnect all external cables before lifting or moving the appliance.
- Ensure that your footing is solid, and balance the weight of the object between your feet.
- Lift the appliance slowly; never move suddenly or twist your body as you lift.
- Keep your back straight and lift with your legs, not your back. If you must bend down to lift the appliance, bend at the knees, not at the waist, to reduce the strain on your lower back muscles.
- Lift the appliance from the bottom; grasp the underside of the appliance exterior with both hands.





## Technical Specifications

---

The Cisco Security Packet Analyzer 2400 series appliances are based on the UCS C240 server. This appendix includes the following sections:

- [Cisco Security Packet Analyzer2400 Technical Specifications](#)
- [Optical Tap Devices](#)

## Cisco Security Packet Analyzer2400 Technical Specifications

The following table contains links to the technical specifications for the Cisco Security Packet Analyzer appliance. For more information about the Cisco UCS C240 server, see the [Cisco UCS C240 Server Installation and Service Guide](#).

## SFP Port Cable Specifications

The Cisco Security Packet Analyzer 2400 uses 10G SFP modules. For SFP cabling specifications, see [Installing the GBIC, SFP, SFP+, XFP, CXP, and CFP Optical Modules in Cisco ONS Platforms](#).

## Optical Tap Devices

You can use an optical tap device to get a copy of traffic flows between two network devices. Passive taps, such as optical tap devices, ensure that the flowing traffic is not altered regardless of its connection to the Packet Analyzer appliance and provide a very low point of failure.

Traffic flows will be interrupted while you connect an optical tap, but doing so should take less than a minute and can be done during a network maintenance window.

Packet Analyzer appliances are designed to receive tapped network traffic from both directions, from multiple links simultaneously, and to accurately merge received traffic to a single stream for high precision analysis.

Although passive optical taps do not alter the network characteristics and dynamics of flowing traffic, an optical tap does reduce the signal strength, so care should be taken to follow the tap specifications including your network link length and tapping location.

**Note**

Pay attention to the optical split ratio of your passive taps with regard to your optical cable lengths. If the cable between the two devices or the cable from the tap to your Cisco Security Packet Analyzer appliance is very long, you might need to select a different split ratio other than 50/50 to make sure the receive side signals on your two devices and Cisco Security Packet Analyzer appliance are all strong enough to not introduce any line errors. Refer to user instructions of your optical tap device for more information.

[Table C-1](#) lists the 10 GE optical tap devices that have been successfully tested with the Cisco Security Packet Analyzer 2400 series appliance in a tap configuration.

**Table C-1**      **10 Gb Optical Taps**

Vendor	Product Description	Model
NetOptics	10 GigaBit Fiber Tap (MM50:50 850 nm SC)	TP-SR4-SCSLM
	10 GigaBit Fiber Tap (MM50:50 850 nm SC)	TP-SR5-SCSLM
	10 GigaBit Fiber Tap (SM50:50 1310 nm SC)	TP-LR5-SCSLM
DataCom Systems	Single channel 10 Gb passive Tap	F50/50/9-S-10G
Network Critical	SMF 9 850/1300NM supports 1000 base-LX, 10 Gig-LR, 10 Gig-ER	FO-S15002-LC
	MMF 50 850/1300NM supports 1000 base-SX, 10 Gig-SR	FO-M35002-LC



## Sample Site Log and Preinstallation Task Checklist

---

The Site Log provides a record of all actions related to installing and maintaining the Cisco Security Packet Analyzer 2400 series appliance. Keep the log in an accessible place near the appliance chassis so that anyone who performs tasks has access to it. Site Log entries might include the following:

- Installation progress—Make a copy of the appliance Installation Checklist (see [Sample Preinstallation Task Checklist, page D-3](#)), and insert it into the Site Log (see [Sample Site Log, page D-1](#)). Make entries as you complete each task.
- Upgrade, removal, and maintenance procedures—Use the Site Log as a record of ongoing appliance maintenance and expansion history. Each time a task is performed on the appliance, update the Site Log to reflect the following information:
  - Installation of new adapter cards
  - Removal or replacement of adapter cards and other upgrades
  - Configuration changes
  - Maintenance schedules and requirements
  - Maintenance procedures performed
  - Intermittent problems
  - Comments and notes

### Sample Site Log

[Table D-1](#) shows a sample site log. Make copies of the sample or design your own site log to meet the needs of your site and equipment.





# Sample Preinstallation Task Checklist

Part of your site preparation includes reviewing a preinstallation checklist of tasks and considerations that need to be addressed and agreed upon before proceeding with the installation. This is an example of a preinstallation checklist:

1. Assign personnel.
2. Determine protection requirements for personnel, equipment, and tools.
3. Evaluate potential hazards that might affect service.
4. Schedule time for installation.
5. Determine any space requirements.
6. Determine any power requirements.
7. Identify any required procedures or tests.
8. On an equipment plan, make a preliminary decision that locates each Cisco Security Packet Analyzer 2400 series appliance that you plan to install.
9. Read this hardware installation guide.
10. Verify the list of replaceable parts for installation (screws, bolts, washers, and so on) so that the parts are identified.
11. Check the required tools list to make sure the necessary tools and test equipment are available.
12. Perform the installation.





# Helper Utility

You can use the helper utility to perform the following tasks on your Cisco Security Packet Analyzer 2400 series appliance:



**Note**

For information about accessing the helper utility, see [Recovery Installation, page 6-3](#).

**Figure E-1**      **Helper Utility Menu**

```
=====
Cisco Systems, Inc.
Network Analysis Module (SEC-PA-2400-K9) helper utility
Version 1.1(0.25)

-----
Main menu
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Install application image from CD and reformat HDD
4 - Display software versions
5 - Reset application image CLI passwords to default
6 - Send Ping
7 - Configure Capture RAID settings
8 - Install application image from flash and reformat HDD
f - Check for and fix file system errors on local disk
s - Show upgrade log
n - Configure network
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine
```

The following sections describe the [Helper Utility Menu](#), what each option does, and any requirements for using a particular option.

# Helper Utility Menu Summary

**Table E-1** *Helper Utility Menu Options Summary*

Menu Option	Description	See...
1	Download the application image and write it to the hard disk drive.	<a href="#">Option 1 - Download Application Image and Write to HDD, page E-3</a>
2	Download the application image and reformat the hard disk drive.	<a href="#">Option 2 - Download Application Image and Reformat HDD, page E-4</a>
3	Install the application image from a CD.	<a href="#">Option 3 - Install Application Image from CD, page E-4</a>
4	Display the current Cisco Security Packet Analyzer application image version stored on your hard disk.	<a href="#">Option 4 - Display Software Versions, page E-4</a>
5	Reset the password for users root and admin to their default values.	<a href="#">Option 5 - Reset Application Image CLI Passwords to Default, page E-5</a>
6	Send a ping to determine if network connectivity exists.	<a href="#">Option 6 - Send Ping, page E-5</a>
7	Configure Capture RAID settings.	<a href="#">Option 7 - Configure Capture RAID Settings, page E-5</a>
8	Install the application image from flash and reformat the hard disk drive.	<a href="#">Option 8 - Install Application Image From Flash and Reformat HDD, page E-6</a>
f	Check for and fix file system errors on the local disk.	<a href="#">Option f - Check For and Fix Filesystem Errors on Local Disk, page E-6</a>
s	Display the upgrade log.	<a href="#">Option s - Show Upgrade Log, page E-6</a>
n	Configure the network parameters for the appliance	<a href="#">Option n - Configure Network, page E-2</a>
r	Exit the helper utility and power cycle (reboot) into the Cisco Security Packet Analyzer application image.	<a href="#">Option r - Exit and Reset Services Engine, page E-6</a>
h	Exit the helper utility and shut down the Cisco Security Packet Analyzer appliance.	<a href="#">Option h - Exit and Shutdown Services Engine, page E-6</a>

## Option n - Configure Network

Use **Option n** to configure the network parameters for the appliance.

**Step 1** When the Configure Network Interface menu displays, enter **1** to configure the network manually.

```
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]: 1
```

**Step 2** The utility prompts you for the IP address, netmask, and default gateway for the appliance.

```
Enter IP configuration:
IP address []: 172.20.122.93
netmask []: 255.255.255.128
default gateway []: 172.20.122.1
```

```
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]:
```

**Step 3** To check your network configuration, enter **2**.

```
Selection [123r]: 2

eth0      Link encap:Ethernet HWaddr 00:0E:0C:EE:50:3E
          inet addr:172.20.122.93 Bcast:172.20.122.127 Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13632 (13.3 KiB) TX bytes:0 (0.0 b)

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
172.20.122.0 0.0.0.0 255.255.255.128 U 0 0 eth0
0.0.0.0 172.20.122.1 0.0.0.0 UG 0 0 eth0
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]:
```

## Option 1 - Download Application Image and Write to HDD

Use **Option 1** to download a version of the current application image from an FTP server location and write the image to the hard disk.



### Note

If the Cisco Security Packet Analyzer application has already been installed and the network settings were configured, they will be automatically be detected by the helper. Otherwise, you must use **Option n** to configure the network *before* using this option.

This option downloads a version of the current application from an FTP server location or from a location you can access using HTTP. You can also [download the latest Cisco Security Packet Analyzer software version](#) from Cisco.com.

This URL requires you to have a Cisco service agreement and access to the internet to download the zipped software.

## Option 2 - Download Application Image and Reformat HDD

Use **Option 2** to download the current application image and write the image to the hard disk.



### Caution

Using this option reformats the hard disk before writing the application image and will destroy all data such as reports, packet captures, and configuration. Network connectivity configuration, however, will be retained.



### Note

If the Cisco Security Packet Analyzer application has already been installed and the network settings were configured, they will be automatically be detected by the helper. Otherwise, you must use **Option n** to configure the network *before* using this option.

This option downloads a version of the current application image from an FTP server location or from a location you can access using HTTP. You can also [download the latest Cisco Security Packet Analyzer software version](#) from Cisco.com.

This URL requires you to have a Cisco service agreement and access to the internet to download the zipped software.

## Option 3 - Install Application Image from CD

Use **Option 3** to install the current application image from the recovery CD. This option might be necessary if you are unable to connect to your network and download a version of Packet Analyzer software you archived earlier.



### Caution

This option reformats the hard disk before writing the application image and will destroy all data such as reports, packet captures, and configuration. Network connectivity configuration, however, will be retained.



### Note

The version of Packet Analyzer software available on the recovery CD is the *first release* of the software and has no patches or upgrades. If you use this option, see [Upgrading Your Software, page 6-2](#).

## Option 4 - Display Software Versions

Use **Option 4** to display the current Cisco Security Packet Analyzer application image version stored on your hard disk.

```
Selection [123456789dnfrh]:4
-----
SECPA application version: 6.2(2) RELEASE SOFTWARE
Selection [123456789dnfrh]:
```

## Option 5 - Reset Application Image CLI Passwords to Default

Use **Option 5** to reset the password for users root and admin to their default values.

## Option 6- Send Ping

Use **Option 7** to send a ping to determine if network connectivity exists. When prompted, enter the IP address or full domain name of the location to send the ping.

```
IP address to ping []: 172.20.122.91

Sending 5 ICMP ECHO_REQUEST packets to 172.20.122.91.
PING 172.20.122.91 (172.20.122.91) 56(84) bytes of data.
64 bytes from 172.20.122.91: icmp_seq=1 ttl=64 time=0.151 ms
64 bytes from 172.20.122.91: icmp_seq=2 ttl=64 time=0.153 ms
64 bytes from 172.20.122.91: icmp_seq=3 ttl=64 time=0.125 ms
64 bytes from 172.20.122.91: icmp_seq=4 ttl=64 time=0.102 ms
64 bytes from 172.20.122.91: icmp_seq=5 ttl=64 time=0.166 ms

--- 172.20.122.91 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.102/0.139/0.166/0.025 ms
```

## Option 7 - Configure Capture RAID Settings

Use **Option 8** to configure the Capture RAID settings. This option contains the following suboptions:

```
-----
Capture RAID Menu
1 - Rebuild all failed disks
2 - Add all new disks to the Capture RAID
3 - Decommission the Capture RAID (destructive)
4 - Construct the Capture RAID (destructive)
c - Show current Capture RAID configuration
p - Show all progress of Capture RAID reconfiguration
r - return to main menu
-
Selection [1234cpr]:
```

The following table describes each of these suboptions.

**Table E-2** Capture RAID Menu Options

Menu Option	Description
1	Rebuild all failed disks.
2	Add new disks to the Capture RAID. If any disks have been installed since the last Cisco Security Packet Analyzer application reformat install, the RAID will be expanded to include them.
3	Decommission the Capture RAID. Using this option cleans the hard disk and will destroy only the capture data; all other data is on the system RAID.

Table E-2 Capture RAID Menu Options

Menu Option	Description
4	Construct the Capture RAID.
c	Show the current Capture RAID configuration.
p	Show the progress of the Capture RAID reconfiguration.
r	Return to the main menu.

## Option 8 - Install Application Image From Flash and Reformat HDD

Use **Option 9** to install the application image from flash and reformat the hard disk.



### Caution

This option reformats the hard disk before writing the application image and will destroy all data such as reports, packet captures, and configuration. Network connectivity configuration, however, will be retained.



### Note

If the Cisco Security Packet Analyzer application has already been installed and the network settings were configured, they will be automatically be detected by the helper. Otherwise, you must use **Option n** to configure the network *before* using this option.

## Option f - Check For and Fix Filesystem Errors on Local Disk

Use **Option f** to find and fix file system errors on the local disk. Depending on the partition size, this option might take a long time.

## Option s - Show Upgrade Log

Use **Option s** to display the upgrade log.

## Option r - Exit and Reset Services Engine

Use **Option r** to exit the helper utility and power cycle (reboot) into the newly installed application image.

## Option h - Exit and Shutdown Services Engine

Use **Option h** to exit the helper utility and shut down the Cisco Security Packet Analyzer appliance.



```
-----  
Selection [12345678fsmrh]: h  
About to exit and shutdown SECPA.  
Are you sure? [y/N] y  
Stopping internet superserver: inetd.  
Stopping OpenBSD Secure Shell server: sshd.  
Stopping internet superserver: xinetd.  
Stopping internet superserver: xinetd-ipv4.  
: done.  
Shutting down SECPA (SECPA2400-K9), part 1:  
Stopping klogd . . .  
Stopping syslogd . . .  
Sending all processes the TERM signal... done.  
Sending all processes the KILL signal... done.  
Unmounting remote filesystems... done.  
Deactivating swap...done.  
Unmounting local filesystems...done.  
Starting halt command: halt  
Power down.  
-----
```

