



CHAPTER 2

Installing the Clean Access Manager

This chapter describes how to install and set up the Cisco NAC Appliance - Clean Access Manager. Topics include:

- [Overview, page 2-1](#)
- [Set Up the Clean Access Manager NAC Appliance, page 2-2](#)
- [Access the CAM Over a Serial Connection, page 2-4](#)
- [Install the Clean Access Manager Software from CD-ROM, page 2-5](#)
- [Perform the Initial Configuration, page 2-7](#)
- [Using the Command Line Interface \(CLI\), page 2-10](#)
- [Troubleshooting Network Card Driver Support Issues, page 2-11](#)
- [Cisco NAC Appliance Connectivity Across a Firewall, page 2-12](#)
- [Access the CAM Web Console, page 2-14](#)

Overview

The Cisco NAC Appliance is a Linux-based network hardware appliance.

Cisco NAC Appliance software is distributed as an installation CD-ROM that will install either the Clean Access Manager or Clean Access 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. Once the software is installed (either CAM or CAS) on a dedicated server, the Cisco NAC Appliance does not support the installation of any other packages or applications onto a CAS or CAM.

If you received the Clean Access Manager on a distribution CD-ROM, you will need to install it on the target machine as follows:

-
- Step 1** Physically connect the server machine to the network.
 - Step 2** Connect a monitor and keyboard to the server, or connect to the server from a workstation with a serial cable.
 - Step 3** For the CD-ROM installation, mount the CD-ROM and run the installation program.
 - Step 4** Perform the initial configuration of the server. For the CD-ROM installation, the server's initial configuration is part of the installation procedure.
-

The following sections describe the installation steps. When finished, you will be able to administer the installed components through the web-based administration console.

**Tip**

Install the Clean Access Server (CAS) first, prior to installing the Clean Access Manager (CAM), to quickly continue to web admin console configuration after CAM installation. See the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(1\)](#) for details on CAS installation.

**Caution**

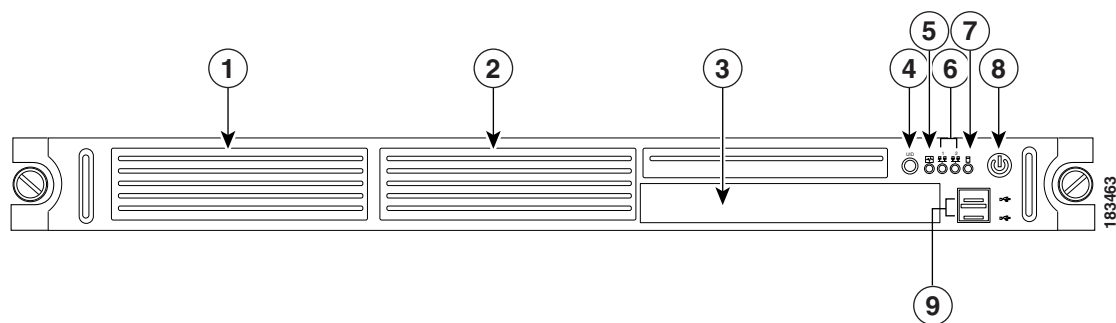
Cisco NAC Appliance (Cisco Clean Access) software is not intended to coexist with other software or data on the target machine. The installation process formats and partitions the target hard drive, destroying any data or software on the drive. Before starting the installation, make sure that the target machine does not contain any data or applications that you need to keep.

Set Up the Clean Access Manager NAC Appliance

These instructions describe how to set up the Clean Access Manager on the CCA-3140-H1 Cisco Clean Access 3140 Appliance server hardware. If you are using different hardware, the connectors on your machine may not match those shown. If needed, refer to the documentation that came with your server machine to find the serial and Ethernet connectors equivalent to those described here.

1. The Clean Access Manager server uses one of the two 10/100/1000BASE-TX interface connectors on the back panel. Connect the network interface (number 7 in [Figure 2-3](#)) on the server machine to your local area network (LAN) with a CAT5 Ethernet cable.
2. Connect the power by plugging one end of the AC power cord into the back of the server machine and the other end into an electrical outlet.
3. Power on the server machine by pressing the power button on the front of the server. 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.

Figure 2-1 Front View— CCA-3140-H1



1	1-inch Non-Hot Plug SATA or SCSI Hard Drive Bay	6	NIC activity LEDs
2	1-inch Non-Hot Plug SATA or SCSI Hard Drive Bay	7	Disc activity LED
3	Optional CD-ROM or DVD drive	8	Power Switch

4	UID LED	9	USB ports
5	System Health Monitor LED		

Figure 2-2 Front View Detail— CCA-3140-H1

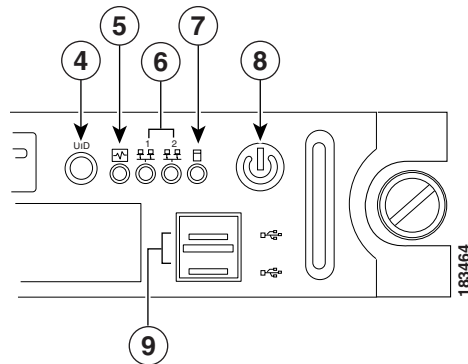
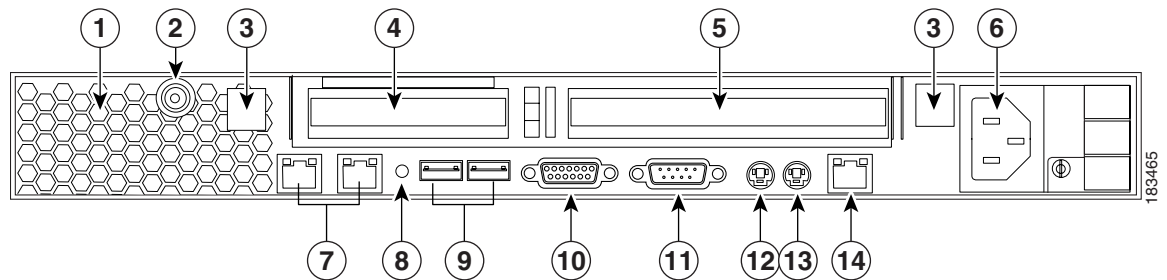


Figure 2-3 Back View— CCA-3140-H1



1	Ventilation holes	8	UID button with LED indicator (blue) This button mirrors the function of the UID button located on the front panel.
2	Thumbscrew for the top cover	9	USB 2.0 ports (black)
3	Thumbscrews for the PCI riser board assembly	10	Video port (blue)
4	Low profile 64-bit/133 MHz PCI-X riser board slot cover	11	Serial port (teal)
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 for NIC 1 (eth0) on the left-hand side and NIC 2 (eth1) on the right-hand side (RJ-45).	14	10/100 Mbps LAN port for IPMI management (RJ-45)



Note

The CCA-3140-H1 Cisco Clean Access NAC Appliance is based on the HP ProLiant DL140 G2 server.

Access the CAM Over a Serial Connection

To install the Clean Access Manager software from CD-ROM or to perform its initial configuration, you will need to access the server's command line. This can be done in one of two ways:

1. Connect a monitor and keyboard directly to the server machine via the keyboard connector and video monitor/console connector on the back panel, or
2. Connect a serial cable from an external workstation (PC/laptop) to the server machine and open a serial connection using terminal emulation software (such as HyperTerminal or SecureCRT) on the external workstation.

This section describes how to access the server over a serial connection.



Note

The steps described here for accessing the server directly through a serial connection can be used later for troubleshooting. If the server cannot be reached through the web admin console, you can serially connect to the server to restore the server to a reachable state, usually by correcting its network settings.

To use a serial connection, first connect the computer you will be using as the admin workstation 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 can use an Ethernet port for the peer connection. For more information, see [Chapter 15, "Configuring High Availability \(HA\)."](#)

After physically connecting the workstation to the server, you can 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.

To set up the HyperTerminal connection:

1. Click **Start > Programs > Accessories > Communications > HyperTerminal** to open the HyperTerminal window.
2. Type a name for the session and click **OK**:



3. 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.



4. Configure the **Port Settings** as follows:
 - Bits per second – 9600
 - Data bits – 8
 - Parity – None
 - Stop bits – 1
 - Flow control – None
5. Go to **File > Properties** to open the Properties dialog for the session. Change the **Emulation** setting to:
 - **Emulation**– VT100

You should now be able to access the command interface for the server. You can now:

- [Install the Clean Access Manager Software from CD-ROM, page 2-5](#)
- [Perform the Initial Configuration, page 2-7](#)



Note

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

Install the Clean Access Manager Software from CD-ROM

This section describes how to install the Clean Access Manager software from the distribution CD-ROM. It is assumed that you have already connected the server to the network, as described in [Set Up the Clean Access Manager NAC Appliance, page 2-2](#) and are working on the server from either a console or over a serial connection.



Caution

The Clean Access Manager 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 2-7](#) should take about 15 minutes.

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



Note The Cisco NAC-3390 Super Manager appliance requires its own .iso installer.

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

```
Cisco Clean Access 4.1-1 Installer (C) 2007 Cisco Systems, Inc.
```

```
Welcome to the Cisco Clean Access 4.1-1 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:
```

3. Depending on your specific NAC Appliance platform and type of connection, at the “boot:” prompt:

For Cisco NAC-3350 and Cisco NAC-3390:

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

For Cisco NAC-3310:

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



Note If you are installing system software on a NAC-3310 Appliance, ensure you note the special instructions defined in [Perform the Initial Configuration, page 2-7](#).

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, 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



Caution

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

5. 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, and a series of questions prompt you for the initial server configuration, as described in the next section, [Configuration Utility Script, page 2-8](#).

If after installation you need to reset the configuration settings for the Clean Access Manager (such as the eth0 IP address), you can modify these values by connecting to the Clean Access Manager machine serially or via SSH and running the `service perfigo config` command. See [Using the Command Line Interface \(CLI\), page 2-10](#) for details.



Note

Most other settings can also be modified later from the web admin console.

Perform the Initial Configuration

When installing the Clean Access Manager from CD-ROM, the [Configuration Utility Script](#) automatically appears after the software packages install to prompt you for the initial 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 2-10](#).

Configuration Utility Script

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

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

```
Welcome to the Cisco Clean Access Manager quick configuration utility.
Note that you need to be root to execute this utility.
The utility will now ask you a series of configuration questions.
Please answer them carefully.
Cisco Clean Access Manager, (C) 2006 Cisco Systems, Inc.
```

2. You are first prompted for the IP address of the interface eth0:

```
Configuring the network interface:
Please enter the IP address for the interface eth0 [10.0.2.15]: 10.201.240.11
You entered 192.168.151.2 Is this correct? (y/n)? [y]
```

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

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

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

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

```
Please enter the IP address for the default gateway [192.168.151.1]
```

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

```
Please enter the hostname [camanager]:
```

6. Specify the IP address of the Domain Name System (DNS) server in your environment or accept the default at the following prompt:

```
The nameserver(s) is currently set to nameserver [192.168.1.1] Would you like to
change this setting? (y/n)?
```

```
Please enter the IP address for the nameserver:
```

7. 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. The default shared secret is **cisco123**. Type and confirm the shared secret at the prompts.



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.

8. Specify the time zone in which the Clean Access Manager is located as follows:

- a. Choose your region from the continents and oceans list. Type the number next to your location on the list, such as **2** for the Americas, and press enter. Enter 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 appear.
 - d. Choose the appropriate time zone region from the list and press enter (for example, **16** for Pacific Time).
 - e. Confirm your choices by entering **1**, or use **2** to cancel and start over.
9. Now configure the SSL security certificate that enables secure connections between the Clean Access Manager and the web-based admin console as follows:

- a. At the following prompt:

```
Enter fully qualified domain name or IP [192.168.1.2]
```

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 (this will normally be the eth0 IP address you already specified).

**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, `information services` or `engineering`).
 - 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`), and press enter.
 - d. Type the name of the city or county in which your organization is legally located, and press enter.
 - e. Enter the two-character state code in which the organization is located, such as `CA` or `NY`, and press enter.
 - f. Type the two-letter country code, such as `us`, and press enter.
 - g. A summary of the values you entered appears. Press enter to accept the values or **n** to start over.
10. Configure the `root` user password for the installed Linux operating system of the Clean Access Manager. The default password is `cisco123`. The `root` user account is used to access the system over a serial connection or through SSH.

Although password rules are not enforced, it is advised that you use strong passwords (for example, at least 6 characters, mixed letters and numbers, etc.), to reduce the vulnerability of your network to password guessing attacks.

**Note**

The default username/password is `admin/cisco123` to access the Clean Access Manager web admin console (the primary administration interface for Cisco NAC Appliance). Passwords for web admin console users (including default user `admin`) are configured through the web console. See [Manage System Passwords, page 14-30](#) for details.

11. When performing a CD install, the following message appears after configuration is complete:

Install has completed. Press <ENTER> to reboot.

- a. If installing from CD, press the Enter key to reboot the server.
- b. If running the configuration script via `service perfigo config`, you must execute the following command to reboot the machine after configuration is complete:

```
# service perfigo reboot
```

After restarting, the CAM is accessible through the web console, as described in [Access the CAM Web Console, page 2-14](#).

- For the commands to manually stop and start the CAM, see [Using the Command Line Interface \(CLI\), page 2-10](#)
- For network card configuration issues, see [Troubleshooting Network Card Driver Support Issues, page 2-11](#).

Important Notes for SSL Certificates

- You must generate the SSL certificate during CAM installation or you will not be able to access your server as an end user.
- 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 CAM, see:
 - [Set System Time, page 14-4](#)
 - [Manage CAM SSL Certificates, page 14-5](#)
 - For details on the CAS, see the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1)*.
- 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 the web user during admin login).

Using the Command Line Interface (CLI)

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

To run the CLI commands, access the server 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 [Access the CAM Over a Serial Connection, page 2-4](#)). The format `service perfigo <command>` is used to enter a command from the command line. [Table 2-1](#) lists the commonly used Cisco NAC Appliance CLI commands.

Table 2-1 CLI Commands

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 Cisco NAC Appliance service.
<code>service perfigo restart</code>	Shuts down the Cisco NAC Appliance service and starts it up again. This is used when the service is already running and you want to restart it. Note <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> and <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.
<code>service perfigo time</code>	Use to modify the time zone settings.

Power Down the CAM

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

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

Restart Initial Configuration

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

This command causes the configuration utility script to start (on either the CAS or CAM). The script lets you configure the network settings for the server (see [Perform the Initial Configuration, page 2-7](#) for instructions). After running and completing `service perfigo config`, make sure to run `service perfigo reboot` or `reboot` to reset the server with the modified configuration settings.

**Note**

For details on restoring the database from automated and manual backup snapshots via command line utility, see [Database Recovery Tool, page 14-35](#).

Troubleshooting Network Card Driver Support Issues

For complete details, refer to the “Troubleshooting Network Card Driver Support Issues” section of the [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#).

Cisco NAC Appliance Connectivity Across a Firewall

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

[Table 2-2](#) shows the ports that are required for communication between the CAS and the CAM (per version of Cisco NAC Appliance).

Table 2-2 Port Connectivity for CAM/CAS

CCA Version	Required Ports
4.1(x) 4.0(x)	TCP ports 443, 1099, and 8995~8996
3.6(x)	TCP ports 80, 443, 1099, and 8995~8996
3.5(x)	TCP ports 80, 443, 1099, and 32768~61000 (usually 32768~32999 are sufficient).

For Single Sign-On (SSO) capabilities, other ports must be open on the CAS and firewall (if any) to allow communication between the Agent and the Active Directory Server, as shown in [Table 2-3](#).

[Table 2-3](#) lists the devices on which you must open ports so that the Cisco NAC Appliance can function properly, the communicating devices, the ports affected, and the purpose of each port.

Table 2-3 Port Usage

Device	Communicating Devices	Ports to Open	Purpose
Firewall, if any	CAM and CAS	TCP 8995, 8996 TCP 1099	Java Management Extensions (JMX) communication between the CAM and CAS, such as pre-connect and connect messages.
		TCP 443	HTTP over Secure Sockets Layer (SSL) communication between Agent/CAS/CAM, such as end user machine remediation via the Agent.
		TCP 80 (for version 3.6.x and earlier)	HTTP communication between Agent/CAS/CAM. Used to download the Agent from the CAM to an end user machine.
	CAS and Agent	UDP 8905, 8906	SWISS, a proprietary CAS-Agent communication protocol used by the Agent for UDP discovery of the CAS. UDP 8905 is used for Layer 2 discovery; and 8906 is used for Layer 3 discovery.
		TCP 8910	Microsoft Active Directory lookup to facilitate Active Directory Single Sign-On (AD SSO).
		TCP 443	HTTP over SSL communication between Agent/CAS/CAM, such as for user redirection to a web login page.
		TCP 80 (for version 3.6.x and earlier)	HTTP communication between Agent/CAS/CAM. Used to download the Agent from the CAM to an end user machine.
CAS and firewall (if any)	Agent and Active Directory (AD) Server	TCP 88, 135, 389, 1025, 1026 UDP 88, 389	<p>AD SSO requires the following ports to be open:</p> <ul style="list-style-type: none"> • TCP 88 (Kerberos) • TCP 135 (RPC) • TCP 389 (LDAP) or TCP 636 (LDAP with SSL) • TCP 1025 (RPC)–non-standard • TCP 1026 (RPC)–non-standard <p>If it is not known whether the AD server is using Kerberos, you must open the following UDP ports instead:</p> <ul style="list-style-type: none"> • UDP 88 (Kerberos) • UDP 389 (LDAP) or UDP 636 (LDAP with SSL) <p>Note If your deployment requires LDAP services, use TCP/UDP port 636 (LDAP with SSL encryption) instead of TCP/UDP port 389 (plain text).</p> <p>For more information on AD SSO, see Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide.</p>

Access the CAM Web Console

The Clean Access Manager web administration console is the web interface for administering the Cisco NAC Appliance deployment. The CAM includes a preconfigured web server, so you do not have to set up a web server to start using the web console.



Warning

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

- Step 1** Launch a web browser from a computer accessible to the Clean Access Manager by network. The web console supports Internet Explorer 6.0 or 7.0.
- Step 2** In the URL field, type the IP address of the CAM (or host name if you have made the required entry in your DNS server).
- Step 3** If using a temporary SSL certificate, click **Yes** at the security alert prompt to accept the certificate. (If using signed certificates, this security dialog does not appear.)
- Step 4** The **Clean Access Manager License Form** (Figure 2-4) appears and prompts you to install your CAM FlexLM license file. For reference, the top of the form displays the CAM's eth0 MAC address.

Figure 2-4 Clean Access Manager License Form

Clean Access Manager License Form

The product license for this installation (MAC Address: 00:30:48:80:43:D6) is either invalid, expired, or not yet set. Please choose the correct license that you will need:

Product Evaluation: If you are evaluating the CCA product, please visit the [Cisco Technical Support site](#) to register and obtain an evaluation product license. Once this is complete you will receive a license key via email which must be saved to a text file. Enter the license file name in the input box below (use the Browse button to navigate to the text file) and hit the Install License button.

Product Authorization Key (PAK): If you have received a Product Authorization Key (PAK) with your purchase, please visit the [Cisco Technical Support](#) site to register and obtain the proper product license. Note: During the registration process, you will be asked for the MAC address from one or more of your systems, please have this information ready. Once this is complete, you will receive a license key via email which must be saved to a text file. Enter the license file name in the input box below (use the Browse button to navigate to the text file) and hit the Install License button:

Clean Access Manager License File

Non PAK: If you didn't receive a PAK with your purchase, then you must email Cisco Licensing at licensing@cisco.com for a product license key. Please include your sales order number, MAC address of the Clean Access Manager and Servers in your email. Once you get the product license key, enter this information below:

Enter Product License:

Re-Enter Product License:

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

**Note**

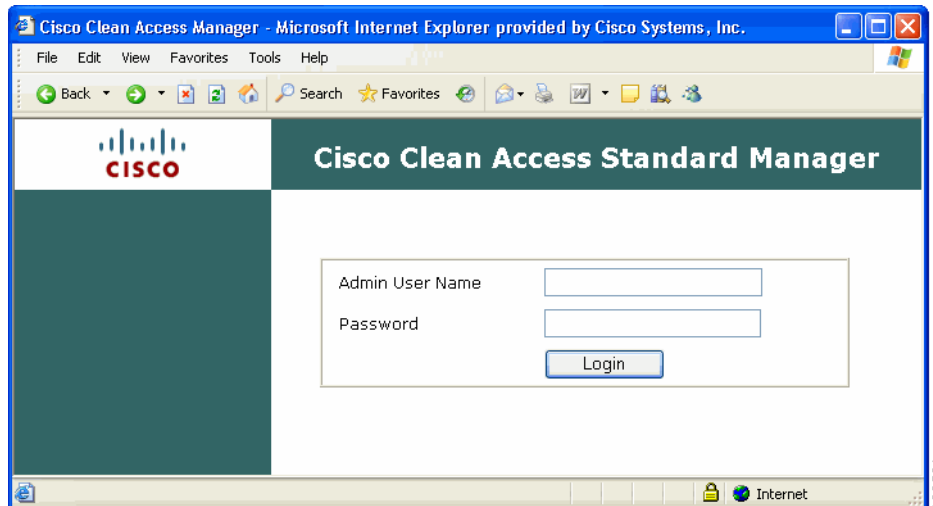
Refer to [Cisco NAC Appliance Service Contract / Licensing Support](#) for complete step-by-step instructions for how to obtain and install product licenses and obtain service contract support for Cisco NAC Appliances.

**Caution**

Cisco recommends obtaining a permanent license before continuing with full-scale deployment. Evaluation licenses are intended for trial purposes and expire after 30 days. Once a license expires, you cannot start Cisco NAC Appliance. Contact a Cisco representative to purchase a permanent license.

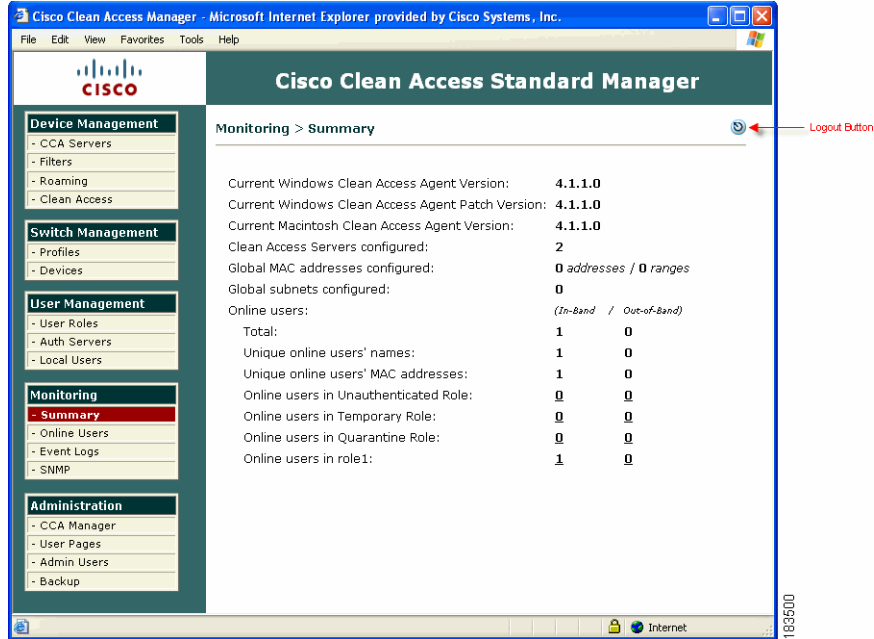
12. Once the license is accepted, the web admin console login window appears (Figure 2-5). Type the username **admin** and default web admin user password **cisco123**, and click **Login**.

Figure 2-5 CAM Web Admin Console Login Page



13. The **Monitoring** summary page and left-hand navigation pane displays (Figure 2-6). You can now configure your deployment through the modules of the web admin console.

Figure 2-6 Monitoring Summary Page



To log out of the web admin console, either click the **Logout** button or close the browser. For further details on creating different levels of admin users for the web console, see [Admin Users](#), page 14-23.