CANAC

Implementing Cisco NAC Appliance

Volume 2

Version 2.1

Student Guide

Editorial, Production, and Web Services: 02.26.07

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.**

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Volume 2

Module 5

Cisco NAC Appliance Monitoring and Administration

Overview

Network security administrators need an easy way to manage their Cisco Network Admission Control (NAC) Appliance deployment. Whether you are in an enterprise network environment or in a medium-sized business, you can manage Cisco NAC Appliance using a web-based administration console. This module describes how to use the web-based administration console to monitor online users and to automatically generate system statistics for each Cisco NAC Appliance Server (Cisco NAS). In this module, you will learn how to configure the Simple Network Management Protocol (SNMP) so that you can use a third-party SNMP management tool. This module also describes how to update your system and back up your configurations. The administration and maintenance tasks described in this module define the ongoing work necessary to ensure a secure and reliable Cisco NAC Appliance solution.

Module Objectives

Upon completing this module, you will be able to maintain a highly available Cisco NAC Appliance deployment in medium-sized and enterprise network environments. This ability includes being able to meet these objectives:

- Monitor the operational information of a Cisco NAC Appliance deployment using the Cisco NAM
- Describe how to manage a Cisco NAC Appliance deployment

Lesson 1

Monitoring a Cisco NAC Appliance Deployment

Overview

The ability to monitor the operational status of a Cisco Network Admission Control (NAC) Appliance deployment is a requirement for network system engineers managing a Cisco NAC Appliance solution. This lesson describes how to monitor the operational information of a Cisco NAC Appliance deployment using the NAC Appliance Manager (Cisco NAM) web-based administration console.

Objectives

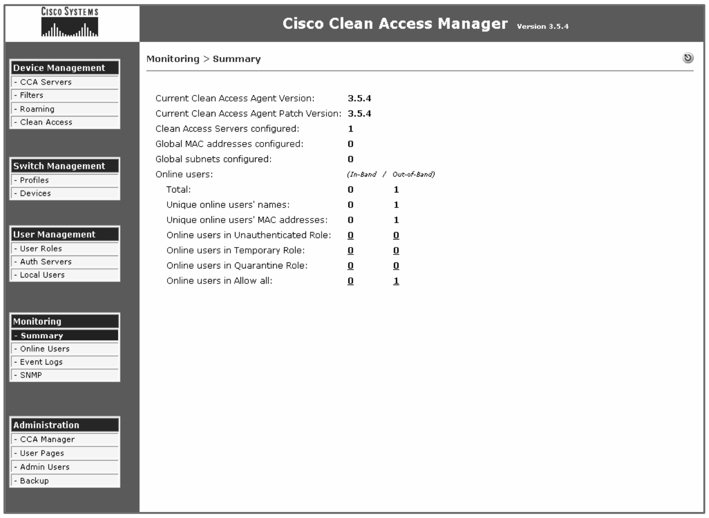
Upon completing this lesson, you will be able to monitor the operational information of a Cisco NAC Appliance deployment using the Cisco NAM. This ability includes being able to meet these objectives:

- Describe how to monitor Cisco NAC Appliance activities
- Describe how to use the Online Users page to monitor online users
- Describe how to use the web-based administrative console to monitor event logging

Introducing Cisco NAC Appliance Monitoring

This topic describes how to monitor Cisco NAC Appliance activities. The Cisco NAM monitoring pages provide operational information on your deployment, including statistics on user activity, syslog events, network configuration changes, and basic Simple Network Management Protocol (SNMP) polling and alerts. Online user activity, event logs, and SNMP information is available under the Cisco NAM monitoring menu.

Introducing Monitoring



Monitoring > Summary

```
Current Clean Access Agent Version:        3.5.4
Current Clean Access Agent Patch Version:  3.5.4
Clean Access Servers configured:           1
Global MAC addresses configured:           0
Global subnets configured:                 0
Online users:                              (In-Band  /  Out-of-Band)
   Total:                                  0            1
   Unique online users' names:             0            1
   Unique online users' MAC addresses:     0            1
   Online users in Unauthenticated Role:   0            0
   Online users in Temporary Role:         0            0
   Online users in Quarantine Role:        0            0
   Online users in Allow all:              0            1
```

CANAC v2.1—5-2

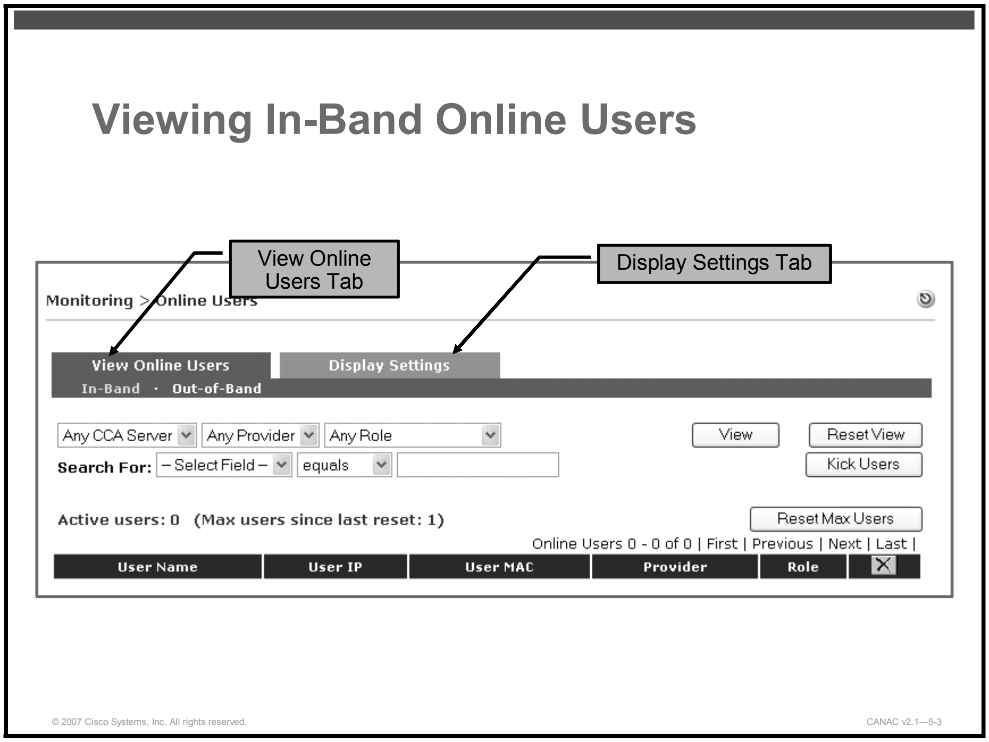
Access the Cisco NAM and choose **Monitoring > Summary**. The Monitoring > Summary Statistics table summarizes the important statistics that are shown in the figure.

Monitoring > Summary Statistics

Item	Description
Current Clean Access Agent Version	The current version of the NAC Appliance Agent (Cisco NAA) installed with the Cisco NAM software or manually uploaded (reflects the contents of the Version field)
Current Clean Access Agent Patch Version	The latest Cisco NAA patch downloaded to the Cisco NAM and NAC Appliance Servers (Cisco NASs) and available for automated client upgrade
Clean Access Servers Configured	The number of Cisco NASs configured in the Cisco NAS management pages for the Cisco NAM domain
Global MAC addresses Configured	The number of addresses currently in the MAC and IP passthrough lists
Global Subnets Configured	The number of subnet addresses currently in the subnet-based passthrough list
Online Users (In-Band/Out-of-Band)	These entries list: ■ Total number of in-band and out-of-band online user names ■ Total number of in-band and out-of-band online MAC addresses ■ Number of in-band and out-of-band online users per user role **Note:** Per-role user totals are links to the Monitoring > Online Users > View Online Users page. Clicking a link displays the in-band or out-of-band online user list for the particular role.

Monitoring Online Users

This topic describes how to use the Online Users page to monitor online users.



Viewing In-Band Online Users

Active users: 0 (Max users since last reset: 1)

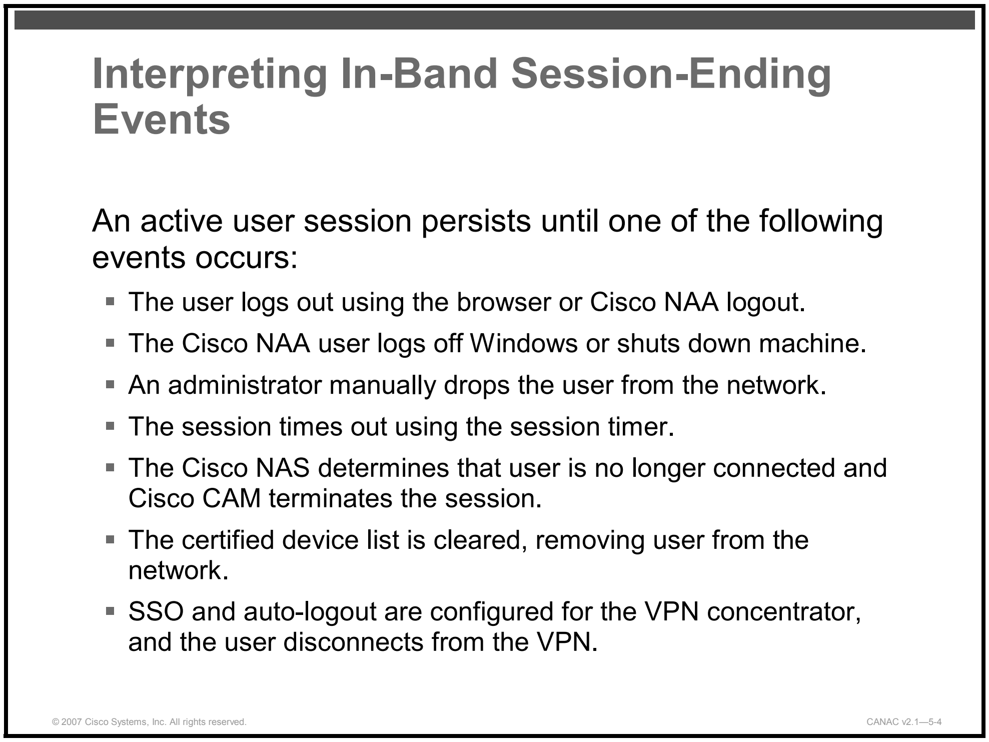
CANAC v2.1—5-3

There are two main tabs in the Monitoring > Online Users page to help you monitor online users: the View Online Users tab and the Display Settings tab. Each of the tabs provides an option to display or configure either in-band or out-of-band online user information.

The figure shows the View Online Users form for in-band users. The in-band online users list tracks all in-band users that are logged onto the Cisco NAC Appliance network at the time that the list is generated. After a user logs onto the network through a web login or through the Cisco NAA, the Cisco NAM adds a client IP and MAC address (if available) to this list. Removing a user from the online users list logs the user off the in-band network.

By default, the View Online Users form displays the login username, IP and MAC address (if available), provider, role of each user, Cisco NAS, VLAN, operating system, and login time. A green background for an entry indicates that a user device is accessing the Cisco NAC Appliance network in a temporary role. The temporary role can be a quarantine role or the configured Cisco NAA temporary role. A device listed on the View Online Users form but not in the Cisco NAC Appliance certified device list generally indicates that the device is in the process of certification. You can find a description of each of the columns in the In-Band monitoring form by choosing the In-Band option on the Display Settings form.

Note For a complete description of the functions of the buttons on the Monitoring > Online Users form, refer to the View Online Users section in the *Cisco NAC Appliance - Cisco Clean Access Manager Installation and Administration Guide.*



Interpreting In-Band Session-Ending Events

An active user session persists until one of the following events occurs:

- The user logs out using the browser or Cisco NAA logout.
- The Cisco NAA user logs off Windows or shuts down machine.
- An administrator manually drops the user from the network.
- The session times out using the session timer.
- The Cisco NAS determines that user is no longer connected and Cisco CAM terminates the session.
- The certified device list is cleared, removing user from the network.
- SSO and auto-logout are configured for the VPN concentrator, and the user disconnects from the VPN.

CANAC v2.1—5-4

After logging onto the in-band Cisco NAC Appliance network, a user continues in an active user session until an event occurs that ends the in-band session. The In-Band Session Events table lists the events that signal the end of an in-band session.

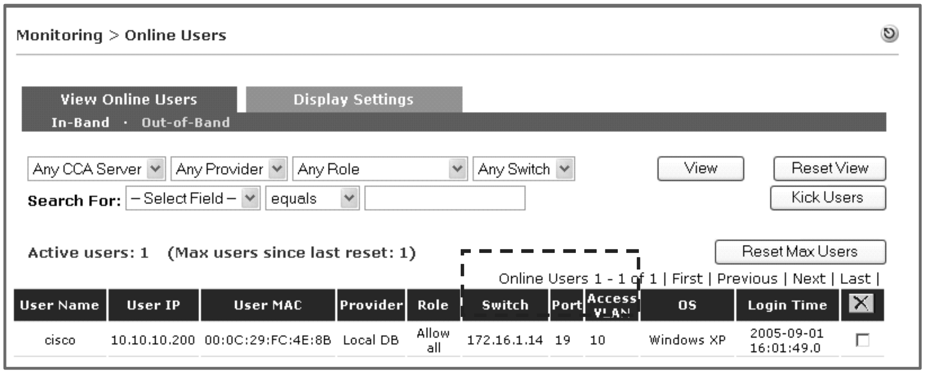
In-Band Session Events

Event	Description
The user logs out of the network through the browser logout page or Cisco NAA logout.	Once on the network, users can remain logged in after a computer shutdown and restart. A user can log out of the network using the web logout page or Cisco NAA logout.
The Cisco NAA user logs out of Windows or shuts down a Windows machine.	You can configure the Cisco NAM and Cisco NAA to log out in-band users only from the Cisco NAC Appliance when the user logs out from the Windows domain or shuts down the machine.
An administrator manually drops the user from the network.	The Monitoring > Online Users > View Online Users page (in-band or out-of-band) can be used to drop users from the network without deleting their clients from the certified list.
The session times out using the session timer.	The session timer works the same way for multihop Layer 3 (in-band) deployments as for Layer 2 (in-band or out-of-band) deployments and is set in User Management > User Roles > Schedule > Session Timer. The session timer is set per user role and logs off any user in the selected role from the network after the configured time has elapsed.

Event	Description
The Cisco NAS uses the heartbeat timer to determine that the user is no longer connected, and the Cisco NAM terminates the session.	The heartbeat timer applies to Layer 2 in-band deployments only and is set for all users regardless of the user role. The heartbeat timer can be set globally for all Cisco NASs using the form User Management > User Roles > Schedule > Heartbeat Timer. The heartbeat timer can be set for a specific Cisco NAS using the local form Device Management > CCA Servers > Manage [Cisco NAS_IP] > Misc > Heartbeat Timer. The heartbeat timer does not function in Layer 3 deployments and does not apply to out-of-band users. However, the heartbeat timer will work if the Cisco NAS is the first hop behind the VPN concentrator. This is because the VPN concentrator responds to Address Resolution Protocol (ARP) queries for the IP addresses of its current tunnel clients.
The certified device list is cleared (automatically or manually) and the user is removed from the network.	The certified list applies to Layer 2 (in-band or out-of-band) deployments only and can be scheduled to be cleared automatically and periodically using the global certified devices timer form (Device Management > Clean Access > Certified Devices > Timer). You can manually clear the certified devices for a specific Cisco NAS from the certified list using the local form Device Management > CCA Servers > Manage [Cisco NAS_IP] > Filters > Clean Access > Certified Devices, or manually clear the certified device list across all Cisco NASs using the Device Management > Clean Access > Certified Devices global form. Since remote virtual private network (VPN) and Layer 3 client sessions are IP-based rather than MAC address-based, the certified device list will not display VPN and Layer 3 client sessions.
Single sign-on (SSO) and auto-logout are configured for the VPN concentrator, and the user disconnects from the VPN.	With auto-logout enabled, when the user disconnects from the VPN client, the user is automatically removed from the online users list (in-band). When SSO is configured for multihop Layer 3 VPN concentrator integration, if the user session on the Cisco NAS times out but the user is still logged in on the VPN concentrator, the user will be able to log back into the Cisco NAS without providing a username and password.

Note Whether the Cisco NAS or another server is used for DHCP, if a user DHCP lease expires, the user remains on the Online Users list (in-band or out-of-band). When the lease expires, the client machine will try to renew the lease.

Viewing OOB Online Users



Any CCA Server | Any Provider | Any Role | Any Switch

Search For: – Select Field – | equals

Active users: 1 (Max users since last reset: 1)

User Name	User IP	User MAC	Provider	Role	Switch	Port	Access VLAN	OS	Login Time	☒
cisco	10.10.10.200	00:0C:29:FC:4E:8B	Local DB	Allow all	172.16.1.14	19	10	Windows XP	2005-09-01 16:01:49.0	□

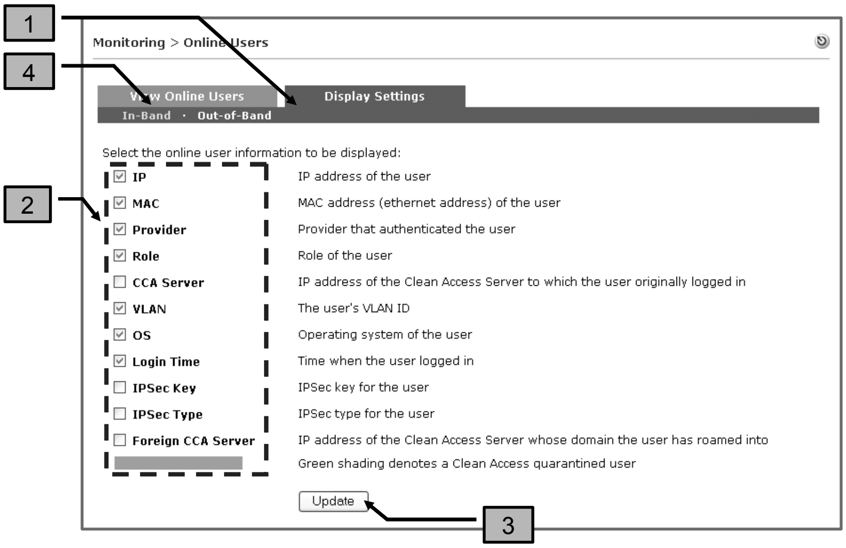
The figure shows the View Online Users page for out-of-band users. The Out-of-Band Online Users list tracks all out-of-band authenticated users that are on the access VLAN (that is, users who are on the trusted network). The Cisco NAM adds a client MAC address to the out-of-band online users list after the client is switched to the access VLAN. You can find a description of each of the columns in the in-band monitoring form by selecting the Out-of-Band submenu on the Display Settings form.

Recall that when an in-band user is removed from the list, the online users list logs the user out of the in-band network. When a user is removed from the out-of-band online users list, these three events occur:

1. The Cisco NAM toggles the switch port off and on.
2. The switch resends SNMP traps to the Cisco NAM.
3. The Cisco NAM changes the VLAN of the port based on the configured Port Profile associated with this controlled port.

Note Removing an out-of-band user from the certified list also removes the user from the out-of-band online users list and bounces the switch port.

Configuring In-Band Display Settings



Select the online user information to be displayed:

☑ IP	IP address of the user
☑ MAC	MAC address (ethernet address) of the user
☑ Provider	Provider that authenticated the user
☑ Role	Role of the user
□ CCA Server	IP address of the Clean Access Server to which the user originally logged in
☑ VLAN	The user's VLAN ID
☑ OS	Operating system of the user
☑ Login Time	Time when the user logged in
□ IPSec Key	IPSec key for the user
□ IPSec Type	IPSec type for the user
□ Foreign CCA Server	IP address of the Clean Access Server whose domain the user has roamed into
▨	Green shading denotes a Clean Access quarantined user

CANAC v2.1—5-6

The figure shows the Display Settings form with the selections for in-band users displayed. Use this form to select which in-band information appears when the In-Band selection is made on the View Online Users form. Complete these four steps to select the information that appears on the View Online Users page:

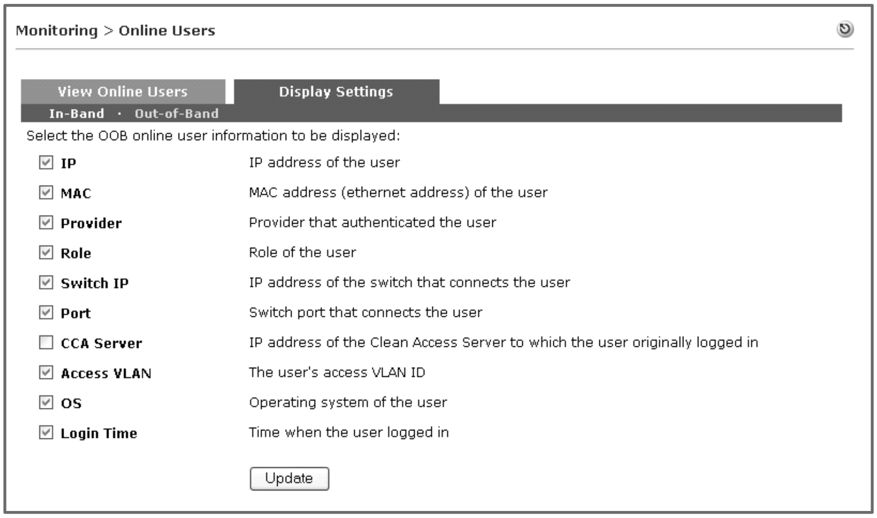
Step 1 Click the **Display Settings** tab.

Step 2 Check the check box next to the item in the list that you want to display.

Step 3 Click **Update.**

Step 4 Click the **View Online Users** tab to see the desired settings displayed.

Configuring Out-of-Band Display Settings



Monitoring > Online Users

Select the OOB online user information to be displayed:

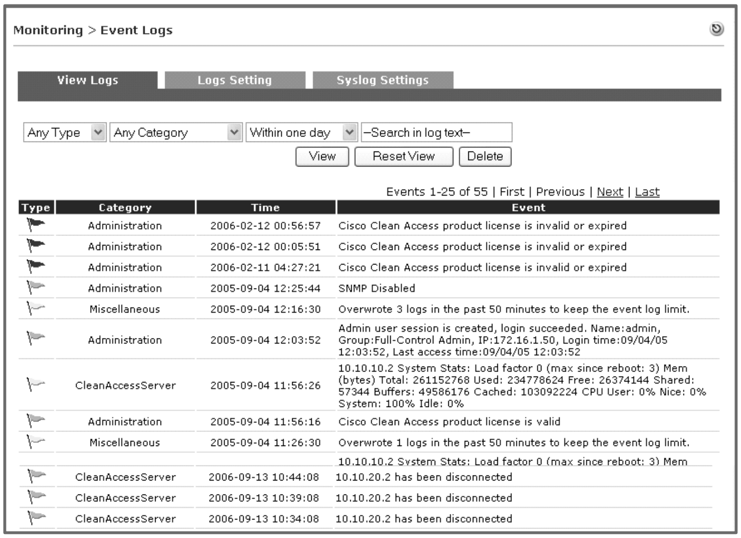
☑ **IP**	IP address of the user
☑ **MAC**	MAC address (ethernet address) of the user
☑ **Provider**	Provider that authenticated the user
☑ **Role**	Role of the user
☑ **Switch IP**	IP address of the switch that connects the user
☑ **Port**	Switch port that connects the user
☐ **CCA Server**	IP address of the Clean Access Server to which the user originally logged in
☑ **Access VLAN**	The user's access VLAN ID
☑ **OS**	Operating system of the user
☑ **Login Time**	Time when the user logged in

The figure shows the Display Settings form for out-of-band users. Use this form and the four steps from the previous in-band settings example to select which out-of-band information appears when the Out-of-Band selection is made on the View Online Users form.

Monitoring Event Logs

This topic describes how to use the web-based administrative console to monitor event logging.

Using the View Logs Form



Events 1-25 of 55 | First | Previous | Next | Last

Type	Category	Time	Event
⚑	Administration	2006-02-12 00:56:57	Cisco Clean Access product license is invalid or expired
⚑	Administration	2006-02-12 00:05:51	Cisco Clean Access product license is invalid or expired
⚑	Administration	2006-02-11 04:27:21	Cisco Clean Access product license is invalid or expired
⚐	Administration	2005-09-04 12:25:44	SNMP Disabled
⚐	Miscellaneous	2005-09-04 12:16:30	Overwrote 3 logs in the past 50 minutes to keep the event log limit.
⚐	Administration	2005-09-04 12:03:52	Admin user session is created, login succeeded. Name:admin, Group:Full-Control Admin, IP:172.16.1.50, Login time:09/04/05 12:03:52, Last access time:09/04/05 12:03:52
⚐	CleanAccessServer	2005-09-04 11:56:26	10.10.10.2 System Stats: Load factor 0 (max since reboot: 3) Mem (bytes) Total: 261152768 Used: 234778624 Free: 26374144 Shared: 57344 Buffers: 49586176 Cached: 103092224 CPU User: 0% Nice: 0% System: 100% Idle: 0%
⚐	Administration	2005-09-04 11:56:16	Cisco Clean Access product license is valid
⚐	Miscellaneous	2005-09-04 11:26:30	Overwrote 1 logs in the past 50 minutes to keep the event log limit.
			10.10.10.2 System Stats: Load factor 0 (max since reboot: 3) Mem
⚐	CleanAccessServer	2006-09-13 10:44:08	10.10.20.2 has been disconnected
⚐	CleanAccessServer	2006-09-13 10:39:08	10.10.20.2 has been disconnected
⚐	CleanAccessServer	2006-09-13 10:34:08	10.10.20.2 has been disconnected

The Cisco NAM View Logs form shown in the figure displays the following event information in the Event column:

- **User activity:** This entry lists information including user login times, logout times, and failed login attempts.
- **Network configuration activity:** This entry shows configuration events, including changes to the MAC or IP passthrough lists and changes to the Cisco NASs.
- **System load:** This entry includes the load for the Cisco NASs.

By default, system statistics are generated every hour for each Cisco NAS managed by the Cisco NAM. The system check timing is configured when you configure the syslog.

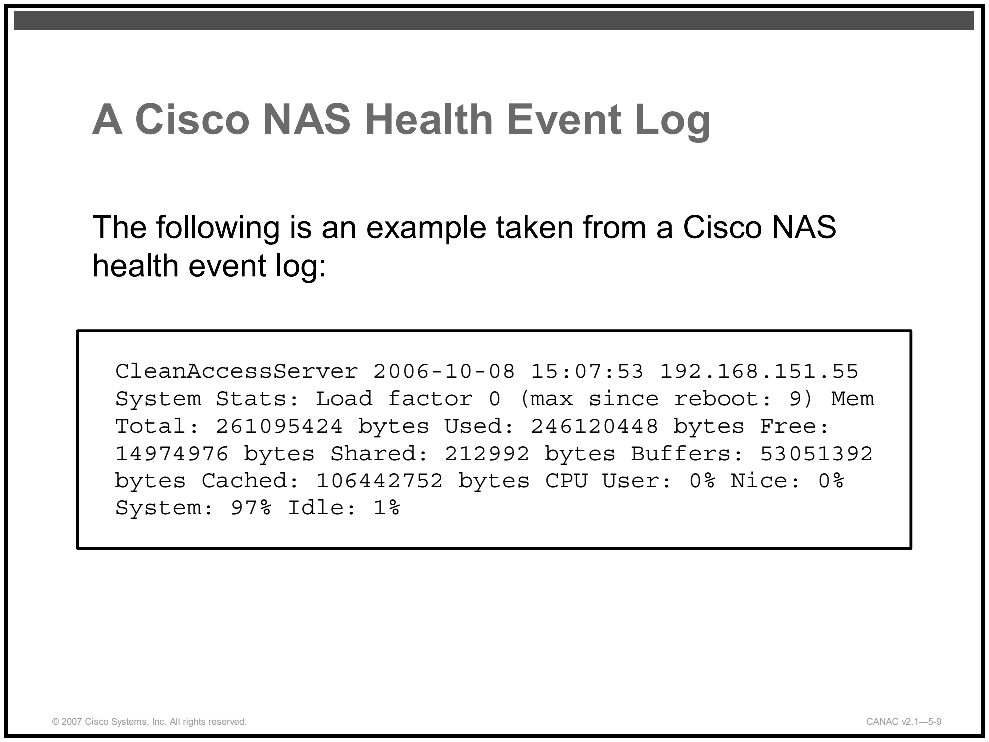
Note The most recent events appear first in the Events column.

The View Log Form Components table describes the navigation, searching capabilities, and syslog information displayed on the View Logs form.

Note At this point in the lesson, the instructor will ask you to view the event log for the lab pod you have been using. Be prepared to discuss red, yellow, and green flags.

View Log Form Components

Activity	Button	Description
Search criteria	Type	Search by Type column criteria and click **View**. ■ Any Type ■ Failure ■ Information ■ Success
	Category	Search by Category column criteria and click **View**. ■ Authentication ■ Administration ■ Client ■ Clean Access Server ■ Clean Access ■ SW_Management (if out-of-band is enabled) ■ Miscellaneous ■ DHCP
	Time	Search by the Time column criteria and click **View**. ■ Within one hour ■ Within one day ■ Within two days ■ Within one week ■ Anytime ■ One hour ago ■ One day ago ■ Two days ago ■ One week ago
	Search in log text	Enter the desired text that you want to search for and click **View**.
Controls	View	After selecting the desired search criteria, click **View** to see the results.
	Reset View	Click **Reset View** to restore the default view. Logs that were recorded within one day appear.
	Delete	Click **Delete** to remove the events filtered through the search criteria across the number of applicable pages. Clicking Delete removes filtered events from Cisco NAM storage. Otherwise, the event log persists through system shutdown. Use the filter event indicator shown to view the total number of filtered events that are subject to being deleted.
Status Display	Type	• **Red flag = Failure:** Indicates an error or otherwise unexpected event • **Green flag = Success:** Indicates a successful or normal use event, such as successful login and configuration activity • **Yellow flag = Information:** Indicates system performance information, such as load information and memory use
	Category	Indicates the module or system component that initiated the log event.
	Time	Displays the date and time (hh:mm:ss) of the event. The most recent events appear first in the list.
	Event	Displays the event for the module. The most recent events are listed first.



A Cisco NAS Health Event Log

The following is an example taken from a Cisco NAS health event log:

```
CleanAccessServer 2006-10-08 15:07:53 192.168.151.55
System Stats: Load factor 0 (max since reboot: 9) Mem
Total: 261095424 bytes Used: 246120448 bytes Free:
14974976 bytes Shared: 212992 bytes Buffers: 53051392
bytes Cached: 106442752 bytes CPU User: 0% Nice: 0%
System: 97% Idle: 1%
```

CANAC v2.1—5-9

The figure shows an example of a typical Cisco NAS health event log.

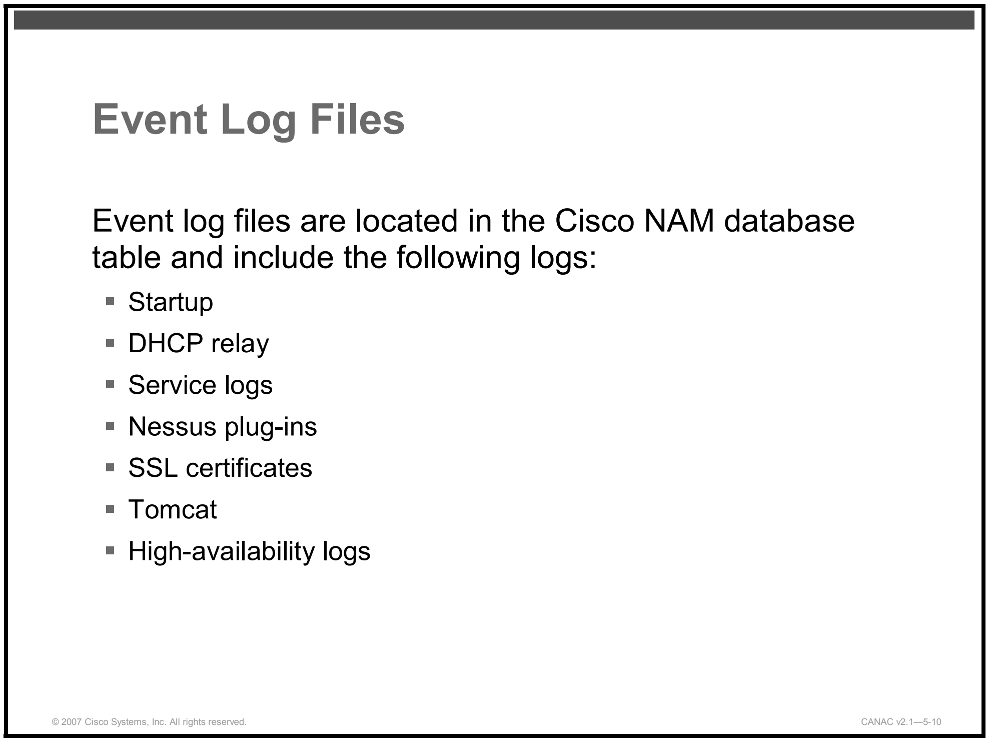
The Cisco NAS Health Event Log Description table describes the key parts of the example health event log.

Cisco NAS Health Event Log Description

Value	Description
CleanAccessServer	A Cisco NAS is reporting the event.
2006-10-08 15:07:53	Date and time of the event.
192.168.151.55	IP address of the reporting Cisco NAS.
System Stats	System statistics regarding memory and CPU processor percentage loads; these statistics are generated every hour by default.
Load factor 0	Load factor is a number that describes the number of packets waiting to be processed by the Cisco NAS (that is, the current load being handled by the Cisco NAS). A growing load factor indicates that packets are waiting in the queue to be processed. A load factor that exceeds 500 for any consistent period of time (for example, five minutes) indicates that the Cisco NAS has a steady high load of incoming traffic or packets. You should be concerned if this number increases to 500 or above.
(max since reboot: <n>)	The maximum number of packets in the queue at any one time (the maximum load handled by the Cisco NAS).

Value	Description
Mem Total: 261095424 bytes Used: 246120448 bytes Free: 14974976 bytes Shared: 212992 bytes Buffers: 53051392 bytes Cached: 106442752 bytes	These statistics show memory use: total memory, used memory, free memory, shared memory, buffer memory, and cached memory.
CPU User: 0% Nice: 0% System: 97% Idle: 1%	These numbers indicate the CPU processor percentage load on the hardware. These four numbers indicate time spent by the system in user, nice, system, and idle processes.

Note Time spent by the CPU in system processes is typically more than 90 percent on a Cisco NAS. This high percentage indicates a healthy system.



Event Log Files

Event log files are located in the Cisco NAM database table and include the following logs:

- Startup
- DHCP relay
- Service logs
- Nessus plug-ins
- SSL certificates
- Tomcat
- High-availability logs

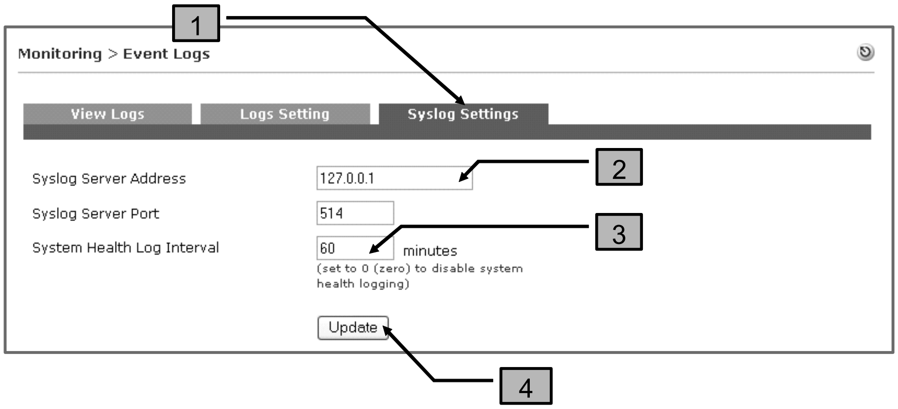
CANAC v2.1—5-10

The event log is located in the Cisco NAM database table and is named “log_info table.” The Cisco NAM Log Files table describes the logs that the Cisco NAM stores and provides a directory path to locate these logs on the Cisco NAM server.

Cisco NAM Log Files

File	Description
/var/log/messages	Startup
/var/log/dhcplog	DHCP relay, DHCP logs
/tmp/perfigo-log0.log.*	Service logs, authentication
/var/nessus/logs/nessusd.messages	Nessus plug-in test logs
/perfigo/control/apache/logs/*	SSL (certificates), Apache error logs
/perfigo/control/tomcat/logs/localhost*.	Tomcat, redirect, JSP logs
/var/log/ha-log	High-availability logs (for Cisco NAM and Cisco NAS)

Configuring the Syslog



Monitoring > Event Logs

Syslog Server Address 127.0.0.1

Syslog Server Port 514

System Health Log Interval 60 minutes

(set to 0 (zero) to disable system health logging)

Follow these four steps to configure syslog logging:

Step 1 Click the **Syslog Settings** tab on the **Monitoring > Event Logs** page.

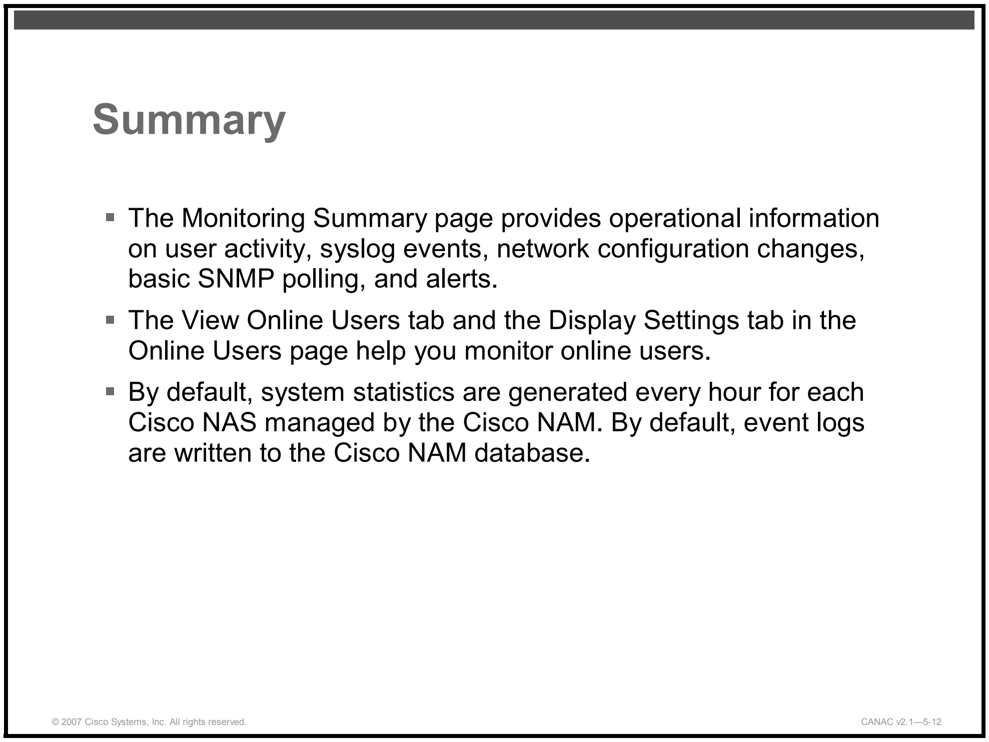
Step 2 Specify the IP address and port for the syslog event that you want written in the Syslog Server Address and Syslog Server Port fields.

Step 3 In the System Health Log Interval field, specify in minutes how often you want the Cisco NAM to log system status information. This setting determines how frequently Cisco NAS statistics are recorded in the event log. The default is 60 minutes.

Step 4 Click the **Update** button to save your changes.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- The Monitoring Summary page provides operational information on user activity, syslog events, network configuration changes, basic SNMP polling, and alerts.
- The View Online Users tab and the Display Settings tab in the Online Users page help you monitor online users.
- By default, system statistics are generated every hour for each Cisco NAS managed by the Cisco NAM. By default, event logs are written to the Cisco NAM database.

CANAC v2.1—5-12

Lesson 2

Administering the Cisco NAM

Overview

Network administration tasks are part of the ongoing work that is necessary to ensure the efficient and effective running of any system. With a Cisco Network Admission Control (NAC) Appliance, continual administration ensures a secure and reliable Cisco NAC Appliance solution and network. This lesson describes how to perform the tasks that you will use to administer a Cisco NAC Appliance deployment using the Cisco NAC Appliance Manager (Cisco NAM) web-based administration console.

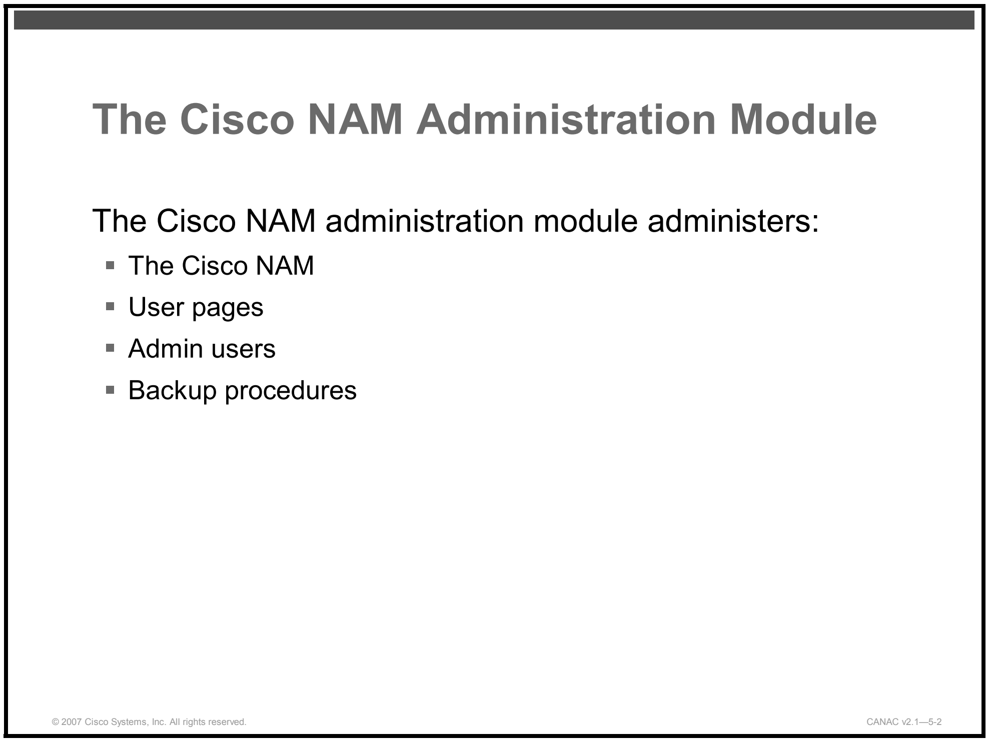
Objectives

Upon completing this lesson, you will be able to describe how to manage a Cisco NAC Appliance deployment. This ability includes being able to meet these objectives:

- Describe the components of the Cisco NAM administration module
- Describe how to manage administrator groups
- Describe how to manage users with administrator privileges
- Describe how to manage user passwords
- Describe how to administer the Cisco NAM system time settings
- Describe how to configure SSL certificate management using the administrator console of the Cisco NAM
- Describe how to manage Cisco NAC Appliance software upgrades and licenses
- Describe the steps used to maintain a Cisco NAM configuration

Defining the Cisco NAM Administration Module

This topic describes the components of the Cisco NAM administration module.



The Cisco NAM Administration Module

The Cisco NAM administration module administers:

- The Cisco NAM
- User pages
- Admin users
- Backup procedures

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—5-2

At installation time, the initial configuration script provides many of the internal administration settings for the Cisco NAM. These settings include interface addresses, Domain Name System (DNS) servers, and other network information. After the installation has been performed, the administration module allows you to access and change the settings.

On the Cisco NAM pages of the administration module, you perform these administration tasks:

- Change network settings for the Cisco NAM.
- Set up Cisco NAM high-availability mode. This component of the administration module has been discussed in a previous lesson on configuring Cisco NAM high availability.
- Manage Cisco NAM system time and Secure Sockets Layer (SSL) certificates on the Cisco NAM.
- Upgrade the software on the Cisco NAM.
- Manage Cisco NAM license files.
- Create support logs for the Cisco NAM to send to Cisco NAC Appliance customer support services.

On the User Pages tab of the administration module, you perform these administration tasks:

- Add the default login page and create or modify all web-user login pages.
- Upload resource files to the Cisco NAM.

On the Admin Users page of the administration module, you perform these administration tasks:

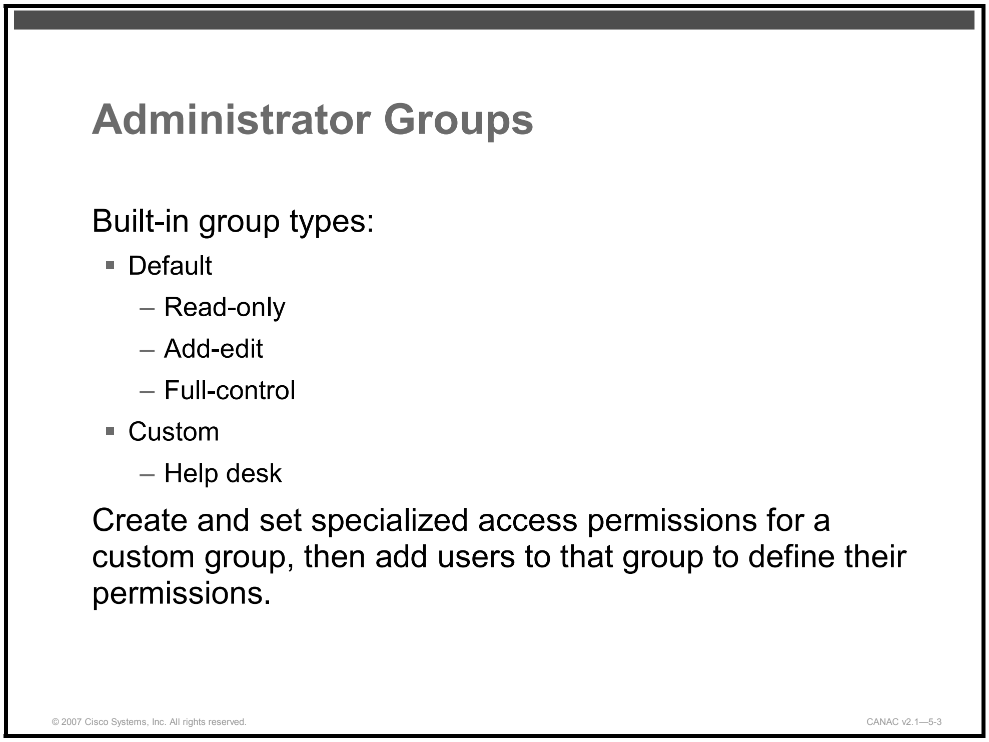
- Add and manage new administrator groups, administrator users, and passwords.
- Configure and manage administrator privileges when new features are added.

The Backup page of the administration module allows you to create manual records of your Cisco NAM in order to back up your Cisco NAM configuration.

Note There is an application programming interface (API) available for the Cisco NAM. For details on the Cisco NAM API, refer to the API Support section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Managing Administrator Groups

This topic describes how to manage administrator (admin) groups.



Administrator Groups

Built-in group types:

- Default
  - Read-only
  - Add-edit
  - Full-control
- Custom
  - Help desk

Create and set specialized access permissions for a custom group, then add users to that group to define their permissions.

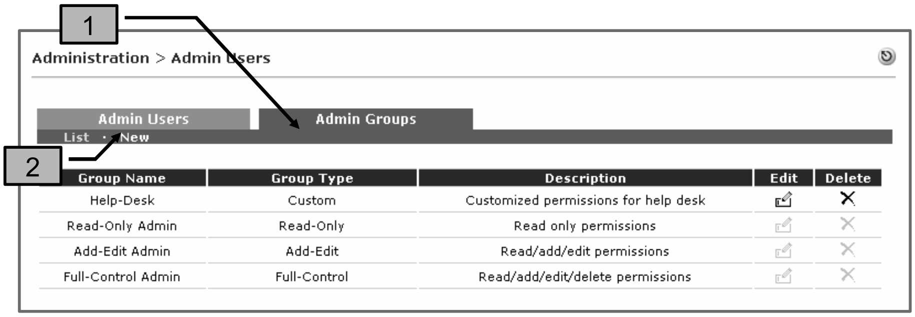
CANAC v2.1—5-3

You can manage multiple admin users by using the Administration > Admin Users module of the Cisco NAM web administration console.

There are two tabs under Administration > Admin Users: the Admin Groups tab and the Admin Users tab.

There are three default admin group types that cannot be removed or edited: read-only, add-edit, and full-control. The full-control option includes delete permissions. You can add users to one of these three default groups. There is one default custom group called the help-desk group, which has a predefined customized setting that you can edit for your help-desk user group. You can also create and set specialized access permissions for a newly created custom group and then add users to that group to define permissions for each user. You can edit each module feature within the new group.

Creating a Custom Admin Group



Administration > Admin Users

Group Name	Group Type	Description	Edit	Delete
Help-Desk	Custom	Customized permissions for help desk	✎	✕
Read-Only Admin	Read-Only	Read only permissions	✎	✕
Add-Edit Admin	Add-Edit	Read/add/edit permissions	✎	✕
Full-Control Admin	Full-Control	Read/add/edit/delete permissions	✎	✕

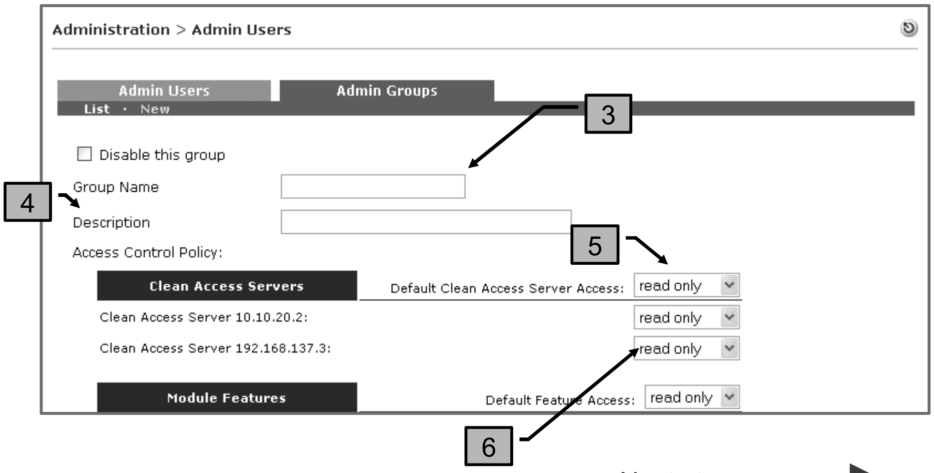
Next steps →

Follow these nine steps to create a custom admin group:

Step 1 Choose **Administration** > **Admin Users** > **Admin Groups**.

Step 2 Click the **New** link to bring up the New Admin Groups configuration form.

Creating a Custom Admin Group (Cont.)



☐ Disable this group

Group Name

Description

Access Control Policy:

Clean Access Servers Default Clean Access Server Access: read only

Clean Access Server 10.10.20.2: read only

Clean Access Server 192.168.137.3: read only

Module Features Default Feature Access: read only

Next steps →

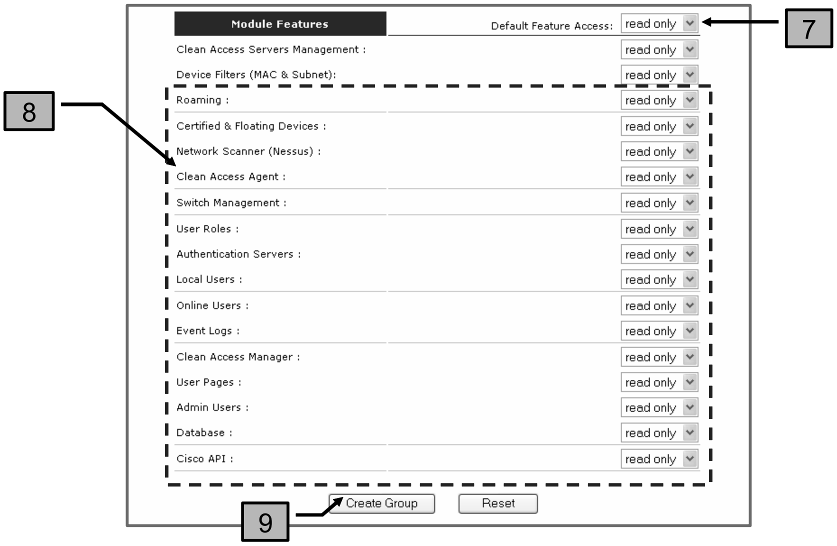
Step 3 Enter a group name for the custom admin group in the Group Name field.

Step 4 Enter an optional description for the group in the Description field.

Step 5 In the Default Clean Access Server Access drop-down menu**,** choose either **read only** (default) or **local admin**. The first option listed defines the default permissions that are used when a new Cisco NAC Appliance Server (Cisco NAS) is added to the managed domain. If no existing access settings are found for the Cisco NAS, this default access policy is used.

Step 6 Choose either **local admin** or **read only** for the access options next to each individual Cisco NAS listed. The local admin option gives the admin group full control over certain Cisco NASs, including control to delete and reboot. The read only option allows the admin group to only view permissions on other servers.

Creating a Custom Admin Group (Cont.)



Module Features	Default Feature Access: read only
Clean Access Servers Management :	read only
Device Filters (MAC & Subnet):	read only
Roaming :	read only
Certified & Floating Devices :	read only
Network Scanner (Nessus) :	read only
Clean Access Agent :	read only
Switch Management :	read only
User Roles :	read only
Authentication Servers :	read only
Local Users :	read only
Online Users :	read only
Event Logs :	read only
Clean Access Manager :	read only
User Pages :	read only
Admin Users :	read only
Database :	read only
Cisco API :	read only

CANAC v2.1—5-6

Step 7 In the Module Features form, click on a drop-down menu to choose either **read only** (default), **add-edit**, or **full control** for the Default Feature Access. The first option listed defines the default permissions for any new feature added to the Cisco NAM. In the case of a software upgrade, admin privilege settings that existed before the upgrade are preserved.

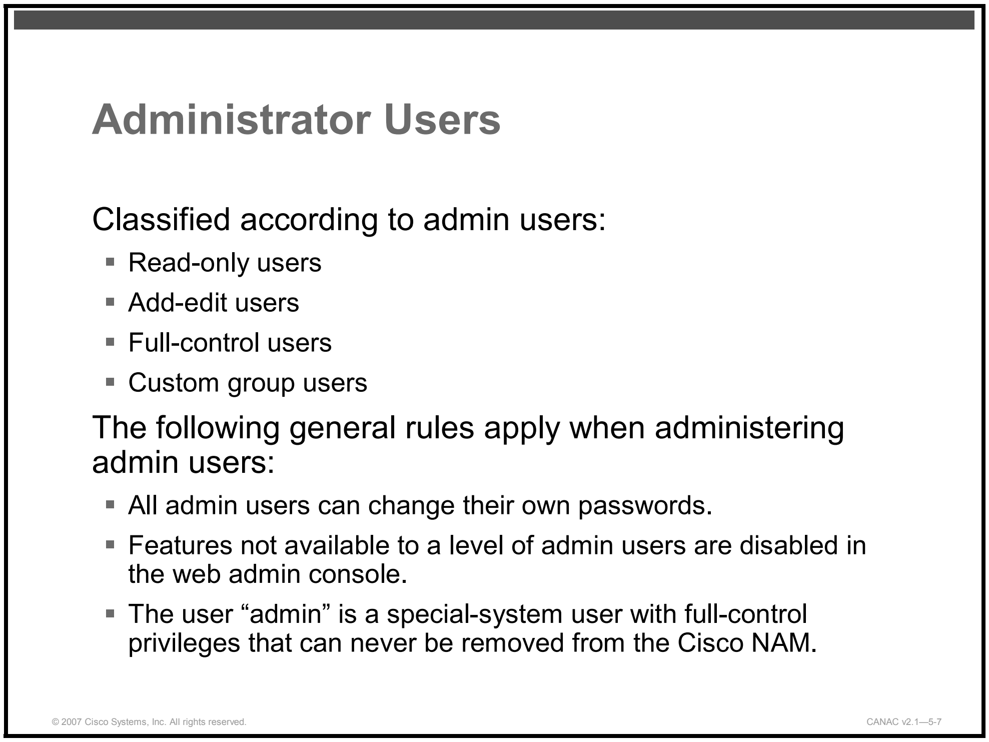
Step 8 Choose group access privileges from the available read only, add-edit, or full control options for each module. This step allows you to tailor admin control over the modules of the Cisco NAM for each admin group.

Step 9 Click **Create Group** to add the appropriate group to the Admin Groups list according to the new access privileges that are granted.

Note You can edit a group later by clicking the **Edit** button next to the group in the list. Click the **Delete** icon next to the group if you want to delete that group. Users in an admin group are not removed when the group is deleted; they are assigned to the default read-only admin group.

Managing Administrator Users

This topic describes how to manage users with administrator privileges.



Administrator Users

Classified according to admin users:

- Read-only users
- Add-edit users
- Full-control users
- Custom group users

The following general rules apply when administering admin users:

- All admin users can change their own passwords.
- Features not available to a level of admin users are disabled in the web admin console.
- The user “admin” is a special-system user with full-control privileges that can never be removed from the Cisco NAM.

CANAC v2.1—5-7

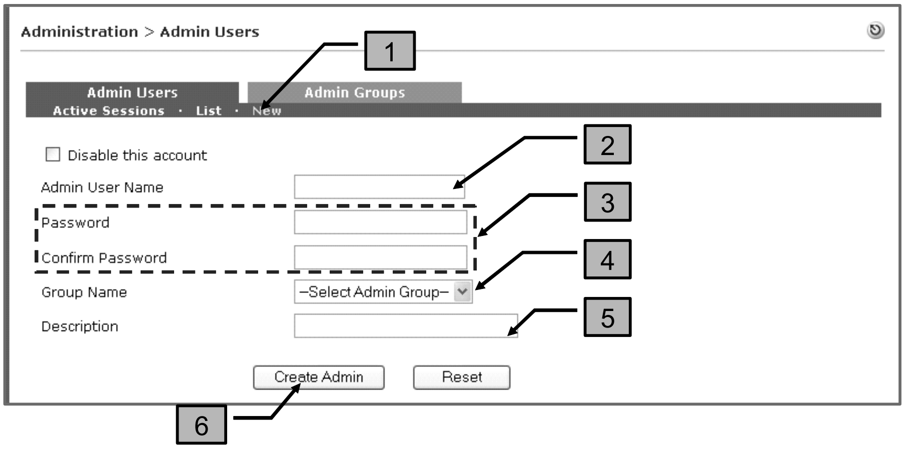
Admin users are classified according to these groups of users:

- **Read-only users:** Read-only users can only view the users, devices, and features in the web administration console.
- **Add-edit users:** Add-edit users can add and edit but cannot remove local users, devices, or features in the web administration console. Add-edit admin users cannot create other admin users.
- **Full-control users:** Full-control users have add, edit, and delete permissions for all aspects of the web administration console. Only full-control admin users can add, edit, or remove other admin users or groups.
- **Custom group users:** Custom group users can be configured to have a combination of access privileges.

The following general rules apply when administering admin users:

- All admin users can access the Administration > Admin Users module and change their own passwords.
- Features that are not available to a level of admin users are disabled in the web administration console for that user.
- The user “admin” is a special system user with full-control privileges that can never be removed from the Cisco NAM. For example, a full-control user can log onto and delete their own account, but they cannot log on as user **admin** and delete the **admin** account.

Adding an Admin User to an Admin Group



CANAC v2.1—5-8

Follow these six steps to add an admin user to an admin group:

Step 1 Choose **Administration > Admin Users > New**.

Step 2 Enter a name in the Admin User Name field.

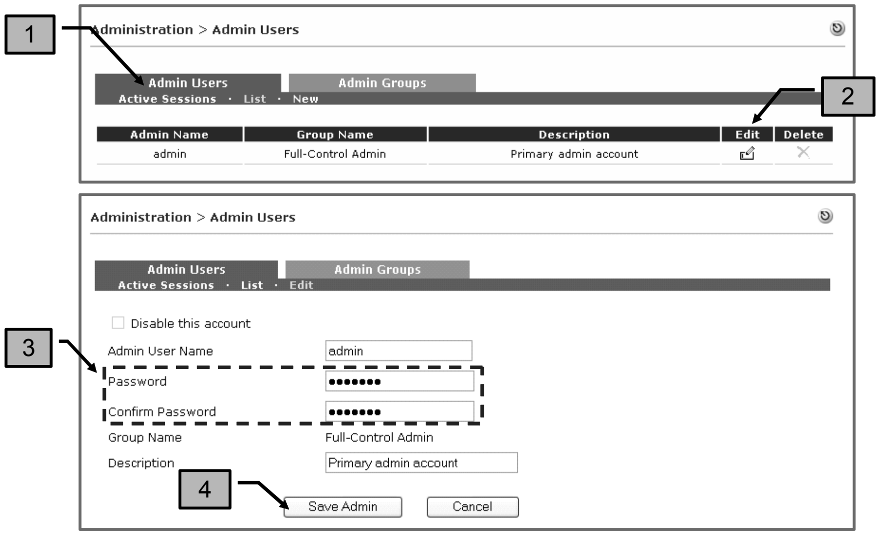
Step 3 Enter a password in the Password and Confirm Password fields.

Step 4 Choose an admin group type from the Group Name drop-down menu.

Step 5 Enter an optional description for the user in the Description field.

Step 6 Click **Create Admin**. The new user now appears under Administration > Admin Users > List.

Editing an Admin User



Administration > Admin Users

Admin Users | Admin Groups

Active Sessions · List · New

Admin Name	Group Name	Description	Edit	Delete
admin	Full-Control Admin	Primary admin account	✎	✕

Administration > Admin Users

Admin Users | Admin Groups

Active Sessions · List · Edit

□ Disable this account

Admin User Name	admin
Password	•••••••
Confirm Password	•••••••
Group Name	Full-Control Admin
Description	Primary admin account

Save Admin | Cancel

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—5-9

Follow these four steps to edit an admin user:

Step 1 Choose **Administration > Admin Users.**

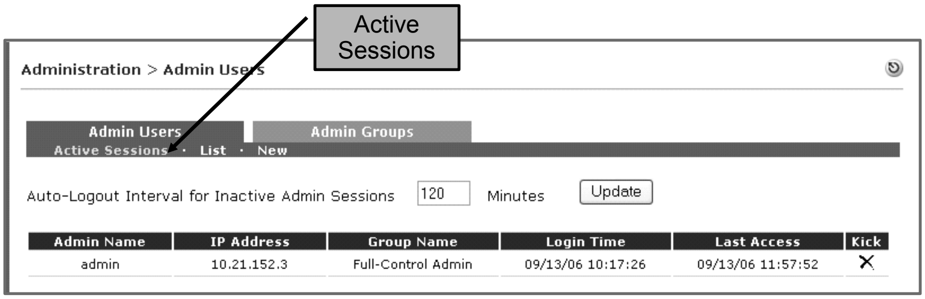
Step 2 Click the **Edit** icon next to the admin user that you want to edit.

Step 3 Change the Password and Confirm Password fields or other desired fields.

Step 4 Click **Save Admin**.

Note You can edit all properties of the system admin user except the system admin user group type.

Viewing Active Admin Users



Active Sessions

Administration > Admin Users

Auto-Logout Interval for Inactive Admin Sessions 120 Minutes

Admin Name	IP Address	Group Name	Login Time	Last Access	Kick
admin	10.21.152.3	Full-Control Admin	09/13/06 10:17:26	09/13/06 11:57:52	✕

You can view which admin users are currently using the Cisco NAM web administration console by choosing **Administration > Admin Users > Active Sessions**. The active sessions list shown in the figure lists all admin users that are currently active. Admin users are session-based. Each browser that an admin user opens to connect to the Cisco NAM web server creates an entry for the user in the active sessions list.

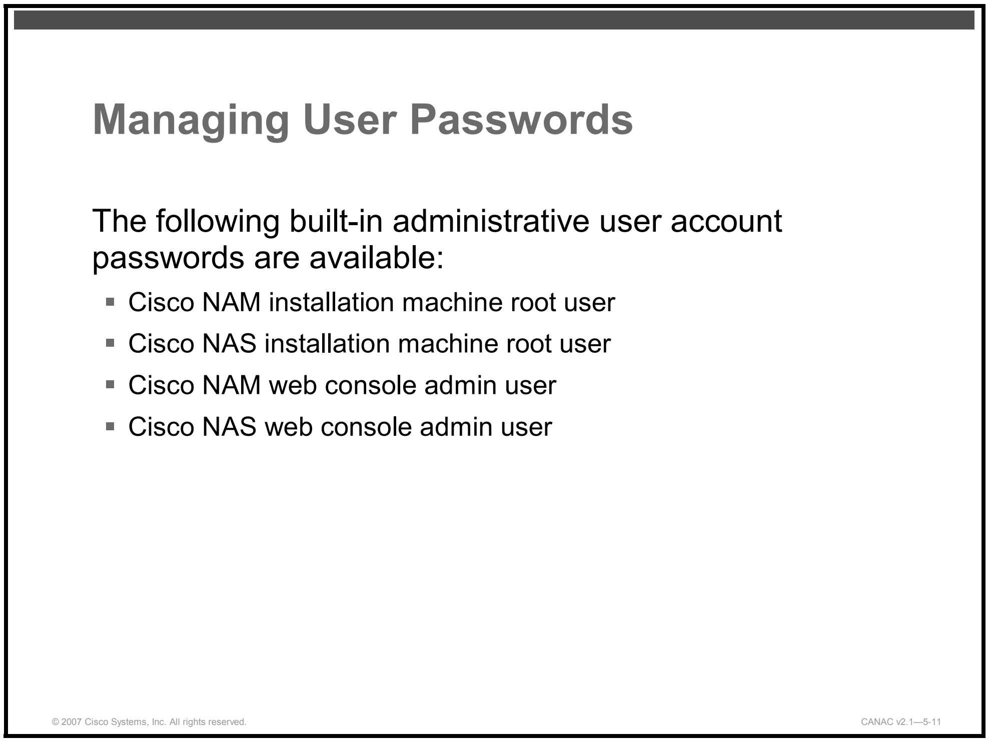
Note If an admin user opens a browser, closes it, then opens a new browser, two entries will remain for a period of time on the active session list. The last access time does not change for the ended session. Eventually the entry is removed by the auto-logout feature.

The Active Sessions page includes the following information:

- **Admin Name:** The name of the current admin user.
- **IP Address:** The IP address of the admin user machine.
- **Group Name:** The access privilege group of the admin user.
- **Login Time:** The start of the admin user session.
- **Last Access:** The last time the admin user clicked a link anywhere in the web administration console. Each click resets the last access time.
- **Auto-Logout Interval for Inactive Admin Sessions:** This value is compared against the Login Time and Last Access time for an active admin user session. If the difference between the login time and last access time is greater than the auto-logout interval that you configured, the user is logged out. The auto-logout interval must be in the range of 1 to 120 minutes. The default setting for the interval is 20 minutes.
- **Kick**: Click this button to log out an active admin user and to remove the session from the active session list.

Managing User Passwords

This topic describes how to manage user passwords.



Managing User Passwords

The following built-in administrative user account passwords are available:

- Cisco NAM installation machine root user
- Cisco NAS installation machine root user
- Cisco NAM web console admin user
- Cisco NAS web console admin user

© 2007 Cisco Systems, Inc. All rights reserved.

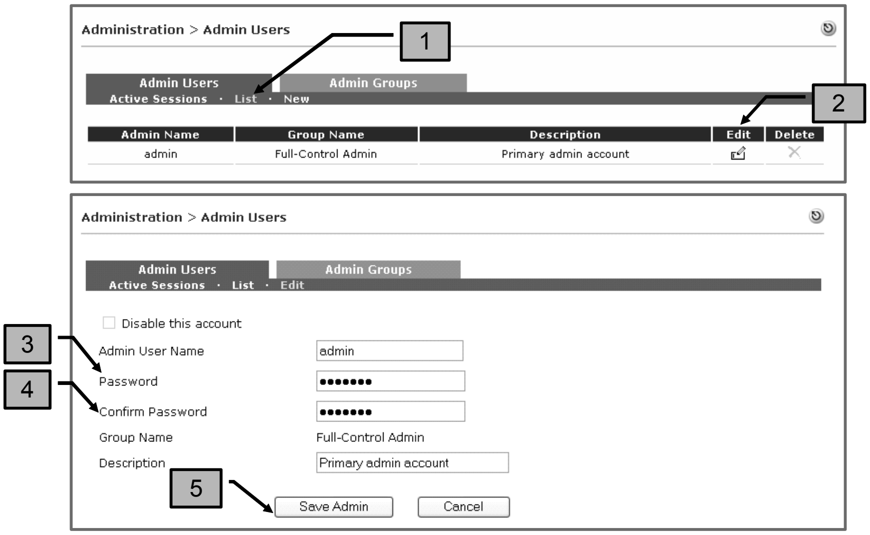
CANAC v2.1—5-11

Use strong passwords (passwords containing at least eight characters that combine letters and numbers) in the Cisco NAC Appliance system. Cisco NAC Appliance contains built-in passwords for these administrative user accounts:

- Cisco NAM installation machine root user
- Cisco NAS installation machine root user
- Cisco NAM web console admin user
- Cisco NAS web console admin user

Note The first three passwords in the list are initially set at installation time. To change these passwords at a later time, access the Cisco NAM or Cisco NAS machine by Secure Shell Protocol (SSH) and log on as the user whose password you want to change. Use the Linux **password** command to change the user password.

Changing Cisco NAM Admin User Passwords



Administration > Admin Users

Admin Name	Group Name	Description	Edit	Delete
admin	Full-Control Admin	Primary admin account		

Administration > Admin Users

□ Disable this account

Admin User Name: admin

Password: •••••••

Confirm Password: •••••••

Group Name: Full-Control Admin

Description: Primary admin account

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—5-12

Follow these five steps to change the Cisco NAM web console admin user password:

Step 1 Choose **Administration** > **Admin Users** > **List**.

Step 2 Click the **Edit** icon for the admin user. The Edit form appears.

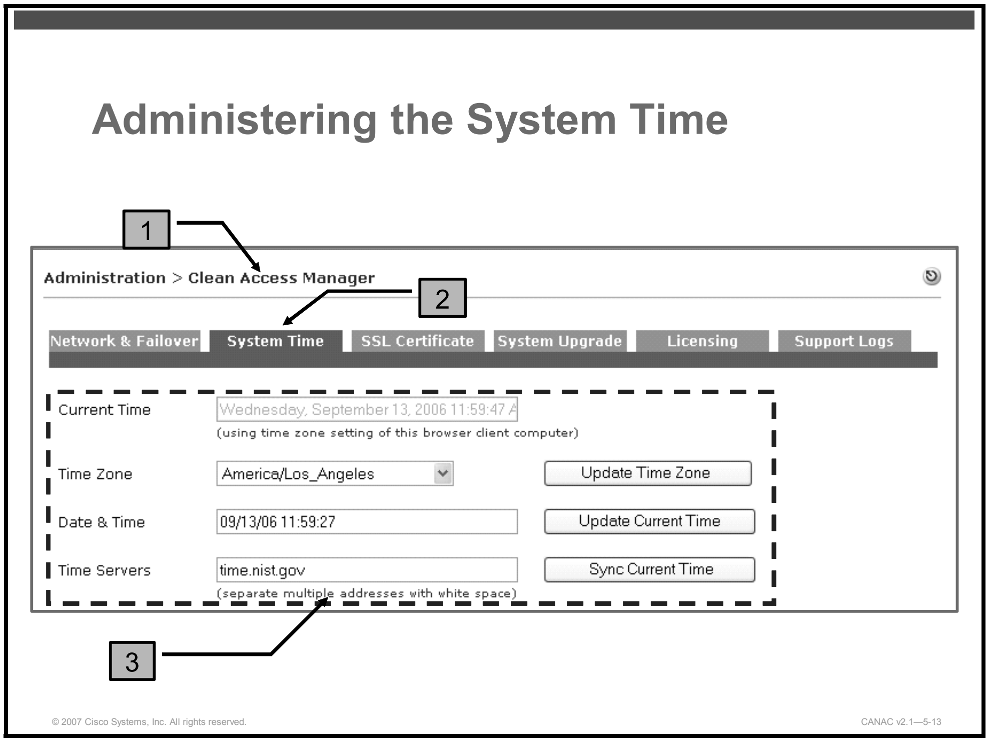
Step 3 Enter the new password in the Password field.

Step 4 Enter the password again in the Confirm Password field.

Step 5 Click the **Save Admin** button. The new password is now in effect.

Administering the System Time

This topic describes how to administer the Cisco NAM system time settings.



Administering the System Time

Administration > Clean Access Manager

Current Time: Wednesday, September 13, 2006 11:59:47 A
(using time zone setting of this browser client computer)

Time Zone: America/Los_Angeles

Date & Time: 09/13/06 11:59:27

Time Servers: time.nist.gov
(separate multiple addresses with white space)

CANAC v2.1—5-13

For login purposes and to accomplish time-based tasks, the Cisco NAM and each Cisco NAS must be correctly synchronized with each other.

The System Time tab lets you view the current time on the Cisco NAM, modify the current time, and change the time zone setting for the Cisco NAM operating system.

To view the current time, complete these three steps:

Step 1 Navigate to the Administration > Clean Access Manager page.

Step 2 Click the **System Time** tab. The system time for the Cisco NAM appears in the Current Time field.

Step 3 Modify the settings in the dashed box in the figure.

There are two ways to modify the system time: manually, by entering the new time, or automatically, by synchronizing from an external time server.

For both the manual and automatic options, begin by clicking the **System Time** tab of the Administration > Clean Access Manager page. From this page, complete one of these tasks:

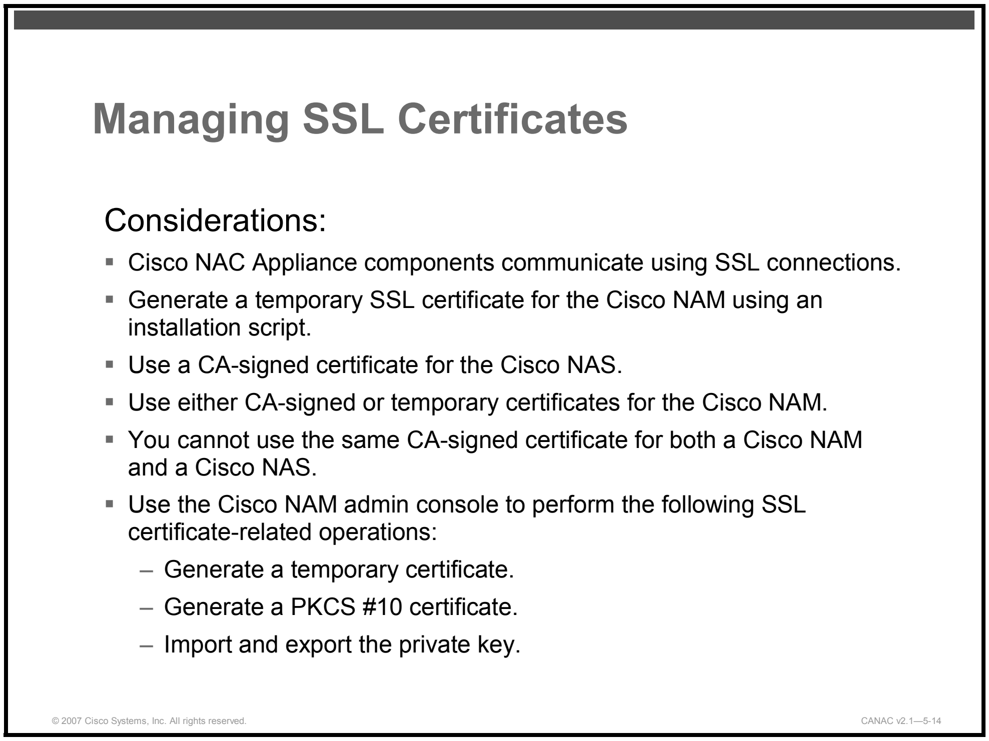
- Manually enter the time in the Date & Time field and click **Update Current Time**. (The time should be in the form: *mm*/*dd*/*yy hh*:*mm:ss*).
- Click the **Sync Current Time** button to have the time updated automatically by one of the time servers listed in the Time Servers field.

Note The default time server used to automatically update the time is the server managed by the National Institute of Standards and Technology (NIST). To specify another time server, enter the URL of the server in the Time Servers field of the Administration > Clean Access Manager page. The server should provide the time in NIST-standard format (mm/dd/yy hh:mm:ss). Use spaces to separate multiple servers.

If more than one time server is listed, the Cisco NAM contacts the first server in the list when synchronizing. If the time is available from that server, the time is updated from that server. If the time is not available from that server, the Cisco NAM tries the next server on the list until a server is reached.

Managing SSL Certificates

This topic describes how to configure SSL certificate management using the administration console of the Cisco NAM.



Managing SSL Certificates

Considerations:

- Cisco NAC Appliance components communicate using SSL connections.
- Generate a temporary SSL certificate for the Cisco NAM using an installation script.
- Use a CA-signed certificate for the Cisco NAS.
- Use either CA-signed or temporary certificates for the Cisco NAM.
- You cannot use the same CA-signed certificate for both a Cisco NAM and a Cisco NAS.
- Use the Cisco NAM admin console to perform the following SSL certificate-related operations:
  - Generate a temporary certificate.
  - Generate a PKCS #10 certificate.
  - Import and export the private key.

CANAC v2.1—5-14

The individual servers and managers of Cisco NAC Appliance communicate with each other securely over SSL connections. SSL connections are used between the Cisco NAM and the Cisco NAS, as well as between the Cisco NAM and the browser used to access the Cisco NAC Appliance administration console. The Cisco NAC Appliance Agent (Cisco NAA) also communicates using SSL.

At installation time, the install script allows you to generate a temporary SSL certificate for the Cisco NAM. When configuring high availability for a Cisco NAS, you should contact a certificate authority (CA), an organization authorized to issue trusted certificates, and obtain a signed SSL certificate (CA-signed certificate). The Cisco NAS certificate is the certificate that is visible to the end user. Consequently, a CA-signed certificate is recommended for the server so that the end user is assured of the authenticity of the Cisco NAS that they are about to connect to. A CA-signed certificate does not require that the user validates a certificate that is unknown to their configuration when logging in. When a temporary certificate is used for the Cisco NAS, the user is asked to accept the temporary certificate, which can be confusing if the user is not familiar with certificates. Because the Cisco NAM does not interact with users, you can choose either a CA-signed or temporary certificate.

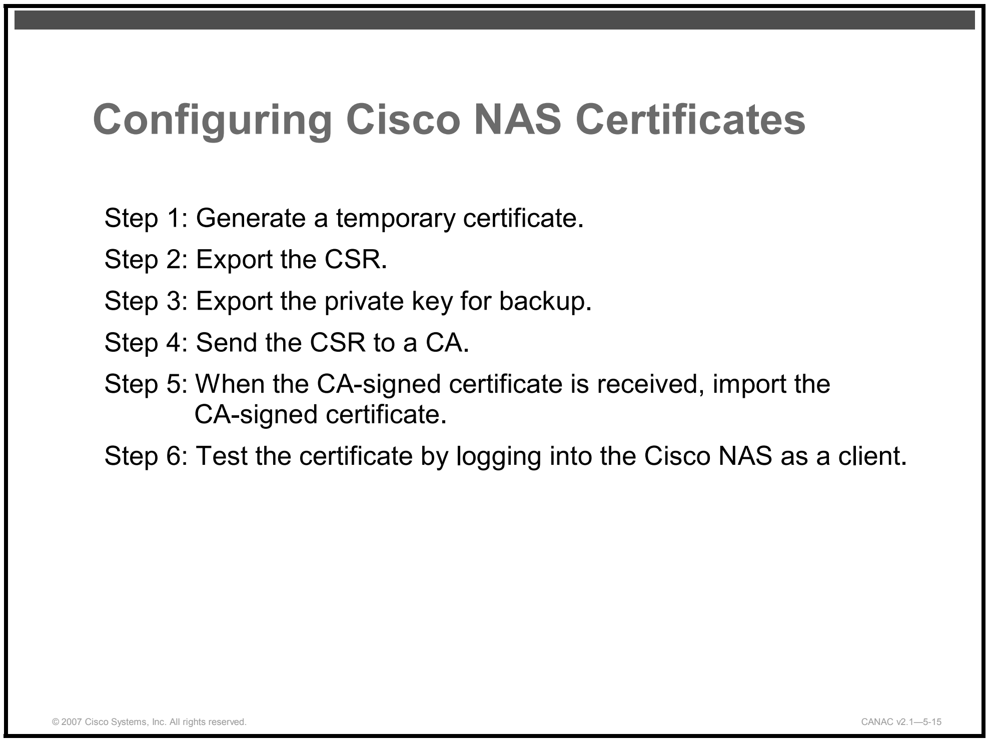
Note	You cannot use the same CA-signed certificate for the Cisco NAM and the Cisco NAS. You must buy a separate certificate for each Cisco NAS.

Use the Cisco NAM administration console to perform these SSL certificate-related operations:

- Generate a temporary certificate.
- Generate a Public-Key Cryptography Standard #10 (PKCS #10) certificate request based on the current certificate.
- Import and export the private key.

Tip You can export a private key and keep it as a copy of a certificate.

Note To review the procedure that is used to generate a PKCS #10 certificate and the procedure that is used to import and export certificates, refer to the Manage SSL Certificates section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide.*



Configuring Cisco NAS Certificates

Step 1: Generate a temporary certificate.

Step 2: Export the CSR.

Step 3: Export the private key for backup.

Step 4: Send the CSR to a CA.

Step 5: When the CA-signed certificate is received, import the CA-signed certificate.

Step 6: Test the certificate by logging into the Cisco NAS as a client.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—5-15

Follow these six steps to configure Cisco NAS certificates for a typical Cisco NAC Appliance installation:

Step 1 Generate a temporary certificate.

Step 2 Export the certificate signing request (CSR).

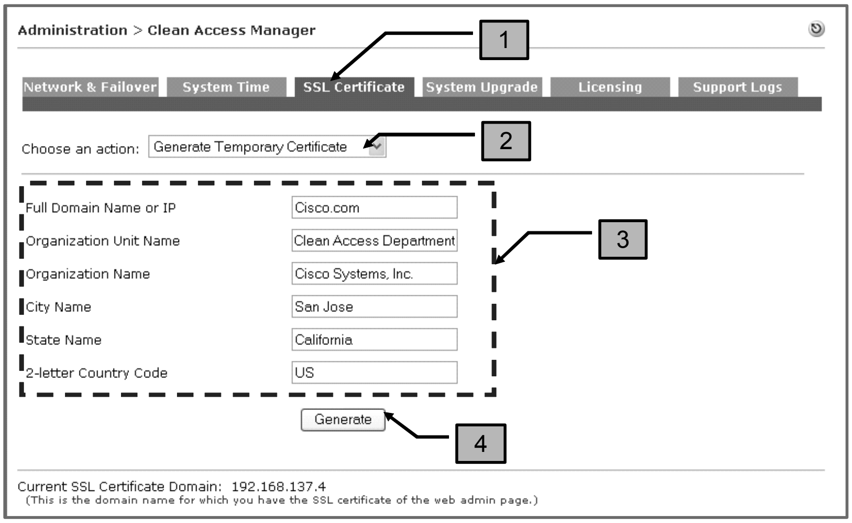
Step 3 Export the private key for backup.

Step 4 Send the CSR to a CA.

Step 5 When the CA-signed certificate is received from the CA, import the CA-signed certificate.

Step 6 Test the configuration by accessing the server as a client.

Generating a Temporary Certificate



Administration > Clean Access Manager

Choose an action: Generate Temporary Certificate

Full Domain Name or IP	Cisco.com
Organization Unit Name	Clean Access Department
Organization Name	Cisco Systems, Inc.
City Name	San Jose
State Name	California
2-letter Country Code	US

Current SSL Certificate Domain: 192.168.137.4
(This is the domain name for which you have the SSL certificate of the web admin page.)

CANAC v2.1—5-16

Follow these four steps to generate a temporary certificate:

Step 1 Choose **Administration > Clean Access Manager** and click the **SSL Certificate** tab.

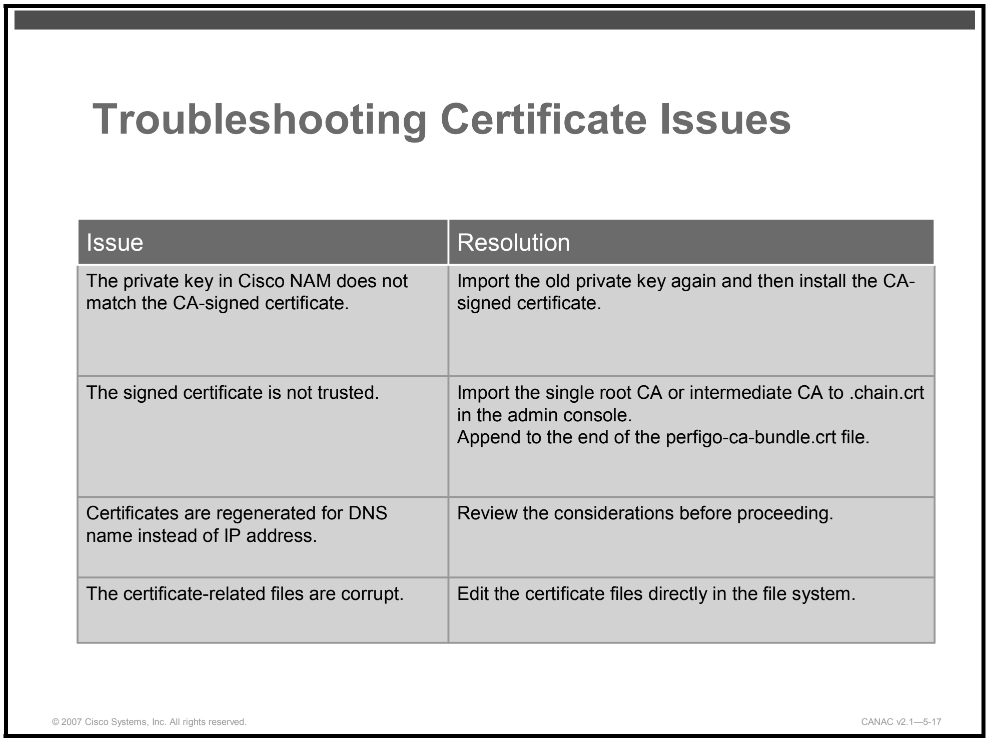
Step 2 Choose **Generate Temporary Certificate** from the Choose an Action drop-down menu.

Step 3 Enter the appropriate values for the following fields:

- **Full Domain Name or IP:** The fully qualified domain name or IP address of the Cisco NAM that you will apply the certificate to. For example: camanager.<*your_domain_name*>
- **Organization Unit Name:** The name of the unit within the organization, if applicable
- **Organization Name:** The legal name of the organization
- **City Name:** The city in which the organization is legally located
- **State Name:** The full name of the state in which the organization is legally located
- **2-Letter Country Code:** The two-character, ISO-format country code, such as GB for Great Britain or US for the United States

Step 4 Click **Generate**.

Note Typically, after generating a temporary certificate, you can generate a certificate-signing request based on the certificate.



Troubleshooting Certificate Issues

Issue	Resolution
The private key in Cisco NAM does not match the CA-signed certificate.	Import the old private key again and then install the CA-signed certificate.
The signed certificate is not trusted.	Import the single root CA or intermediate CA to .chain.crt in the admin console. Append to the end of the perfigo-ca-bundle.crt file.
Certificates are regenerated for DNS name instead of IP address.	Review the considerations before proceeding.
The certificate-related files are corrupt.	Edit the certificate files directly in the file system.

These are the issues regarding certificate management in Cisco NAC Appliance:

- The private key in Cisco NAM may not match the CA-signed certificate. This issue can arise, for example, if an administrator generates a CSR, backs up the private key, and then sends the CSR to a CA. After the CSR has been sent, another administrator regenerates a temporary certificate. When the CA-signed certificate is returned from the CA, the private key on which the CA certificate is based no longer matches the one in the Cisco NAM.

  To resolve this issue, import the old private key again and then install the CA-signed certificate.

- The signed certificate may not be trusted. If the user sees a page warning that the certificate is not trusted after the CA-signed certificate has been installed, the likely cause is that the CA is not in the root CA bundle for Cisco NAC Appliance. There are two ways to resolve this issue:
  - Import the single root CA or intermediate CA to chain.crt in the administration console.
  - Append the needed root to the end of the perfigo-ca-bundle.crt file.

- The certificates are regenerated using their DNS name instead of their IP address. To regenerate certificates based on the DNS name instead of the IP address of your servers, complete these tasks:
  - Ensure that the CA-signed certificate that you are importing is the certificate that you generated the CSR with and that you have not subsequently generated another temporary certificate. Generating a new temporary certificate creates a new private-public key combination. In addition, always export and save the private key when you are generating a CSR for signing. This step ensures that the private key is convenient to access.

Note When you import certain CA-signed certificates, the system may warn you that you need to import the root certificate (the CA root certificate) that was used to sign the CA-signed certificate, or the intermediate root certificate may need to be imported.

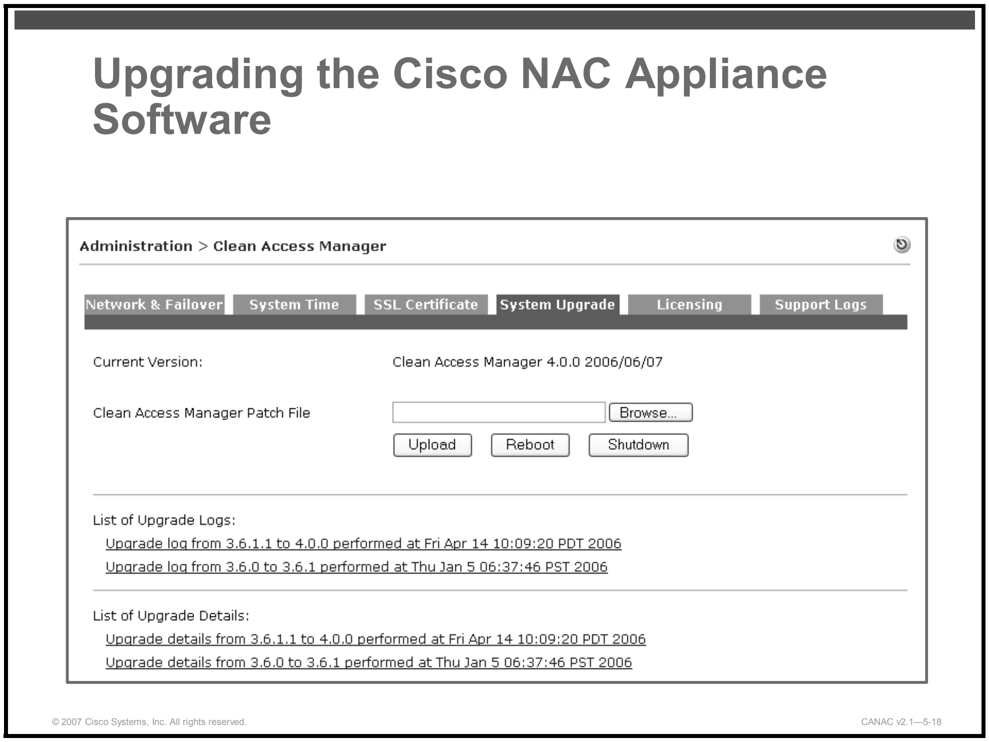
- — Ensure that there is a DNS entry in the DNS server.
- — Ensure that the DNS address in your Cisco NAS is correct.
- — Use the DNS name for the Service IP (virtual DNS) for high-availability (failover) configurations.
- — Reboot any time you generate a new certificate or import a CA-signed certificate.

Note When you use a DNS-based certificate, if the certificate is not CA-signed, the user is prompted to accept the certificate.

- Certificate-related files can be corrupted. For troubleshooting purposes, the certificate-related files used by the Cisco NAM may need to be modified directly in the file system of the Cisco NAM. An example of this issue is when the administration console becomes unreachable due to a disparity in the CA certificate and private key combination. For details on the names of the certificate-related files, refer to the Manage SSL Certificates section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Managing the Cisco NAC Appliance Software

This topic describes how to manage Cisco NAC Appliance software upgrades and licenses.



Upgrading the Cisco NAC Appliance Software

Administration > Clean Access Manager

Current Version: Clean Access Manager 4.0.0 2006/06/07

Clean Access Manager Patch File

List of Upgrade Logs:

- Upgrade log from 3.6.1.1 to 4.0.0 performed at Fri Apr 14 10:09:20 PDT 2006
- Upgrade log from 3.6.0 to 3.6.1 performed at Thu Jan 5 06:37:46 PST 2006

List of Upgrade Details:

- Upgrade details from 3.6.1.1 to 4.0.0 performed at Fri Apr 14 10:09:20 PDT 2006
- Upgrade details from 3.6.0 to 3.6.1 performed at Thu Jan 5 06:37:46 PST 2006

CANAC v2.1—5-18

Cisco periodically issues software updates for the Cisco NAM and Cisco NAS. The following list describes what is affected by each type of upgrade and upgrade numbering scheme:

- **Major releases (X.0; for example, 4.0):** New platform with new features
- **Minor releases (4.x, for example 4.1):** Platform maintenance, additional features, or both; includes interim patches and updates
- **Software patches and updates (4.x.x, for example, 4.0.1):** interim patch or update for a minor release

Caution For major and minor releases, you must upgrade your Cisco NAM and each Cisco NAS concurrently. For upgrade instructions, refer to the release notes at http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca40/index.htm

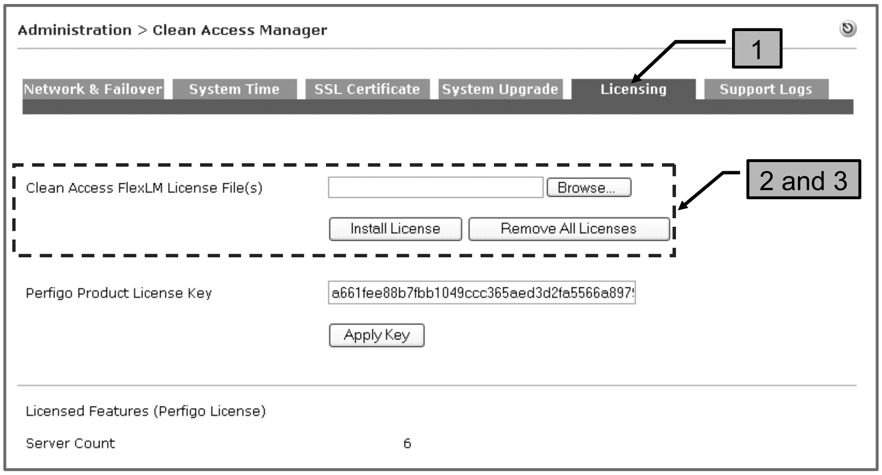
Starting with version 3.5.3 of Cisco NAC Appliance, you can upgrade the Cisco NAM and Cisco NAS software by uploading the upgrade file in tar.gz format via the web console by choosing **Administration > Software Update**. The Cisco NAM automatically performs all the upgrade tasks that are currently executed manually, including creating snapshots before and after an upgrade, undoing the tar file, changing the directory to store, and running the upgrade script.

The figure shows the Cisco Clean Access System Upgrade form. The key components of the form are as follows:

- **Shutdown button:** This button shuts down the service on the machine without shutting down the machine itself (equivalent to the **service perfigo stop** command). To restart the service, use the **service perfigo restart** or **reboot** command from a command shell.
- **List of Upgrade Logs:** This list displays how many upgrades have been executed. A list of individual upgrades and the log information from each upgrade is provided.
- **List of Upgrade Details:** This list displays the actions performed by the upgrade for the purpose of customer-support troubleshooting.

Beginning with Cisco NAC Appliance version 3.5.3, you can upgrade the Cisco NAS software from the Cisco NAS direct-access web-administration console by choosing Administration > Software Update. To upgrade the software for the Cisco NAS, refer to the Administer the Clean Access Server section in the *Cisco NAC Appliance - Cisco Clean Access Server Administration and Installation Guide*.

Maintaining Cisco NAC Appliance Licenses



Administration > Clean Access Manager

Clean Access FlexLM License File(s)

Perfigo Product License Key a661fee88b7fbb1049ccc365aed3d2fa5566a897

Licensed Features (Perfigo License)

Server Count 6

CANAC v2.1—5-19

The Cisco NAM and Cisco NASs require a valid license before they function. Follow these three steps to install Cisco NAC Appliance licensing:

Step 1 Choose **Administration > Clean Access Manager > Licensing**.

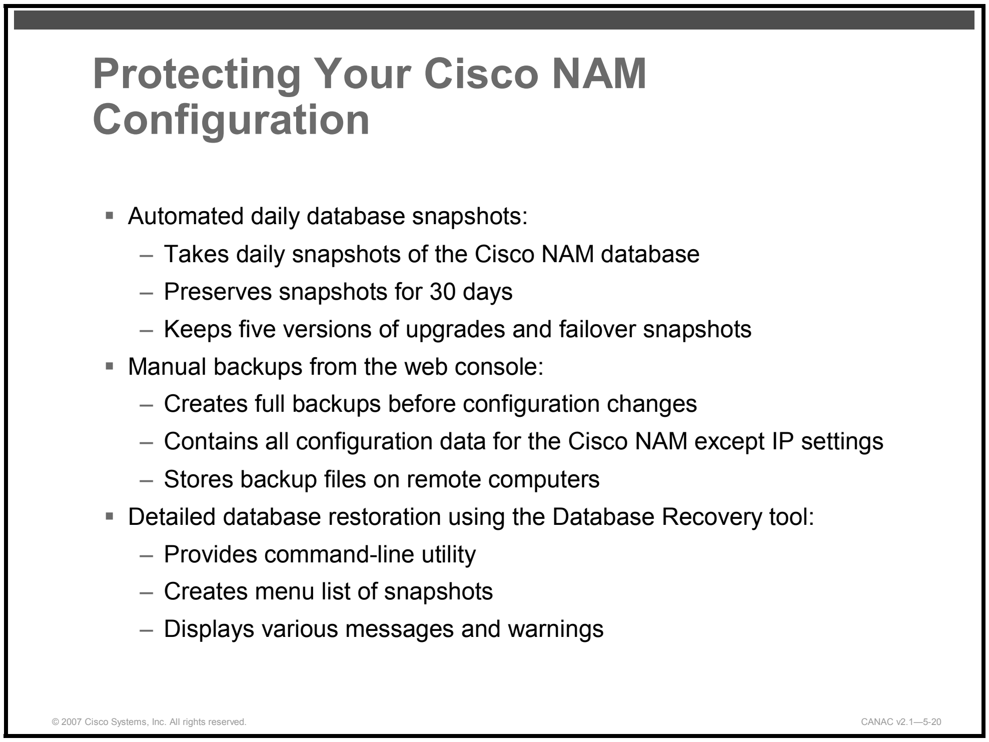
Step 2 In the Clean Access FlexLM License File(s) field, choose the license file for your Cisco NAS or Cisco NAS bundle and click **Install License** for that entry. If the license is installed successfully, a green confirmation text string and the Cisco NAS increment count (for example, "License added successfully. Out-of-Band Server Count is now 10.") appears at the top of the window.

Step 3 Repeat this step for each Cisco NAS license file that you need to install. You should have received one license file for each Product Authorization Key (PAK) that you submitted during customer registration. The status information at the bottom of the page displays the total number of Cisco NASs enabled per successful license file installation.

Note You cannot remove individual FlexLM license files. To remove a file, you must remove all license files. After a permanent FlexLM license is installed, this permanent FlexLM license overrides an evaluation FlexLM license. Also, after FlexLM licenses are installed, FlexLM licenses (either permanent or evaluation) override legacy license keys (even though the legacy key does remain installed). When an evaluation FlexLM expires or is removed, an existing legacy license key will again take effect.

Protecting Your Cisco NAM Configuration

This topic describes the steps used to maintain a Cisco NAM configuration.



Protecting Your Cisco NAM Configuration

- Automated daily database snapshots:
  - Takes daily snapshots of the Cisco NAM database
  - Preserves snapshots for 30 days
  - Keeps five versions of upgrades and failover snapshots
- Manual backups from the web console:
  - Creates full backups before configuration changes
  - Contains all configuration data for the Cisco NAM except IP settings
  - Stores backup files on remote computers
- Detailed database restoration using the Database Recovery tool:
  - Provides command-line utility
  - Creates menu list of snapshots
  - Displays various messages and warnings

CANAC v2.1—5-20

In addition to protecting against loss of configuration data, snapshots provide an easy way to duplicate a configuration among several Cisco NAMs. Duplicating a configuration is required when deploying Cisco NAMs in high-availability mode.

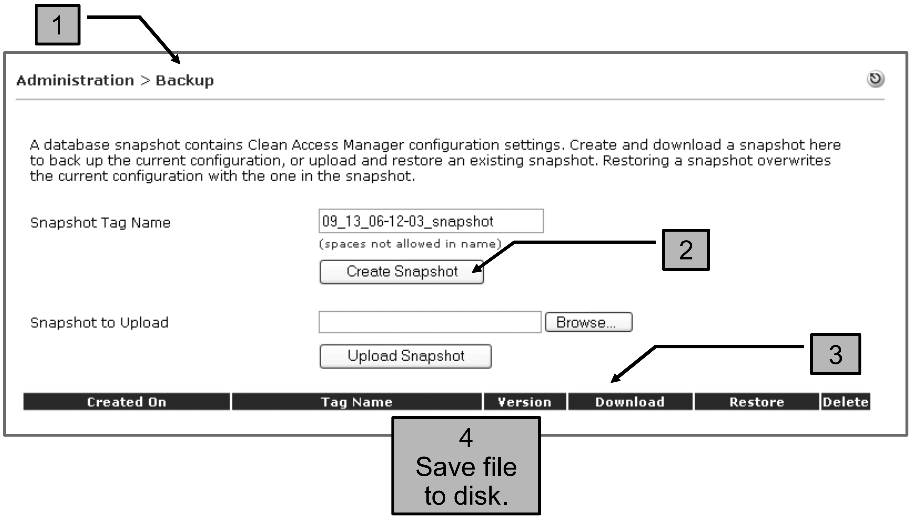
A backup contains all configuration data for the Cisco NAM except IP settings.

The Cisco NAM provides these backup procedures:

- **Automated daily database snapshots:** Cisco NAC Appliance automatically creates daily snapshots of the Cisco NAM database and preserves each snapshot recorded in the last 30 days. Cisco NAC Appliance also automatically creates snapshots before and after software upgrades and before and after failover events. In the event of upgrades and failovers, only the last five backup snapshots are kept.
- **Manual backups from the web console:** You should create a backup of the Cisco NAM configuration before making major changes to the configuration. Backing up the configuration regularly ensures that you have access to a recent backup that you know has a correct configuration profile. This backup can be referred to in case of a malfunction due to incorrect configuration settings.
- **The Database Recovery tool:** The Database Recovery tool is used to restore the database from the following types of backup snapshots:
  - Automated daily backups (the most recent 30 copies)
  - Backups made before and after software upgrades
  - Backups made before and after failover events
  - Manual snapshots created by the administrator via the web console

Although the web console already allows you to create and upload snapshots (via Administration > Backup), a more focused tool, the command-line interface (CLI) tool, presents the process in more detail. This tool provides a list of the snapshots that you can choose from in order to restore configuration data. Details listed by the CLI tool include various messages and warnings, such as how many tables are in the database, whether all files are in the proper format (for example: .tar.zip), whether files are corrupt, and whether the snapshot to be restored is for a different release than the release that is currently installed. After the administrator confirms that the configuration should be restored, the database is replaced with the chosen snapshot.

Creating Backups Manually for the Cisco NAM Configuration



Administration > Backup

A database snapshot contains Clean Access Manager configuration settings. Create and download a snapshot here to back up the current configuration, or upload and restore an existing snapshot. Restoring a snapshot overwrites the current configuration with the one in the snapshot.

Snapshot Tag Name 09_13_06-12-03_snapshot (spaces not allowed in name)

Create Snapshot

Snapshot to Upload Browse...

Upload Snapshot

Created On	Tag Name	Version	Download	Restore	Delete

CANAC v2.1—5-21

Follow these four steps to manually back up your Cisco NAM configuration:

Step 1 Choose **Administration > Backup**. The database Snapshot Tag Name field already contains a name that incorporates the current time and date (such as “11_10_04-18-13_snapshot”). You can either accept the default name or enter a new name in the field.

Step 2 Click **Create Snapshot**. The Cisco NAM generates a snapshot file that is added to the snapshot list.

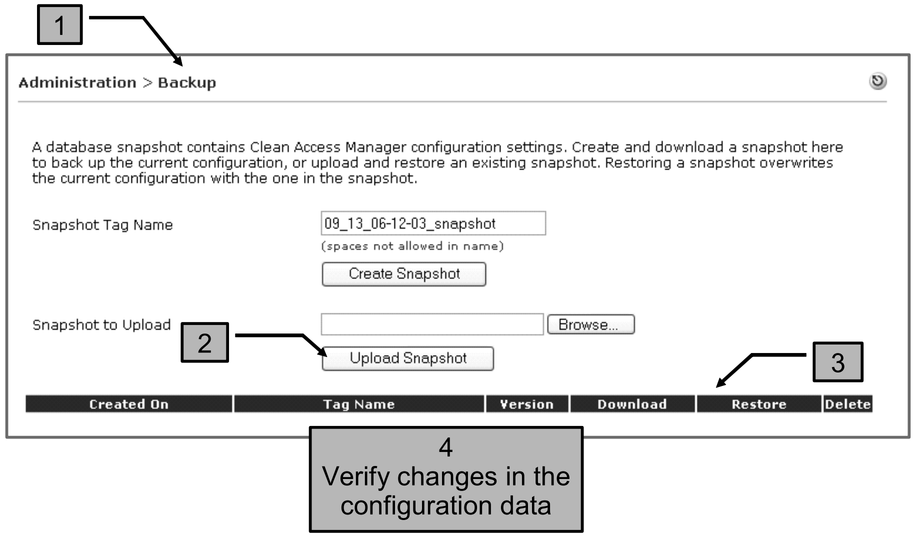
Note The file still physically resides on the Cisco NAM machine. For archiving purposes, the file can remain there. However, to back up a configuration that can be used in case of a system failure, the snapshot should be downloaded to another computer.

Step 3 To download the snapshot to another computer, click either the **Download** button or the tag name of the snapshot that you want to download. The file download dialog box appears.

Step 4 In the file download dialog box, choose the **Save File to Disk** option. You can now save the file to your local computer with the name that you provide.

Note To restore the Cisco NAM to the configuration state of the chosen snapshot, click the **Restore** button. The existing configuration is now overridden by the configuration in the snapshot. To remove the snapshot from the snapshot list, click the **Delete** button.

Recovering a Configuration From a Downloaded File



Administration > Backup

A database snapshot contains Clean Access Manager configuration settings. Create and download a snapshot here to back up the current configuration, or upload and restore an existing snapshot. Restoring a snapshot overwrites the current configuration with the one in the snapshot.

Snapshot Tag Name 09_13_06-12-03_snapshot
(spaces not allowed in name)

Create Snapshot

Snapshot to Upload Browse...

Upload Snapshot

Created On	Tag Name	Version	Download	Restore	Delete

4
Verify changes in the configuration data

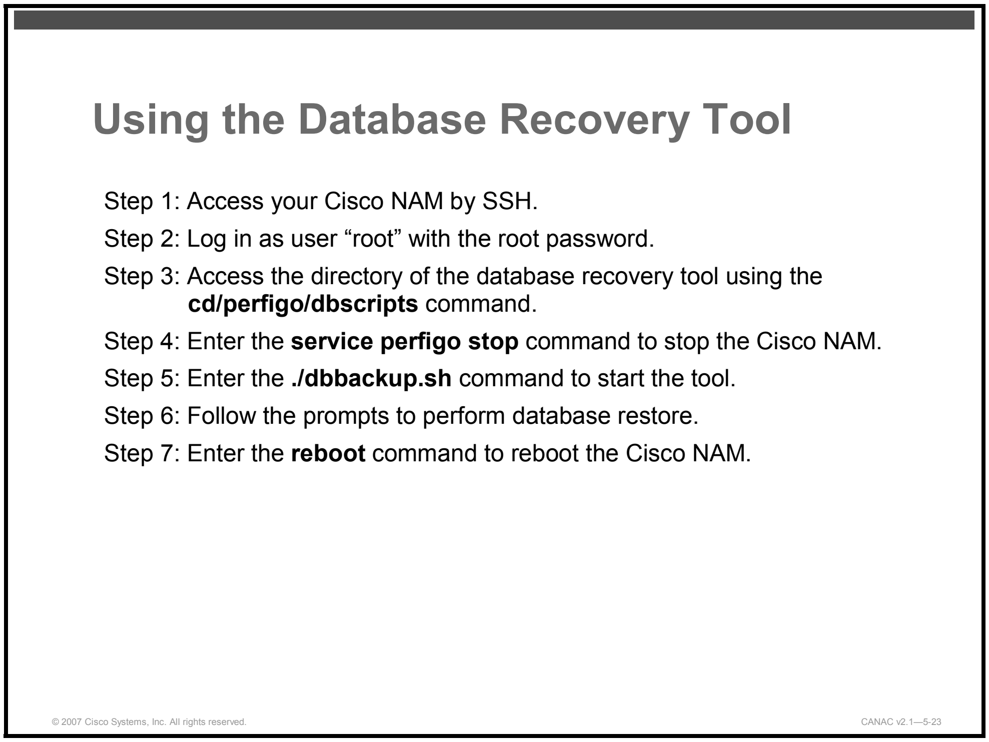
Follow these four steps to restore a Cisco NAM configuration from a file that is stored on a remote computer:

Step 1 Choose **Administration** > **Backup**. Click the **Browse** button next to the Snapshot to Upload field. Find the file you need in the directory system.

Step 2 Click **Upload Snapshot** and confirm that the snapshot now appears in the snapshot list.

Step 3 Click the **Restore** button next to the snapshot that you want to use. This action overwrites the current configuration with the snapshot configuration.

Step 4 Confirm the operation by verifying changes in the configuration data.



Using the Database Recovery Tool

Step 1: Access your Cisco NAM by SSH.

Step 2: Log in as user “root” with the root password.

Step 3: Access the directory of the database recovery tool using the **cd/perfigo/dbscripts** command.

Step 4: Enter the **service perfigo stop** command to stop the Cisco NAM.

Step 5: Enter the **./dbbackup.sh** command to start the tool.

Step 6: Follow the prompts to perform database restore.

Step 7: Enter the **reboot** command to reboot the Cisco NAM.

CANAC v2.1—5-23

Follow these seven steps to run the CLI Database Recovery tool:

Step 1 Access your Cisco NAM by SSH.

Step 2 Log on as user “root” with the root password (default password is “cisco123”).

Step 3 Access the directory of the Database Recovery tool using the **cd /perfigo/dbscripts** command.

Step 4 Enter the **service perfigo stop** command to stop the Cisco NAM.

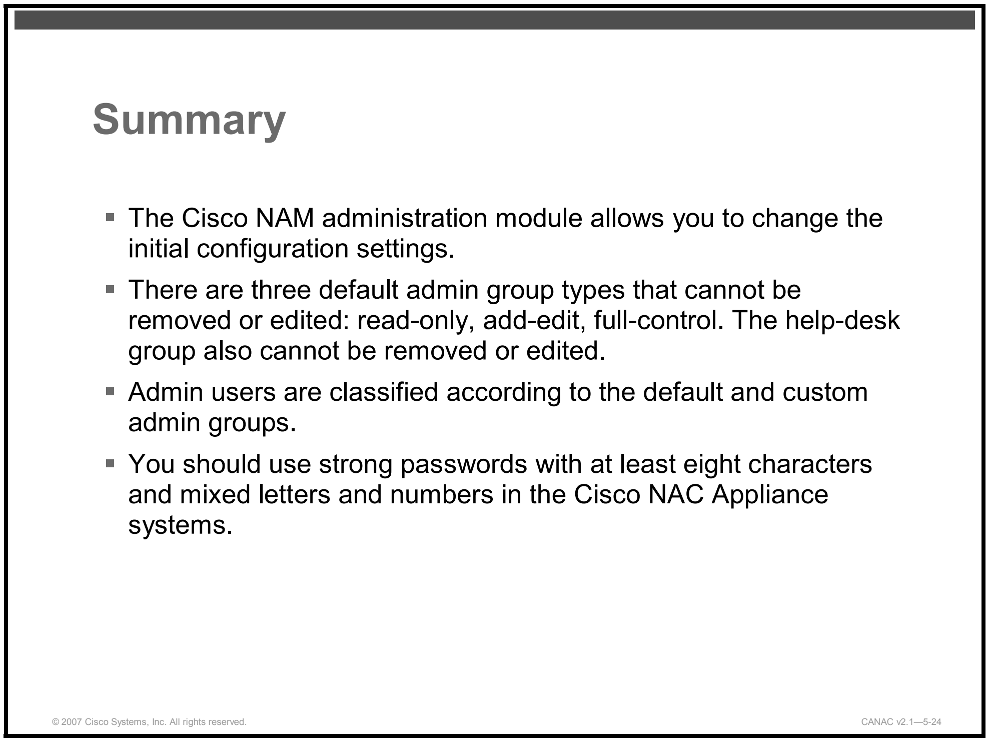
Step 5 Enter the**./dbbackup.sh** command to start the tool.

Step 6 Follow the prompts to restore the database.

Step 7 Enter the **reboot** command to reboot the Cisco NAM after running the utility.

Summary

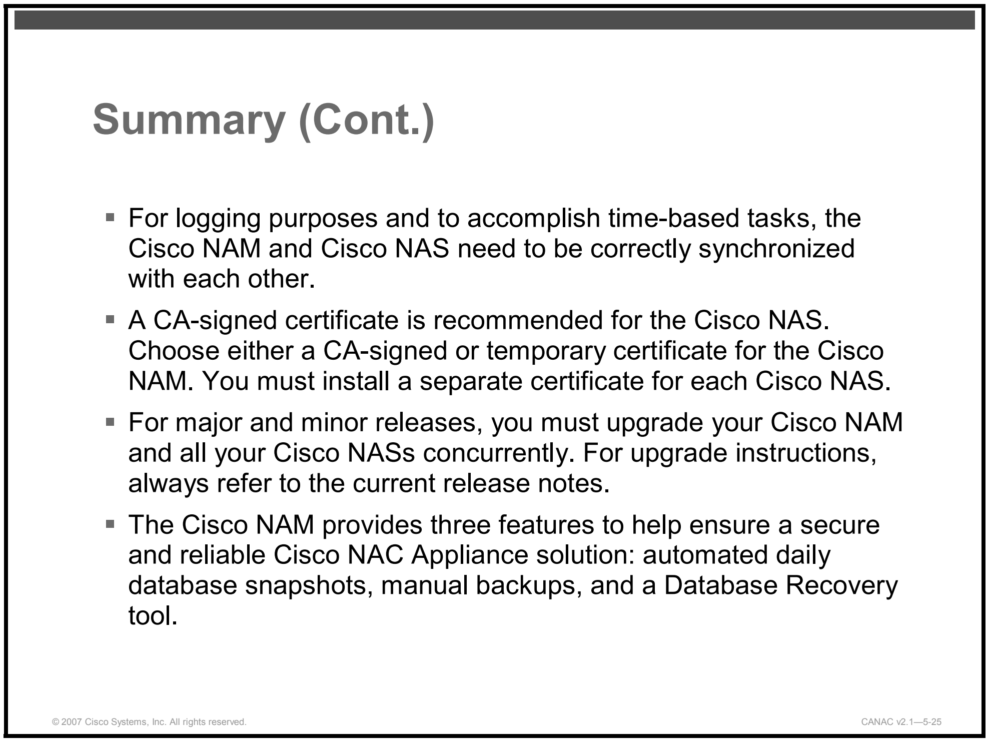
This topic summarizes the key points that were discussed in this lesson.



Summary

- The Cisco NAM administration module allows you to change the initial configuration settings.
- There are three default admin group types that cannot be removed or edited: read-only, add-edit, full-control. The help-desk group also cannot be removed or edited.
- Admin users are classified according to the default and custom admin groups.
- You should use strong passwords with at least eight characters and mixed letters and numbers in the Cisco NAC Appliance systems.

CANAC v2.1—5-24



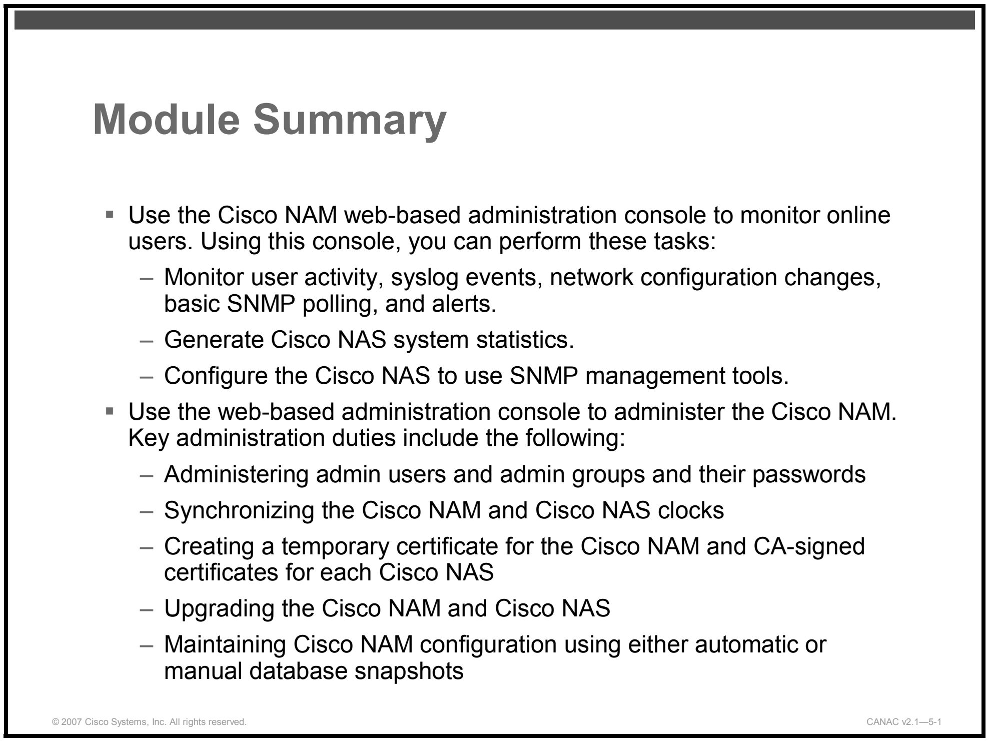
Summary (Cont.)

- For logging purposes and to accomplish time-based tasks, the Cisco NAM and Cisco NAS need to be correctly synchronized with each other.
- A CA-signed certificate is recommended for the Cisco NAS. Choose either a CA-signed or temporary certificate for the Cisco NAM. You must install a separate certificate for each Cisco NAS.
- For major and minor releases, you must upgrade your Cisco NAM and all your Cisco NASs concurrently. For upgrade instructions, always refer to the current release notes.
- The Cisco NAM provides three features to help ensure a secure and reliable Cisco NAC Appliance solution: automated daily database snapshots, manual backups, and a Database Recovery tool.

CANAC v2.1—5-25

Module Summary

This topic summarizes the key points that were discussed in this module.



Module Summary

- Use the Cisco NAM web-based administration console to monitor online users. Using this console, you can perform these tasks:
  - Monitor user activity, syslog events, network configuration changes, basic SNMP polling, and alerts.
  - Generate Cisco NAS system statistics.
  - Configure the Cisco NAS to use SNMP management tools.
- Use the web-based administration console to administer the Cisco NAM. Key administration duties include the following:
  - Administering admin users and admin groups and their passwords
  - Synchronizing the Cisco NAM and Cisco NAS clocks
  - Creating a temporary certificate for the Cisco NAM and CA-signed certificates for each Cisco NAS
  - Upgrading the Cisco NAM and Cisco NAS
  - Maintaining Cisco NAM configuration using either automatic or manual database snapshots

CANAC v2.1—5-1

This module describes how to administer and maintain a secure and reliable Cisco NAC Appliance solution in medium and enterprise network environments. The web-based administration console provides an easy-to-use interface to monitor online users, automatically generate system statistics, maintain current software versions, and keep configurations backed up. Although the Cisco NAC Appliance supports limited Simple Network Management Protocol (SNMP) capabilities, you can still manage your deployment using a third-party SNMP management tool. This module also provides you with the opportunity to practice your management and administration skills in a hands-on lab.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*. http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.
- Cisco Systems, Inc. *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*. http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) Which two items of information are found on the Cisco NAC Appliance Monitoring > Summary page? (Choose two.) (Source: Monitoring a Cisco NAC Appliance Deployment)

A) global subnets configured
B) current Cisco NAC Appliance Server version
C) current Cisco NAC Appliance Manager patch version
D) Cisco NAC Appliance Agents configured
E) online users

Q2) What is the last step that the Cisco NAM performs after a user is removed from the Out-of-Band Online Users list? (Source: Monitoring a Cisco NAC Appliance Deployment)

A) The Cisco NAM turns the switch port off and on.
B) The Cisco NAM changes the VLAN of the port based on the configured port profile associated with this controlled port.
C) The switch resends SNMP traps to the Cisco NAM.

Q3) Where are event logs located? (Source: Monitoring a Cisco NAC Appliance Deployment)

A) in the Cisco NAM database table
B) in the Cisco NAS database table
C) in the Cisco NAM installation root directory

Q4) What does the load factor refer to in a Cisco NAS health event log? (Source: Monitoring a Cisco NAC Appliance Deployment)

A) the current load being handled by the Cisco NAM
B) the number of packets waiting to be processed by the Cisco NAS
C) the maximum number of packets in the queue at any one time

Q5) What is an SNMP trap sink? (Source: Monitoring a Cisco NAC Appliance Deployment)

A) a computer configured to perform SNMP management
B) a computer configured with version 1.2a traps
C) an object created in the Cisco NAM to temporarily hold SNMP trap information

Q6) When does the Cisco NAM send SNMP traps? (Source: Monitoring a Cisco NAC Appliance Deployment)

A) when the Cisco NAA comes online
B) when the Cisco NAM shuts down
C) when user devices log on

Q7) How are admin users classified? (Source: Administering the Cisco NAM)

A) by user roles
B) by user role types
C) by administrator groups

Q8) How do you change the Cisco NAM root user password, the Cisco NAS root user password, and admin user password? (Source: Administering the Cisco NAM)

A) Use Telnet to access the appropriate server machine, log in as the user, and use the Linux **passwd** command to change the user password.
B) Use SSH to access the appropriate server machine, log in as the user, and use the Linux **passwd** command to change the user password.
C) Use the appropriate web-based administration console, navigate to the Administration > Admin Users > List, and change the passwords from that page.

Q9) How do you adjust the Cisco NAM system time? (Source: Administering the Cisco NAM)

A) Use SSH to connect to the Cisco NAM server, invoke the configtm.exe utility, and follow the instructions.
B) Navigate to the System Time tab from the Administration > Clean Access Manager page and manually change the time.
C) Navigate to the Change Time tab from the Administration > System Time page and select the NIST time server for automatic time updates.

Q10) Which SSL certificate-related operations can be performed using the Cisco NAM administration console? (Source: Administering the Cisco NAM)

A) Generate a CA-signed certificate.
B) Generate a PKCS #15 certificate request.
C) Import and export CA-signed private keys.
D) Generate a PKCS #10 certificate request.

Q11) What information does a Cisco NAM backup contain? (Source: Administering the Cisco NAM)

A) all configuration data for the Cisco NAM except IP settings
B) all configuration data for the complete restoration of Cisco NAM functionality
C) only configuration data from the Cisco NAM tables, IP settings, failover groups, and high-availability settings (if used)

Module Self-Check Answer Key

Q1)	A,E
Q2)	B
Q3)	A
Q4)	B
Q5)	A
Q6)	C
Q7)	C
Q8)	B
Q9)	B
Q10)	D
Q11)	A