Cisco NAC Appliance Hardware Installation Guide

Release 4.8
January 2011

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

Text Part Number: OL-20326-01

Cisco NAC Appliance Hardware Installation Guide

CONTENTS

About This Guide

Revised February 1, 2011, OL-20326-01

This preface includes the following sections:

Audience

This guide is for network administrators who are installing the Cisco NAC Appliance hardware and performing initial configuration to introduce the Clean Access Manager (CAM) and Clean Access Server (CAS) into the network. Use this document along with the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* and *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* to install, configure, and administer your Cisco NAC Appliance deployment.

Purpose

The *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* describes how to install and initially configure the Clean Access Manager and Clean Access Server on all Cisco NAC Appliance platforms. Once you have installed and initially configured the CAM and CAS, you can use the Clean Access Manager (CAM) and its web-based administration console to manage multiple Clean Access Servers (CASs) in a deployment. End users connect through the Clean Access Server to the network via web login or Cisco NAC Agent. This guide also describes how to implement High Availability for the CAMs and CASs in your network.

See the Product Documentation section for further details on the document set for Cisco NAC Appliance.

Document Organization

This guide combines hardware and installation information for both the Clean Access Manager and Clean Access Server. Starting from Release 4.7(0), the *Cisco NAC Appliance Hardware Installation Guide* replaces the installation chapters that were formerly located in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* and *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide.*

Table 1 Document Organization

Chapter	Description
Chapter 1, "Cisco NAC Appliance Hardware Platforms"	Provides information about the hardware platforms available in Cisco NAC Appliance
Chapter 2, "Preparing for Installation"	Outlines the steps necessary to ensure your environment is ready to install Cisco NAC Appliance hardware
Chapter 3, "Installing the Clean Access Manager and Clean Access Server"	Describes how to install and initially configure the Clean Access Manager and Clean Access Server
Chapter 4, "Configuring High Availability (HA)"	Describes how to set up a pair of Clean Access Manager or Clean Access Server machines for high availability
Chapter 5, "Password Recovery"	Defines the steps necessary to recover a lost Cisco NAC Appliance root password
Appendix A, "Open Source License Acknowledgements"	Contains Open Source License information for Cisco products

Document Conventions

Table 2 Document Conventions

Item	Convention
Indicates command line output.	`Screen` font
Indicates information you enter.	**`Boldface screen`** font
Indicates variables for which you supply values.	*`Italic screen`* font
Indicates web admin console modules, menus, tabs, links and submenu links.	**Boldface** font
Indicates a menu item to be selected.	**Administration > User Pages**

New Features in this Release

For a brief summary of the new features and enhancements available in this release refer to Documentation Updates and the "New and Changed Information" section of the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.

Product Documentation

Table 3 lists the technical documentation available for Cisco NAC Appliance on Cisco.com at http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html.

When using the online publications, refer to the documents that match the software version running on your Cisco NAC Appliance (e.g. “Release 4.8”).

See also the following product literature for additional details:

- *Cisco NAC Appliance Data Sheet*
- *Cisco NAC Appliance Ordering Guide*

Tip To access external URLs referenced in the PDF of this document, right-click the link in Adobe Acrobat and select “Open in Weblink in Browser.”

Table 3 Cisco NAC Appliance Document Set

Document Title	Refer to This Document For Information On:
Cisco NAC Appliance Service Contract/Licensing Support	• Obtaining and installing product licenses • Information on service contracts, ordering and RMA
Supported Hardware and System Requirements for Cisco NAC Appliance	• Supported Hardware Platforms, Troubleshooting Network Card Driver Support Issues, and System Requirements
Regulatory Compliance and Safety Information for Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	• Regulatory Compliance and Safety Information
Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later	• Agent System Requirements, Agent/Server Version Compatibility, Agent/OS/Browser Support Matrix, Agent/AD Server Compatibility for AD SSO, and Agent Localized Language Template Support
Switch Support for Cisco NAC Appliance	• Which switches and NMEs support OOB deployment • Known issues/troubleshooting for switches and WLCs
Connecting Cisco Network Admission Control Network Modules	• Connecting Cisco NAC network module (NME-NAC-K9) in an Integrated Services Router
Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide	• Provides instructions to upgrade your existing Cisco NAC-3310, NAC-3350, and NAC-3390 with a field-replaceable FIPS card necessary to introduce FIPS compliance in your network

Table 3 Cisco NAC Appliance Document Set

Document Title	Refer to This Document For Information On:
Release Notes for Cisco NAC Appliance, Version 4.8(1)	Details on the latest 4.8(1) release, including: • New features and enhancements • Fixed caveats • Upgrade instructions • Supported AV/AS product charts • CAM/CAS/Agent compatibility and version information
Cisco NAC Appliance Hardware Installation Guide, Release 4.8	Details on CAM/CAS installation topics: • Hardware specifications on the various CAM/CAS platforms • How to install the Clean Access Manager and Clean Access Server Platforms • How to install Cisco NAC Appliance software on the CASM/CAS • How to configure CAM and CAS pairs for High Availability
Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)	Complete CAM details, including: • How to install the CAM software • Overviews of major concepts and features of Cisco NAC Appliance • How to use the CAM web console to perform global configuration of Cisco NAC Appliance (applying to all CASs in the deployment) • How to configure CAM pairs for High Availability
Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)	CAS-specific details, including: • How to install the CAS software • Where to deploy the CAS on the network (general information) • How to perform local (CAS-specific) configuration using the CAS management pages of the CAM web console, or the CAS direct access console • How to configure CAS pairs for High Availability

Table 3 Cisco NAC Appliance Document Set

Document Title	Refer to This Document For Information On:
Cisco NAC Profiler Installation and Configuration Guide	• Details on installing and configuring the Cisco NAC Profiler Server /Collector
Cisco NAC Appliance Migration Guide - Release 4.1(8) to Release 4.7(0)	• Upgrading from an earlier Cisco NAC Appliance release on non-Cisco hardware to a next generation (NAC-3315/3355/3395) platform using the Cisco NAC Appliance Migration utility

Documentation Updates

Table 4 Updates to Cisco NAC Appliance Hardware Installation Guide, Release 4.8

Date	Description
1/31/2011	Release 4.8(1)
12/7/10	Added a note about number of users supported by NAC-3315 and NAC-3310, when they are FIPS-Compliant, to Cisco NAC-3315 Front and Rear Panels, page 1-5 and Cisco NAC-3310 Front and Rear Panels, page 1-18
10/5/10	Updated the Hardware Specification for NAC-3315 in Cisco NAC Appliance Hardware Summary
9/9/10	Added note about installing and running Release 4.8 on CCA-3140s to FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1 and Upgrading Cisco NAC Appliance Software, page 2-27
8/16/10	Adjusted FIPS card position on NAC-3355/3395 chassis rear panel views: • Cisco NAC-3355 Front and Rear Panels, page 1-8 • Cisco NAC-3395 Front and Rear Panels, page 1-12
7/26/10	Release 4.8

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Cisco NAC Appliance Hardware Platforms

This chapter provides general information on the Cisco NAC Appliance network access control system, as well as hardware specifications for all Clean Access Manager (CAM) and Clean Access Server (CAS) platforms available from Cisco Systems, Inc.

This chapter covers the following topics:

About Cisco NAC Appliance

Cisco® NAC Appliance is a Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as laptops, desktops, and corporate assets are compliant with a network's security policies, and it repairs any vulnerabilities before permitting access to the network.

Cisco NAC Appliance is a network-centric integrated solution administered from the web console of the Clean Access Manager (CAM), enforced through the Clean Access Server (CAS), and applied on clients through the Cisco NAC Agent and Cisco NAC Web Agent client software. You can deploy the Cisco NAC Appliance solution in the configuration that best meets the needs of your network.

FIPS 140-2 Compliant and Non-FIPS Hardware Platforms

FIPS 140-2 compliant and non-FIPS Cisco NAC Appliance hardware platforms are Linux-based network hardware appliances which are pre-installed with either the CAM or CAS application, the operating system, and all relevant components on a dedicated server machine. In Release 4.7(0) and later, the operating system comprises a hardened Linux kernel based on CentOS 5.3. Cisco NAC Appliance does not support the installation of any other packages or applications onto a CAM or CAS dedicated machine.

Cisco NAC Appliance Release 4.8(1) and Release 4.8 only support and can only be installed on the following Cisco NAC Appliance platforms:

Platform	FIPS Option	Non-FIPS Option
NAC-3315 CAM/CAS [1]	Yes	Yes
NAC-3355 CAM/CAS [1]	Yes	Yes
NAC-3395 CAM [1]	Yes	Yes
NAC-3310 CAM/CAS	Yes (with FIPS card field-replaceable unit only)	Yes
NAC-3350 CAM/CAS	Yes (with FIPS card field-replaceable unit only)	Yes
NAC-3390 CAM	Yes (with FIPS card field-replaceable unit only)	Yes
NAC-3140 (EOL) [2,3]	No	Yes

1. If the FIPS card in a Cisco NAC-3315/3355/3395 CAM/CAS ceases to work correctly, make sure the FIPS card operation switch is set to "O" (for operational mode), as described in the "FIPS 140-2 Compliance" section of the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*. If the FIPS card is still not operational, you will need to RMA the appliance with Cisco Systems and replace it with a new Cisco NAC-3315/3355/3395. Refer to the "Cisco NAC Appliance RMA and Licensing" section of the *Cisco NAC Appliance Service Contract/Licensing Support* document for details.
2. Cisco NAC Appliance Release 4.8(1) does not support CCA-3140.
3. The Cisco CCA-3140 (CCA-3140-H1) NAC Appliance (EOL) requires CD installation of either the Clean Access Server or Clean Access Manager software. Due to limited hardware resources on the CCA-3140, some combinations of Release 4.8 features may cause undesirable system behavior. If you are experiencing problems with Release 4.8 on the CCA-3140, please contact the Cisco Technical Assistance Center (TAC).

Refer to the *Release Notes for Cisco NAC Appliance, Version 4.8(1)* for additional hardware compatibility information, including issues regarding FIPS 140-2 compliance.

Table 1-1 and Table 1-2 summarize the hardware specifications for each Cisco NAC Appliance. See the "Diagrams" column for links to detailed diagrams showing NIC ports, power supply sockets, LEDs and buttons.

NAC-3315, NAC-3355, and NAC-3395

Table 1-1 Cisco NAC Appliance Hardware Summary

Cisco NAC Appliance	Product	Hardware Specifications	Diagrams
NAC-3315	**MANAGER** Lite Manager supporting up to 3 standalone or HA-pair CASs **SERVER** CAS supporting 100, 250, or 500 users	• **Single processor**: Quad-core Intel Xeon (Core 2 quad) • 4GB RAM • **2** x 250 GB SATA HDD • **4 10/100/1000 LAN ports** [2 integrated NICs; 2 Gigabit NICs (PCI-E)] • CD/DVD-ROM Drive • 4 USB Ports (2 front, 2 rear) • Power supply: 350W **Note** The NAC-3315 is based on the IBM System x3250 M2 server platform.	• Figure 1-2 on page 1-5 "Cisco NAC-3315 Front Panel" • Figure 1-3 on page 1-6 "Cisco NAC-3315 Front Panel LEDs/Buttons" • Figure 1-4 on page 1-6 "Cisco NAC-3315 (With Installed FIPS Card) Rear Panel" • Figure 1-5 on page 1-7 "Cisco NAC-3315 (With Installed FIPS Card) Rear Panel LEDs"

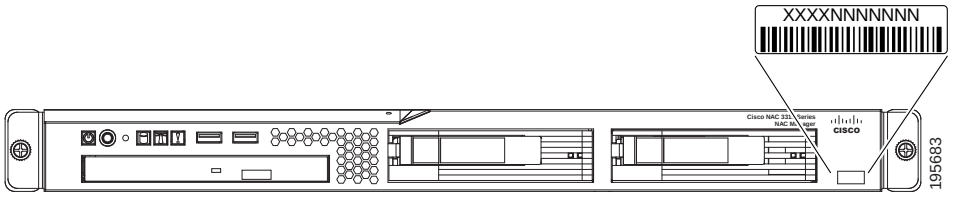
Table 1-1 Cisco NAC Appliance Hardware Summary (continued)

Cisco NAC Appliance	Product	Hardware Specifications	Diagrams
NAC-3355	**MANAGER** Standard Manager supporting up to 20 standalone or HA-pair CASs **SERVER** CAS supporting 1500, 2500, or 3500 and 5000 users	• **Single processor**: Quad-core Intel Xeon (Nehalem) • 4 GB RAM • **2** x 300 GB SAS RAID **HDD** • **4 10/100/1000 LAN ports** [2 integrated NICs; 2 Gigabit NICs (PCI-E)] • CD/DVD-ROM Drive • 4 USB Ports (1 front, 1 internal, 2 rear) • Cavium CN1120-NHB-E SSL Accelerator Card *or* nCipher Card (FIPS 140-2 Level 2 Common Criteria EAL2) • Power supply: Dual 675W (redundant) **Note** The NAC-3355 is based on the IBM System x3550 M2 server platform.	• Figure 1-7 on page 1-8 "Cisco NAC-3355 Front Panel" • Figure 1-8 on page 1-9 "Cisco NAC-3355 Front Panel LEDs/Buttons" • Figure 1-9 on page 1-10 "Cisco NAC-3355 (With Installed FIPS Card) Rear Panel" • Figure 1-10 on page 1-10 "Cisco NAC-3355 (With Installed FIPS Card) Rear Panel LEDs"
NAC-3395	**MANAGER** Super Manager supporting up to 40 standalone or HA-pair CASs	• **Dual processor**: 2 x Quad-core Intel Xeon (Nehalem) • 8GB RAM • **4** x 300 GB SAS RAID **HDD** • **4 10/100/1000 LAN ports** [2 integrated NICs; 2 Gigabit NICs (PCI-E)] • CD/DVD-ROM Drive • 4 USB Ports (1 front, 1 internal, 2 rear) • Cavium CN1120-NHB-E SSL Accelerator Card *or* nCipher Card (FIPS 140-2 Level 2 Common Criteria EAL2) • Power supply: Dual 675W (redundant) **Note** The NAC-3395 is based on the IBM System x3550 M2 server platform.	• Figure 1-12 on page 1-12 "Cisco NAC-3395 Front Panel" • Figure 1-13 on page 1-13 "Cisco NAC-3395 Front Panel LEDs/Buttons" • Figure 1-14 on page 1-14 "Cisco NAC-3395 (With Installed FIPS Card) Rear Panel" • Figure 1-15 on page 1-14 "Cisco NAC-3395 (With Installed FIPS Card) Rear Panel LEDs"

NAC-3315 Serial Number Location

The serial number label is located at the lower left of the front-panel of the NAC-3315. (See Figure 1-1.)

Figure 1-1 NAC-3315 Appliance Serial Number Location



Note The serial number for the NAC-3315 is 7 characters long. You can also view the NAC-3315 serial number location on the Cisco Support website using the Cisco Product Identification Tool. For details, see Cisco Product Identification Tool, page 1-27.

Cisco NAC-3315 Front and Rear Panels

The Cisco NAC-3315 platform is recommended for Clean Access Lite Manager and Clean Access Server (100/250/500 user count) deployments. A NAC-3315 CAM Lite can manage up to 3 Clean Access Servers or 3 HA-CAS pairs. A NAC-3315 CAS can support 100, 250, or 500 users.

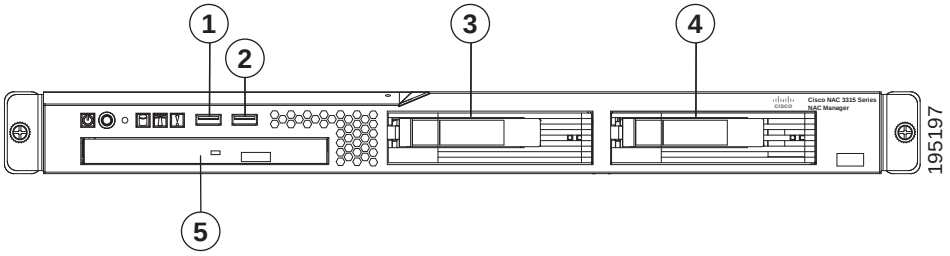
Note FIPS 140-2 compliant NAC-3315 CAS can support only 250 or 500 users.

The Cisco NAC-3315 comes equipped with 4 network interfaces to provide flexibility in NIC interface selection and to facilitate CAS high availability configuration.

For additional details, see FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1.

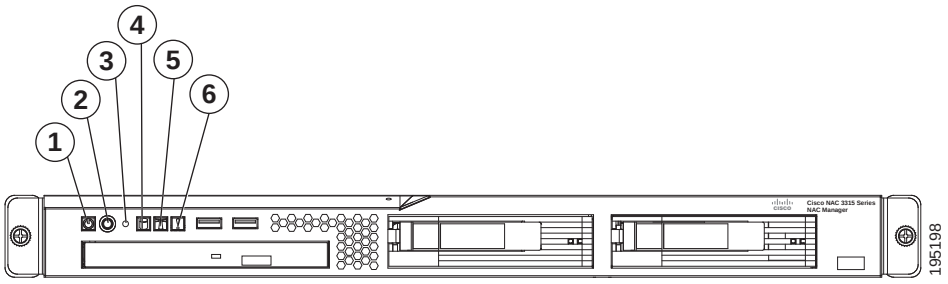
Front Panel Features

Figure 1-2 Cisco NAC-3315 Front Panel



1	Front USB port 1	4	Hard disk drive (HDD) bay 2
2	Front USB port 2	5	CD-ROM/DVD drive
3	Hard disk drive (HDD) bay 0		

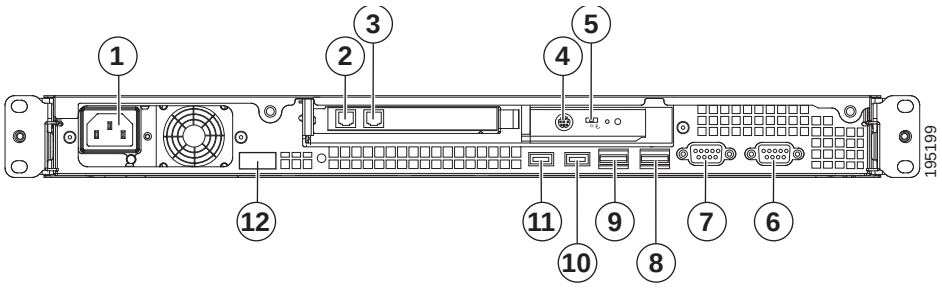
Figure 1-3 Cisco NAC-3315 Front Panel LEDs/Buttons



1	Power status LED	Green = The appliance has AC power and is powered up Off = The appliance is powered off (AC power disconnected)
2	Power button (recessed)	
3	Reset button (recessed)	
4	HDD activity LED	Flashing green = Ongoing drive activity Off = No drive activity
5	Locator button/LED	Flashing blue = The Locator button has been pressed
6	System health LED	Off = System health is normal Amber = A pre-failure system threshold has been breached. This can be any of the following: • At least one fan failure (system or processor fan) • At least one of the temperature sensors reached critical level (system or processor thermal sensors) • At least one memory module failure • A power supply unit error has occurred

Rear Panel Features

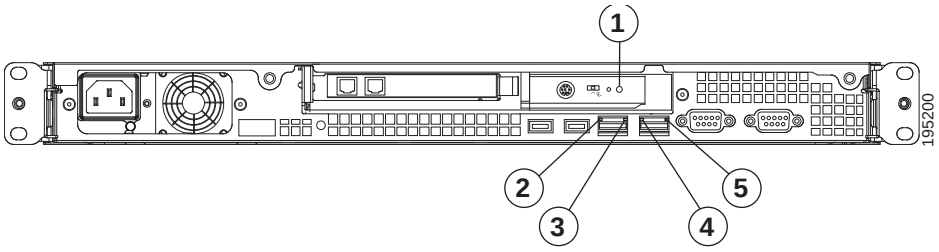
Figure 1-4 Cisco NAC-3315 (With Installed FIPS Card) Rear Panel



1	Power supply cable socket	7	Video port
2	NIC 3 (eth2) add-on card	8	NIC 2 (eth1) GbE interface
3	NIC 4 (eth3) add-on card	9	NIC 1 (eth0) GbE interface

4	FIPS card mini-DIN Smart card reader port	10	Rear USB port 4
5	FIPS card mode switch	11	Rear USB port 3
6	Serial port	12	Console port

Figure 1-5 Cisco NAC-3315 (With Installed FIPS Card) Rear Panel LEDs

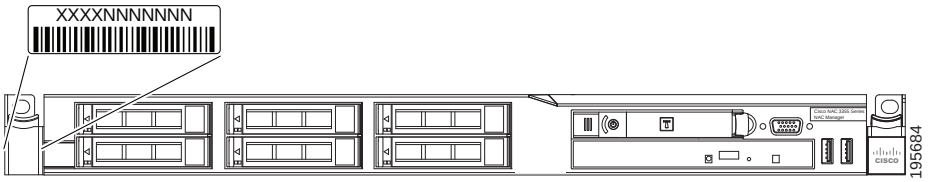


1	FIPS card status LED	Solid blue occasionally blinking off = FIPS card is enabled and accepting commands Two short blue flashes followed by a pause = FIPS card is in initialization mode Two longer blue flashes followed by a pause = FIPS card is in maintenance mode Repeatedly flashing morse code distress call (. . . - - - . . .)—three short blue flashes followed by three longer blue flashes followed again by three more short blue flashes = FIPS card is in error mode Off = There is no power source connected to the FIPS card
2	NIC 1 (eth0) activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
3	NIC 1 (eth0) link LED	Green = Link exists Off = No link exists
4	NIC 2 (eth1) activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
5	NIC 2 (eth1) link LED	Green = Link exists Off = No link exists

NAC-3355 Serial Number Location

The serial number label is located at the lower left of the front-panel of the NAC-3355. (See Figure 1-6.)

Figure 1-6 NAC-3355 Appliance Serial Number Location



Note The serial number for the NAC-3355 is 7 characters long. You can also view the NAC-3315 serial number location on the Cisco Support website using the Cisco Product Identification Tool. For details, see Cisco Product Identification Tool, page 1-27.

Cisco NAC-3355 Front and Rear Panels

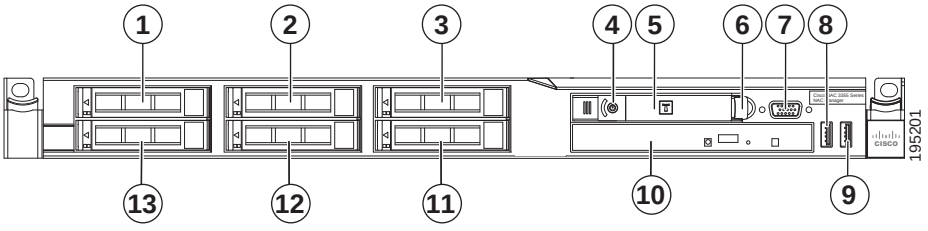
The Cisco NAC-3355 FIPS 140-2 compliant platform provides enhanced capability for enterprise wide Clean Access Standard Manager and Clean Access Server (1500/2500/3500 user count) deployments. A NAC-3355 Standard CAM can manage up to 20 Clean Access Servers or 20 HA-CAS pairs. A NAC-3355 CAS can support up to 1500, 2500, or 3500 users.

Similar to the Cisco NAC-3315, the Cisco NAC-3355 comes equipped with 4 network interfaces to provide flexibility in NIC interface selection and facilitate CAS high availability configuration. The Cisco NAC-3355 additionally provides 2 GB of RAM, two SAS drives configured in RAID 0 and 1, dual power supplies, and an SSL accelerator card to support large network deployments and provide added reliability for a centralized CAM/CAS deployment in the network core.

For additional details, see FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1.

Front Panel Features

Figure 1-7 Cisco NAC-3355 Front Panel

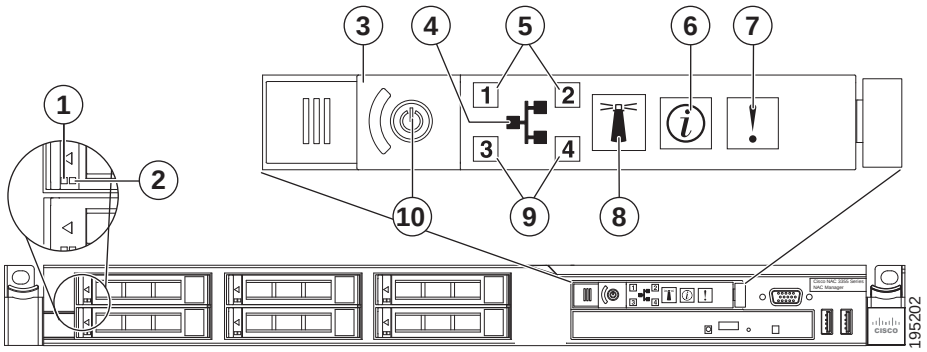


1	Hard disk drive (HDD) bay 0	8	Front USB port 1
2	Empty (unused) hard disk drive (HDD) bay [1]	9	Front USB port 2
3	Empty (unused) hard disk drive (HDD) bay [1]	10	CD-ROM/DVD drive
4	Power button with LED indicator (bicolor: green/amber)	11	Empty (unused) hard disk drive (HDD) bay [1]

5	Operator information panel	12	Empty (unused) hard disk drive (HDD) bay [1]
6	Operator information panel release switch	13	Hard disk drive (HDD) bay 1
7	Video port		

1. Cisco does not support installing additional hard drives in the NAC-3355 appliance.

Figure 1-8 Cisco NAC-3355 Front Panel LEDs/Buttons

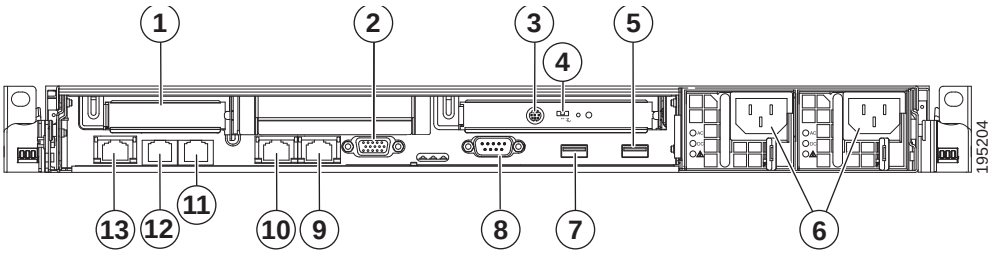


1	HDD activity LED	Green = Hard disk drive activity Flashing Green = Hard disk drive activity Off = Hard disk drive is idle or disabled
2	HDD status LED	Amber = Hard disk drive is in error state Off = Hard disk drive is functioning or disconnected from power
3	Power switch button cover	Slides left and right to expose or protect power switch
4	Ethernet icon LED	Green = Ethernet interfaces are configured and up Off = No Ethernet interfaces are currently configured or Ethernet interfaces are all down
5	Ethernet interface activity LEDs (NIC 1 and NIC 2)	Green = Activity exists Flashing green = Activity exists Off = No activity exists
6	Information LED	Amber = A non-critical system event has occurred Off = System is functioning normally
7	System health LED	Off = System health is normal Amber = A pre-failure system threshold has been breached. This can be any of the following: • At least one fan failure (system or processor fan) • At least one of the temperature sensors reached critical level (system or processor thermal sensors) • At least one memory module failure • A power supply unit error has occurred

8	Front Locator button/LED	Flashing blue = The Locator button has been pressed.
9	Ethernet interface activity LEDs (NIC 3 and NIC 4)	Green = Activity exists Flashing green = Activity exists Off = No activity exists
10	Power button with LED	Green = The appliance has AC power and is powered up Rapidly flashing green = The appliance is off and is not yet ready to be turned on (the appliance typically only remains in this state for 1 to 3 minutes) Slowly flashing green = The appliance is currently off and ready to be turned on slowly fading on/off green = The appliance is in power-save mode and is ready to be turned on Off = The appliance is powered off (AC power disconnected)

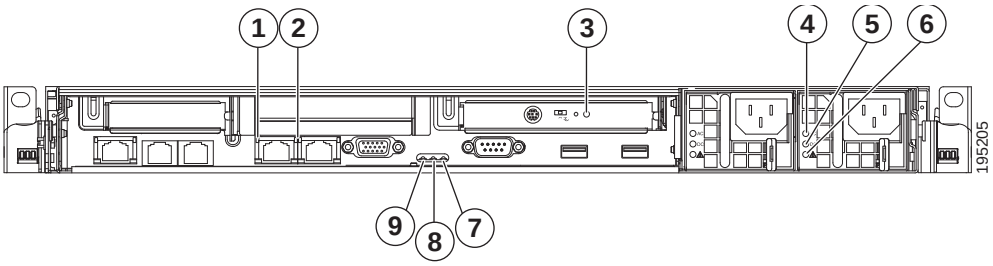
Rear Panel Features

Figure 1-9 Cisco NAC-3355 (With Installed FIPS Card) Rear Panel



1	FIPS card mini-DIN Smart card reader port	8	Serial port
2	FIPS card mode switch	9	NIC 2 (eth1) GbE interface
3	Video port	10	NIC 1 (eth0) GbE interface
4	Empty (unused) PCI slot	11	NIC 4 (eth3) add-on card
5	Rear USB port 4	12	NIC 3 (eth2) add-on card
6	Power supply cable sockets	13	Console port
7	Rear USB port 3		

Figure 1-10 Cisco NAC-3355 (With Installed FIPS Card) Rear Panel LEDs

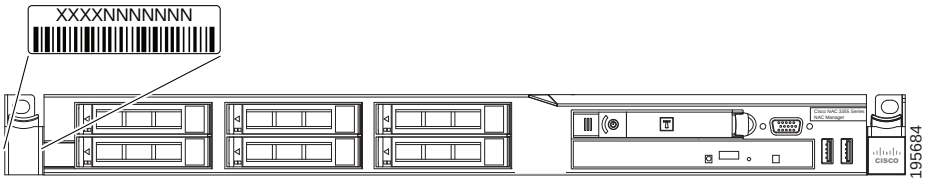


1	FIPS card status LED	Solid blue occasionally blinking off = FIPS card is enabled and accepting commands Two short blue flashes followed by a pause = FIPS card is in initialization mode Two longer blue flashes followed by a pause = FIPS card is in maintenance mode Repeatedly flashing morse code distress call (. . . - - - . . .)—three short blue flashes followed by three longer blue flashes followed again by three more short blue flashes = FIPS card is in error mode Off = There is no power source connected to the FIPS card
2	NIC 1 (eth0) activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
3	NIC 1 (eth0) link LED	Green = Link exists Off = No link exists
4	AC power LED	Green = AC power source is connected to power supply Off = No AC power source is connected to power supply
5	DC power LED	Green = DC power source is connected to power supply Off = No DC power source is connected to power supply
6	Power supply error LED	Amber = Power source to power supply is present, but power supply is in error state Off = Power supply is functioning normally (if AC and DC power indicators are green) or power supply is disconnected
7	System error LED	Amber = Indicates that a system error has occurred Off = The system is functioning normally
8	Rear Locator LED	Flashing blue = The Front Locator button has been pressed
9	Power LED	Green = The appliance has AC power and is powered up Rapidly flashing green = The appliance is off and is not yet ready to be turned on (the appliance typically only remains in this state for 1 to 3 minutes) Slowly flashing green = The appliance is currently off and ready to be turned on slowly fading on/off green = The appliance is in power-save mode and is ready to be turned on Off = The appliance is powered off (power is disconnected)

NAC-3395 Serial Number Location

The serial number label is located at the lower left of the front-panel of the NAC-3355. (See Figure 1-11.)

Figure 1-11 NAC-3395 Appliance Serial Number Location



Note The serial number for the NAC-3395 is 7 characters long. You can also view the NAC-3315 serial number location on the Cisco Support website using the Cisco Product Identification Tool. For details, see Cisco Product Identification Tool, page 1-27.

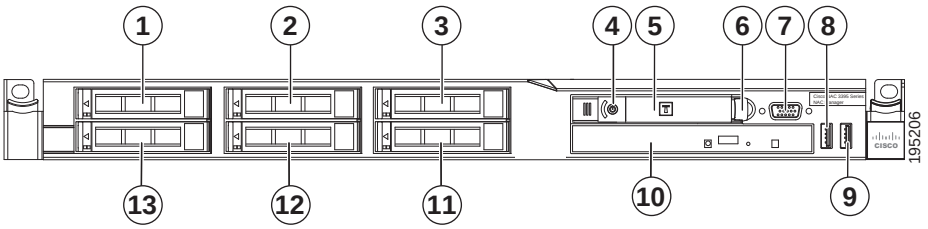
Cisco NAC-3395 Front and Rear Panels

The Cisco NAC-3395 FIPS 140-2 compliant platform provides the enhanced processing, memory, and power necessary for enterprise wide deployment of the Clean Access Super Manager (Super CAM) which can support up to 40 Clean Access Servers or 40 HA-CAS pairs. The Cisco NAC-3390 features dual processors, dual power supplies, 4 GB of RAM, 4 hard disk drives, 4 network interfaces, and an SSL accelerator card. For additional details, see FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1.

Note The Super CAM software is supported **only** on the Cisco NAC-3395 and Cisco NAC-3390 platforms.

Front Panel Features

Figure 1-12 Cisco NAC-3395 Front Panel

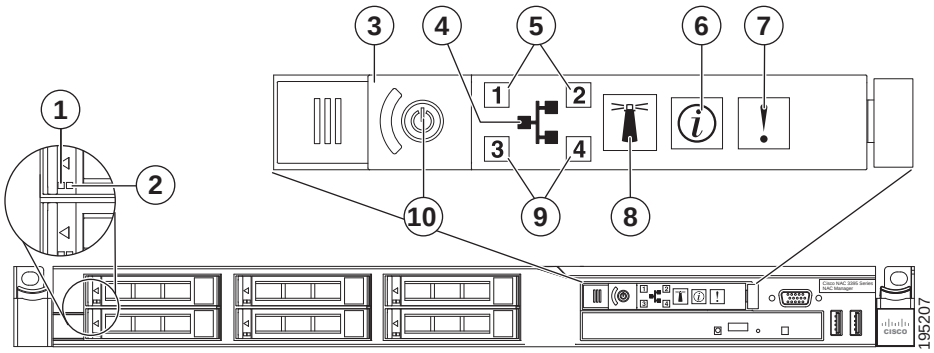


1	Hard disk drive (HDD) bay 0	8	Front USB port 1
2	Hard disk drive (HDD) bay 2	9	Front USB port 2
3	Empty (unused) hard disk drive (HDD) bay [1]	10	CD-ROM/DVD drive
4	Power button with LED indicator (bicolor: green/amber)	11	Empty (unused) hard disk drive (HDD) bay [1]

5	Operator information panel	12	Hard disk drive (HDD) bay 3
6	Operator information panel release switch	13	Hard disk drive (HDD) bay 1
7	Video port		

1. Cisco does not support installing additional hard drives in the NAC-3395 appliance.

Figure 1-13 Cisco NAC-3395 Front Panel LEDs/Buttons

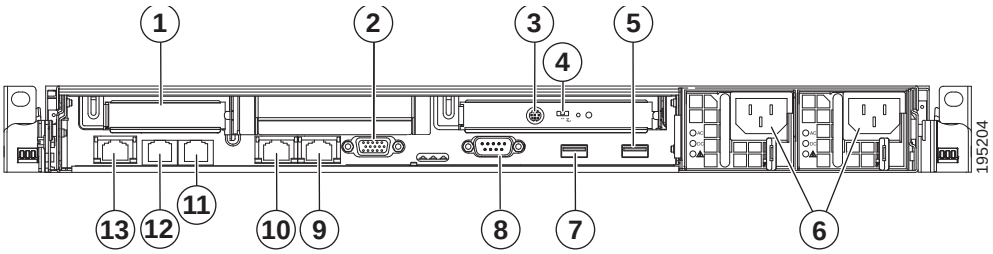


1	HDD activity LED	Green = Hard disk drive activity Flashing Green = Hard disk drive activity Off = Hard disk drive is idle or disabled
2	HDD status LED	Amber = Hard disk drive is in error state Off = Hard disk drive is functioning or disconnected from power
3	Power switch button cover	Slides left and right to expose or protect power switch
4	Ethernet icon LED	Green = Ethernet interfaces are configured and up Off = No Ethernet interfaces are currently configured or Ethernet interfaces are all down
5	Ethernet interface activity LEDs (NIC 1 and NIC 2)	Green = Activity exists Flashing green = Activity exists Off = No activity exists
6	Information LED	Amber = A non-critical system event has occurred Off = System is functioning normally
7	System health LED	Off = System health is normal Amber = A pre-failure system threshold has been breached. This can be any of the following: • At least one fan failure (system or processor fan) • At least one of the temperature sensors reached critical level (system or processor thermal sensors) • At least one memory module failure • A power supply unit error has occurred

8	Locator button/LED	Flashing blue = The Locator button has been pressed.
9	Ethernet interface activity LEDs (NIC 3 and NIC 4)	Green = Activity exists Flashing green = Activity exists Off = No activity exists
10	Power button/LED	Green = The appliance has AC power and is powered up Rapidly flashing green = The appliance is off and is not yet ready to be turned on (the appliance typically only remains in this state for 1 to 3 minutes) Slowly flashing green = The appliance is currently off and ready to be turned on slowly fading on/off green = The appliance is in power-save mode and is ready to be turned on Off = The appliance is powered off (AC power disconnected)

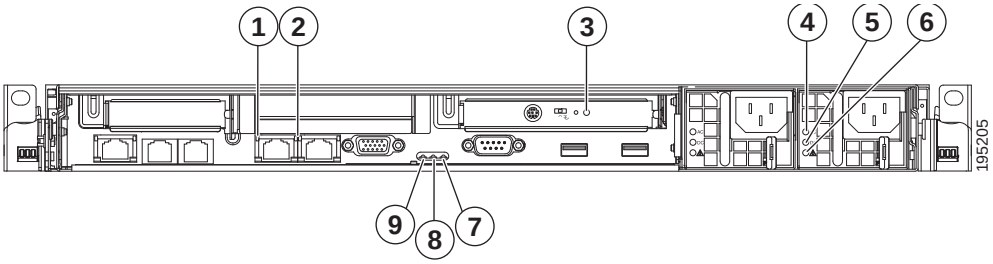
Rear Panel Features

Figure 1-14 Cisco NAC-3395 (With Installed FIPS Card) Rear Panel



1	FIPS card mini-DIN Smart card reader port	8	Serial port
2	FIPS card mode switch	9	NIC 2 (eth1) GbE interface
3	Video port	10	NIC 1 (eth0) GbE interface
4	Empty (unused) PCI slot	11	NIC 4 (eth3) add-on card
5	Rear USB port 4	12	NIC 3 (eth2) add-on card
6	Power supply cable sockets	13	Console port
7	Rear USB port 3		

Figure 1-15 Cisco NAC-3395 (With Installed FIPS Card) Rear Panel LEDs



1	FIPS card status LED	Solid blue occasionally blinking off = FIPS card is enabled and accepting commands Two short blue flashes followed by a pause = FIPS card is in initialization mode Two longer blue flashes followed by a pause = FIPS card is in maintenance mode Repeatedly flashing morse code distress call (. . . - - - . . .)—three short blue flashes followed by three longer blue flashes followed again by three more short blue flashes = FIPS card is in error mode Off = There is no power source connected to the FIPS card
2	NIC 1 (eth0) activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
3	NIC 1 (eth0) link LED	Green = Link exists Off = No link exists
4	AC power LED	Green = AC power source is connected to power supply Off = No AC power source is connected to power supply
5	DC power LED	Green = DC power source is connected to power supply Off = No DC power source is connected to power supply
6	Power supply error LED	Amber = Power source to power supply is present, but power supply is in error state Off = Power supply is functioning normally (if AC and DC power indicators are green) or power supply is disconnected
7	System error LED	Amber = Indicates that a system error has occurred Off = The system is functioning normally
8	Rear Locator LED	Flashing blue = The Front Locator button has been pressed
9	Power LED	Green = The appliance has AC power and is powered up Rapidly flashing green = The appliance is off and is not yet ready to be turned on (the appliance typically only remains in this state for 1 to 3 minutes) Slowly flashing green = The appliance is currently off and ready to be turned on slowly fading on/off green = The appliance is in power-save mode and is ready to be turned on Off = The appliance is powered off (power is disconnected)

NAC-3310, NAC-3350, and NAC-3390

Table 1-2 Cisco NAC Appliance Hardware Summary

Cisco NAC Appliance	Product	Hardware Specifications	Diagrams
NAC-3310 [1,2]	**MANAGER** Lite Manager supporting up to 3 standalone or HA-pair CASs **SERVER** CAS supporting 100, 250, or 500 users	• **Single processor**: Xeon 2.33 GHz dual core • 1 GB RAM • 160 GB NHP SATA HDD **Note** Newer Cisco NAC-3310 CAMs/CASs feature a 160GB hard drive, while older NAC-3310s originally shipped with 80GB hard drives. Both of these hard drive sizes support High Availability (HA) deployments, and you can safely deploy a 160GB model in an HA pair with an 80GB model. • **4 10/100/1000 LAN ports** [2 Broadcom 5721 integrated NICs; 2 Intel e1000 PCI-X NICs (HP #NC360T)] • CD/DVD-ROM Drive • 4 USB Ports (2 front, 2 rear) **Note** The NAC-3310 is based on the HP ProLiant DL140 G3 server platform.	• Figure 1-16 on page 1-18 “Cisco NAC-3310 Front Panel” • Figure 1-17 on page 1-19 “Cisco NAC-3310 Front Panel LEDs/Buttons” • Figure 1-18 on page 1-20 “Cisco NAC-3310 Rear Panel” • Figure 1-19 on page 1-20 “Cisco NAC-3310 Rear Panel LEDs”

Table 1-2 Cisco NAC Appliance Hardware Summary (continued)

Cisco NAC Appliance	Product	Hardware Specifications	Diagrams
NAC-3350 [3]	**MANAGER** Standard Manager supporting up to 20 standalone or HA-pair CASs **SERVER** CAS supporting 1500, 2500, or 3500 users	• **Single processor**: Xeon 3.0 GHz dual core • Dual power supply • 2 GB RAM • **2** x 72 GB SFF SAS RAID **HDD** • Smart Array E200i Controller • **4 10/100/1000 LAN ports** [2 Broadcom 5708 integrated NICs; 2 Intel e1000 PCI-X NICs (HP #NC360T)] • CD/DVD-ROM Drive • 4 USB Ports (1 front, 1 internal, 2 rear) • Cavium CN1120-NHB-E SSL Accelerator Card **Note** The NAC-3350 is based on the HP ProLiant DL360 G5 server platform.	• Figure 1-20 on page 1-21 "Cisco NAC-3350 Front Panel" • Figure 1-21 on page 1-22 "Cisco NAC-3350 Front Panel LEDs/Buttons" • Figure 1-22 on page 1-23 "Cisco NAC-3350 Rear Panel" • Figure 1-23 on page 1-23 "Cisco NAC-3350 Rear Panel LEDs"
NAC-3390 [3]	**MANAGER** Super Manager supporting up to 40 standalone or HA-pair CASs	• **Dual processor**: Xeon 3.0 GHz dual core • Dual power supply • 4 GB RAM • **4** x 72 GB SFF SAS RAID **HDD** • Smart Array E200i Controller • **4 10/100/1000 LAN ports** [2 Broadcom 5708 integrated NICs; 2 Intel e1000 PCI-X NICs (HP #NC360T)] • CD/DVD-ROM Drive • 4 USB Ports (1 front, 1 internal, 2 rear) • Cavium CN1120-NHB-E SSL Accelerator Card **Note** The NAC-3390 is based on the HP ProLiant DL360 G5 server platform.	• Figure 1-24 on page 1-25 "Cisco NAC-3390 Front Panel" • Figure 1-25 on page 1-25 "Cisco NAC-3390 Front Panel LEDs /Buttons" • Figure 1-26 on page 1-26 "Cisco NAC-3390 Rear Panel" • Figure 1-27 on page 1-26 "Cisco NAC-3390 Rear Panel LEDs/Buttons"

1. NAC-3310 may require a firmware/BIOS upgrade for HP ProLiant DL140 G3. See Upgrading Firmware, page 2-28.
2. NAC-3310 supports iLO (Lights Out 100i Remote Management). The default iLO "Administrator" account has default username/password: **admin**/**admin**. Defaults can be changed through the BIOS setup.
3. NAC-3350 and NAC-3390 support iLO2 (Integrated Lights Out, version 2). See panel tags for admin account details.

Cisco NAC-3310 Front and Rear Panels

Note The Cisco NAC-3310 is only FIPS-compliant after you have purchased and installed a field-replaceable FIPS card as described in the *Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide*.

The Cisco NAC-3310 Appliance is the recommended platform for Clean Access Lite Manager and Clean Access Server (100/250/500 user count) deployments. A NAC-3310 CAM Lite can manage up to 3 Clean Access Servers or 3 HA-CAS pairs. A NAC-3310 CAS can support 100, 250, or 500 users.

Note If Cisco NAC-3310 has been made FIPS-compliant, then NAC-3310 CAS can support only 250 or 500 users.

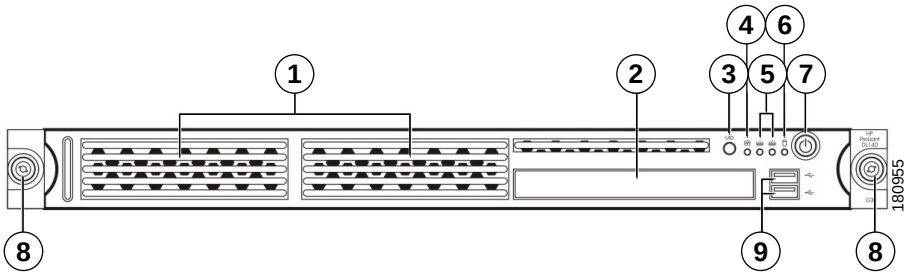
The Cisco NAC-3310 comes equipped with 4 network interfaces to provide flexibility in NIC interface selection and to facilitate CAS high availability configuration.

Note Newer Cisco NAC-3310 CAMs/CASs feature a 160GB hard drive, while older NAC-3310s originally shipped with 80GB hard drives. Both of these hard drive sizes support High Availability (HA) deployments, and you can safely deploy a 160GB model in an HA pair with an 80GB model.

For additional details, see FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1.

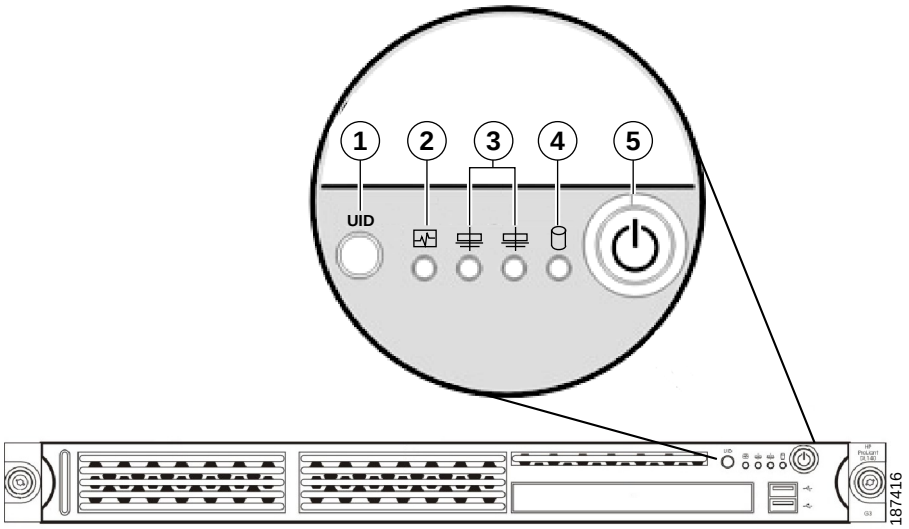
Front Panel Features

Figure 1-16 Cisco NAC-3310 Front Panel



1	Hard disk drive (HDD) bay	6	HDD activity LED indicator (green)
2	CD-ROM/DVD drive	7	Power button with LED indicator (bicolor: green/amber)
3	UID (Unit identification) button with recessed LED indicator (blue)	8	Thumbscrews for the front bezel
4	System health LED indicator (amber)	9	Front USB ports
5	Activity/link status LED indicators for NIC 1 (eth0) and NIC2 (eth1) (green)		

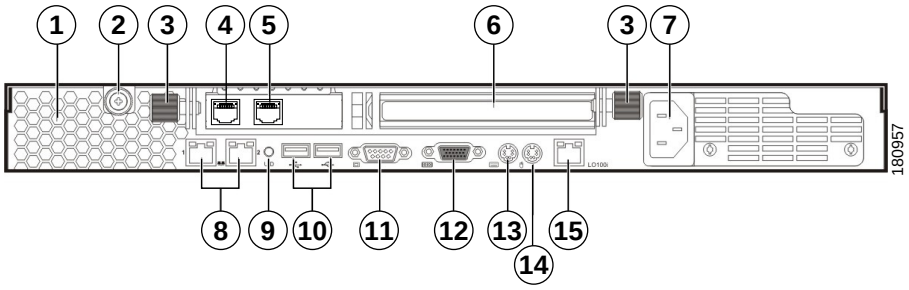
Figure 1-17 Cisco NAC-3310 Front Panel LEDs/Buttons



1	UID LED (recessed)	Blue = A UID button has been pressed.
2	System health LED	Off = System health is normal Amber = A pre-failure system threshold has been breached. This can be any of the following: • At least one fan failure (system or processor fan) • At least one of the temperature sensors reached critical level (system or processor thermal sensors) • At least one memory module failure • A power supply unit error has occurred
3	Activity/link status LED for NIC 1 (eth0) and NIC 2 (eth1)	Solid green = An active network link exists Flashing green = An ongoing network data activity exists Off = The server is off-line
4	HDD activity LEDs	Flashing green = Ongoing drive activity Off = No drive activity
5	Power status LED (recessed)	Green = The server has AC power and is powered up Amber = The server has AC power and is in standby mode Off = The server is powered off (AC power disconnected)

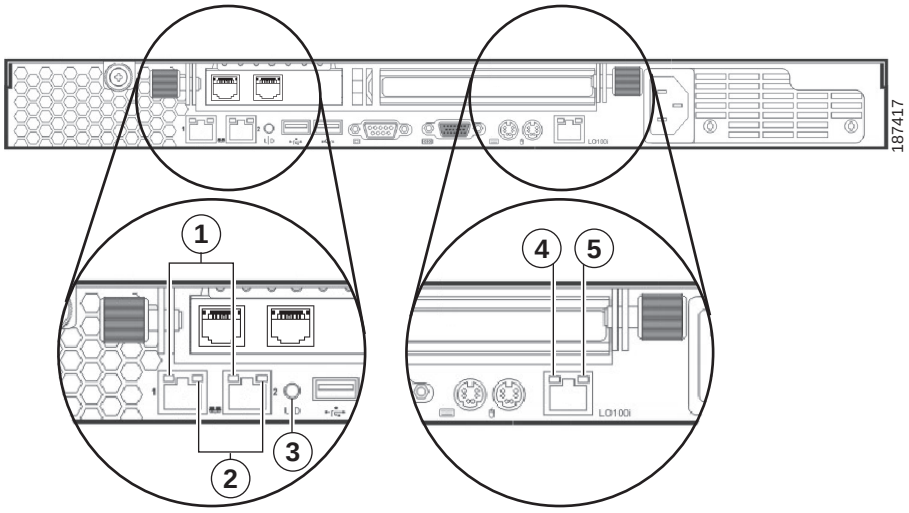
Rear Panel Features

Figure 1-18 Cisco NAC-3310 Rear Panel



1	Ventilation holes	9	UID button with recessed LED indicator (blue)
2	Thumbscrew for the top cover	10	Rear USB ports (black)
3	Thumbscrews for the PCI riser board assembly	11	Video port (blue)
4	NIC 3 (eth2) and NIC 4 (eth3) PCI Express GbE LAN (RJ-45) ports (Intel)	12	Serial port
5		13	PS/2 keyboard port (purple)
6	Standard height/full-length PCI Express x16/PCI-X riser board slot cover	14	PS/2 mouse port (green)
7	Power supply cable socket	15	10/100 Mbps iLO LAN port for IPMI management (RJ-45)
8	NIC 1 (eth0) and NIC 2 (eth1) integrated GbE LAN (RJ-45) ports (Broadcom)		

Figure 1-19 Cisco NAC-3310 Rear Panel LEDs



1	NIC activity/link status LEDs for NIC 1 (eth0) and NIC 2 (eth1)	Solid green = An active network link exists Flashing green = An ongoing network data activity exists Off = The server is off-line
2	NIC network speed LEDs	Steady amber = The LAN connection is using a GbE link Steady green = The LAN connection is using a 100 Mbps link Off = The LAN connection is using a 10 Mbps link
3	UID LED (recessed)	Blue = A UID button has been pressed
4	Link status LED for the 10/100 Mbps LAN port	Green = A network link exists Off = No network link exists
5	Activity status LED for the 10/100 Mbps LAN port	Flashing green = Network activity exists Off = No network activity exists

Cisco NAC-3350 Front and Rear Panels

Note The Cisco NAC-3350 is only FIPS-compliant after you have purchased and installed a field-replaceable FIPS card as described in the *Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide*.

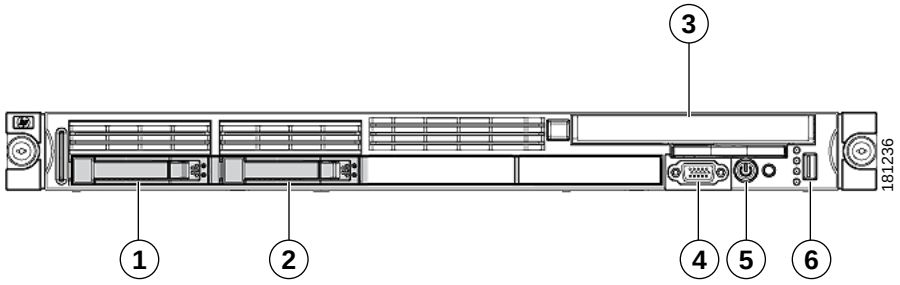
The Cisco NAC-3350 Appliance provides enhanced capability for enterprise wide Clean Access Standard Manager and Clean Access Server (1500/2500/3500 user count) deployments. A NAC-3350 Standard CAM can manage up to 20 Clean Access Servers or 20 HA-CAS pairs. A NAC-3350 CAS can support up to 1500, 2500, or 3500 users.

Similar to the Cisco NAC-3310, the Cisco NAC-3350 comes equipped with 4 network interfaces to provide flexibility in NIC interface selection and facilitate CAS high availability configuration. The Cisco NAC-3350 additionally provides 2 GB of RAM, two SAS drives configured in RAID 0 and 1, dual power supplies, and an SSL accelerator card to support large network deployments and provide added reliability for a centralized CAM/CAS deployment in the network core.

For additional details, see FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1.

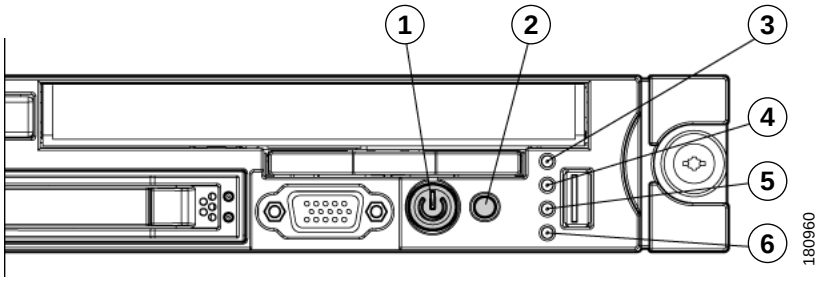
Front Panel Features

Figure 1-20 Cisco NAC-3350 Front Panel



1	Hard drive bay 1	4	Video connector
2	Hard drive bay 2	5	HP Systems Insight Display
3	CD-ROM/DVD drive	6	USB connector

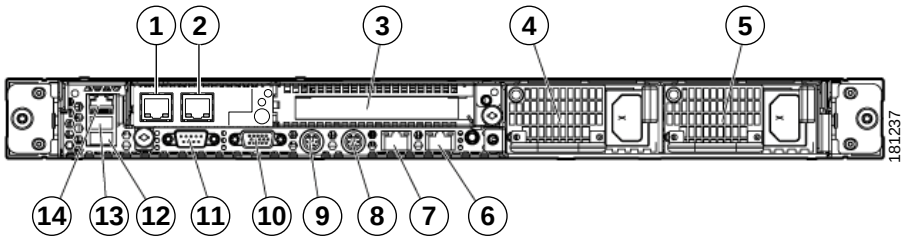
Figure 1-21 Cisco NAC-3350 Front Panel LEDs/Buttons



1	Power On/Standby button and system power LED	Green = System is on Amber = System is shut down, but power is still applied Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed; facility power is not available, or disconnected power button cable
2	UID button/LED	Blue = Identification is activated Flashing blue = System is being managed remotely Off = Identification is deactivated
3	Internal health LED	Green = System health is normal Amber = System health is degraded. (To identify the component in a degraded state, refer to “HP Systems Insight Display and LEDs.”) Red = System health is critical. (To identify the component in a critical state, refer to “HP Systems Insight Display and LEDs.”) Off = System health is normal when in standby mode
4	External health LED (power supply)	Green = Power supply health is normal Amber = Power redundancy failure occurred Off = Power supply health is normal when in standby mode
5	NIC 1 (eth0) link/activity LED	Green = Network link exists Flashing green = Network link and activity exist Off = No link to network exists If power is off, the front panel LED is not active. For status, view the rear panel LED for the RJ-45 connector (Figure 1-23 on page 1-23).
6	NIC 2 (eth1) link/activity LED	Green = Network link exists Flashing green = Network link and activity exist Off = No link to network exists If power is off, the front panel LED is not active. For status, view the rear panel LED for the RJ-45 connector (Figure 1-23 on page 1-23).

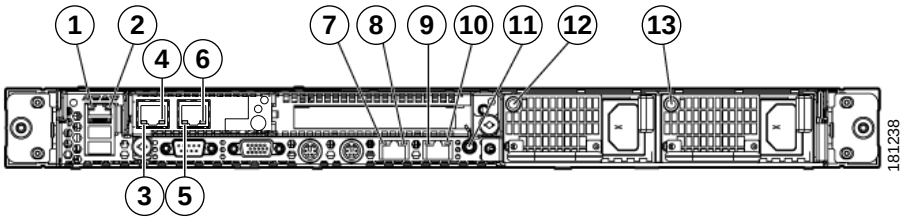
Rear Panel Features

Figure 1-22 Cisco NAC-3350 Rear Panel



1	NIC 3 (eth2) PCI-X port (Intel)	8	Keyboard connector (purple)
2	NIC 4 (eth3) PCI-X port (Intel)	9	Mouse connector (green)
3	PCI Express expansion slot 2	10	Video connector (blue)
4	Power supply bay 1	11	Serial connector
5	Power supply bay 2	12	USB connector
6	Integrated NIC 2 (eth1) port (Broadcom)	13	USB connector
7	Integrated NIC 1 (eth0) port (Broadcom)	14	iLO 2 NIC connector (RJ-45)

Figure 1-23 Cisco NAC-3350 Rear Panel LEDs



1	iLO 2 NIC activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
2	iLO 2 NIC link LED	Green = Link exists Off = No link exists
3	10/100/1000 NIC 3 (Intel) Activity LED	Steady green = High activity Flashing green = Activity exists Off = No activity (if link LED is off, link is dead)
4	10/100/1000 NIC 3 (Intel) Link LED	Orange = 1000 Mbps Green = 100 Mbps Off = 10 Mbps (if activity LED is off, link is dead)
5	10/100/1000 NIC 4 (Intel) Activity LED	Steady green = High activity Flashing green = Activity exists Off = No activity (if link LED is off, link is dead)
6	10/100/1000 NIC 4 (Intel) Link LED	Orange = 1000 Mbps Green = 100 Mbps Off = 10 Mbps (if activity LED is off, link is dead)

7	10/100/1000 NIC 1 (Broadcom) Activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
8	10/100/1000 NIC 1 (Broadcom) Link LED	Green = Link exists Off = No link exists
9	10/100/1000 NIC 2 (Broadcom) Activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
10	10/100/1000 NIC 2 (Broadcom) Link LED	Green = Link exists Off = No link exists
11	UID button/LED	Blue = Identification is activated Flashing blue = System is being managed remotely Off = Identification is deactivated
12	Power supply 1 LED	Green = Normal Off = System is off or power supply has failed
13	Power supply 2 LED	Green = Normal Off = System is off or power supply has failed

Cisco NAC-3390 Front and Rear Panels

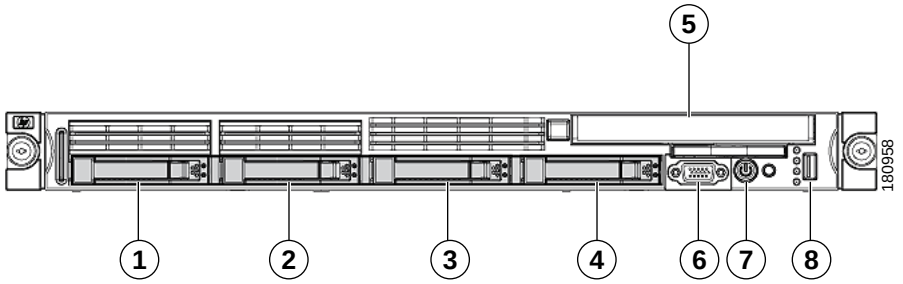
Note The Cisco NAC-3390 is only FIPS-compliant after you have purchased and installed a field-replaceable FIPS card as described in the *Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide*.

The Cisco NAC-3390 Appliance platform provides the enhanced processing, memory, and power necessary for enterprise wide deployment of the Clean Access Super Manager (Super CAM) which can support up to 40 Clean Access Servers or 40 HA-CAS pairs. The Cisco NAC-3390 features dual processors, dual power supplies, 4 GB of RAM, 4 hard disk drives, two integrated NICs, and an SSL accelerator. For additional details, see FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1.

Note The Super CAM software is supported **only** on the Cisco NAC-3395 and Cisco NAC-3390 platforms.

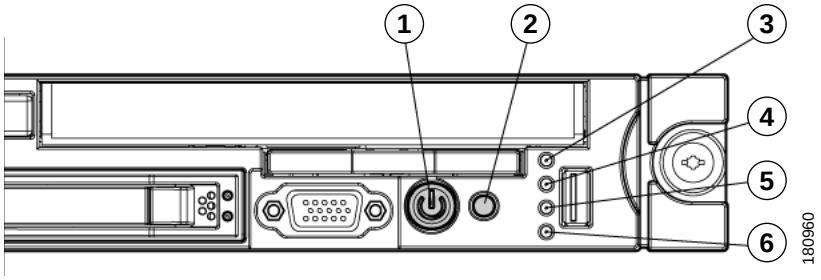
Front Panel Features

Figure 1-24 Cisco NAC-3390 Front Panel



1	Hard drive bay 1	5	CD-ROM/DVD drive
2	Hard drive bay 2	6	Video connector
3	Hard drive bay 3	7	HP Systems Insight Display
4	Hard drive bay 4	8	USB connector

Figure 1-25 Cisco NAC-3390 Front Panel LEDs /Buttons

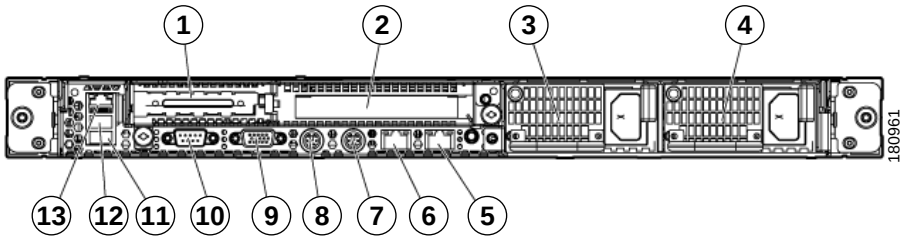


1	Power On/Standby button and system power LED	Green = System is on Amber = System is shut down, but power is still applied Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed; facility power is not available, or disconnected power button cable
2	UID button/LED	Blue = Identification is activated Flashing blue = System is being managed remotely Off = Identification is deactivated
3	Internal health LED	Green = System health is normal Amber = System health is degraded. (To identify the component in a degraded state, refer to “HP Systems Insight Display and LEDs.”) Red = System health is critical. (To identify the component in a critical state, refer to “HP Systems Insight Display and LEDs.”) Off = System health is normal when in standby mode

4	External health LED (power supply)	Green = Power supply health is normal Amber = Power redundancy failure occurred Off = Power supply health is normal when in standby mode
5	NIC 1 link/activity LED	Green = Network link exists Flashing green = Network link and activity exist Off = No link to network exists If power is off, the front panel LED is not active. For status, view the rear panel LED for the RJ-45 connector (Figure 1-27 on page 1-26)
6	NIC 2 link/activity LED	Green = Network link exists Flashing green = Network link and activity exist Off = No link to network exists If power is off, the front panel LED is not active. For status, view the rear panel LED for the RJ-45 connector (Figure 1-27 on page 1-26)

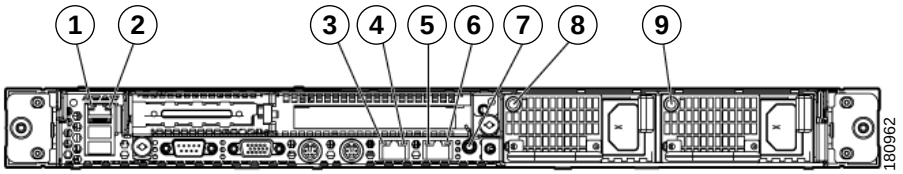
Rear Panel Features

Figure 1-26 Cisco NAC-3390 Rear Panel



1	PCI Express expansion slot 1, low-profile, half-length	8	Mouse connector (green)
2	Cavium SSL Accelerator Card (PCI Express expansion slot 2)	9	Video connector (blue)
3	Power supply bay 1	10	Serial connector
4	Power supply bay 2	11	USB connector
5	Integrated NIC 2 (eth1) port (Broadcom)	12	USB connector
6	Integrated NIC 1 (eth0) port (Broadcom)	13	iLO 2 NIC connector (RJ-45)
7	Keyboard connector (purple)		

Figure 1-27 Cisco NAC-3390 Rear Panel LEDs/Buttons



1	iLO 2 NIC activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
2	iLO 2 NIC link LED	Green = Link exists Off = No link exists
3	10/100/1000 NIC 1 Activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
4	10/100/1000 NIC 1 Link LED	Green = Link exists Off = No link exists
5	10/100/1000 NIC 2 Activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
6	10/100/1000 NIC 2 Link LED	Green = Link exists Off = No link exists
7	UID button/LED	Blue = Identification is activated Flashing blue = System is being managed remotely Off = Identification is deactivated
8	Power supply 1 LED	Green = Normal Off = System is off or power supply has failed
9	Power supply 2 LED	Green = Normal Off = System is off or power supply has failed

Cisco Product Identification Tool

The Cisco Product Identification (CPI) tool helps you retrieve the serial number of your Cisco products.

Before you submit a request for service online or by phone, use the CPI tool to locate your product serial number. You can access this tool from the Cisco Support website.

To access the Cisco Product Identification Tool:

Step 1 Click the **Get Tools & Resources** link.

Step 2 Click the **All Tools (A-Z)** tab.

Step 3 Select **Cisco Product Identification Tool** from the alphabetical drop-down list.

This tool offers three search options:

- Search by product ID or model name.
- Browse for Cisco model.
- Copy and paste the output of the **show** command to identify the product.

Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before you place a service call.

You can access the CPI tool at:

http://tools.cisco.com/Support/CPI/index.do

To access the CPI tool, you require a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at:

http://tools.cisco.com/RPF/register/register.do

CHAPTER 2

Preparing for Installation

This chapter provides preparatory installation instructions for Cisco NAC Appliance. It provides instructions for how to verify your hardware and other required equipment, install your Cisco NAC Appliance in a four-post rack, and upgrade the existing Cisco NAC Appliance software and chassis firmware.

Note This Installation Guide does not cover the Cisco NAC Network Module (NME-NAC-K9). For information on Cisco NAC Network Module installation and configuration, see *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

This chapter covers the following topics:

Safety Guidelines

Before you begin installing the Cisco NAC Appliance CAM/CAS, review the safety guidelines in this chapter and Rack-Mounting Your Cisco NAC Appliance CAM/CAS, page 2-14 to avoid injuring yourself or damaging the equipment.

This section contains:

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 may 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 trip 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 may get caught in the appliance chassis.
- Wear safety glasses when working under conditions that may 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.** 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 is intended to be grounded. Ensure that the host is connected to earth ground during normal use.** Statement 39

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 Cisco NAC Appliance CAM/CAS is electrically connected to ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the 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

A Cisco NAC Appliance CAM/CAS weighs between 15 lb (9.071 kg) and 33 lb (14.96 kg) depending on what hardware options are installed in the appliance. 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.

Preparing Your Site for Installation

Before installing a Cisco NAC Appliance CAM/CAS, it is important to prepare the following:

1. Prepare the site (see Site Planning, page 2-6) and review the installation plans or method of procedures (MOPs).
2. Unpack and inspect the appliance.
3. Gather the tools and test equipment required to properly install the appliance.

This section contains:

Site Planning

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

Typically, you should have prepared the installation site beforehand. As part of your preparation, obtain a floor plan of the site and the equipment rack where the Cisco NAC Appliance CAM/CAS will be housed. Determine the location of any existing appliances and their interconnections, including communications and power. Following the airflow guidelines (see Airflow Guidelines, page 2-8) ensures that adequate cooling air is provided to the appliance.

All personnel involved in the installation of the appliance, including installers, engineers, and supervisors, should participate in the preparation of a MOP for approval by the customer. For more information, see Method of Procedure, page 2-10.

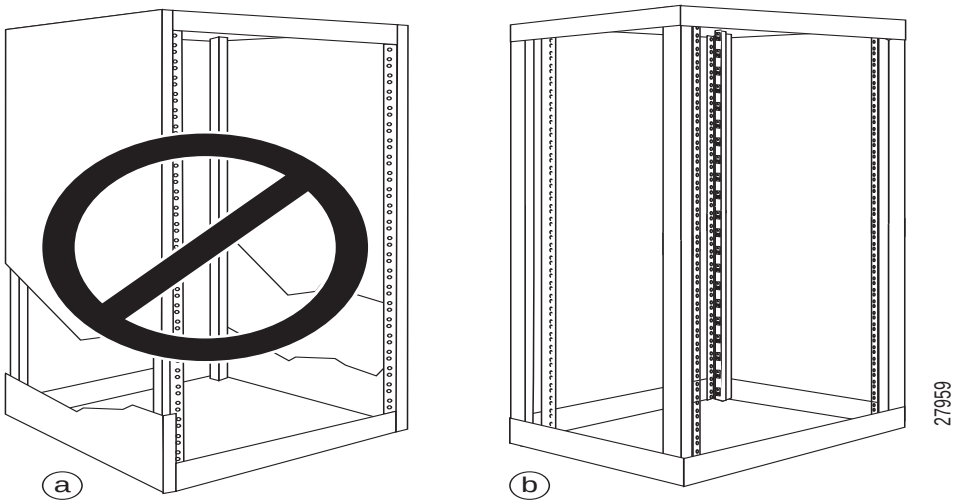
The following sections provide the site requirement guidelines that you must consider before installing the appliance:

Rack Installation Safety Guidelines

The Cisco NAC Appliance CAM/CAS can be mounted in most 4-post (telco-type), 19-inch equipment racks that comply with the Electronics Industries Association (EIA) standard for equipment racks (EIA-310-D). The rack must have at least two posts with mounting flanges to mount the appliance. The distance between the center lines of the mounting holes on the two mounting posts must be 18.31 inches +/- 0.06 inch (46.50 cm +/- 0.15 cm). The rack-mounting hardware included with the appliance is suitable for most 19-inch equipment racks or telco-type frames.

Figure 2-1 shows examples of a 4-post (telco-type) equipment racks.

Figure 2-1 Equipment Rack Types



Enclosed Rack (Do Not Use)

Figure 2-1a shows a freestanding, enclosed rack with two mounting posts in the front. The Cisco NAC Appliance CAM/CAS should *not* be installed in this type of enclosed rack, because the appliance requires an unobstructed flow of cooling air to maintain acceptable operating temperatures for its internal components. Installing the appliance in any type of enclosed rack—*even with the front and back doors removed*—could disrupt the airflow, trap heat next to the appliance, and cause an overtemperature condition inside the appliance.

4-Post (Open) Rack

Figure 2-1b shows a freestanding, 4-post open rack with two mounting posts in front and two mounting posts at the back. The mounting posts in this type of rack are often adjustable so that you can position the rack-mounted unit within the depth of the rack rather than flush-mount it with the front of the rack.

Before installing your Cisco NAC Appliance CAM/CAS in a rack, review the following guidelines:

- Two or more people are required to install the appliance in a rack.
- Ensure that the room air temperature is below 95°F (35°C).
- Do not block any air vents; usually, 6 inches (15 cm) of space provides proper airflow.

- Plan the appliance installation starting from the bottom of the rack.
- Do not extend more than one appliance out of the rack at the same time.
- Connect the appliance to a properly grounded outlet.
- Do not overload the power outlet when installing multiple devices in the rack.
- Do not place any object weighing more than 110 lb (50 kg) on top of rack-mounted devices.

Site Environment

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

The following precautions will help you plan an acceptable operating environment for your appliance and will help you avoid environmentally caused equipment failures:

- Ensure that the room where your appliance operates has adequate circulation. Electrical equipment generates heat. Without adequate circulation, ambient air temperature may not cool equipment to acceptable operating temperatures. For more information, see Airflow Guidelines, page 2-8.
- Ensure that the site of the rack includes provisions for source AC power, grounding, and network cables.
- Allow sufficient space to work around the rack during the installation. You need:
  - At least 3 feet (9.14 m) adjacent to the rack to move, align, and insert the appliance.
  - At least 24 inches (61 cm) of clearance in front of and behind the appliance for maintenance after installation.
- To mount the appliance between two posts or rails, the usable aperture (the width between the *inner* edges of the two mounting flanges) must be at least 17.7 inches (45.0 cm).

Note The rack-mount kit does not include a 2-post equipment rack.

- Use appropriate strain-relief methods to protect cables and equipment connections.
- To avoid noise interference in network interface cables, do not route them directly across or along power cables.
- Always follow ESD-prevention procedures as described in Preventing Electrostatic Discharge Damage, page 2-5 to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.

Airflow Guidelines

To ensure adequate airflow through the equipment rack, it is recommended that you maintain a clearance of at least 6 inches (15.24 cm) at the front and the rear of the rack. If airflow through the equipment rack and the appliances that occupy it is blocked or restricted, or if the ambient air being drawn into the rack is too warm, an overtemperature condition within the rack and the appliances that occupy it can occur.

The site should also be as dust-free as possible. Dust tends to clog the appliance fans, reducing the flow of cooling air through the equipment rack and the appliances that occupy it. This reduction increases the risk of an overtemperature condition.

Additionally, the following guidelines will help you plan your equipment rack configuration:

- Besides airflow, you must allow clearance around the rack for maintenance.
- When mounting an appliance in an open rack, ensure that the rack frame does not block the front intakes or the rear exhausts.

Temperature and Humidity Guidelines

Table 2-1 lists the operating and non-operating environmental site requirements for the Cisco NAC Appliance CAM/CAS. The appliance normally operates within the ranges listed; however, a temperature measurement approaching a minimum or maximum parameter indicates a potential problem. Maintain normal operation by anticipating and correcting environmental anomalies before they approach critical values by properly planning and preparing your site before you install the appliance.

Table 2-1 Operating and Nonoperating Environmental Specifications

Specification	Minimum	Maximum
Temperature, ambient operating	50°F (10°C)	95°F (35°C)
Temperature, ambient nonoperating and storage	-40°F (°C)	158°F (70°C)
Humidity, ambient (noncondensing) operating	10%	90%
Humidity, ambient (noncondensing) nonoperating and storage	5%	95%
Vibration, operating	5–500 Hz, 2.20 g RMS random	—

Power Considerations

You configure the Cisco NAC Appliance CAM/CAS with AC-input power only. Ensure that all power connections conform to the rules and regulations in the National Electrical Codes (NECs), as well as local codes. When planning power connections to your appliance, the following precautions and recommendations must be followed:

- Check the power at your site before installation and periodically after installation to ensure that you are receiving clean power (free of spikes and noise). Install a power conditioner if necessary.
- The AC power supply includes the following features:
  - Autoselect feature for 110-V or 220-V operation.
  - An electrical cord for all appliances. (A label near the power cord indicates the correct voltage, frequency, current draw, and power dissipation for the appliance.)

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

- Install proper grounding to your host equipment rack to avoid damage from lightning and power surges.

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

- The AC-input power supply that operates on input voltage and frequency within the ranges of 100 to 240 VRMS and 50/60 Hz without the need for operator adjustments.

Method of Procedure

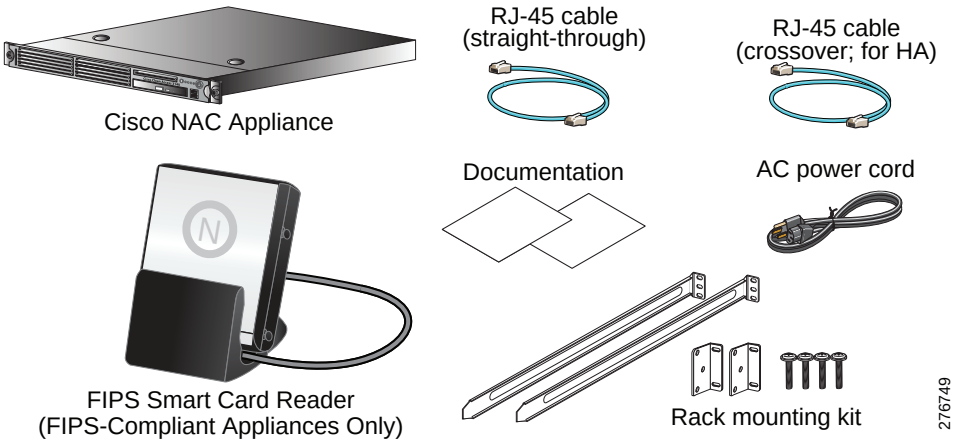
As described previously, part of your preparation includes reviewing installation plans or MOPs. An example of a MOP (a preinstallation checklist of tasks and considerations that need to be addressed and agreed upon before proceeding with the installation) is as follows:

1. Assign personnel.
2. Determine protection requirements for personnel, equipment, and tools.
3. Evaluate potential hazards that may 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 NAC Appliance CAM/CAS 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. For more information, see Required Equipment, page 2-11.
12. Perform the installation.

Shipping Package Contents

Verify the contents of the packing box, shown in Figure 2-2, to ensure that you have received all items necessary to install your Cisco NAC Appliance. Save the packing material in case you need to repack the unit. If any item is missing or damaged, contact your Cisco representative or reseller for instructions. Some Cisco NAC Appliance models might include additional items that are not shown.

Figure 2-2 Shipping Box Contents



Note Because product software is preloaded onto the Cisco NAC Appliance CAM/CAS, the shipping contents do not include a separate Cisco NAC Appliance software installation CD. Refer to Upgrading Cisco NAC Appliance Software, page 2-27 for additional details.

Failover Bundles

If you ordered a Failover Bundle, you will receive two physical Cisco NAC Appliances, and you will need to perform the initial configuration on each machine as described in this guide. After initial configuration is complete, configure High Availability (HA) using the CAM or CAS web console and physically connect the appliances to create the HA pair. Refer to Chapter 4, "Configuring High Availability (HA)"for CAM and CAS HA configuration details.

Note When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for the Cisco NAC Appliance CAM/CAS. Refer to the "Disable BIOS Redirection for Serial HA (Failover) Connections" section of the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for details.

Required Equipment

You need to supply a workstation (PC or laptop) and keyboard/monitor/mouse to run the Cisco NAC Appliance Configuration Utility on the appliance. Once the initial configuration is complete, you will need a standard (straight-through) Ethernet Category 5 network cable with RJ-45 connectors to connect the interfaces of the Cisco NAC Appliance to the network (eth0 for the CAM; eth0 and eth1 for the CAS). You will need a crossover RJ-45 Ethernet cable to connect HA-pair appliances together. The FIPS 140-2 Compliant and Non-FIPS Hardware Platforms, page 1-1 provides interface details for each model.

Configuration Worksheets

You will need the following information to complete the initial configuration of your Cisco NAC Appliances:

- Clean Access Manager (CAM) Configuration Worksheet
- Clean Access Server (CAS) Configuration Worksheet
- CAS Mode IP Addressing Considerations

Note If planning to configure your appliances for high availability (HA), you first must perform initial installation on each appliance, then configure HA via the CAM and/or CAS web console(s). You will need to create a virtual Service IP for the HA-pair via web configuration.

Clean Access Manager (CAM) Configuration Worksheet

Table 2-2 CAM Configuration Utility Worksheet

For Clean Access Manager NAC Appliance	
a. IP address for eth0 interface (trusted) [1]:	
b. Subnet mask (IP netmask) for eth0 interface:	
c. Default gateway IP address for eth0 interface:	
d. Host name for your CAM:	
e. IP address of Domain Name Server on your network:	
f. Master secret: **Note** The master secret must be the same for CAMs/CASs deployed as HA peers.	
g. Date, time and timezone:	
h. To generate the required temporary SSL certificate (you can change this at a later time): FQDN or IP address of CAM: Organization unit (e.g. Sales) Organization name (e.g. Cisco) Organization location (e.g. San Jose, CA, US) **Note** If using FQDN, make sure your DNS server is set up for the domain name.	
i. Root user password:	
j. Web console password [2]:	

1. eth0 and eth1 generally correlate to the first two network cards—NIC 1 and NIC 2—on the server hardware.
2. Cisco highly recommends replacing default password(s) with “strong” passwords (at least 8 characters long, comprised of a combination of two characters from each of the upper- and lower-case letters, numbers, and special characters categories)

Clean Access Server (CAS) Configuration Worksheet

Table 2-3 CAS Configuration Utility Worksheet

For Clean Access Server NAC Appliance	
a. IP address for eth0 interface (trusted) [1]:	
b. Subnet mask (IP netmask) for eth0 interface:	

Table 2-3 CAS Configuration Utility Worksheet

c. Default gateway IP address for eth0 interface:	
d. IP address for eth1 interface (untrusted):	
e. Subnet mask (IP netmask) for eth1 interface:	
f. Default gateway IP address for eth1 interface [1]:	
g. Host name for your CAS:	
h. IP address of Domain Name Server on your network:	
i. Master secret: **Note** The master secret must be the same for CAMs/CASs deployed as HA peers.	
j. Date, time and timezone:	
k. To generate the required temporary SSL certificate (you can change this at a later time): FQDN or eth0 IP address of CAS: Organization unit (e.g. Sales) Organization name (e.g. Cisco) Organization location (e.g. San Jose, CA, US) **Note** If using FQDN, make sure your DNS server is set up for the domain name.	
l. Root user password:	
m. Web console password [2]:	

1. eth0 and eth1 generally correlate to the first two network cards—NIC 1 and NIC 2—on the server hardware.
2. Cisco highly recommends replacing default password(s) with “strong” passwords (at least 8 characters long, comprised of a combination of two characters from each of the upper- and lower-case letters, numbers, and special characters categories)

CAS Mode IP Addressing Considerations

Table 2-4 CAS Modes— IP addressing Considerations

CAS Mode	Comments
Real-IP	• The trusted (eth0) and untrusted (eth1) interfaces of the CAS must be on different subnets. • Add static routes on the L3 switch or router to route traffic for the managed subnets to the trusted interface of the respective CASs. • If using DHCP relay, make sure the DHCP server has a route back to the managed subnets.

Table 2-4 CAS Modes— IP addressing Considerations (continued)

CAS Mode	Comments
Virtual Gateway	**CAUTION:** To avoid switch errors, do not connect the untrusted interface (eth1) of a Virtual Gateway (IB or OOB) CAS to the switch until after the CAS is added to the CAM via the web console, and VLAN mapping is configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* for details. • The CAS and CAM must be on different subnets (or VLANs). • The trusted (eth0) and untrusted interfaces (eth1) of the CAS can have the same IP address. (Note: this is equivalent to an L3 SVI IP address.) • All end devices in the bridged subnet must be on the CAS untrusted side. • The CAS is automatically configured for DHCP Passthrough when set to Virtual Gateway mode. • Managed subnets must be configured on the CAS for all the user subnets that are managed by the CAS. When configuring the Managed subnet, make sure that you type an unused IP address in that subnet (for the CAS to use), and not a subnet address. • Traffic from clients must pass through the CAS before hitting the gateway. • When the CAS is an OOB VGW, the following also applies: CAS interfaces must be on a separate subnet (or VLAN) from the CAM. The CAS management VLAN must be on a different VLAN than the user or Access VLANs. See also “Determining VLANs For Virtual Gateway” in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* for further details.

Rack-Mounting Your Cisco NAC Appliance CAM/CAS

Each Cisco NAC Appliance CAM/CAS has a set of rack handles (installed at the factory). You will use these handles later when you install the appliance in a 4-post rack. You can front (flush) mount or mid-mount the appliance in a 19-inch (48.3-cm) equipment rack that conforms to the 4-post rack specification (the inside width of the rack should be 17.5 inches [44.45 cm]). Mount the appliance in the brackets. When the appliance is installed in the rack, it requires one EIA 1.75-inch (4.4-cm) vertical mounting space or 1 rack unit (RU) for mounting.

This section addresses the following two procedures:

- Mounting the NAC-3315 Appliance in a 4-Post Rack, page 2-15
- Mounting the NAC-3355/3395 Appliance in a 4-Post Rack, page 2-21

Caution You must leave clearance in the front and rear of the Cisco NAC Appliance CAM/CAS to allow cooling air to be drawn in through the front and circulated through the appliance and out the rear of the appliance.

The Rack Installation Safety Guidelines, page 2-7 and the following information will help you plan the equipment rack configuration:

- When mounting an appliance in an equipment rack, ensure that the rack is bolted to the floor.

- Because you may install more than one appliance in the rack, ensure that the weight of all the appliances installed does not make the rack unstable.

Caution Some equipment racks are also secured to ceiling brackets due to the weight of the equipment in the rack. If you use this type of installation, make sure that the rack you are using to install the appliances is secured to the building structure.

- As mentioned in Airflow Guidelines, page 2-8, maintain a 6-inch (15.2-cm) clearance at the front and rear of the appliance to ensure adequate air intake and exhaust.
- Avoid installing appliances in an overly congested rack. Air flowing to or from other appliances in the rack might interfere with the normal flow of cooling air through the appliances, increasing the potential for overtemperature conditions within the appliances.
- Allow at least 24 inches (61 cm) of clearance at the front and rear of the rack for appliance maintenance.

Caution To prevent appliance overheating, never install an appliance in an enclosed rack or a room that is not properly ventilated or air conditioned.

- Follow your local practices for cable management. Ensure that cables to and from appliances do not impede access for performing equipment maintenance or upgrades.

Note The rack-mount hardware kit does not include a 2-post equipment rack.

Mounting the NAC-3315 Appliance in a 4-Post Rack

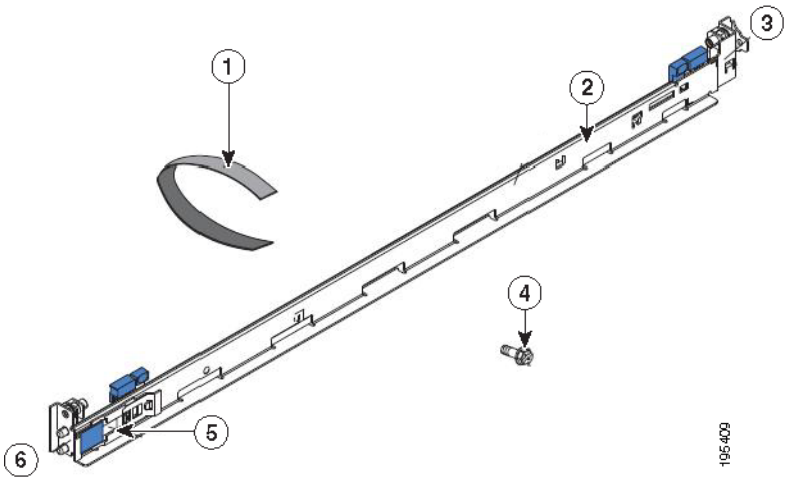
Warning **When the appliance is installed in a rack and is fully extended on its slide rail, it is possible for the rack to become unstable and tip over, which could cause serious injury. To eliminate the risk of rack instability from extending the rail or in the event of an earthquake, you should affix the rack to the floor.**

This section contains:

NAC-3315 4-Post Rack-Mount Hardware Kit

Figure 2-3 shows the items that you need to install the NAC-3315 appliance in a 4-post rack.

Figure 2-3 Release Levers on the NAC-3315 Slide Rail Hardware



1	Cable straps (6)	**4**	M6 screws (6)
2	Slide rail (2)	**5**	Shipping bracket
3	Front of rail	**6**	Rear of rail

Installing the NAC-3315 Slide Rails into a Rack

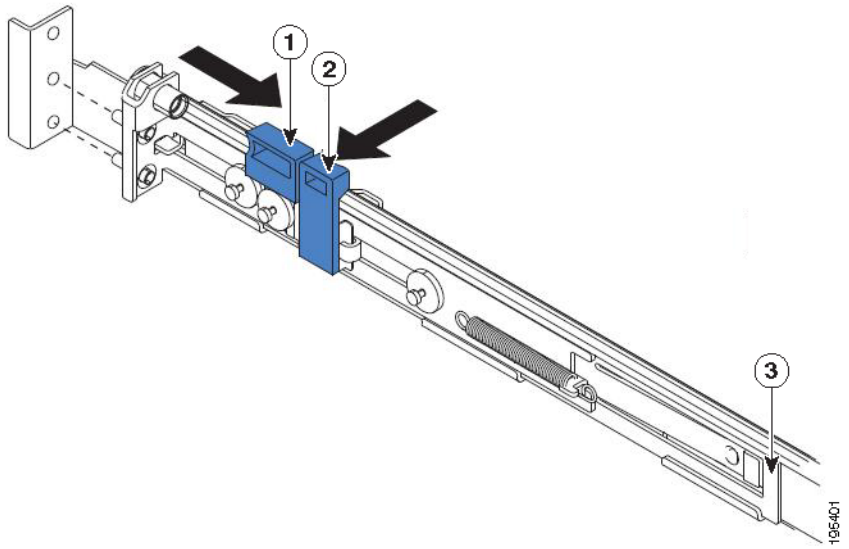
To install the NAC-3315 appliance in a rack:

Step 1 Press on the rail-adjustment bracket on the rear of the slide rail (see Figure 2-4) to prevent the bracket from moving.

Step 2 Press on Tab 1 and 2 (see Figure 2-4) and slide the rail-locking carrier toward the front of the slide rail until it snaps into place.

Step 3 Press on Tab 1 and 2 and slide the rail-locking carrier toward the rear of the slide until it snaps into place.

Figure 2-4 Installing the Slide Rail into the Rack



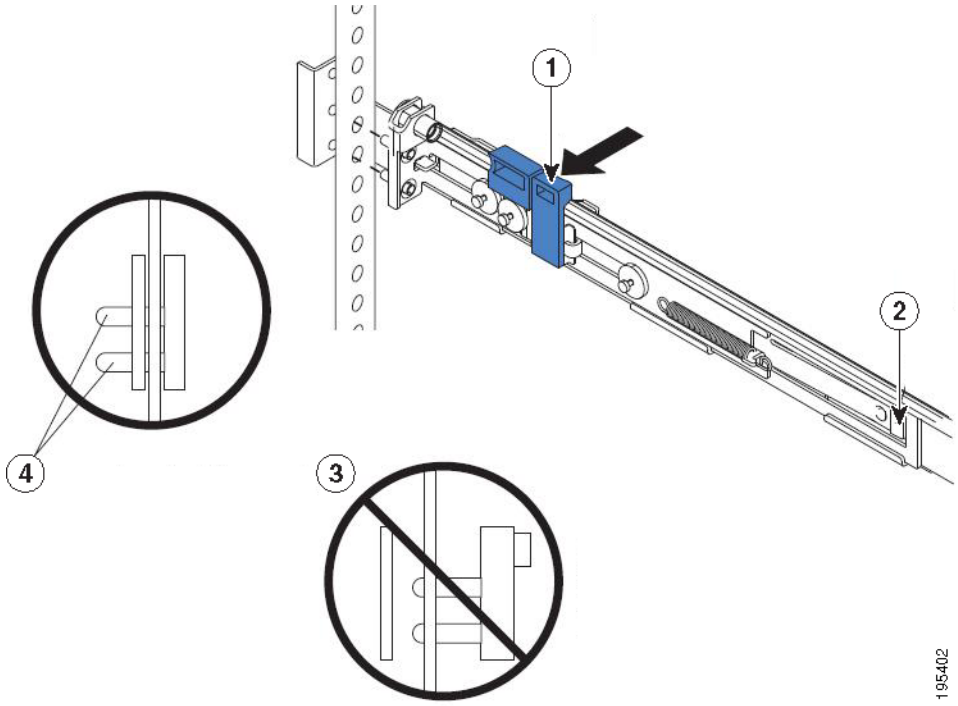
1	Adjustment tab 1	**3**	Rail-adjustment bracket
2	Adjustment tab 2		

Step 4 If you need to adjust the slide-rail length, lift the release tab (see Figure 2-5) and fully extend the rail-adjustment bracket from the rear of the slide rail until it snaps into place.

Step 5 Align the pins on the rear rail-locking carrier with the holes on the rear mounting flange. Then, press the tab (see Figure 2-5) to secure the rear of the slide rail to the rear mounting flange.

Note Ensure that the pins are fully extended through the mounting flange and slide rail.

Figure 2-5 Adjusting the Slide-rail Length



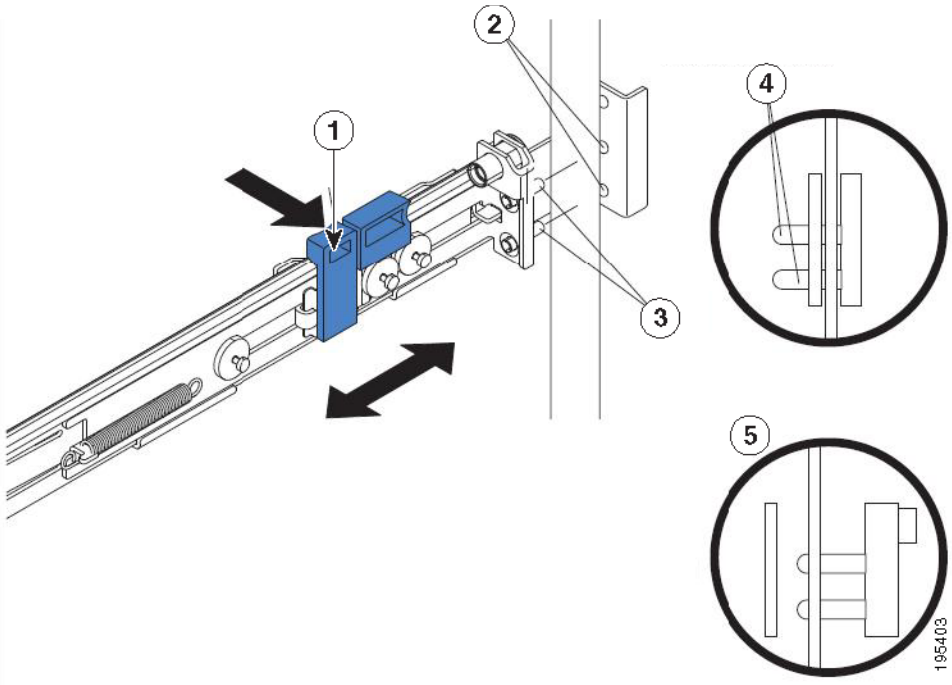
1	Adjustment tab	**3**	Pins not extended through the mounting flange and slide rail
2	Release tab	**4**	Pins extended through the mounting flange and slide rail

Step 6 Align the pins (see Figure 2-6) on the front rail-locking carrier to the front mounting flange. If you have adjusted the rail length, push the rail-locking carrier back toward the rear of the slide rail to align the slide rail with the mounting flange. Then, press the tab to secure the front of the slide rail to the front mounting flange.

Note Ensure that the pins are fully extended through the mounting flange and the slide rail.

Step 7 Repeat the steps from 1 to 6 for the other slide rail.

Figure 2-6 Aligning the Slide Rail with the Mounting Flange



1	Adjustment tab	**4**	Pins extended through the mounting flange and slide rail
2	Mounting flange	**5**	Pins not extended through the mounting flange and slide rail
3	Pins		

Installing the NAC-3315 Appliance into the Slide Rails

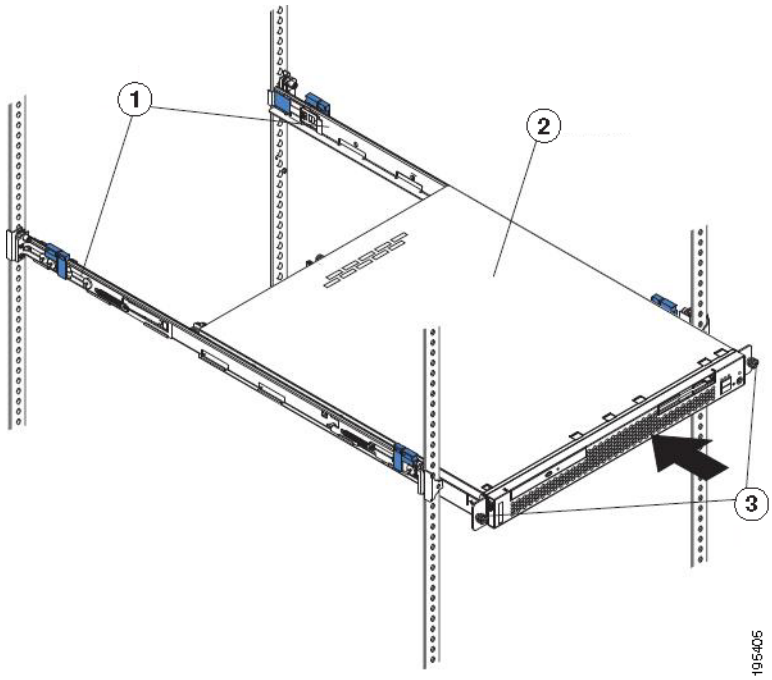
To install the NAC-3315 appliance in the slide rails:

Step 1 Align the CAM/CAS on the slide rails and push the CAM/CAS fully into the rack cabinet.

Step 2 Secure the CAM/CAS to the front mounting flanges with the captive thumbscrews (see Figure 2-7).

Note You must leave the shipping brackets attached to the slide rails unless the shipping brackets impede the CAM/CAS from sliding fully in the rack cabinet. If you need to remove the shipping brackets, see Step 3.

Figure 2-7 Aligning the NAC-3315 on the Slide Rails



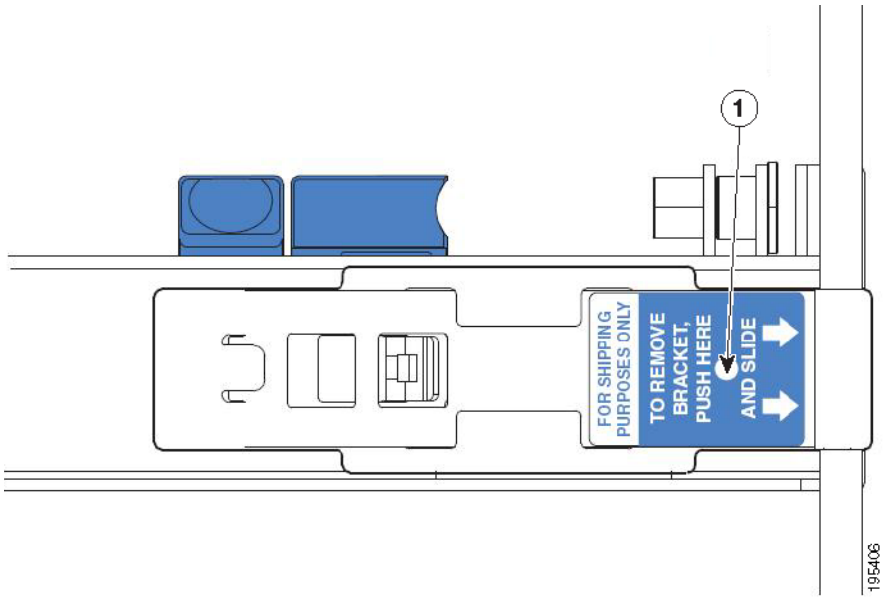
1	Shipping brackets	**3**	Thumbscrews
2	NAC-3315 appliance		

Step 3 Press on the release tab (see Figure 2-8) as indicated on the shipping bracket, and remove the shipping bracket from the slide rail.

Step 4 Repeat step 3 for the other shipping bracket. Store the shipping brackets for future use.

Note You must reinstall the shipping brackets on the slide rails before you transport the rack cabinet with the CAM/CAS installed. To reinstall the shipping brackets, reverse the steps.

Figure 2-8 Removing the Shipping Brackets



1	Release tab		

Mounting the NAC-3355/3395 Appliance in a 4-Post Rack

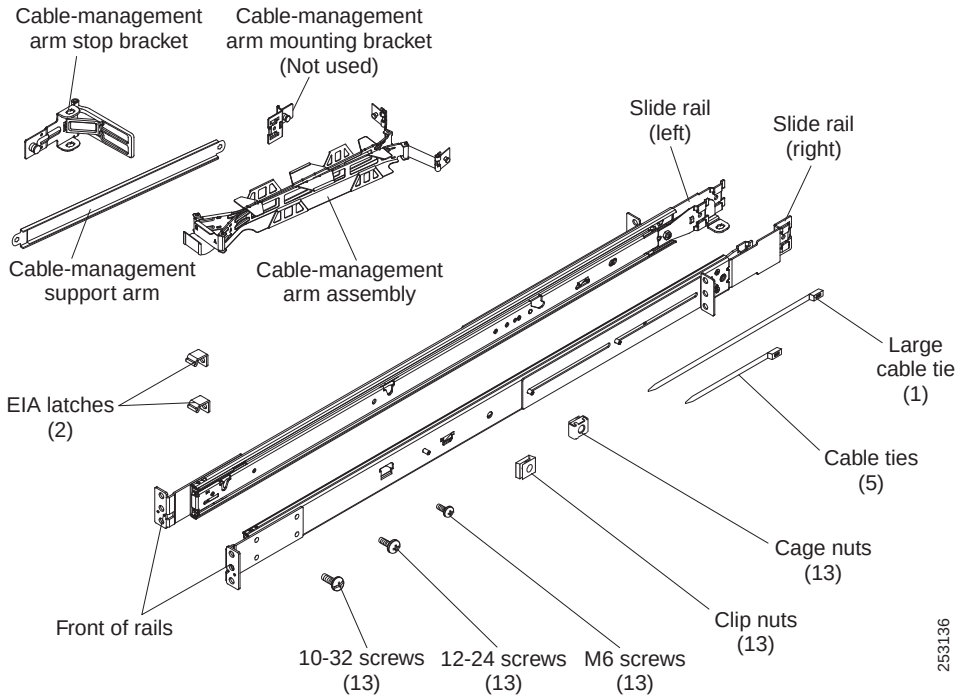
Warning **When the appliance is installed in a rack and is fully extended on its slide rail, it is possible for the rack to become unstable and tip over, which could cause serious injury. To eliminate the risk of rack instability from extending the rail or in the event of an earthquake, you should affix the rack to the floor.**

This section contains:

NAC-3355/3395 4-Post Rack-Mount Hardware Kit

Figure 2-9 shows the items that you need to install the NAC-3355/3395 appliance in a 4-post rack.

Figure 2-9 NAC-3355/3395 Rack Installation Kit Contents



Note Some of the items in Figure 2-9 are shipped in the NAC-3355/3395 shipping container, not necessarily with the rack installation kit.

Installing the NAC-3355/3395 Slide Rails Into the 4-Post Rack

When installing the NAC-3355/3395 slide rails in your equipment rack, Cisco recommends using cage nuts with square-holed racks, clip nuts with round-holed racks, and your own rack screws with thread-hole racks.

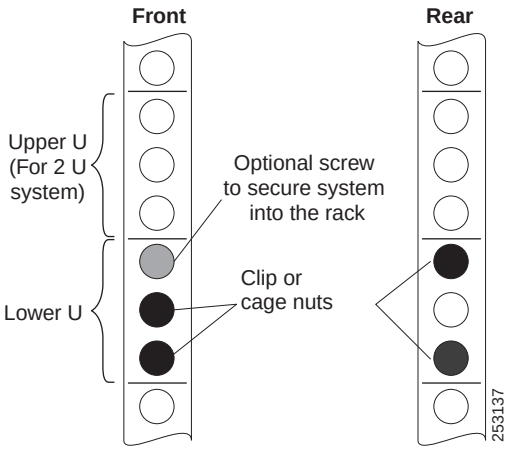
Note If the slide rails that arrived in your shipping container include shipping thumbscrews, remove them before performing the following procedure.

Step 1 Identify an available space in your rack to install the NAC-3355/3395.

Step 2 If you have either a round-holed or square-holed rack, install cage nuts or clip nuts, in the middle and bottom holes of the rack unit space on each side of the rack your NAC-3355/3395 will occupy (see Figure 2-10).

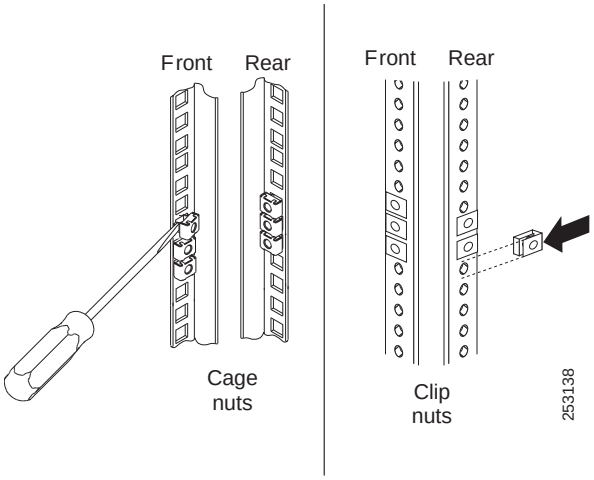
Step 3 Install cage nuts or clip nuts in the top and bottom holes for each side of the respective rear rack mounting rails (see Figure 2-10).

Figure 2-10 Position Cage Nuts or Clip Nuts



Step 4 Use a screwdriver to install the cage nuts or clip nuts on the inside of the mounting rail, as required for your particular rack, into the selected holes (see Figure 2-11).

Figure 2-11 Install Cage Nuts or Clip Nuts

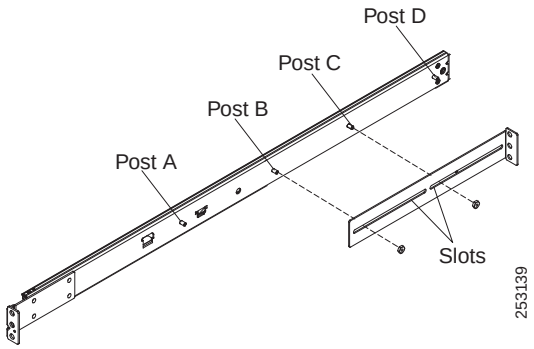


Step 5 Use the tab on the rear of the slide rails to align the rear of the slide rail to the rear of the 4-post rack.

Step 6 Select the best range among Posts A, B, C, and D to fit into the slots. Adjust the length of the slide rails by moving around the depth adjustment screws and nuts (see Figure 2-12).

Step 7 Once you have the combination and fit you want for your NAC-3355/3395, reinstall and tighten the screws and nuts for *both* slide rails.

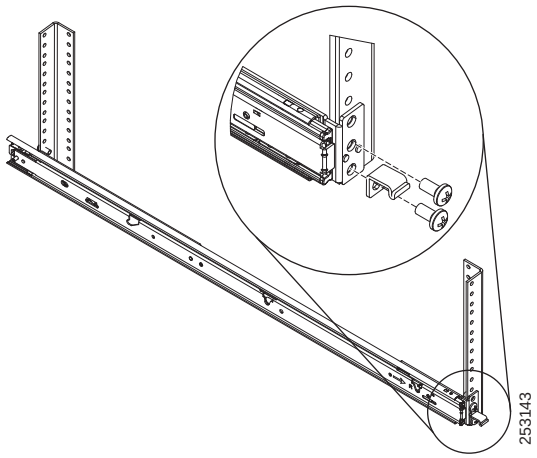
Figure 2-12 Set Up Slide Rails



Step 8 Fasten the front of the slide rail and EIA latch to the front of the 4-post rack by installing a screw in the bottom hole of the selected rack space for your NAC-3355/3395. Then, install another screw in the middle hole to secure the front of the slide rail to the 4-post rack (see Figure 2-13).

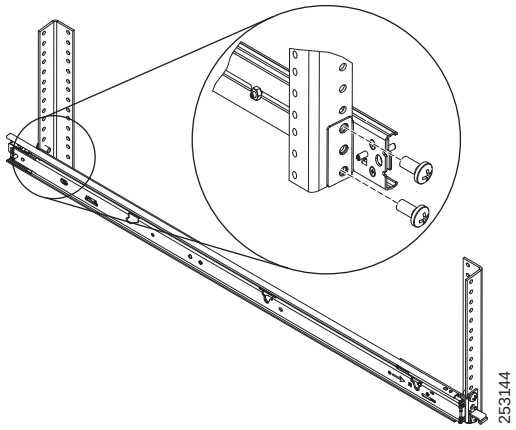
Note Use the 12-24 screws that came in the rack installation kit if you have installed clip nuts or cage nuts in the 4-post rack mounting rails.

Figure 2-13 Fasten Front of Slide Rail to 4-Post Rack



Step 9 Use two screws to fasten the rear of the slide rail to the respective rear mounting rail of the 4-post rack in the upper and bottom holes of the selected rack space for your NAC-3355/3395 (see Figure 2-14).

Figure 2-14 Fasten Rear of Slide Rail to 4-Post Rack



Step 10 Repeat Step 8 and Step 9 to attach the other slide rail to the selected rack space for your NAC-3355/3395.

Installing the NAC-3355/3395 Appliance Into the Slide Rails

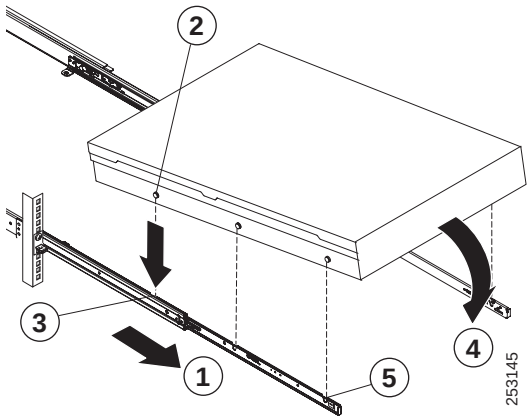
Step 1 Extend the slide rails forward out of the 4-post rack until they click (twice) into place.

Step 2 Carefully lift the NAC-3355/3395 and tilt it into position over the slide rails so that the rear chassis nail heads on the CAM/CAS line up with the rear slots on the slide rails (see Figure 2-15).

Step 3 Slide the CAM/CAS down so that the rear chassis nail heads slip into the two rear slots, and then slowly lower the front of the CAM/CAS until the other chassis nail heads slip into their respective slots on the slide rails.

Note Ensure that the front latch slides over the chassis nail heads.

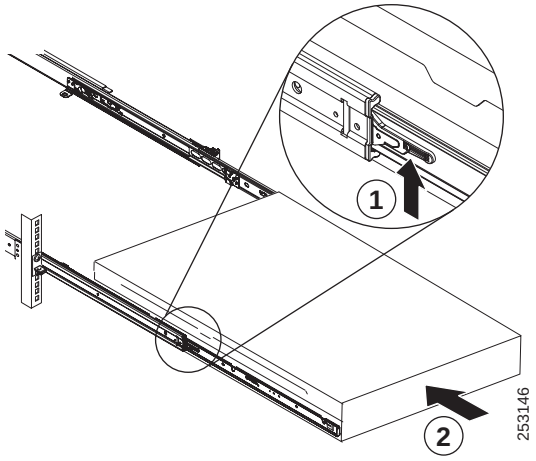
Figure 2-15 Position the NAC-3355/3395 In the Slide Rails



1	Extend the slide rails forward	**4**	Lower the CAM/CAS into position
2	Chassis nail heads	**5**	Front latches
3	Rear slide rail slots		

Step 4 Lift the locking levers on the slide rails and push the CAM/CAS all the way into the rack until it clicks into place (see Figure 2-16).

Figure 2-16 Push the NAC-3355/3395 Into the Rack



1	Locking levers	**2**	Push the CAM/CAS into the rack

Cisco NAC Appliance Licensing

You need at least one Clean Access Manager license and one Clean Access Server license for your Cisco NAC Appliance system to work. Both licenses are installed via the Clean Access Manager administration web console. For Out-of-Band (OOB) deployments, you must add both the OOB CAS license and the CAS as an Out-of-Band device to the CAM to access the OOB Management module of the CAM web console.

- For instructions on how to **obtain** new license(s) for your system, see *Cisco NAC Appliance Service Contract/Licensing Support*.
- For instructions on how to **install** licenses for your system (after initial configuration is complete), see Install CAM License, page 3-13 and Add Additional Licenses, page 3-15.

Upgrading Cisco NAC Appliance Software

Note This Installation Guide does not cover the Cisco NAC Network Module (NME-NAC-K9). For information on Cisco NAC Network Module installation and configuration, see *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

Cisco NAC Appliance CAMs/CASs are preloaded with a default version of the Cisco NAC Appliance software, which may not match the latest release image. Cisco recommends you always run the latest supported version of the system software to ensure you have the latest product enhancements and fixes.

You can install Cisco NAC Appliance Release 4.8(1) only on the following Cisco NAC Appliance platforms:

- NAC-3315, NAC-3355, and NAC-3395
- NAC-3310, NAC-3350, and NAC-3390
- Cisco NAC Network Module (NME-NAC-K9)

In addition to the above, you can install Cisco NAC Appliance Release 4.8 on CCA-3140 (EOL).

Note Due to limited hardware resources on the CCA-3140, some combinations of Release 4.8 features may cause undesirable system behavior. If you are experiencing problems with Release 4.8 on the CCA-3140, please contact the Cisco Technical Assistance Center (TAC).

Upgrading to Release 4.8(1)

In Cisco NAC Appliance release 4.8(1), you use a .tar.gz upgrade process similar to that used for upgrading CAM/CAS appliances in Cisco NAC Appliance Release 4.7(2), 4.5(x), and 4.6(1). (Cisco NAC Appliance release 4.7(0) and 4.7(1) requires users to perform “in-place” upgrades via an .ISO image on a CD-ROM.)

To upgrade to Release 4.8(1), follow the appropriate upgrade instructions in the “Upgrading” section of the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.

Note You cannot use the Release 4.8(1) .ISO CD-ROM to perform an upgrade. You must use the .tar.gz upgrade file method.

Downloading Cisco NAC Appliance Software

You can access the latest versions of the Cisco NAC Appliance Release 4.8(1) installation .ISO file as follows.

Caution Before downloading or installing any Cisco NAC Appliance software, make sure to refer to the *Release Notes for Cisco NAC Appliance, Version 4.8(1)* to understand the enhancements, caveats, and upgrade impact to your existing deployment.

Step 1 Log in to the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. You will likely be required to provide your CCO credentials.

Step 2 Navigate to **Security > Endpoint Security > Cisco Network Access Control > Cisco NAC Appliance > Cisco NAC Appliance 4.8**.

Step 3 Download the latest 4.8(1) .ISO image (e.g. **nac-4.8-K9.iso**) and burn the image as a bootable disk to a CD-R.

Note Cisco recommends burning the .ISO image to a CD-R using speeds 10x or lower. Higher speeds can result in corrupted/unbootable installation CDs.

Upgrading Firmware

Cisco NAC Appliance CAMs/CASs are subject to any system BIOS/Firmware upgrades required for the server model on which they are based.

- The NAC-3315 is based on the IBM System x3250 M2 server platform and the NAC-3355/3395 are based on the IBM System x3550 M2 server platform.
- The NAC-3310 is based on the HP ProLiant DL140 G3 server platform and the NAC-3350/3390 are based on the HP ProLiant DL360 G5 server platform.

Note For Cisco NAC-3310 platforms, be sure to also refer to the "DL140 G3 Required BIOS/Firmware Upgrades" section of the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for further details.

CHAPTER 3

Installing the Clean Access Manager and Clean Access Server

This chapter covers the following topics:

Overview

This chapter provides installation instructions for Cisco NAC Appliance. It provides instructions for how to initially configure your CAM and CAS using the Configuration Utility, access the CAM web console, and install product licenses. Once the initial configuration of your CAM and CAS is complete, you will be able to access the CAM web console to continue the rest of the configuration for your deployment.

For comprehensive configuration information, refer to the latest *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* and *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* documents available on Cisco.com under http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html. When using the online publications, make sure to refer to the documents that match the software version running on your Cisco NAC Appliance (e.g. “Release 4.8”).

Important Release Information

Refer to the *Release Notes for Cisco NAC Appliance, Version 4.8(1)* for additional and late-breaking information on 4.8(1) software releases.

Installing the Clean Access Manager

This section describes how to install the Clean Access Manager. Topics include:

Overview

The Cisco NAC Appliance CAM/CAS hardware platforms are Linux-based network hardware appliances which are pre-installed with either the CAM (MANAGER) or CAS (SERVER) application, the operating system, and all relevant components on a dedicated server machine. In Release 4.7(0) and later, the operating system comprises a hardened Linux kernel based on CentOS 5.3. Cisco NAC Appliance does not support the installation of any other packages or applications onto a CAM or CAS dedicated machine.

When you receive a new Cisco NAC Appliance, you will need to connect to the appliance and perform initial configuration.

If you want to install a different version of the software than what is shipped on the appliance, you can perform software installation via CD first. Refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for details on the software versions supported on Cisco NAC Appliance CAM/CAS platforms.

This chapter contains information for performing CD software installation and initial configuration of a Clean Access Manager.

With Cisco NAC Appliance software installation via CD, you must select whether to install the Clean Access Manager or Clean Access Server application. Once the CAM or CAS is installed on the dedicated appliance (application, OS, and relevant components), the installation of any other packages or applications on the CAM or CAS is not supported.

Note Static IP addresses must be configured for the CAM/CAS interfaces. DHCP mode is not supported for configuration of these interfaces.

Note For installation details on the Cisco NAC Network Module (CAS on a network module), refer to *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

Summary of Steps For New Installation

Note If relevant, back up your current Clean Access Manager configuration and save the snapshot to your local computer for safekeeping as described in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Step 1 Follow the instructions on your welcome letter to obtain a valid license file for your installation. Refer to the instructions in *Cisco NAC Appliance Service Contract/Licensing Support* for details. (If you are evaluating Cisco NAC Appliance, visit http://www.cisco.com/go/license/public to obtain an evaluation license.)

When you add the initial CAM license, the top of the CAM web console will display the type of Clean Access Manager license installed:

- **Cisco Clean Access Lite Manager** supports 3 Clean Access Servers
- **Cisco Clean Access Standard Manager** supports 20 Clean Access Servers
- **Cisco Clean Access Super Manager** supports 40 Clean Access Servers (SuperCAM runs only on the NAC-3390 platform)

Additionally, the **Administration > CCA Manager > Licensing** page will display the types of licenses present after they are added. See Install CAM License, page 3-13 for further details.

Step 2 Obtain a bootable CD of the latest version of the software. You can log in and download the latest 4.8(1) .ISO image from Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml, or click the “Download Software” link from the Cisco NAC Appliance support page here and burn it as a bootable disk to a CD-R.

Note Cisco recommends burning the .ISO image to a CD-R using speeds 10x or lower. Higher speeds can result in corrupted/unbootable installation CDs.

Step 3 Connect the CAM to the network and connect a monitor and keyboard to the CAM, or connect your workstation to the CAM via serial cable, as described in Connect the Clean Access Manager, page 3-4.

Step 4 Install the software as described in Install the Clean Access Manager (CAM) Software from CD-ROM, page 3-5.

Note If your NAC-3310 appliance does not read the software on the CD ROM drive and instead attempts to boot from the hard disk, before proceeding you will need to change the appliance settings to boot from CD ROM as described in Configuring Boot Settings on the Cisco NAC Appliance CAM/CAS, page 3-40.

Step 5 Perform the initial configuration of the CAM, as described in Perform the Initial CAM Configuration, page 3-6.

Note For High Availability mode, install and initially configure each CAM first before configuring HA. Refer to Installing a Clean Access Manager High Availability Pair, page 4-3 for details.

You must use identical appliances (e.g. NAC-3350 and NAC-3350) in order to configure High Availability (HA) pairs of Clean Access Managers (CAMs) or Clean Access Servers (CASs).

Step 6 Access the CAM web console and install a valid FlexLM license file for the Clean Access Manager as described in Access the CAM Web Console, page 3-11.

Step 7 In the web console, navigate to **Administration > CCA Manager > Licensing** to install any additional FlexLM license files for your Clean Access Servers, as described in Install CAM License, page 3-13.

Step 8 Add your Clean Access Server(s) to the Clean Access Manager, as described in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Connect the Clean Access Manager

To install the Clean Access Manager software from CD-ROM or to perform its initial configuration, you will need to connect the target machine and access the CAM's command line.

Step 1 The Clean Access Manager requires one of the two 10/100/1000BASE-TX interface connectors on the back panel of the CAM for its eth0 network interface. Connect the NIC1 network interface on the target machine to your local area network (LAN) using a CAT5 Ethernet cable.

Step 2 Connect the power by plugging one end of the AC power cord into the back of the machine and the other end into an electrical outlet.

Step 3 Connect the external FIPS Smart card reader module to a FIPS 140-2 compliant NAC-3315, NAC-3355, or NAC-3395 by plugging the Smart card reader mini-DIN cable into the female mini-DIN FIPS card port on the back of the appliance (see Figure 1-4 on page 1-6, Figure 1-9 on page 1-10, and Figure 1-14 on page 1-14). (Ensure you also have a Smart card inserted into the reader.)

Step 4 Power on the CAM by pressing the power button on the front of the machine. The diagnostic LEDs will flash a few times as part of an LED diagnostic test. Status messages are displayed on the console as the CAM boots up.

Step 5 Access the CAM's command line by either:

- Connecting a monitor and keyboard directly to the CAM via the keyboard connector and video monitor/console connector on the back panel.
- Connecting a serial cable from an external workstation (PC/laptop) to the CAM and open a serial connection using terminal emulation software (such as HyperTerminal or SecureCRT) on the external workstation, as described in Serial Connection to the CAM and CAS, page 3-39.

Note Cisco NAC Appliances assume the keyboard connected to be of US layout for both direct and IP-KVM connections. Use a US layout keyboard or ensure that you know the key mapping if you are connecting a keyboard of different layout.

Note The eth1 interface (NIC2) of the CAM is only required when connecting High Availability CAM pairs.

Note Static IP addresses must be configured for the CAM/CAS interfaces. DHCP mode is not supported for configuration of these interfaces.

Install the Clean Access Manager (CAM) Software from CD-ROM

The following steps describe how to perform optional CD installation of the Clean Access Manager software on the NAC-3310/3315 MANAGER, NAC-3350/3355 MANAGER, and NAC-3390/3395 MANAGER appliances.

Step 1 Connect the target installation machine to the network and access the command line of the machine by direct console or over a serial connection, as described in Serial Connection to the CAM and CAS, page 3-39.

Step 2 Download the latest software version supported on the target machine as follows:

a. Log in to the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. You will likely be required to provide your CCO credentials.

b. Navigate to **Security > Endpoint Security > Cisco Network Access Control > Cisco NAC Appliance > Cisco NAC Appliance 4.8**.

c. Download the latest 4.8(1) .ISO image (e.g. **nac-4.8-K9.iso**) and burn the image as a bootable disk to a CD-R.

Note Cisco recommends burning the .ISO image to a CD-R using speeds 10x or lower. Higher speeds can result in corrupted/unbootable installation CDs.

Step 3 Insert the CD-ROM containing the Cisco NAC Appliance .ISO file into the CD-ROM drive and reboot the machine.

Step 4 The Cisco Clean Access Installer welcome screen appears after the machine restarts:

```
Cisco Clean Access 4.8.1 Installer (C) 2010 Cisco Systems, Inc.

                Welcome to the Cisco Clean Access Installer!

 -  To install a Cisco Clean Access device, press the <ENTER> key.

 -  To install a Cisco Clean Access device over a serial console, enter serial a
t the boot prompt and press the <ENTER> key.

boot:
```

Step 5 At the "`boot`:" prompt, type one of the following options depending on the type of connection:

- Press the Enter key if your monitor and keyboard are directly connected to the appliance.
- Type **`serial`** and press enter in the terminal emulation console if you are accessing the appliance over a serial connection.

Step 6 If the install CD detects an existing installation of Cisco NAC Appliance, you are presented with the following prompt:

```
Checking for existing installations.
Clean Access Manager 4.7.0 installation detected.
Please choose one of the following actions:
1) Install.
2) Exit.
```

Step 7 Choose `1` to perform a fresh installation of the Cisco NAC Appliance software.

Step 8 Next, the Cisco NAC Appliance software installer asks you to specify whether you are installing a Clean Access Manager or Clean Access Server. At the following prompt, enter `1` to perform the installation for a Clean Access Manager.

```
Please choose one of the following configurations:
1) CCA Manager.
2) CCA Server.
3) Exit.
```

Caution Only one CD is used for installation of the Clean Access Manager or Clean Access Server software. You must select the appropriate type, **either** CAM or CAS, for the target machine on which you are performing installation.

Step 9 The Clean Access Manager Package Installation then executes. The installation takes several minutes. When finished, the installation script presents the following message, prompting you to press Enter to reboot the CAM and launch the Clean Access Manager quick configuration utility.

```
Installation complete. Press <ENTER> to continue
```

After you press Enter, the welcome screen for the Clean Access Manager quick configuration utility appears, and a series of questions prompt you for the initial configuration, as described in Perform the Initial CAM Configuration, next.

Perform the Initial CAM Configuration

When installing the Clean Access Manager from CD-ROM, the Configuration Utility Script automatically appears after the software packages install to prompt you for the initial configuration.

Note If necessary, you can always manually start the Configuration Utility Script as follows:

1. Over a serial connection or working directly on the CAM, log onto the CAM as user **`root`** with correct password.
2. Run the initial configuration script by entering the following command:

   `service perfigo config`

You can run the **`service perfigo config`** command to modify the configuration of the CAM if it cannot be reached through the web admin console. For further details on CLI commands, see CAM CLI Commands, page 3-42.

Configuration Utility Script

The configuration utility script suggests default values for particular parameters. To configure the installation, either accept the default value or provide a new one, as described below.

Step 1 After the software is installed from the CD and package installation is complete, the welcome script for the configuration utility appears:

```
Welcome to the Cisco Clean Access Manager quick configuration utility.
```

```
Note that you need to be root to execute this utility.

The utility will now ask you a series of configuration questions.
Please answer them carefully.

Cisco Clean Access Manager, (C) 2010 Cisco Systems, Inc.
```

Note If this prompt does not appear after you install the Cisco NAC Appliance software and restart the CAM, refer to Manually Restarting the CAM/CAS Configuration Utility, page 3-46.

Step 2 If your CAM is a FIPS-compliant platform (NAC-3315, NAC-3355, or NAC-3395) the first prompt asks if you want to initialize the on-board FIPS card (used to ensure FIPS compliant functions on the appliance). Otherwise, skip to Step 6.

```
Do you want to initialize the fips cards? (y/n)? [y]
```

Step 3 Choose **y** to enable FIPS on your appliance. The appliance automatically initializes the FIPS card and attempts to establish the security world.

```
 -- Running startup script 45drivers

 -- Running startup script 46exard

 -- Running startup script 50hardserver

Security world not found
Creating the security world and initializing the smart cards

Next, the FIPS setup process prompts you to specify how many Smart Cards (from 1-6) you
want to initialize to enable FIPS compliance on the CAM.
How many cards do you want to initialize (1-6)? [1]
Set ncipher card switch in i mode and press Return to continue
```

Step 4 Enter the number of Smart Cards you want to initialize, ensure that the FIPS card operation switch on the back of the CAM is switched to “I” (for “initialize”), and press Return.

```
Module 1, command ClearUnit: OK

Create Security World:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: unknown card
 Module 1 slot 0: - no passphrase specified - overwriting card
Module #1 Slot #0: Processing ...

Card writing complete.

security world generated on module #1; hknso = 909bd9f06542521a01f42fc881c8abcba
b0812ee
Set ncipher card switch in o mode and press Return to continue
```

Step 5 Switch the FIPS card switch back to “O” (for “operational”) and press Return.

```
Module 1, command ClearUnit: OK

Card(s) check passed

Do you want to continue with the rest of the NAC Manager Configuration?  (y/n)? [y]
```

Step 6 When prompted, enter an IP address for the eth0 (trusted) interface of the CAM.

```
Configuring the network interface:

Please enter the IP address for the interface eth0 []: 10.201.240.11
```

```
You entered 10.201.240.11 Is this correct? (y/n)? [y]
```

At the prompt, enter **y** to accept the default address, or **n** to specify another IP address. In this case, type the address you want to use for the trusted network interface in dotted-decimal format. Confirm the value when prompted.

Step 7 Type the subnet mask for the interface address at the prompt or press enter for the default. Confirm the value when prompted.

```
Please enter the netmask for the interface eth0 []: 255.255.255.0
You entered 255.255.255.0, is this correct? (y/n)? [y]
```

Step 8 Specify and confirm the address of the default gateway for the Clean Access Manager. This is typically the IP address of the router between the Clean Access Manager subnet and the Clean Access Server subnet.

```
Please enter the IP address for the default gateway []: 10.201.240.1
You entered 10.201.240.1. Is this correct? (y/n)? [y]
```

Step 9 Provide a host name for the Clean Access Manager. The host name will be matched with the interface address in your DNS server, enabling it to be used to access the Clean Access Manager admin console from a browser. The default host name is **nacmanager**.

```
Please enter the hostname [nacmanager]: cam3355
You entered cam3355 Is this correct? (y/n)? [y]
```

Step 10 Specify the IP address of the Domain Name System (DNS) server in your environment:

```
Please enter the IP addresses for the name servers: []: 63.93.96.94
You entered 63.93.96.94 Is this correct? (y/n)? [y]
```

Step 11 The Clean Access Managers and Clean Access Servers use a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to restore database snapshots on the CAM when you need them and are able to fail over to the HA peer CAM/CAS in HA deployments. (You cannot upload a CAM database snapshot that was created when the system was configured with a different master secret password, and HA-Secondary CAMs/CASs are not able to assume the “active” role following a failover event when the master secret passwords are different.) Type and confirm the master secret at the prompts.

```
The master secret is used to encrypt sensitive data.
Remember to configure all HA pairs with the same secret.
Please enter the master secret:
Please confirm the master secret:
```

Caution If your master secret is lost or becomes corrupted, use the procedure in Recover From Corrupted Master Secret, page 3-48.

Step 12 Specify the time zone in which the Clean Access Manager is located as follows:

```
The timezone is currently not set on this system.
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
```

a. Choose your region from the continents and oceans list. Type the number next to your location on the list, such as **2** for the Americas, and press Enter. Type **11** to enter the time zone in Posix TZ format, such as `GST-10`.

b. The next list that appears shows the countries for the region you chose. Choose your country from the country list, such as **47** for the United States, and press Enter.

c. If the country contains more than one time zone, the time zones for the country appears.

d. Choose the appropriate time zone region from the list, such as `21` for Pacific Time, and press Enter.

e. Confirm your choices by entering `1`, or use `2` to cancel and start over.

```
The following information has been given:
        United States
        Pacific Time
Is the above information OK?
1) Yes
2) No
#? 1
```

Step 13 Type and confirm the current date and time, using format hh:mm:ss mm/dd/yy.

```
Current date and time hh:mm:ss mm/dd/yy [11:53:12 08/22/08]: 11:53:12 08/22/08
You entered 11:53:12 08/22/08 Is this correct? (y/n)? [y] y
```

Step 14 Follow the prompts to configure the temporary SSL security certificate that enables secure connections between the CAM and the administrator web console as follows:

a. Type the IP address or domain name for which you want the certificate to be issued, or press enter to accept the default IP address (typically the eth0 IP address you already specified, for example `10.201.240.11`).

Note This is also the IP address or domain name to which the web server responds. If DNS is not already set up for a domain name, the CAM web console will not load. Make sure to create a DNS entry in your servers, or else use an IP address for the CAM.

b. For the organization unit name, enter the group **within** your organization that is responsible for the certificate (for example, `DOC`).

c. For the organization name, type the name of your organization or company for which you would like to receive the certificate (for example, `Cisco Systems`), and press Enter.

d. Type the name of the city or county in which your organization is legally located (for example, `San Jose`), and press Enter.

e. Type the two-character state code in which the organization is located (for example, `CA` or `NY`), and press Enter.

f. Type the two-letter country code (for example, `US`), and press Enter.

Step 15 Confirm values and press Enter to generate the SSL certificate or type `n` to restart.

```
You entered the following:
Domain: 10.201.240.11
Organization unit: DOC
Organization name: Cisco Systems
City name: San Jose
State code: CA
Country code: US
Is this correct? (y/n)? [y] y
```

Note You must generate the temporary SSL certificate or you will not be able to access the CAM web console.

Step 16 Specify whether or not you want the CAM to feature Pre-login Banner Support at the following prompt.

```
Enable Prelogin Banner Support? (y/n)? [n]
```

For more information and an example of the Pre-login Banner feature, see Figure 3-2 on page 3-14.

Step 17 Configure the **root** user password for the installed Linux operating system of the Clean Access Manager. The **root** user account is used to access the system over a serial connection or through SSH.

Cisco NAC Appliance supports using Strong Passwords for root user login. Passwords must be at least 8 characters long and feature a combination of upper- and lower-case letters, digits, and other characters. For example, the password **10-9=One** does not satisfy the requirements because it does not contain two characters from each category, but **1o-9=OnE** is a valid password. For more details, see the "Administering the CAM" chapter of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*.

```
For security reasons, it is highly recommended that you change the password for the root
user.

** Please enter a valid password for root user as per the requirements below! **

Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters,
digits, and other characters. Minimum of 8 characters and maximum
of 16 characters with characters from all of these classes. Minimum
of 2 characters from each of the four character classes is mandatory.
An upper case letter that begins the password and a digit that ends
it do not count towards the number of character classes used.

Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully.
```

Step 18 Next type the password for the **admin** user for the CAM direct access web console.

```
Please enter an appropriately secure password for the web console admin user.

New password for web console admin:
Confirm new password for web console admin:
Web console admin password changed successfully.
```

Note Passwords for web admin console users (including default user **admin**) are configured through the web console. See the "Manage System Passwords" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for details.

Step 19 The final step in the initial configuration process is to choose whether or not to turn on FIPS mode for your NAC-3315, NAC-3355, or NAC-3395 CAM. To enable FIPS operation, enter **y** at the following prompt.

```
Would you like to turn on fips mode? (y/n)? [y]

 -- Running startup script 45drivers

 -- Running startup script 46exard

 -- Running startup script 50hardserver

Security world already exists
```

Step 20 If you want to initialize any additional Smart cards at this time, enter **y** at the following prompt. Otherwise, enter **n** to complete the FIPS set up process.

```
Do you want to recreate security world and initialize cards (y/n)? [n]
writing RSA key
```

```
Card(s) check passed
```

Step 21 After the configuration is complete, press Enter to reboot the CAM. After rebooting, the CAM will be accessible from the web console.

```
Configuration is complete.
Changes require a REBOOT of Clean Access Manager.
```

Enter the following command to reboot the CAM after configuration is complete:

```
# reboot
```

The CAM initial configuration is now complete.

Step 22 After restarting, test the CAM installation:

a. Ping the eth0 interface address from a command line. If working properly, the interface should respond to the ping.

b. For a FIPS-compliant CAM, verify FIPS functionality as follows:

- Ensure the FIPS card operation switch is set to “O” (for operational mode).
- Log into the CAM console interface as `root`.
- Navigate to the **/perfigo/common/bin/** directory.
- Enter `./test_fips.sh info` and verify the following output:

```
Installed FIPS card is nCipher
Info-FIPS file exists
Info-card is in operational mode
Info-httpd worker is in FIPS mode
Info-sshd up
```

c. If the CAM does not respond, try connecting to the CAM using SSH (Secure Shell). Connect with the `root` username and password. Once connected, try pinging the default gateway to see if the CAM can reach the external network.

If after installation you need to reset the initial configuration settings for the CAM, connect to the CAM machine directly or through SSH and use the CLI command `service perfigo config`.

Once the CAM is configured, you will be able to access the CAM web console to add product licenses, and add initially configured Clean Access Servers to the CAM for management and further configuration, as described in Access the CAM Web Console, page 3-11.

If both tests fail, make sure that you have configured the IP address correctly and that the other network settings are correct.

The CAM should now be accessible through the web console, as described in Access the CAM Web Console, page 3-11.

- For the commands to manually stop and start the CAM, see CAM CLI Commands, page 3-42.
- For network card configuration issues, see Configuring Additional NIC Cards, page 3-37.

Access the CAM Web Console

The Clean Access Manager web administration console is the primary interface for administering the Cisco NAC Appliance deployment. After initial configuration is complete, use the following steps to access the CAM web console.

Warning **You must already have obtained a product or evaluation license to access the CAM/CAS and CAM web console. Refer to *Cisco NAC Appliance Service Contract / Licensing Support* for complete step-by-step instructions on how to obtain and install product licenses and obtain service contract support for Cisco NAC Appliance.**

Step 1 Launch a web browser from a computer accessible to the CAM by network.

Step 2 If you are using Internet Explorer Version 6 to access the CAM (and CAS) web console, ensure you have enabled TLS version 1 in the browser Advanced settings. For details, see Enabling TLSv1 on Internet Explorer Version 6, page 3-49.

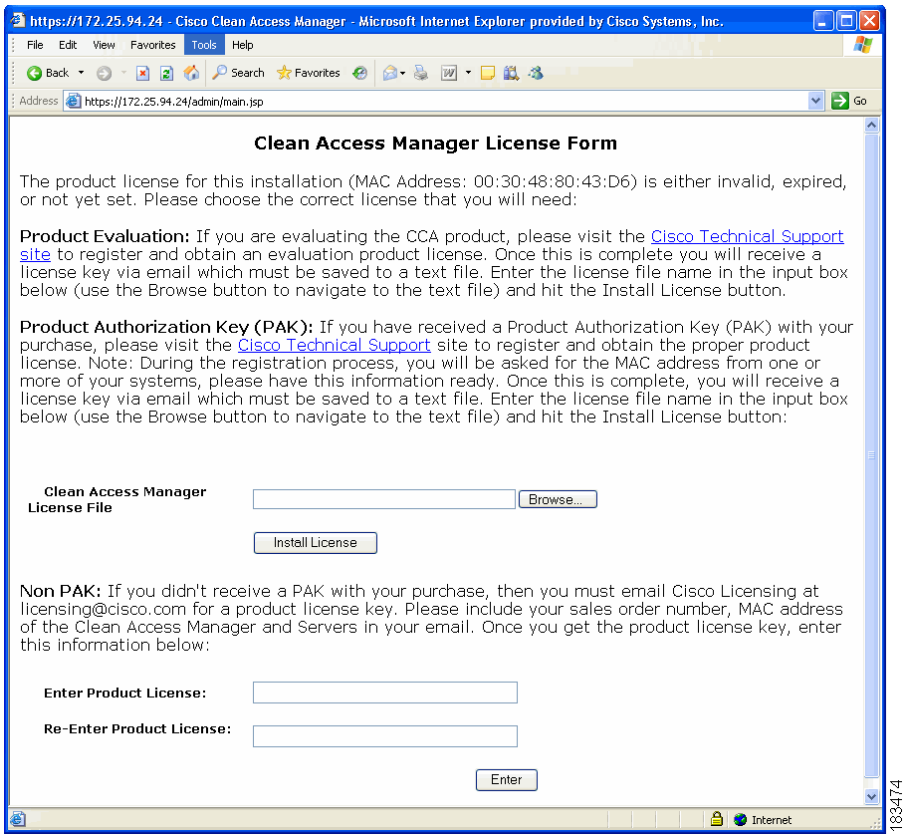
Step 3 In the URL/address field, type the IP address of the CAM (or the host name if you have made the required entry in your DNS server).

Step 4 If using a temporary SSL certificate, the security alert appears and you are prompted to accept the certificate. Click **Yes** to accept the certificate. (If using signed certificates, security dialogs do not appear.)

The **Clean Access Manager License Form** (Figure 3-1) appears and prompts you to install your CAM FlexLM license file. For reference, the top of the form displays the CAM's eth0 MAC address. You will need to obtain and save your product license files to disk on the PC/laptop from which you are accessing the CAM web console. See *Cisco NAC Appliance Service Contract/Licensing Support* for details on how to obtain product and evaluation licenses.

Note To aid in license requests, the top of the form displays the CAM's eth0 MAC address.

Figure 3-1 Clean Access Manager License Form



Install CAM License

Step 5 Browse to the license file you received in the **Clean Access Manager License File** field and click the **Install License** button.

Step 6 To enter a license in the **Clean Access Manager License File** field, click the **Browse** button to locate the license file you received for the CAM and click the **Install License** button.

Note If you have purchased a CAM Failover (HA) license, install the Failover license to the Primary CAM first, then load all the other licenses. This facilitates upgrading CAM HA-pairs.

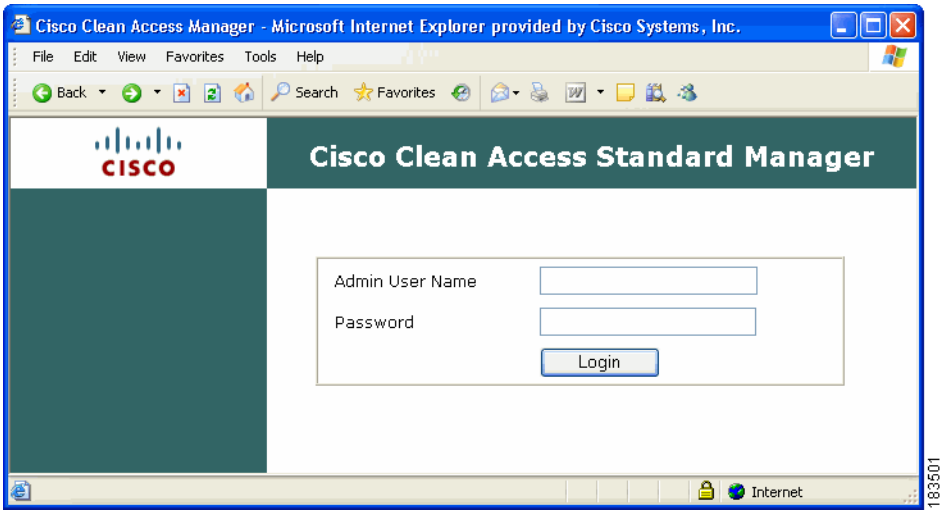
Step 7 Once the license is accepted, the customizable CAM Pre-login Banner (Figure 3-2) appears (if you have chosen to enable Pre-login Banners during your initial CAM configuration) or the web admin console login window appears (Figure 3-3). Type the username **admin** and web admin user password, and click **Login**.

Figure 3-2 CAM Prelogin Banner Example

The Pre-login Banner enables you to present a broad range of messages, including warnings, system/network status, access requirements, etc., to administrator users before they enter authentication credentials in the CAM/CAS. Administrators can specify the text of the Pre-login Banner by enabling this feature on the appliance, logging into the command-line console, and editing the **/root/banner.pre** file. The text of the Pre-login Banner appears in both the web console interface and the command-line interface when admin users are logging into the CAM/CAS.

You can enable or disable the Pre-login Banner during the initial CAM/CAS configuration CLI session and whenever you choose to alter your base CAM/CAS configuration with the `service perfigo config` CLI command.

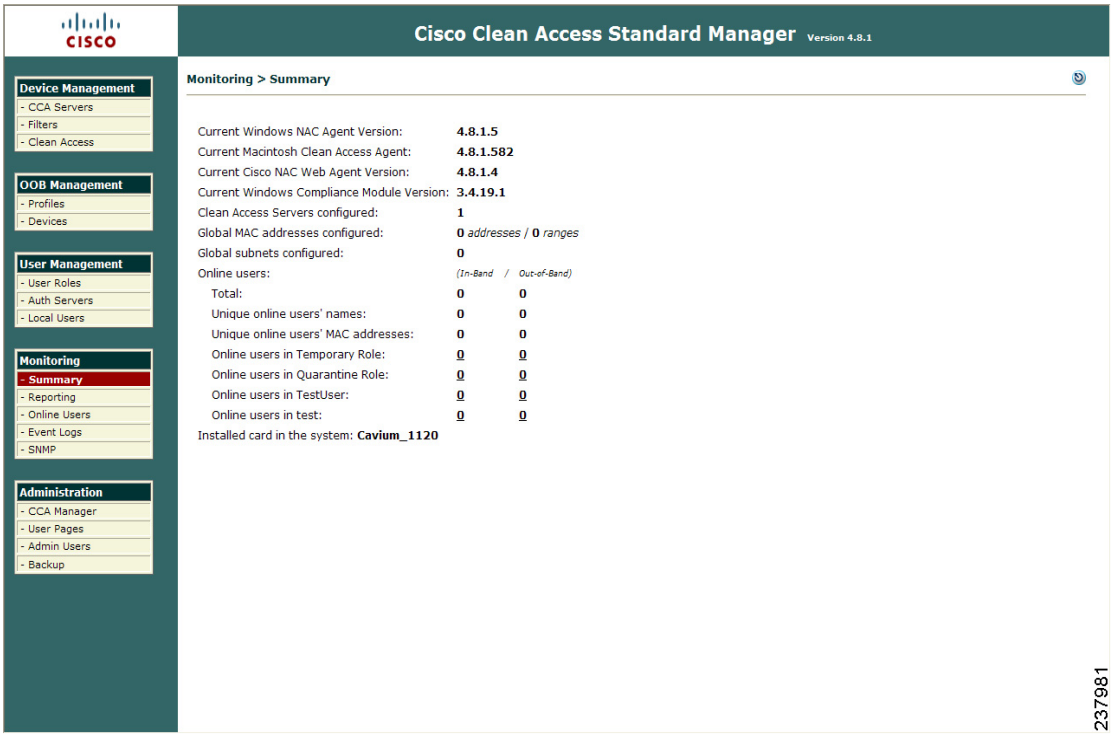
Figure 3-3 CAM Administrator Web Console Login Page



Step 8 The **Monitoring** > **Summary** page and left-hand navigation pane appears (Figure 3-4).

Step 9 Type the username **admin** and web console admin password you specified during installation and initial configuration, and click **Login**.

Figure 3-4 Monitoring Summary Page (FIPS 140-2 Compliant CAM)

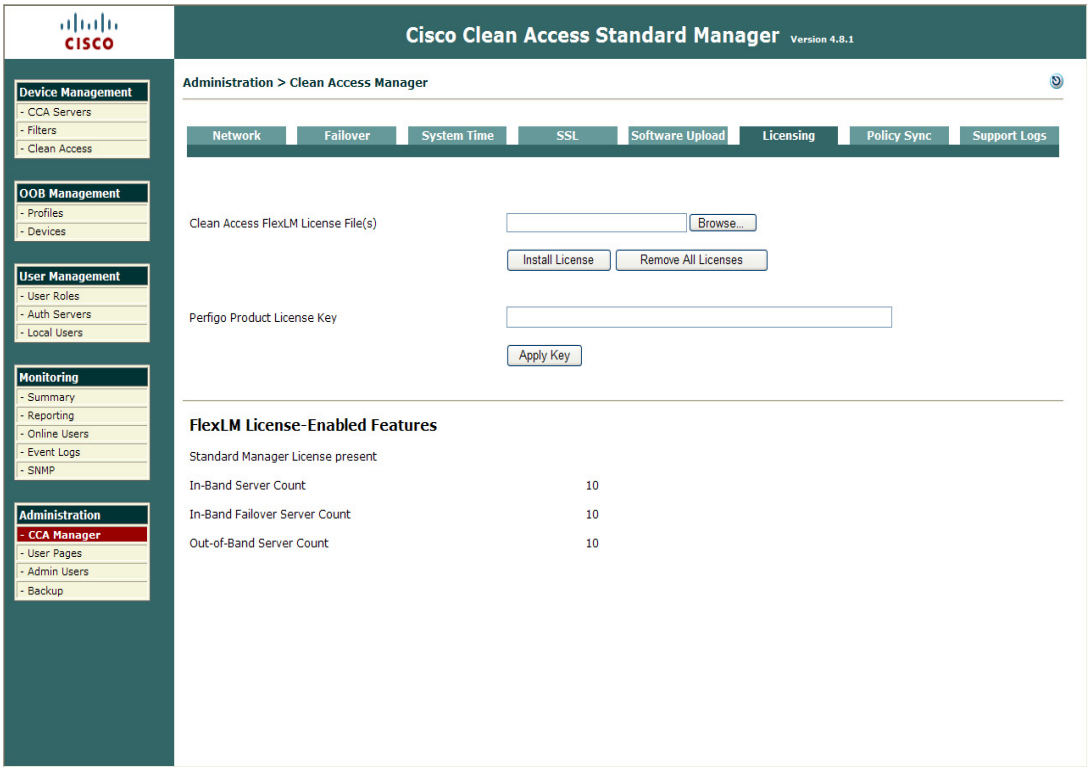


Add Additional Licenses

Step 10 To add additional licenses for your Clean Access Servers, go to **Administration > CCA Manager > Licensing** (Figure 3-5) in the CAM administrator web console.

Note A Manager Failover license must be present for HA-CAS machines. When a Manager Failover license is installed, the Server count increment can represent either 1 standalone CAS or 1 CAS HA-pair.

Figure 3-5 Licensing Page



Step 11 In the **Clean Access FlexLM License File(s)** field, **Browse** to the license file for your CAS or CAS bundle, and click **Install License**. You should see a green confirmation text string at the top of the page which indicates: success/failure to install the license, type of license added, and, for a CAS license, the Server increment count (for example, “License added successfully. CCA Manager License added. Out-of-Band Server Count is now 20."). The status text at the bottom of the page will indicate the presence of a Lite, Standard or Super Manager license and whether it is Failover, as well as the IB or OOB CAS license count.

Step 12 Repeat Step 11 for each license file you need to install (you should have received one license file per PAK submitted during customer registration). The Server Count information at the bottom of the page will display the total number of CASs enabled per successful license file installation.

Note Clicking the **Remove All Licenses** button removes all FlexLM license files from the system. You cannot remove individual license files. (Authenticated user traffic will continue to pass through if you remove all licenses and install them again.)

You must enter the CAM license to be able to access the administrator web console. Refer to *Cisco NAC Appliance Service Contract/Licensing Support* for details.

Step 13 Licenses are now installed. You can continue the configuration of your deployment using the CAM web console. Refer to the following documents for further configuration guidelines:

- *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*
- *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*

Step 14 To log out of the web console, either click the administrator session **Logout** button, at the top right-hand corner of the console, or simply close the browser.

Important Notes for SSL Certificates

1. You must generate the temporary SSL certificate during CAM installation or you will not be able to access your CAM as an end user.
2. After CAM and CAS installation, make sure to synchronize the time on the CAM and CAS via the web console interface before regenerating a temporary certificate on which a Certificate Signing Request (CSR) will be based.
3. In order to establish the initial secure communication channel between a CAM and CAS, you must import the root certificate from each appliance into the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.
4. Before deploying the CAM in a production environment, Cisco strongly recommends acquiring a trusted certificate from a third-party Certificate Authority to replace the temporary certificate (in order to avoid the security warning that is displayed to the web user during admin login).

For further details on the CAM, see the "Set System Time" and "Manage CAM SSL Certificates" sections of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*. For details on the CAS, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.

Note If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.8(1). You must correct your certificate chain to successfully upgrade to release 4.8(1). For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.8(1), refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.

Installing the Clean Access Server

Note The installation example and references in this chapter focus on Cisco NAC Appliance CAMs/CASs. For Cisco NAC network module installation information, refer to *Getting Started with Cisco NAC Network Modules in Cisco Access Routers* and *Installing Cisco Network Modules in Cisco Access Routers*.

Note If you are configuring the Cisco NAC Appliance Profiler Collector on the Clean Access Server, refer to the *Cisco NAC Profiler Configuration Guide* for additional details.

This section describes how to install and initially configure the Clean Access Server (CAS). Topics include:

Overview

When you receive a new Cisco NAC Appliance, you will need to connect to the appliance and perform initial configuration. If you want to install a different version of the software than what is shipped on the appliance, you can perform software installation via CD first. Refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for details on the software versions supported on Cisco NAC Appliance CAM/CAS platforms.

This chapter contains information for performing CD software installation and initial configuration of a Clean Access Server. With Cisco NAC Appliance software installation via CD, you must select whether to install the Clean Access Manager or Clean Access Server application. Once the CAM or CAS is installed on the appliance (application, OS, and relevant components), the installation of any other packages or applications on the CAM or CAS is not supported.

Note Static IP addresses must be configured for the CAM/CAS interfaces. DHCP mode is not supported for configuration of these interfaces.

Switch/Router Configuration

The Clean Access Server does not advertise routes. Instead, static routes must be added to the next hop router indicating that traffic to the managed subnets must be relayed to the Clean Access Server's trusted interface.

When the Clean Access Server is in Real-IP Gateway mode, it can act as a DHCP Server or DHCP Relay. With DHCP functionality enabled, the CAS provides the appropriate gateway information (that is, the CAS's untrusted interface IP address) to the clients. If the CAS is working as a DHCP Relay, then the DHCP server in your network must be configured to provide the managed clients with the appropriate gateway information (that is, the Clean Access Server's untrusted interface IP address).

Virtual Gateway Mode Connection Requirements

For all deployments, if planning to configure the Clean Access Server in Virtual Gateway mode (IB or OOB), do not connect the untrusted interface (eth1) of the standalone CAS or HA-Primary CAS until after you have added the CAS to the CAM from the web admin console. For Virtual Gateway HA-CAS pairs, also do not connect the eth1 interface of the HA-Secondary CAS until after HA configuration is fully complete. Keeping the eth1 interface connected while performing initial installation and configuration of the CAS for Virtual Gateway mode can result in network connectivity issues.

When setting up a CAS in Virtual Gateway mode, you specify the same IP address for the trusted (eth0) and untrusted (eth1) network interfaces during the initial installation of the CAS via CLI. At this point in the installation, the CAS does not recognize that it is a Virtual Gateway. It will attempt to connect to the network using both interfaces, causing collisions and possible port disabling by the switch. Disconnecting the untrusted interface until after adding the CAS to the CAM in Virtual Gateway mode prevents these connectivity issues. Once the CAS has been added to the CAM in Virtual Gateway mode, you can reconnect the untrusted interface.

Administrators must use the following procedure for correct configuration of a Virtual Gateway Central Deployment. To prevent looping on any central/core switch as you plug both interfaces of the Clean Access Server into the switch, perform the following steps:

Step 1 Before you connect both interfaces of the CAS to the switch, physically disconnect the eth1 interface.

Step 2 Physically connect the eth0 interface of the CAS to the network.

Step 3 Add the CAS to the CAM in the CAM web console under **Device Management > CCA Servers > New Server**, as described in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Step 4 Manage the CAS by accessing the CAS management pages, via **Device Management > CCA Servers > Manage [CAS_IP]** as described in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.

Step 5 Configure VLAN mapping. This is a **mandatory** step for a Central Deployment where both interfaces of the CAS connect to the same switch. (Note that you can configure VLAN mapping in Edge Deployments with no adverse affect, but you are not required to do so.)

a. Make sure you check the "**Enable VLAN Mapping**" checkbox and click **Update**.

b. Make sure to set the Untrusted VLAN-to-Trusted VLAN mapping under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See the "VLAN Mapping in Virtual Gateway Modes" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Note **Enable VLAN Pruning** is checked by default on the Virtual Gateway CAS (starting from release 4.1(1) and later) under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**.

Step 6 Once the preceding steps are completed, physically connect the eth1 interface of the CAS to the switch.

Note If the CAM is down and the CAS is performing VLAN mapping in "fail open" state, do not reboot the CAS because the VLAN mapping capability will be lost until the CAM comes back online.

Step 7 For the 802.1q ports configuration on the switch, make sure to prune all other VLANs for switches trunking to eth0 and eth1 of the CAS except those used for the CAS Management VLAN and the User VLANs.

Step 8 Prune VLAN 1 on the switch ports connecting to the CAS eth0 and eth1 interfaces. For details, see: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12122ea7/scg/swvlan.htm#wp1150302.

Switch Support for CAS Virtual Gateway/VLAN Mapping (IB and OOB)

For details on Cisco Catalyst switch model/NME support for the Virtual Gateway VLAN Mapping feature of the Clean Access Server for either in-band (IB) or out-of-band (OOB) deployments, refer to *Switch Support for Cisco NAC Appliance*.

Determining VLANs For Virtual Gateway

Before you start the initial installation for a Clean Access Server Virtual Gateway deployment, ensure that following is in place for your deployment:

- The CAS and CAM must be on different subnets (and VLANs).
- The CAS management VLAN must be on a different VLAN than the user authentication and access VLANs.
- Configure the native VLAN to be different than the CAS management VLAN. Setting native VLANs helps prevent inadvertent switching loops. The native VLAN must **not** be the same on the eth0 and eth1 interfaces of the CAS.
  - CAS native VLAN (eth0) (e.g. unused "dummy" VLAN 999)
  - CAS native VLAN (eth1) (e.g. unused "dummy" VLAN 998)
- Configure different user authentication and access VLANs on the switches, and configure untrusted subnets on the CAS as Managed Subnets (refer to Configuring Managed Subnets).
- Ensure there are no common VLANs being forwarded on the switch ports connecting the trusted (eth0) and untrusted (eth1) ports of the CAS. For every VLAN that is allowed on the trunk links going to the Virtual Gateway CAS, there must be a corresponding VLAN Mapping entry (except for the CAS management VLAN).
- Make sure the eth1 untrusted interface of the CAS is not connected to the network until after VLAN Mapping is configured.
- Switch(es) must not have SVI (Layer 3) interfaces for the user authentication VLANs anywhere on the network.
- User authentication VLANs should be on the CAS untrusted interface only and must be pruned from all other trunk links.

See the "Understanding VLAN Settings" and "VLAN Mapping in Virtual Gateway Modes" sections in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for additional details.

Summary of Steps For New Installation

Note Refer to the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for additional deployment information for new installations.

Step 1 Follow the instructions on your welcome letter to obtain a valid license file for your installation. Refer to the instructions in *Cisco NAC Appliance Service Contract/Licensing Support* for details. (If you are evaluating Cisco NAC Appliance, visit http://www.cisco.com/go/license/public to obtain an evaluation license.)

Note CAS licenses are generated based on the eth0 address of the CAM. Both CAM and CAS licenses are installed via the CAM web admin console.

Step 2 Obtain a bootable CD of the latest version of the software. You can log in to Cisco Secure Software and download the latest 4.8(1) .ISO image.

Step 3 Connect the CAS to the network and connect a monitor and keyboard to the CAS, or connect your workstation to the CAS via serial cable, as described in Connect the Clean Access Server, page 3-22.

Step 4 Install the software as described in Install the Clean Access Server (CAS) Software from CD-ROM, page 3-22.

Note If your NAC-3310 appliance does not read the software on the CD ROM drive and instead attempts to boot from the hard disk, before proceeding you will need to change the appliance settings to boot from CD ROM as described in Configuring Boot Settings on the Cisco NAC Appliance CAM/CAS, page 3-40.

Step 5 Perform the initial configuration of the CAS, as described in Perform the Initial CAS Configuration, page 3-24.

Note For High Availability mode, install and initially configure each CAS first before configuring HA. Refer to Installing a Clean Access Server High Availability Pair, page 4-17 for details.

You must use identical appliances (e.g. NAC-3350 and NAC-3350) in order to configure High Availability (HA) pairs of Clean Access Managers (CAMs) or Clean Access Servers (CASs).

Step 6 Make sure your Clean Access Manager is installed and initially configured as described in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1).* Valid FlexLM license file(s) for your Clean Access Server (s) must be installed via the Clean Access Manager web console to complete configuration of the CAS.

Step 7 Add your Clean Access Server(s) to the Clean Access Manager, as described in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*. From this point, you can configure your Clean Access Servers via the CAM web console, or via the CAS direct access web console for certain specific settings.

Connect the Clean Access Server

To install the Clean Access Server software from CD-ROM or to perform its initial configuration, you will need to connect the target machine and access the CAS command line interface.

Step 1 The Clean Access Server requires two 10/100/1000BASE-TX interface connectors on the back panel of the CAS for its eth0 (trusted) and eth1 (untrusted) network interface. Connect the NIC1 (eth0) network interface on the target machine to your local area network (LAN) using a CAT5 Ethernet cable.

Warning **Do not physically connect the eth1 (NIC2) untrusted network interface on a Virtual Gateway CAS until the proper configuration has been performed. Refer to Install the Clean Access Server (CAS) Software from CD-ROM, page 3-22 for details.**

Step 2 Connect the power by plugging one end of the AC power cord into the back of the machine and the other end into an electrical outlet.

Step 3 Connect the external FIPS Smart card reader module to a FIPS 140-2 compliant NAC-3315, NAC-3355, or NAC-3395 by plugging the Smart card reader mini-DIN cable into the female mini-DIN FIPS card port on the back of the appliance (see Figure 1-4 on page 1-6, Figure 1-9 on page 1-10, and Figure 1-14 on page 1-14). (Ensure you also have a Smart card inserted into the reader.)

Step 4 Power on the machine by pressing the power button on the front of the appliance. The diagnostic LEDs will flash a few times as part of an LED diagnostic test. Status messages are displayed on the console as the CAS boots up.

Step 5 Access the command line or the CAS by either:

a. Connecting a monitor and keyboard directly to the CAS via the keyboard connector and video monitor/console connector on the back panel.

b. Or, connecting a serial cable from an external workstation (PC/laptop) to the CAS and open a serial connection using terminal emulation software (such as HyperTerminal or SecureCRT) on the external workstation, as described in Serial Connection to the CAM and CAS, page 3-39.

Note Cisco NAC Appliances assume the keyboard connected to be of US layout for both direct and IP-KVM connections. Use a US layout keyboard or ensure that you know the key mapping if you are connecting a keyboard of different layout.

Note Static IP addresses must be configured for the CAM/CAS interfaces. DHCP mode is not supported for configuration of these interfaces.

Install the Clean Access Server (CAS) Software from CD-ROM

The following steps describe how to perform optional CD installation of the Clean Access Server software on NAC-3310/3315 SERVER or NAC-3350/3355 SERVER appliances.

Step 1 Connect the target installation machine to the network and access the command line of the machine by direct console or over a serial connection, as described in Serial Connection to the CAM and CAS, page 3-39.

Step 2 Download the latest software version supported on the target machine as follows:

a. Log in to the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. You will likely be required to provide your CCO credentials.

b. Navigate to **Security > Endpoint Security > Cisco Network Access Control > Cisco NAC Appliance > Cisco NAC Appliance 4.8**.

c. Download the latest 4.8(1) .ISO image (e.g. **nac-4.8.1-K9.iso**) and burn the image as a bootable disk to a CD-R.

Note Cisco recommends burning the .ISO image to a CD-R using speeds 10x or lower. Higher speeds can result in corrupted/unbootable installation CDs.

Step 3 Insert the CD-ROM containing the Clean Access Server .ISO file into the CD-ROM drive of the target CAS machine.

Step 4 Reboot the machine. The Cisco Clean Access Installer welcome screen appears after the machine restarts:

```
Cisco Clean Access 4.8.1 Installer (C) 2010 Cisco Systems, Inc.

                Welcome to the Cisco Clean Access Installer!

 -  To install a Cisco Clean Access device, press the <ENTER> key.

 -  To install a Cisco Clean Access device over a serial console, enter serial a
t the boot prompt and press the <ENTER> key.

boot:
```

Step 5 At the "`boot`:" prompt, type one of the following options depending on the type of connection:

- Press the Enter key if your monitor and keyboard are directly connected to the CAS.
- Type **`serial`** and press enter in the terminal emulation console if you are accessing the appliance over a serial connection.

Step 6 If the install CD detects an existing installation of Cisco NAC Appliance, you are presented with the following prompt:

```
Checking for existing installations.
Clean Access Server 4.8.0 installation detected.
Please choose one of the following actions:
1) Install.
2) Exit.
```

Step 7 Choose `1` to perform a fresh installation of the Cisco NAC Appliance software.

Step 8 Next, the Cisco NAC Appliance software installer asks you to specify whether you are installing a Clean Access Manager or Clean Access Server. At the following prompt, enter `2` to perform the installation for a Clean Access Server.

```
Please choose one of the following configurations:
1) CCA Manager.
2) CCA Server.
3) Exit.
```

Caution Only one CD is used for installation of the Clean Access Manager or Clean Access Server software. You must select the appropriate type, **either** CAM or CAS, for the target machine on which you are performing installation.

Step 9 The Clean Access Server Package Installation then executes. The installation takes several minutes. When finished, the installation script presents the following message, prompting you to press Enter to reboot the CAS and launch the Clean Access Server quick configuration utility.

```
Installation complete. Press <ENTER> to continue
```

When finished, the welcome screen for the Clean Access Server quick configuration utility appears, and a series of questions prompt you for the initial CAS configuration, as described in Configuration Utility Script, page 3-6.

Perform the Initial CAS Configuration

When installing the Clean Access Server from CD-ROM, the Configuration Utility Script automatically appears after software package installation to prompt you for the initial CAS configuration.

Note If necessary, you can always manually start the Configuration Utility Script as follows:

1. Over a serial connection or working directly on the CAS, log onto the CAS as user **`root`** with the root user password.
2. Run the initial configuration script by entering the following command:

   `service perfigo config`

You can run the **`service perfigo config`** command to modify the configuration of the CAS if it cannot be reached through the web admin console. For further details on CLI commands, see CAS CLI Commands, page 3-43.

Configuration Utility Script

Step 1 The configuration utility script suggests default values for particular parameters. To configure the installation, either accept the default value or provide a new one, as described below.

Step 2 After the software is installed from the CD and package installation is complete, the welcome script for the configuration utility appears:

```
Welcome to the Cisco Clean Access Server quick configuration utility.

Note that you need to be root to execute this utility.

The utility will now ask you a series of configuration questions.
Please answer them carefully.

Cisco Clean Access Server, (C) 2010 Cisco Systems, Inc.
```

Note If this prompt does not appear after you install the Cisco NAC Appliance software and restart the CAS, refer to Manually Restarting the CAM/CAS Configuration Utility, page 3-46.

Step 3 If your CAS is a FIPS-compliant platform (NAC-3315 or NAC-3355) the first prompt asks if you want to initialize the on-board FIPS card (used to ensure FIPS compliant functions on the appliance). Otherwise, skip to Step 7.

```
Do you want to initialize the fips cards? (y/n)? [y]
```

Step 4 Choose **y** to enable FIPS on your appliance. The appliance automatically initializes the FIPS card and attempts to establish the security world.

```
-- Running startup script 45drivers

 -- Running startup script 46exard

 -- Running startup script 50hardserver

Security world not found
Creating the security world and initializing the smart cards
```

Next, the FIPS setup process prompts you to specify how many Smart Cards (from 1-6) you want to initialize to enable FIPS compliance on the CAS.

```
How many cards do you want to initialize (1-6)? [1]
Set ncipher card switch in i mode and press Return to continue
```

Step 5 Enter the number of Smart Cards you want to initialize, ensure that the FIPS card operation switch on the back of the CAS is switched to “I” (for “initialize”), and press Return.

```
Module 1, command ClearUnit: OK

Create Security World:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: unknown card
 Module 1 slot 0: - no passphrase specified - overwriting card
Module #1 Slot #0: Processing ...

Card writing complete.

security world generated on module #1; hknso = 65cc642b8d38a1f99b58c8afa560f4d94
522d2ad
Set ncipher card switch in o mode and press Return to continue
```

Step 6 Switch the FIPS card switch back to “O” (for “operational”) and press Return.

```
Module 1, command ClearUnit: OK

Card(s) check passed

Do you want to continue with the rest of the NAC Server Configuration?  (y/n)? [y]
```

Step 7 When prompted, enter an IP address for the eth0 (trusted) interface of the CAS. Confirm the value when prompted, or type **n** and press Enter to correct the entry.

```
Configuring the network interfaces:

Please enter the IP address for the interface eth0 []: 10.201.1.20
You entered 10.201.1.20 Is this correct? (y/n)? [y]
```

At the prompt, type the eth0 IP address of the CAS and press Enter. Note that the eth0 IP address of the CAS is the same as the Management IP address. At the confirmation prompt, type **y** to accept the entry or type **n** to change it and enter another address for the trusted eth0 network interface. When prompted, press Enter to confirm the value.

Note The eth0 IP address of the CAS is the same as the Management IP address.

Step 8 Type the subnet mask of the eth0 interface or press Enter to accept the default of 255.255.255.0. Confirm the value at when prompted.

```
Please enter the netmask for the interface eth0 []: 255.255.255.0
You entered 255.255.255.0, is this correct? (y/n)? [y]
```

Step 9 Accept the default gateway address or enter a default gateway for the eth0 address of the CAS. Confirm the default gateway at the prompt.

```
Please enter the IP address for the default gateway []: 10.201.240.1
You entered 10.201.240.1 Is this correct? (y/n)? [y]
```

Step 10 At the Vlan Id Passthrough prompt, type **n** and press Enter (or just press Enter) to keep VLAN ID passthrough disabled as the default behavior of the CAS. By default, VLAN IDs are stripped from traffic passing through the interface to the CAS. Typing **y** enables VLAN IDs to be passed through the CAS for traffic from the trusted to the untrusted network.

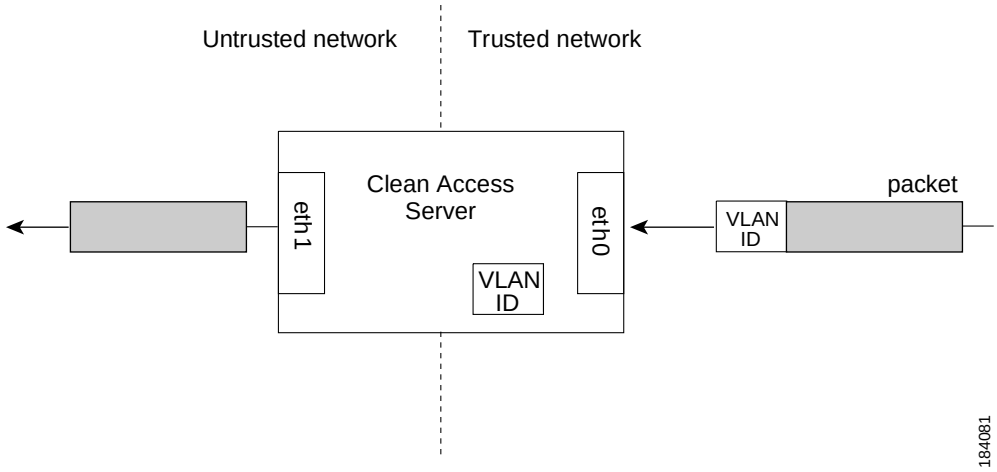
```
[Vlan Id Passthrough] for packets from eth0 to eth1 is disabled.
Would you like to enable it? (y/n)? [n]
```

Note

- In most cases, enabling VLAN ID passthrough is not needed. Only enable VLAN ID passthrough if you are sure you need it. If you choose not to enable it at this time, you can always change this option later from the CAS **Network > IP** page of the web console or using the **service perfigo config** utility. Note that either method requires a reboot of the CAS.
- Faulty VLAN settings can render the Clean Access Server unreachable from the Clean Access Manager, so use caution when configuring VLAN settings.

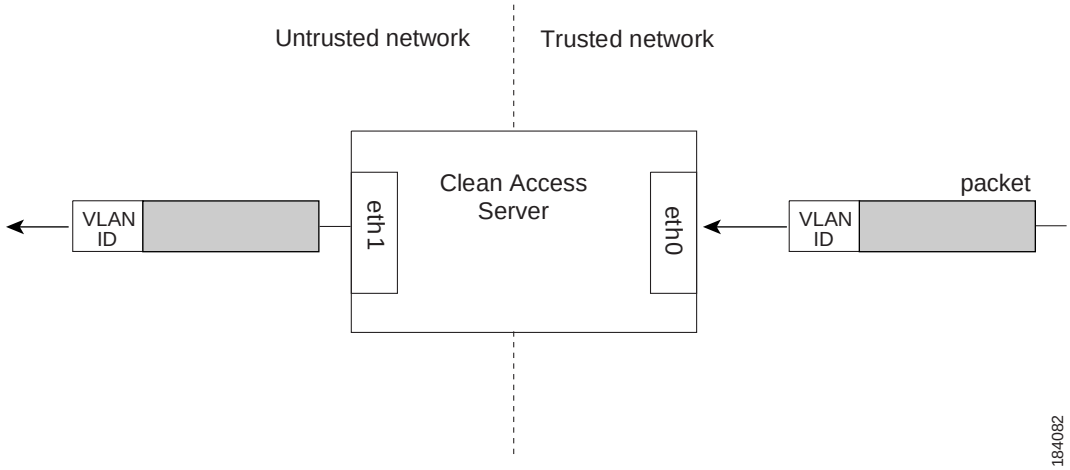
By default, the VLAN ID is not passed through, that is, the VLAN ID is stripped from packets passed through the CAS, as illustrated in Figure 3-6. The IDs are retained by the Clean Access Server and attached to response messages passed from the untrusted network back to the trusted network.

Figure 3-6 VLAN ID Termination



In VLAN ID passthrough, the identifier is retained on traffic that passes through the interface.

Figure 3-7 VLAN ID Passthrough



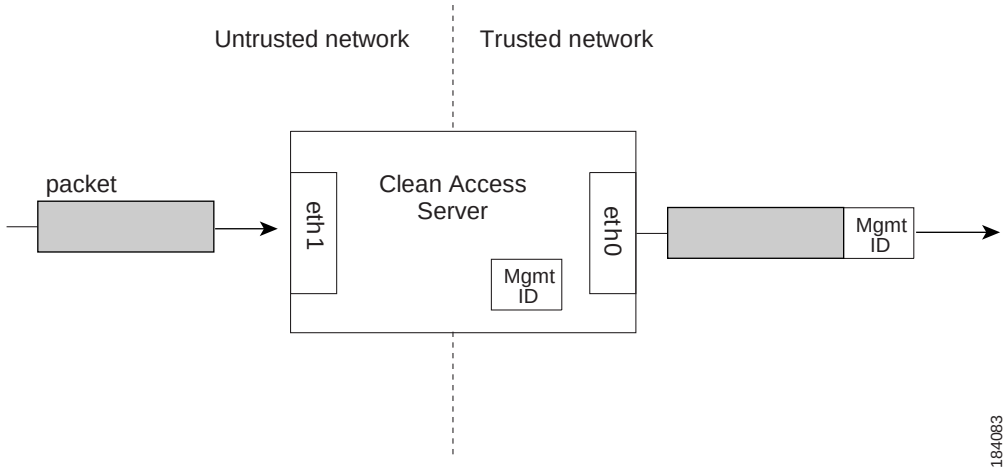
Step 11 At the Management VLAN Tagging prompt, type `n` and press Enter (or just press Enter) to keep Management VLAN tagging disabled (default). Or, type `y` and press Enter to enable Management VLAN tagging with the specified VLAN ID for the eth0 interface. (You can change the Management VLAN ID later from the CAS **Network > IP** web console page; however, changing settings on the CAS **IP** page requires a reboot of the CAS.)

```
[Management Vlan Tagging] for egress packets of eth0 is disabled.
Would you like to enable it? (y/n)? [n]
```

Note CAS eth0 interface settings are required for basic connection to the CAM. CAS eth1 interface settings can be reconfigured later from the CAM web console.

A Management VLAN identifier is a default VLAN identifier that is added to a packet if it does not have its own VLAN identifier or if the identifier was originally stripped by the adjacent interface. The setting at the prompt applies to traffic passing from the untrusted network to the trusted network.

Figure 3-8 Eth0 Egress Packets with Management VLAN ID Tagging



Note

- In most cases, enabling Management VLAN tagging is not needed. You should only enable it if you are sure it is necessary. If you choose not to enable it at this time, you can change the option later in the web console or using **`service perfigo config`** utility. (Management VLAN tagging is necessary when the trusted side of the CAS is a trunk, such as in Virtual Gateway deployments. In this case, you will need to enable Management VLAN tagging and specify the VLAN ID to which the trusted interface of the CAS belongs.)
- Also note that faulty VLAN settings can render the Clean Access Server unreachable from the Clean Access Manager, so be sure to use care when configuring VLAN settings.

Step 12 Next configure the untrusted interface. This is the interface to the untrusted (managed) network. At the prompt type the address you want to use for the untrusted interface (eth1) and press Enter. Unless deploying the Clean Access Server in a bridge (Virtual Gateway) configuration, the trusted and untrusted interfaces must be on separate subnets. Confirm the value when prompted.

```
Please enter the IP address for the untrusted interface eth1 []: 10.10.10.10
You entered 10.10.10.10 Is this correct? (y/n)? [y]
```

Note For Virtual Gateways, the eth1 address most commonly used is the eth0 address. To prevent looping, do not connect eth1 to the network until after you have added the CAS to the CAM in the web console. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* for further details.

Step 13 Type the subnet mask of the eth1 interface or press Enter to accept the default of 255.255.255.0. Confirm the value at when prompted.

```
Please enter the netmask for the interface eth1 []: 255.255.255.0
You entered 255.255.255.0, is this correct? (y/n)? [y]
```

Step 14 Enter the default gateway address for the untrusted interface:

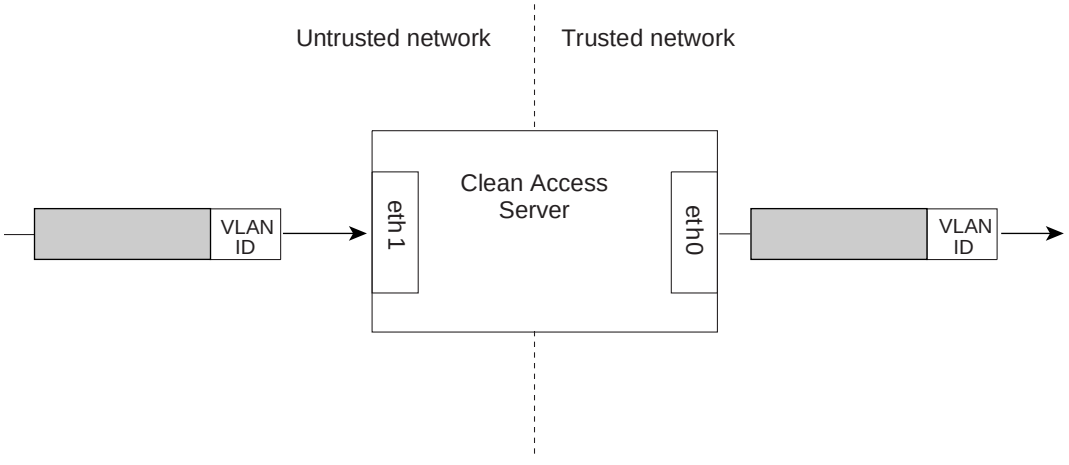
- If the Clean Access Server will act as a Real-IP gateway, this should be the IP address of the CAS's untrusted interface eth1.
- If the Clean Access Server will act as a Virtual gateway (i.e. a bridge), this can be the same default gateway address used for the trusted side.

```
Please enter the IP address for the default gateway []: 10.10.10.1
You entered 10.10.10.1 Is this correct? (y/n)? [y]
```

Step 15 Specify VLAN passthrough behavior for traffic passing from the untrusted to the trusted network. At the prompt, type **n** and press Enter (or just press Enter) to accept the default behavior (disabled) or enter **y** to enable VLAN ID passthrough for traffic from the untrusted network.

```
[Vlan Id Passthrough] for packets from eth1 to eth0 is disabled.
Would you like to enable it? (y/n)? [n]
```

Figure 3-9 VLAN ID Passthrough

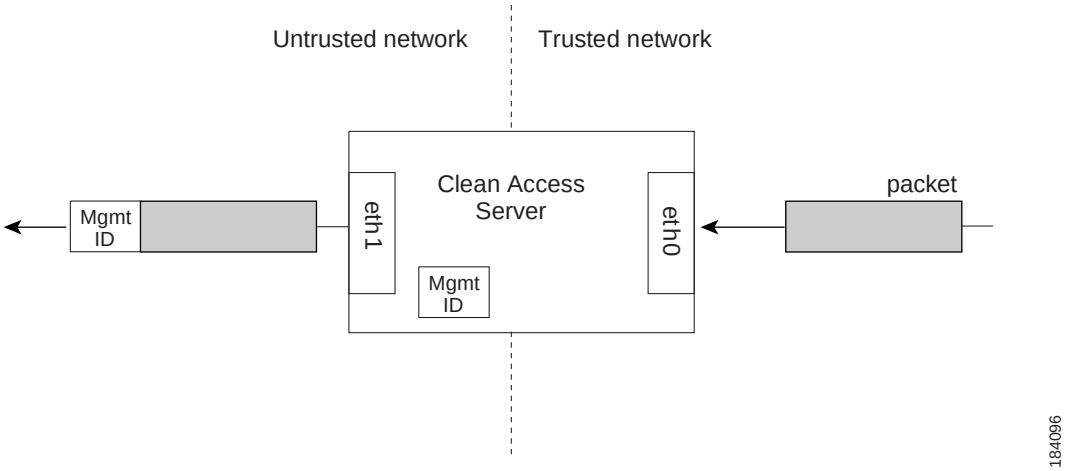


Step 16 Specify Management VLAN Tagging for the untrusted interface at the next prompt. Type **N** and press Enter (or just press Enter) to keep Management VLAN tagging disabled (default). Or, type **Y** and press Enter to enable Management VLAN tagging and specify the Management VLAN ID to use for the CAS untrusted interface.

```
[Management Vlan Tagging] for egress packets of eth1 is disabled.
Would you like to enable it? (y/n)? [n]
```

Note You can change the Management VLAN ID later from the CAS **Network > IP** web console page; however, changing settings on the CAS **IP** page requires a reboot of the CAS.

Figure 3-10 Eth1 Egress Packets with Management VLAN ID Tagging



Step 17 Specify the host name for the Clean Access Server (**nacserver** is the default). Type and confirm the address when prompted:

```
Please enter the hostname [nacserver]: cas1
You entered cas1 Is this correct? (y/n)? [y]
```

Step 18 Specify the IP address of the Domain Name System (DNS) server in your environment. Type and confirm the address when prompted:

```
Please enter the IP address for the name server: []: 172.10.16.16
You entered 172.10.16.16 Is this correct? (y/n)? [y]
```

Step 19 The Clean Access Managers and Clean Access Servers use a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to restore database snapshots on the CAM when you need them and are able to fail over to the HA peer CAM/CAS in HA deployments. (You cannot upload a CAM database snapshot that was created when the system was configured with a different master secret password, and HA-Secondary CAMs/CASs are not able to assume the "active" role following a failover event when the master secret passwords are different.) Type and confirm the master secret at the prompts.

```
The master secret is used to encrypt sensitive data.
Remember to configure all HA pairs with the same secret.
Please enter the master secret:
Please confirm the master secret:
```

Caution If your master secret is lost or becomes corrupted, use the procedure in Recover From Corrupted Master Secret, page 3-48.

Step 20 Specify time settings for the Clean Access Server as follows:

a. Choose your region from the continents and oceans list. Type the number next to your location on the list, such as `2` for the Americas, and press Enter. Type `11` to enter the time zone in Posix TZ format, such as `GST-10`.

b. The next list that appears shows the countries for the region you chose. Choose your country from the country list, such as **47** for the United States, and press Enter.

c. If the country contains more than one time zone, the time zones for the country appears.

d. Choose the appropriate time zone region from the list, such as `21` for Pacific Time, and press Enter.

e. Confirm your choices by entering `1`, or use `2` to cancel and start over.

```
The following information has been given:
        United States
        Pacific Time
Is the above information OK?
1) Yes
2) No
#? 1
```

Step 21 Type and confirm the current date and time, using format hh:mm:ss mm/dd/yy.

```
Updating timezone information...

Current date and time hh:mm:ss mm/dd/yy [07:52:52 04/30/07]: 15:52:00 04/30/07
You entered 15:52:00 04/30/07 Is this correct? (y/n)? [y]
Mon Apr 30 15:52:00 PDT 2007
```

Note The time set on the CAS must fall within the creation date/expiry date range set on the CAM's SSL certificate. The time set on the user machine must fall within the creation date /expiry date range set on the CAS's SSL certificate.

Step 22 Press Enter to configure the temporary SSL certificate. The certificate secures the login exchange between the Clean Access Server and untrusted (managed) clients. Configure the certificate as follows:

a. Type the IP address or domain name for which you want the certificate to be issued.

Note This is also the IP address or domain name to which the web server responds. If DNS is not already set up for a domain name, the CAS web console will not load. Make sure to create a DNS entry in your servers, or else use an IP address for the CAS.

b. For the organization unit name, enter the group **within** your organization that is responsible for the certificate (for example, `doc`).

c. For the organization name, type the name of your organization or company for which you would like to receive the certificate (for example, `Cisco Systems`), and press Enter.

d. Type the name of the city or county in which your organization is legally located (for example, `San Jose`), and press Enter.

e. Type the two-character state code in which the organization is located (for example, `CA` or `NY`), and press Enter.

f. Type the two-letter country code (for example, `US`), and press Enter.

Step 23 Confirm values and press Enter to generate the SSL certificate, or type `n` to restart:

```
You entered the following:
Domain: 10.201.240.10
Organization unit: doc
Organization name: Cisco Systems
City name: San Jose
State code: CA
Country code: US
Is this correct? (y/n)? [y] y
```

Note You must generate the temporary SSL certificate or you will not be able to access your CAS as an end user.

Step 24 Specify whether or not you want the CAS to feature Pre-login Banner Support at the following prompt.

```
Enable Prelogin Banner Support? (y/n)? [n]
```

For more information and an example of the Pre-login Banner feature, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.

Step 25 Configure the **root** user password for the installed Linux operating system of the Clean Access Server. The **root** user account is used to access the system over a serial connection or through SSH.

Cisco NAC Appliance supports using Strong Passwords for root user login. Passwords must be at least 8 characters long and feature a combination of upper- and lower-case letters, digits, and other characters. For example, the password **10-9=One** does not satisfy the requirements because it does not contain two characters from each category, but **1o-9=OnE** is a valid password. For more details, see the "Administering the CAM" chapter of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

```
For security reasons, it is highly recommended that you change the password for the root
user.

** Please enter a valid password for root user as per the requirements below! **

Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters,
digits, and other characters. Minimum of 8 characters and maximum
of 16 characters with characters from all of these classes. Minimum
of 2 characters from each of the four character classes is mandatory.
An upper case letter that begins the password and a digit that ends
it do not count towards the number of character classes used.

Enter new password:
Re-type new password:
passwd: all authentication tokens updated successfully.
```

Step 26 Next type the password for the **admin** user for the CAS direct access web console.

```
Please enter an appropriately secure password for the web console admin user.

New password for web console admin:
Confirm new password for web console admin:
Web console admin password changed successfully.
```

Step 27 The final step in the initial configuration process is to choose whether or not to turn on FIPS mode for your NAC-3315 or NAC-3355 CAS. To enable FIPS operation, enter **y** at the following prompt.

```
Would you like to turn on fips mode? (y/n)? [y]

 -- Running startup script 45drivers

 -- Running startup script 46exard

 -- Running startup script 50hardserver

Security world already exists
```

Step 28 If you want to initialize any additional Smart cards at this time, enter **y** at the following prompt. Otherwise, enter **n** to complete the FIPS set up process.

```
Do you want to recreate security world and initialize cards (y/n)? [n]
writing RSA key
Card(s) check passed
```

Step 29 After the configuration is complete, press Enter to reboot the CAS.

```
Configuration is complete.
Changes require a REBOOT of Clean Access Server.
```

Step 30 Enter the following command to reboot the CAS after configuration is complete:

```
# reboot
```

The CAS initial configuration is now complete. Once the Clean Access Manager is also installed and initially configured, use the CAM web administration console to add the CAS to the CAM as described in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Step 31 Following CAS installation and initial configuration:

a. Ping the eth0 interface address from a command line. If working properly, the interface should respond to the ping.

b. For a FIPS-compliant CAS, verify FIPS functionality as follows:

- Ensure the FIPS card operation switch is set to "O" (for operational mode).
- Log into the CAS console interface as **root**.
- Navigate to the **/perfigo/common/bin/** directory.
- Enter **./test_fips.sh info** and verify the following output:

```
Installed FIPS card is nCipher
Info-FIPS file exists
Info-card is in operational mode
Info-httpd worker is in FIPS mode
Info-sshd up
```

c. If the CAS is not responding, try connecting to the CAS using SSH (Secure Shell). Connect with the **root** username and password. Once connected, try pinging the gateway and/or an external website from the CAS to see if the CAS can reach the external network.

If both tests fail, make sure that you have configured the IP address correctly and that the other network settings are correct.

If after installation you need to reset the initial configuration settings for the Clean Access Server, connect to the CAS machine directly or through SSH and use the **service perfigo config** command.

Important Notes for SSL Certificates

1. You must generate the temporary SSL certificate during CAS installation or you will not be able to access your CAS. Before deploying in a live environment, obtain a trusted certificate for the CAS from a Certificate Authority to replace the temporary certificate.
2. After CAM and CAS installation, make sure to synchronize the time on the CAM and CAS via the web console interface before regenerating a temporary certificate on which a Certificate Signing Request (CSR) will be based.
3. In order to establish the initial secure communication channel between a CAM and CAS, you must import the root certificate from each appliance into the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.

4. Before deploying the CAS in a production environment, Cisco Strongly recommends acquiring a trusted certificate from a third-party Certificate Authority to replace the temporary certificate (in order to avoid the security warning that is displayed to end users during user login).

For further details, see the "Manage CAS SSL Certificates" and "Synchronize System Time" sections of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*. For details on CAM certificates, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Cisco NAC Appliance Connectivity Across a Firewall

The Clean Access Manager (CAM) uses Java Remote Method Invocation (RMI) for parts of its communication with the Clean Access Server (CAS), which means it uses dynamically allocated ports for this purpose. If your deployment has a firewall between the CAS and the CAM, you will need to set up rules in the firewall to allow communication between the CAS and CAM machines, that is, a rule that allows traffic originating from the CAM destined to the CAS and vice versa.

Note If there is a NAT router between the CAS and CAM, also refer to section "Configuring the CAS Behind a NAT Firewall" in the Installation chapter of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* for additional details.

Table 3-1 lists the ports that are required for communication between the CAS and the CAM (per version of Cisco NAC Appliance).

Table 3-1 Port Connectivity for CAM/CAS

Cisco NAC Appliance Version	Required Ports
4.8 **4.7(x)** **4.6(1)** **4.5(x)** **4.1(x)** **4.0(x)**	TCP ports 443, 1099, and 8995~8996
3.6(x)	TCP ports 80, 443, 1099, and 8995~8996
3.5(x)	TCP ports 80, 443, 1099, and 32768~61000 (usually 32768~32999 are sufficient).

For example, for Single Sign-On (SSO) capabilities, additional ports must be opened on the CAS and firewall (if any) to allow communication between the Agent and the Active Directory Server, as shown in Table 3-2. Table 3-2 provides further details about communicating devices, the ports affected, and the purpose of each port.

Table 3-2 Port Usage

Device	Communicating Devices	Ports to Open	Purpose
Firewall, if any	CAM and CAS	TCP 8995, 8996 TCP 1099	Java Management Extensions (JMX) communication between the CAM and CAS, such as pre-connect and connect messages.
		TCP 443	HTTP over Secure Sockets Layer (SSL) communication between Agent/CAS/CAM, such as end user machine remediation via the Agent.
		TCP 80 (for version 3.6.x and earlier)	HTTP communication between Agent/CAS/CAM. Used to download the Agent from the CAM to an end user machine.
	CAS and Agent	UDP 8905, 8906	SWISS, a proprietary CAS-Agent communication protocol used by the Agent for UDP discovery of the CAS. UDP 8905 is used for Layer 2 discovery; and 8906 is used for Layer 3 discovery. For more information, see the "Connecting to the CAS Using the SWISS Protocol" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.
		TCP 443	HTTP over SSL communication between Agent/CAS/CAM, such as for user redirection to a web login page.
		TCP 80 (for version 3.6.x and earlier)	HTTP communication between Agent/CAS/CAM. Used to download the Agent from the CAM to an end user machine.

Table 3-2 Port Usage (continued)

Device	Communicating Devices	Ports to Open	Purpose
CAS and firewall (if any)	Agent (Windows OS) and Active Directory (AD) Server	TCP 88, 135, 389, 445, 1025, 1026 UDP 88, 389	AD SSO requires the following ports to be open: • TCP 88 (Kerberos) • TCP 135 (RPC) • TCP 389 (LDAP) or TCP 636 (LDAP with SSL) **Note** When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments. • TCP 445 (Microsoft-SMB; e.g. needed for password change notices from DC to PC) • TCP 1025 (RPC)–non-standard • TCP 1026 (RPC)–non-standard If it is not known whether the AD server is using Kerberos, you must open the following UDP ports instead: • UDP 88 (Kerberos) • UDP 389 (LDAP) or UDP 636 (LDAP with SSL) **Note** When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments. If your deployment requires LDAP services, use TCP/UDP 636 (LDAP with SSL encryption) instead of TCP/UDP 389 (plain text). For more information on AD SSO, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.

Configuring the CAS Behind a NAT Firewall

Caution If deploying a NAT firewall between the CAS and the CAM, the CAS must be in Standalone mode. Cisco NAC Appliance does not support High Availability CAS pairs when a NAT firewall is deployed on the trusted side of the CAS HA pair.

If deploying the Clean Access Server behind a firewall (there is a NAT router between CAS and CAM), you will need to perform the following steps to make the CAS accessible:

Step 1 Connect to the CAS by SSH or use a serial console. Log in as **root** user.

Step 2 Change directories to `/perfigo/access/bin/`.

Step 3 You will need to edit two files: `restartweb` and `starttomcat`.

Step 4 Locate the `CATALINA_OPTS` variable definition in each file.

Step 5 Add **`-Djava.rmi.server.hostname=<`***`caserver1_hostname`***`>`** to the variable, replacing *caserver1_hostname* with the host name of the server you are modifying. For example:

```
CATALINA_OPTS="-server -Xms64m -Xmx${MAX}m -Xincgc
-Djava.util.logging.config.file=${CATALINA_HOME}/conf/redirect-log.properties
-Dperfigo.jmx.context=${PERFIGO_SECRET}
-Djava.security.auth.login.config=${CATALINA_HOME}/conf/sso-login.conf
-Dsun.net.inetaddr.ttl=60 -Dsun.net.inetaddr.negative.ttl=10
-Djava.security.egd=file:/dev/urandom"
-Djava.rmi.server.hostname=caserver1”
```

Step 6 Restart the CAS by entering the **`service perfigo restart`** command.

Step 7 Repeat the preceding steps for each Clean Access Server in your deployment.

Step 8 Connect to the Clean Access Manager by SSH or using a serial console. Login as **`root`**.

Step 9 Change directories to `/etc/`.

Step 10 Edit the hosts file by appending the following line:

```
<public_IP_address>  <caserver1_hostname> <caserver2_hostname>
```

where:

- *<public_IP_address>* – The address that is accessible outside the firewall.
- *<caservern_hostname>* – The host name of each Clean Access Server behind the firewall.

The Clean Access Server(s) should now be addressable behind the firewall.

Connectivity Across a Wide Area Network

When deploying the CAM/CAS across a WAN, you must prioritize all CAM/CAS traffic and SNMP traffic, and include the eth0/eth1 IP addresses of the CAM and CAS in addition to the Service IP address for HA pairs.

Configuring Additional NIC Cards

The Configuration Utility script requires that the CAM and CAS machines come with eth0 (NIC1) and eth1 (NIC2) interfaces by default and prompts you to configure these during initial installation. If your system has additional network interface cards (e.g. NIC3, NIC4), you can use the following instructions to configure the additional interfaces (e.g. eth2, eth3) on those cards. Typically, eth2 needs to be configured when setting up CAS systems for High Availability (HA). For HA, once the eth2 (NIC3) interface is configured with the proper addressing, it can then be configured as the dedicated and/or redundant UDP heartbeat interface for the HA-CAM/CAS.

Note

- For Cisco NAC Appliance hardware, the following instructions assume that the NIC is plugged in and “working” (i.e. recognized by BIOS and by Linux).

- If the NIC card is not recognized by BIOS (for example, for a non-appliance server machine), you may need to adjust IRQ/memory settings as per the manufacturer's recommendations.
- Once the NIC is recognized by BIOS, it should be automatically recognized by the software (Linux). If for some reason, the NIC is recognized by BIOS, but not by Linux, then login to the system and run "kudzu". This will bring up a utility that helps you configure the NIC.

To Configure an Additional NIC:

Step 1 To verify that the NIC has been recognized by Linux, type `ifconfig ethn` (where ***n*** is the interface number). For example, if adding a NIC to a system that already has two built-in Ethernet interfaces (eth0 and eth1), ***n*** is 2 and you enter `ifconfig eth2`.

Step 2 Verify that the output displays information about the interface including MAC address and transmit and receive counters. This means the interface is recognized by Linux and can be used.

Step 3 Change to the following directory:

```
cd /etc/sysconfig/network-scripts
```

Step 4 Use vi to edit the `ifcfg-ethn` file for the interface, for example:

```
vi ifcfg-eth2
```

Step 5 Add the following lines into the file—replacing `IPADDR`, `NETMASK`, `BROADCAST`, and `NETWORK` values with the actual values suitable for your network:

```
DEVICE=eth2
IPADDR=192.168.0.253
NETMASK=255.255.255.252
BROADCAST=192.168.0.255
NETWORK=192.168.0.252
BOOTPROTO=static
ONBOOT=yes
TYPE=Ethernet
```

Step 6 Save the file and reboot the system. The network interface is now ready to be used for HA.

Note If the NIC card is not recognized by BIOS (for example, for a non-appliance server machine), you may need to adjust IRQ/memory settings as per the manufacturer's recommendations.

Once the NIC is recognized by BIOS, it should be automatically recognized by the software (Linux). If for some reason, the NIC is recognized by BIOS, but not by Linux, then login to the system and run `kudzu`. This brings up a utility that helps you to configure the NIC.

Note Static IP addresses must be configured for the CAM/CAS interfaces. DHCP mode is not supported for configuration of these interfaces.

See Chapter 4, "Configuring High Availability (HA)"for details on configuring HA.

Serial Connection to the CAM and CAS

This section details how to access the CAM and CAS command line via serial connection.

Step 1 Connect the serial port of your admin computer to an available serial port on the CAM or CAS with a serial cable.

Note If the CAM or CAS is already configured for High-Availability (failover), one of its serial connections may be in use for the peer heartbeat connection. In this case, the machine must have at least two serial ports to be able to manage the peer CAM or CAS over a serial connection. If it does not, you can use an Ethernet port for the peer connection. For more information, see Installing a Clean Access Manager High Availability Pair, page 4-3

Step 2 After physically connecting the workstation to the CAM or CAS, access the serial connection interface using any terminal emulation software. The following steps describe how to connect using Microsoft® HyperTerminal. If you are using different software, the steps may vary.

Setting Up the HyperTerminal Connection

Step 3 Open the HyperTerminal window by clicking **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal**.

Step 4 Type a name for the session and click **OK**.

Step 5 In the **Connect using** list, choose the COM port on the workstation to which the serial cable is connected (usually either COM1 or COM2) and click **OK**.

Step 6 Configure the **Port Settings** as follows:

- Bits per second – 9600
- Data bits – 8
- Parity – None
- Stop bits – 1
- Flow control – None

Step 7 Go to **File** > **Properties** to open the Properties dialog for the session and change the **Emulation** setting to `VT100`.

Step 8 You should now be able to access the command interface for the CAM or CAS. You can now:

- Install the Clean Access Manager (CAM) Software from CD-ROM, page 3-5
- Install the Clean Access Server (CAS) Software from CD-ROM, page 3-22
- Perform the Initial CAM Configuration, page 3-6
- Perform the Initial CAS Configuration, page 3-24

Note If you already performed the initial installation, but need to modify the original settings, you can log in as user `root` and run the `service perfigo config` command.

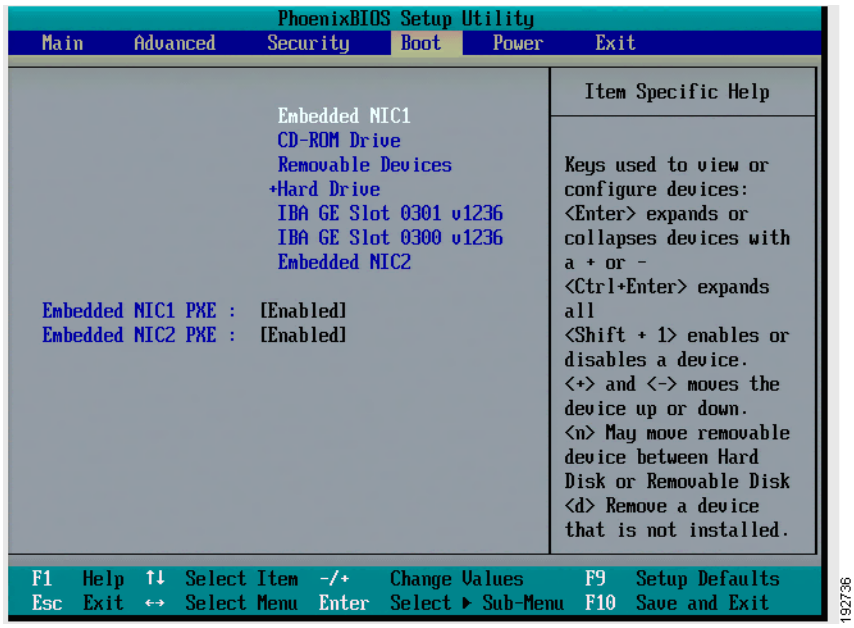
Configuring Boot Settings on the Cisco NAC Appliance CAM/CAS

If your CAM or CAS does not read the software on the CD-ROM drive, and instead attempts to boot from the hard disk, use the following steps to configure the appliance to boot from CD-ROM before attempting to re-image or upgrade the appliance from CD.

Step 1 Press the F10 key while the system is booting.

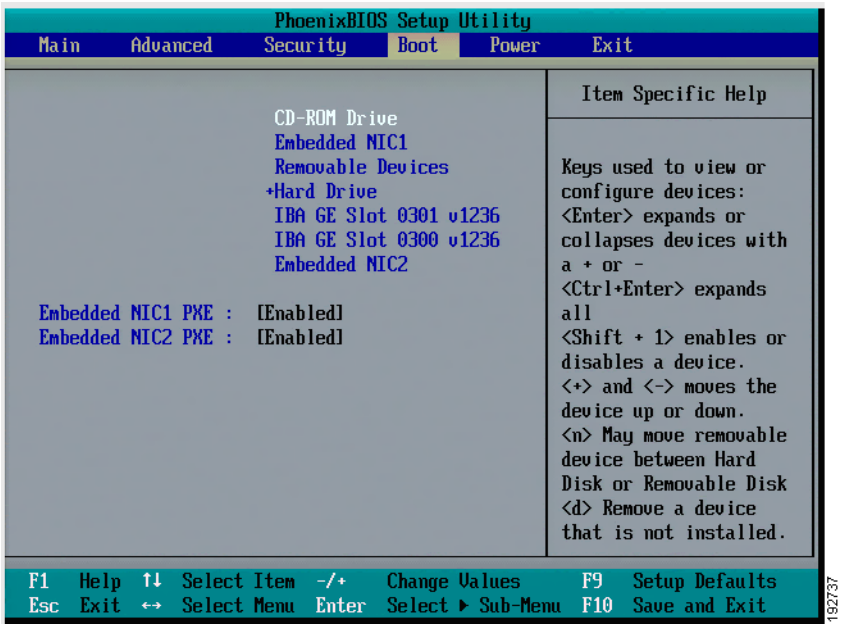
Step 2 Go to the Boot menu (Figure 3-11).

Figure 3-11 Boot Menu



Step 3 Change the setting to boot from CD ROM by selecting “CD-ROM Drive” from the menu and pressing the plus (“+”) key (Figure 3-12).

Figure 3-12 Boot from CD-ROM Drive



Step 4 Press the F10 key to Save and Exit.

Useful CLI Commands for the CAM/CAS

This section covers CLI commands for both the Clean Access Manager and Clean Access Server:

CAM CLI Commands

You can perform most administration tasks for the Clean Access Manager through the web admin console, such as configure behavior, and perform operations such as starting and rebooting the CAM. However, in some cases you may need to access the CAM configuration directly, for example if the web admin console is unavailable due to incorrect network or VLAN settings. You can use the Cisco NAC Appliance command line interface (CLI) to set basic operational parameters directly on the CAM.

To run the CLI commands, access the CAM using SSH and log in as user **`root`** and enter the corresponding password. If already serially connected to the CAM, you can run CLI commands from the terminal emulation console after logging in as **`root`** (see Connect the Clean Access Manager, page 3-4). The format `service perfigo <command>` is used to enter a command from the command line. Table 3-3 lists the commonly used Cisco NAC Appliance CLI commands.

Table 3-3 CLI Commands

Command	Description
`service perfigo start`	Starts up the appliance. If the CAM is already running, a warning message appears. The CAM must be stopped for this command to be used.
`service perfigo stop`	Shuts down the Cisco NAC Appliance service.
`service perfigo restart`	Shuts down the Cisco NAC Appliance service and starts it up again. This is used when the service is already running and you want to restart it. **Note** **`service perfigo restart`** should not be used to test high availability (failover). Instead, Cisco recommends "shutdown" or "reboot" on the machine to test failover, or if a CLI command is preferred, **`service perfigo stop`** and **`service perfigo start`**.
`service perfigo reboot`	Shuts down and reboots the machine. You can also use the Linux **`reboot`** command.
`service perfigo config`	Starts the configuration script to modify the CAM configuration. After completing **`service perfigo config`**, you must reboot the CAM.
`service perfigo time`	Use to modify the time zone settings.

Power Down the CAM

To power down the CAM, use one of the following recommended methods while connected via SSH:

- Type **`service perfigo stop`**, then power down the machine, or
- Type **`/sbin/halt`**, then power down the machine.

Restart Initial Configuration

To start the configuration script, type **`service perfigo config`** while connected through SSH. For example: `[root@camanager root]# service perfigo config`

This command causes the configuration utility script to start (on either the CAS or CAM). The script lets you configure the network settings for the CAM (see Perform the Initial CAM Configuration, page 3-6 for instructions). After running and completing **`service perfigo config`**, make sure to run **`service perfigo reboot`** or **`reboot`** to reset the CAM with the modified configuration settings.

Note For details on restoring the database from automated and manual backup snapshots via command line utility, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

CAS CLI Commands

The CAM web admin console allows you to perform most of the tasks required for administering Cisco NAC Appliance deployment. However, there are two cases where the command line interface of the CAS can be or must be used:

- Use the CAS CLI Commands for Cisco NAC Appliance to access the CAS configuration directly for initial configuration of the CAS or if the web admin console is unavailable due to incorrect network or VLAN settings.
- If you have purchased the Cisco NAC Profiler solution, use the CAS CLI Commands for Cisco NAC Profiler to enable the Cisco NAC Profiler Collector application on the Clean Access Server.

To run the CLI commands, access the CAS using SSH and log in as user **`root`** and enter the root user password. If already serially connected to the CAS, you can run CLI commands from the terminal emulation console after logging in as **`root`** (see Connect the Clean Access Manager, page 3-4).

CAS CLI Commands for Cisco NAC Appliance

The format `service perfigo <command>` is used to enter a command from the command line. Table 3-3 lists the commonly used Cisco NAC Appliance CLI commands.

Table 3-4 Cisco NAC Appliance CLI Commands for CAS

Command	Description
`service perfigo start`	Starts up the CAS. If the CAS is already running, a warning message appears. The CAS must be stopped for this command to be used.
`service perfigo stop`	Shuts down the Cisco NAC Appliance service. **Note** When the management VLAN is set, this command will cause the CAS to lose network connectivity when issued. You can use **`service perfigo maintenance`** instead.

Table 3-4 Cisco NAC Appliance CLI Commands for CAS

Command	Description
`service perfigo maintenance`	This command brings the CAS to maintenance mode, in which only the basic CAS router runs and continues to handle VLAN-tagged packets. The command allows communication through the management VLAN and is intended for environments where the CAS is in trunk mode and the native VLAN is different than the management VLAN. **Note** You can use `service perfigo maintenance` to stop the service when testing high availability (failover) for Virtual Gateway CASs over an SSH connection.
`service perfigo platform`	This command allows you to determine whether the CAS is a standard Clean Access Server appliance or a Cisco NAC network module installed in a Cisco ISR router chassis. The output displays either "APPLIANCE" or "NME-NAC" as the platform setting. For detailed installation and configuration information, see *Getting Started with Cisco NAC Network Modules in Cisco Access Routers* and *Installing Cisco Network Modules in Cisco Access Routers*.
`service perfigo restart`	Shuts down the Cisco NAC Appliance service and starts it up again. This is used when the service is already running and you want to restart it. **Note** `service perfigo restart` should not be used to test high availability (failover). Instead, Cisco recommends "shutdown" or "reboot" on the machine to test failover, or, if a CLI command is preferred, `service perfigo stop` or `service perfigo maintenance` followed by `service perfigo start`
`service perfigo reboot`	Shuts down and reboots the machine. You can also use the Linux `reboot` command.
`service perfigo config`	Starts the configuration script to modify the CAS configuration. After completing `service perfigo config`, you must reboot the CAS. For instructions on using the script, see Perform the Initial CAM Configuration, page 3-6
`service perfigo time`	Use to modify the time zone settings.

CAS CLI Commands for Cisco NAC Profiler

All Cisco NAC Appliance releases are shipped with a default version of the Cisco NAC Profiler Collector component. Cisco NAC Appliance 4.8(1) releases are shipped with Collector version 3.1.0-24 by default. When upgrading the NAC Server to a newer NAC Appliance release, the current version of the Collector will be replaced with the default version of the Collector shipped with the NAC Appliance release. For example, if you are running Release 4.7(2) and Collector 3.1.1, and you upgrade to NAC 4.8(1), Collector will be downgraded to 3.1.0.24. You need to manually upgrade the 3.1.0.24 Collector to 3.1.1 again and configure it after the NAC Server upgrade.

The Clean Access Server is shipped with a default version of the Cisco NAC Profiler Collector component, which needs to be enabled and configured separately when integrating with the Cisco NAC Profiler solution. Table 3-5 lists CLI commands issued on the CAS for the Cisco NAC Profiler Collector service. For complete details on the Cisco NAC Profiler solution, refer to the *Cisco NAC Profiler Installation and Configuration Guide* and *Release Notes for Cisco NAC Profiler*.

Note To display the version of the Collector on the CAS, SSH to the CAS machine running the Collector service and type **rpm -q Collector**.

Table 3-5 Cisco NAC Profiler Collector CLI Commands for CAS

Command	Description
`service collector start`	Starts the Collector service on the CAS.
`service collector stop`	Shuts down the Collector service on the CAS.

`service collector verify`	Displays the configured Collector Services running on the CAS
	`Collector Network Configuration`
	`Collector Name = bcas1-fw`
	`Connection Type = server`
	`Listen on IP = 10.40.1.10`
	`Network IP ACL`
	`127.0.0.1`
	`10.10.0.211`
	`10.10.0.210`
	`10.10.0.212`
	`Port Number = 31416`
	`Encryption type = AES`
	`Shared secret = profiler`

`service collector status`	Displays the running status of the individual Collector modules on the CAS, for example:
	`Profiler Status`
	`o Server Not Installed`
	`o Forwarder Running`
	`o NetMap Running`
	`o NetTrap Running`
	`o NetWatch Running`
	`o NetInquiry Running`
	`o NetRelay Running`

Table 3-5 Cisco NAC Profiler Collector CLI Commands for CAS

Command	Description
`service collector restart`	Stops and then restarts the Collector service on the CAS. This is used when the service is already running and you want to restart it.

`service collector config`	Starts the Collector service configuration script to allow communication with the Cisco NAC Profiler Server. For example:
	`[root@caserver12 /]# service collector config`
	`Enable the NAC Collector (y/n) [y]:`
	`Configure NAC Collector (y/n) [y]:`
	`Network configuration to connect to a NAC Profiler Server`
	`  Connection type (server/client) [client]:`
	`  Connect to IP [127.0.0.1]: 192.168.96.20`
	`  Port number [31416]:`
	`  Encryption type (AES, blowfish, none) [AES]: none`
	`  Shared secret []: cisco1232`
	`-- Configured caserver12-fw`
	`-- Configured caserver12-nm`
	`-- Configured caserver12-nt`
	`-- Configured caserver12-nw`
	`-- Configured caserver12-ni`
	`-- Configured caserver12-nr`
	`NAC Collector has been configured`
	For detailed installation and configuration information, see the *Cisco NAC Profiler Installation and Configuration Guide*.

Manually Restarting the CAM/CAS Configuration Utility

If after installation you need to reset the configuration settings, or if you need to start the configuration utility manually, you can issue the **`service perfigo config`** CLI command on either the Clean Access Server or Clean Access Manager. When using **`service perfigo config`**, you will also need to enter **`service perfigo reboot`** or **`reboot`** after configuration is complete to reboot the machine.

Step 1 Connect to the CAS or CAM through direct console connection, serial connection, or SSH.

Step 2 Login as **`root`** with the correct password.

Step 3 Enter the **`service perfigo config`** command.

Step 4 Accept the default values or provide new ones for all prompts (as described in Perform the Initial CAM Configuration, page 3-6 or Perform the Initial CAS Configuration, page 3-24).

Step 5 When configuration is done, enter **`service perfigo reboot`** or **`reboot`** to reboot the machine.

Troubleshooting the Installation

This section addresses the following troubleshooting topics:

Note If the FIPS card in a Cisco NAC-3315/3355/3395 CAM/CAS ceases to work correctly, make sure the FIPS card operation switch is set to "O" (for operational mode), as described in the "FIPS 140-2 Compliance" section of the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*. If the FIPS card is still not operational, you will need to RMA the appliance with Cisco Systems and replace it with a new Cisco NAC-3315/3355/3395. Refer to the "Cisco NAC Appliance RMA and Licensing" section of *Cisco NAC Appliance Service Contract/Licensing Support* for details.

For further troubleshooting information, see the latest version of the Release Notes.

Verify/Change Current Master Secret on CAM/CAS

Clean Access Managers and Clean Access Servers use a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to fail over to the HA peer CAM/CAS in an HA deployment. (HA-Secondary CAMs/CASs are not able to assume the "active" role following a failover event when the master secret passwords are different.) If you suspect that the CAM/CAS master secret is different from its peer in an HA deployment, you can do the following to verify and/or change the master secret on CAM/CAS HA peers:

Step 1 Log in to the CLI of the HA-Primary CAM/CAS as "root."

Step 2 Enter `cat /root/.perfigo/master` and record the master secret signatures for that CAM/CAS.

Step 3 Log in to the CLI of the HA-Secondary CAM/CAS as "root" and enter the same `cat /root/.perfigo/master` command.

Step 4 If the two CAM/CAS master secret signatures are different, use `service perfigo config` to "reconfigure" the CAM/CAS with the incorrect master secret, accepting the previous values for all settings other than the master secret, which, in the case of an HA peer, you specify to match the other appliance in the HA pair.

a. Enter `service perfigo stop` on the HA-Secondary CAM/CAS.

b. Enter `service perfigo stop` on the HA-Primary CAM/CAS.

c. Enter `service perfigo config` to "reconfigure" the CAM/CAS with the incorrect master secret. (Once you have completed the initial configuration, you will also need to reboot the appliance.)

d. Enter `service perfigo start` to bring up the HA-Primary CAM/CAS.

e. When the HA-Primary CAM/CAS comes back up, enter `service perfigo start` to bring up the HA-Secondary CAM/CAS.

After approximately 5 minutes, an HA-Secondary CAM automatically synchronizes with the HA-Primary.

Recover From Corrupted Master Secret

Note This procedure applies to both standalone and HA CAMs and CASs. In order to use this procedure for an HA CAM/CAS with a corrupted master secret, you must bring both peers in the HA deployment to "standalone" state before performing the steps necessary to recover from the corrupted master secret.

If the master secret changes (by using **service perfigo config**, for example) and the CAM/CAS database is synchronized from a peer CAM/CAS that has a different master secret, the database can become corrupted rendering the appliance unusable. You can recover from this scenario by going through the following steps:

Step 1 Log in to the CLI of the CAM/CAS with the corrupted master secret as "root."

Step 2 Remove **/root/.perfigo/master** file from the affected CAM/CAS.

Step 3 Use `service perfigo config` to "reconfigure" the CAM/CAS initial configuration, accepting the previous values for all settings other than the master secret, which, in the case of an HA peer, you specify to match the other appliance in the HA pair.

Step 4 If deployed as part of an HA pair, bring the HA-Primary CAM/CAS back up, and then bring the HA-Secondary CAM/CAS back up. Database synchronization between active and standby CAMs takes place automatically, restoring the proper master secret in both the database and file system.

Network Interface Card (NIC) Driver Not Supported

For complete details, refer to the "Troubleshooting Network Card Driver Support Issues" section of the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*.

Resetting and Restoring an Unreachable Clean Access Server

If incorrect network, SSL certificate, or VLAN settings have rendered the Clean Access Server unreachable from the Clean Access Manager, you can reset the Clean Access Server's configuration. Note that resetting the configuration restores the Clean Access Server configuration to its install state. Any configuration settings made since installation will be lost.

To reset the configuration:

Step 1 Connect to the Clean Access Server by SSH.

Step 2 Delete the `env` file:

```
# rm /perfigo/access/bin/env
```

Step 3 Then reboot using:

```
# service perfigo reboot
```

You can now add the CAS to the CAM. See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Enabling TLSv1 on Internet Explorer Version 6

Cisco NAC Appliance network administrators managing the CAM/CAS via web console *and* client machine browsers accessing a FIPS-compliant Cisco NAC Appliance Release 4.8(1) network require TLSv1 in order to "talk" to the network, which is disabled by default in Microsoft Internet Explorer Version 6.

To locate and enable this setting in IE version 6:

Step 1 Got to **Tools** > **Internet Options**.

Step 2 Select the **Advanced** tab.

Step 3 Scroll down to locate the **Use TLS 1.0** option under **Security**.

Step 4 Click on the checkbox to enable the **Use TLS 1.0**. option and click **Apply**.

Step 5 If necessary, close the browser and open a new one where the TLS 1.0 option should now be automatically enabled.

Note Mozilla Firefox has not shown this limitation.

Powering Down the NAC Appliance

To power down the CAM/CAS, use one of the following recommended methods while connected via console/SSH. These methods prevent database corruption when powering down the CAM.

- Type `service perfigo stop` and power down the machine.
- Type `/sbin/halt` and power down the machine.

CHAPTER 4

Configuring High Availability (HA)

This chapter covers the following topics:

Adding High Availability Cisco NAC Appliance To Your Network

The following diagrams illustrate how HA-CAMs and HA-CASs can be added to an example core-distribution-access network (with Catalyst 6500s in the distribution and access layers).

Figure 4-1 shows a network topology without Cisco NAC Appliance, where the core and distribution layers are running HSRP (Hot Standby Router Protocol), and the access switches are dual-homed to the distribution switches.

Figure 4-1 Example Core-Distribution-Access Network Before Cisco NAC Appliance

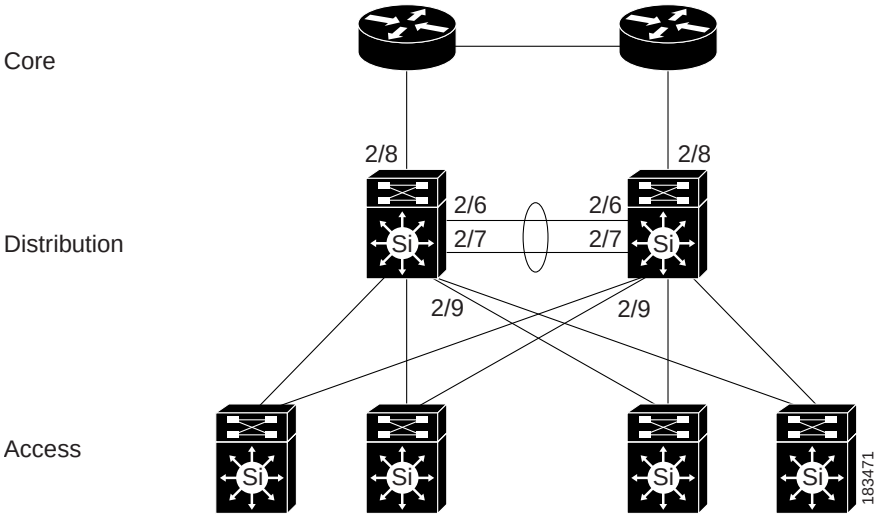


Figure 4-2 shows how HA-CAMs can be added to the core-distribution-access network. In this example, the HA heartbeat connection is configured over both serial and eth1 interfaces.

Figure 4-2 Adding HA CAMs to Network

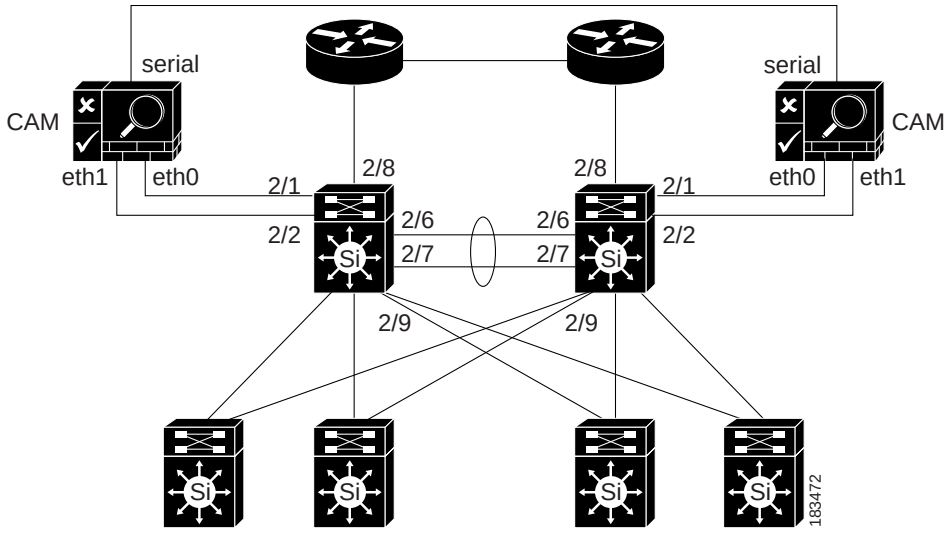
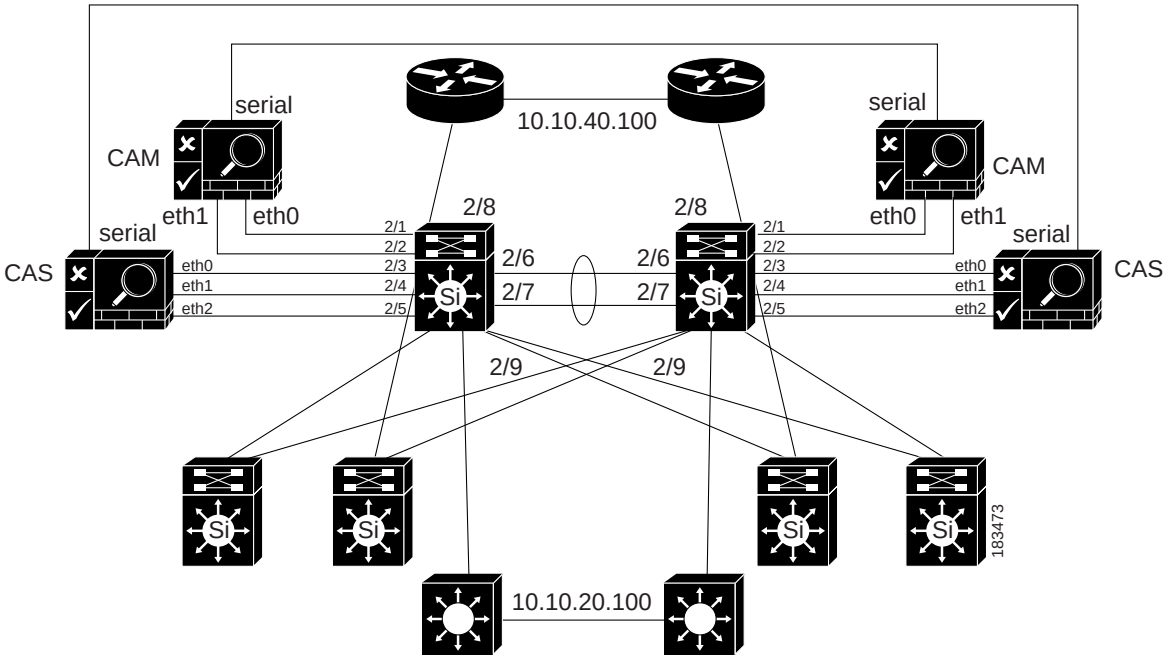


Figure 4-3 shows how HA-CASs can be added to the core-distribution-access network. In this example, the CAS is configured as an L2 OOB Virtual Gateway in Central Deployment. The HA heartbeat connection is configured over both a serial interface and a dedicated eth2 interface. Link-failure based failover connection can also be configured over the eth0 and/or eth1 interfaces.

Note Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

Figure 4-3 Adding HA CAS to Network



Installing a Clean Access Manager High Availability Pair

This section describes how to set up a pair of Clean Access Manager machines for high-availability. By deploying Clean Access Managers in high-availability mode, you can ensure that important monitoring, authentication, and reporting tasks continue in the event of an unexpected shutdown. Topics include:

Note You must use identical appliances (e.g. NAC-3350 and NAC-3350) in order to configure High Availability (HA) pairs of Clean Access Managers (CAMs) or Clean Access Servers (CASs).

CAM High Availability Overview

Caution CAM-CAS communication and HA-CAM and/or HA-CAS peer communication can break down and adversely affect network functionality when SSL certificates expire. For more information, see the "HA Active-Active Situation Due to Expired SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

The following key points provide a high-level summary of HA-CAM operation:

- The Clean Access Manager high-availability mode is an Active/Passive two-server configuration in which a standby CAM machine acts as a backup to an active CAM machine.
- The active Clean Access Manager performs all tasks for the system. The standby CAM monitors the active CAM and keeps its database synchronized with the active CAM's database.

  Note CAM Authorization settings are not automatically passed from one CAM to the other in an HA-pair. If you use the Authorization feature in a CAM HA-pair, follow the guidelines in the "Backing Up and Restoring CAM/CAS Authorization Settings" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* to ensure you are able to *exactly* duplicate your Authorization settings from one CAM to its high availability counterpart.

- Clean Access Managers and Clean Access Servers use a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to fail over to the HA peer CAM/CAS in HA deployments. (HA-Secondary CAMs/CASs are not able to assume the "active" role following a failover event when the master secret passwords are different.)

- Both CAMs share a virtual Service IP for the eth0 trusted interface. The Service IP must be used for the SSL certificate.
- The Service IP address is used for all messages and requests sent to the CAM, including communication from the CAS and the administration web console.
- The CAM uses its individual (eth0) IP address for all communications sent to the CAS and proxy authentication messages.
- The primary and secondary CAM machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
- To support FIPS 140-2 compliance, HA CAMs/CASs automatically establish an IPSec tunnel to ensure all communications between the HA Pair appliances remains secure across the network.
- In order to ensure an active CAM is always available, its trusted interface (eth0) must be up. To avoid a situation where a CAM is active but is not accessible via its trusted interface (that is, the standby CAM receives heartbeat packets from the active CAM, but the active CAM's eth0 interface fails), the link-detect mechanism allows the standby CAM to be aware of when the active CAM's eth0 interface becomes unavailable.
- Both the Clean Access Manager and Clean Access Server are designed to automatically reboot in the event of a hard-drive failure, thus automatically initiating failover to the standby CAM/CAS.
- Newer Cisco NAC-3310 CAMs/CASs feature a 160GB hard drive, while older NAC-3310s originally shipped with 80GB hard drives. Both of these hard drive sizes support High Availability (HA) deployments, and you can safely deploy a 160GB model in an HA pair with an 80GB model.
- You can choose to “automatically configure” the eth1 interface in the **Administration** > **CCA Manager > Failover** page, but you must manually configure other (eth2 or eth3) HA interfaces with an IP address, netmask, etc. prior to configuring HA on the CAM.
- The eth0, eth1 and eth2/eth3 interfaces can be used for heartbeat packets and database synchronization. In addition, any available serial (COM) interface can also be used for heartbeat packets. If using more than one of these interfaces, then all the heartbeat interfaces need to fail for failover to occur.

Note If you are configuring your CAM for HA, you must use eth1 for heartbeat and database synchronization. All other Ethernet interfaces (eth0 and eth2/eth3) are optional for this purpose.

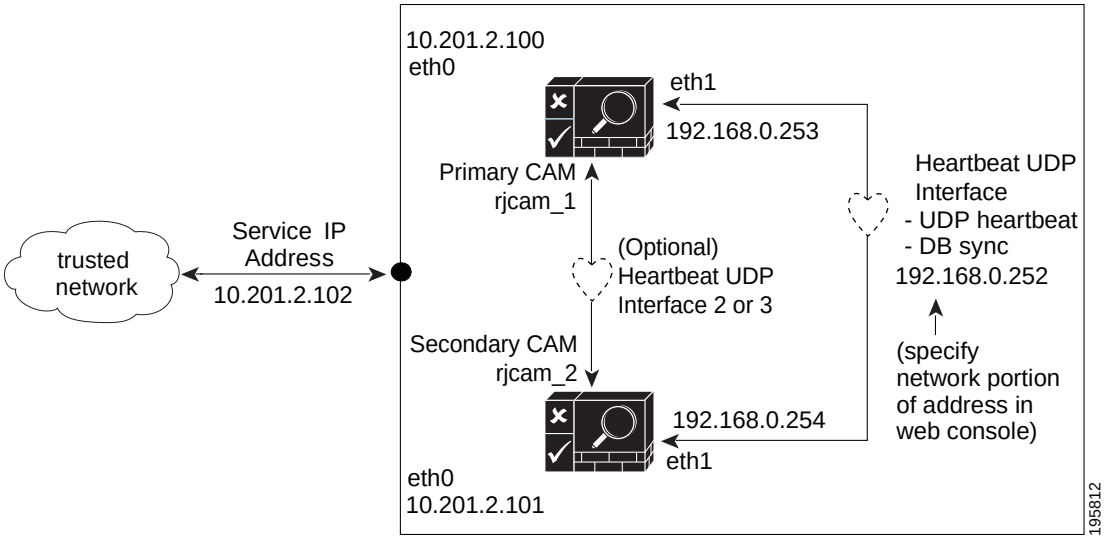
Note In CAM HA, when heartbeat is configured on multiple interfaces and eth1 is down, the standby CAM fails to do the database synchronization. The perfigo service is stopped on the standby CAM as the database synchronization happens only on eth1, which is down. Cisco recommends using only eth1 as heartbeat interface for CAM HA instead of using multiple HA interfaces.

Note When deploying the CAM/CAS across a WAN, you must prioritize all CAM/CAS traffic and SNMP traffic, and include the eth0/eth1 IP addresses of the CAM and CAS in addition to the Service IP address for HA pairs.

Caution The connection between HA pairs must be extremely reliable, with communication between HA pairs unimpeded. The best practice is to use a dedicated Ethernet cable. Breaking communication between HA pairs will result in two active nodes, which can have serious negative operational consequences. A key aspect of the link between HA pairs is the ability to restore that link should it go down; restoration may be fundamental to network stability, depending on your design.

Figure 4-4 illustrates a sample configuration.

Figure 4-4 Clean Access Manager Example High-Availability Configuration



The Clean Access Manager high-availability mode is an Active/Passive two-server configuration in which a standby Clean Access Manager machine acts as a backup to an active Clean Access Manager machine. While the active CAM carries most of the workload under normal conditions, the standby monitors the active CAM and keeps its data store synchronized with the active CAM's data.

If a failover event occurs, such as the active CAM shuts down or stops responding to the peer's "heartbeat" signal, the standby assumes the role of the active CAM.

When first configuring the HA peers, you must specify an HA-Primary CAM and HA-Secondary CAM. Initially, the HA-Primary is the active CAM, and the HA-Secondary is the standby (passive) CAM, but the active/passive roles are not permanently assigned. If the primary CAM goes down, the secondary (standby) becomes the active CAM. When the original primary CAM restarts, it assumes the backup role.

Note If *both* the HA-Primary and HA-Secondary CAMs in your HA deployment lose their configuration, you can restore the system using the guidelines in the "Restoring Configuration from CAM Snapshot—HA-CAM or HA-CAS" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

When the Clean Access Manager starts up, it checks to see if its peer is active. If not, the starting CAM assumes the active role. If the peer is active, on the other hand, the starting CAM becomes the standby.

You can configure two Clean Access Managers as an HA pair at the same time, or you can add a new Clean Access Manager to an existing standalone CAM to create a high-availability pair. In order for the pair to appear to the network as one entity, you must specify a **Service IP Address** to be used as the trusted interface (eth0) address for the HA pair. This Service IP address is also used to generate the SSL certificate.

To create the Heartbeat UDP Interface link over which HA information is exchanged, you connect the eth1 ports of both CAMs and specify a private network address not currently routed in your organization (the default Heartbeat UDP interface IP address is 192.168.0.252). The Clean Access Manager then creates a private, secure two-node network for the eth1 ports of each CAM to exchange UDP heartbeat traffic and synchronize databases.

Note The CAM always uses eth1 as the UDP heartbeat interface.

Note When the primary eth1 link has been disconnected and only the serial link remains, the CAM returns a database error indicating that it cannot sync with its HA counterpart, and the administrator sees the following error in the CAM web console: “WARNING! Closed connections to peer [standby IP] database! Please restart peer node to bring databases in sync!!”

Warning **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for Cisco NAC Appliance CAMs/CASs and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.**

Note For serial cable connection for HA (either HA-CAM or HA-CAS), the serial cable must be a “null modem” cable. For details, refer to http://www.nullmodem.com/NullModem.htm.

The following sections describe the steps for setting up high availability.

Note The instructions in this section assume that you are adding a Clean Access Manager to a standalone CAM in order to configure the HA pair for a test network.

Before Starting

Warning **To prevent any possible data loss during database synchronization, always make sure the standby (secondary) Clean Access Manager is up and running before failing over the active (primary) Clean Access Manager.**

Before configuring high availability, ensure that:

- You have obtained a high-availability (failover) license.

Note When installing a CAM Failover (HA) license, install the Failover license to the Primary CAM first, then load all the other licenses.

- Both CAMs are installed and configured (see Perform the Initial CAM Configuration, page 3-6).
- The two CAMs in the HA pair must remain Layer 2 adjacent to support heartbeat and sync functions.
- For heartbeat, each CAM needs to have a unique hostname (or node name). For HA CAM pairs, this host name will be provided to the peer, and must be resolved via DNS or added to the peer's /etc/hosts file.
- You have a CA-signed certificate for the Service IP of the HA CAM pair. (For testing, you can use the CA-signed certificate of the HA-Primary CAM, but this requires additional steps to configure the HA-Primary CAM's IP as the Service IP).
- The HA-Primary CAM is fully configured for runtime operation. This means that connections to authentication sources, policies, user roles, access points, and so on, are all specified. This configuration is automatically duplicated in the HA-Secondary (standby) CAM.
- If you use the Authorization feature in a CAM HA-pair, follow the guidelines in "Backing Up and Restoring CAM/CAS Authorization Settings" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* to ensure you are able to *exactly* duplicate your Authorization settings from one CAM to its high availability counterpart. (CAM Authorization settings are not automatically passed from one CAM to the other in an HA-pair.)
- Both Clean Access Managers are accessible on the network (try pinging them to test the connection).
- The machines on which the CAM software is installed have at least one free Ethernet port (eth1) and at least one free serial port. Use the specification manuals for the server hardware to identify the serial port (ttyS0 or ttyS1) on each machine.
- In Out-of-Band deployments, Port Security is not enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

The following procedures require you to reboot the Clean Access Manager. At that time, its services will be briefly unavailable. You may want to configure an online CAM when downtime has the least impact on your users.

Note Cisco NAC Appliance web admin consoles support the Internet Explorer 6.0 or above browser.

Connect the Clean Access Manager Machines

There are two types of connections between HA-CAM peers: one for exchanging runtime data relating to the Clean Access Manager activities and one for the heartbeat signal. In High Availability, the Clean Access Manager **always** uses the eth1 interface for both data exchange and heartbeat UDP exchange. When the UDP heartbeat signal fails to be transmitted and received within a certain time period, the standby system takes over. In order to provide an extra measure of heartbeat redundancy, Cisco recommends you use more Ethernet interfaces in addition to eth1 (mandatory) interface for heartbeat exchange. In order for a failover to occur, all configured heartbeat interfaces must report heartbeat exchange failure. (The eth0 and eth2/eth3 can be used for additional heartbeat interfaces.) Note, however, that the eth1 connection between the CAM peers is mandatory.

Physically connect the peer Clean Access Managers as follows:

- Use a crossover cable to connect the eth1 Ethernet ports of the Clean Access Manager machines. This connection is used for the heartbeat UDP interface and data exchange (database mirroring) between the failover peers.
- Use null modem serial cable to connect the serial ports (highly recommended).
- Optionally connect eth2 and/or eth3 interfaces on the CAM to counterpart interfaces on the HA peer using either crossover cables or via an in-line switch. (Remember: you must configure these interfaces manually before configuring your CAM for HA).

Note For serial cable connection for HA, the serial cable must be a "null modem" cable. For details, refer to http://www.nullmodem.com/NullModem.htm.

Serial Connection

By default, the first serial port detected on the CAM server is configured for console input/output (to facilitate installation and other types of administrative access).

If the machine has only one serial port (COM1 or ttyS0), you can reconfigure the port to serve as the high-availability heartbeat connection. This is because, after the CAM software is installed, SSH or KVM console can always be used to access the command line interface of the CAM.

Note When the primary eth1 link has been disconnected and only the serial link remains, the CAM returns a database error indicating that it cannot sync with its HA counterpart, and the administrator sees the following error in the CAM web console: "WARNING! Closed connections to peer [standby IP] database! Please restart peer node to bring databases in sync!!"

Warning **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for Cisco NAC Appliance CAMs/CASs and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.**

Configure the HA-Primary CAM

Once you have verified the prerequisites, perform the following steps to configure the Clean Access Manager as the HA-Primary for the high availability pair. See Figure 4-4 for an example high-availability configuration.

Step 1 Open the web admin console for the Clean Access Manager to be designated as the HA-Primary, and go to **Administration** > **CCA Manager > SSL > X509 Certificate** to configure the SSL certificate for the primary CAM.

Note The HA configuration steps in this chapter assume that a temporary certificate will be exported from the HA-Primary CAM to the HA-Secondary CAM.

If using a temporary certificate for the HA pair:

a. Click **Generate Temporary Certificate**, enter information for all of the fields in the form, and click **Generate**. The certificate must be associated with the Service IP addresses of the HA pair.

b. When finished generating the temporary certificate, click the checkboxes for the certificate and Private Key to highlight them in the table.

c. Click **Export** to save the certificate and Private Key to your local machine. You must import the certificate and Private Key later when configuring the HA-Secondary CAM.

If using a CA-signed certificate for the HA pair:

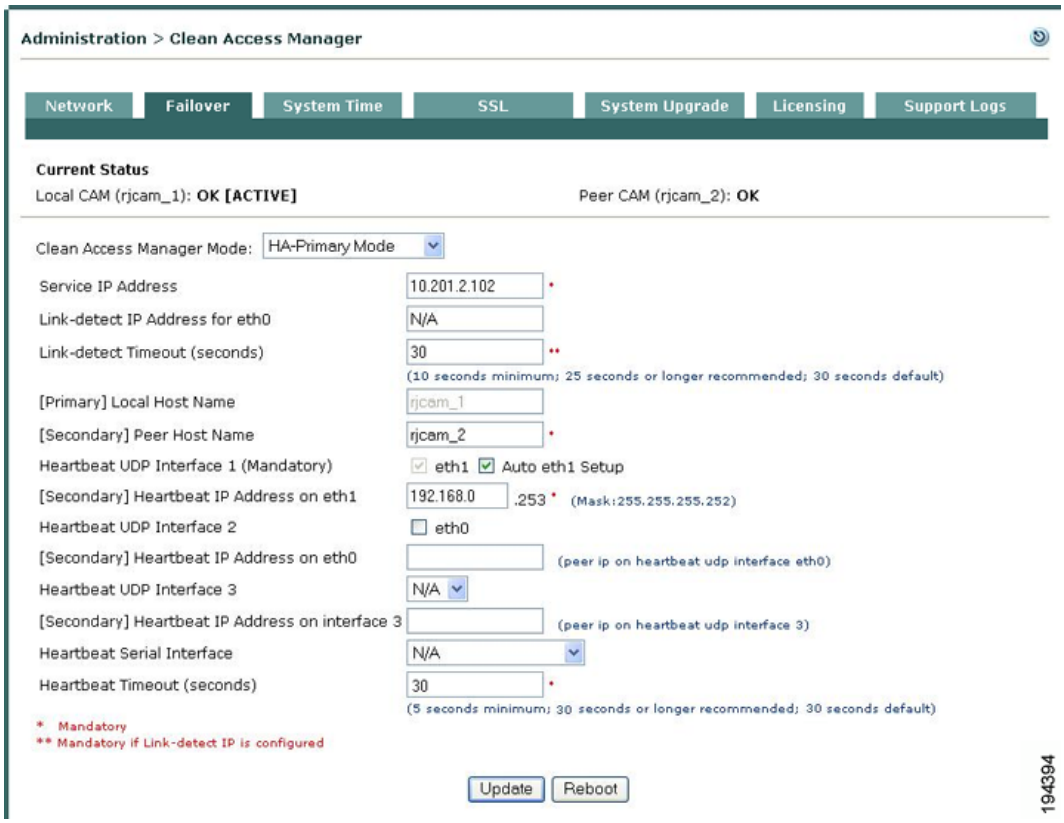
Note This process assumes you have already generated a Certificate Signing Request and accompanying Private Key, submitted the request to your Certificate Authority, and have received your CA-signed certificate. If you have not yet obtained a CA-signed certificate for the CAS, be sure to follow the instructions in the "Manage CAM SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for details.

a. Click **Browse** and navigate to the directory on your local machine containing the CA-signed certificate and Private Key.

b. Click **Import**. Note that you will need to import the same certificate later to the HA-Secondary CAS.

Step 2 Go to **Administration** > **CCA Manager** and click the **Failover** tab. Choose the **HA-Primary** option from the **Clear Access Manager Mode** dropdown menu. The high availability settings appear:

Figure 4-5 HA-Primary Clean Access Manager Failover Settings



Step 3 Copy the value from the **IP Address** field under **Administration** > **CCA Manager > Network** and enter it in **Service IP Address** field. The Network Settings IP Address is the existing IP address of the primary Clean Access Manager. The idea here is to turn this IP address, which the Clean Access Servers already recognize, into the virtual Service IP address Clean Access Servers use for the Clean Access Manager pair.

Step 4 Change the **IP address** under **Administration** > **CCA Manager > Network** to an available address (for example *x.x.x.*121).

Step 5 (Recommended) Specify parameters to enable failover based on eth0 link failure detection for the HA-Primary CAM:

a. Enter IP addresses for the interfaces the HA pair uses to failover from the primary to the secondary CAM in the **Link-detect IP Address for eth0** field. When IP addresses are entered in this field, the HA-Secondary CAM attempts to ping the specified HA-Primary CAM IP address to verify connectivity. Typically, the same IP address is entered on both the HA-Primary and HA-Secondary CAM, but you *can* specify different addresses for each CAM if your network topology allows.

b. Specify the duration (in seconds) the CAM continues to ping the Link-detect IP address before determining that the eth0 interface may have gone down, thus initiating a failover to the secondary CAM, in the **Link-detect Timeout** field. The minimum value for this setting is 10 seconds, but Cisco recommends at least a 25-second timeout interval.

Note Link-detect settings on the CAM (Release 4.1(3) and later) are needed to allow the active CAM to failover to the standby CAM in case of a switch port failure or a link failure on the switch port connected to eth0 of the active CAM. In the event a failover must take place, the Link detect setting allows the standby CAM to ensure that the secondary CAM eth0 interface is up and able to take on the active role.

Step 6 Each Clean Access Manager must have a unique host name (such as `rjcam_1` and `rjcam_2`). Type the host name of the HA-Primary CAM in the **Host Name** field under **Administration** > **CCA Manager** > **Network**, and type the host name of the HA-Secondary CAM in the **Peer Host Name** field under **Administration** > **CCA Manager** > **Failover**.

Note
- A **Host Name** value is mandatory when setting up high availability, while the **Host Domain** name is optional.
- The **Host Name** and **Peer Host Name** fields are case-sensitive. Make sure to match what is typed here with what is typed for the HA-Secondary CAM later.

Step 7 If you are using the default setting for the mandatory eth1 UDP heartbeat interface, leave the **Auto eth1 Setup** checkbox enabled (checked). If you want to specify a different **[Secondary] Heartbeat eth1 Address**, uncheck the **Auto eth1 Setup** checkbox and enter the new IP address in the **(peer IP on heartbeat udp interface on eth1)** field.

Note The **Auto eth1 Setup** option automatically assigns 192.168.0.254 as the primary CAM's eth1 (heartbeat) interface and assumes the IP address for the peer (secondary) eth1 interface is 192.168.0.253.

Warning **To specify redundant failover links as described in Step 9, you must first configure the appropriate Ethernet interfaces on the CAM before you try to set up HA. If you attempt to configure these interfaces and the NICs on which the Ethernet interfaces reside are not configured correctly, the CAM will enter maintenance mode (will not boot properly) when you reboot.**

Step 8 (Optional) If you want to enable the CAM's **Heartbeat UDP Interface 2** function that sets up a redundant failover heartbeat via the CAM eth0 interface, enable the **eth0** checkbox and specify an associated peer IP address in the **[Secondary] Heartbeat IP Address on eth0** field. Otherwise, leave this N/A if not using the additional UDP heartbeat interface.

Step 9 (Optional) If you want to enable the CAM's **Heartbeat UDP Interface 3** function, select **eth2** or **eth3** from the dropdown menu and specify an associated peer IP address in the **[Secondary] Heartbeat IP Address on interface 3** field. Otherwise, leave this N/A if not using the additional UDP heartbeat interface.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

Step 10 Specify the **Heartbeat Timeout** value for the HA primary CAM to set the duration the CAM should wait before declaring that it has lost communication with its HA peer, thus assuming the role of the active CAM in the HA pair. The default **Heartbeat Timeout** value is 30 seconds.

Note Starting from Cisco NAC Appliance Release 4.6(1), the **Heartbeat Timeout** default value has been increased to 30 seconds to help accommodate CAM HA peers located in relatively distant locations on the network, where latency issues might cause a standby HA CAM to assume the active role when it has not received heartbeat packets from its HA peer within the specified **Heartbeat Timeout** period. In the resulting network scenario, you could potentially end up with two "active" CAMs performing Cisco NAC Appliance functions, requiring you to reboot both CAMs to re-establish the correct primary/secondary HA peer relationship.

Step 11 Click **Update** and then **Reboot** to restart the Clean Access Manager.

After the Clean Access Manager restarts, make sure that the CAM machine is working properly. Check to see if the Clean Access Servers are connected and new users are being authenticated.

Configure the HA-Secondary CAM

Step 1 Open the web admin console for the Clean Access Manager to be designated as the HA-Secondary, and go to **Administration** > **CCA Manager > SSL > X509 Certificate**.

Step 2 Before starting:

- Back up the secondary CAM's private key.
- Make sure the private key and SSL certificate files associated with the Service IP/HA-Primary CAM are available (previously exported as described in Configure the HA-Primary CAM, page 4-8).

Step 3 Import the HA-Primary CAM's private key file and certificate as described below:

If using a temporary certificate for the HA pair:

a. Click **Browse** and navigate to the location on your local machine where you have saved the temporary certificate and Private Key you previously exported from the HA-Primary CAS.

b. Select the certificate file and click **Import**.

c. Repeat the process to import the Private Key.

If using a CA-signed certificate for the HA pair:

a. Click **Browse** and navigate to the location on your local machine where you have saved the CA-signed certificate you received from your Certificate Authority and the associated Private Key you exported from the HA-Primary CAS and saved to your local machine.

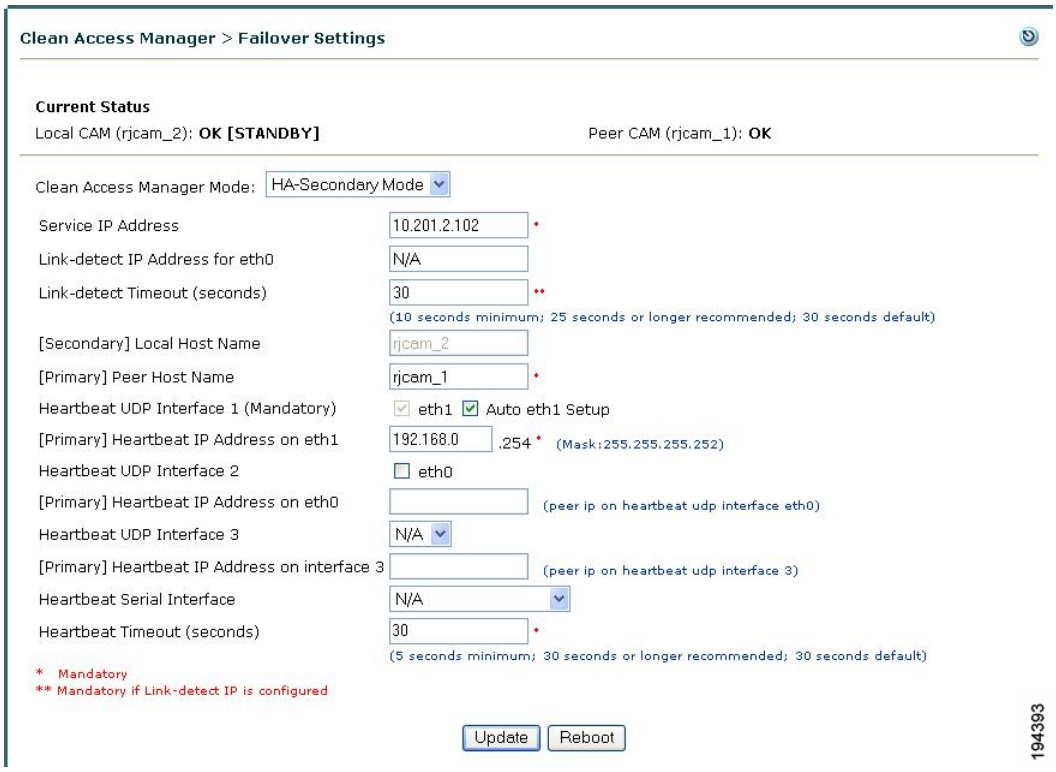
b. Select the CA-signed certificate file and click **Import**.

c. Repeat the process to import the Private Key.

For more information, see the "Manage CAM SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Step 4 Go to the **Administration** > **CCA Manager** > **Network** and change the **IP Address** of the secondary CAM to an address that is different from the HA-Primary CAM IP address and the Service IP address (such as *x.x.x.*122).

Figure 4-6 HA-Secondary Clean Access Manager Failover Settings



Step 5 Set the **Host Name** value to the same value set for the **Peer Host Name** in the HA-Primary CAM configuration. See Figure 4-4 on page 4-5.

Note The **Host Name** and **Peer Host Name** fields are case-sensitive. Make sure to match what is typed here with what was typed for the HA-Primary CAM.

Step 6 Choose **HA-Secondary** in the **Clean Access Manager Mode** dropdown menu. The high availability settings appear.

Step 7 Set the **Service IP Address** value to the same value set for the **Service IP Address** in the HA-Primary CAM configuration.

Step 8 (Recommended) Specify parameters to enable failover based on eth0 link failure detection for the HA-Secondary CAM:

a. Enter IP addresses for the interfaces the HA pair uses to failover from the primary to the secondary CAM in the **Link-detect IP Address for eth0** field.

b. Specify the duration (in seconds) the CAM continues to ping the Link-detect IP address before determining that the eth0 interface may have gone down, thus initiating a failover to the secondary CAM, in the **Link-detect Timeout** field. The minimum value for this setting is 10 seconds, but Cisco recommends at least a 25-second timeout interval.

Note Link-detect settings on the CAM (Release 4.1(3) and later) are needed to allow the active CAM to failover to the standby CAM in case of a switch port failure or a link failure on the switch port connected to eth0 of the active CAM. In the event a failover must take place, the Link detect setting allows the standby CAM to ensure that the secondary CAM eth0 interface is up and able to take on the active role.

Step 9 Set the **[Primary] Peer Host Name** value to the HA-Primary CAM's host name.

Step 10 If you are using the default setting for the mandatory eth1 UDP heartbeat interface, leave the **Auto eth1 Setup** checkbox enabled (checked). If you want to specify a different **[Primary] Heartbeat eth1 Address**, uncheck the **Auto eth1 Setup** checkbox and enter the new IP address in the **(peer IP on heartbeat udp interface on eth1)** field.

Note The **Auto eth1 Setup** option automatically assigns 192.168.0.254 as the primary CAM's eth1 (heartbeat) interface and assumes the IP address for the peer (secondary) eth1 interface is 192.168.0.253.

Warning **To specify redundant failover links as described in Step 12, you must first configure the appropriate Ethernet interfaces on the CAM before you try to set up HA. If you attempt to configure these interfaces, however, and the NICs on which the Ethernet interfaces reside are not configured correctly, the CAM will enter maintenance mode (will not boot properly) when you reboot.**

Step 11 (Optional) If you enabled the HA-Primary CAM's **Heartbeat UDP Interface 2** function that sets up a redundant failover heartbeat via the CAM eth0 interface on the HA-Primary CAM, enable the **eth0** checkbox and specify the same peer IP address in the **[Primary] Heartbeat IP Address on eth0** field as on the HA-Primary CAM.

Step 12 (Optional) If you enabled the HA-Primary CAM's **Heartbeat UDP Interface 3** function on the HA-Primary CAM, select **eth2** or **eth3** from the dropdown menu and the same associated peer IP address in the **[Primary] Heartbeat IP Address on interface 3** field as on the HA-Primary CAM.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

Step 13 Specify the **Heartbeat Timeout** value for the HA secondary CAM to set the duration the CAM should wait before declaring that it has lost communication with its HA peer, thus assuming the role of the active CAM in the HA pair. The default **Heartbeat Timeout** value is 30 seconds.

Note Starting from Cisco NAC Appliance Release 4.6(1), the **Heartbeat Timeout** default value has been increased to 30 seconds to help accommodate CAM HA peers located in relatively distant locations on the network, where latency issues might cause a standby HA CAM to assume the active role when it has not received heartbeat packets from its HA peer within the specified **Heartbeat Timeout** period. In the resulting network scenario, you could potentially end up with two "active" CAMs performing Cisco NAC Appliance functions, requiring you to reboot both CAMs to re-establish the correct primary/secondary HA peer relationship.

Warning **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for Cisco NAC Appliance CAMs/CASs and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.**

Step 14 Click **Update** and then **Reboot**.

When the standby CAM starts up, it automatically synchronizes its database with the active CAM.

Step 15 Finally, open the admin console for the standby again and complete the configuration as follows. Notice that the admin console for the standby CAm displays limited management modules (Figure 4-7 and Figure 4-8).

Figure 4-7 Standby Web Admin Console Example—Summary Page

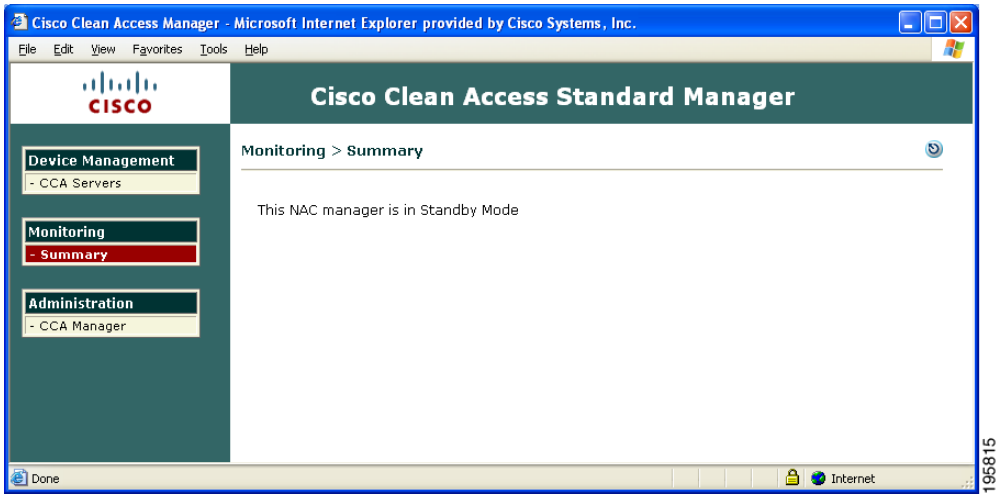
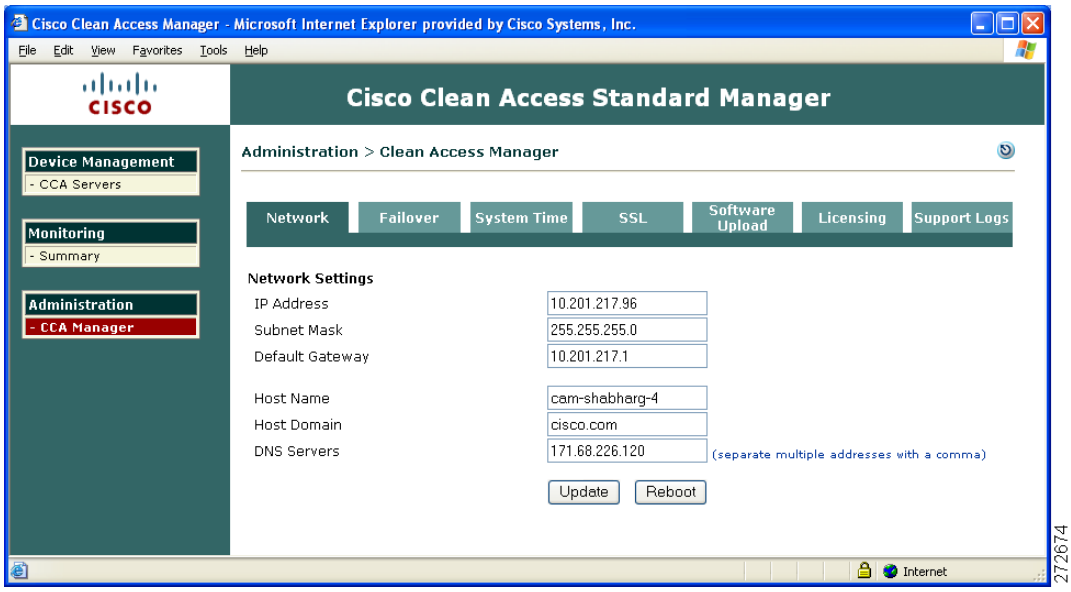


Figure 4-8 Standby Web Admin Console Example—CCA Manager > Network Page



Complete the Configuration

Verify settings in the **Failover** pages for both the active and standby CAMs. The high availability configuration is now complete.

Upgrading an Existing Failover Pair

For instructions on how to upgrade an existing failover pair to a new Cisco NAC Appliance release, see "Upgrading High Availability Pairs" in the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.

Failing Over an HA-CAM Pair

Warning **To prevent any possible data loss during database synchronization, always make sure the standby CAM is up and running before failing over the active CAM.**

To failover an HA-CAM pair, SSH to the active machine in the pair and perform one of the following commands:

- `shutdown`, or
- `reboot`, or
- `service perfigo stop`

This stops all services on the active machine. When heartbeat fails, the standby machine will assume the active role. Perform `service perfigo start` to restart services on the stopped machine. This should cause the stopped machine to assume the standby role.

Note `service perfigo restart` should not be used to test high availability (failover). Instead, Cisco recommends "shutdown" or "reboot" on the machine to test failover, or, the CLI commands `service perfigo stop` and `service perfigo start`. See Useful CLI Commands for HA, page 4-41.

Accessing High Availability Pair CAM Web Consoles

Determining Active and Standby CAM

Access the web console for each CAM in the HA pair by typing the IP address of each individual CAM (not the Service IP) in the URL/Address field of a web browser. You should have two browsers open. The web console for the Standby (inactive) CAM only displays a subset of the module menus and respective submenus available on the Active CAM.

Note The CAM configured as HA-Primary may not be the currently Active CAM.

Determining Primary and Secondary CAM

In each CAM web console, go to **Administration > CCA Manager > Failover**.

- The Primary CAM is the CAM you configured as the **HA-Primary** when you initially set up HA.
- The Secondary CAM is the CAM you configured as the **HA-Secondary** when you initially set up HA.

Note For releases prior to 4.0(0), the Secondary CAM is labeled as **HA-Standby** (CAM) for the initial HA configuration.

Installing a Clean Access Server High Availability Pair

This chapter describes how to set up two Clean Access Servers in high availability (HA) mode.By deploying Clean Access Servers in high-availability mode, you can ensure that important user authentication and connection tasks continue in the event of an unexpected shutdown. Topics include:

Note You must use identical appliances (e.g. NAC-3350 and NAC-3350) in order to configure High Availability (HA) pairs of Clean Access Managers (CAMs) or Clean Access Servers (CASs).

CAS High Availability Overview

Caution CAM-CAS communication and HA-CAM and/or HA-CAS peer communication can break down and adversely affect network functionality when SSL certificates expire. For more information, see the "HA Active-Active Situation Due to Expired SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.

Note Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

The following key points provide a high-level overview of HA-CAS operation:

- The Clean Access Server high-availability mode is an Active/Passive two-server configuration in which a standby CAS machine acts as a backup to an active CAS machine.
- The active CAS performs all tasks for the system. Since most of the CAS configuration is stored on the CAM, when CAS failover occurs, the CAM pushes the configuration to the newly-active CAS.

Note If you use the Authorization feature in a CAS HA-pair, follow the guidelines in "Backing Up and Restoring CAM/CAS Authorization Settings" in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* to ensure you are able to exactly duplicate your Authorization settings from one CAS to its high availability counterpart.

- Clean Access Managers and Clean Access Servers use a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to fail over to the HA peer CAM/CAS in HA deployments. (HA-Secondary CAMs/CASs are not able to assume the "active" role following a failover event when the master secret passwords are different.)
- The standby CAS does not forward any packets between its interfaces.
- The standby CAS monitors the health of the active CAS via heartbeat interface (serial and one or more UDP interfaces). Heartbeat packets can be sent on the dedicated eth2 interface, dedicated eth3 interface, or eth0/eth1 interface (if no eth2 or eth3 interface is available).
- The primary and secondary CAS machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
- In addition to heartbeat-based failover, the CAS also provides link-based failover based on eth0 or eth1 link failure. The CAS sends ICMP ping packets to an external IP address via the eth0 and/or eth1 interface. Failover will occur if only one CAS can ping the external addresses.

Note The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

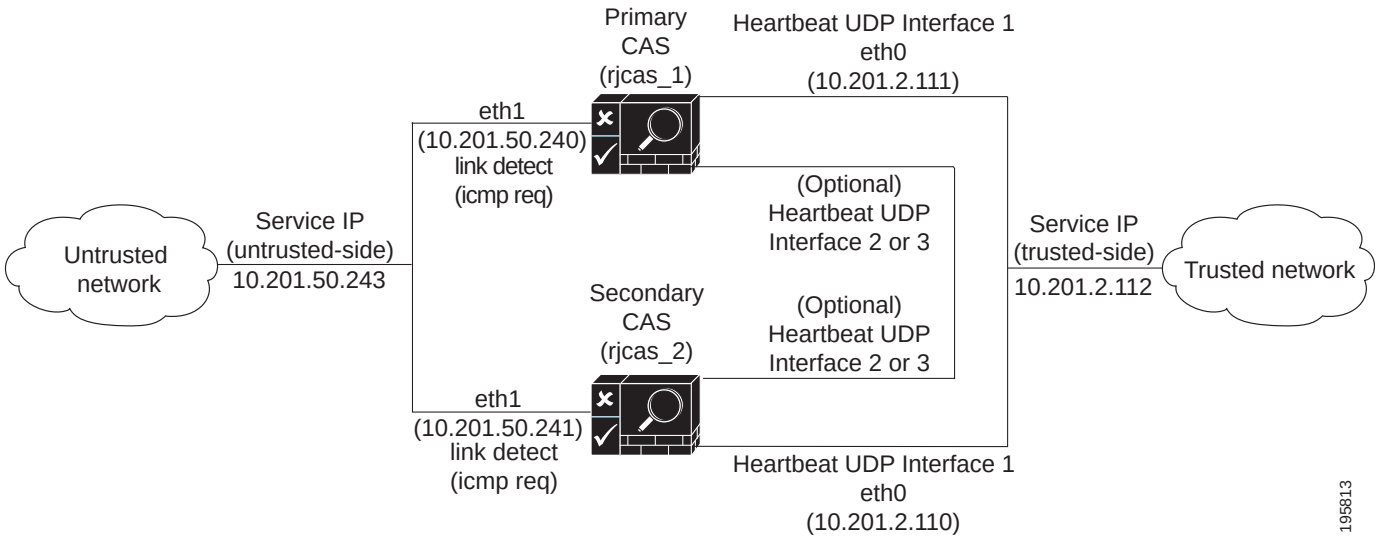
- Both Clean Access Servers share a virtual Service IP for the eth0 trusted interface and eth1 untrusted interface. The Service IP should be used for SSL certificates.
- Newer Cisco NAC-3310 CAMs/CASs feature a 160GB hard drive, while older NAC-3310s originally shipped with 80GB hard drives. Both of these hard drive sizes support High Availability (HA) deployments, and you can safely deploy a 160GB model in an HA pair with an 80GB model.
- To support FIPS 140-2 compliance, HA CAMs/CASs automatically establish an IPSec tunnel to ensure all communications between the HA Pair appliances remains secure across the network.
- Starting from release 4.5(1), when a standby CAS assumes the role of an active CAS that is performing DHCP address management and has gone into Fallback state, the new active CAS also assumes DHCP functions in addition to user login.

Caution The connection between HA pairs must be extremely reliable, with communication between HA pairs unimpeded. The best practice is to use a dedicated Ethernet cable. Breaking communication between HA pairs will result in two active nodes, which can have serious negative operational consequences. A key aspect of the link between HA pairs is the ability to restore that link should it go down; restoration may be fundamental to network stability, depending on your design.

Tip To avoid the HA pairs resulting in two active nodes, Cisco recommends to setup the eth2/eth3 interfaces on HA CASs for heartbeat.

Figure 4-9 illustrates the basic connections in an example HA-CAS configuration.

Figure 4-9 Clean Access Server Example High-Availability Configuration



Note "Primary/Secondary" denotes the server mode when it is configured for HA. "Active/Standby" denotes the runtime status of the server.

When first configuring the HA peers, you must specify an HA-Primary CAS and HA-Secondary CAS. Initially, the HA-Primary is the active CAS, and the HA-Secondary is the standby (passive) CAS. If a failover event occurs, such as the active CAS shuts down or stops responding to the peer's heartbeat signal, the standby assumes the role of the active CAS.

Note If *both* the HA-Primary and HA-Secondary CASs in your HA deployment lose their configuration, you can restore the system using the guidelines in the "Restoring Configuration from CAM Snapshot In HA Deployment" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1).*

When the CAS starts up again, it checks to see if its peer is active. If the peer is active, the starting CAS becomes the standby. If the peer is not active, then the starting CAS assumes the active role.

Typically, Clean Access Servers are configured as an HA pair at the same time, but you can add a new Clean Access Server to an existing standalone CAS to create a high-availability pair. In order for the pair to appear to the network and to the Clean Access Manager as one entity, you must specify a **Service IP Address** for the trusted interface (eth0) and a Service IP address for untrusted interface (eth1) of the pair.

Use the Service IP of the CASs to add the CAS to the CAM. Figure 4-10 shows how the active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair in the **List of Servers** in the CAM web console. In addition, either the trusted or untrusted interface Service IP address should be used to generate the SSL certificate.

Figure 4-10 Active CAS in an HA-Pair

Note If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA. After HA configuration is complete on both CASs, the Service IP is then entered in the **New Server** form to add the HA-CAS pair to the CAM.

Note To ensure heartbeat redundancy, Cisco recommends configuring optional Heartbeat UDP Interface 2 or 3 between the HA CASs in your deployment.

Failover Events

- If multiple heartbeat UDP interfaces are configured, then they must all fail for the standby system to take over. See Physical Connection, page 4-21 for additional details.
- If the CAS is unable to communicate with the CAM:
  - Users that are already connected will not be affected.
  - New users will not be able to log in.
- You can configure link-based failover. Two IP addresses that are external to the CAS are configured for Link-detect: one on the trusted network, the other on the untrusted network.
  - The active and standby CAS will send ICMP ping packets via eth0 to the IP address on the trusted network.
  - The active and standby CAS will send ICMP ping packets via eth1 to the IP address on the untrusted network.

Note If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the **/etc/ha.d/linkdetect.conf** file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See Link-Detect Interfaces, page 4-43 for more details.

The status of these ping packets is communicated between the CASs via the heartbeat signal:

- If the active and standby CAS can ping both external IPs, no failover occurs
- If the active and standby CAS cannot ping either of the external IPs, no failover occurs
- If the active CAS cannot ping either of the external IPs, but the standby CAS can ping them, failover occurs

- Both the Clean Access Manager and Clean Access Server are designed to automatically reboot in the event of a hard-drive failure, thus automatically initiating failover to the standby CAM/CAS.

Choosing External IPs for Link-Based Failover

- Keep in mind that when the CAS initiates traffic, it will always send packets out of its untrusted (eth1) interface except for packets destined to its default gateway. Therefore, when choosing an external IP on trusted network for CAS to ping via the eth0 interface, choose any IP belonging to a subnet other than the CAS subnet.
- When choosing an external IP on the untrusted network for CAS to ping via the eth1 interface:
  - This IP has to exist on the CAS management subnet
  - It cannot be the default gateway of the CAS
  - The CAS will send these ping packets out of the eth1 interface
  - Verify whether **Set Management VLAN ID** is enabled for the eth1 interface. If this option is not enabled, CAS will send traffic out untagged on the eth1 interface. The switch will determine whether these packets should be received on its native VLAN. Therefore, on the untrusted interface, ensure that the native VLAN is being forwarded.
  - The external IP address will be in the CAS management subnet, but on the untrusted side, the traffic will be going out from the CAS in the native VLAN; hence ensure the native VLAN is being forwarded towards the external IP device.

Refer to c. Configure HA-Primary Mode and Update, page 4-26 and c. Configure HA-Secondary Mode and Update, page 4-34 for additional configuration details.

CAS High Availability Requirements

This section describes addition planning considerations when implementing high availability.

Note In a CAS HA deployment using NAT on the trusted (eth0) side, you must ensure that the -Dperfigo.nat.serviceip=<*NAT'ed service IP or CAS service hostname*> property is set for the **starttomcat** and **restartweb** files on both the Primary and Secondary CAS.

For example, `-Dperfigo.nat.serviceip=172.10.20.100`.

Physical Connection

Cisco recommends using a **dedicated** connection for failover heartbeat on Clean Access Server high-availability pairs. You can use:

- A dedicated Ethernet NIC card, configured as the eth2 or eth3 interface of the CAS

  Note If a dedicated Ethernet interface (e.g. eth2 or eth3) is not available on the server machine, eth0 and eth1 are supported for the Heartbeat UDP interface. (This function does not apply, however, if you have deployed your CASs in Virtual Gateway mode *and* the eth0 and eth1 interfaces have the *same* IP address.) See Selecting and Configuring the Heartbeat UDP Interface, page 4-24.

  If additional network interfaces (e.g. eth2 or eth3) are available, you can use them for UDP heartbeat instead of eth0. In this case, the eth2 or eth3 interfaces on the two machines are connected using a crossover cable. If installing an additional Ethernet interface, configure the IP address for the interface. For instructions, see Configuring Additional NIC Cards, page 3-37.

Switch Interfaces for OOB Deployment

For Out-of-Band deployments, ensure that Port Security is not enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

Service IP Addresses

In addition to the IP addresses for the trusted and untrusted interfaces for each individual CAS, you will need to provide two Service IP addresses for the trusted and untrusted interfaces of the CAS pair (see Figure 4-9 on page 4-19 for an example configuration). A **Service IP address** is the common IP address that the external network uses to address the pair.

In addition, either the trusted or untrusted interface Service IP address should be used to generate the SSL certificate. If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA.

After HA configuration is complete on both CASs, use the Service IP in the **New Server** form to add the HA-CAS pair to the CAM. Note that the HA-CAS pair is automatically added as the same Server Type (for example, Out-of-Band Virtual Gateway).

Host Names

For heartbeat, each CAS needs to have a unique hostname (or node name). For HA CAS pairs, this host name will be provided to the peer, and must be resolved via DNS or added to the peer's /etc/hosts file.

DHCP Synchronization

When you configure two CASs that also perform DHCP functions for your deployment as an HA pair, Cisco NAC Appliance automatically synchronizes and exchanges the required keys between the HA-Primary and HA-Secondary CASs to ensure DHCP continues to work properly following a failover event.

SSL Certificates

As in standalone mode, in HA mode the Clean Access Servers can use either a temporary, self-signed certificate or a CA (Certificate Authority)-signed certificate. A temporary certificate is useful for testing or development. A production deployment should have a CA-signed certificate. Considerations in either case are:

1. Both the temporary or CA-signed certificates can use either the Service IP address (for either the trusted interface or untrusted interface) or a domain name as the certificate domain name.
2. If creating a certificate using a domain name, then the domain name must map to the Service IP in DNS. If you are not using a domain name in the certificate, then the DNS mapping is not necessary.
3. For a temporary certificate, generate the temporary certificate on one of the Clean Access Servers, and transfer it from that CAS to the other CAS.
4. For a CA-signed certificate, you will need to import the CA-signed certificate into each of the Clean Access Servers in the pair.

Note The CA-signed certificate must be either based on the Service IP or a hostname/domain name resolvable to the Service IP through DNS.

Note The Clean Access Server retrieves session information from the CAM during failover. For example, if user A is logged into the system in role B, when failover occurs, user A will still be logged in and have access specified by role B.

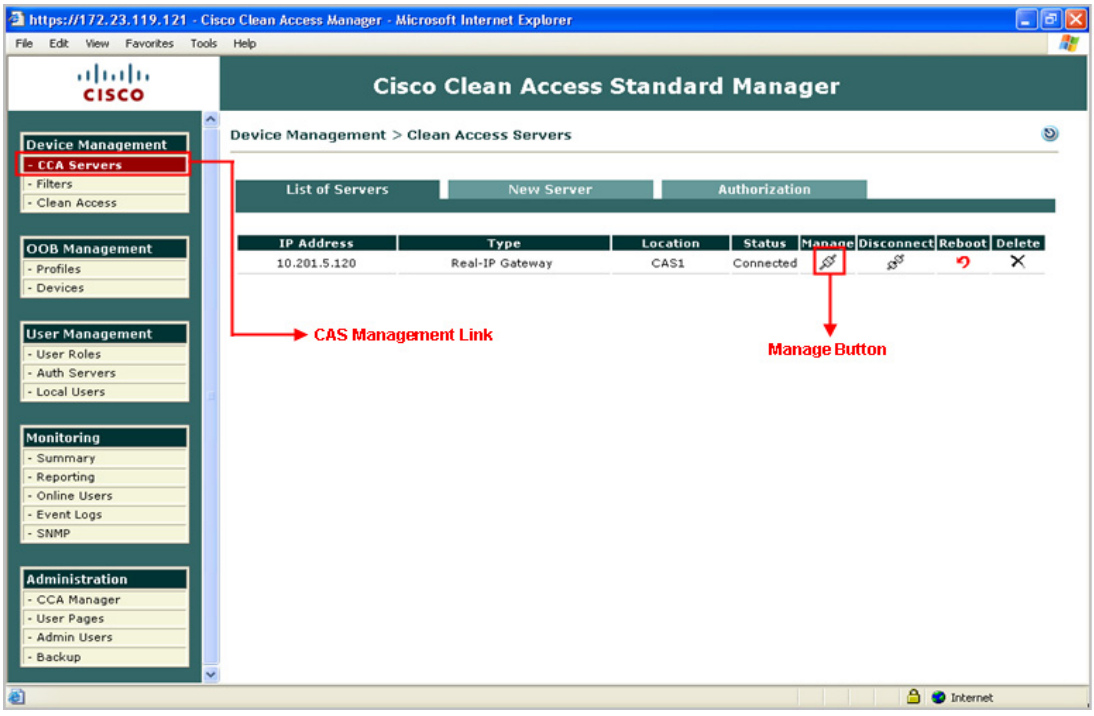
If the CAS is the DHCP server and failover occurs, user A also retains his/her assigned IP address because to HA CASs *do* directly exchange DHCP failover information.

Note For HA CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the HA-Secondary CAS unit through its direct access web console. These settings include updating the SSL certificate, system time, time zone, DNS, or Service IP. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* and Modifying CAS High Availability Settings, page 4-40 for details.

Before Starting

1. Before starting, make sure that both Clean Access Servers are installed and accessible over the network. See Perform the Initial CAS Configuration, page 3-24.
2. The two Clean Access Servers in the HA pair must remain Layer 2 adjacent to support heartbeat and sync functions.
3. If the Clean Access Servers have already been added to the management domain of a CAM, they should be removed. Use the **Delete** button in the **List of Servers** tab to remove the CASs.

Figure 4-11 List of Servers



Note Cisco NAC Appliance web consoles support Internet Explorer 6.0 and 7.0 browsers.

Selecting and Configuring the Heartbeat UDP Interface

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

The Heartbeat UDP interface, if specified, is used to send UDP heartbeat traffic related to high availability. The interface used depends on the interfaces available on the server machine and the load level expected. This interface can use either a dedicated Ethernet interface (such as eth2 or eth3) or the trusted interface eth0, if a dedicated interface is not available.

When using an additional Ethernet interface, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see Configuring Additional NIC Cards, page 3-37. When a dedicated interface is used, the dedicated interfaces on both machines should be connected using a crossover cable.

Servers running a CAS typically use both available interfaces (eth0 and eth1), with eth0 configured as the trusted network interface. Cisco recommends using the eth2 and eth3 interfaces for heartbeat redundancy, thus freeing up the eth0 and eth1 interfaces to handle Cisco NAC Appliance traffic.

Note If using eth0 as the UDP heartbeat interface, make sure that the management interfaces on the CAS are in their own VLAN, not on a VLAN with other user traffic. This is a general best practice that allows you to segment and protect management traffic when running the failover heartbeat over the same physical interface.

Serial Port High-Availability Connection

If each machine running the CAS software has two serial ports, use one of the ports for the serial cable connection.

By default, the first serial connector detected on the server is configured for console input/output (to facilitate installation and other types of administrative access).

Warning **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for Cisco NAC Appliance CAMs/CASs and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.**

When high-availability mode is selected, the serial console login (ttyS0) is automatically disabled to free the serial port for HA mode. To re-enable ttyS0 as the console login, deselect the **Disable Serial Login** checkbox on the **Failover > General** tab after clicking **Update** and before clicking **Reboot**. For details, see steps c. Configure HA-Primary Mode and Update, page 4-26 and c. Configure HA-Secondary Mode and Update, page 4-34.

Configure High Availability

Note Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

The following sections describe how to set up high availability in four general procedures:

- Step 1: Configure the HA-Primary Clean Access Server, page 4-25
- Step 2: Configure the HA-Secondary Clean Access Server, page 4-33
- Step 3: Connect the Clean Access Servers and Complete the Configuration, page 4-38
- Step 4: Failing Over an HA-CAS Pair, page 4-39

Note "Primary/Secondary" denotes the server mode when it is configured for HA.
"Active/Standby" denotes the runtime status of the server.

Configure the HA-Primary Clean Access Server

The general sequence to configure the HA-Primary CAS is as follows:

a. Access the HA-Primary CAS Directly, page 4-25

b. Configure the Host Information for the HA-Primary CAS, page 4-26

c. Configure HA-Primary Mode and Update, page 4-26

d. Configure the SSL Certificate, page 4-31

e. Reboot the HA-Primary CAS, page 4-33

f. Add the CAS to the CAM Using the Service IP, page 4-33

When done, continue to Configure the HA-Secondary Clean Access Server, page 4-33.

a. Access the HA-Primary CAS Directly

Each Clean Access Server has its own web admin console that allows configuration of certain limited Administration settings directly on the CAS. The CAS direct access web console must be used to configure CAS pairs for HA.

To access the HA-Primary Clean Access Server's direct access web admin console:

1. Open a web browser and type the IP address of the trusted (eth0) interface of the CAS in the URL/address field, as follows: **https://<primary_CAS_eth0_IP_address>/admin** (for example, `https://172.16.1.2/admin`).
2. Accept the temporary certificate and log in as user `admin` with the web console password specified during initial configuration.

Note

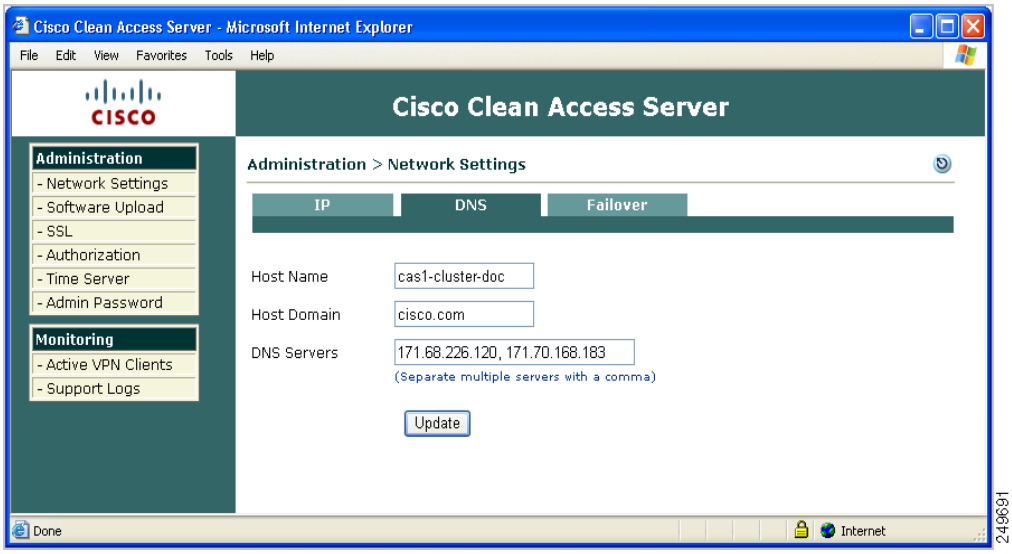
- In order to copy and paste values to/from configuration forms, Cisco recommends keeping both web consoles open for each CAS (primary and secondary). See also a. Access the HA-Secondary CAS Directly, page 4-33.
- To ensure security, Cisco recommends changing the default password of the CAS.

b. Configure the Host Information for the HA-Primary CAS

3. Click the **Network Settings** link, then the **DNS** tab.
4. In the **Host Name** field, type the host name for the HA-Primary CAS. Make sure there is a domain in the **Host Domain** field, such as cisco.com. If necessary, add one and click **Update**.

Note When configuring HA, it is mandatory to specify a Host Name for each machine in the HA-pair. The Host Name is case-sensitive and cannot be an IP address. Host Names are needed later for the **Local Host Name** and **Peer Host Name** fields of the HA Primary and HA Secondary configuration. The **Local Host Name** and **Peer Host Name** do not need to be resolvable via DNS; however, they are case-sensitive and need to match the Host Names you have specified for the machines.

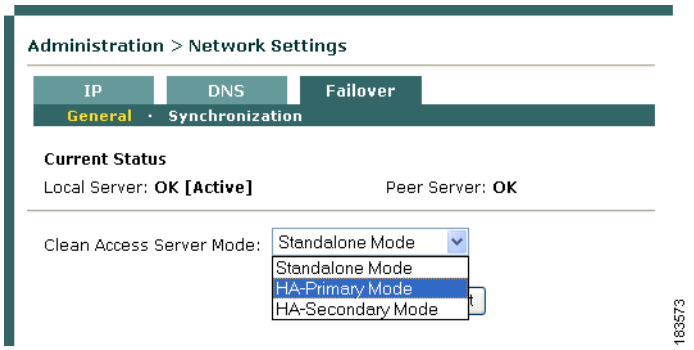
Figure 4-12 DNS Tab



c. Configure HA-Primary Mode and Update

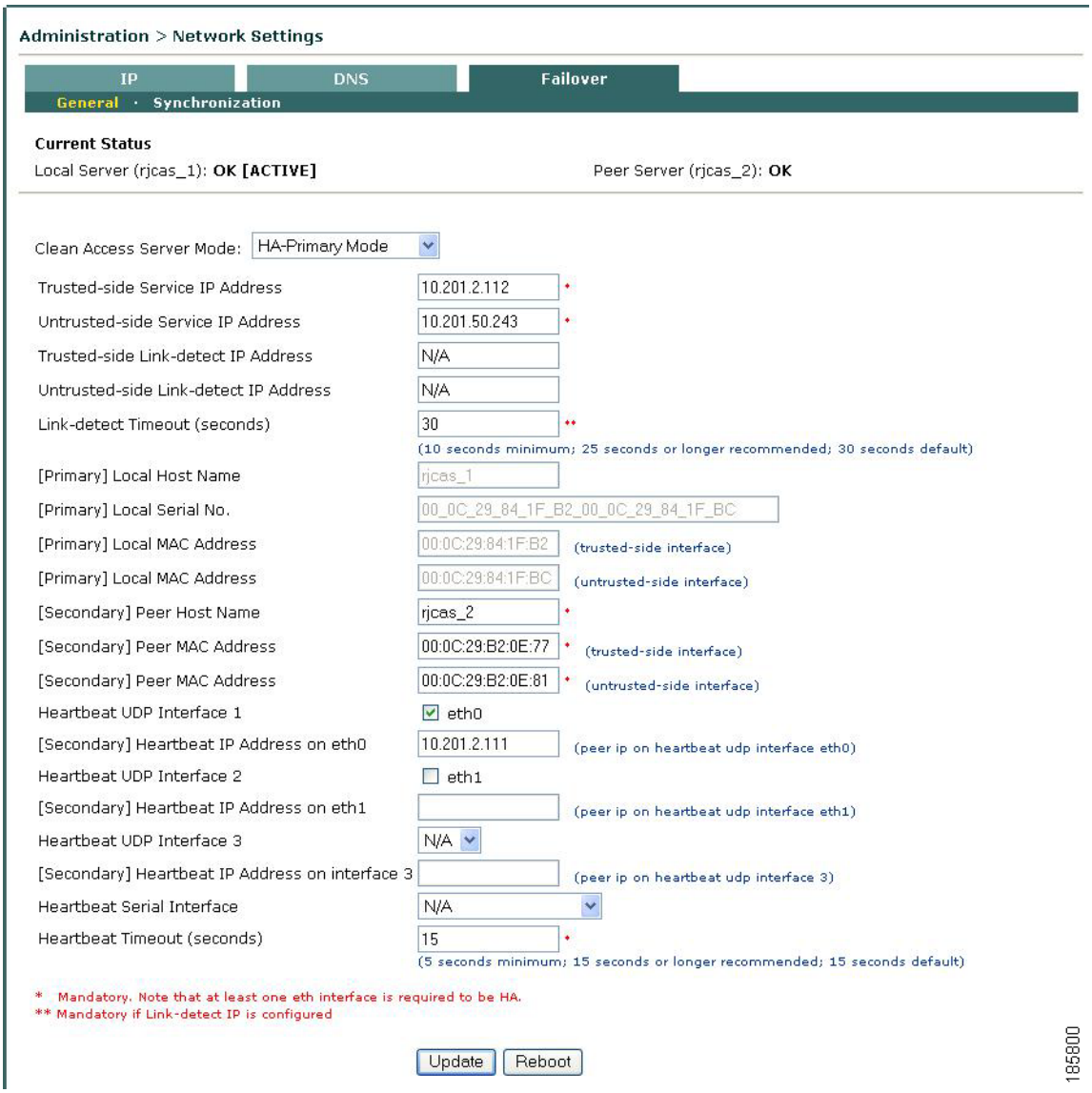
5. Click the **Failover > General** tab and choose **HA-Primary Mode** from the **Clean Access Server Mode** dropdown menu.

Figure 4-13 Failover —Choose Mode



6. In the **HA-Primary Mode** form that opens, type values for the following fields.

Figure 4-14 Failover —HA-Primary Mode



  - **Trusted-side Service IP Address**: The common IP address by which the pair is addressed from the trusted network (10.201.2.112 in the example in Figure 4-9 on page 4-19).
  - **Untrusted-side Service IP Address**: The common address for the pair on the untrusted (managed) network (10.201.50.243 in the sample).

- **Trusted-side Link-detect IP Address**: When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS attempts to ping this external address. Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.
- **Untrusted-side Link-detect IP Address**: When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this external address. You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.

Note If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the **/etc/ha.d/linkdetect.conf** file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See Link-Detect Interfaces, page 4-43 for more details.

- **Link-detect Timeout (seconds)**: This configures the length of time the CAS attempts to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Cisco recommends entering a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.

Note In addition to UDP Interface configuration, you can optionally configure the CAS to respond to link failures on the trusted and/or untrusted sides as failover events. The CAS attempts to ping the trusted and/or untrusted link-detect addresses specified, then counts the number of nodes it can reach:

0-for no addresses

1-for either trusted/untrusted

2-for both trusted/untrusted

If the Standby CAS can reach more nodes than the Active CAS, the Standby CAS will take over and become the Active CAS. If both CASs can ping the same number of addresses (all addresses or only one address), no failover event occurs, since neither CAS has the advantage. To enable link-detect, enter at least one link-detect IP address on each CAS and a link-detect timeout. See also Choosing External IPs for Link-Based Failover, page 4-21 for further details.

Note The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

The CAS performs Heartbeat connection and (optionally) Link-detect according to the same interval, approximately every 1-2 seconds.

- **[Primary] Local Host Name**: This is filled in by default for the HA-Primary CAS, as configured under **Administration > Network Settings > DNS | Host Name** ("rjcas_1" in Figure 4-12).
- **[Primary] Local Serial No**: Filled in by default for the HA-Primary CAS. The local serial number identifies this CAS to the Clean Access Manager (and is composed of eth0/eth1 MAC addresses). In an HA-CAS pair, the serial number of the Primary CAS is the key used to associate all the configuration information specific to this CAS in the CAM database.
- **[Primary] Local MAC Address (trusted-side interface)**: Filled in by default; the MAC address of the eth0 interface for the HA-Primary CAS.

- **[Primary] Local MAC Address (untrusted-side interface)**: Filled in by default; the MAC address of the eth1 interface for the HA-Primary CAS.

Note

- You may want to copy and paste the **[Primary] Local Host Name**, **[Primary] Local Serial No**, and **[Primary] Local MAC Address (trusted/untrusted)** values into a text file. These values are necessary later when configuring the HA-Secondary CAS.
- To enter the HA-Secondary CAS information into the form for the HA-Primary CAS, copy and paste the corresponding fields from the HA-Secondary CAS web console.

- **[Secondary] Peer Host Name**: Type the host name for the HA-Secondary CAS peer ("rjcas_2" in this example). The Secondary Peer Host Name is case-sensitive and must exactly match the **Host Name** specified in the peer machine **DNS** tab (under **Administration > Network Settings > DNS | Host Name**).
- **[Secondary] Peer MAC Address (trusted-side interface)**: This is the peer MAC address from the trusted (eth0) side of the HA-Secondary CAS.
- **[Secondary] Peer MAC Address (untrusted-side interface)**: This is the peer MAC address from the untrusted (eth1) side of the HA-Secondary CAS.
- **Heartbeat UDP Interface 1**: This setting specifies eth0 as a failover IP interface on the CAS. If a dedicated Ethernet connection is not available,
- **[Secondary] Heartbeat IP Address on eth0**: The IP address of the trusted interface (eth0) of the HA-Secondary CAS.
- **Heartbeat UDP Interface 2**: This setting specifies eth1 as a failover IP interface on the CAS. If you configure your CAS HA system to use eth0 as the primary failover heartbeat connection, you can also use the eth1 interface as a redundant heartbeat monitor.
- **[Secondary] Heartbeat IP Address on eth1**: The IP address of the untrusted interface (eth1) of the HA-Secondary CAS.
- **Heartbeat UDP Interface 3**: Options are N/A, eth2, or eth3. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 or another Ethernet interface for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.

Note Before you can specify either the eth2 or eth3 interfaces to be **Heartbeat UDP Interface 3**, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see Configuring Additional NIC Cards, page 3-37.

- **[Secondary] Heartbeat IP Address on Interface 3**: The IP address of the tertiary failover heartbeat link configured on the HA-Secondary CAS.

Note You must configure at least one of the additional Ethernet interfaces on the HA-Primary CAS to connect to a peer interface on the Secondary CAS in order to support HA behavior. In an HA scenario, The Ethernet interface you configure serves as the medium for data sync between the Primary and Secondary CAS.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

- **Heartbeat Timeout (seconds)**: Choose a value greater than 15 seconds.

  Note To avoid a potentially serious network issue where two CASs deployed as an HA pair reboot at the same time (in the event power returning after an outage, for example) and *both* come up as the active CAS in the HA pair, Cisco recommends setting the **Heartbeat Timeout** to a value greater than 30 seconds. The possible network implication in this scenario is that the to "active" CASs can introduce a Layer 2 broadcast loop that almost immediately brings down the network.

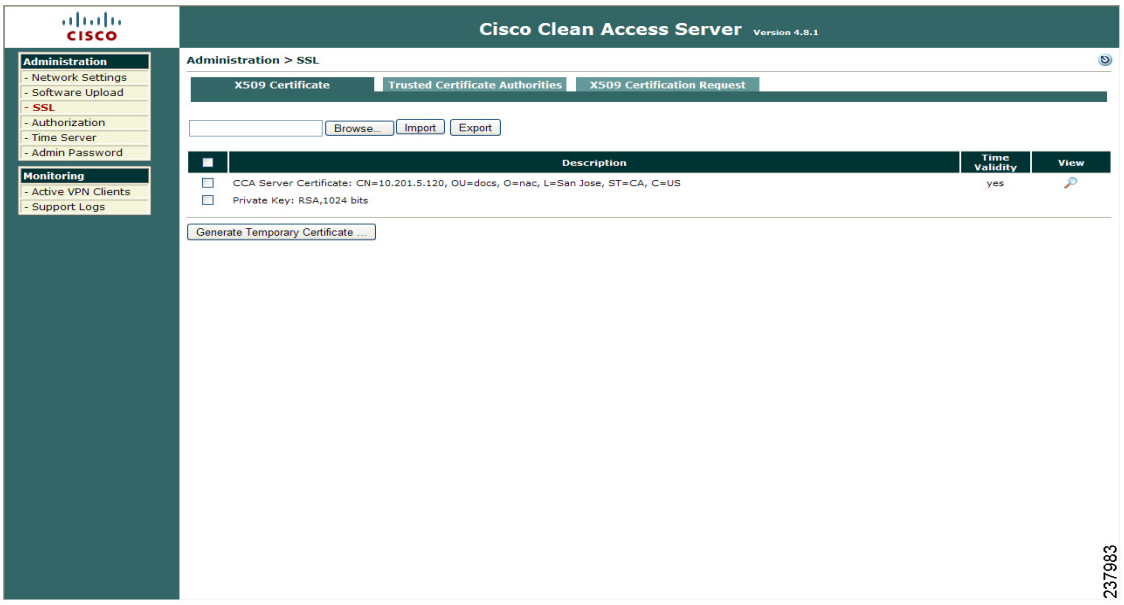
  Another method you can use to avoid this scenario is to ensure you use an additional Ethernet interface link (eth2, eth3) for heartbeat monitoring between your CAS Ha pair nodes. See **Heartbeat UDP Interface 2** and **Heartbeat UDP interface 3**, above and Configuring Additional NIC Cards, page 3-37, for more information.

- **Update**: Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot**: This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Primary CAS. Navigate to **Administration > SSL > X509 Certificate**.

Figure 4-15 Administration > SSL > X509 Certificate



8. Perform one of the following procedures, depending on whether you intend to use a temporary, self-signed certificate or a CA-signed certificate:

If using a temporary certificate for the HA pair:

a. Click **Generate Temporary Certificate**, enter information for all of the fields in the form, and click **Generate**. The certificate must be associated with the Service IP addresses of the HA pair.

b. When finished generating the temporary certificate, click the checkboxes for the certificate and Private Key to highlight them in the table.

c. Click **Export** to save the certificate and Private Key to your local machine. You must import the certificate and Private Key later when configuring the HA-Secondary CAS.

If using a CA-signed certificate for the HA pair:

Note This process assumes you have already generated a Certificate Signing Request and accompanying Private Key, submitted the request to your Certificate Authority, and have received your CA-signed certificate. If you have not yet obtained a CA-signed certificate for the CAS, be sure to follow the instructions in the "Manage CAS SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.

a. Click **Browse** and navigate to the directory on your local machine containing the CA-signed certificate and Private Key.

b. Click **Import**. Note that you will need to import the same certificate later to the HA-Secondary CAS.

Note The CA-signed certificate must either be based on the Service IP or a host name/domain name resolvable to the Service IP through DNS.

e. Reboot the HA-Primary CAS

9. **Reboot** the Clean Access Server from either the CAS direct access interface (**Network Settings** > **Failover** > **General** > **Reboot** button) or from the CAM web console (**Administration** > **CCA Manager** > **Network** > **Reboot** button).

f. Add the CAS to the CAM Using the Service IP

10. In the CAM web console, go to **Device Management** > **CCA Servers** > **New Server**, and add the CAS to the CAM using the Service IP for the pair (10.201.2.112) as the **Server IP** address.
11. Configure any other settings desired, such as DHCP settings, to control the runtime behavior of the CAS.
12. Test the configuration by trying to log into the untrusted (managed) network from a computer connected to the untrusted interface of the Clean Access Server. Proceed to the next step only if you can successfully access the network.

Configure the HA-Secondary Clean Access Server

Note Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

The general sequence to configure the HA-Secondary CAS is as follows:

a. Access the HA-Secondary CAS Directly

b. Configure the Host Information for the HA-Secondary CAS

c. Configure HA-Secondary Mode and Update

d. Configure the SSL Certificate

e. Reboot the HA-Secondary CAS

a. Access the HA-Secondary CAS Directly

1. Access the web console for the HA-Secondary CAS by opening a web browser and typing the IP address of the trusted (eth0) interface of the HA-Secondary CAS in the URL/address field, as follows: **https://<standby_CAS_eth0_IP_address>/admin** (for example, `https://172.16.1.3/admin`)
2. Log in as user `admin` and provide the correct password.

Note

- In order to copy and paste values to/from configuration forms, Cisco recommends keeping both web consoles open for each CAS (primary and secondary). See also a. Access the HA-Primary CAS Directly, page 4-25.
- To ensure security, Cisco recommends changing the default password of the CAS.

b. Configure the Host Information for the HA-Secondary CAS

3. In the **Network Settings** page, open the **DNS** tab.

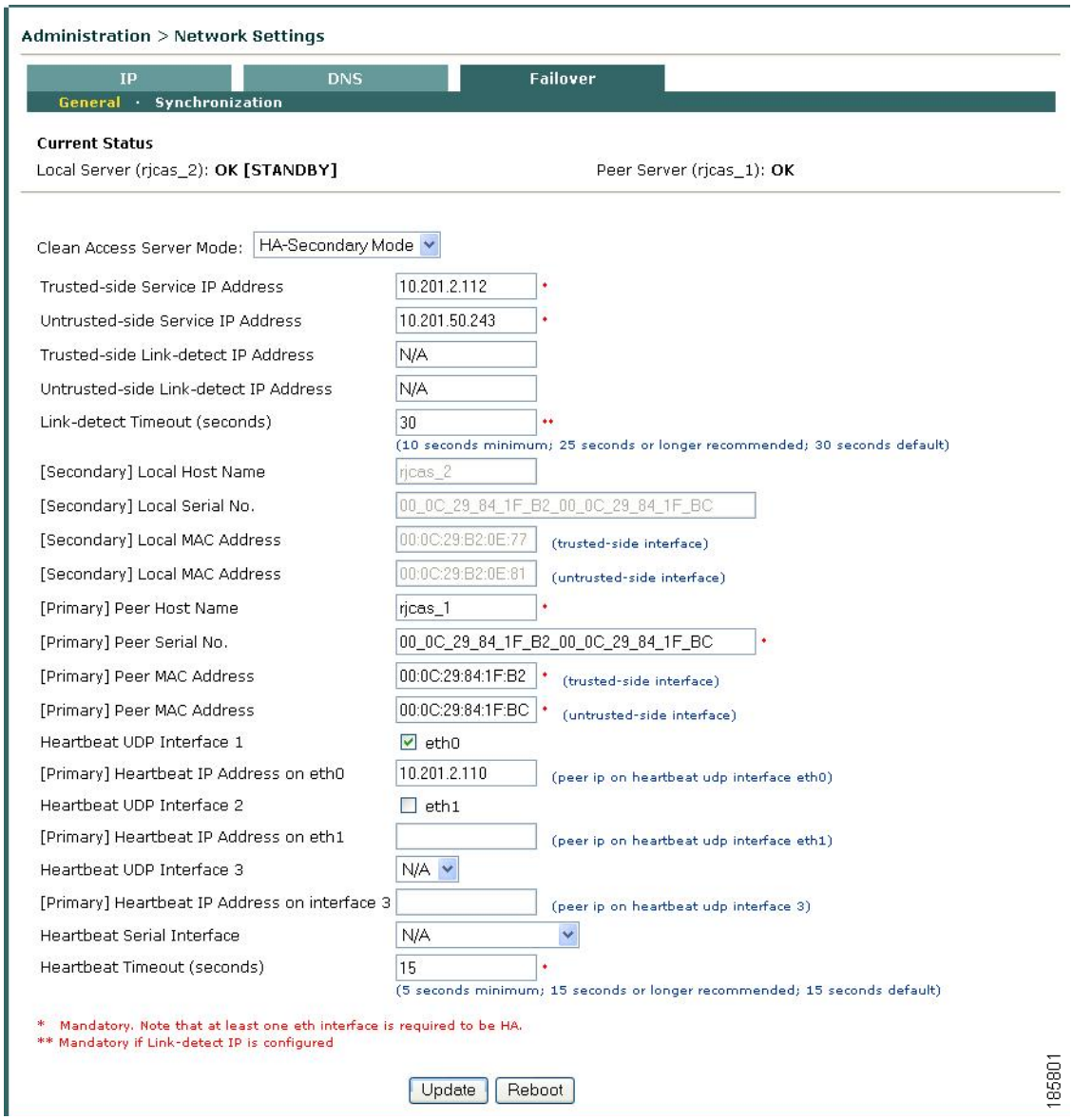
4. Make sure the host name is a unique host name for the HA-Secondary CAS, such as “rjcas_2.” You must have the same domain name specified in this tab as you did for the HA-Primary CAS (see b. Configure the Host Information for the HA-Primary CAS, page 4-26).

Note When configuring HA, it is mandatory to specify a Host Name for each machine in the HA-pair. The Host Name is case-sensitive and cannot be an IP address. Host Names are needed later for the **Local Host Name** and **Peer Host Name** fields of the HA Primary and HA Secondary configuration. The **Local Host Name** and **Peer Host Name** do not need to be resolvable via DNS; however, they are case-sensitive and need to match the Host Names you have specified for the machines.

c. Configure HA-Secondary Mode and Update

5. Click the **Failover** > **General** tab and select **HA-Secondary Mode** from the **Clean Access Server Mode** dropdown menu.

Figure 4-16 Failover —HA-Secondary Mode



6. In the HA-Secondary form, complete the following fields:
   - **Trusted-side Service IP Address**: The IP address by which the pair is addressed from the *trusted* network. Use the same value as for the primary CAS (10.201.2.112 in the example in Figure 4-9 on page 4-19).
   - **Untrusted-side Service IP Address**: The IP address by which the pair is addressed from the *untrusted* (managed) network. Use the same value as for the primary CAS (10.201.50.243 in the example).

- **Trusted-side Link-detect IP Address (Optional)**: When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS will attempt to ping this address. Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.

- **Untrusted-side Link-detect IP Address (Optional)**: When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this address. You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.

Note If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the **/etc/ha.d/linkdetect.conf** file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See Link-Detect Interfaces, page 4-43 for more details.

- **Link-detect Timeout (seconds) (Optional)**: This configures the length of time the CAS will attempt to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Enter a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.

Note The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

See Choosing External IPs for Link-Based Failover, page 4-21 for additional details.

- **[Secondary] Local Host Name**: This is filled in by default for the HA-Secondary CAS, as configured under **Administration > Network Settings > DNS | Host Name** ("rjcas_2" in this example).
- **[Secondary] Local Serial No**: Filled in by default for the HA-Secondary CAS.
- **[Secondary] Local MAC Address (trusted-side interface)**: Filled in by default; the MAC address of the eth0 interface for the HA-Secondary CAS.
- **[Secondary] Local MAC Address (untrusted-side interface)**: Filled in by default; the MAC address of the eth1 interface for the HA-Secondary CAS.

Note

- You may want to copy and paste the **[Secondary] Local Host Name**, **[Secondary] Local Serial No**. and **[Secondary] Local MAC Address (trusted/untrusted)** values into a text file. These values are needed to configure the HA-Primary CAS.
- To enter the HA-Primary CAS information into the form for the HA-Secondary CAS, copy and paste the corresponding fields from the web console of the HA-Primary CAS.

- **[Primary] Peer Host Name**: Type the host name of the HA-Primary CAS ("rjcas_1" in Figure 4-12). The **[Primary] Peer Host Name** is case-sensitive and must exactly match the Host Name specified in the peer machine **DNS** tab (under **Administration > Network Settings > DNS | Host Name**).
- **[Primary] Peer Serial No**: The serial number of the HA-Primary CAS. When the HA-Secondary CAS becomes Active, it must use the serial number of the HA-Primary CAS to identify itself to the CAM in order to access the CAS configuration information.

- **[Primary] Peer MAC Address (trusted-side interface)**: The peer MAC address from the trusted side (eth0) of the HA-Primary CAS.
- **[Primary] Peer MAC Address (untrusted-side interface)**: The peer MAC address from the untrusted side (eth1) of the HA-Primary CAS.
- **Heartbeat UDP Interface 1**: This setting specifies eth0 as a failover IP interface on the CAS. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.
- **[Primary] Heartbeat IP Address on eth0**: The IP address of the trusted interface (eth0) of the HA-Primary CAS.
- **Heartbeat UDP Interface 2**: This setting specifies eth1 as a failover IP interface on the CAS. If you configure your CAS HA system to use eth0 as the primary failover heartbeat connection, you can also use the eth1 interface as a redundant heartbeat monitor.
- **[Primary] Heartbeat IP Address on eth1**: The IP address of the untrusted interface (eth1) of the HA-Primary CAS.
- **Heartbeat UDP Interface 3**: Options are N/A, eth2, or eth3. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 or another Ethernet interface for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.

Note Before you can specify either the eth2 or eth3 interfaces to be **Heartbeat UDP Interface 3**, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see Configuring Additional NIC Cards, page 3-37.

- **[Primary] Heartbeat IP Address on Interface 3**: The IP address of the tertiary failover heartbeat link configured on the HA-Primary CAS.

Note You must configure at least one of the additional Ethernet interfaces on the HA-Primary CAS to connect to a peer interface on the Secondary CAS in order to support HA behavior. In an HA scenario, The Ethernet interface you configure serves as the medium for data sync between the Primary and Secondary CAS.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

- **Heartbeat Timeout (seconds)**: Choose a value greater than 15 seconds.

Note To avoid a potentially serious network issue where two CASs deployed as an HA pair reboot at the same time (in the event power returning after an outage, for example) and *both* come up as the active CAS in the HA pair, Cisco recommends setting the **Heartbeat Timeout** to a value greater than 30 seconds. The possible network implication in this scenario is that the to "active" CASs can introduce a Layer 2 broadcast loop that almost immediately brings down the network.

Another method you can use to avoid this scenario is to ensure you use an additional Ethernet interface link (eth2, eth3) for heartbeat monitoring between your CAS Ha pair nodes. See **Heartbeat UDP Interface 2** and **Heartbeat UDP interface 3**, above and Configuring Additional NIC Cards, page 3-37, for more information.

- **Update**: Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot**: This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Secondary CAS. Navigate to **Administration > SSL > X509 Certificate** and perform one of the following procedures:

If using a temporary certificate for the HA pair:

a. Click **Browse** and navigate to the location on your local machine where you have saved the temporary certificate and Private Key you previously exported from the HA-Primary CAS.

b. Select the certificate file and click **Import**.

c. Repeat the process to import the Private Key.

If using a CA-signed certificate for the HA pair:

a. Click **Browse** and navigate to the location on your local machine where you have saved the CA-signed certificate you received from your Certificate Authority and the associated Private Key you exported from the HA-Primary CAS and saved to your local machine.

b. Select the CA-signed certificate file and click **Import**.

c. Repeat the process to import the Private Key.

For more information, see the "Manage CAS SSL Certificates" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)*.

e. Reboot the HA-Secondary CAS

8. From the CAS direct access interface (**Network Settings > Failover > General**), click the **Reboot** button to reboot the Clean Access Server.

Connect the Clean Access Servers and Complete the Configuration

1. Shut down the HA-Primary CAS machine and connect the `rjcas_1` and `rjcas_2` machines using a serial null modem cable (connecting available serial ports) and/or a crossover cable (connecting Ethernet ports if using a pair of Ethernet interfaces such as eth2 or eth3 for failover).

2. Open the Clean Access Manager administration console.
3. Go to **Device Management > CCA Servers > List of Servers**. The Active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in Figure 4-17. Since the HA-Primary CAS is turned off, the IP address of the HA-Secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.

Figure 4-17 Active CAS in an HA-Pair

4. Click the **Manage** button for the pair. The management pages of the HA-Secondary CAS (now the Active CAS) should appear.
5. From a client computer connected to the Clean Access Server's untrusted interface, test the configuration by trying to log on to the untrusted (managed) network as an authorized user. If successful, remain logged on and proceed to the next step.

Failing Over an HA-CAS Pair

To test your HA system, use the following steps:

1. Turn on the HA-Primary CAS machine. Make sure that the CAS is fully started and functioning before proceeding.
2. From the client computer, log off the user's session and try to log onto the untrusted (managed) network again as the user.
3. The HA-Secondary CAS should still be active and providing services for the user.
4. Shut down the HA-Secondary CAS machine.

Note Cisco recommends "shutdown" or "reboot" on the machine to test failover, or, if a CLI command is preferred, `service perfigo stop` and `service perfigo start`. For a Virtual Gateway CAS, use `service perfigo maintenance` instead to bring the CAS to maintenance mode and allow network connectivity to the management VLAN. See Useful CLI Commands for HA, page 4-41 for details.

5. After about 15 seconds, you should be able to continue browsing, with the HA-Primary CAS becoming the Active server and providing the service.
6. Turn on the HA-Secondary CAS machine (the standby server).
7. Check the event log on the Clean Access Manager. It should correctly indicate the status of the Clean Access Servers (e.g., "`rjcas_1 is dead. rjcas_2 is up`").
8. Testing of the high availability configuration is now complete.

Modifying CAS High Availability Settings

The following instructions describe how to change settings for an existing high-availability Clean Access Server pair. Changing the Service IP, the subnet mask, or the default gateway for a high-availability pair requires updating the Clean Access Manager and rebooting the Clean Access Server.

Additionally, if the Service IP address is changed and the SSL certificate for the Clean Access Server is based on the Service IP, a new certificate must be generated and imported to each Clean Access Server in the high-availability pair. If the SSL certificate is based on the host name of the Clean Access Server, generating a new certificate is not necessary. However, make sure to change the IP address for that host name in your DNS server.

The general sequence of steps is as follows:

1. Update the Clean Access Server settings in the Clean Access Manager first (but do not reboot).
2. Update the HA settings in the direct access web console for the primary CAS and reboot the primary CAS.
3. While the primary CAS reboots, wait for the secondary CAS to become active in the CAM's List of Servers.
4. Repeat steps 1-3 for the secondary CAS and reboot the secondary CAS.
5. While the secondary CAS reboots, the primary CAS becomes active in the Clean Access Manager and displays the new settings.

To Change IP Settings for an HA-CAS

1. From the CAM web admin console, go to **Device Management** > **CCA Servers**.
2. Click the **Manage** button for the Clean Access Server.
3. Click the **Network** tab.
4. Change the **IP Address**, **Subnet Mask**, or **Default Gateway** settings for the trusted/untrusted interfaces as desired.
5. Click the **Update** button only.

Caution Do not click the **Reboot** button at this stage.

6. If the SSL certificate for the CAS was based on the previous IP address, you will need to generate a new SSL certificate based on the new IP address configured. This can be done under **Administration** > **SSL** > **X509 Certificate**. See the "Manage CAS SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* for details.
7. If the SSL certificate was based on the host name of your Clean Access Server, you do not need to generate a new certificate. However, make sure to change the IP address for that host name in your DNS server.
8. Next, open the direct access web admin console for the **primary** Clean Access Server as follows:

   `https://<primary_CAS_eth0_IP_address>/admin`

9. The IP form for the primary CAS will reflect the changes you made in the CAM web console under **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Network** > **IP**.
10. In Clean Access Server direct access console, click the **Network** > **Failover**> **General** tab.

11. Change the following as needed:
    - Trusted-side Service IP Address
    - Untrusted-side Service IP Address
    - [Secondary] Peer Host Name
    - [Secondary] Peer MAC Address (trusted-side interface)
    - [Secondary] Peer MAC Address (untrusted-side interface)
    - [Secondary] Heartbeat IP Address
12. Click the **Update** button, then the **Reboot** button.
13. From the Clean Access Manager administrator web console, go to **Device Management** > **CCA Servers** and wait for the secondary Clean Access Server to become active. (Note that this can take a few minutes.) The active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in Figure 4-9 on page 4-19. The IP address of the secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.
14. Once the IP address of the secondary CAS appears in brackets in the **List of Servers**, and the CAS has a status of Connected, repeat steps 1-11 for the secondary CAS.
15. Once changes are made and the secondary CAS is rebooted, the primary CAS will appear as the active server on the List of Servers and displays all the new IP information.

Upgrading an Existing Failover Pair

For instructions on upgrading an existing failover pair to a new Cisco NAC Appliance release, see "Upgrading High Availability Pairs" in the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.

Useful CLI Commands for HA

Clean Access Manager

The following are useful files to know about for HA on the CAM:

- /etc/ha.d/perfigo.conf
- /etc/ha.d/ha.cf

The following example shows the location of the HA debug/log files, as well as the name of each CAM (node) in the HA pair:

```
[root@rjcam_1 ha.d]# more ha.cf
# Generated by make-hacf.pl
udpport         694
bcast           eth1
auto_failback   off
apiauth         default uid=root
log_badpack     false
debug           0
debugfile       /var/log/ha-debug
logfile         /var/log/ha-log
#logfacility    local0
watchdog        /dev/watchdog
keepalive       2
```

```
warntime        10
deadtime        15
node            rjcam_1
node            rjcam_2
```

Verifying Active/Standby Runtime Status on the HA CAM

The following example shows how to use the CLI to determine the runtime status (active or standby) of each CAM in the HA pair. You can run the **fostate.sh** command from the **/perfigo/common/bin/** directory on new and upgraded CAMs.

1. Run the fostate.sh script on the first CAM:

```
[root@rjcam_1 ~]# ./fostate.sh
My node is active, peer node is standby
[root@rjcam_1 ~]#
```

   This CAM is the active CAM in the HA-pair.

2. Run the fostate.sh script on the second CAM:

```
[root@rjcam_2 ~]# ./fostate.sh
My node is standby, peer node is active
[root@rjcam_2 ~]#
```

   This CAM is the standby CAM in the HA-pair.

Clean Access Server

The following are useful files to know about for HA on the CAS:

- HA CAS Configuration Status (**/etc/ha.d/perfigo.conf**)
- Heartbeat/Link-Based Connections (**/etc/ha.d/ha.cf**)
- Link-Detect Interfaces (**/etc/ha.d/linkdetect.conf**)
- Active/Standby Status (**/perfigo/common/bin/fostate.sh**)

HA CAS Configuration Status

The **/etc/ha.d/perfigo.conf** file shows a variety of configuration information for an HA-CAS, including hostname (rjcas_1), peer hostname (rjcas_2), HA mode (Primary), heartbeat interface (UDP/serial), and Link-detect interface information:

```
[root@rjcas_1 ha.d]# more perfigo.conf
#linux-ha
#Mon Aug 28 18:50:15 PDT 2006
WIRELESS_SERVICEIP=10.10.20.4
PING_DEAD=25
HOSTNAME=rjcas_1
HA_DEAD=15
PEERGUSSK=
PEERMAC=00\:16\:35\:BF\:FE\:67
PEERHOSTNAME=rjcas_2
TRUSTED_PINGNODE=10.10.40.100
UNTRUSTED_PINGNODE=10.10.20.100
HAMODE=PRIMARY
PEERMAC0=00\:16\:35\:BF\:FE\:66
PEERHOSTIP=10.10.50.2
HA_FAILBACK=off
```

```
HA_UDP=eth2
WIRED_SERVICEIP=10.10.20.4
HA_SERIAL=ttyS0
```

Heartbeat/Link-Based Connections

The **/etc/ha.d/ha.cf** file shows additional information about the heartbeat and link-based connections:

```
[root@rjcas_1 ha.d]# more ha.cf
# Generated by make-hacf-ss.pl
udpport         694
ucast           eth2 10.10.50.2
baud            19200
serial          /dev/ttyS0
keepalive       2
deadtime        15
deadping        25
auto_failback   off
apiauth         default uid=root
respawn         hacluster /usr/lib64/heartbeat/ipfail
ping            10.10.20.100
ping            10.10.40.100

log_badpack     false
warntime        10
debug           0
debugfile       /var/log/ha-debug
logfile         /var/log/ha-log
watchdog        /dev/watchdog
node            rjcas_1
node            rjcas_2
```

Link-Detect Interfaces

The **/etc/ha.d/linkdetect.conf** file is useful if your network topology restricts configuring external (pingable) interfaces for Link-detect functionality between your CAS HA pair appliances. This file specifies the CAS network interfaces (eth0, eth1, or both) to monitor for Link-detect functionality. If a monitored interface loses connectivity with its associated external interface, the active CAS fails over and the standby CAS assumes the active role.

To create and/or update the **linkdetect.conf** file in the CAS:

Step 1 Log in to the CAS direct console CLI and direct console as the root user.

Step 2 Navigate to the **/etc/ha.d/** directory on the CAS.

Step 3 Using a standard text editor (like vi), edit the linkdetect.conf file so that it contains the interface names you want to monitor, or (if the linkdetect.conf file does not currently exist on the CAS) add the linkdetect.conf file to this directory.

Step 4 Verify the contents of the file:

```
[root@rjcas_1 ha.d]# more linkdetect.conf

# The following network interfaces will be monitored for link healthiness
# The active CAS will change to standby mode when any link failure is detected
#
eth0
eth1
```

Step 5 Enable the new function by stopping and restarting CAS services with the **service perfigo stop** and **service perfigo start** commands.

In the above **linkdetect.conf** file example, both the eth0 and eth1 interfaces on the CAS are monitored for network connectivity.

Note Any other CAS interfaces specified in the **linkdetect.conf** file (like eth2 or eth3, for example) are ignored for purposes of Link-detect behavior.

Active/Standby Status

The following example shows how to use the CLI to determine the runtime status (active or standby) of each CAS in the HA pair. You can find the fostate.sh command in the **/perfigo/common/bin/** directory on new and upgraded CASs.

1. Cd to `/perfigo/common/bin/`, and run the fostate.sh script on the first CAS:

```
[root@rjcas_1 bin]# ./fostate.sh
My node is active, peer node is standby
[root@rjcas_1 bin]#
```

   This CAS is the active CAS in the HA-pair.

2. Run the fostate.sh script on the second CAS:

```
[root@rjcas_2 bin]# ./fostate.sh
My node is standby, peer node is active
[root@rjcas_2 bin]#
```

   This CAS is the standby CAS in the HA-pair.

Accessing High Availability Pair CAS Web Consoles

Determining Active and Standby CAS

From the CAM web console, go to **Device Management > CCA Servers > List of Servers** to view your HA-CAS pairs. The List of Servers page displays the **Service IP** of the CAS pair first, followed by the IP address of the Active CAS in brackets. When a secondary CAS takes over, its IP address will be listed in the brackets as the Active server.

Note The CAS configured in HA-Primary Mode may not be the currently Active CAS.

Determining Primary and Secondary CAS

Open the direct access console for each CAS in the pair by typing the following in the URL/Address field of a web browser (you should have two browsers open):

- For the Primary CAS, type: **https://**<*primary_CAS_eth0_IP_address*>**/admin**. For example, `https://172.16.1.2/admin`.

- For the Secondary CAS, type: **https://**<*secondary_CAS_eth0_IP_address*>**/admin**. For example, `https://172.16.1.3/admin`.

In each CAS web console, go to **Administration > Network Settings > Failover > General**.

- The Primary CAS is the CAS you configured in **HA-Primary Mode** when you initially set up HA**.**
- The Secondary CAS is the CAS you configured in **HA-Secondary Mode** when you initially set up HA.

For releases prior to 4.0(0), the Secondary CAS is labelled as **HA-Standby Mode** (CAS) for the initial HA configuration.

CHAPTER 5

Password Recovery

Recovering Root Password for CAM/CAS

Use the following procedure to recover the root password for a CAM or CAS machine. The following password recovery instructions assume that you are connected to the CAM/CAS via a keyboard and monitor (i.e. console or KVM console, NOT a serial console).

Step 1 Power up the machine.

Step 2 When you see the boot loader screen with the "`Press any key to enter the menu…`" message, press any key.

Step 3 You will be at the GRUB menu with one item in the list "'`Cisco Clean Access (2.6.18-128.1.10.el5PAE)`." Press "**`e`**" to edit.

Step 4 You will see multiple choices as follows:

```
root (hd0,0)
kernel /vmlinuz-2.6.18-128.1.10.el5PAE ro root=/dev/cciss/c0d0p2 console=tty0
console=ttyS0,9600n8 crashkernel=128M@16M
initrd /initrd-2.6.18-128.1.10.el5PAE.img
```

Step 5 Scroll to the second entry (line starting with "`kernel…`") and press "**`e`**" to edit the line.

Step 6 Delete the line "`console=ttyS0,9600n8`" and edit the line so it appears as follows:

```
kernel /vmlinuz-2.6.18-128.1.10.el5PAE ro root=/dev/cciss/c0d0p2 console=tty0 single
```

Step 7 Press "**`b`**" to boot the machine in single user mode. You should be presented with a root shell prompt after boot-up (note that you will not be prompted for password).

Step 8 At the prompt, type "**`passwd`**", press Enter and follow the instructions.

Step 9 After the password is changed, enter "**`reboot`**" to reboot the appliance.

Recovering Root Password for CAM/CAS (Release 3.5.x or Below)

To recover the root password for CAM/CAS on release 3.5(x), you can use the Linux procedure to boot to single user mode and change the root password:

Step 1 Connect to the CAM/CAS machine via console.

Step 2 Power cycle the machine.

Step 3 After power-cycling, the GUI mode displays. Press Ctrl-x to switch to text mode. This displays a “boot:” prompt.

Step 4 At the prompt type: `linux single`. This boots the machine into single user mode.

Step 5 Type: `passwd`.

Step 6 Change the password.

Step 7 Reboot the machine using the `reboot` command.

APPENDIX A

Open Source License Acknowledgements

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

   The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

INDEX

Numerics

A

C

D

E

F

G

Text Part Number:

H

I

K

L

M

P

R

S

T

U

V