Performing User and System Administration

This chapter provides information about what user and system administration tasks are required or optional, how to generate diagnostic information when requesting technical assistance, and provide user access.

This chapter contains the following topics:

- Managing System Data, page 6-1
- Performing System Administration, page 6-2
- Troubleshooting Using Diagnostics Tools, page 6-12
- Controlling User Access, page 6-14

Managing System Data

One of the roles of an administrator is to manage Prime NAM’s network data collection and retention so that it:

- Scales to fit the real needs of the system’s users.
- Minimizes the burden on monitored devices, applications, and network bandwidth.
- Survives hardware failures.

The following sections explain how to achieve these goals, and how to perform other data management tasks.

- Handling Backups, page 6-1
- Shrinking Storage Requirements, page 6-1

Handling Backups

It is critical to have your system backed up so that you can restore your configuration and data if required. Ensure you have sufficient data backups scheduled.

Shrinking Storage Requirements

Network administrators are consistently looking for ways to shrink their network storage requirements and improve bandwidth efficiency on tasks like backup and recovery.
By configuring Prime NAM packet deduplication on supported platforms, packets whose inspected segments match another packet within the specific time window are marked as duplicates and not forwarded.

For configuration guidelines and instructions, see Configuring Hardware Deduplication, page 3-36.

You can also move capture files to an external storage location to save on local disk space. See Capturing to Data Storage, page 5-20.

Performing System Administration

You can perform the following system administration tasks:

- Setting Network Parameters, page 6-4
- Setting the SNMP Agent, page 6-4
- Synchronizing Your System Time, page 6-6
- Setting Up E-Mail Notifications for Alarms, page 6-9
- Sharing NAM Data by Enabling Web Data Publication, page 6-10
- Setting Remote Servers to Receive Syslog Messages, page 6-10
- Configuring Hosts to Receive SNMP Traps from Prime NAM, page 6-11
- Resetting System Preferences, page 6-11

Monitoring Prime NAM Health and Traffic Statistics

Ensuring that your Cisco NAM processes your traffic efficiently and effectively without becoming overloaded is a critical task.

To view the network traffic coming into the Cisco NAM as well as data about its health (such as server network details and CPU, memory, and data usage) use Administration > System > Overview.

Use the data provided in the Inputs and Resources tabs to determine scalability issues and to assist with troubleshooting.

Table 6-1 describes the types of information of the System Overview window.
### Table 6-1 System Overview

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inputs Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Cumulative Input</td>
<td>Health and usage information on all the traffic received by the NAM. It shows the number of packets received (Rx Packets), number of packets lost or dropped (Rx Packets Lost), and number of bytes received (Rx Bytes). The Cumulative column shows cumulative counts since the start of the NAM, and the Rate column one shows the same counters for the last ten seconds.</td>
</tr>
<tr>
<td>Input Traffic</td>
<td>Usage information in bytes and packets based on the input you select. You can toggle between a chart or table format. Data is updated every 30 seconds and contains data from the past hour. The table time interval cannot be changed. The input table rate is calculated every 10 seconds. A table legend provides data for standard statistics provided by the software for data collected over a period of time.</td>
</tr>
<tr>
<td>Note</td>
<td>In order to view PA traffic on this page, you must configure your device to use port 3000 to send PA traffic to the NAM.</td>
</tr>
<tr>
<td></td>
<td>To reset the traffic counters, click on Reset Traffic at the bottom of Input Traffic chart.</td>
</tr>
<tr>
<td><strong>Resources Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Current date and time synchronized with the switch, router, or NTP server.</td>
</tr>
<tr>
<td>Host Name</td>
<td>NAM host name.</td>
</tr>
<tr>
<td>IPv4 Address IPv6</td>
<td>Based on your configuration, IPv4 address and/or IPv6 address displays.</td>
</tr>
<tr>
<td>System Uptime</td>
<td>Length of time the host has been running uninterrupted.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Config, data, and root partitions with their total and free space. Also shows the amount of disk space used by the performance data base files (DB) and the packet capture to disk (capture files). Use this information to ensure you have enough disk space and perform the needed maintenance as necessary.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Percentage of memory resources being consumed by the NAM as well as the total memory available.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>Percentage of CPU resources being consumed by the NAM. Each individual CPU in a multi-CPU platform is listed separately.</td>
</tr>
</tbody>
</table>
Setting Network Parameters

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Network Parameters. The Network Parameters window displays.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter or change the information.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• To save the changes, click Submit.</td>
</tr>
<tr>
<td></td>
<td>• To cancel the changes, click Reset.</td>
</tr>
</tbody>
</table>

Setting the 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 statistics. 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 6-5.

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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; SNMP Agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter or change the information in the NAM SNMP window. The fields are detailed in Table 6-2.</td>
</tr>
</tbody>
</table>
Chapter 6  Performing User and System Administration

Performing System Administration

---

**Step 3**
To create community strings, see Creating NAM Community Strings, page 6-5.

**Step 4**
To delete community strings, select the entry and click **Delete**.

**Step 5**
Do one of the following:
- To save the changes, click **Submit**.
- To cancel the changes, click **Reset**.

---

**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**.

---

**Table 6-2  System SNMP Dialog Box**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>The name of the person responsible for the NAM.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the NAM.</td>
</tr>
<tr>
<td>Location</td>
<td>(Optional) The physical location of the switch or router in which the NAM is installed.</td>
</tr>
</tbody>
</table>
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**.

Synchronizing Your System Time

Ensure that the Prime NAM software application’s Linux system time is synchronized with the packet timestamp and the standard time source outside of the NAM platform. Packet timing analysis uses system time to support application response time measurements, voice and video quality metrics, packet decode data, reporting, and many other network statistics.
The NAM gets the UTC (GMT) time from several sources, depending on its NAM platform type. All NAMs can be set up to get their time from an external NTP server. Other NAM platforms may prefer to use an IEEE 1588 Precision Time Protocol (PTP)-based time master due to its high accuracy and precision.

You should also configure any PTP switches that are between the NAM and the master clock to use Edge-to-Edge (E2E) mode. E2E is preferred because it reduces PTP messaging bandwidth and eliminates delay accumulation when daisy chaining many nodes. If the master clock and/or PTP switches are not configured correctly, all of the clocks on the NAM will be synced with each other, but to the wrong time.

⚠️ 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 incorrect, then the data shown in the GUI is incorrect.

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.

0xec:44:76:ff:fe:5d:12:0

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

For details on how to configure the NAM system time for your specific hardware platform, see Synchronizing NAM System Time for Specific Platforms, page 6-7.

### Synchronizing NAM System Time for Specific Platforms

Ensure that the NAM system time is configured correctly. If the system time is incorrect, NAM data presentation may be inaccurate due to time ranges, hence providing incorrect interpretations of NAM data.

Some platforms are synchronized automatically, but client browsers need to be synchronized in addition to the NAM and the router or switch in order for the data to be accurate. We recommend you perform the time synchronization for your platform.

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 6-8**
  
  This option is valid only for NAM-1X, NAM-2X, NAM-3, SM-SREs, and NAM-NX1.

- **Synchronizing the NAM System Time Locally, page 6-8**
  
  This option is valid for Cisco NAM appliances, Nexus 1000 VSB, and vNAM.

- **Configuring the NAM System Time with an NTP Server, page 6-8**
  
  This is valid for all platforms and is the recommended option.

- **Configuring the NAM System Time with Precision Time Protocol (IEEE 1588), page 6-9**
  
  This option is valid for NAM-3 and NAM-NX1.
Synchronizing the NAM System Time with the Switch or Router

Note This section is valid only for NAM-1X, NAM-2X, NAM-3, SM-SREs, and NAM-NX1. For additional platform options, see Synchronizing NAM System Time for Specific Platforms, page 6-7.

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

1. Choose Administration > System > System Time.
2. Choose the Switch or NTP Server radio button.
3. Select the Region and local time zone from the lists.
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 1000V, and vNAM. For additional platform options, see Synchronizing NAM System Time for Specific Platforms, page 6-7.

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

1. Log into the NAM command line interface.
2. Set the clock using the CLI clock set command.

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

3. On the Prime NAM GUI, choose Administration > System > System Time.
4. Click the Local radio button.
5. Select the Region and local time zone from the lists.
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:

1. On the NAM appliance GUI, choose Administration > System > System Time.
2. Choose the NTP Server radio button.
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.

Note  This section is applicable to the NAM-3 and NAM-NX1. For details on any hardware setup requirements related to this feature, see your specific NAM installation guide. For additional platform options, see Synchronizing NAM System Time for Specific Platforms, page 6-7.

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.

Tip  Set the PTP interface IP address so that it is not in the same subnet as the management interface. If they are in the same subnet, there may be routing issues for outbound management traffic (http, for example).

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.

Setting Up E-Mail Notifications for Alarms

You can configure Prime NAM to provide e-mail notification of alarms and to e-mail reports.
To set up e-mail notifications:

Step 1  Choose Administration > System > E-Mail Setting.
Step 2  Check the Enable Mail check box and enter the required or optional field information. Table 6-3 describes the Mail Configuration Options.
Step 3  Check the optional Advanced Settings check box and enter the details in the fields provided.
Step 4  Click Submit to save your modifications, or click Reset to clear the dialog of any characters you entered or restore the previous settings.
Performing System Administration

Chapter 6      Performing User and System Administration

Performing System Administration

Sharing NAM Data by Enabling 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.

Setting Remote Servers to Receive Syslog Messages

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Mail</td>
<td>Enables e-mail of reports and notification of alarms</td>
</tr>
<tr>
<td>External Mail Server</td>
<td>Distinguished name of external mail server</td>
</tr>
<tr>
<td>Send Test Mail to</td>
<td>Optional. List e-mail addresses for up to three e-mail recipients.</td>
</tr>
<tr>
<td>Mail Alarm to</td>
<td>This recipient will receive alarm notifications and scheduled exports.</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>Enables you to designate an e-mail access server port, as well as select a encryption protocol.</td>
</tr>
<tr>
<td>Mail Server Port</td>
<td>Optional. Designate an e-mail port for the NAM.</td>
</tr>
<tr>
<td>Mail Server Encryption</td>
<td>Optional. Select Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption for e-mail messaging.</td>
</tr>
</tbody>
</table>

Table 6-3       Mail Configuration Options
Performing System Administration

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 \texttt{local7}. Check the syslog collector configuration to ensure that \texttt{local7} is handled properly.

To set up the NAM syslog:

\begin{enumerate}
\item Choose \textit{Administration} > \textit{System} > \textit{Syslog Setting}.
\item The NAM Syslog Setting window displays.
\item 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).
\item Click \textit{Submit} to save your changes, or click \textit{Reset} to cancel.
\end{enumerate}

Configuring Hosts to Receive SNMP Traps from Prime NAM

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.

To configure, edit, or delete a host destination to which Prime NAM will send traps:

\begin{enumerate}
\item Choose \textit{Administration} > \textit{System} > \textit{SNMP Trap Setting}.
\item The SNMP Trap Setting window displays.
\item Click the \textit{Create} button.
\item In the “Community” field, enter the community string set in the NAM Thresholds.
\item In the “IP Address” field, enter the IP address to which the trap is sent if the alarm and trap community strings match.
\item In the “UDP Port” field, enter the UDP port number.
\item Click \textit{Submit} to save your changes, or click \textit{Reset} to cancel and leave the configuration unchanged.
\end{enumerate}

Resetting System Preferences

To change the Prime NAM display or logging characteristics, choose \textit{Administration} > \textit{System} > \textit{Preferences}. \textit{Table 6-4} describes the fields of the Preferences window.

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Field} & \textbf{Description} \\
\hline
Refresh Interval (60-3600 sec) & Amount of time between refresh of information on dashboards. \\
\hline
Top N Entries (1-10) & Number of colored bars on the Top N charts. \\
\hline
\end{tabular}
\caption{System View and Logging Preferences}
\end{table}
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 6-12
- Audit Trail, page 6-12
- Tech Support, page 6-13

For additional information on troubleshooting NAM, see Troubleshooting Network and NAM Issues.

### 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
- NetFlow 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 limits.

---

**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 6-12.

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 e-mail 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 Establishing TACACS+ Authentication and Authorization, page 6-17.

**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.
Controlling User Access

You can control your user’s access using the Administration options:

- Local Database, page 6-14
- Establishing TACACS+ Authentication and Authorization, page 6-17
- Configuring a TACACS+ Server to Support NAM Authentication and Authorization, page 6-18
- Current User Sessions, page 6-22

Local Database

When you first install the NAM, 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 (root, admin, and webuser), you can create additional accounts, enabling or disabling different levels of access independently for each user.

Table 6-7 provides information about User Privileges and describes each privilege.

For additional information about creating and editing users, see Creating a New User, page 6-15 and Establishing TACACS+ Authentication and Authorization, page 6-17.

If you have forgotten your password, use the helper utility to reset your root or user passwords (see Resetting Passwords, page 6-14).

Resetting Passwords

There are several methods you can use to reset your NAM passwords. Use the options documented in Table 6-5 based on your needs.

<table>
<thead>
<tr>
<th>NAM User</th>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root, Admin, and webuser</td>
<td>Boot into helper utility</td>
<td>Restart your NAM and choose option 5 or enter reboot-helper at the NAM CLI.</td>
</tr>
<tr>
<td>Root and webuser</td>
<td>clear system-passwords NAM CLI command</td>
<td>The easiest way to reset NAM passwords. This command resets both the root and guest user passwords to the factory default state. You must have appropriate privileges to reset passwords.</td>
</tr>
<tr>
<td>Root, Admin, and webuser</td>
<td>CLI commands on the switch or router</td>
<td>See your platform installation guide.</td>
</tr>
</tbody>
</table>
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 6-7 for an explanation of user privileges. Table 6-6 describes the fields in the New User Dialog Box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The account name</td>
<td>Enter the user’s account name.</td>
</tr>
<tr>
<td>Password</td>
<td>The account password</td>
<td>Enter a password that adheres to your site security policies.</td>
</tr>
<tr>
<td>Verify Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileges</td>
<td>Privileges associated with this account</td>
<td>Select each privilege to grant to the user.</td>
</tr>
</tbody>
</table>

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.

Step 4 Select a single or multiple check box to set user privileges. Table 6-7 provides information about each privilege.
### Table 6-7 User Privileges

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccountMgmt</td>
<td>Enables a user to create, delete, and edit user accounts.</td>
</tr>
<tr>
<td>SystemConfig</td>
<td>Enables a user to edit basic NAM system parameters such as IP address, gateway, HTTP port, and so on.</td>
</tr>
<tr>
<td>Capture</td>
<td>Enables a user to perform packet captures and manage capture sessions and use the NAM protocol decode.</td>
</tr>
<tr>
<td>AlarmConfig</td>
<td>Enables a user to create, delete, and edit alarms on the switch/router and NAM.</td>
</tr>
<tr>
<td>MonitorConfig</td>
<td>Enables a user to create, delete, and edit the following:</td>
</tr>
<tr>
<td></td>
<td>• Collections and reports</td>
</tr>
<tr>
<td></td>
<td>• Protocol directory entries</td>
</tr>
<tr>
<td></td>
<td>• Protocol groups</td>
</tr>
<tr>
<td></td>
<td>• URL-based applications</td>
</tr>
<tr>
<td>MonitorView</td>
<td>Enables a user to view monitoring data and reports (granted to all users).</td>
</tr>
</tbody>
</table>

**Step 5** Click **Submit** to create the user or **Reset** to clear the dialog of any characters you entered.

### Invalid User Name and Password Characters

For usernames, do not use the following:

- Exclamation point `!`
- At sign `@`
- Pound sign `#`
- Dollar sign `$`
- Percent `%`
- Carot `^`
- Ampersand `&`
- Asterisk `*`
- Left or right parentheses `( )`
- Greater than `<`
- Less than `>`
- Comma `,`
- Period `.`
- Double quote `“`
- Single quote `’`
- Forward slash `/`
- Backward slash `\`
For web user passwords, do not use the following:

- Double quote "
- Single quote ’
- Greater than <
- Less than <

For root or guest user passwords, only the single quote is not allowed.

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 6-8).

<table>
<thead>
<tr>
<th>Table 6-8</th>
<th>TACACS+ Authentication and Authorization Dialog Box</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Usage Notes</td>
</tr>
</tbody>
</table>
| 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. |
Controlling User Access

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 supports 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. When configuring NAM within ACS 5.x, deselect the check box for the Single Connect Device option under the TACACS+ settings.

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:

- Add a NAM user or user group. See Adding a NAM User or User Group for Version 4.2, page 6-19.

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.
Controlling User Access

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.

Use the following sections to configure your Cisco ACS server:
Controlling User Access

- Add a NAM user or user group. See Adding a NAM User or User Group for Version 5.x, page 6-20.

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 and deselect the check box for the Single Connect Device option under the TACACS+ settings.

**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 6-20 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), 5.2, and 5.3 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 check the check box Permit any command that is not in the table below.

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

- permit capture
- permit system
- permit collection
- permit account
- permit alarm
- permit view

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

Step 4  Go to Access Policies > Access Services > namAdmin > Authorization > Customize to set up customized conditions which are needed in later step. For example, you may choose: NDG: Device Type, Device IP Address, and so on). Replace namAdmin with the service you created in this step.

Step 5  Go to Access Policies > Access Services > namAdmin > Authorization > Create to set up the condition to qualify all login requests. NAM devices use these conditions and follow 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 6  Click Access Policies > Service Selection Rules to choose a service (for example, the service you created in Step 3).

Step 7  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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>shell</td>
</tr>
<tr>
<td>cmd</td>
<td>web</td>
</tr>
<tr>
<td>cmd-arg</td>
<td>One or more the following: accountmgmt, system, capture, alarm, collection, view</td>
</tr>
<tr>
<td>password authentication method—Password Authentication Protocol (PAP)</td>
<td>pap</td>
</tr>
</tbody>
</table>

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 6-9) displays.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user ID used to log into the NAM.</td>
</tr>
<tr>
<td>From</td>
<td>The name of the machine the user logged in from.</td>
</tr>
<tr>
<td>Login Time</td>
<td>The time the user logged in.</td>
</tr>
<tr>
<td>Last Activity</td>
<td>The time stamp of the last user activity.</td>
</tr>
</tbody>
</table>