CHAPTER 5

Performing User and System Administration

This chapter provides information about performing user and system administration tasks in Cisco Prime Network Analysis Module 5.1(3) and generating diagnostic information for obtaining technical assistance.

This chapter contains the following sections:

- System Administration, page 5-1, describes menu options that enable you to perform system administrative tasks and manage the NAM.
- Diagnostics, page 5-11, describes menu options that help you diagnose and troubleshoot problems.
- User Administration, page 5-13, describes how you configure either a local database or provide information for a ACS/TACACS+ database for user authentication and authorization. This section also describes the current user session window.
- Out-of-Band Management, page 5-22, describes how to use the Cisco Management Integrated Controller (CIMC) on the Cisco Prime NAM 2300 Series Appliances.

System Administration

The System option of the Administration menu provides access to the following functions:

- Resources, page 5-2
- Network Parameters, page 5-2
- SNMP Agent, page 5-3
- System Time, page 5-6
- E-Mail Setting, page 5-8
- Web Data Publication, page 5-9
- Syslog Setting, page 5-9
- SNMP Trap Setting, page 5-10
- Preferences, page 5-11

Resources

Choose **Administration** > **System** > **Resources** to view the System Overview window. Table 5-1 describes the fields of the System Overview window.

Table 5-1 System Overview

Field	Description
Date	Current date and time synchronized with the switch, router, or NTP server.
Hostname	NAM hostname.
IP Address	NAM IP address.
System Uptime	Length of time the host has been running uninterrupted.
CPU Utilization	Percentage of CPU resources being consumed by the NAM. Average, at top, indicates the average CPU usage of all CPUs. Each individual CPU in a multi-CPU platform is listed separately.
Memory Utilization	Percentage of memory resources being consumed by the NAM.
Memory Total	Total amount of system memory.
Disk Usage	Shows **root**, **config**, and **data** partitions with their total and free space.
Data Files	Shows the amount of disk space used up by the performance data base files (DB) and the packet capture to disk (capture files).
NIC Statistics	Shows the health and usage information on the data ports, where the NAM receives most of the traffic to be analyzed. It shows the number of packets received (rx pkts), number of bytes received (rx bytes) and number of packets lost or dropped (rx lost). The first number shows cumulative counts since the start of the NAM, and the second one shows the same counters for the last ten seconds.

Network Parameters

To view and set network parameters such as your site's name servers:

Step 1 Choose **Administration > System > Network Parameters**.

The Network Parameters window displays.

Step 2 Enter or change the information detailed in Table 5-2.

Note NAM 5.1(x) does not support using IPv6 for the network parameter IP address.

Table 5-2 Network Parameters Dialog Box

Field	Description
IP Address	NAM IP address.
IP Broadcast	NAM broadcast address.
Subnet Mask	NAM subnet mask.
IP Gateway	NAM IP gateway address.
Host Name	NAM hostname.
Domain name	NAM domain name.
Nameservers	NAM nameserver address or addresses.

Step 3 Do one of the following:

- To save the changes, click **Submit**.
- To cancel the changes, click **Reset**.

SNMP Agent

An SNMP Agent is a network management software module that resides in a managed device. It has local knowledge of management information and translates that information into a form compatible with SNMP.

You can manage devices with SNMPv3 in addition to SNMPv2 and SNMPv1. The NAM polls the managed device to get its basic health and interface stats. For NAM blades, the managed device is the switch in which the NAM is inserted, and the NAM software negotiates with the switch to use SNMP and a community string to do the polling. This community string is only valid for use with the NAM. For security purposes, the switch associates the community string with the NAM's IP address only, and no other SNMP application can use this community string to communicate with the switch. For more information about community strings, see Working with NAM Community Strings, page 5-4.

Also, to further alleviate any security concerns, the SNMP exchanges between NAM blades and the switch take place on an internal backplane bus. These SNMP packets are not visible on any network, nor any interface outside of the switch. It is a completely secure out-of-band channel inside the switch.

For other platforms, such as Cisco NAM appliances, you can type in any IP address and use it as the managed device. In setting managed devices, virtual NAM platforms managed devices function just like the NAM appliances. On all platforms, NAM can only monitor and display data for one managed device at a time.

In this case, the managed device may only want to use SNMPv3 since it is more secure.

Note NAM blades use SNMPv2 to manage the locally managed device.

To view and set the NAM SNMP Agent:

Step 1 Choose **Administration > System > SNMP Agent**.

Step 2 Enter or change the information in the NAM SNMP window. The fields are detailed in Table 5-3.

Table 5-3 System SNMP Dialog Box

Field	Description
Contact	The name of the person responsible for the NAM.
Name	The name of the NAM.
Location	The physical location of the switch or router in which the NAM is installed.

Step 3 Do one of the following:

- To save the changes, click **Submit**.
- To cancel the changes, click **Reset**.

Step 4 Set the NAM community strings. See Working with NAM Community Strings, page 5-4.

Working with NAM Community Strings

You use community strings so that other applications can send SNMP get and set requests to the NAM, set up collections, poll data, and so on.

Creating NAM Community Strings

To create the NAM community strings:

Step 1 Choose **Administration > System > SNMP Agent**.

At the bottom of the window, the NAM Community Strings Dialog Box displays.

Step 2 Click **Create**.

The SNMP Agent Dialog Box displays.

Step 3 Enter the community string (use a meaningful name).

Step 4 Enter the community string again in the Verify Community field.

Step 5 Assign read-only or read-write permissions using the following criteria:

- Read-only allows only read access to SNMP MIB variables (get).
- Read-write allows full read and write access to SNMP MIB variables (get and set).

Step 6 Do one of the following:

- To make the changes, click **Submit**.
- To reset, click **Reset**.

- To cancel and return to the previous window, click **Cancel**.

Deleting NAM Community Strings

To delete the NAM community strings:

Step 1 Choose **Administration > System > SNMP Agent**.

At the bottom of the window, the NAM Community Strings Dialog Box displays.

Step 2 Select an entry, then click **Delete**.

⚠

Caution Deleting the NAM community strings blocks SNMP requests to the NAM from outside SNMP agents.

The community string is deleted.

Testing the Router Community Strings

Before the router can send information to the NAM using SNMP, the router community strings set in the NAM must match the community strings set on the actual router. The Router Parameters dialog box displays the router name, hardware, Supervisor engine software version, system uptime, location, and contact information.

The local router IP address and the SNMP community string must be configured so that the NAM can communicate with the local router.

To set the community strings on the router, use the router CLI. For information on using the CLI, see the documentation that accompanied your device.

⚠

Caution The router community string you enter must match the read-write community strings on the router. Otherwise you cannot communicate with the router.

To test router community strings:

Step 1 Choose **Setup** > **Managed Device > Device Information**.

The Device Information dialog box displays.

Step 2 Enter the Device's Community String.

Step 3 Click **Test Connectivity**.

Step 4 Wait for a while for NAM to communicate with the Device. If it comes back OK, then click on **Submit**.

System Time

The NAM gets the UTC (GMT) time from several sources, depending on its the NAM type. All NAMs can be set up to get their time from an external NTP server.

Caution Both the client computer and the NAM server must have the time set accurately for their respective time zones. If either the client or the server time is wrong, then the data shown in the GUI will be wrong.

The clock identity is the first three octets of the MAC address, followed by “ff fe,” and then the last three octets of the MAC address, as shown in the example below.

```
root@nam.localdomain# sho time ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xec:44:76:ff:fe:5d:12:0
  Parent Port Number: 6
```

After the NAM acquires the time, you can set the local time zone using the NAM System Time configuration window.

You can configure the NAM system time by using one of the following methods:

- Synchronizing the NAM System Time with the Switch or Router, page 5-6

  This option is valid only for WS-SVC-NAM-1, WS-SVC-NAM-2, WS-SVC-NAM-3, NME-NAMs, and SM-SREs.

- Synchronizing the NAM System Time Locally, page 5-7

  This option is valid for Cisco Prime NAM appliances, Nexus 1010 VSB, and WAAS Virtual Blade NAM.

- Configuring the NAM System Time with an NTP Server, page 5-7
- Configuring the NAM System Time with Precision Time Protocol (IEEE 1588), page 5-7

  This option is valid for WS-SVC-NAM-3.

Synchronizing the NAM System Time with the Switch or Router

Note This section is valid only for WS-SVC-NAM-1, WS-SVC-NAM-2, and NME-NAMs.

To configure the NAM system time from the switch or router:

Step 1 Choose **Administration > System > System Time**.

Step 2 Choose the Switch or Router radio button.

Step 3 Select the Region and local time zone from the lists.

Step 4 Do one of the following:

- To save the changes click **Submit**.
- To leave the configuration unchanged, click **Reset**.

Synchronizing the NAM System Time Locally

Note This section is valid for Cisco NAM appliances, Nexus, and WAAS NAM.

To configure the NAM system time locally using the NAM appliance command line:

Step 1 Log into the NAM appliance command line interface.

Step 2 Set the clock using the CLI **clock set** command.

clock set *<hh:mm:ss:> <mm/dd/yyyy>*

Step 3 On the NAM appliance GUI, choose **Administration > System > System Time**.

Step 4 Click the **Local** radio button.

Step 5 Select the Region and local time zone from the lists.

Step 6 Do one of the following:

- To save the changes click **Submit**.
- To leave the configuration unchanged, choose **Reset**.

Configuring the NAM System Time with an NTP Server

To configure the NAM system time with an NTP server:

Step 1 On the NAM appliance GUI, choose **Administration > System > System Time**.

Step 2 Choose the **NTP Server** radio button.

Step 3 Enter one or two NTP server names or IP address in the NTP server name/IP Address text boxes.

Step 4 Select the Region and local time zone from the lists.

Step 5 To save the changes, click **Submit**.

Configuring the NAM System Time with Precision Time Protocol (IEEE 1588)

To use Precision Time Protocol (PTP), you will need to have a PTP-aware or multicast-enabled switch connected to the sync port on the front of the NAM-3, as well as a PTP master connected to the switch.

To configure the NAM system time using PTP:

Step 1 On the NAM, choose **Administration > System > System Time**.

Step 2 Choose the **PTP** radio button.

Step 3 Enter the IP address of the PTP interface in the “PTP Interface IP Address” field.

Step 4 Enter the subnet mask in the “PTP Interface Subnet Mask” field.

Step 5 For NAM Local Time Zone, select the Region and the Zone from the drop-down lists.

Step 6 To save the changes, click **Submit** and continue to the next section, Displaying Precision Time Protocol Status, to show detailed PTP information.

Displaying Precision Time Protocol Status

Step 1 Configure PTP using the Configuring the NAM System Time with Precision Time Protocol (IEEE 1588) steps above (this must be done before the status can successfully be displayed).

Step 2 Choose **Administration > System > System Time**.

Step 3 Make a selection from the drop-down menu and click the **Show** button. The pop-up window that appears will give you detailed information about the selection you chose:

- clock
- foreign-master-record
- parent
- time-property

E-Mail Setting

You can configure the NAM to provide e-mail notification of alarms and to e-mail reports. To configure the NAM for e-mail notifications:

Step 1 Choose **Administration** > **System > E-Mail Setting**.

Step 2 The Mail Configuration Window displays. Table 5-4 describes the Mail Configuration Options.

Table 5-4 Mail Configuration Options

Field	Description
Enable Mail	Enables e-mail of reports and notification of alarms
External Mail Server	Distinguished name of external mail server
Send Test Mail	List e-mail addresses for up to three e-mail recipients
Mail Alarm to	This recipient will receive alarm notifications and scheduled exports.

Step 3 Check the **Enable Mail** check box.

Step 4 Enter the distinguished name of the **External Mail Server**.

Step 5 Put an e-mail address in the **Send Test Mail to** field (optional). A test e-mail will be sent to this recipient.

Step 6 Put an e-mail address in the **Mail Alarm to** field. Alarm notifications and Exports will be sent to this recipient.

Step 7 Click **Submit** to save your modifications, or click **Reset** to clear the dialog of any characters you entered or restore the previous settings.

Web Data Publication

Web Data Publication allows general web users and websites to access (or link to) selected NAM monitor and report windows without a login session.

Web Data Publication can be open or restricted using Access Control List (ACL) and/or publication code. The publication code, if required, must be present in the URL address or cookie to enable access to published data.

To enable Web Data Publishing:

Step 1 Choose **Administration** > **System > Web Data Publication**.

Step 2 Check the Enable Web Data Publication check box.

Step 3 Enter a Publication Code (Optional). This is the pass code required in a URL's cookie to access the published page. For example, a publication code set to *abc123* would be able to access the following published window:

http://<nam-hostname>/application-analysis/index?publicationcode=abc123

Step 4 Enter an ACL Permit IP Address/Subnets to permit only those IP addresses or subnets access to web publications. No entry provides open access to all.

Step 5 Click **Submit** to enable web publishing, or click **Reset** to clear the dialog of any characters you entered.

Note Before the new iSCSI storage entry takes effect, you must reboot the NAM system.

Syslog Setting

NAM syslogs are created for alarm threshold events, voice threshold events, or system alerts. You can specify whether syslog messages should be logged locally on the NAM, on a remote host, or both. You can use the NAM to view the local NAM syslogs.

Note Prime NAM sends syslog alerts for audit trail events and configured alarm threshold events. Prime NAM does *not* send syslog alerts about its own physical state (temperature levels or interface status changes). For a list of user activities logged in the audit trail window, see Audit Trail, page 5-12.

If logging on a remote host, in most Unix-based systems, the syslog collector that handles the incoming syslog messages uses the facility field to determine what file to write the message to, and it will use a facility called *local7*. Check the syslog collector configuration to ensure that *local7* is handled properly.

To set up the NAM syslog:

Step 1 Choose **Administration** > **System > Syslog Setting**.

The NAM Syslog Setting window displays.

Step 2 In the Remote Server Names field, enter the IP address or DNS name of up to five remote systems where syslog messages are logged. Each address you enter receives syslog messages from all three alarms (Alarm Thresholds, Voice Signaling Thresholds, and System).

Step 3 Click **Submit** to save your changes, or click **Reset** to cancel.

SNMP Trap Setting

Traps are used to store alarms triggered by threshold crossing events. When an alarm is triggered, you can trap the event and send it to a separate host. Trap-directed notifications can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests.

These topics help you set up and manage NAM traps:

- Creating a NAM Trap Destination, page 5-10
- Editing a NAM Trap Destination, page 5-10
- Deleting a NAM Trap Destination, page 5-11

Creating a NAM Trap Destination

To create a NAM trap destination:

Step 1 Choose **Administration > System > SNMP Trap Setting**.

The SNMP Trap Setting window displays.

Step 2 Click the **Create** button.

Step 3 In the "Community" field, enter the community string set in the NAM Thresholds.

Step 4 In the "IP Address" field, enter the IP address to which the trap is sent if the alarm and trap community strings match.

Step 5 In the "UDP Port" field, enter the UDP port number.

Step 6 Click **Submit** to save your changes, or click **Reset** to cancel and leave the configuration unchanged.

Editing a NAM Trap Destination

To edit a NAM trap destination:

Step 1 Choose **Administration > System > SNMP Trap Setting**.

The NAM Trap Destinations page displays.

Step 2 Select the trap to edit, then click **Edit**.

The Edit Trap dialog box displays.

Step 3 Make the necessary changes.

Step 4 Click **Submit** to save your changes, or click **Reset** to remove any entry.

Deleting a NAM Trap Destination

To delete an existing trap, simply select it from the Traps table, then click **Delete**.

Preferences

Choose **Administration > System > Preferences** to configure characteristics for the NAM such as NAM display, audit trail, and file format preferences. Table 5-5 describes the fields of the Preferences window.

Table 5-5 Preferences

Field	Description
Refresh Interval (60-3600 sec)	Amount of time between refresh of information on dashboards.
Top N Entries (1-10)	Number of colored bars on the Top N charts.
Perform IP Host Name Resolution	Wherever an IP address is displayed, it will get translated to a hostname via DNS lookup.
Data Displayed In	Data displayed in Bytes or Bits.
International Notation	Choose the way you would like numbers displayed.
Audit Trail	The Audit Trail option displays a listing of recent critical activities that have been recorded in an internal syslog log file. Syslog messages can also be sent to an external log.
Capture File Download Format	Choose ENC (**.enc**) or PCAP (**.pcap**) format for captured files.

Diagnostics

The Diagnostics option of the **Administration** menu provides tools to aid in troubleshooting. You can use these tools when you have a problem that might require assistance from the Cisco Technical Assistance Center (TAC). There are options for:

- System Alerts, page 5-11
- Audit Trail, page 5-12
- Tech Support, page 5-12

System Alerts

You can view any failures or problems that the NAM has detected during normal operations. To view System Alerts, choose **Administration** > **Diagnostics > System Alerts**.

Each alert includes a date, the time the alert occurred, and a message describing the alert. The NAM displays up to one thousand (1,000) of the most-recent alerts. If more than 1,000 alerts have occurred, you need to use the NAM CLI command **show tech support** to see all of the alerts.

If you notice an alert condition and troubleshoot and attempt to solve the condition causing the alert, you might want to click **Clear** to remove the list of alerts to see if additional alerts occur.

Audit Trail

The Audit Trail option displays a listing of recent critical activities that have been recorded in an internal **syslog** log file. Syslog messages can also be sent to an external log.

The following user activities are logged in the audit trail:

- All CLI commands
- User logins (including failed attempts)
- Unauthorized access attempts
- SPAN changes
- NDE data source changes
- Enabling and disabling data collections
- Starting and stopping captures
- Adding and deleting users

Each log entry will contain the following:

- User ID
- Time stamp
- IP address (in case of remote web access)
- Activity description

To access the audit trail window:

Step 1 Choose **Administration** > **Diagnostics** > **Audit Trail**.

The Audit Trail Window displays.

The Audit Trail window provides a way to view the user access log and filter entries based on time, user, (IP address) from or activity. The internal log files are rotated after reaching certain size limit.

Tech Support

The NAM syslog records NAM system alerts that contain event descriptions and date and time stamps, indicating unexpected or potentially noteworthy conditions. This feature generates a potentially extensive display of the results of various internal system troubleshooting commands and system logs. For a list of user activities logged in the audit trail window, see Audit Trail, page 5-12.

This information is unlikely to be meaningful to the average user. It is intended to be used by the Cisco TAC for debugging purposes. You are not expected to understand this information; instead, you should save the information and attach it to an email message to the Cisco TAC.

Before you can view the Tech-Support page, you must enable the System Config user privilege on the **Administration** > **Users > Local Database** page. For more information on editing user privileges, see Editing a User, page 5-15.

Note You can also view this information from the NAM CLI. For information on using the NAM CLI, see *Cisco Network Analysis Module Command Reference*.

To view tech support:

Step 1 Choose **Administration > Diagnostics > Tech Support**.

After a few minutes, extensive diagnostic information is generated and displayed in the Diagnostics Tech Support Window.

Step 2 To save the information, either select **File>Save As...** from the browser menu, or scroll to the bottom, click on NAM-logs.tar.bz2, and save it to your local PC.

Downloading Core Files

To download core files from the Tech-Support page, scroll down to the Core Files section and click on the filename and follow the instructions.

User Administration

The User Administration option of the **Administration** menu provides the following options:

- Local Database, page 5-13
- Establishing TACACS+ Authentication and Authorization, page 5-16
- Configuring a TACACS+ Server to Support NAM Authentication and Authorization, page 5-17
- Current User Sessions, page 5-21

Local Database

When you first install the NAM, you use the NAM command-line interface (CLI) to enable the HTTP server and establish a username and password to access the NAM for the first time.

After setting up the initial user accounts, you can create additional accounts, enabling or disabling different levels of access independently for each user.

Table 5-6 provides information about User Privileges and describes each privilege.

Table 5-6 User Privileges

Privilege	Access Level
AccountMgmt	Enables a user to create, delete, and edit user accounts.
SystemConfig	Enables a user to edit basic NAM system parameters such as IP address, gateway, HTTP port, and so on.
Capture	Enables a user to perform packet captures and manage capture sessions Use the NAM protocol decode.
AlarmConfig	Enables a user to create, delete, and edit alarms on the switch/router and NAM.

Table 5-6 User Privileges (continued)

Privilege	Access Level
MonitorConfig	Enables a user to create, delete, and edit the following: • Collections and reports • Protocol directory entries • Protocol groups • URL-based applications
MonitorView	Enables a user to view monitoring data and reports (granted to all users).

For additional information about creating and editing users, see Creating a New User, page 5-14 and Editing a User, page 5-15.

Resetting Passwords

You can recover passwords by using CLI commands on the switch or router. A user with appropriate privileges can reset the NAM CLI and passwords to the factory default state.

For information on resetting the NAM passwords, see your platform installation guide on Cisco.com.

If you have forgotten the NAM administrator password, you can recover it using one of these methods:

- If other users have account management permission, delete the user for whom you have forgotten the password; then create a new one by logging in as that other user by choosing **Admin > Users > Local Database**.
- If no other local users are configured other than the user for whom you have forgotten the password, use the NAM **rmwebusers** CLI command; then enable http or https to prompt for the creation of a NAM user.

Changing Predefined NAM User Accounts on the Switch or Router

The predefined root and guest NAM user accounts (accessible through either a switch or router **session** command or a Telnet login to the NAM CLI) are static and independent of the NAM. You cannot change these static accounts nor can you add other CLI-based users with the NAM.

Creating a New User

To create a new user:

Step 1 Choose **Administration** > **Users > Local Database**.

The GUI displays the users in the local database. Checks indicate the privileges each user has for the functions listed.

Step 2 Click **Create**.

The GUI displays the New User Dialog Box.

Step 3 Enter the information required to create new user and select each privilege to grant to the user. See Table 5-6 for an explanation of user privileges. Table 5-7 describes the fields in the New User Dialog Box.

Table 5-7 New User Dialog Box

Field	Description	Usage Notes
Name	The account name	Enter the user's account name.
Password **Verify Password**	The account password	Enter a password that adheres to your site security policies.
Privileges	Privileges associated with this account	Select each privilege to grant to the user.

Usernames and passwords cannot exceed 32 characters and can be alphanumeric. The following special characters are not allowed:

'!' '@' '#' '$' '%' '^' '&' '*' '(' ')'

- Greater than (<)
- Less than (>)
- Comma (,)
- Period (.)
- Double quote (")
- Single quote (')
- Left or right parentheses
- Other special characters (!,@,$,%,^,&,*)

Step 4 Click **Submit** to create the user or **Reset** to clear the dialog of any characters you entered.

Editing a User

To edit a user's configuration:

Step 1 Choose **Administration** > **Users > Local Database**.

The Users table displays.

Step 2 Select the username.

Step 3 Click **Edit**.

Step 4 In the Modify Users dialog box, change whatever information is necessary.

Click **Submit** to save your changes, or click **Reset** to clear the dialog of any characters you entered and restore the previous settings.

Deleting a User

To delete a user:

Step 1 Choose the **Administration** > **Users > Local Database**.

The Users table displays.

Step 2 Select the username.

Step 3 Click **Delete**.

Note If you delete user accounts while users are logged in, they remain logged in and retain their privileges. The session remains in effect until they log out. Deleting an account or changing permissions in mid-session affects only future sessions. To force off a user who is logged in, restart the NAM.

Establishing TACACS+ Authentication and Authorization

Terminal Access Controller Access Control System (TACACS) is an authentication protocol that provides remote access authentication, authorization, and related services such as event logging. With TACACS, user passwords and privileges are administered in a central database instead of an individual switch or router to provide scalability.

TACACS+ is a Cisco Systems enhancement that provides additional support for authentication and authorization.

When a user logs into the NAM, TACACS+ determines if the username and password are valid and what the access privileges are.

To establish TACACS+ authentication and authorization:

Step 1 Choose **Administration** > **Users > TACACS+**. The TACACS+ Authentication and Authorization Dialog Box displays.

Step 2 Enter or select the appropriate information in the TACACS+ Authentication and Authorization Dialog Box (Table 5-8).

Table 5-8 TACACS+ Authentication and Authorization Dialog Box

Field	Usage Notes
Enable TACACS+ Authentication and Authorization	Determines whether TACACS+ authentication and authorization is enabled. • To enable, check the check box. • To disable, uncheck the check box.
Primary TACACS+ Server	Enter the IP address of the primary server.
Backup TACACS+ Server	Enter the IP address of the backup server (optional). **Note** If the primary server does not respond after 30 seconds, the backup server will be contacted.
Secret Key	Enter the TACACS+ secret key.
Verify Secret Key	Reenter the TACACS+ secret key.

Step 3 Do one of the following:

- To save the changes, click **Submit**.
- To cancel, click **Reset**.

Tip If you cannot log into the NAM with TACACS+ configured, verify that you entered the correct TACACS+ server name and secret key.

Configuring a TACACS+ Server to Support NAM Authentication and Authorization

In addition to enabling the TACACS+ option, you must configure your TACACS+ server so that it can authenticate and authorize NAM users. NAM 5.1 and later releases support ACS versions 5.2, 5.1 (including Patch 1), and 4.2.

Note Configuration methods vary depending on the type of TACACS+ server you use.

Continue to the section specific to your particular version:

- Configuring a Cisco ACS Server, Version 4.2.
- Configuring a Cisco ACS Server, Version 5.x
- Configuring a Generic TACACS+ Server

Configuring a Cisco ACS Server, Version 4.2

To configure a version 4.2 Cisco ACS server, you must perform two tasks:

- Configure the NAM hostname and IP address on the ACS server. See Configuring NAM on ACS for Windows NT and 2000 Systems for Version 4.2, page 5-17.
- Add a NAM user or user group. See Adding a NAM User or User Group for Version 4.2, page 5-18.

Configuring NAM on ACS for Windows NT and 2000 Systems for Version 4.2

To configure a Cisco ACS TACACS+ server (version 4.2):

Step 1 Log into the ACS server.

Step 2 Click **Network Configuration**.

Step 3 Click **Add Entry**.

Step 4 For the Network Access Server, enter the NAM hostname and IP address.

Step 5 Enter the secret key.

Note The secret key must be the same as the one configured on the NAM.

Step 6 In the Authenticate Using field, select **TACACS+**.

Step 7 Click **Submit+Apply**.

Step 8 Continue to Adding a NAM User or User Group for Version 4.2 to complete the next configuration task.

Adding a NAM User or User Group for Version 4.2

To add a NAM user or user group:

Step 1 Click **User Setup**.

Step 2 Enter the user login name.

Step 3 Click **Add/Edit**.

Step 4 Enter the user data.

Step 5 Enter a user password.

Step 6 If necessary, assign a user group.

Step 7 In the TACACS+ settings:

a. Select **Shell**.

b. Select **IOS Command**.

c. Select **Permit**.

d. Select **Command**.

e. Enter **web**.

f. In the Arguments field, enter:

```
permit capture
permit system
permit collection
permit account
permit alarm
permit view
```

Step 8 In Unlisted Arguments, select **Deny**.

Step 9 Click **Submit**.

Configuring a Cisco ACS Server, Version 5.x

To configure a version 5.1 (Patch 1) or 5.2 Cisco ACS server, you must perform these tasks. There is an additional configuration task that enables you to set up policy rules for your users or groups.

- Configure the NAM hostname and IP address on the ACS server. SeeConfiguring NAM on ACS For Windows NT and 2000 Systems for Version 5.x, page 5-19.
- Add a NAM user or user group. See Adding a NAM User or User Group for Version 5.x, page 5-19.
- Set up your policy rules. See Configuring Access Policies for ACS and NAM for Version 5.x, page 5-19.

Configuring NAM on ACS For Windows NT and 2000 Systems for Version 5.x

To configure a Cisco ACS TACACS+ server (version 5.1(P1) or 5.2):

Step 1 Log into the ACS server.

Step 2 To set up an optional device type for NAM, click **Network Resources > Network Device Groups > Device Type** and create a device type. For example, you may choose to name your device type *NAM_Module*.

Step 3 Click **Network Resources > Network Devices and AAA Clients** to add NAM devices.

Step 4 For the Network Access Server, enter the NAM hostname and IP address.

Step 5 Under Authentication Options field, select **TACACS+**.

Step 6 Enter the secret key.

Note The secret key must be the same as the one configured on the NAM.

Step 7 Click **Submit**.

Step 8 Continue to Adding a NAM User or User Group for Version 5.x, page 5-19 to complete the next configuration task.

Adding a NAM User or User Group for Version 5.x

To add a NAM user or user group:

Step 1 Click **Users and Identity Stores > Internal Identity Stores > Users.**

Step 2 Click **Create**.

Step 3 Enter the user login name.

Step 4 Enter the user data.

Step 5 If necessary, assign a user group.

Step 6 Enter the password information.

Step 7 Click **Submit**.

Configuring Access Policies for ACS and NAM for Version 5.x

In versions 5.1(P1) and 5.2 you must set up access policies to complete your ACS and NAM configuration.

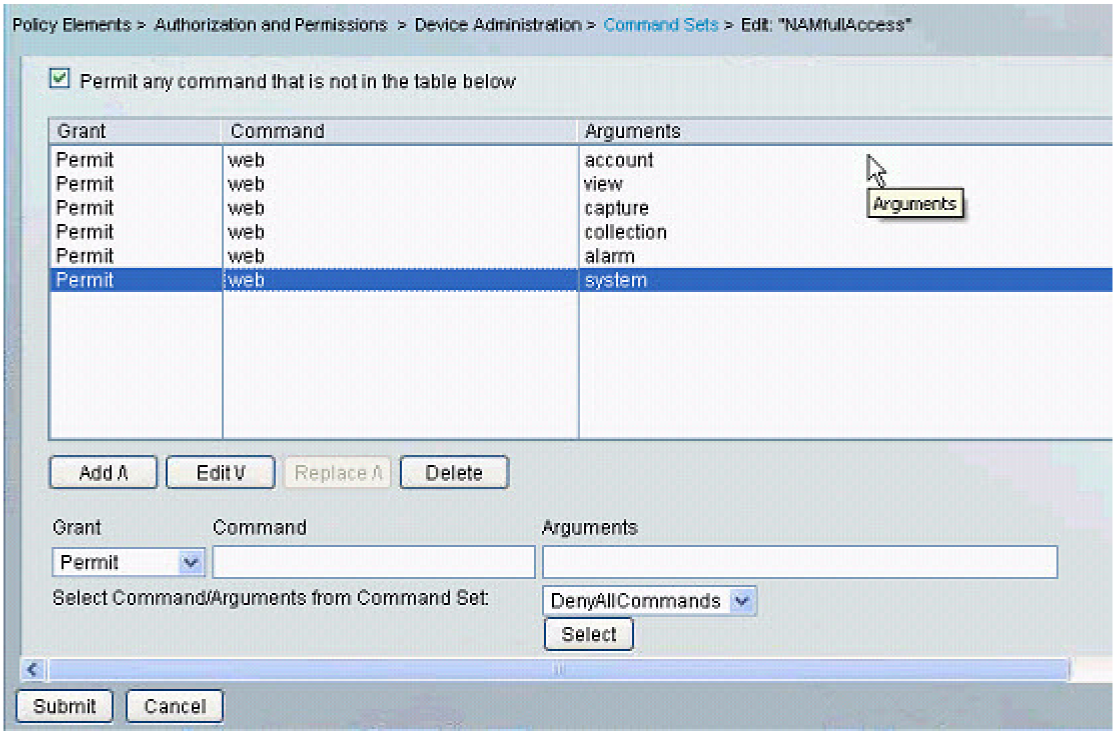
Step 1 On the ACS server, click **Policy Elements > Authorization and Permissions > Device Administration > Command Sets** and click **Create** to create NAM command sets.

For example, if you want to provide full access to the NAM, create a command set called *NAMfullAccess* and select the checkbox **Permit any command that is not in the table below**.

Step 2 Click **Submit** when you have completed entering the NAM command sets (see . Ensure you include all of the following commands:

```
permit capture
permit system
permit collection
permit account
permit alarm
permit view
```

Figure 5-1 NAMFullAccess Command Set Example



Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Edit: "NAMfullAccess"

☑ Permit any command that is not in the table below

Grant	Command	Arguments
Permit	web	account
Permit	web	view
Permit	web	capture
Permit	web	collection
Permit	web	alarm
Permit	web	system

Grant: Permit
Command:
Arguments:
Select Command/Arguments from Command Set: DenyAllCommands

Step 3 Click **Access Policies > Access Services > Create** to create a new Service (for example, name = *namAdmin*; Service Type = Device Administration.)

Go to **Access Policy > Access Services >** *namAdmin* **> Authorization**. Replace *namAdmin* with the service you created in this step.

Set up the condition to qualify all login requests; NAM devices uses these conditions and follows the command set (created in Step 1). For example: your condition may be == NDG: Device Type is All Device Types: NAM device which you set up in Step 2.

Step 4 Log into the NAM and click **NAM > Administration > Users > TACACS+** to set up the ACS server IP and secret key.

Configuring a Generic TACACS+ Server

To configure a generic TACACS+ server:

Step 1 Specify the NAM IP address as a Remote Access Server.

Step 2 Configure a secret key for the TACACS+ server to communicate with the NAM.

Note The secret key must be the same as the one configured on the NAM.

Step 3 For each user or group to be allowed access to the NAM, configure the following TACACS+ parameters:

Parameter	Enter
service	**shell**
cmd	**web**
cmd-arg	One or more the following: **accountmgmt** **system** **capture** **alarm** **collection** **view**
password authentication method—Password Authentication Protocol (PAP)	**pap**

Current User Sessions

The Current User Sessions table is a record of the users who are logged into the application. The user session times out after 30 minutes of inactivity. After a user session times out, that row is removed from the table.

To view the current user sessions table:

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

The Current User Sessions Table (Table 5-9) displays.

Table 5-9 Current User Sessions Table

Field	Description
User ID	The user ID used to log into the NAM.
From	The name of the machine the user logged in from.
Login Time	The time the user logged in.
Last Activity	The time stamp of the last user activity.

Out-of-Band Management

There are several tasks for which you should use the Prime NAM 2300 series appliances' management interface known as the Cisco Integrated Management Controller (CIMC). You can use this out-of-band management GUI tool by connecting to LAN port 1 (which provides external system console access to both the CIMC and NAM management port.

Table 5-10 provides details about the tasks you can use the CIMC to perform. You can also access the CIMC online help by selecting the help button on the window's task menu.

Table 5-10 When to Use CIMC

CIMC Menu	Management Tasks
Power On Server	Power on the appliance
Power Off Server	Power off the appliance
Shut Down Server	Shut down the appliance.
Power Cycle Server (instead of pulling out the power plug)	Immediately power off the server and power it on again.
Hard Reset Server—reboots the appliance.	Reboot the appliance.
Launch KVM Console	• View the serial console remotely without any connection to a terminal server • Perform a recovery/ISO install
Turn On Locator LED/Turn Off Locator LED	Locate the physical appliance in a rack using a blinking LED.
See Server Properties in the Server Summary view.	Access appliance information such as the serial number, product ID, and BIOS version.

For additional details, see the Cisco Integrated Management Controller online help. We recommend you use the CIMC GUI, but if desired you can access the CIMC CLI. For details on other CIMC documentation, see the Documentation Overview.

To review CIMC setup details, see the *Cisco Prime NAM 2300 Series Appliances Installation and Configuration Guide*.