



CHAPTER 4

Installing the Clean Access Server



Note

The installation example and references in this chapter focus on Cisco NAC 3300 Series appliances. 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*.

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

- [Overview, page 4-1](#)
- [Summary of Steps For New Installation, page 4-3](#)
- [Connect the Clean Access Server, page 4-4](#)
- [Virtual Gateway Mode Connection Requirements, page 4-6](#)
- [Install the Clean Access Server Software from CD-ROM, page 4-8](#)
- [Perform the Initial Configuration, page 4-9](#)
- [Using the Command Line Interface \(CLI\), page 4-19](#)
- [CAM/CAS Connectivity Across a Firewall, page 4-21](#)
- [Configuring the CAS Behind a NAT Firewall, page 4-21](#)
- [Configuring Additional NIC Cards, page 4-22](#)
- [Troubleshooting the Installation, page 4-23](#)

Overview

The Cisco NAC Appliance 3300 Series 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. 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.

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 3300 Series platforms.

**Tip**

The [Cisco NAC Appliance Hardware Installation Quick Start Guide](#) covers all necessary instructions for powering up a new Cisco NAC Appliance.

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

**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](#) and [Installing Cisco Network Modules in Cisco Access Routers](#).

Legacy customers can perform Cisco NAC Appliance software installation via CD on certain customer-supplied hardware platforms, which must be listed as supported in the [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#). 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 server (application, OS, and relevant components), the installation of any other packages or applications on the CAM or CAS is not supported.

**Caution**

Cisco NAC Appliance (Cisco Clean Access) 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. Before starting the installation, make sure that the target machine does not contain any data or applications that you need to keep.

**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).

Summary of Steps For New Installation



Note Refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* for general 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 Clean Access, 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 login to Cisco Secure Software and download the latest 4.1(2).ISO image from <http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml> and burn it as a bootable disk to a CD-R.

Step 3 Connect the server to the network, as described in [Connect the Clean Access Server, page 4-4](#).

Step 4 Connect a monitor and keyboard to the server, or connect your workstation to the server via serial cable, as described in [Connect the Clean Access Server, page 4-4](#).

Step 5 Install the software as described in [Install the Clean Access Server Software from CD-ROM, page 4-8](#).

Step 6 Perform the initial configuration of the server, as described in [Perform the Initial Configuration, page 4-9](#)



Note For High Availability mode, install and initially configure each CAS first before configuring HA. Refer to [Chapter 14, “Configuring High Availability \(HA\)”](#) for details.

Step 7 Make sure your Clean Access Manager is installed and initially configured as described in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*. 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 8 Add your Clean Access Server(s) to the Clean Access Manager, as described in [Add the CAS to the CAM, page 5-2](#). 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 server's command line.

- Step 1** The Clean Access Server requires two 10/100/1000BASE-TX interface connectors on the back panel of the server 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 [Virtual Gateway Mode Connection Requirements, page 4-6](#) for details.

If needed, refer to “Cisco NAC Appliance Hardware Summary” in the *Cisco NAC Appliance Hardware Installation Quick Start Guide*, or the documentation that came with your server to find the serial and Ethernet connectors.

- 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** Power on the machine by pressing the power button on the front of the server or 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 server boots up.

- Step 4** Access the command line or the CAS by either:
- Connecting a monitor and keyboard directly to the server via the keyboard connector and video monitor/console connector on the back panel
 - Or, connecting a serial cable from an external workstation (PC/laptop) to the server and open a serial connection using terminal emulation software (such as HyperTerminal or SecureCRT) on the external workstation, as described in [Install the Clean Access Server Software from CD-ROM, page 4-8](#).

**Note**

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

Serial Connection to the CAS

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

- Step 1** Connect the serial port of your admin computer to an available serial port on the server machine with a serial cable.

**Note**

If the server 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 server machine must have at least two serial ports to be able to manage the server over a serial connection. If it does not, you have the option of freeing the serial port by using an Ethernet connection for the peer connection. For more information, see [Chapter 14, “Configuring High Availability \(HA\).”](#)

- Step 2** After physically connecting the workstation to the server, 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** Give any name to 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. Change the **Emulation** setting to:
- **Emulation**– vt100
- Step 8** You should now be able to access the command interface for the server. You can now:
- [Install the Clean Access Server Software from CD-ROM, page 4-8](#)
 - [Perform the Initial Configuration, page 4-9](#)

**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.

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 [Add the CAS to the CAM, page 5-2](#).
- Step 4** Manage the CAS by accessing the CAS management pages, via **Device Management > CCA Servers > Manage [CAS_IP]** as described in [Navigating the CAS Management Pages, page 5-7](#).
- Step 5** Configure VLAN mapping on the CAS. This is a mandatory step if the eth0 and eth1 interfaces of the CAS have the same IP address but belong to different VLANs (e.g. a Central Deployment where both interfaces of the CAS connect to the same switch).
- 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 [VLAN Mapping in Virtual Gateway Modes, page 5-25](#).



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** 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 7** 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>.
- Step 8** Once the preceding steps are completed, physically connect the eth1 interface of the CAS to the switch.

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](#).

Before You Start —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 [Understanding VLAN Settings, page 5-24](#) and [VLAN Mapping in Virtual Gateway Modes, page 5-25](#) for additional details.

Install the Clean Access Server Software from CD-ROM

Once you are connected to the command line of the CAS (as described in [Connect the Clean Access Server, page 4-4](#)) use the following steps to install the Clean Access Server software from CD-ROM.



Caution

Cisco NAC Appliance (Cisco Clean Access) 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. Before starting the installation, make sure that the target machine does not contain any data or applications that you need to keep.

CD Installation Steps

The entire installation process, including the configuration steps described in [Perform the Initial Configuration, page 4-9](#) should take about 15 minutes.

Step 1 Insert the distribution CD-ROM that contains the Clean Access Server .iso file into the CD-ROM drive of the target server machine.

Step 2 Reboot the machine. The Cisco Clean Access Installer welcome screen appears after the machine restarts:

```
Cisco Clean Access 4.1-2 Installer (C) 2007 Cisco Systems, Inc.

Welcome to the Cisco Clean Access 4.1-2 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 3 At the “boot:” prompt, type one of the following options, depending on your specific NAC Appliance platform and type of connection:

For Cisco NAC-3310:

- Type **DL140** if you are directly connected (monitor, keyboard, and mouse) to the appliance.
- Type **serial_DL140** if you are installing the software via serial console connection.

For Cisco NAC-3350:

- 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 4** The Package Group Selection screen appears next to prompt you to choose CCA Manager software installation or CCA Server software installation. At the following screen prompt, you **MUST** choose **cca server** and select **OK** to begin the Clean Access Server 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: 679
|
| [ ] CCA Manager #
| [*] CCA Server #
|                                     #
|                                     #
|                                     #
|                                     #
|                                     #
|                                     #
|
+-----+      +-----+
|  OK  |      | Cancel |
+-----+      +-----+

```

<Space>,<+>,<-> selection | <F2> Group Details | <F12> next screen



Caution

Only one CD is used for installation of the Clean Access Server or Clean Access Manager software. The installation script does not automatically detect CAS or CAM installation for the target server. The Package Group Selection is set by default to **CCA Manager**. You must select the appropriate type, **CCA Server**, for the target machine on which you are performing installation, then tab to the OK field and press Enter to start the installation.

- Step 5** 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, and a series of questions prompt you for the initial server configuration, as described in the next section, [Configuration Utility Script, page 4-10](#).



Note

If after installation you need to reset the CAS configuration settings (such as the eth0 IP address), connect to the CAS machine serially or via SSH and run the `service perfigo config` command. See [Using the Command Line Interface \(CLI\), page 4-19](#) for details. Most other settings can also be modified later from the web console.

Perform the Initial 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 server 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 server machine, log onto the server as user `root` with default password `cisco123`.
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 server if it cannot be reached through the web admin console. For further details on CLI commands, see [Using the Command Line Interface \(CLI\)](#), page 4-19.

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.
```
- Step 3** The script first asks for settings for the trusted interface (eth0). The trusted interface is the interface to the protected, backend network.
- ```
Configuring the network interfaces:
Please enter the IP address for the interface eth0 [10.0.2.15]: 10.201.240.12
You entered 10.201.240.12 Is this correct? (y/n)? [y] y
```
- At the prompt, type the eth0 IP address of the CAS and press Enter. 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.
- Step 4** 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 5** Specify the default gateway address for the trusted interface and press Enter. Confirm the value at when prompted.
- ```
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 6** Specify VLAN ID passthrough behavior for the trusted interface. At the prompt, type `n` and press Enter (or just press Enter) to accept the default behavior where VLAN passthrough is disabled and VLAN IDs are stripped from traffic passing through the interface. Or, enter `y` to enable VLAN ID passthrough for traffic passing from the trusted network to the untrusted network.
- ```
[Vlan Id Passthrough] for packets from eth0 to eth1 is disabled.
Would you like to enable it? (y/n)? [n]
eth1 is disabled.
Would you like to enable it? (y/n)? [n] y
```

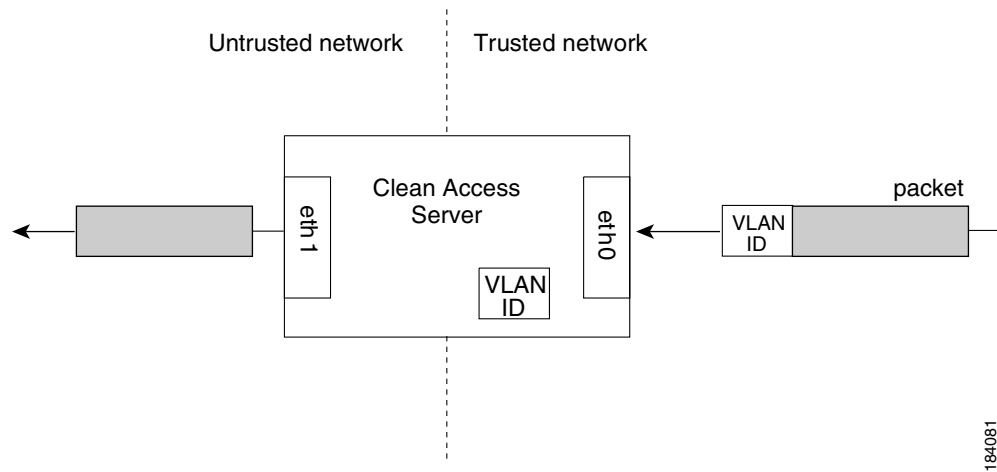


**Note**

- 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 4-1. The IDs are retained by the Clean Access Server and attached to response messages passed from the untrusted network back to the trusted network.

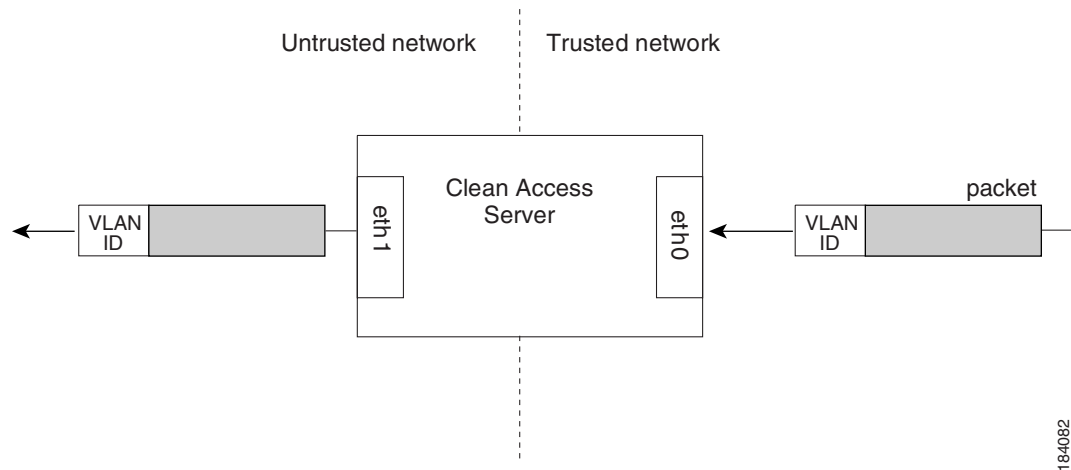
**Figure 4-1 VLAN ID Termination**



184081

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

**Figure 4-2 VLAN ID Passthrough**



184082

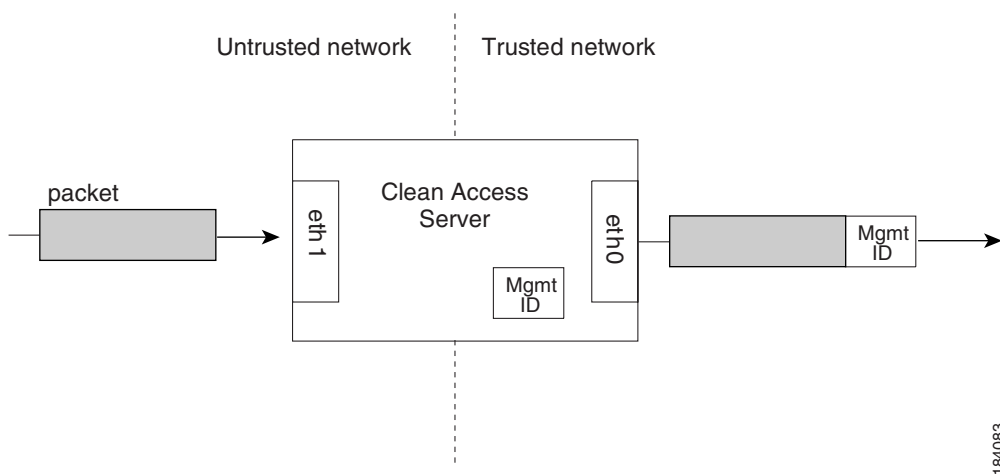
- Step 7** Specify Management VLAN Tagging for the trusted interface at the next prompt. Type **n** and press Enter (or just press Enter) to keep Management VLAN tagging disabled (default). Or, type **y** and press Enter to enable Management VLAN tagging and specify the Management VLAN ID to use for the CAS trusted interface.



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

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 4-3 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.
  - 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 8** 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 [192.168.0.1]:
You entered 192.168.0.1 Is this correct? (y/n)? [y]
```

- Step 9** 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]: 255.255.0.0
You entered 255.255.0.0, is this correct? (y/n)? [y]
```

- Step 10** Enter the default gateway address for the untrusted interface:

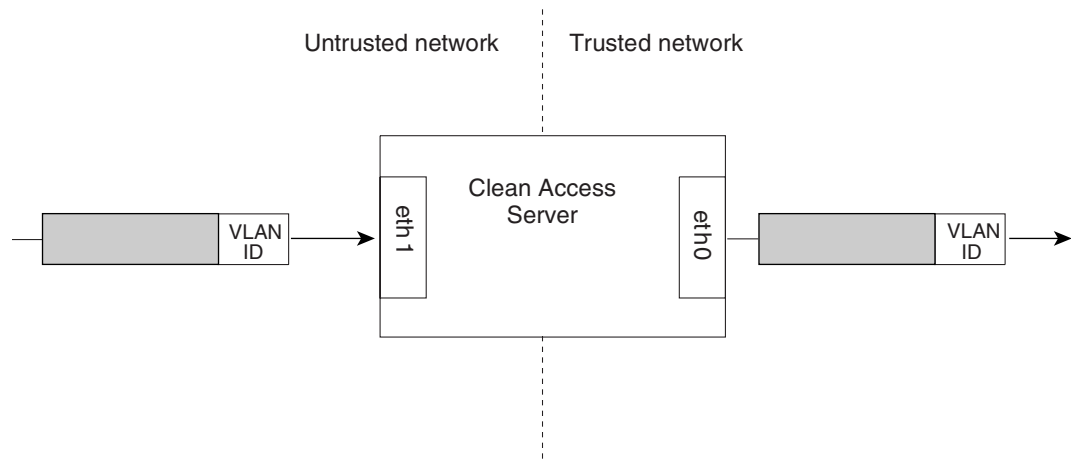
- If the Clean Access Server will act as a Real-IP gateway or NAT gateway, this should be the IP address of the CAS's untrusted interface eth1.
- If the Clean Access Server will act as a Virtual gateway (i.e., a bridge), this can be the same default gateway address used for the trusted side.

```
Please enter the IP address for the default gateway [192.168.0.1]:
You entered 192.168.0.1 Is this correct? (y/n)? [y]
```

**Step 11** 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 4-4** VLAN ID Passthrough



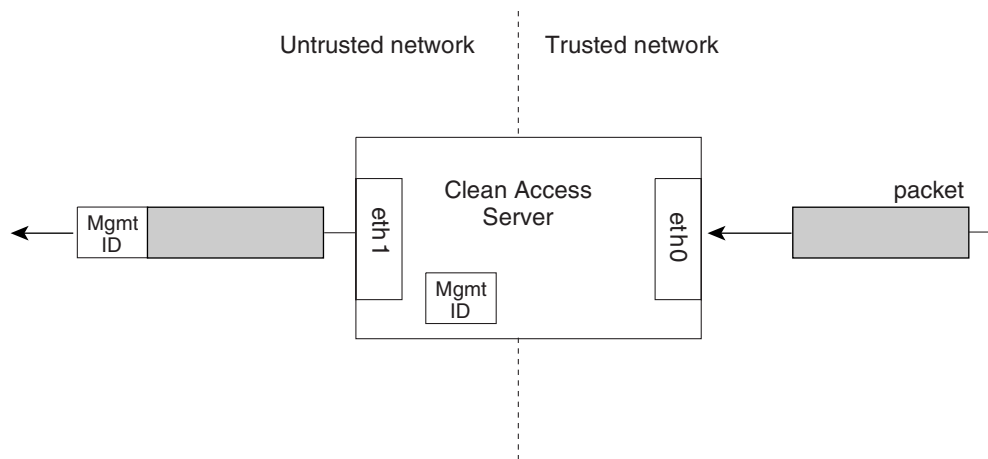
184095

**Step 12** 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** page of the web console; however, changing settings on the CAS **IP** page requires a reboot of the CAS.

**Figure 4-5 Eth1 Egress Packets with Management VLAN ID Tagging**

18-4096

- Step 13** Specify the host name for the Clean Access Server (`caserver` is the default). Type and confirm the address when prompted:

```
Please enter the hostname [caserver]: caserver10
You entered caserver10 Is this correct? (y/n)? [y]
```

- Step 14** 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: [172.68.226.120]:
You entered 172.68.226.120 Is this correct? (y/n)? [y]
```

- Step 15** The Clean Access Manager and Clean Access Servers in a deployment authenticate each other through a shared secret. The shared secret serves as an internal password for the deployment. Type and confirm the shared secret when prompted:

```
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 16** Specify time settings for the Clean Access Server.

- a. Choose the timezone location 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. Enter **11** to enter the time zone in Posix TZ format, such as `GST-10`.

```
>>> 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.
1) Africa
```

```

2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 2

```

- b. Choose a country for the chosen timezone. Select your country from the country list, such as **45** for the United States, and press Enter.

```

Please select a country.
1) Anguilla 18) Ecuador 35) Paraguay
2) Antigua & Barbuda 19) El Salvador 36) Peru
3) Argentina 20) French Guiana 37) Puerto Rico
4) Aruba 21) Greenland 38) St Kitts & Nevis
5) Bahamas 22) Grenada 39) St Lucia
6) Barbados 23) Guadeloupe 40) St Pierre & Miquelon
7) Belize 24) Guatemala 41) St Vincent
8) Bolivia 25) Guyana 42) Suriname
9) Brazil 26) Haiti 43) Trinidad & Tobago
10) Canada 27) Honduras 44) Turks & Caicos Is
11) Cayman Islands 28) Jamaica 45) United States
12) Chile 29) Martinique 46) Uruguay
13) Colombia 30) Mexico 47) Venezuela
14) Costa Rica 31) Montserrat 48) Virgin Islands (UK)
15) Cuba 32) Netherlands Antilles 49) Virgin Islands (US)
16) Dominica 33) Nicaragua
17) Dominican Republic 34) Panama
#? 45

```

- c. If the country contains more than one time zone, time zone regions for the country appear. Choose the appropriate time zone region from the list and press enter (for example, **16** for Pacific Time).

```

Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Standard Time - Indiana - most locations
6) Eastern Standard Time - Indiana - Crawford County
7) Eastern Standard Time - Indiana - Starke County
8) Eastern Standard Time - Indiana - Switzerland County
9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands
22) Hawaii
#? 16

```

- d. Confirm your choices or cancel your choices and start over, by entering 1 to confirm or 2 to start over.

The following information has been given:

```
United States
Pacific Time
```

Is the above information OK?

```
1) Yes
2) No
#? 1
```

Updating timezone information...

- Step 17** Confirm the current date and time at the next prompt by pressing enter, or provide the correct date and time in the format shown. Confirm the values when prompted.

```
Current date and time hh:mm:ss mm/dd/yy [04:08:29 02/15/06]: 18:08:29 02/15/06
You entered 18:08:29 02/15/06 Is this correct? (y/n)? [y]
Wed Feb 15 18:08:29 PST 2006
```

- Step 18** 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. At the following prompt, type the IP address or domain name for which you want the certificate to be issued.

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: 10.201.240.12

- b. For the organization unit name, enter the group within your organization that is responsible for the certificate (for example, IT or engineering).

Enter organization unit name: engineering

- c. For the organization name, type the name of your company or organization for which you would like to receive the certificate, and press enter.

Enter organization name: Cisco Systems

- d. Type the name of the city or county in which your organization is legally located, and press enter.

Enter city name: San Jose

- e. Enter the two-character state code in which the organization is located, such as CA or NY, and press enter.

Enter state code: CA

- f. Type the two-letter country code and press enter.

Enter 2 letter country code: US

- g. A list of the values you entered appears. Press enter to accept the values or N to restart.

```
You entered the following:
Domain: 10.201.240.12
Organization unit: engineering
Organization name: Cisco Systems
City name: San Jose
State code: CA
Country code: US
Is this correct? (y/n)? [y]
Generating SSL Certificate...
CA signing: /root/.tomcat.csr -> /root/.tomcat.crt:
CA verifying: /root/.tomcat.crt <-> CA cert
```

```

/root/.tomcat.crt: OK

Done

```

When you confirm your values, the certificate is generated and the Clean Access Server database is initialized.

**Step 19** Now configure passwords on the CAS for the root user account (SSH users), and the CAS direct access web console. The CAS web console gives you direct access to limited CAS-specific settings, and is primarily used to set up high availability. The specific passwords to set are as follows:

- a. The first password is for the **root** user of the installed Linux operating system. You can use this account when accessing the CAS over a serial connection.

```

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

```

- b. Next type the password for the **admin** user for the CAS direct access web console.

```

Would you like to change the default password for the web console admin user password?
(y/n)? [y]
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 20** If installing from the CD-ROM, press the Enter key to reboot the CAS when configuration is complete:

```

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

```

**Step 21** If running the **service perfigo config** configuration utility, run the following command to reboot the server:

```

service perfigo reboot

```

**Step 22** The 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 [Chapter 5, “Configuring CAS Managed Network.”](#)

## Important Notes for SSL Certificates

- You must generate the temporary SSL certificate during CAS installation or you will not be able to access your CAS.
- 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. For further details on the CAS, see:
  - [Manage CAS SSL Certificates, page 13-4](#)
  - [Synchronize System Time, page 13-27](#)
  - For details on CAM certificates, see the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)*.

- Before deploying the server in a production environment, you can acquire a trusted certificate from a Certificate Authority to replace the temporary certificate (in order to avoid the security warning that is displayed to end users during user login).

## Using the Command Line Interface (CLI)

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 \(Table 4-1\)](#) 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 \(Table 4-2\)](#) 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` (default password is `cisco123`). If already serially connected to the server, you can run CLI commands from the terminal emulation console after logging in as `root` (see [Install the Clean Access Server Software from CD-ROM, page 4-8](#)).

## CAS CLI Commands for Cisco NAC Appliance

The format `service perfigo <command>` is used to enter a command from the command line. [Table 4-1](#) lists the commonly used Cisco NAC Appliance CLI commands.

**Table 4-1** Cisco NAC Appliance CLI Commands for CAS

| Command                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>service perfigo start</code>       | Starts up the server. If the server is already running, a warning message appears. The server must be stopped for this command to be used.                                                                                                                                                                                                                                                                                                                                                                       |
| <code>service perfigo stop</code>        | Shuts down the Clean Access service.<br><b>Note</b> When the management VLAN is set, this command will cause the CAS to lose network connectivity when issued. You can use <code>service perfigo maintenance</code> instead.                                                                                                                                                                                                                                                                                     |
| <code>service perfigo maintenance</code> | 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.<br><b>Note</b> You can use <code>service perfigo maintenance</code> to stop the service when testing high availability (failover) for Virtual Gateway CASs over an SSH connection. |
| <code>service perfigo platform</code>    | 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.<br>For detailed installation and configuration information, see <a href="#">Getting Started with Cisco NAC Network Modules in Cisco Access Routers</a> and <a href="#">Installing Cisco Network Modules in Cisco Access Routers</a> .                       |

**Table 4-1 Cisco NAC Appliance CLI Commands for CAS**

| Command                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>service perfigo restart</code> | Shuts down the Clean Access service and starts it up again. This is used when the service is already running and you want to restart it.<br><br><b>Note</b> <code>service perfigo restart</code> 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, <code>service perfigo stop</code> or <code>service perfigo maintenance</code> followed by <code>service perfigo start</code> |
| <code>service perfigo reboot</code>  | Shuts down and reboots the machine. You can also use the Linux <code>reboot</code> command.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>service perfigo config</code>  | Starts the configuration script to modify the server configuration. After completing <code>service perfigo config</code> , you must reboot the server. For instructions on using the script, see <a href="#">Perform the Initial Configuration, page 4-9</a>                                                                                                                                                                                                                                                |
| <code>service perfigo time</code>    | Use to modify the time zone settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## CAS CLI Commands for Cisco NAC Profiler

Table 4-2 lists CLI commands issued on the CAS for the Cisco NAC Profiler Collector service. Refer to the [Cisco NAC Profiler Installation and Configuration Guide](#) for complete details on the Cisco NAC Profiler solution.



### 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 4-2 Cisco NAC Profiler Collector CLI Commands for CAS**

| Command                               | Description                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>service collector start</code>  | Starts the Collector service on the CAS.                                                                                                                                                                                                                                                                                                                            |
| <code>service collector stop</code>   | Shuts down the Collector service on the CAS.                                                                                                                                                                                                                                                                                                                        |
| <code>service collector status</code> | Displays the running status of the individual Collector modules on the CAS, for example:<br><br>Profiler Status<br><ul style="list-style-type: none"> <li>o Server Not Installed</li> <li>o Forwarder Running</li> <li>o NetMap Running</li> <li>o NetTrap Running</li> <li>o NetWatch Running</li> <li>o NetInquiry Running</li> <li>o NetRelay Running</li> </ul> |

Table 4-2 Cisco NAC Profiler Collector CLI Commands for CAS

| Command                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>service collector restart</code> | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>service collector config</code>  | <p>Starts the Collector service configuration script to allow communication with the Cisco NAC Profiler Server. For example:</p> <pre>[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</pre> <p>For detailed installation and configuration information, see the <a href="#">Cisco NAC Profiler Installation and Configuration Guide</a>.</p> |

## CAM/CAS Connectivity Across a Firewall

See the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1\(2\)](#) for details on which ports to open in a firewall to allow communication between the Clean Access Manager and Clean Access Server(s).

## 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.

Configuring Additional NIC Cards

The Configuration Utility script assumes that the CAM and CAS machines come with `eth0` (NIC1) and `eth1` (NIC2) interfaces by default and allows 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 Clean Access Server 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, 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 eth<n>` (where `<n>` is the interface number). For example, `<n>` will be 2 if adding a NIC to a system that already has two built-in Ethernet interfaces; therefore, you would type:

```
ifconfig eth2
```

Step 2 You should see information about the interface including MAC address, transmit and receive counters. This means the interface has been 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` 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.

Step 7 The network interface is now ready to be used for HA.

**Note**

See [CAS High Availability Requirements, page 14-4](#) for additional details.

Troubleshooting the Installation

**Note**

For further troubleshooting information, see the latest version of the [Release Notes](#).

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 the Clean Access Server Configuration

If incorrect network, shared secret, 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 [Chapter 5, “Configuring CAS Managed Network.”](#)
