



Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.0

INCLUDING LICENSE AND WARRANTY

- 1** Verifying the Package Contents
- 2** Cisco NAC Appliance Hardware Summary
- 3** Starting the Initial Configuration
- 4** Access the CAM Web Console
- 5** CLI Commands
- 6** CD Installation on Cisco NAC Appliance
- 7** Configuring Additional NIC Cards
- 8** Obtaining Documentation, Obtaining Support, and Security Guidelines
- 9** Cisco Limited Lifetime Hardware Warranty Terms

About the Cisco NAC Appliance

Cisco® NAC Appliance (formerly Cisco Clean Access) 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 Clean Access Agent client software. You can deploy the Cisco NAC Appliance solution in the configuration that best meets the needs of your network.

The Cisco NAC Appliance is a Linux-based network hardware appliance which is pre-installed with either the CAM (MANAGER) or CAS (SERVER) application, the operating system and all relevant components on a dedicated server machine. The operating system comprises a hardened Linux kernel based on a Fedora core. Cisco NAC Appliance does not support the installation of any other packages or applications onto a CAM or CAS dedicated machine.

About This Document

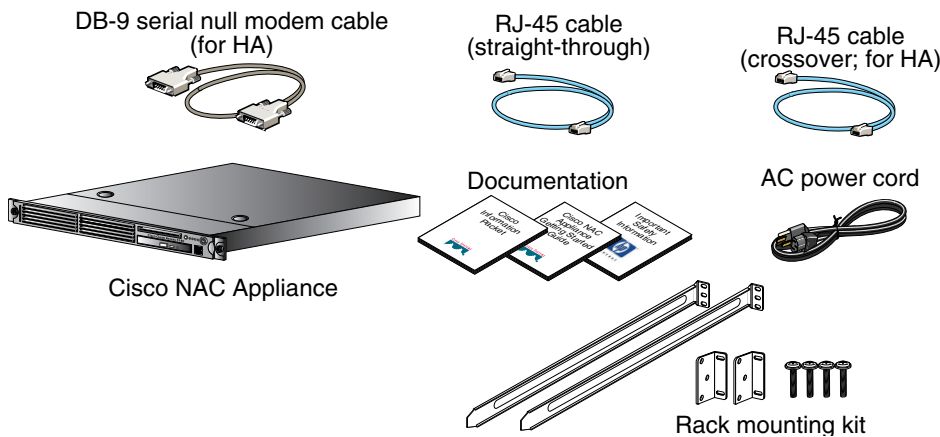
Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.0 (this guide) provides basic hardware specifications for the Cisco NAC Appliance. It also provides instructions for how to initially configure your CAM and CAS using the Configuration Utility, install product licenses, and access the CAM web console. 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 [Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.0](#) and [Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.0](#). When using the online publications, refer to the documents that match the software version running on your NAC Appliance.

1 Verifying the Package Contents

Verify the contents of the packing box (Shipping Box Contents, page 3) 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 in the diagram.

Shipping Box Contents




Note

Because product software is preloaded onto Cisco NAC-3300 Series appliances, the shipping contents do not include a separate Cisco Clean Access (CCA) software installation CD.


Note

If you ordered a Failover Bundle, you will receive two physical NAC Appliances, which you will need to connect together and configure via web console to create a High-Availability pair. Refer to “Configuring High Availability (HA)” in the [Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.0](#) and [Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.0](#) for complete HA configuration details.

Equipment Required

You need to supply a workstation (PC or laptop) and keyboard/monitor/mouse to run the Cisco NAC Appliance Configuration Utility. 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 NAC Appliance to the network (eth0 for the CAM; eth0 and eth1 for the CAS). The Cisco NAC Appliance Hardware Summary, page 6 provides interface details for each model.

Rack Mounting

The Cisco NAC Appliance occupies one rack unit (1U). An optional rack-mounting kit is included in the shipment. For rack-mounting information and instructions, refer to the *1U Rack Hardware Installation Instructions for HP Products* document also included in the shipment.

NAC Appliance Licensing

You need at least 1 CAM license and 1 CAS license for your NAC Appliance system to work. Both licenses are installed via the Clean Access Manager web admin 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 34 and [Add Additional Licenses](#), page 37.

Upgrading NAC Appliance Software

NAC-3300 Series appliances are preloaded with a default version of the CCA software. Cisco recommends that you upgrade your appliances to the most current supported version of the system software to ensure you have the latest product enhancements and fixes.



Note

Release 4.0(5) and 4.1(1) (forthcoming) are the minimum software versions recommended for NAC-3300 series appliances. For details, refer to [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#) and the applicable 4.0(x) and 4.1(1) Release Notes at http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

When upgrading appliances, a single .tar.gz upgrade file is downloaded from Cisco Secure Downloads and applied to the Lite/Standard/Super CAM or CAS either via direct console/SSH or using the web console (for non-HA systems). The upgrade mechanism automatically determines whether the machine is a Clean Access Manager (CAM) or Clean Access Server (CAS), and executes accordingly.

For step-by-step upgrade instructions, refer to the “Upgrading” section of the applicable [Release Notes](#).



Note The NAC-3390 MANAGER software is upgraded using the same upgrade .tar.gz file as other systems. However, new software installation via CD on the NAC-3390 requires its own Super CAM .ISO file (see CD Installation on Cisco NAC Appliance, page 40 for further details).

Upgrading Firmware

NAC-3300 Series appliances are subject to any system BIOS/Firmware upgrades required for the server model on which they are based.



Note NAC-3310 is based on the HP ProLiant DL 140 G3 and requires a firmware upgrade as described in the [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#).

For More Information

For more information, refer to these documents at www.cisco.com/go/nac/appliance:

- The “Upgrading to 4.0(x)” section of the [Release Notes for Cisco NAC Appliance \(Cisco Clean Access\), Version 4.0\(x\)](#)
- [Cisco NAC Appliance Data Sheet](#)
- [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#)
- [Cisco NAC Appliance Service Contract/Licensing Support](#)
- [Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.0](#)
- [Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.0](#)

For the latest online updates to this guide, refer to http://www.cisco.com/en/US/products/ps6128/prod_installation_guides_list.html

For details on how to obtain technical support, refer to section Obtaining Documentation, Obtaining Support, and Security Guidelines, page 47.

2 Cisco NAC Appliance Hardware Summary

Table 1 summarizes 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.

Table 1 Cisco NAC Appliance Hardware Summary



Cisco NAC Appliance	Product	Hardware Specifications	Diagrams
Cisco NAC Appliance 3300 Series			
NAC-3310 ^{1,2}	MANAGER Lite Manager supporting up to 3 standalone or HA-pair CASs	Single processor: Xeon 2.33 GHz dual core 1 GB RAM 160 GB NHP SATA HDD  Note	<ul style="list-style-type: none"> NAC-3310 Front Panel, page 9 NAC-3310 Rear Panel, page 9
	SERVER CAS supporting 100, 250, or 500 users	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. <hr/> Smart Array E200i Controller 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	

Table 1 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	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 NAC-3350 is based on HP ProLiant DL360 G5 .	<ul style="list-style-type: none"> • NAC-3350 Front Panel, page 11 • NAC-3350 Front Panel LEDs/Buttons • NAC-3350 Rear Panel, page 12 • NAC-3350 Rear Panel LEDs
	SERVER CAS supporting 1500, 2500, or 3500 users		
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 2 NICs (2 Broadcom 5708 integrated NICs) CD/DVD-ROM Drive 4 USB Ports (1 front, 1 internal, 2 rear) Cavium CN1120-NHB-E SSL Accelerator Card  Note NAC-3390 is based on HP ProLiant DL360 G5 .	<ul style="list-style-type: none"> • NAC-3390 Front Panel, page 15 • NAC-3390 Front Panel LEDs/Buttons • NAC-3390 Rear Panel, page 17 • NAC-3390 Rear Panel LEDs/Buttons

Table 1 Cisco NAC Appliance Hardware Summary (continued)

Cisco NAC Appliance	Product	Hardware Specifications	Diagrams
Cisco NAC Appliance 3100 Series			
CCA-3140-H1 ^{2,4}	Clean Access Manager (CAM)	Single processor: Xeon 2.8 GHz single core 1 GB SDRAM, DDR2-400 MHz	<ul style="list-style-type: none"> • CCA-3140-H1 Front Panel, page 18 • CCA-3140-H1 Rear Panel, page 19
	Clean Access Server (CAS)	80 GB NPH SATA hard disk drive (HDD) Embedded SATA RAID Controller 2 10/100/1000 LAN ports (2 Broadcom 5721 integrated NICs) 24x CD-ROM Drive 2 PCI full slots 4 USB Ports (2 front, 2 rear)	
		 <p>Note CCA-3140-H1 is based on HP ProLiant DL140 G2.</p> <p>CCA-3140-H1 requires CD install of Cisco NAC Appliance software</p>	

1. NAC-3310 requires a firmware/BIOS upgrade for HP ProLiant DL140 G3. See Upgrading Firmware, page 5.
2. NAC-3310 and CCA-3140 support [iLO \(Lights Out 100i Remote Management\)](#). The default iLO “Administrator” account has default username/password: **admin/admin**. Defaults can be changed through the CCA-3140 BIOS setup.
3. NAC-3350 and NAC-3390 support [iLO2 \(Integrated Lights Out, version 2\)](#). See panel tags for admin account details.
4. You cannot order the CCA-3140-H1 after August 3, 2007 (EOL).

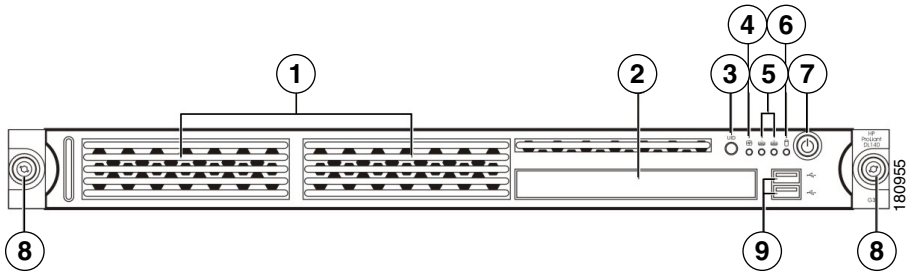
NAC-3310 Front and Rear Panels

The 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.

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

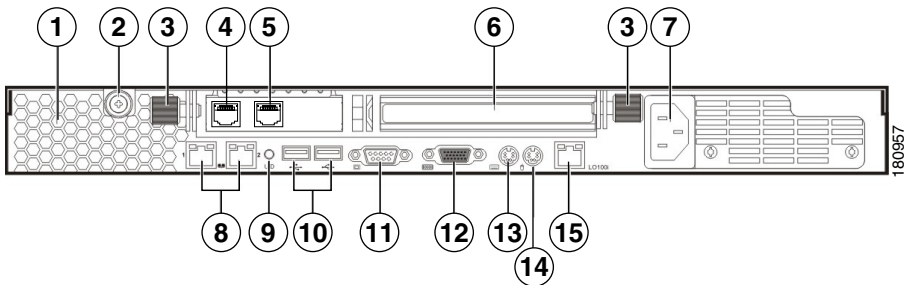
For additional details, see Cisco NAC Appliance Hardware Summary, page 6.

Figure 1 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 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 2 NAC-3310 Rear Panel



1	Ventilation holes	9	UID button with 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)		



Note

The three LAN ports each have their own LED indicators for activity/link status and network speed.

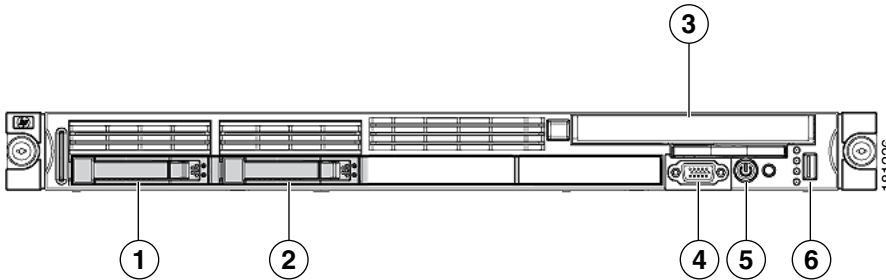
NAC-3350 Front and Rear Panels

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

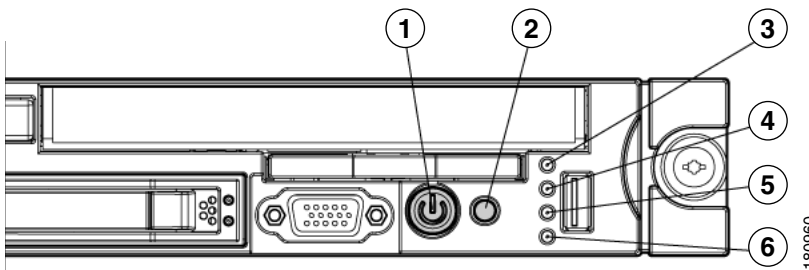
For additional details, see Cisco NAC Appliance Hardware Summary, page 6.

Figure 3 NAC-3350 Front Panel



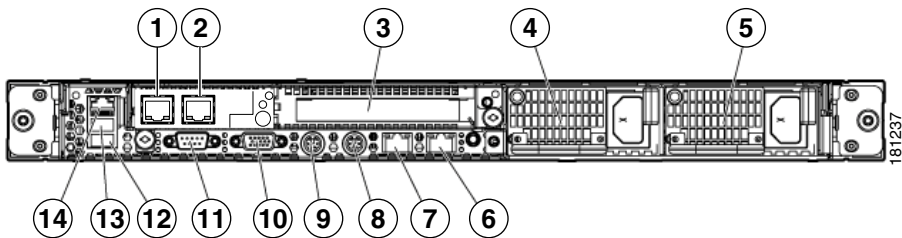
1	Hard drive bay 1	4	Video connector
2	Hard drive bay 2	5	HP Systems Insight Display
3	CD-ROM/DVD drive	6	USB connector

Figure 4 NAC-3350 Front Panel LEDs/Buttons



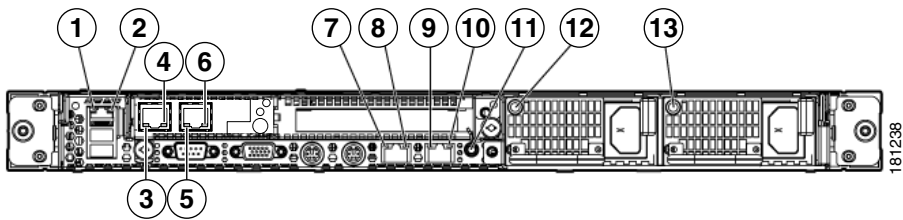
1	Power On/Standby button and system power LED	Green = System is on. Amber = System is shut down, but power is still applied. Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed; facility power is not available, or disconnected power button cable.
2	UID 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 6 on page 13)
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 6 on page 13)

Figure 5 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 6 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.

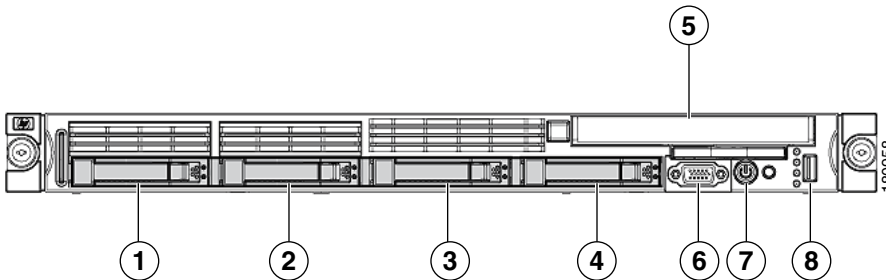
NAC-3390 Front and Rear Panels

The 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 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 Cisco NAC Appliance Hardware Summary, page 6.



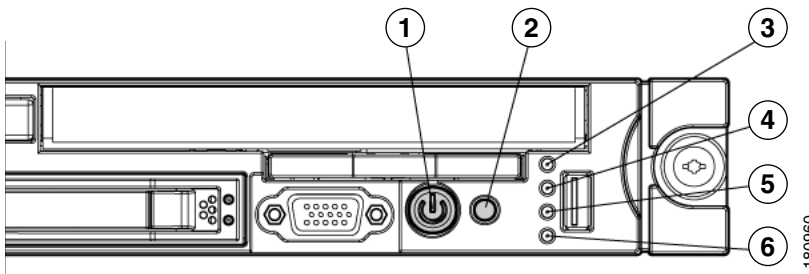
Note The Super CAM software is supported **only** on the Cisco NAC-3390 Appliance platform.

Figure 7 NAC-3390 Front Panel



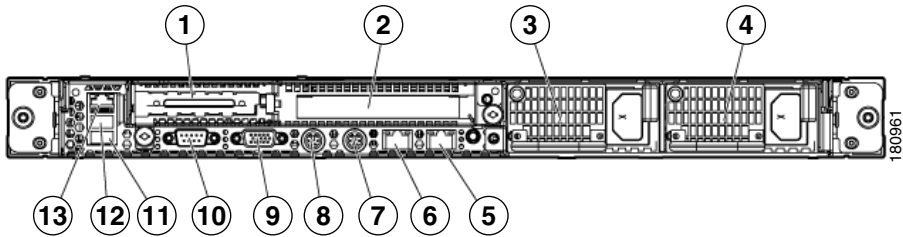
1	Hard drive bay 1	5	CD-ROM/DVD drive
2	Hard drive bay 2	6	Video connector
3	Hard drive bay 3	7	HP Systems Insight Display
4	Hard drive bay 4	8	USB connector

Figure 8 NAC-3390 Front Panel LEDs /Buttons



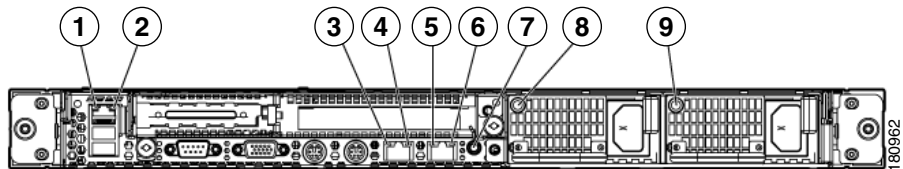
1	Power On/Standby button and system power LED	Green = System is on. Amber = System is shut down, but power is still applied. Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed; facility power is not available, or disconnected power button cable.
2	UID 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 10 on page 17)
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 10 on page 17)

Figure 9 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 10 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

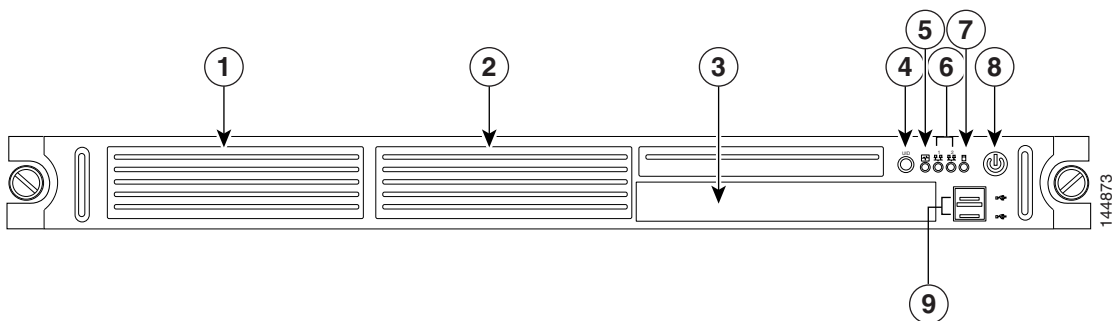
4	10/100/1000 NIC 1 Link LED	Green = Link exists Off = No link exists
5	10/100/1000 NIC 2 Activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
6	10/100/1000 NIC 2 Link LED	Green = Link exists Off = No link exists
7	UID button/LED	Blue = Identification is activated 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.

CCA-3140-H1 Front and Rear Panels

The Cisco Clean Access 3140 (CCA-3140-H1) requires that the customer load either the Clean Access Server or Clean Access Manager software. See *Installing CCA-3140 Cisco NAC Appliance*, page 41 for instructions.

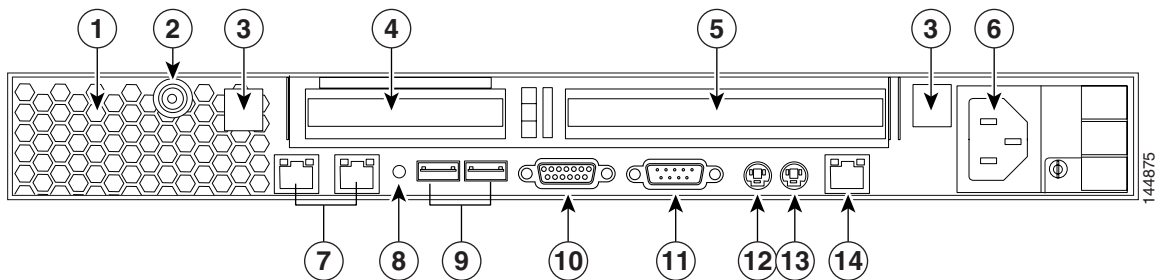
For additional details, see *Cisco NAC Appliance Hardware Summary*, page 6.

Figure 11 CCA-3140-H1 Front Panel



1	1-inch Non-Hot Plug SATA or SCSI Hard Drive Bay	6	NIC 1 and NIC 2 activity LEDs
2	1-inch Non-Hot Plug SATA or SCSI Hard Drive Bay	7	Disc activity LED
3	CD-ROM drive	8	Power Switch
4	UID LED	9	USB ports
5	System Health Monitor LED		

Figure 12 CCA-3140-H1 Rear Panel



1	Ventilation holes	8	UID button with LED indicator (blue); mirrors function of UID button located on front panel.
2	Thumbscrew for the top cover	9	USB 2.0 ports (black)
3	Thumbscrews for the PCI riser board assembly (lateral)	10	Video port (blue)
4	Low profile 64-bit/133 MHz PCI-X riser board slot cover	11	Serial port
5	Standard height/ full-length 64-bit/133 MHz PCI-X riser board slot cover	12	PS/2 keyboard port (purple)
6	Power supply cable socket	13	PS/2 mouse port (green)
7	GbE LAN ports (RJ-45) for NIC 1 (eth0) on left-hand side NIC 2 (eth1) on right-hand side	14	10/100 Mbps iLO port for IPMI management (RJ-45)

3 Starting the Initial Configuration

This section provides information on the following:

- Connecting the NAC Appliance, page 20
- Configuration Worksheets, page 22
- Running the Configuration Utility, page 24
- Important Notes for SSL Certificates, page 33
- Manually Restarting the Configuration Utility, page 33

Connecting the NAC Appliance

To perform initial configuration, you will need to connect to your NAC Appliance and access its command line.

-
- Step 1** You can access the command line of the NAC Appliance in one of two ways:
- a. Connect a monitor and keyboard directly to the machine via the keyboard/video monitor connectors on the back panel of the machine (preferred method), or
 - b. Connect a serial cable from a workstation (PC/laptop) to the machine and open a serial connection on the workstation using terminal emulation software (such as HyperTerminal or SecureCRT). For details, see [Connecting Serially to the NAC Appliance](#), page 21.
- Step 2** Connect a straight-through Category 5 Ethernet cable to the eth0 (NIC1) 10/100/1000 Ethernet port on the back panel of the NAC Appliance (CAM or CAS) and to your local area network.
- Step 3** If planning to configure the CAS NAC Appliance as a **NAT Gateway** or **Real-IP Gateway** for testing, connect a straight-through Category 5 Ethernet cable to the eth1 (NIC2) 10/100/1000 Ethernet port on the back panel of the CAS and to your local area network.



Note If planning to configure the CAS as a **Virtual Gateway**—either an In-Band (IB) or Out-of-Band (OOB)—leave the untrusted interface (eth1) of the CAS unplugged until after you have added the CAS to the CAM from the web admin console (and, for Central Deployments, configured VLAN Mapping) to prevent network connectivity issues. For details, see the [Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.0](#).

- Step 4** Connect the AC power cord to the back panel of the NAC Appliance and to a grounded AC outlet.

- Step 5** Power on the NAC Appliance by pressing the power button on the front of the appliance. The diagnostic LEDs will flash a few times as part of the power-on self-test (POST). Status messages are displayed on the console as the appliance boots up.
- Step 6** Proceed to the instructions in Running the Configuration Utility, page 24.
-

Connecting Serially to the NAC Appliance

This section describes how to access the command line of the NAC Appliance over a serial connection.

- Step 1** To use a serial connection, use a serial cable (DB9, female-female) to connect your PC/laptop to the serial port on the NAC Appliance. (You can use the null modem cable shipped in the box if needed.)

After physically connecting your workstation to the appliance, you can access the serial connection interface using any terminal emulation software. The following steps may vary depending on the software being used.

- Step 2** If using Microsoft® HyperTerminal, click **Start > All Programs > Accessories > Communications > HyperTerminal** to open the HyperTerminal window.
- Step 3** Type a name for the session and click **OK**.
- Step 4** In the **Connect using** list, choose the COM port on the workstation to which the serial cable is connected (e.g. COM3 or COM1) and click **OK**.
- Step 5** Configure the **Port Settings** as follows: Bits per second – 9600, Data bits – 8, Parity – None, Stop bits – 1, Flow control – Hardware (CTS/RTS) (or None).
- Step 6** Click the **Disconnect** icon, then go to **File > Properties** to open the Properties dialog for the session. Click the **Settings** tab, and set the **Emulation** dropdown to **VT100**. Click **OK**, then click the **Call** icon.

You should be able to access the command line interface of the appliance (it may take a minute).



- Note** If a NAC Appliance is configured for high availability (HA), and serial heartbeat is being used for HA, then the serial port can no longer be used for serial console.
-

Configuration Worksheets

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

- Clean Access Manager (CAM) Configuration Worksheet
- Clean Access Server (CAS) Configuration Worksheet

Clean Access Manager (CAM) Configuration Worksheet

Table 2 **CAM Configuration Utility Worksheet**

For Clean Access Manager NAC Appliance:	
a. IP address for eth0 interface (trusted):	
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. Shared secret: Must be the same for the CAM and all CAS(es)	
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:	



Note

Cisco highly recommends changing the default password and the use of strong passwords (with at least 6 characters, mixed letters and numbers).

Clean Access Server (CAS) Configuration Worksheet

Table 3 CAS Configuration Utility Worksheet

For Clean Access Server NAC Appliance:	
a.	IP address for eth0 interface (trusted):
b.	Subnet mask (IP netmask) for eth0 interface:
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:
g.	Host name for your CAS:
h.	IP address of Domain Name Server on your network:
i.	Shared secret: Must be the same for the CAM and all CAS(es)
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:

Running the Configuration Utility



Note For CCA-3140 only, you must perform CD installation of the software before running the Configuration Utility. Follow the steps in *Installing CCA-3140 Cisco NAC Appliance*, page 41 first before proceeding with this section if you have received a CCA-3140.

When you turn on the NAC-3310, NAC-3350, or NAC-3390 appliance and login as `root`, you will be prompted to perform the initial configuration as described in this section.

- To configure the **MANAGER**, follow the steps in *Run CAM Configuration Utility Script*, page 24.
- To configure the **SERVER**, follow the steps in *Run CAS Configuration Utility Script*, page 28.

After completing initial configuration on both the **MANAGER** (CAM) and **SERVER** (CAS), see *Access the CAM Web Console*, page 34.

Run CAM Configuration Utility Script

Step 1 Connect and power on the NAC-3310, NAC-3350, or NAC-3390 **MANAGER** appliance as described in *Connecting the NAC Appliance*, page 20.

(For CCA-3140 only, proceed to Step 3 after completing *Install the Clean Access Manager (CAM) Software from CD-ROM*, page 42.)

Step 2 Log in as user `root` with default password `cisco123`.

Step 3 The following Configuration Utility Welcome screen 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) 2006 Cisco Systems, Inc.
```

Step 4 At the first prompt, type an IP address for the `eth0` (trusted) interface of the CAM (from field **a.** of the CAM Worksheet) and press Enter. Confirm the value when prompted, or type `n` and press Enter to correct the entry.

```
Configuring the network interface:
Please enter the IP address for the interface eth0 [10.0.2.15]: 10.201.240.11
You entered 10.201.240.11 Is this correct? (y/n)? [y]
```

Step 5 Type the subnet mask for the interface address (from field **b.**) at the prompt or press Enter for the default (255.255.255.0). 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 6 Accept the default gateway or specify and confirm a default gateway address (from field c.) for the Clean Access Manager. This is typically the IP address of the router between the CAM subnet and the CAS 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 7 Type a host name for the Clean Access Manager (from field d.) To use the CAM host name for the CAM web console, make sure to create an entry in your DNS server.

```
Please enter the hostname [localhost.localdomain]: cam3350
You entered cam3350 Is this correct? (y/n)? [y]
```

Step 8 Type the IP address of the Domain Name System (DNS) server in your environment (from field e.) or accept the default at the following prompt:

```
Please enter the IP address for the name server [10.0.2.1]: 63.93.96.94
You entered 63.93.96.94 Is this correct? (y/n)? [y]
```

Step 9 The Clean Access Manager and Clean Access Servers in a deployment authenticate each other through a shared secret that serves as an internal password. The default shared secret is **cisco123**. Type and confirm the shared secret (from field f.) at the prompts.

```
The shared secret used between Clean Access Manager and Clean Access Server is the
default string: cisco123
This is highly insecure. It is recommended that you choose a string that is unique
to your installation.
Please enter the shared secret: cisco123
You entered: cisco123
Is this correct? (y/n)? [y]
```



Caution

The shared secret must be the same for the Clean Access Manager and all Clean Access Servers in the deployment. If they have different shared secrets, they cannot communicate.

Step 10 Specify the time zone in which the Clean Access Manager is located (from field g.) as follows:

```
>>> Configuring date and time:
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 **45** 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 **19** 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 11 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 07/09/06]: 15:52:00 10/09/06
You entered 15:52:00 10/09/06 Is this correct? (y/n)? [y]
Mon Oct 9 15:52:00 PDT 2006
```

Step 12 Follow the prompts to configure the temporary SSL security certificate that enables secure connections between the CAM and the web admin console (using field **h.**):

You must generate a valid SSL certificate in order to use the Clean Access Manager's secure web console.

Please answer the following questions correctly.

Information for a new SSL certificate:

```
Enter fully qualified domain name or IP: 10.201.240.11
Enter organization unit name: DOC
Enter organization name: Cisco Systems
Enter city name: San Jose
Enter state code: CA
Enter 2 letter country code: US
```

- 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 13 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

Generating SSL Certificate...
CA signing: /root/.tomcat.csr -> /root/.tomcat.crt:
CA verifying: /root/.tomcat.crt <-> CA cert
/root/.tomcat.crt: OK
Done
```

Step 14 Configure the **root** user password for the installed Linux operating system of the CAM (from field **i.**). The default password is **cisco123**. The **root** user account is used to access the system over direct/serial/SSH console connection.

```
For security reasons, it is highly recommended that you change the passwords for
the root user.
User: root
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd(pam_unix)[1823]: password changed for root
passwd: all authentication tokens updated successfully.
```



Note Cisco recommends using strong passwords (for example, at least 6 characters, mixed letters and numbers, etc.) to reduce the vulnerability of your network to password guessing attacks.

Step 15 After the configuration is complete, press Enter to reboot the CAM.

```
Changes require a RESTART of Clean Access Manager.
Configuration is complete.
Done
Install has completed. Press <ENTER> to reboot.
```



Note If you used `service perfigo config` to start the configuration utility, you must type `service perfigo reboot` or `reboot` and press Enter to reboot the machine after configuration. See Manually Restarting the Configuration Utility, page 33.

Step 16 After restarting, the CAM will be accessible through the web console, as described in Access the CAM Web Console, page 34.

Run CAS Configuration Utility Script

Step 1 Turn on the NAC-3310 or NAC-3350 SERVER appliance, as described in Connecting the NAC Appliance, page 20.
(For CCA-3140 only, proceed to Step 3 after completing Install the Clean Access Server (CAS) Software from CD-ROM, page 44.)

Step 2 Log in as user `root` with default password `cisco123`.

Step 3 The following Configuration Utility Welcome screen 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) 2006 Cisco Systems, Inc.
```

Step 4 At the first prompt, type an IP address for the eth0 (trusted) interface of the CAS (from field a. of the CAS Worksheet) and press Enter. 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 [10.0.2.15]: 10.201.240.100  
You entered 10.201.240.100 Is this correct? (y/n)? [y]
```



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

Step 5 Type the subnet mask for the interface address (from field b.) at the prompt or press Enter for the default (255.255.255.0). 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 6 Accept the default gateway address or type a default gateway (from field c.) for the eth0 address of the CAS and press Enter. 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 7 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, VLAN passthrough is not needed.

Step 8 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.

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



Note 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.



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.

Step 9 Type an IP address for the eth1 (untrusted) interface of the CAS (from field **d**.) and press Enter. Confirm the value when prompted, or type **n** and press Enter to correct the entry.

```
Please enter the IP address for the untrusted interface eth1 [10.0.2.15]:
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 CAS guide for further details.

Step 10 Type the subnet mask of the eth1 interface (from field **e**.) 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 11 Enter the default gateway address for the eth1 untrusted interface (from field f.):

- a. If the CAS will be a Real-IP or NAT Gateway, this is the IP address of the CAS's untrusted interface eth1.
- b. If the CAS will be a Virtual Gateway, this can be the same default gateway address used for the trusted interface.

```
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 12 At the next prompt, type **n** and press Enter (or just press Enter) to keep VLAN ID passthrough disabled for the eth1 interface.

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

Step 13 At the Management VLAN Tagging prompt, type **n** and press Enter (or just press Enter) to keep Management VLAN tagging disabled (default) for the eth1 interface.

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

Step 14 Type and confirm the host name for the Clean Access Server (from field g.).

```
Please enter the hostname [localhost.localdomain]: cas3350
You entered cas3350 Is this correct? (y/n)? [y]
```

Step 15 Type the IP address of the DNS server in your environment (from field h.) or accept the default at the following prompt:

```
Please enter the IP address for the name server [10.0.2.1]: 63.93.96.94
You entered 63.93.96.94 Is this correct? (y/n)? [y]
```

Step 16 Type and confirm the shared secret for the CAM and CAS (from field i.) at the prompts.

```
The shared secret used between Clean Access Manager and Clean Access Server is the
default string: cisco123.
This is highly insecure. It is recommended that you choose a string that is unique
to your installation.
Please enter the shared secret: cisco123
You entered: cisco123
Is this correct? (y/n)? [y]
```



Caution

The shared secret must be the same for the Clean Access Manager and all Clean Access Servers in the deployment. If they have different shared secrets, they cannot communicate.

Step 17 Specify time settings for the Clean Access Server (from field j.) as follows:

```
>>> Configuring date and time:
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 **45** 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 **19** 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 18 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 07/09/06]: 15:52:00 10/09/06
You entered 15:52:00 10/09/06 Is this correct? (y/n)? [y]
Mon Oct 9 15:52:00 PDT 2006
```



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 19 Follow the prompts to configure the temporary SSL security certificate that secures the login exchange between the Clean Access Server and untrusted (managed) clients (using field k.):

```
You must generate a valid SSL certificate in order to use the Clean Access
Server's secure web console.
Please answer the following questions correctly.
Information for a new SSL certificate:
Enter fully qualified domain name or IP: 10.201.240.10
Enter organization unit name: doc
Enter organization name: Cisco Systems
Enter city name: San Jose
Enter state code: CA
Enter 2 letter country code: US
```

- a. For the organization unit name, enter the group **within** your organization that is responsible for the certificate (for example, **doc**).
- b. 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.
- c. Type the name of the city or county in which your organization is legally located (for example, **San Jose**), and press Enter.
- d. Type the two-character state code in which the organization is located (for example, **CA** or **NY**), and press Enter.
- e. Type the two-letter country code (for example, **us**), and press Enter.

Step 20 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
Generating SSL Certificate...
CA signing: /root/.tomcat.csr -> /root/.tomcat.crt:
CA verifying: /root/.tomcat.crt <-> CA cert
/root/.tomcat.crt: OK
Done
```

Step 21 Type the **root** user password for the installed Linux operating system of the CAS (from field **l.**). The default password is **cisco123**. The **root** user account is used to access the system over direct/serial/SSH connection.

```
For security reasons, it is highly recommended that you change the password for
the root user.
User: root
Changing password for user root.
New UNIX password:
Retype new UNIX password:
```

Step 22 Type the **admin** user password for the CAS direct access web console (from field **m.**). The default password is **cisco123**. The CAS web console provides limited CAS-specific settings, and is primarily used to set up High Availability.

```
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 23 After the configuration is complete, press Enter to reboot the CAS.

```
Configuration is complete.  
Done  
Install has completed. Press <ENTER> to reboot.
```



Note If you used `service perfigo config` to start the configuration utility, you must type `service perfigo reboot` or `reboot` and press Enter to reboot the machine after configuration.

The CAS initial configuration is now complete.

Step 24 Ping the CAM from the CAS to verify that the CAM and CAS can ping (route) to each other.

Step 25 Continue to the instructions in Access the CAM Web Console, page 34.

Important Notes for SSL Certificates

- You must generate the temporary SSL certificates during the initial configuration of both the CAM and CAS or you will not be able to access your NAC Appliance as an admin or end user.
- Before deploying the CAM or CAS in a production environment, you can obtain a trusted certificate from a Certificate Authority to replace the temporary certificate. A CA-signed certificate for the CAS prevents the security warning when end users log in, and a CA-signed certificate for the CAM prevents the admin web login security warning.
- 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. For further details see the “Set System Time” and “Manage SSL Certificates” sections of the CAM and CAS guides.

Manually Restarting the Configuration Utility

If after installation you need to reset the configuration settings — for either the Clean Access Server or Clean Access Manager — you can use the `service perfigo config` CLI command:

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

Step 2 Login as user: `root`, password: `cisco123` (default).

Step 3 Run the following command: `service perfigo config`

Step 4 Accept the default values or provide new ones for all prompts (as described in Running the Configuration Utility, page 24).

Step 5 When configuration is done, reboot the machine with the command: `service perfigo reboot`

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`, then power down the machine, or
- Type `/sbin/halt`, then power down the machine.

4 Access the CAM Web Console

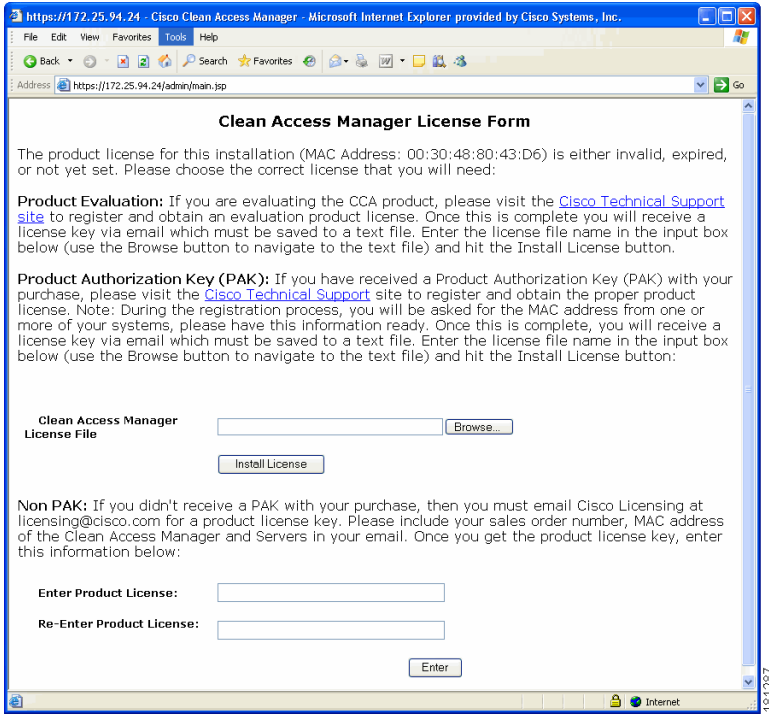
The Clean Access Manager web administration console is the primary interface for administering the Cisco NAC Appliance deployment. After initial configuration is complete, use the following steps to access the CAM web console.

-
- Step 1** Launch a web browser from a computer accessible to the CAM by network. (Microsoft Internet Explorer 6.0 and 7.0 are supported.)
- Step 2** 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 3** 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 will not appear.)

Install CAM License

- Step 4** The Clean Access Manager License Form displays (Figure 13). For convenience, the top of the form displays the eth0 MAC address of the CAM appliance. Make sure you have already obtained and saved your product license files to disk on the PC/laptop from which you are accessing the CAM web console (as described in NAC Appliance Licensing, page 4).

Figure 13 Clean Access Manager License Form



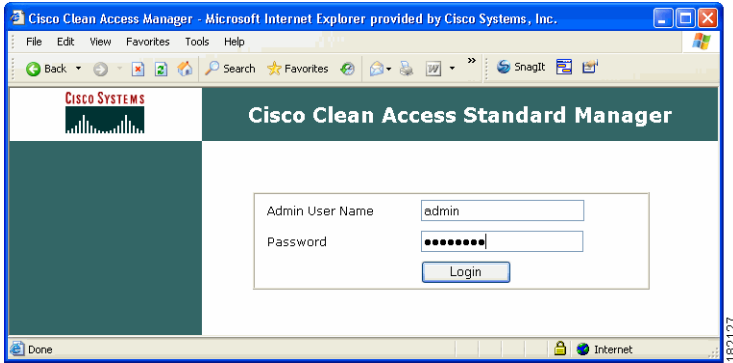
Step 5 For the Clean Access Manager License File field, Browse to the license file you received for the CAM and click the Install License button.



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 upgrade of HA-CAM pairs.

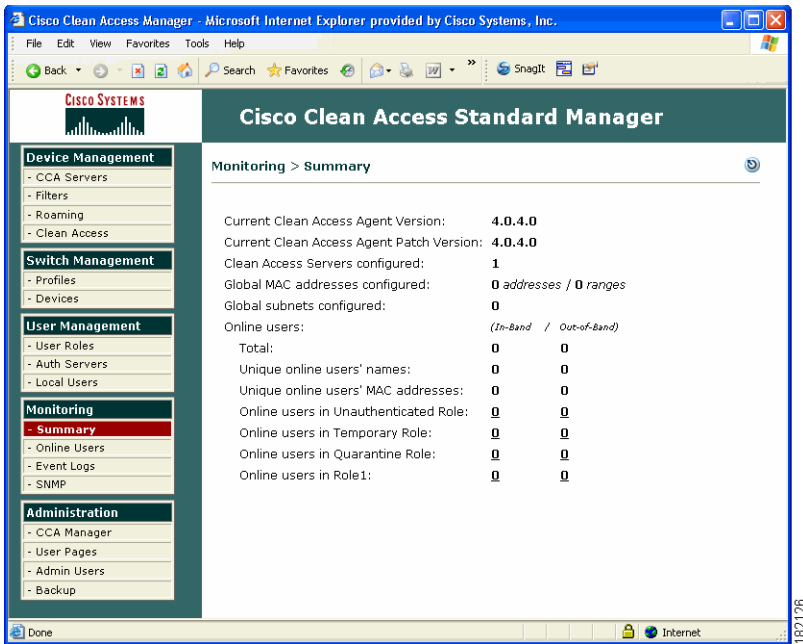
Step 6 Once the license is accepted, the web admin console login window appears (Figure 14). Type the default username **admin** and default web admin user password **cisco123**, and click **Login**.

Figure 14 CAM Web Admin Console Login Page



Step 7 The Monitoring Summary page and left-hand navigation pane displays (Figure 15).

Figure 15 Monitoring Summary Page



Add Additional Licenses

Step 8 To add additional CAS licenses, go to **Administration > CCA Manager > Licensing** (Figure 16).

Figure 16 Licensing Page

The screenshot shows the 'Administration > Clean Access Manager' interface. At the top, there is a navigation bar with tabs for 'Network & Failover', 'System Time', 'SSL Certificate', 'System Upgrade', 'Licensing', and 'Support Logs'. Below the navigation bar, a green message states: 'License added successfully. CCA Manager License added. In-Band Server Count is now 11.' The main content area has two sections. The first section is for 'Clean Access FlexLM License File(s)', featuring a text input field, a 'Browse...' button, and two buttons: 'Install License' and 'Remove All Licenses'. The second section is for 'Perfigo Product License Key', featuring a text input field and an 'Apply Key' button. At the bottom, there is a table titled 'FlexLM License-Enabled Features' with the following data:

Feature	Count
Manager Failover License present	
In-Band Server Count	11
Out-of-Band Server Count	10

Step 9 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. Out-of-Band Server Count is now 10."). 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. 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 HAS-CAS pair.

Step 10 Repeat Step 9 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 web admin console.

Once installed, a permanent FlexLM license takes precedence and replaces an evaluation FlexLM license. Once installed, a FlexLM license (either permanent or evaluation) takes precedence and replaces a legacy license key (even though the legacy key is still installed).

When an evaluation FlexLM expires or is removed, an existing legacy license key will again take effect. Refer to *NAC Appliance Licensing*, page 4 for further details.

Step 11 Licenses are now installed. You can continue the configuration of your deployment using the CAM web console. Refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.0* and *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.0* for complete details.

Step 12 To log out of the web console, either click the admin session **Logout** button, at the top right-hand corner of the console, or simply close the browser.





Note

The CAM web console manages all Clean Access Servers in the CAM domain. You can also access limited/advanced settings on a specific CAS through the CAS direct access web console (via **https://<CAS_IP>/admin**; default username/password: **admin/cisco123**). The CAS direct access console is typically used only for advanced configuration, such as HA.

5 CLI Commands

You can use the NAC Appliance command line interface (CLI) to set basic operational parameters directly on the CAM or CAS machine if the web console is unavailable (for example, due to incorrect network or VLAN settings). Table 4 lists commonly used CLI commands. To run them, access the NAC Appliance via KVM, SSH or serial console, and log in as user **root** (default password **cisco123**).

Table 4 CLI Commands

Command	Description
<code>service perfigo config</code>	Starts the configuration utility to modify CAM or CAS network settings and configuration. When done, run <code>service perfigo reboot</code> or <code>reboot</code> to reset the appliance with the modified settings. See Manually Restarting the Configuration Utility, page 33.
<code>service perfigo start</code>	Starts up the CAM or CAS. The appliance must be stopped to use this command. If the appliance is running, a warning message appears.
<code>service perfigo stop</code>	Shuts down the Clean Access service on the CAM or CAS  Note When the management VLAN is set, this command causes the CAS to lose network connectivity when issued.
<code>service perfigo maintenance</code> (CAS-only command)	CAS-only command that 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.
<code>service perfigo restart</code>	Shuts down the Clean Access service and starts it up again on the CAM or CAS. This is used when the service is already running and you want to restart it.  Note Do not use <code>service perfigo restart</code> to test high availability (failover). Instead, use the <code>shutdown</code> or <code>reboot</code> Linux command on the appliance to test failover, or, CLI commands <code>service perfigo stop</code> and <code>service perfigo start</code> .
<code>service perfigo reboot</code>	Shuts down and reboots the CAM or CAS. Or, use Linux <code>reboot</code> .
<code>service perfigo time</code>	Use to modify time zone settings. To view time, use Linux <code>clock</code> .

6 CD Installation on Cisco NAC Appliance

NAC-3300 Series Appliances

NAC-3310, NAC-3350, and NAC-3390 appliances are preloaded with a default version of the CCA system software. The first time a NAC-3300 appliance is powered on, it prompts for a root login and starts the initial configuration script as described in Running the Configuration Utility, page 24. For configured appliances, Cisco recommends upgrading to the latest software release supported for the NAC-3300 series as mentioned in Upgrading NAC Appliance Software, page 4. Optionally, or for new appliances preloaded with an older version of software, you can perform CD installation to a new supported software version. Note that CD software installation on a configured appliance will remove all previous configuration.



Note Release 4.0(5) and 4.1(1) (forthcoming) are the minimum software versions recommended for NAC-3300 series appliances. For details, refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* and the applicable 4.0(x) and 4.1(1) Release Notes at http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

- For CD software installation on a **MANAGER** appliance, follow the instructions in Install the Clean Access Manager (CAM) Software from CD-ROM, page 42.
- For CD software installation on a **SERVER** appliance, follow the instructions in Install the Clean Access Server (CAS) Software from CD-ROM, page 44.



Note For CD software installation on the NAC-3310 **only**, you **must** type an installation directive at the boot: prompt—either **DL140** if directly connected, or **serial_DL140** if serially connected to the appliance. See the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for details.



Note For CD software installation on the NAC-3390 **MANAGER only**, a separate Super CAM .ISO file is required to create a bootable CD-ROM. The Super CAM software is supported **only** on the NAC-3390 platform.

NAC-3100 Series Appliances

For CCA-3140 only, the software is not preloaded and must always be installed on the machine from CD-ROM as described in Installing CCA-3140 Cisco NAC Appliance, page 41.

Installing CCA-3140 Cisco NAC Appliance

For the CCA-3140-H1 only, you must install the Cisco NAC Appliance software from CD before the configuration utility can be run. The same installation CD is used to install either the CAM or CAS software on the machine. During the installation, you will be prompted to choose whether to install the CCA Manager (default) or CCA Server package. You must choose one or the other for the package installation to execute.

- To install CAM software on the CCA-3140, follow the steps in *Install the Clean Access Manager (CAM) Software from CD-ROM*, page 42.
- To install CAS software on the CCA-3140, follow the steps in *Install the Clean Access Server (CAS) Software from CD-ROM*, page 44.

After package installation completes, the configuration utility automatically starts and you can follow the instructions described in *Running the Configuration Utility*, page 24.



Note Cisco NAC Appliance software is not intended to coexist with other software or data on the target machine. The installation process formats and partitions the target hard drive, destroying any data or software on the drive.

The entire installation process, including the configuration steps described in *Running the Configuration Utility*, page 24 should take about 15 minutes per appliance.

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

The following steps describe how to perform CD installation of the Clean Access Manager software on the CCA-3140-H1 (required), or NAC-3310 MANAGER, NAC-3350 MANAGER, and NAC-3390 MANAGER appliances (optional).

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 Connecting the NAC Appliance, page 20.

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



Note For the latest version compatibility details, refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* and applicable Release Notes at http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

- For CCA-3140-H1, insert the product CD in the CD-ROM drive of the target machine.
- Or, **Log In** to Cisco Secure Software, and download the latest supported .ISO file from <http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml>
 - For NAC-3310 MANAGER, NAC-3350 MANAGER, or CCA-3140-H1, download the `cca-<version>-K9.iso` file.
 - For NAC-3390 MANAGER only, download the `supercam-cca-<version>-K9.iso` file.
 - Burn the .ISO as a bootable disk to a CD-R. Insert the CD into the CD-ROM drive of each installation machine.

Step 3 Reboot the machine. The Cisco Clean Access Installer welcome screen appears after the machine restarts:

```
Cisco Clean Access 4.0-5 Installer (C) 2006 Cisco Systems, Inc.  
      Welcome to the Cisco Clean Access 4.0-5 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 at the boot prompt and press the <ENTER> key.  
boot:
```

Step 4 At the “boot:” prompt:

- For NAC-3310 MANAGER only:
 - Type **DL140** and press the Enter key if your monitor and keyboard are directly connected to the NAC-3310, or
 - Type **serial_DL140** and press Enter in the terminal emulation console if you are accessing the NAC-3310 over a serial connection.

- For CCA-3140-H1, NAC-3350 MANAGER, or NAC-3390 MANAGER:
 - Press the Enter key if your monitor and keyboard are directly connected to the target machine, or
 - Type `serial` and press Enter in the terminal emulation console if you are accessing the target machine over a serial connection.

Step 5 The Package Group Selection screen appears next to prompt you to choose **CCA Manager** software installation (default) or **CCA Server** software installation. At the following screen prompt, choose **CCA Manager** and select **OK** to begin the installation. Use the space bar and the “+” and “-” keys to select the appropriate type. Use the Tab key to tab to the **OK** field, and press the Enter key when done to start the installation of the package type selected.

```
Welcome to Cisco Clean Access

++ Package Group Selection ++
|
| Total install size: 679M
|
|   [*] CCA Manager #
|   [ ] CCA Server  #
|                                     #
|                                     #
|                                     #
|                                     #
|                                     #
|                                     #
|
| +-----+      +-----+
| | OK |      | Cancel |
| +-----+      +-----+
|
+-----+
|<Space>,<+>,<-> selection | <F2> Group Details | <F12> next screen
```



Note The Package Group Selection is set by default to **CCA Manager**. However, you must still tab to the **OK** field and press Enter to start the installation.

Step 6 The Clean Access Manager Package Installation then executes. The installation takes a few minutes. When finished, the welcome screen for the Clean Access Manager quick configuration utility appears.

Step 7 Continue the initial configuration of the CAM by following the instructions in Run CAM Configuration Utility Script, page 24.

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

The following steps describe how to perform CD installation of the Clean Access Server software on the CCA-3140-H1 (required), or NAC-3310 SERVER and NAC-3350 SERVER appliances (optional).

-
- 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 Connecting the NAC Appliance, page 20.
- Step 2** Download and install the latest software version supported on the target machine as follows:



Note For the latest version compatibility details, refer to the [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#) and applicable [Release Notes](#).

- For CCA-3140-H1, insert the product CD in the CD-ROM drive of the target machine.
- Or, Log In to Cisco Secure Software, and download the latest supported .ISO file from <http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml>:
 - For NAC-3310 SERVER, NAC-3350 SERVER, or CCA-3140-H1 download the `cca-<version>-K9.iso` file.
 - Burn the ISO as a bootable disk to a CD-R. Insert the CD into the CD-ROM drive of each installation machine.

- Step 3** Reboot the machine. The Cisco Clean Access Installer welcome screen appears after the machine restarts:

```
Cisco Clean Access 4.0-5 Installer (C) 2006 Cisco Systems, Inc.  
Welcome to the Cisco Clean Access 4.0-5 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 at the boot prompt and press the <ENTER> key.  
boot:
```

- Step 4** At the “boot:” prompt:
- For NAC-3310 SERVER only:
 - Type **DL140** and press the Enter key if your monitor and keyboard are directly connected to the NAC-3310, or
 - Type **serial_DL140** and press Enter in the terminal emulation console if you are accessing the NAC-3310 over a serial connection.
 - For CCA-3140-H1 or NAC-3350 SERVER:
 - Press the Enter key if your monitor and keyboard are directly connected to the target machine, or


- Type **serial** and press Enter in the terminal emulation console if you are accessing the target machine over a serial connection.

Step 5 The Package Group Selection screen appears next to prompt you to choose **CCA Manager** software installation (default) or **CCA Server** software installation. At the following screen prompt, choose **CCA Server** and select **OK** to begin the installation. Use the space bar and the “+” and “-” keys to select the appropriate type. Use the Tab key to tab to the **OK** field, and press the Enter key when done to start the installation of the package type selected.

```

Welcome to Cisco Clean Access
++ Package Group Selection ++
|
| Total install size: 679M
|
| [ ] CCA Manager #
| [*] CCA Server #
| #
| #
| #
| #
| #
| #
|
+-----+ +-----+
| OK | | Cancel |
+-----+ +-----+
|
+-----+
|
|<Space>,<+>,<-> selection | <F2> Group Details | <F12> next screen

```

 **Note** The Package Group Selection is set by default to **CCA Manager**. You must select **CCA Server** then tab to the **ok** field and press Enter to start installation of the CAS.

Step 6 The Clean Access Server Package Installation then executes. The installation takes a few minutes. When finished, the welcome screen for the Clean Access Server quick configuration utility appears.

Step 7 Continue the initial configuration of the CAS by following the instructions in Run CAS Configuration Utility Script, page 28.

7 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. For HA, once the eth2 (NIC3) interface is configured with the proper addressing, it can then be configured as the dedicated UDP heartbeat interface for the HA-CAS.



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

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** You should see 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 will bring up a utility that helps you configure the NIC.

See the “Configuring High Availability (HA)” sections of the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.0* and *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.0* for further details on configuring HA.

8 Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

9 Cisco Limited Lifetime Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranties and license agreements applicable to Cisco software, is available on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty and license agreements from Cisco.com.

1. Launch your browser, and go to this URL:
http://www.cisco.com/univercd/cc/td/doc/es_inpk/cetrans.htm
The Warranties and License Agreements page appears.
2. To read the *Cisco Information Packet*, follow these steps:
 - a. Click the **Information Packet Number** field, and make sure that the part number 78-5235-03B0 is highlighted.
 - b. Select the language in which you would like to read the document.
 - c. Click **Go**.
 - d. The Cisco Limited Warranty and Software License page from the Information Packet appears.
 - e. Read the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe’s website: <http://www.adobe.com>

3. To read translated and localized warranty information about your product, follow these steps:
 - a. Enter 78-6310-02C0 in the Warranty Document Number field.
 - b. Select the language in which you would like to view the document.
 - c. Click **Go**.

The Cisco warranty page appears.

- d. Read the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

http://www.cisco.com/public/Support_root.shtml.

Duration of Hardware Warranty

A Cisco product hardware warranty is supported for as long as the original end user continues to own or use the product, provided that the fan and power supply warranty is limited to five (5) years. In the event of a discontinuance of product manufacture, the Cisco warranty support is limited to five (5) years from the announcement of the discontinuance.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of the Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference.

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	



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

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 800 020 0791
Fax: 31 0 20 357 1100

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

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2007 Cisco Systems, Inc. All rights reserved.

Printed in the USA on recycled paper containing 10% postconsumer waste.