CHAPTER 15

Performing Administrative Tasks

The Administration enables you to schedule tasks, administer accounts, and configure local and external authentication and authorization. Also, set logging options, configure mail servers, and data management related to configuring the data retain periods. Information is available about the types of NCS licenses and how to install a license.

This chapter describes the Cisco NCS administrative tasks. It contains the following sections:

Performing Background Tasks

You can use the NCS Background Tasks page to schedule and monitor data collection tasks and other background tasks.

This section contains the following topics:

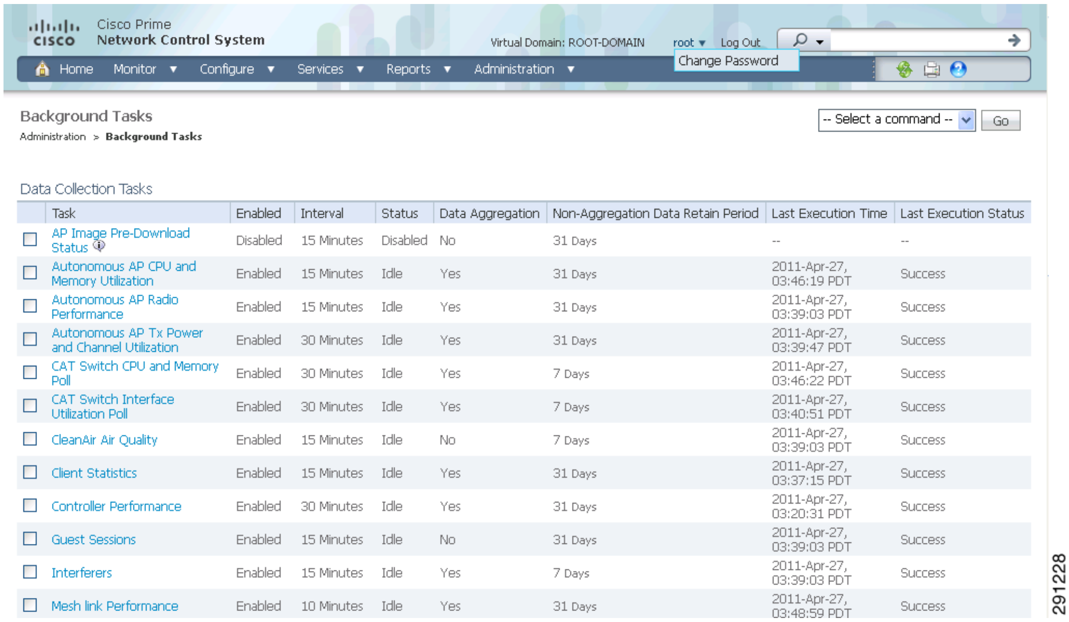
For more information on data collection and other background tasks, see the "Data Collection Tasks" section on page 15-5 and "Other Background Tasks" section on page 15-32.

About Background Tasks

A background task is a scheduled program running in the background with no visible pages or other user interfaces. In NCS background tasks can be anything from data collection to taking backups of the configurations.

Note Choose **Administration > Background Tasks** to view several scheduled tasks. The Background Tasks page appears (see Figure 15-1).

Figure 15-1 Background Tasks Page



Background Tasks
Administration > **Background Tasks**

Data Collection Tasks

	Task	Enabled	Interval	Status	Data Aggregation	Non-Aggregation Data Retain Period	Last Execution Time	Last Execution Status
□	AP Image Pre-Download Status	Disabled	15 Minutes	Disabled	No	31 Days	--	--
□	Autonomous AP CPU and Memory Utilization	Enabled	15 Minutes	Idle	Yes	31 Days	2011-Apr-27, 03:46:19 PDT	Success
□	Autonomous AP Radio Performance	Enabled	15 Minutes	Idle	Yes	31 Days	2011-Apr-27, 03:39:03 PDT	Success
□	Autonomous AP Tx Power and Channel Utilization	Enabled	30 Minutes	Idle	Yes	31 Days	2011-Apr-27, 03:39:47 PDT	Success
□	CAT Switch CPU and Memory Poll	Enabled	30 Minutes	Idle	Yes	7 Days	2011-Apr-27, 03:46:22 PDT	Success
□	CAT Switch Interface Utilization Poll	Enabled	30 Minutes	Idle	Yes	7 Days	2011-Apr-27, 03:40:51 PDT	Success
□	CleanAir Air Quality	Enabled	15 Minutes	Idle	No	7 Days	2011-Apr-27, 03:39:03 PDT	Success
□	Client Statistics	Enabled	15 Minutes	Idle	Yes	31 Days	2011-Apr-27, 03:37:15 PDT	Success
□	Controller Performance	Enabled	30 Minutes	Idle	Yes	31 Days	2011-Apr-27, 03:20:31 PDT	Success
□	Guest Sessions	Enabled	15 Minutes	Idle	No	31 Days	2011-Apr-27, 03:39:03 PDT	Success
□	Interferers	Enabled	15 Minutes	Idle	Yes	7 Days	2011-Apr-27, 03:39:03 PDT	Success
□	Mesh link Performance	Enabled	10 Minutes	Idle	Yes	31 Days	2011-Apr-27, 03:48:59 PDT	Success

You can view the administrative and operating status, task interval, and time of day in which the task occurs. To execute a particular task, select the check box of the desired task and choose **Execute Now** from the Select a command drop-down list. The task is executed based on what you have configured for the specific task.

The tasks are listed in tables with the following columns:

- Check box—Select to choose the desired task. Chosen tasks are targets for operations initiated from the Select a command drop-down list including the following:
  - Execute Now—Run all of the data sets with a selected check box.
  - Enable Collection—Enable the data set to run at its scheduled interval.
  - Disable Collection—Prevent the data set from running at its scheduled interval.
- Task—Task name that serves as a link to a configuration page. Click a task name to go to that task configuration page.
- Enabled—Indicates that the task is enabled or disabled.
- Interval—Time period between executions of task.
- Status—Indicates that the task is idle, disabled, or executing.
- Data Aggregation (Data Collections only)—If set to Yes, the data set is aggregate data.

- Non-Aggregation Data Retain Period (Days) (Data Collections only)—The number of days that non-aggregated data is retained.

Note See the "NCS Historical Data" section on page 15-60 for more information on aggregated and non-aggregated data in NCS.

- Last Execution Time—The date and time the task was executed.
- Last Execution Status—Indicates that the task executed was a success, failure, or a partial success.

This page enables you to view the status of scheduled NCS tasks. Scheduled tasks are divided into two types: for more information, see the "Data Collection Tasks" section on page 15-5 and the "Other Background Tasks" section on page 15-32.

Performing a Data Collection Task

Data collection tasks are data-set tasks that collect and organize information that might be useful for creating reports.

Note All tasks related to collecting data or any other background task are handled in a similar manner.

Step 1 Choose **Administration > Background Tasks** to display the Background Tasks page (see Figure 15-1). This page displays the following information:

- Enabled—Whether the tasks have been enabled or disabled.
- Interval—Indicates the time period (in minutes) between task executions. You can set the interval from the data collection configuration page for the task.
- Status—The present state of the task.
- Data Aggregation (Data Collection Tasks only)—If set to Yes, the data set combines data.
- Non-Aggregation Data Retain Period (Days) (Data Collection Tasks only)—The number of days that the non-aggregated data is retained. You can set the retention period from the data collection configuration page of the task.
- Last Execution Time—The time and date when the task was last run.
- Last Execution Status—The status after the last task was run.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**.
- Enable the task.

  Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task changes from dimmed to available after enabling is complete.
- Disable the task.

  Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed after the disabling is complete.

- View details of a task.

  Click a URL in the Data Collection Tasks or Other Background Tasks column to view a specific task. The details on that task appear. Data collections are data-set tasks that collect and organize a specific type of information useful for creating reports. For more information on the various Data Collection Tasks, see "Data Collection Tasks" section on page 15-5.

To access the configuration page of a data set, select the name of the data set in the Data Collection page. Each data set configuration page displays a table of the executions of the data set. The table has following columns:

- Executed task information includes the following:
  - Last Execution Start Time—Indicates the date and time that the data-set task began running.
  - End Time—Indicates the date and time that the data-set task stopped running.
  - Elapsed Time (secs)—Indicates the amount of time (in seconds) it took to complete the task.
  - Result—Indicates the success or failure of the task.
  - Additional Information—Provides any additional information regarding a specific task.

Each data set configuration page contains the following parameters and information in the Collection Set Details group box:

- Description—Provides a brief display only description of the data set.
- Data Aggregation—Indicates whether or not data collected by the data set is aggregated.
- Used By Report(s)—Displays names of the reports that use the data set.
  - CleanAir Air Quality—This data set is used for Worst Air Quality APs and Air Quality versus Time reports.
  - Interferers—This data set us used for Worst Interferers reports.
- Collection Status—Select the **Enabled** check box to enable data collection.

Interval (min.)—Enter the time (in minutes) for the data set execution interval. The valid value is 1 to 120 minutes.

Each data set configuration page contains the following parameters in the Data Management group box:

- Non-Aggregation Data Retain Period (Days)—Enter the number of days to retain non-aggregated data collected by the data set. The valid value is 1 to 31 days.
- Retain Aggregation Raw Data—Select the **Enable** check box to enable the retention of aggregated raw data.

  Note The Aggregation Raw Data Retain Period setting is for polled raw data. To configure the retention period for aggregated trend data, choose **Administration > Settings**, then choose **Data Management** from the left sidebar menu.

  Note See the "Configuring Auto Provisioning for Controllers" section on page 9-230 for more information on aggregated and non-aggregated data.

Note For this example, performing an NCS server backup was selected as the task. The information entered in the fields for each page vary based on the task you choose.

Step 3 Select the **Enabled** check box.

Step 4 Select the **Report History Backup** check box.

Step 5 In the Max Backups to Keep text box, enter the maximum number of backup files to save on the server.

Range: 7 to 50

Default: 7

Note To prevent the NCS platform from running out of disk space, the server automatically deletes old backup files when the number of files exceeds the value entered for this text box.

Step 6 In the Interval (Days) text box, enter the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 7 In the Time of Day text box, enter the backup start time. It must be in this format: *hh*:*mm AM/PM* (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Note Backing up a large database affects the performance of the NCS server. Therefore, we recommend that you schedule backups to run when the NCS server is idle (for example, in the middle of the night).

Step 8 Click **Submit** to save your settings. The backup file is saved as a .zip file in the ftp-install-dir/ftp-server/root/NCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Data Collection Tasks

Table 15-1 lists and describes the various data collection tasks in the NCS.

Table 15-1 Data Collection Tasks

Task Name	Task Status	Default Schedule	Description
AP Image Pre-Download Status	Disabled	15 minutes	This task is used to see the Image Predownload status of the associated APs in the controllers. To see the status of the access points, the Pre-download software to APs check box should be selected while downloading software to the controller.
Autonomous AP CPU and Memory Utilization	Enabled	15 minutes	This task is used to collect information about memory and CPU utilization of autonomous APs.
Autonomous AP Inventory	Enabled	180 minutes	This task is used to collect the inventory information for autonomous APs.

Table 15-1 Data Collection Tasks (continued)

Task Name	Task Status	Default Schedule	Description
Autonomous AP Radio Performance	Enabled	15 minutes	This task is used to collect information about radio performance information as well as radio up or down status for autonomous APs.
Autonomous AP Tx Power and Channel Utilization	Enabled	30 minutes	This task is used to collect information about radio performance of autonomous APs.
CAT Switch CPU and Memory Poll	Enabled	30 minutes	This task is used to collect information about CAT switch CPU and memory p oll.
CAT Switch Interface Utilization Poll	Enabled	30 minutes	This task is used to collect information about CAT switch interface utilization poll.
CleanAir Air Quality	Enabled	15 minutes	This task is used to collect information about CleanAir air quality.
Client Statistics	Enabled	15 minutes	This task helps you to get the statistical information for the autonomous and lightweight clients.
Controller Performance	Enabled	30 minutes	This task is used to collect performance information for controllers.
Guest Sessions	Enabled	15 minutes	This task is used to collect information about the guest sessions.
Interferers	Enabled	15 minutes	This task is used to collect information about the interferers.
Media Stream Clients	Enabled	15 minutes	This task is used to collect information about media stream for clients.
Mesh link Performance	Enabled	10 minutes	This task is used to collect information about the performance of Mesh links.
Mesh Link Status	Enabled	5 minutes	This task is used to collect status of the Mesh links.
Mobility Service Performance	Enabled	15 minutes	This task is used to collect information about the performance of mobility service engines.
Radio Performance	Enabled	15 minutes	This task is used to collect statistics from wireless radios.
Rogue AP	Enabled	120 minutes	This task is used to collect information about the rogue access points.
Traffic Stream Metrics	Enabled	8 minutes	This task helps you to get traffic stream metrics for the clients.
CCX Client Statistics	Disabled	60 minutes	This task is used to collect the Dot11 and security statistics for CCX Version 5 and Version 6 clients.
Wired Switch Inventory	Enabled	Daily at midnight	This task is used to collect inventory information for wired switches.
Wireless Controller Inventory	Disabled	Daily at midnight	This task is used to collect inventory information for wireless controllers.

Performing Other Background Tasks

You can also perform other background tasks using the NCS Administration.

This section contains the procedures for the other NCS background tasks and contains the following topics:

For more information on the other background tasks, see the "Other Background Tasks" section on page 15-32.

Viewing Appliance Status

To view the appliance status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Appliance Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

or

- Enable the task.

  Select the **Appliance Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Appliance Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Appliance Status** link in the Background Tasks column. The Task > Appliance Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Appliance Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Autonomous AP Client Status

To view the Autonomous AP Client Status page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Autonomous AP Client Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Autonomous AP Client Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Autonomous AP Client Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Autonomous AP Client Status** link in the Background Tasks column. The Task > Autonomous AP Client Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Autonomous AP Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Autonomous AP Operational Status

To view the Autonomous AP Operational Status page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Autonomous AP Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Autonomous AP Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Autonomous AP Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Autonomous AP Operational Status** link in the Background Tasks column. The Task > Autonomous AP Operational Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Appliance Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing a Configuration Sync

To perform a configuration sync, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Configuration Sync** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Configuration Sync** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

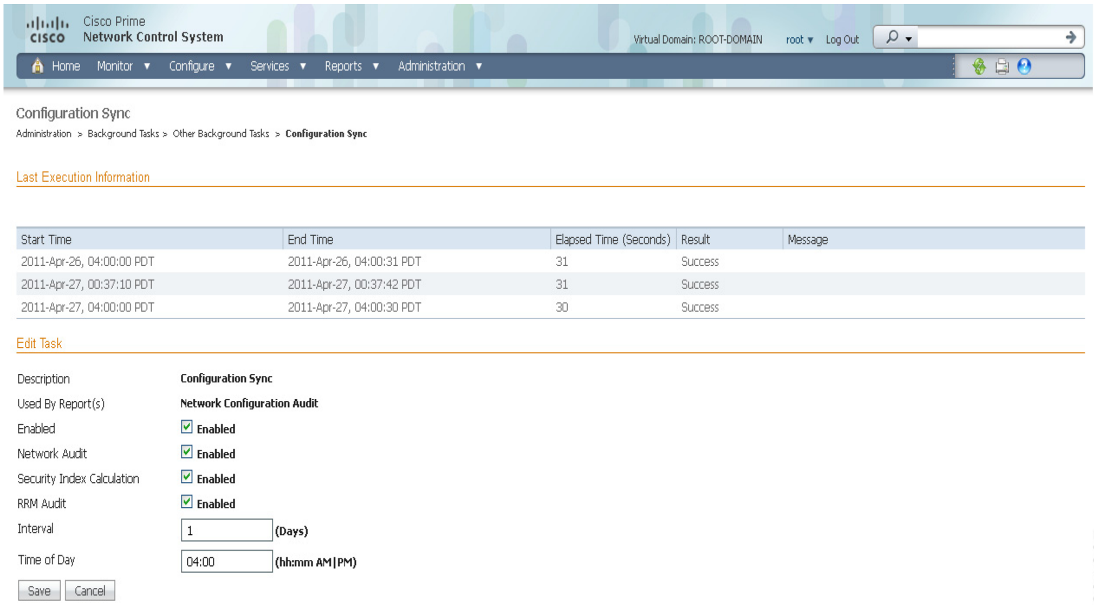
  or

- Disable the task.

  Select the **Configuration Sync** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Configuration Sync** link in the Background Tasks column. The Task > Configuration Sync page appears (see Figure 15-2).

Figure 15-2 Task > Configuration Sync



Configuration Sync

Administration > Background Tasks > Other Background Tasks > **Configuration Sync**

Last Execution Information

Start Time	End Time	Elapsed Time (Seconds)	Result	Message
2011-Apr-26, 04:00:00 PDT	2011-Apr-26, 04:00:31 PDT	31	Success	
2011-Apr-27, 00:37:10 PDT	2011-Apr-27, 00:37:42 PDT	31	Success	
2011-Apr-27, 04:00:00 PDT	2011-Apr-27, 04:00:30 PDT	30	Success	

Edit Task

Description	**Configuration Sync**
Used By Report(s)	**Network Configuration Audit**
Enabled	☑ **Enabled**
Network Audit	☑ **Enabled**
Security Index Calculation	☑ **Enabled**
RRM Audit	☑ **Enabled**
Interval	1 **(Days)**
Time of Day	04:00 **(hh:mm AM|PM)**

Save Cancel

291297

Step 4 Click the background task in the Task column to open the task details page.

The Configuration Sync page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success, warning, or error.
  - Message—Text message regarding this task.

Note If the Result is a Warning and the Message appears as Failed, the device is unreachable.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Used By Report(s)—Indicates the NCS reports that use these task results.
- Enabled—Select the check box to enable this task.
- Network Audit—Select the check box to enable the secondary network audit.
- Security Index Calculation—Select the check box to enable security index calculation. The Security Index is available in the Monitor > Security page.
- RRM Audit—Select the check box to enable an RRM audit.

Note The controller audit finds the discrepancies between the values in the NCS database with the device.

Note To query the SNMP values from the device, you can use the https://<NCS-IP>/webacs/manObjDiagQueryAction.do URL in the NCS.

Note The Network Audit audits all controllers in the network, and also runs the RRM audit and Security audit. These options are selectable from the **Administration** > **Background Tasks > Other Background Tasks** > **Configuration Sync** page.

- Time of Day (hh:mm AM|PM)—Indicate the time of day (AM or PM) for the execution of this task.

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Lightweight Client Status

Choose **Administration > Background Tasks**, then click **Lightweight Client Status** to access this page.

This page enables you to view the history and current status of lightweight client status polling backups.

In the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Lightweight Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Controller Configuration Backup Status

Choose **Administration > Background Tasks**, then click **Controller Configuration Backup** to access this page.

This page enables you to view the history and current status of Cisco WLAN Solution configuration backups.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Controller Configuration Backup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.
- Time of Day (hh:mm AM|PM)

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

- TFTP Server or FTP Server—Select either of the following:
  - TFTP Server—If you select TFTP Server, choose the server or **Default Server** from the drop-down list.
  - FTP Server—If you select FTP Server, choose the server or **Default Server** from the drop-down list, enter the FTP Username, FTP Password and FTP port information in the respective text box.

Note TFTP must be enabled in Administration > Settings > Server Settings for 'Default Server' options. For more information, see the "Configuring Server Settings" section on page 15-71.

Note The Server drop-down list is populated with the server names only if you add FTP or TFTP servers in the NCS. To add an FTP or TFTP server, see the "Configuring TFTP or FTP Servers" section on page 9-247.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Controller Operational Status

Device status polls controller reachability and WiSM peer information.

Choose **Administration > Background Tasks**, then click **Controller Operational Status** to access this page.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable Controller Operational Status task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the **Controller Operational Status** check box to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the **Controller Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the **Controller Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the Controller Operational Status task, follow these steps:

Step 1 Click the Controller Operational Status background task in the Task column to open the task details page.

The Controller Operational Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in minutes) of the task.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Data Cleanup Status

Choose **Administration > Background Tasks**, then click **Database Cleanup** to access this page.

This page enables you to view the history and current status of Cisco WLAN Solution database cleanups.

To modify this task, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Click the background task in the Task column to open the task details page.

The Data Cleanup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 3 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Time of Day (hh:mm AM|PM)

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Step 4 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Device Data Collection

To perform a device data collection, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Device Data Collection** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Device Data Collection** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Device Data Collection** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the **Device Data Collection** link in the Background Tasks column. The Task > Device Data Collector page appears.

Step 4 Click the background task in the Task column to open the task details page.

The Device Data Collector page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

Step 5 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Controller IP address—The IP address of the controller to collect data from.
- CLI Commands—Enter the command-line interface commands separated by comma, which you would want to run on the specified controller.
- Clean Start—Select or unselect this check box to enable or disable a clean start before data collection.
- Repeat—Enter the number of times you would want the data collection to happen.
- Interval—Enter the interval, in days, that you would want the data collection to happen. The valid range is 1 to 360 days.

Step 6 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Guest Accounts Sync

Choose **Administration > Background Tasks**, then click **Guest Accounts Sync** to access this page.

This page enables you to view the history and current status of Guest Accounts Synchronization tasks.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Guest Accounts Synchronization page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.
- Time of Day (hh:mm AM|PM)

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Identity Services Engine Status

To update the identity services engine status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

Select the **Identity Services Engine Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

or

- Enable the task.

  Select the **Identity Services Engine Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Identity Services Engine Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the Identity Services Engine Status task, click the **Identity Services Engine Status** link in the Background Tasks column. The Identity Services Engine Status page appears.

Step 4 Click the Identity Services Engine Status background task in the Task column to open the task details page.

Step 5 The Identity Services Engine Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

  Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Updating License Status

To update the license status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

Select the **License Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

or

- Enable the task.

  Select the **License Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

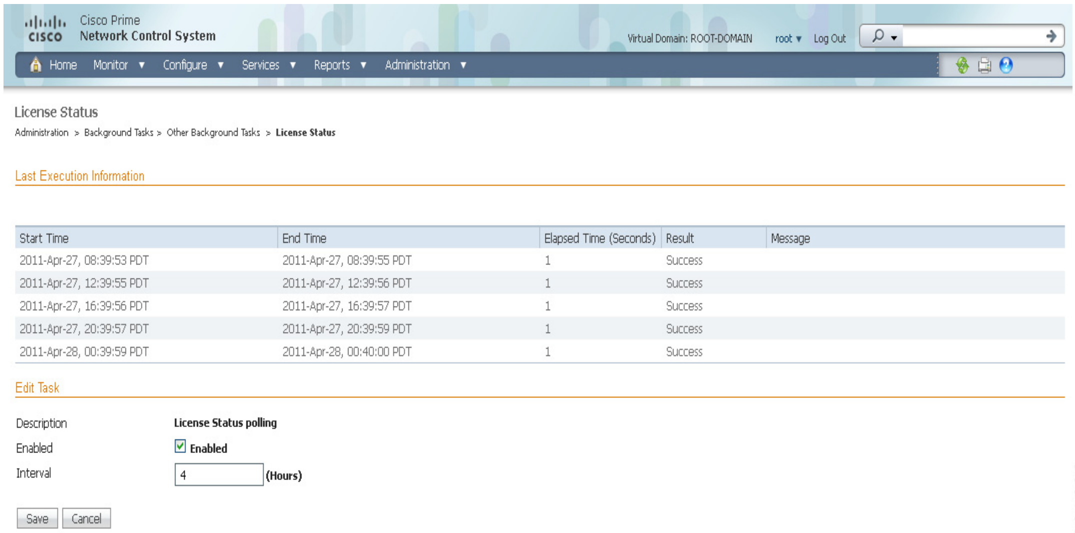
  or

- Disable the task.

  Select the **License Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **License Status** link in the Background Tasks column. The License Status page appears (see Figure 15-3).

Figure 15-3 License Status Page



License Status

Administration > Background Tasks > Other Background Tasks > **License Status**

Last Execution Information

Start Time	End Time	Elapsed Time (Seconds)	Result	Message
2011-Apr-27, 08:39:53 PDT	2011-Apr-27, 08:39:55 PDT	1	Success	
2011-Apr-27, 12:39:55 PDT	2011-Apr-27, 12:39:56 PDT	1	Success	
2011-Apr-27, 16:39:56 PDT	2011-Apr-27, 16:39:57 PDT	1	Success	
2011-Apr-27, 20:39:57 PDT	2011-Apr-27, 20:39:59 PDT	1	Success	
2011-Apr-28, 00:39:59 PDT	2011-Apr-28, 00:40:00 PDT	1	Success	

Edit Task

Description	**License Status polling**
Enabled	☑ **Enabled**
Interval	4 **(Hours)**

Save Cancel

This page shows when the latest license resynchronizations occurred. By default, it runs every 4 hours. From this page, you can disable this task or change the interval.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The License Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.

- Enabled—Select this check box to enable the task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Lightweight AP Operational Status

To view the Lightweight AP Operational status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Lightweight AP Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Lightweight AP Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Lightweight AP Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **Lightweight AP Operational Status** link in the Background Tasks column. The License Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Lightweight AP Operational Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable the task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Lightweight AP Client Status

To view the Lightweight AP Client status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Lightweight AP Client Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Lightweight AP Client Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Lightweight AP Client Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **Lightweight AP Client Status** link in the Background Tasks column. The License Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Lightweight AP Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Location Appliance Backup

Choose **Administration > Background Tasks**, then click **Location Appliance Backup** to access this page.

This page enables you to schedule a backup of the mobility services engine database.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Mobility Service Backup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Max backups to keep—Enter the maximum number of location backups to be kept on the backup server.
- Interval (days)—Enter the frequency of backup.
- Time of the Day (hh:mm AM/PM)—Enter the time at which the backup starts on the scheduled day.

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

- When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Location Appliance Status

Choose **Administration > Background Tasks**, then click **Location Appliance Status** to access this page.

This page displays the status of the mobility services engine.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Mobility Service Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval (days)—Enter the frequency of backup.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing Location Appliance Synchronization

Choose **Administration > Background Tasks**, then click **Location Appliance Synchronization** to access this page.

This page enables you to synchronize mobility services engine(s).

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The Mobility Service Synchronization page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Out of Sync Alerts—When enabled, this generates minor alarms when location server is not synchronized with the NCS changes that you have made.
- Auto Synchronization—Use this setting to enable auto synchronization of the location server. This ensures that when you make changes to the NCS, the location server auto synchronizes with the changes.
- Interval (minutes)—Specify the auto synchronization interval.

Step 3 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing NCS Server Backup

Choose **Administration > Background Tasks**, then click **NCS Server Backup** to access this page.

This page enables you to schedule a backup of the NCS server.

From the Administration > Background Tasks page, you can execute, enable, or disable this task. To execute, enable, or disable this task from the Administration > Background Tasks page, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Select the check box(es) of the Background Task(s) that you want to execute, enable, or disable.

Step 3 Use the Select a command drop-down list to perform one of the following tasks:

- Execute the task now—Select the check box of the task you want to execute. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. The status changes in the Enabled column.

  or

- Enable the task—Select the check box of the task you want to enable. From the Select a command drop-down list, choose **Enable Task**, and click **Go**.

  or

- Disable the task—Select the check box of the task you want to disable. From the Select a command drop-down list, choose **Disable Task**, and click **Go**.

To modify the task, follow these steps:

Step 1 Click the background task in the Task column to open the task details page.

The NCS Server Backup page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 2 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Report History Backup—Select the check box to enable the NCS to back up report histories.
- Max Backups to Keep—Enter the maximum number of NCS server backups to be kept on the backup server.
- Backup Repository—Select an existing backup repository or click **Create** to create a new backup repository.
- Interval (days)—Enter a value between 1 and 360. The NCS server data is backed up every *n* days, where *n* is the value that you have specified in this field.
- Time of the Day (hh:mm AM/PM)—Enter the time at which the backup starts on the scheduled day.

Note Time of Day (hh:mm AM|PM) must be in this format: hh:mm AM/PM (for example: 03:00 AM). If no AM/PM notation is designated, the entered hour is always AM. If you want to specify 5PM, you can enter 17:00 or 5:00 PM. When the page is revisited after saving, the time is displayed as hh:mm (in this case 17:00), without the PM designation.

- When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing OSS Server Status

To view the OSS Server status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **OSS Server Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **OSS Server Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **OSS Server Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the controller license reset task, click the **OSS Server Status** link in the Background Tasks column. The OSS Server Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The OSS Server Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

  Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing the Switch NMSP and Location Status

You can view the Switch NMSP and Location Status using the Switch NMSP and Location Status option under Cisco NCS Administration.

To view the Switch NMSP and Location Status, follow these steps:

Step 1 Choose **NCS** > **Administration** > **Background Tasks**.

Step 2 From the Other Background Tasks table, click the **Switch NMSP and Location Status** link.

The Switch NMSP and Location Status page appears.

The Switch NMSP and Location Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.

- Result—Success or error.
- Message—Text message regarding the task execution.

Step 3 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval (hours)—Enter the frequency of backup.

Step 4 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Viewing Switch Operational Status

To view the Switch Operational status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Switch Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Switch Operational Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Switch Operational Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to avaialble in the Enabled column after the disabling is complete.

Step 3 To modify the Switch Operational Status task, click the **Switch Operational Status** link in the Background Tasks column. The Switch Operational Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Switch Operational Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Performing wIPS Alarm Synchronization

To perform wIPS Alarm Synchronization, follow these steps :

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **wIPS Alarm Sync** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **wIPS Alarm Sync** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **wIPS Alarm Sync** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the wIPS Alarm Sync task, click the **wIPS Alarm Sync** link in the Background Tasks column. The wIPS Alarm Sync page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The wIPS Alarm Sync page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Indicates the frequency (in days) of the task.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Wired Client Status

To view the Wired Client status, follow these steps:

Step 1 Choose **Administration > Background Tasks**.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the **Wired Client Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

  or

- Enable the task.

  Select the **Wired Client Status** check box. From the Select a command drop-down list, choose **Enable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column.

  or

- Disable the task.

  Select the **Wired Client Status** check box. From the Select a command drop-down list, choose **Disable Task**, and click **Go**. The task converts from dimmed to available in the Enabled column after the disabling is complete.

Step 3 To modify the Wired Client Status task, click the **Wired Client Status** link in the Background Tasks column. The Wired Client Status page appears.

Step 4 Click the background task in the Task column to open the task details page.

Step 5 The Wired Client Status page displays the following information:

- Last Execution Information
  - Start and end times.
  - Elapsed time in seconds.
  - Result—Success or error.
  - Message—Text message regarding the task execution.

Step 6 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select this check box to enable this task.

Note If the Enabled check box is not selected, the task is not executed at the specified time.

- Interval—Enter the interval, in hours, that you want the wired client status polling to happen. The valid range is 1 to 8640 hours.
- Major Polling—Specify two time periods at which you want the major pollings to happen. Valid format: hh:mm AM|PM. Example: 12:49 AM.

  For wired clients, the NCS polls managed switches at regular interval to discover new clients or changes to the existing clients. To find this, the NCS caches the last change time of the interface. In the next poll, it checks the new value of the change time of the interface with the cached value to determine whether there is any change on any interface. Then polling happens only for the interfaces where there is a change. If there is no change on an interface between the polling, no polling happens for that interface. When polling happens during major polling schedule, a complete polling is done irrespective of whether there is a change on the interface or not. The reason for having major and minor polling is because, polling the switches for wired clients on all interfaces is expensive and resource-intensive for the NCS and switches. So then, the major polling happens only twice a day.

Step 7 When finished, click **Submit** to confirm task changes or **Cancel** to return to the Administration > Background Tasks page with no changes made.

Other Background Tasks

Table 15-2 describes the other background tasks that are available in the NCS:

Table 15-2 Other Background Tasks

Task Name	Default Schedule	Description	Editable Options
Appliance Status	5 minutes	This task is used to view the details of the appliance polling. This task populates the appliance polling details from **Administration > Appliance > Appliance Status** page. In addition, this background task populates information such as the performance and fault checking capabilities of the appliance.	Default—Enabled Interval—Valid interval - 1 - 10080 For more information, see the "Viewing Appliance Status" section on page 15-7.
Autonomous AP Client Status	5 minutes	This task helps you to discover the autonomous AP client from the network.	Default—Enabled. For more information, see the "Viewing Autonomous AP Client Status" section on page 15-8.
Autonomous AP Operational Status	5 minutes	This task helps you to view the autonomous AP operational status polling.	Default: Enabled Interval—Valid interval - 1 - 10080 For more information, see the "Viewing Autonomous AP Operational Status" section on page 15-9.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Configuration Sync	Daily at 4 am.	This task is used to view the configuration synchronization.	Enable—Select or unselect this check box to enable or disable configuration synchronization. Default: Enabled. Enable—Select or unselect this check box to enable or disable Network Audit. Default: Enabled. Enable—Select or unselect this check box to enable or disable Security Index calculation. Default: Enabled. Enable—Select or unselect this check box to enable or disable RRM audit. The default is Enabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing a Configuration Sync" section on page 15-10.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Controller Configuration Backup	Daily at 10 pm	This task is used to view the controller configuration backup activities.	Enable—Select or unselect this check box to enable or disable controller configuration backup. The default is Disabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. TFTP Server—Select the IP address of the server to which you want to back up the controller configuration. For more information, see the "Viewing Controller Configuration Backup Status" section on page 15-13.
Controller Operational Status	5 minutes	This task is used to schedule and view the controller operational status.	Enable—Select or unselect this check box to enable or disable Controller Configuration Backup. The default is enabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. For more information, see the "Viewing Controller Operational Status" section on page 15-15.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Data Cleanup	Daily at 2 am.	This task is used to schedule a data cleanup	Time of Day—Enter the time of the day that you want the data cleanup to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. The default is Enabled. For more information, see the "Viewing Data Cleanup Status" section on page 15-16.
Device Data Collector	30 minutes	This task is used to schedule a data collection based on the specified command-line interface commands at a configured time interval.	Enabled—Select or unselect this check box to enable or disable data collection for a specified controller. The default is Disabled. Controller IP address—The IP address of the Controller to collect data from. CLI Commands—Enter the CLI commands, separated by commas, which you want to run on the specified controller. Clean Start—Select or unselect this check box to enable or disable a clean start before data collection. Repeat—Enter the number of times that you want the data collection to happen. Interval—Enter the interval, in days, that you want the data collection to happen. The valid range is 1 to 360 days. For more information, see the "Performing Device Data Collection" section on page 15-16.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Guest Accounts Sync	Daily at 1 am.	This task is used to schedule guest account polling and synchronization.	Enable—Select or unselect this check box to enable or disable guest account synchronization. The default is Enabled. Interval—Enter the interval, in days, that you want the guest account synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the guest account synchronization to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing Guest Accounts Sync" section on page 15-17.
Identity Services Engine Status	15 minutes	This task is used to schedule the Identity Services Engine polling.	Enable—Select or unselect this check box to enable or disable Identity Services Engine polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Identity Services Engine polling to happen. The valid range is 1 to 360 days. For more information, see the "Viewing Identity Services Engine Status" section on page 15-18.
License Status	4 hours.	This task is used to schedule the license status polling.	Enable—Select or unselect this check box to enable or disable license status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the license status polling to happen. The valid range is 1 to 360 days. For more information, see the "Updating License Status" section on page 15-19.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Lightweight AP Operational Status	5 minutes.	This task helps you to view the Lightweight AP operational status polling.	Enable—Select or unselect this check box to enable or disable Lightweight AP Operational Status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Lightweight AP Operational Status polling to happen. The valid rangeis 1 to 360 days. For more information, see the "Lightweight AP Operational Status" section on page 15-21.
Lightweight Client Status	5 minutes.	This task helps you to discover the Lightweight AP client from the network.	Enable—Select or unselect this check box to enable or disable Lightweight Client Status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Lightweight Client Status polling to happen. The valid range is 1 to 360 days. For more information, see the "Lightweight AP Client Status" section on page 15-22.
Mobility Service Backup	Every 7 days at 1 am.	This task is used to schedule mobility services backup polling.	Enable—Select or unselect this check box to enable or disable mobility service backup. The default is disabled. Interval—Enter the interval, in days, that you want the mobility services back up to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the mobility services back up to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing Location Appliance Backup" section on page 15-23.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Mobility Service Status	5 minutes.	This task is used to schedule mobility services status polling.	Enable—Select or unselect this check box to enable or disable mobility services status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the mobility services status polling to happen. The valid range is 1 to 360 days. For more information, see the "Viewing Location Appliance Status" section on page 15-24.
Mobility Service Synchronizati on	60 minutes.	This task is used to schedule mobility services synchronization.	Out of Sync Alerts—Select this check box if you want to enable out of sync alerts. Smart Synchronization—Select this check box if you want to enable smart synchronization. The default is Enabled. Interval—Enter the interval, in minutes, that you want the mobility services synchronization to happen. The valid range is 1 to 10080 minutes. For more information, see the "Performing Location Appliance Synchronization" section on page 15-25.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
NCS Server Backup	Every 7 days at 1 am.	This task is used to schedule the NCS server backup.	Enable—Select or unselect this check box to enable or disable NCS server backup. The default is Disabled. Interval—Enter the interval, in days, that you want the NCS server back up to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the NCS server back up to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Performing NCS Server Backup" section on page 15-26.
OSS Server Status	5 minutes.	This task is used to schedule OSS server status polling.	Enable—Select or unselect this check box to enable or disable OSS Server polling. The default is Enabled. Interval—Enter the interval, in minutes, that you want the OSS server polling to happen. The valid range is 1 to 10080 minutes. For more information, see the "Viewing OSS Server Status" section on page 15-27.
Switch NMSP and Location Status	4 hours	This task is used to schedule the Switch NMSP and Civic Location Polling.	Enable—Select or unselect this check box to enable or disable Switch NMSP and Civic Location polling. The default is Enabled. Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes. For more information, see the "Viewing the Switch NMSP and Location Status" section on page 15-28.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Switch Operational Status	5 minutes. Full poll is 15 minutes.	This task is used to schedule switch operational status polling.	Enable—Select or unselect this check box to enable or disable Switch NMSP and Civic Location polling. Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes. Full operational status interval—Enter the interval, in minutes. The valid range is 1 to 1440 minutes. For more information, see the "Viewing Switch Operational Status" section on page 15-29.

Table 15-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
wIPS Alarm Sync	120 minutes.	This task is used to schedule wIPS alarm synchronization.	Enable—Select or unselect this check box to enable or disable wIPS alarm synchronization. The default is Enabled. Interval—Enter the interval, in minutes, that you want the wIPS alarm synchronization to happen. The valid range is 1 to 10080 minutes. For more information, see the "Performing wIPS Alarm Synchronization" section on page 15-30.
Wired Client Status	2 hours.	This task is used to schedule wired client status polling.	Enable—Select or unselect this check box to enable or disable wired client status polling. The default is Enabled. Interval—Enter the interval, in hours, that you want the wired client status polling to happen. The valid range is 1 to 8640 hours. Major Polling—Specify two time periods that you want the major pollings to happen. The valid format is hh:mm AM|PM. Example: 12:49 AM. For more information, see the "Wired Client Status" section on page 15-31.

Configuring a Virtual Domain

An NCS Virtual Domain consists of a set of NCS devices and/or maps and restricts the user view to information relevant to these managed objects.

Through a virtual domain, an administrator can ensure that users are only able to view the devices and maps for which they are responsible. In addition, because of the virtual domain filters, users are able to configure, view alarms, and generate reports for *only* their assigned part of the network.

Note The following elements can be partitioned in a virtual domain: maps, controllers, access points, templates, and config groups.
The following cannot be partitioned in a virtual domain (and are only available from the root partition: Google Earth Maps, Auto Provisioning, and Mobility Services).

The administrator specifies a set of allowed virtual domains for each user. Only one of these can be active for that user at login. The user can change the current virtual domain by choosing a different allowed virtual domain from the Virtual Domain drop-down list. All reports, alarms, and other functionality are now filtered by that virtual domain.

In the NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. If you do not add a virtual domain to ACS then you are not permitted to log in. This applies regardless of whether you have a single or multiple domains.

Use the Administration > Virtual Domain page to create, edit, delete, import, or export virtual domains. Each virtual domain might contain a subset of the elements included with its parent virtual domain. You can assign additional maps, controllers, access points, and switches to the new virtual domain. See the "Managing a Virtual Domain" section on page 15-47 for more information on managing virtual domains.

The following buttons are available in the Virtual Domain page:

- New—Click to create a new virtual domain. See the "Creating a New Virtual Domain" section on page 15-46 for more information.
- Delete—Click to delete the selected virtual domain from the hierarchy.
- Import—Click to import a CSV file.
- Export—Click to configure custom attributes for the selected virtual domain. See the "Virtual Domain RADIUS and TACACS+ Attributes" section on page 15-49 for more information.

This section contains the following topics:

- Understanding Virtual Domain Hierarchy, page 15-42
- Creating a New Virtual Domain, page 15-46
- Managing a Virtual Domain, page 15-47
- Virtual Domain RADIUS and TACACS+ Attributes, page 15-49
- Understanding Virtual Domains as a User, page 15-50

Understanding Virtual Domain Hierarchy

Virtual domains are organized hierarchically. Subsets of an existing virtual domain contain the network elements that are contained in the parent virtual domain.

Note The default or "ROOT-DOMAIN" domain includes all virtual domains.

Because network elements are managed hierarchically, some features and components such as report generation, searches, templates, config groups, and alarms are affected.

Note If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports. If you create a partition with only a few controllers, choose **Configure > Access Points**, and click an individual link in the AP Name column, the complete list of NCS-assigned controllers is displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

Note If the configuration of a controller is modified by multiple virtual domains, complications might arise. To avoid this, manage each controller from only one virtual domain at a time.

This section describes the effects of partitioning and contains the following topics:

- Reports, page 15-43
- Search, page 15-43
- Alarms, page 15-44
- Templates, page 15-44
- Config Groups, page 15-44
- Maps, page 15-44
- Access Points, page 15-45
- Controllers, page 15-46
- Email Notification, page 15-46

Reports

Reports only include components assigned to the current virtual domain. For example, if you create a virtual domain with only access points and no controllers assigned, all controllers are not displayed when you generate a controller inventory report.

If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

Note Reports are only visible in the current virtual domain. The parent virtual domain cannot view the reports from its subvirtual domain.

Client reports such as Client Count only include clients that belong to the current virtual domain.

Note If new clients are assigned to this partition by the administrator, the previous reports do not reflect these additions. Only new reports reflect the new clients.

Search

Search results only include components that are assigned to the virtual domain in which the search is performed. Search results do not display floor areas when the campus is not assigned to the virtual domain.

Note The saved searches are only visible in the current virtual domain. The parent virtual domain cannot view these search results.

Note The NCS does not partition network lists. If you search a controller by network list, all controllers are returned.

Note Search results do not display floor areas when the campus is not assigned to the virtual domain.

Alarms

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain. Only newly-generated alarms are visible. For example, when a new controller is added to a virtual domain, any alarms generated for that controller prior to its addition do not appear in the current virtual domain.

Alarms are not deleted from a virtual domain when the associated controllers or access points are deleted from the same virtual domain.

Note Alarm Email Notifications—Only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and NCS e-mail notification.

Templates

When you create or discover a template in a virtual domain, it is only available to that virtual domain unless it is applied to a controller. If it is applied to a controller and that controller is assigned to a subvirtual domain, the template stays with the controller in the new virtual domain.

Note If you create a subvirtual domain and then apply a template to both network elements in the virtual domain, the NCS might incorrectly reflect the number of partitions to which the template was applied.

Config Groups

Config groups in a virtual domain can also be viewed by the parent virtual domain. A parent virtual domain can modify config groups for a sub (child) virtual domain. For example, the parent virtual domain can add or delete controllers from a subvirtual domain.

Maps

You can only view the maps that your administrator assigned to your current virtual domain.

- When a campus is assigned to a virtual domain, all buildings in that campus are automatically assigned to the same virtual domain.
- When a building is assigned to a virtual domain, it automatically includes all of the floors associated with that building.
- When a floor is assigned, it automatically includes all of the access points associated with that floor.

Note If only floors are assigned to a virtual domain, you lose some ability to choose map-based features. For example, some reports and searches require you to drill down from campus to building to floor. Because campuses and buildings are not in the virtual domain, you are not able to generate these types of reports or searches.

Note Coverage areas shown in the NCS are only applied to campuses and buildings. In a floor-only virtual domain, the NCS does not display coverage areas.

Note If a floor is directly assigned to a virtual domain, it cannot be deleted from the virtual domain which has the building to which the floor belongs.

Note Search results do not display floor areas when the campus is not assigned to the virtual domain.

Access Points

When a controller or map is assigned to a virtual domain, the access points associated with the controller or map are automatically assigned as well. Access points can also be assigned manually (separate from the controller or map) to a virtual domain.

Note If the controller is removed from the virtual domain, all of its associated access points are also removed. If an access point is manually assigned, it remains assigned even if its associated controller is removed from the current virtual domain.

Note If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

Note If a manually added access point is removed from a virtual domain but is still associated with a controller or map that is assigned to the same virtual domain, the access point remains visible in the virtual domain. Any alarms associated with this access point are not deleted with the deletion of the access point.

Note When maps are removed from a virtual domain, the access points on the maps can be removed from the virtual domain.

Note If you later move an access point to another partition, some events (such as generated alarms) might reside in the original partition location.

Note Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, the NCS uses the detecting controller.
If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

Controllers

Because network elements are managed hierarchically, controllers might be affected by partitioning. If you create a virtual domain with only access points and no controllers assigned, you lose some ability to choose controller-based features. For example, some options require you to drill down from controller to access points. Because controllers are not in the virtual domain, you are not able to generate associated reports.

If you create a partition with only a few controllers, choose Configure > Access Points, and click an individual link in the AP Name column, the complete list of NCS-assigned controllers is displayed for primary, secondary, and tertiary controllers rather than the limited number specified in the partition.

Note If a controller configuration is modified by multiple virtual domains, complications might arise. To avoid this, manage each controller from only one virtual domain at a time.

Email Notification

E-mail notification can be configured per virtual domain. An e-mail is sent only when alarms occur in that virtual domain.

Creating a New Virtual Domain

Note See the "Managing a Virtual Domain" section on page 15-47 for more information.

To create a new virtual domain, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

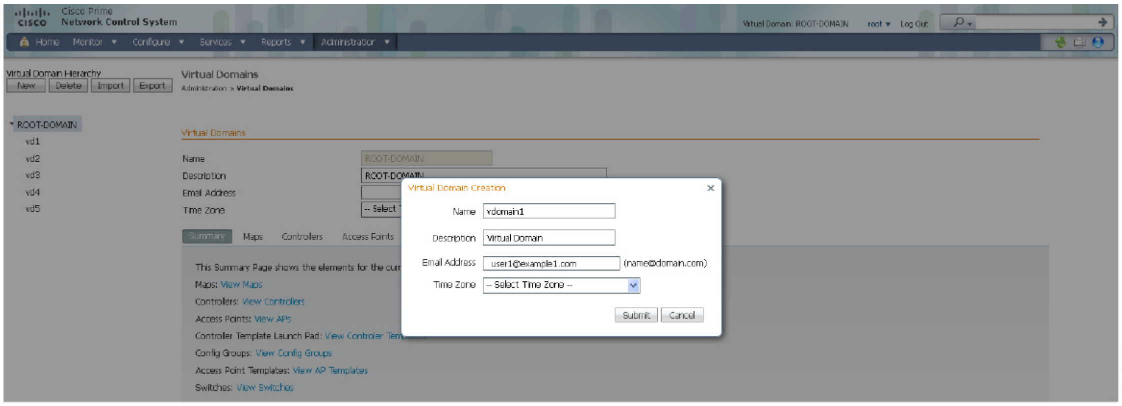
Step 2 From the Virtual Domain Hierarchy left sidebar menu, select the virtual domain to which you want to add a sub (child) virtual domain.

Note The selected virtual domain becomes the parent virtual domain of the newly created subvirtual domain.

Step 3 Click **New** (see Figure 15-4).

The Virtual Domain Creation pop-up dialog box appears.

Figure 15-4 Virtual Domains



Name: ROOT-DOMAIN
Description: ROOT-DOMAIN
Email Address:
Time Zone: -- Select T

This Summary Page shows the elements for the cur
Maps: View Maps
Controllers: View Controllers
Access Points: View APs
Controller Template Launch Pad: View Controller Tem
Config Groups: View Config Groups
Access Point Templates: View AP Templates
Switches: View Switches

Virtual Domain Creation
Name: vdomain1
Description: Virtual Domain
Email Address: user1@example1.com (name@domain.com)
Time Zone: -- Select Time Zone --
Submit Cancel

Step 4 Enter the virtual domain name in the text box.

Step 5 Click **Submit** to create the virtual domain or **Cancel** to close the pop-up dialog box with no changes.

Note Each virtual domain might contain a subset of the elements included with its parent virtual domain. When a user is assigned a virtual domain, that user might view the same maps, controllers, and access points that are assigned to its parent virtual domain.

Note To modify or update a current virtual domain name or description, choose **Administration > Virtual Domains**. From the Virtual Domain Hierarchy left sidebar menu, choose the virtual domain you want to edit.

Managing a Virtual Domain

Choose a virtual domain from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned maps, controllers, access points, and switches. The Summary page appears. This page includes tabs for viewing the currently logged-in virtual domain-available maps, controllers, access points, and switches.

Note Because all maps, controllers, and access points are included in the partition tree, this page takes several seconds to load.

The Maps, Controllers, Access Points, and Switches tabs are used to add or remove components assigned to this virtual domain.

To assign a map, controller, or access point to this domain, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 Choose a virtual domain hierarchy from the Virtual Domain Hierarchy left sidebar menu.

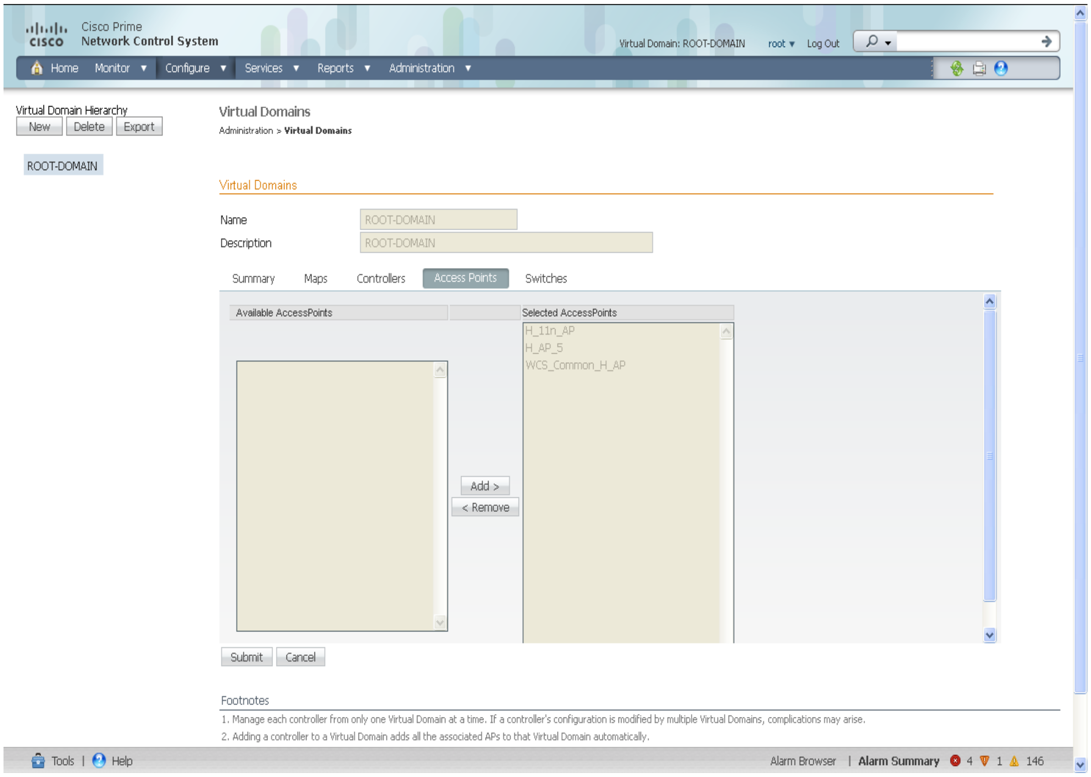
Note Because all maps, controllers, and access points are included in the partition tree, it takes several minutes to load. This time increases if you have a system with a significant number of controllers and access points.

Step 3 Click the applicable **Maps**, **Controller**, or **Access Points** tab.

Step 4 In the Available (Maps, Controllers, or Access Points) column, click to highlight the new component(s) you want to assign to the virtual domain.

Step 5 Click **Add** to move the component(s) to the Selected (Maps, Controllers, or Access Points) column (see Figure 15-5).

Figure 15-5 Virtual Domains Access Points Tab



Name ROOT-DOMAIN

Description ROOT-DOMAIN

Selected AccessPoints:
H_11n_AP
H_AP_5
WCS_Common_H_AP

Footnotes

1. Manage each controller from only one Virtual Domain at a time. If a controller's configuration is modified by multiple Virtual Domains, complications may arise.
2. Adding a controller to a Virtual Domain adds all the associated APs to that Virtual Domain automatically.

Note To remove a component from the virtual domain, click to highlight the component in the Selected (Maps, Controllers, or Access Points) column, and click **Remove**. The component returns to the Available column.

Note If you delete a switch, a controller, or an autonomous AP from the ROOT-DOMAIN, the device is removed from the NCS. If the device is explicitly associated with the ROOT-DOMAIN or any other virtual domain that is not the child of the current virtual domain and if you delete the device from the current virtual domain, the device is removed from this virtual domain but it is not removed from the NCS.

Step 6 Click **Submit** to confirm the changes.

Note After assigning elements to a virtual domain and submitting the changes, the NCS might take some time to process these changes depending on how many elements are added.

Virtual Domain RADIUS and TACACS+ Attributes

The Virtual Domain Custom Attributes page allows you to indicate the appropriate protocol-specific data for each virtual domain. The Export button on the Virtual Domain Hierarchy left sidebar menu preformats the virtual domain RADIUS and TACACS+ attributes. You can copy and paste these attributes into the ACS server. This allows you to copy only the applicable virtual domains into the ACS server page and ensures that the users only have access to these virtual domains.

To apply the preformatted RADIUS and TACACS+ attributes to the ACS server, follow these steps:

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the Virtual Domain Hierarchy left sidebar menu, choose the virtual domain for which you want to apply the RADIUS and TACACS+ attributes.

Step 3 Click **Export**.

Step 4 Highlight the text in the RADIUS or TACACS+ Custom Attributes list (depending on which one you are currently configuring), go to menu of the browser, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to User or Group Setup.

Note If you want to specify virtual domains on a per-user basis, then you need to make sure you add all of the custom attributes (for example, tasks, roles, virtual domains) information to the User custom attribute page.

Step 7 For the applicable user or group, click **Edit Settings**.

Step 8 Use your browser Edit > Paste feature to place the RADIUS or TACACS+ custom attributes into the applicable field.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

Note For more information on adding RADIUS and TACACS+ attributes to the ACS server, see the "Adding NCS User Groups into ACS for TACACS+" section on page 15-105 or the "Adding NCS User Groups into ACS for RADIUS" section on page 15-109.

Understanding Virtual Domains as a User

When you log in, you can access any of the virtual domains that the administrator assigned to you.

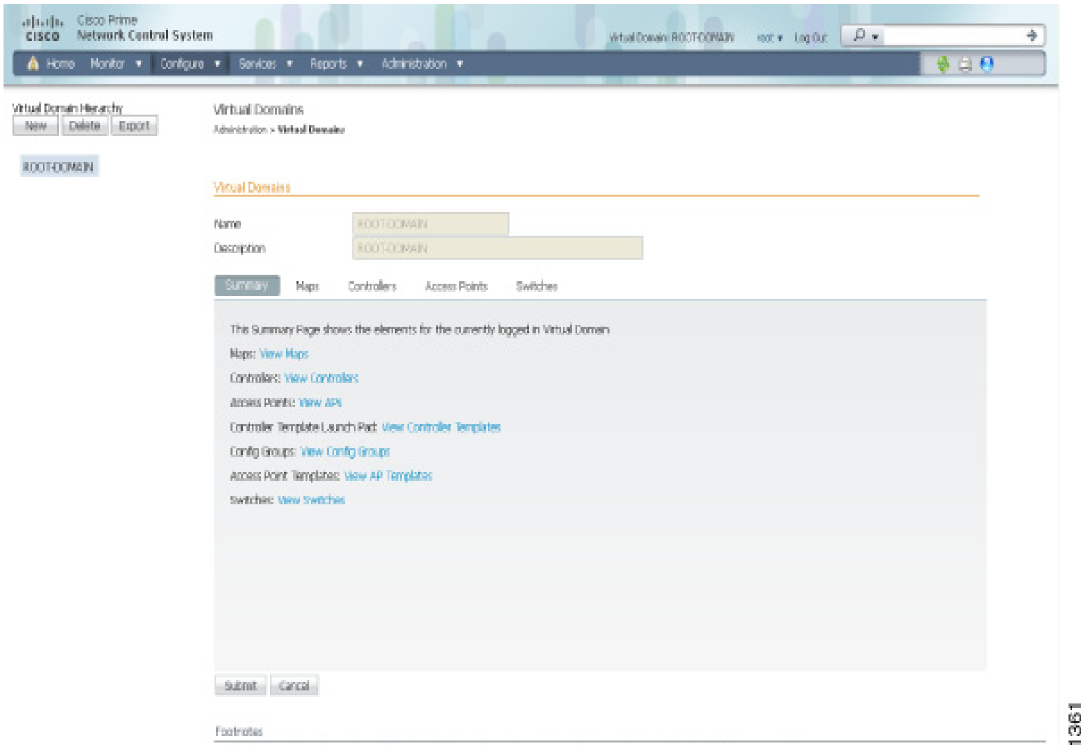
Only one virtual domain can be active at login. You can change the current virtual domain by using the Virtual Domain drop-down list at the top of the page. Only virtual domains that have been assigned to you are available in the drop-down list.

When you select a different virtual domain from the drop-down list, all reports, alarms, and other functionality are filtered by the conditions of the new virtual domain.

Viewing Assigned Virtual Domain Components

To view all components (including maps, controllers, access points, and switches) assigned to the current virtual domain, choose **Administration > Virtual Domains** (see Figure 15-6). Click a link on the Summary tab to view the assigned components for your virtual domain.

Figure 15-6 Virtual Domains Summary Tab



Virtual Domains

Administration > **Virtual Domains**

Virtual Domains

Name: ROOT-DOMAIN

Description: ROOT-DOMAIN

This Summary Page shows the elements for the currently logged in Virtual Domain

Maps: View Maps

Controllers: View Controllers

Access Points: View APs

Controller Template Launch Pad: View Controller Templates

Config Groups: View Config Groups

Access Point Templates: View AP Templates

Switches: View Switches

Limited Menu Access

Non-ROOT-DOMAIN virtual domain users do not have access to the following NCS menus:

- Monitor > RRM
- Configure > Auto Provisioning
- Configure > ACS View Servers

- Mobility > Mobility Services
- Mobility > Synchronize Servers
- Administration > Background Tasks
- Administration > Settings
- Administration > User Preferences
- Tools > Voice Audit
- Tools > Config Audit

Configuring Administrative Settings

Settings contain options for managing the NCS data retention functions. This section describes the sets of options that are available and contains the following topics:

- Configuring Alarms, page 15-51
- Configuring an Audit, page 15-53
- Configuring Clients, page 15-55
- Configuring Protocols for CLI Sessions, page 15-58
- Configuring Controller Upgrade, page 15-58
- Configuring Data Management, page 15-59
- Configuring Guest Account Settings, page 15-61
- Configuring Login Disclaimer, page 15-62
- Configuring the Mail Server, page 15-62
- Configuring the Notification Receiver, page 15-64
- Configuring Reports, page 15-70
- Configuring Server Settings, page 15-71
- Configuring Alarm Severities, page 15-71
- Configuring SNMP Credentials, page 15-72
- Configuring SNMP Settings, page 15-76
- Configuring Switch Port Tracing, page 15-77

Configuring Alarms

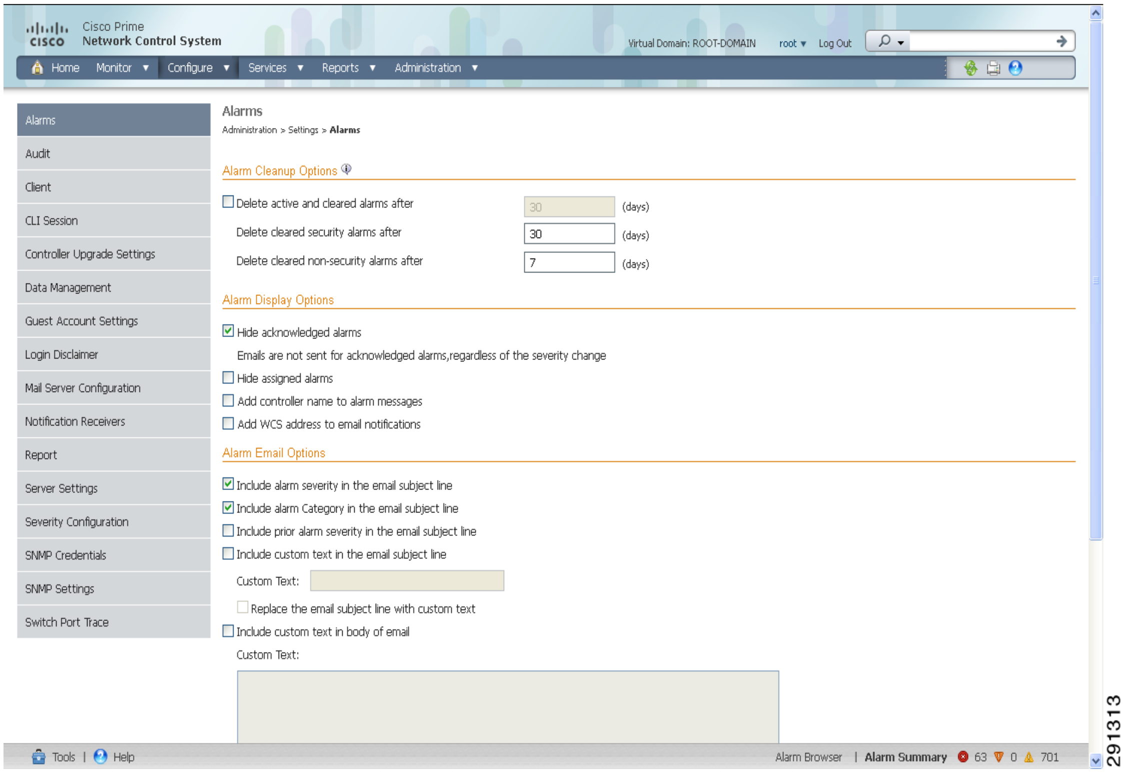
This Alarms page enables you to handle old alarms and display assigned and acknowledged alarms in the Alarm Summary page.

To open this page, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Alarms**. The Administration > Settings > Alarms page appears (see Figure 15-7).

Figure 15-7 Settings > Alarms Page



Alarms

Administration > Settings > **Alarms**

Alarm Cleanup Options

□ Delete active and cleared alarms after 30 (days)

Delete cleared security alarms after 30 (days)

Delete cleared non-security alarms after 7 (days)

Alarm Display Options

☑ Hide acknowledged alarms

Emails are not sent for acknowledged alarms,regardless of the severity change

□ Hide assigned alarms

□ Add controller name to alarm messages

□ Add WCS address to email notifications

Alarm Email Options

☑ Include alarm severity in the email subject line

☑ Include alarm Category in the email subject line

□ Include prior alarm severity in the email subject line

□ Include custom text in the email subject line

Custom Text:

□ Replace the email subject line with custom text

□ Include custom text in body of email

Custom Text:

Step 3 Add or modify the following Alarms parameters:

- Alarm Cleanup Options
  - Delete active and cleared alarms after—Enter the number of days after which active and cleared alarms are deleted. This option can be disabled by unselecting the check box.
  - Delete cleared security alarms after—Enter the number of days after which Security, Rogue AP, and Adhoc Rogue alarms are deleted.
  - Delete cleared non-security alarms after—Enter the number of days after which non-security alarms are deleted. Non-security alarms include all alarms that do not fall under the Security, Rogue AP, or Adhoc Rogue categories.

Note Data cleanup tasks run nightly to delete old alarms. In addition to the data cleanup task, the NCS has an hourly task to check alarm table size. When the alarm table size exceeds 300 K, the task deletes the oldest cleared alarms until the alarm table size is within 300 K.

Note If you want to keep the cleared alarms for more than 7 days, then you can specify a value more than 7 days in the Delete cleared non-security alarms after text box until the alarm table size reaches 300 K.

- Alarm Display Options

Note These preferences only apply to the Alarm Summary page. Quick searches or alarms for any entity display all alarms regardless of the acknowledged or assigned state.

  - Hide acknowledged alarms—When the check box is selected, Acknowledged alarms do not appear on the Alarm Summary page. This option is enabled by default.

    Note E-mails are not generated for acknowledged alarms regardless of severity change.

  - Hide assigned alarms—When the check box is selected, assigned alarms do not appear in the Alarm Summary page.
  - Add controller name to alarm messages—Select the check box to add the name of the controller to alarm messages.
  - Add NCS address to e-mail notifications—Select the check box to add the NCS address to e-mail notifications.

- Alarm E-mail Options
  - Include alarm severity in the e-mail subject line—Select the check box to include alarm severity in the e-mail subject line.
  - Include alarm Category in the e-mail subject line—Select the check box to include alarm category in the e-mail subject line.
  - Include prior alarm severity in the e-mail subject line—Select the check box to include prior alarm severity in the e-mail subject line.
  - Include custom text in the e-mail subject line—Select the check box to add custom text in the e-mail subject line. You can also replace the e-mail subject line with custom text by selecting the Replace the e-mail subject line with custom text check box.
  - Include custom text in body of e-mail—Select the check box to add custom text in the body of e-mail.
  - Include alarm condition in body of e-mail—Select the check box to include alarm condition in the body of e-mail.
  - Add link to Alarm detail page in body of e-mail—Select the check box to add a link to the Alarm detail page in the body of e-mail.
  - Enable Secure Message Mode—Select the check box to enable a secure message mode. If you select the Mask IP Address and Mask Controller Name check boxes, the alarm e-mails are sent in secure mode where all the IP addresses and controller names are masked.

Step 4 Click **Save**.

Configuring an Audit

The Settings > Audit page allows you to determine the type of audit and on which parameters the audit is performed.

- Audit Mode—Choose between basic auditing and template based auditing.
- Audit On—Choose to audit on all parameters or on selected parameters for a global audit.

Audit Mode

The audit mode group box allows you to choose between basic auditing and template based auditing. Basic audit is selected by default.

- Basic Audit—Audits the configuration objects in the NCS database against current WLC device values. Prior to the 5.1.0.0 version of the NCS, this was the only audit mode available.

  Note Configuration objects refer to the device configuration stored in the NCS database.

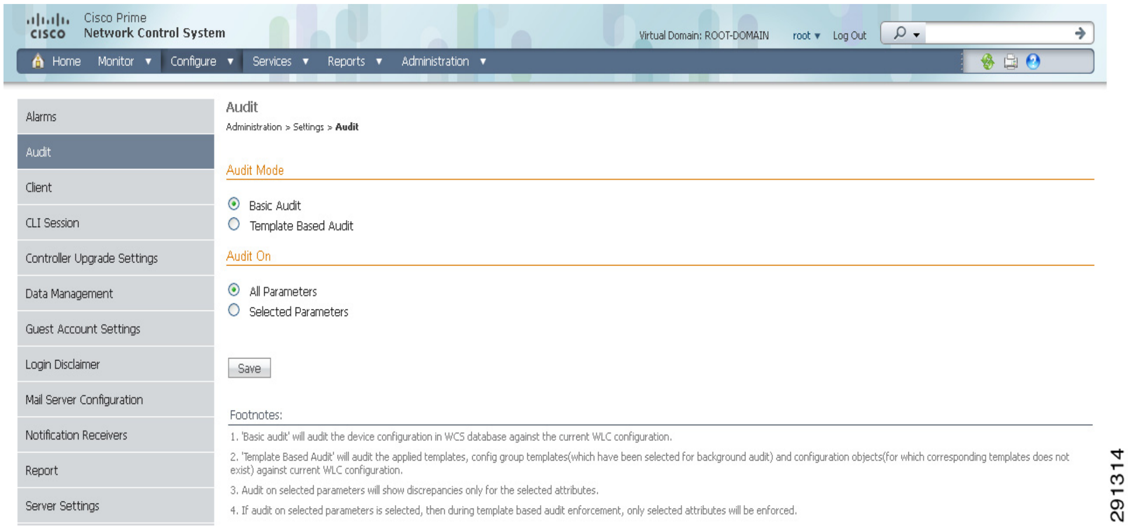
- Template-based Audit—Audits on the applied templates, config group templates (which have been selected for the background audit), and configuration audits (for which corresponding templates do not exist) against current Controller device values.

To indicate the type of audit you want to perform, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Audit**. The Audit Setting page appears (see Figure 15-8).

Figure 15-8 Audit Settings Page



Audit

Administration > Settings > **Audit**

Audit Mode

● Basic Audit
○ Template Based Audit

Audit On

● All Parameters
○ Selected Parameters

Save

Footnotes:

1. 'Basic audit' will audit the device configuration in WCS database against the current WLC configuration.
2. 'Template Based Audit' will audit the applied templates, config group templates(which have been selected for background audit) and configuration objects(for which corresponding templates does not exist) against current WLC configuration.
3. Audit on selected parameters will show discrepancies only for the selected attributes.
4. If audit on selected parameters is selected, then during template based audit enforcement, only selected attributes will be enforced.

Step 3 Select the **Basic Audit** or **Template Based Audit**. A basic audit audits the device configuration in the NCS database against the current Controller configuration. A template-based audit audits the applied templates, config group templates, and configuration objects (for which corresponding templates do not exist) against current Controller configuration.

Step 4 Choose if you want the audit to run on all parameters or only on selected parameters. If you select the Selected Parameters radio button, you can access the Configure Audit Parameters configuration page. (See the "Configuring Audit Parameters" section on page 15-55). The Select audit parameters URL appears.

The selected audit parameters are used during network and controller audits.

Step 5 Click **Save**.

Note These settings are in effect when the controller audit or network audit is performed.

Audit On

The Audit On group box allows you to audit on all parameters or to select specific parameters for an audit. When the Selected Parameters radio button is selected, you can access the Select Audit Parameters configuration page.

The selected audit parameters are used during network and controller audits.

Configuring Audit Parameters

To configure the audit parameters for a global audit, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Audit**.

Step 3 Select the **Selected Parameters** radio button to display the Select Audit Parameters link.

Step 4 Click **Save**.

Step 5 Click **Select Audit Parameters** to choose the required parameters for the audit in the Audit Configuration > Parameter Selection page.

Step 6 Select the parameters that you want audited from each of the tabs. The tabs include System, WLAN, Security, Wireless, and Selected Attributes.

Step 7 When all desired audit parameters are selected, click **Submit** to confirm the parameters or click **Cancel** to close the page without saving any audit parameters.

Once you click **Submit**, the selected audit parameters display on the Selected Attributes tab.

A current Controller Audit Report can be accessed from the Configure > Controllers page by selecting an object from the Audit Status column.

Note You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the Configure > Controllers page, or by clicking **Audit Now** directly from the Controller Audit report. See the "Viewing Audit Status (for Access Points)" section on page 9-196.

Configuring Clients

You can configure the following client processes to improve NCS performance and scalability. This section contains the following topics:

- Processing Diagnostic Trap, page 15-56
- Host Name Lookup, page 15-57
- Data Retention, page 15-57

- Client Traps and Syslogs, page 15-58
- Autonomous Client Traps, page 15-58

To confirm changes to these client configurations, click **Save** at the bottom of the page.

Note See the "Client Troubleshooting Dashlet" section on page 10-4 for further information on client troubleshooting.

Processing Diagnostic Trap

The Settings > Client page allows you to enable automatic client troubleshooting on a diagnostic channel.

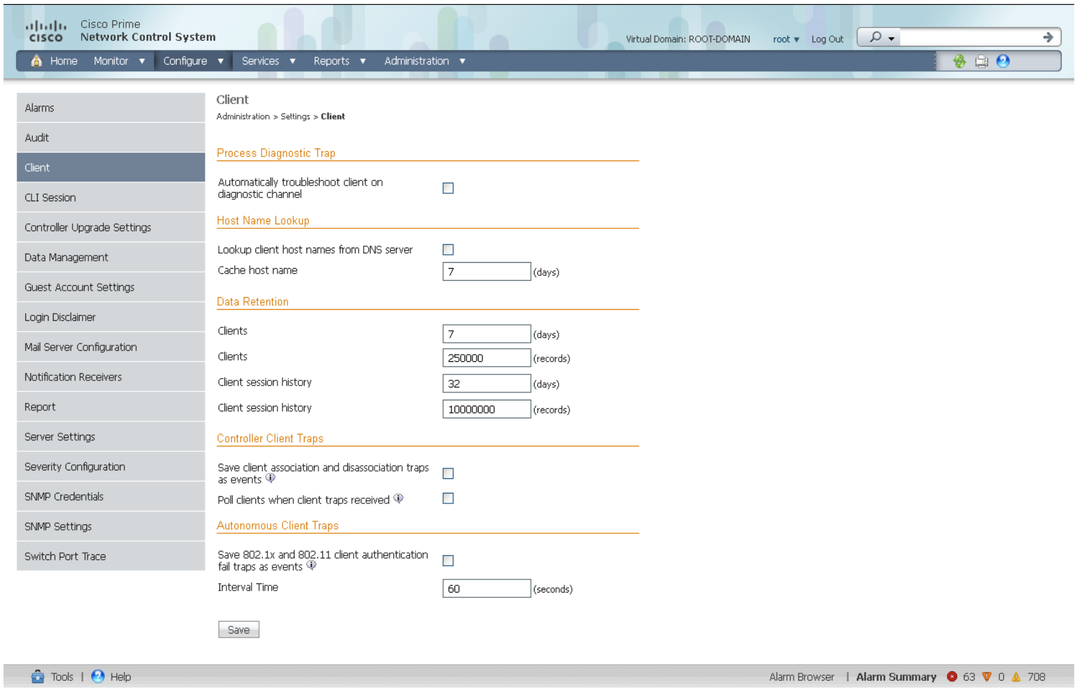
Note Automatic client troubleshooting is only available for CCXV5 or CCXv6 clients.

To enable this automatic client troubleshooting, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**. The Client page appears (see Figure 15-9).

Figure 15-9 Administration > Settings > Client Page



Client
Administration > Settings > **Client**

Process Diagnostic Trap

Automatically troubleshoot client on diagnostic channel □

Host Name Lookup

Lookup client host names from DNS server □
Cache host name 7 (days)

Data Retention

Clients 7 (days)
Clients 250000 (records)
Client session history 32 (days)
Client session history 10000000 (records)

Controller Client Traps

Save client association and disassociation traps as events □
Poll clients when client traps received □

Autonomous Client Traps

Save 802.1x and 802.11 client authentication fail traps as events □
Interval Time 60 (seconds)

Step 3 Select the **Automatically troubleshoot client on diagnostic channel** check box.

Note If the check box is selected, the NCS processes the diagnostic association trap. If it is not selected, the NCS raises the trap, but automated troubleshooting is not initiated.

Note While processing the diagnostic association trap, the NCS invokes a series of tests on the client. The client is updated on all completed tasks. The automated troubleshooting report is placed in dist/acs/win/webnms/logs. When the test is complete, the location of the log is updated in client details pages:V5 tab:Automated Troubleshooting Report group box. An export button allows you to export the logs.

Step 4 Click **Save**.

Host Name Lookup

DNS lookup can take a considerable amount of time. Because of this, you can enable or disable the DNS lookup for client host name. It is set to Disable by default.

To enable host name lookup, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Select the **Lookup client host names from DNS server** check box.

Step 4 Enter the number of days that you want the host name to remain in the cache.

Step 5 Click **Save**.

Data Retention

Client association history can take a lot of database and disk space. This can be an issue for database backup and restore functions. The retaining duration of a client association history can be configured to help manage this potential issue.

To configure data retention parameters, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Enter or edit the following data retention parameters:

- Dissociated Clients (days)—Enter the number of days that you want NCS to retain the data. The default is 7 days. The valid range is 1 to 30 days.
- Client session history (days)—Enter the number of days that you want NCS to retain the data. The default is 32 days. The valid range is 7 to 365 days.

Step 4 Click **Save**.

Client Discovery

If you select the **Poll clients when client traps/syslogs received** check box, the NCS polls clients to quickly identify client sessions. In a busy network, you might want to disable polling while the client traps are received. This option is disabled by default.

Client Traps and Syslogs

In some deployments, the NCS might receive large amounts of client association and disassociation traps. Saving these traps as events might cause a slight performance issue. In such cases, other events that might be useful might be aged out sooner than expected.

To ensure that the NCS does not save client association and disassociation traps as events, unselect the **Save client association and disassociation traps as events** check box. Click **Save** to confirm this configuration change. This option is disabled by default.

For more information on traps and syslogs, see the "Enabling Traps and Syslogs on Switches for Wired Client Discovery" section on page 9-208.

Autonomous Client Traps

Select the **Save 802.1x and 802.11 client authentication fail traps as events** check box if you want to save the Save 802.1x and 802.11 client authentication failed traps as events.

Interval Time—Enter the time interval in seconds to poll for the failed traps.

Configuring Protocols for CLI Sessions

Many NCS features such as autonomous access point and controller command-line interface templates, along with migration templates require executing command-line interface commands on the autonomous access point or controller. These command-line interface commands can be executed by establishing Telnet or SSH sessions. The CLI session page allows you to select the session protocol. SSH is the default.

Note In command-line interface templates, you are not required to answer the question responses (such as *Yes* or *No* answer to a command, *Press enter to continue*, and so on.). This is automatically performed by the NCS.

To configure the protocols for CLI sessions, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **CLI Session**.

Step 3 The default controller session protocol SSH is selected. To choose Telnet, select that radio button.

Step 4 The default autonomous access point session protocol SSH is selected. To choose Telnet, select the radio button.

Step 5 The **Run Autonomous AP Migration Analysis on discovery** radio button is set to **No** by default. Choose **Yes** if you want to discover the autonomous APs as well as perform migration analysis.

Step 6 Click **Save**.

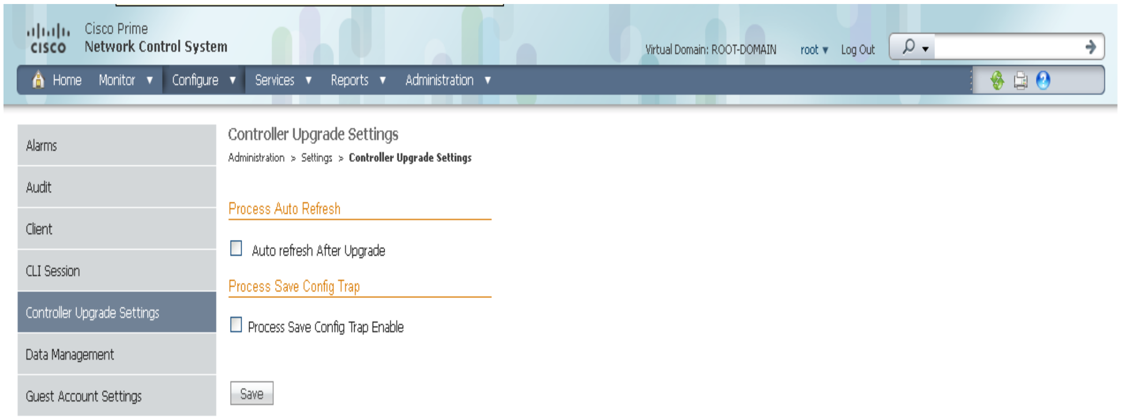
Configuring Controller Upgrade

The Controller Upgrade Settings page allows you to auto-refresh after a controller upgrade. To perform an auto-refresh, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Controller Upgrade Settings** (see Figure 15-10).

Figure 15-10 Controller Upgrade Settings



Controller Upgrade Settings

Administration > Settings > **Controller Upgrade Settings**

Process Auto Refresh

□ Auto refresh After Upgrade

Process Save Config Trap

□ Process Save Config Trap Enable

Save

Step 3 Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the controller image.

Step 4 Determine the action the NCS takes when a save config trap is received. When this check box is enabled, you can choose to retain or delete the extra configurations present on the device but not on the NCS. The setting is applied to all controllers managed by the NCS.

Note If you select the Auto Refresh on Save Config Trap check box in the Configure > Controllers > Properties > Settings page, it overrides this global setting.

Note It might take up to three minutes for the automatic refresh to occur.

Step 5 Click **Save**.

Whenever a save config trap is received by the NCS this check box is selected. When this check box is enabled, it determines the action taken by the NCS.

When this check box is enabled, the user can choose to retain or delete the extra configurations present on device and not on the NCS.

This setting is applied to all of the controllers managed by the NCS. The setting in the controller > properties page for processing the save config trap overrides this global setting.

When there is a change in the controller image, the configuration from the controller is automatically restored.

Configuring Data Management

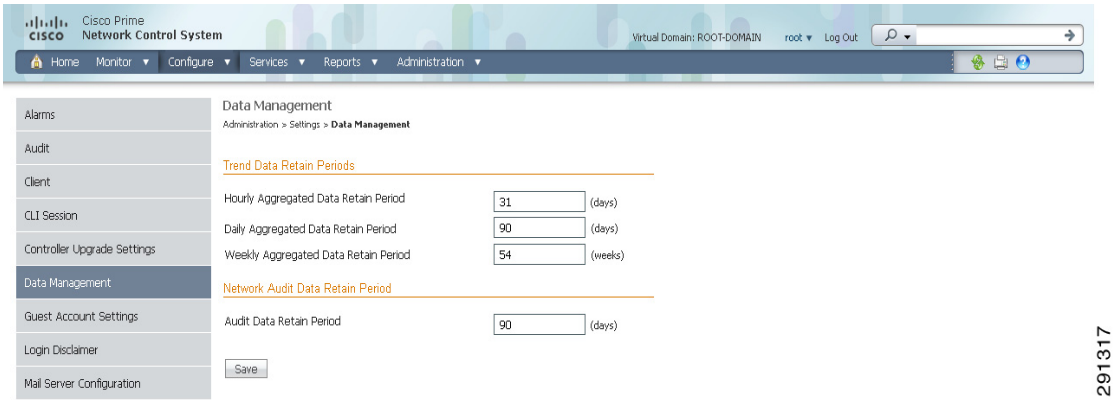
You can configure retention periods on an hourly, daily, and weekly basis.

To set retention periods for aggregated data used in timed calculations and network audit calculations, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Data Management**. The Data Management page appears (see Figure 15-11).

Figure 15-11 Data Management Page



Data Management

Administration > Settings > **Data Management**

Trend Data Retain Periods

Hourly Aggregated Data Retain Period 31 (days)

Daily Aggregated Data Retain Period 90 (days)

Weekly Aggregated Data Retain Period 54 (weeks)

Network Audit Data Retain Period

Audit Data Retain Period 90 (days)

Step 3 Specify the number of days to keep the hourly data. The valid range is 1 to 31. The default is 31 days.

Step 4 Specify the number of days to keep the daily data. The valid range is 7 to 365. The default is 90 days.

Step 5 Specify the number of weeks to keep the weekly data. The valid range is 2 to 108. The default is 54 weeks.

Step 6 Specify the number of days to retain the audit data collected by the Network Audit background task before purging. The limit is 365 days, and the minimum cleanup interval is 7 days. The default is 90 days.

Note For the best interactive graph data views, change the default settings to the maximum possible: 90 days for daily aggregated data and 54 weeks for weekly aggregated data. You must also make the appropriate measures to increase RAM and CPU capacity to compensate for these adjustments.

Step 7 Click **Save**.

NCS Historical Data

There are two types of historical data in the NCS, including the following:

- Aggregated historical data—Numeric data that can be gathered as a whole and aggregated to minimum, maximum, or average. Client count is one example of aggregated historical data.

  Use the Administration > Settings > Data Management page to define the aggregated data retention period. Aggregation types include hourly, daily, and weekly.

  The retention period for these aggregation types are defined as Default, Minimum, and Maximum (see Table 15-3).

Table 15-3 Aggregated Data Retention Periods

Aggregated Data	Default	Minimum	Maximum
Hourly	31 days	1 day	31 days
Daily	90 days	7 days	365 days
Weekly	54 weeks	2 weeks	108 weeks

- Non-aggregated historical data—Numeric data that cannot be gathered as a whole (or aggregated). Client association history is one example of non-aggregated historical data.

  You can define a non-aggregated retention period in each data collection task and other settings.

  For example, you define the retention period for client association history in Administration > Settings > Client. By default, the retention period is 31 days or 1 million records. This retention period can be increased to 365 days.

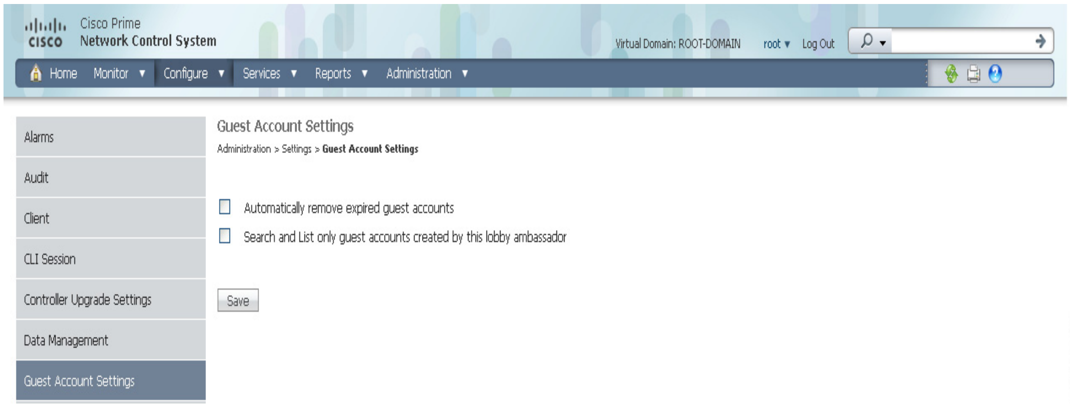
Configuring Guest Account Settings

The Guest Account Settings page allows you to globally remove all expired templates. To configure guest account settings, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Guest Account Settings** (see Figure 15-12).

Figure 15-12 Guest Account Settings Page



Guest Account Settings
Administration > Settings > **Guest Account Settings**

□ Automatically remove expired guest accounts
□ Search and List only guest accounts created by this lobby ambassador

Step 3 When the **Automatically remove expired guest accounts** check box is selected, the guest accounts whose lifetime has ended are not retained, and they are moved to the Expired state. Those accounts in the expired state are deleted from the NCS.

Step 4 By default, the NCS Lobby Ambassador can access all guest accounts irrespective of who created them. If you select the **Search and List only guest accounts created by this lobby ambassador** check box, the Lobby Ambassadors can access only the guest accounts that have been created by them.

Step 5 Click **Save**.

Configuring Login Disclaimer

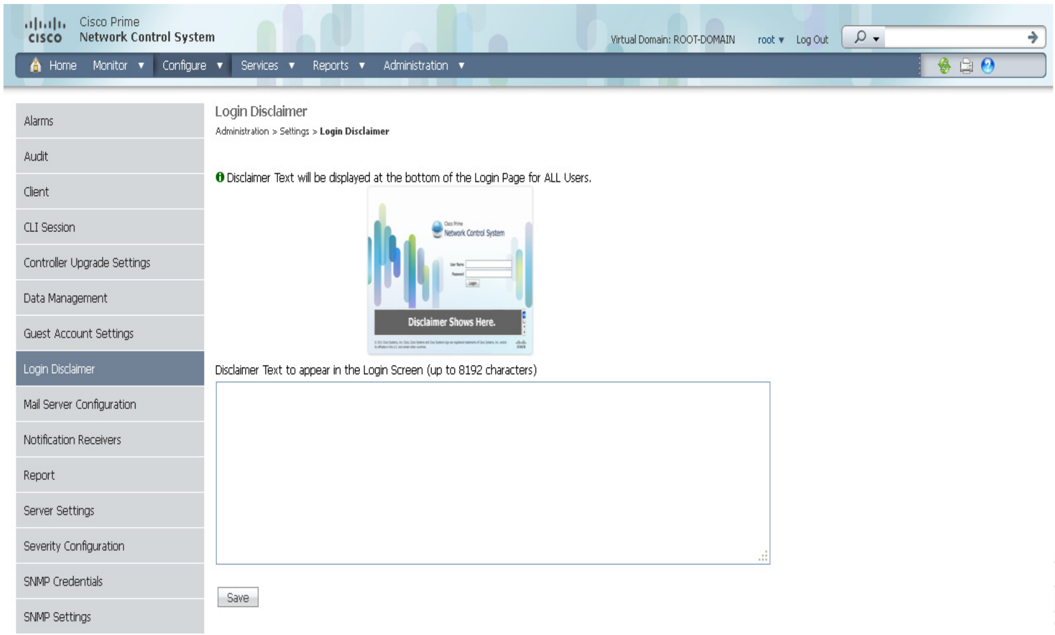
The Login Disclaimer page allows you to enter disclaimer text at the top of the Login page for all users.

To enter Login Disclaimer text, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Login Disclaimer**. The Login Disclaimer page appears (see Figure 15-13).

Figure 15-13 Login Disclaimer Page



Disclaimer Text will be displayed at the bottom of the Login Page for ALL Users.

Disclaimer Text to appear in the Login Screen (up to 8192 characters)

Step 3 Enter your Login Disclaimer text in the available text box.

Step 4 Click **Save**.

Configuring the Mail Server

You can configure global e-mail parameters for sending e-mails from NCS reports, alarm notifications, and so on. This mail server page enables you to configure e-mail parameters in one place. The Mail Server page enables you to set the primary and secondary SMTP server host and port, the e-mail address of the sender, and the e-mail addresses of the recipient.

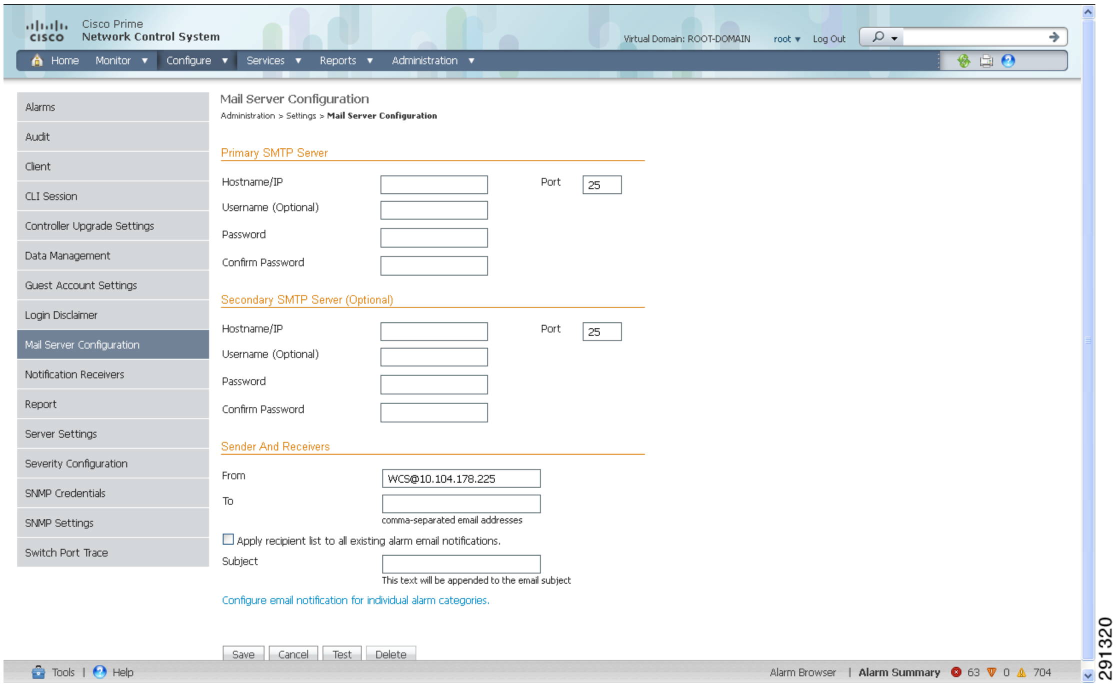
To configure global e-mail parameters, follow these steps:

Note You must configure the global SMTP server before setting global e-mail parameters.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Mail Server Configuration**. The page in Figure 15-14 appears.

Figure 15-14 Mail Server Configuration Page



Mail Server Configuration

Administration > Settings > **Mail Server Configuration**

Primary SMTP Server

Hostname/IP Port 25

Username (Optional)

Password

Confirm Password

Secondary SMTP Server (Optional)

Hostname/IP Port 25

Username (Optional)

Password

Confirm Password

Sender And Receivers

From WCS@10.104.178.225

To

comma-separated email addresses

□ Apply recipient list to all existing alarm email notifications.

Subject

This text will be appended to the email subject

Configure email notification for individual alarm categories.

Step 3 Enter the hostname of the primary SMTP server.

Step 4 Enter the username of the SMTP server.

Step 5 Provide a password for logging on to the SMTP server and confirm it.

Note Both Username and Password are optional.

Step 6 Provide the same information for the secondary SMTP server (only if a secondary mail server is available).

Step 7 The From text box in the Sender and Receivers portion of the page is populated with *NCS@<NCS server IP address>*. You can change it to a different sender.

Step 8 Enter the e-mail addresses of the recipient in the To text box. The e-mail address you provide serves as the default value for other functional areas, such as alarms or reports. Multiple e-mail addresses can be added and should be separated by commas.

Note Global changes you make to the recipient e-mail addresses in Step 7 are disregarded if e-mail notifications were set.

You must indicate the primary SMTP mail server and fill the From address text boxes.

If you want all alarm categories applied to the provided recipient list, select the **Apply recipient list to all alarm categories** check box.

Step 9 Enter the text that you want to append to the e-mail subject.

Step 10 If you click the Configure e-mail notification for individual alarm categories link, you can specify the alarm categories and severity levels you want to enable. E-mail notifications are sent when an alarm occurs that matches categories and the severity levels you select.

Note You can set each alarm severity by clicking the alarm category, choosing Critical, Major, Minor, or Warning, and providing an e-mail address.

Step 11 Click the **Test** button to send a test e-mail using the parameters you configured. The results of the test operation appear on the same page. The test feature checks the connectivity to both primary and secondary mail servers by sending an e-mail with a "NCS test e-mail" subject line.

If the test results were satisfactory, click **Save**.

Configuring the Notification Receiver

The Notification Receiver page displays current notification receivers that support guest access. Alerts and events are sent as SNMPv2 notifications to configured notification receivers.

In this page, you can view current or add additional notification receivers.

This section contains the following topics:

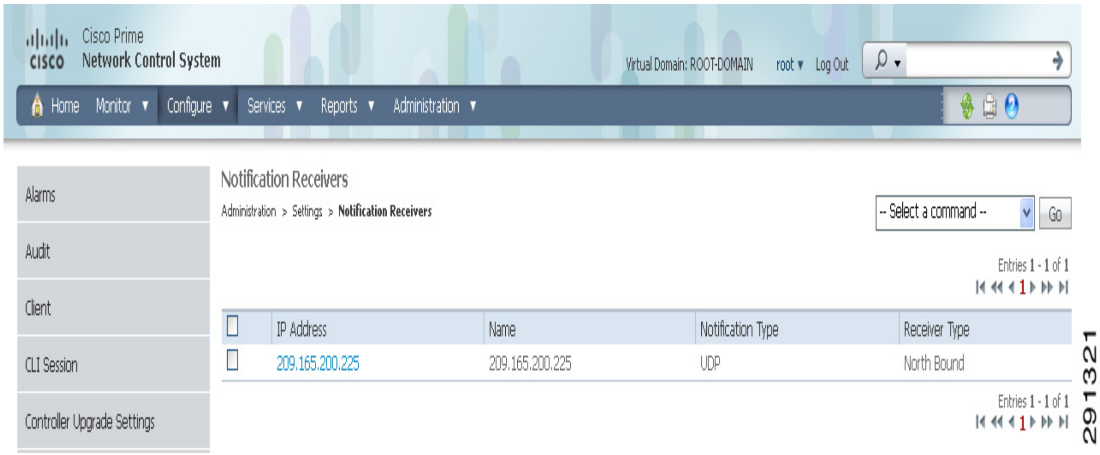
- Adding a Notification Receiver to the NCS, page 15-65
- Removing a Notification Receiver, page 15-66

To access the Notification Receiver page, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear in this page. If you want to add one, choose **Add Notification Receiver** from the Select a command drop-down list, and click **Go** (see Figure 15-15).

Figure 15-15 Notification Receiver Page



Notification Receivers

Administration > Settings > **Notification Receivers**

Entries 1 - 1 of 1

□	IP Address	Name	Notification Type	Receiver Type
□	209.165.200.225	209.165.200.225	UDP	North Bound

Entries 1 - 1 of 1

Adding a Notification Receiver to the NCS

To view current or add additional notification receivers, follow these steps:

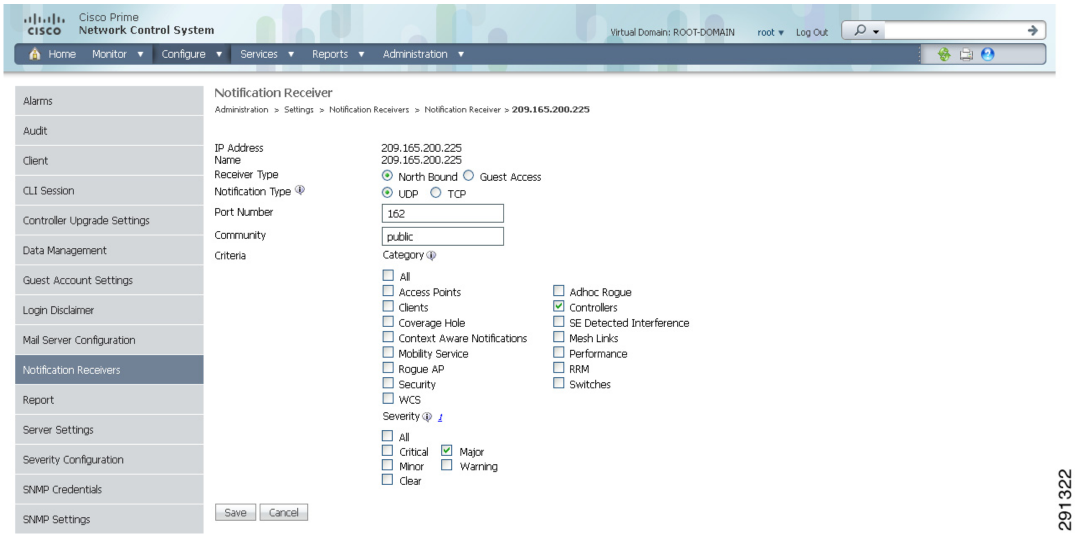
Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.

Step 3 From the Select a command drop-down list, choose **Add Notification Receiver**.

Step 4 Click **Go** (see Figure 15-15).

Figure 15-16 Notification Receiver Page



Notification Receiver

Administration > Settings > Notification Receivers > Notification Receiver > **209.165.200.225**

IP Address 209.165.200.225
Name 209.165.200.225
Receiver Type ● North Bound ○ Guest Access
Notification Type ● UDP ○ TCP
Port Number 162
Community public
Criteria Category

□ All
□ Access Points □ Adhoc Rogue
□ Clients ☑ Controllers
□ Coverage Hole □ SE Detected Interference
□ Context Aware Notifications □ Mesh Links
□ Mobility Service □ Performance
□ Rogue AP □ RRM
□ Security □ Switches
□ WCS

Severity

□ All
□ Critical ☑ Major
□ Minor □ Warning
□ Clear

Save Cancel

Step 5 Enter the server IP address and name.

Step 6 Select either the **North Bound** or **Guest Access** radio button.

The Notification Type automatically defaults to UDP.

Step 7 Enter the UDP parameters including Port Number and Community.

Note The receiver that you configure should be listening to UDP on the same port that is configured.

Step 8 If you selected North Bound as the receiver type, specify the criteria and severity.

Note Alarms for only the selected category are processed.

Note Alarms with only the selected severity matching the selected categories are processed.

Step 9 Click **Save** to confirm the Notification Receiver information.

Note

- By default, only INFO level events are processed for the selected Category.
- Only SNMPV2 traps are considered for North Bound notification.

Removing a Notification Receiver

To delete a notification receiver, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receivers**. All currently configured servers appear on this page.

Step 3 Select the check box(es) of the notification receiver(s) that you want to delete.

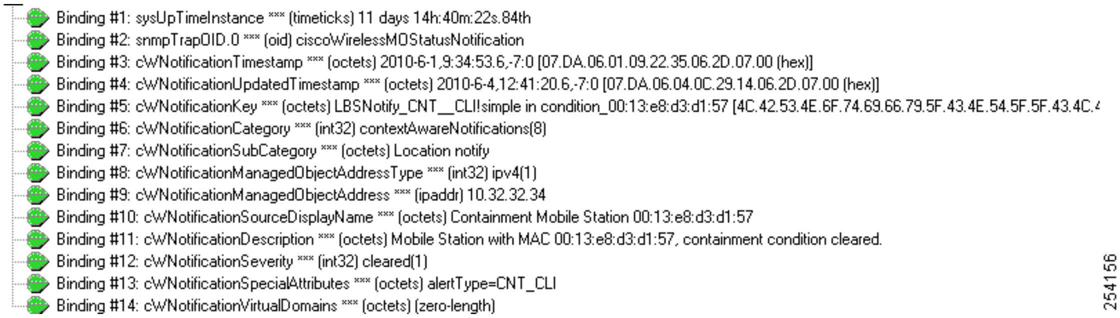
Step 4 From the Select a command drop-down list, click **Remove Notification Receiver**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

The sample display from a North Bound SNMP receiver that has received event traps from the NCS follows:

Figure 15-17 Sample Display from a North Bound SNMP Receiver



```
Binding #1: sysUpTimeInstance *** (timeticks) 11 days 14h:40m:22s.84th
Binding #2: snmpTrapOID.0 *** (oid) ciscoWirelessMOStatusNotification
Binding #3: cWNotificationTimestamp *** (octets) 2010-6-1,9:34:53.6,-7:0 [07.DA.06.01.09.22.35.06.2D.07.00 (hex)]
Binding #4: cWNotificationUpdatedTimestamp *** (octets) 2010-6-4,12:41:20.6,-7:0 [07.DA.06.04.0C.29.14.06.2D.07.00 (hex)]
Binding #5: cWNotificationKey *** (octets) LBSNotify_CNT__CLI!simple in condition_00:13:e8:d3:d1:57 [4C.42.53.4E.6F.74.69.66.79.5F.43.4E.54.5F.5F.43.4C.4
Binding #6: cWNotificationCategory *** (int32) contextAwareNotifications(8)
Binding #7: cWNotificationSubCategory *** (octets) Location notify
Binding #8: cWNotificationManagedObjectAddressType *** (int32) ipv4(1)
Binding #9: cWNotificationManagedObjectAddress *** (ipaddr) 10.32.32.34
Binding #10: cWNotificationSourceDisplayName *** (octets) Containment Mobile Station 00:13:e8:d3:d1:57
Binding #11: cWNotificationDescription *** (octets) Mobile Station with MAC 00:13:e8:d3:d1:57, containment condition cleared.
Binding #12: cWNotificationSeverity *** (int32) cleared(1)
Binding #13: cWNotificationSpecialAttributes *** (octets) alertType=CNT_CLI
Binding #14: cWNotificationVirtualDomains *** (octets) (zero-length)
```

The following sample output shows the log file generated by the NCS. This log file is located in the log file directory on the NCS server (/opt/NCS 1.x/webnms/logs). The log output helps you troubleshoot when alarms are not being received by the North Bound SNMP receiver.

```
06/04/10 08:30:58.559 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]Adding into queue
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrTotalNotifications2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrHandledInNotification2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrNonCongestedIn2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][addNBAlert]Added into queue
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][getNbAlarm]incrHandledOutNotification2
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][startNotifier]Processing the
alertNoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.notification] :
[NbAlertToNmsAlertCorrelator][formVarBindList]Generating the varbind list for NB
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.2.1.1.3.0 variable value: 10 days, 20:22:17.26
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.6.3.1.1.4.1.0 variable value:
1.3.6.1.4.1.9.9.199991.0.1
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.2 variable value:
07:da:05:18:0c:30:0d:09:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.3 variable value:
07:da:06:04:08:1e:3a:04:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.4 variable value:
NoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.5 variable value: 2
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.6 variable value: Radio
load threshold violation
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.7 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.8 variable value:
172.19.29.112
```

```
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.9 variable value: AP
1250-LWAP-ANGN-170-CMR, Interface 802.11b/g/n
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.10 variable value:
Noise changed to acceptable level on '802.11b/g/n' interface of AP
'1250-LWAP-ANGN-170-CMR', connected to Controller '172.19.29.112'.
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.11 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.12 variable value:
06/04/10 08:30:58.565 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.14 variable value:
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]OSS list
size with reachability status as up1
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]Sending
UDP Notification for receiver:172.19.27.85 on port:162
```

MIB to NCS Alert/Event Mapping

Table 15-4 summarizes the Cisco-NCS-Notification-MIB to NCS alert/event mapping.

Table 15-4 Cisco-NCS-Notification-MIB to NCS Alert/Event Mapping

Field Name and Object ID	Data Type	NCS Event/Alert field	Description
cWNotificationTimestamp	DateAndTime	createTime - NmsAlert eventTime - NmsEvent	Creation time for alarm/event.
cWNotificationUpdatedTimestamp	DateAndTime	modTime - NmsAlert	Modification time for Alarm. Events do not have modification time.
cWNotificationKey	SnmpAdminString	objectId - NmsEvent entityString-NmsAlert	Unique alarm/event ID in string form.
cWNotificationSubCategory	OCTET STRING	Type field in alert and eventType in event.	This object represents the subcategory of the alert.
cWNotificationServerAddress	InetAddress	N/A	NCS IP address.

Table 15-4 Cisco-NCS-Notification-MIB to NCS Alert/Event Mapping (continued)

Field Name and Object ID	Data Type	NCS Event/Alert field	Description
cWNotificationManagedObjectAddressType	InetAddressType	N/A	The type of Internet address by which the managed object is reachable. Possible values: 0 - unknown 1 - IPv4 2 - IPv6 3 - IPv4z 4 - IPv6z 16 - DNS Always set to "1" because NCS only supports ipv4 addresses.
cWNotificationManagedObjectAddress	InetAddress	getNode() value is used if present	getNode is populated for events and some alerts. If it is not null, then it is used for this field.
cWNotificationSourceDisplayName	OCTET STRING	sourceDisplayName field in alert/event.	This object represents the display name of the source of the notification.
cWNotificationDescription	OCTET STRING	Text - NmsEvent Message - NmsAlert	Alarm description string.
cWNotificationSeverity	INTEGER	severity - NmsEvent, NmsAlert	Severity of the alert/event critical(1), major(2), minor(3), warning(4), clear(5), info(6), unknown(7).

Table 15-4 Cisco-NCS-Notification-MIB to NCS Alert/Event Mapping (continued)

Field Name and Object ID	Data Type	NCS Event/Alert field	Description
cWNotificationSpecialAttributes	OCTET STRING	All the attributes in alerts/events apart from the base alert/event class.	This object represents the specialized attributes in alerts like APAssociated, APDisassociated, RogueAPAlert, CoverageHoleAlert, and so on. The string is formatted in 'property=value' pairs in CSV format.
cWNotificationVirtualDomains	OCTET STRING	N/A	Virtual Domain of the object that caused the alarm. This field is not populated for running release and this is populated with empty string.

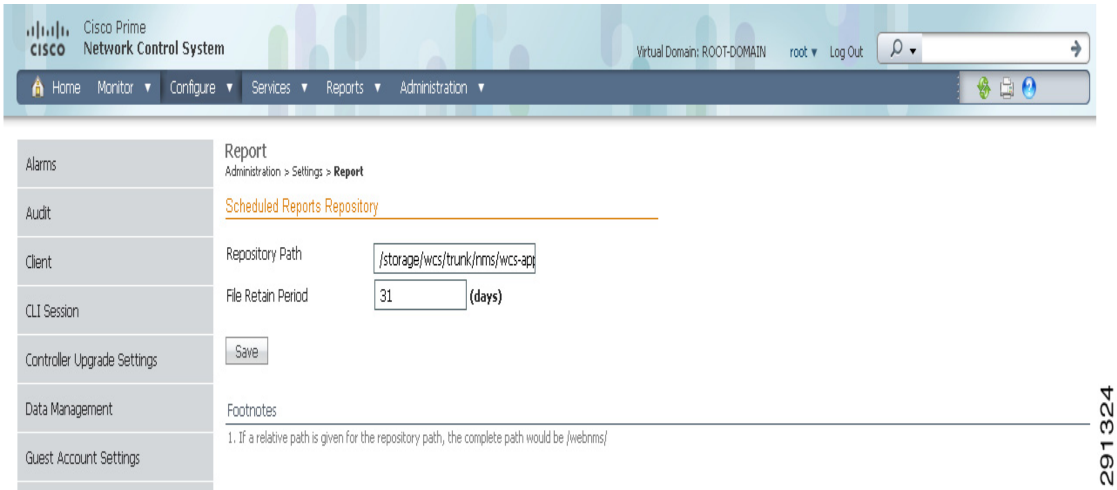
Configuring Reports

To indicate where the scheduled reports reside and for how many days, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Report**. The Report page appears (see Figure 15-18).

Figure 15-18 Report Page



Report
Administration > Settings > **Report**

Scheduled Reports Repository

Repository Path /storage/wcs/trunk/nms/wcs-apr

File Retain Period 31 **(days)**

Save

Footnotes

1. If a relative path is given for the repository path, the complete path would be /webnms/

Step 3 Enter the path for saving report data files on a local PC. You can edit the existing default path.

Step 4 Specify the number of days to retain report data files.

Step 5 Click **Save**.

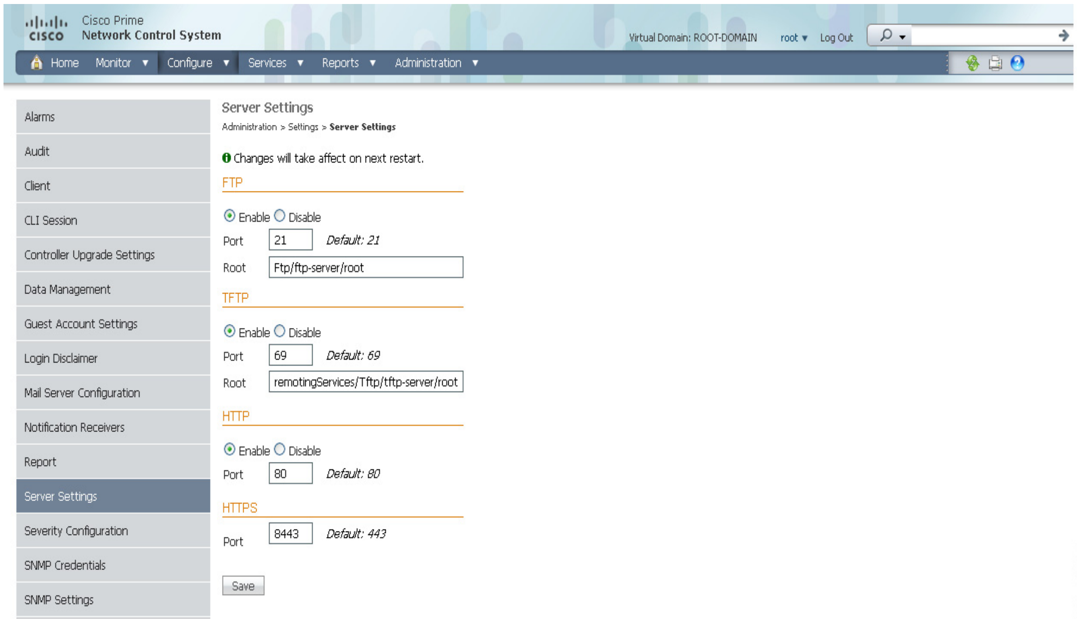
Configuring Server Settings

To turn TFTP, FTP, HTTP, or HTTPS on or off, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Server Setting**. The Server Settings page appears (see Figure 15-19).

Figure 15-19 Server Settings Page



Server Settings

Administration > Settings > **Server Settings**

Changes will take affect on next restart.

FTP

● Enable ○ Disable

Port 21 *Default: 21*

Root Ftp/ftp-server/root

TFTP

● Enable ○ Disable

Port 69 *Default: 69*

Root remotingServices/Tftp/tftp-server/root

HTTP

● Enable ○ Disable

Port 80 *Default: 80*

HTTPS

Port 8443 *Default: 443*

291325

Step 3 If you want to modify the FTP and TFTP directories or the HTTP and HTTPS ports that were established during installation, enter the port number (or port number and root where required) that you want to modify and click **Enable** or **Disable**.

The changes are reflected after a restart.

Configuring Alarm Severities

You can change the severity level for newly generated alarms.

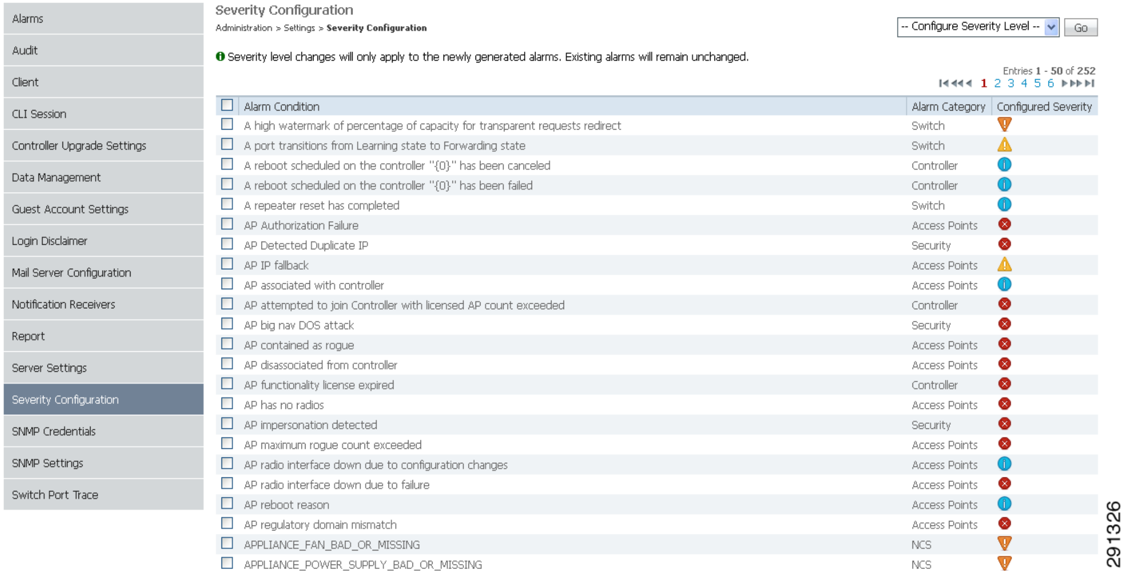
Note Existing alarms remain unchanged.

To change the severity level of newly generated alarms, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 Choose **Severity Configuration** from the left sidebar menu. The Severity Configuration page appears (see Figure 15-20).

Figure 15-20 Severity Configuration Page



Severity Configuration

Administration > Settings > **Severity Configuration**

Severity level changes will only apply to the newly generated alarms. Existing alarms will remain unchanged.

Entries **1** - **50** of **252**

|◀ ◀◀ ◀ 1 2 3 4 5 6 ▶ ▶▶ ▶|

□	Alarm Condition	Alarm Category	Configured Severity
□	A high watermark of percentage of capacity for transparent requests redirect	Switch	▼
□	A port transitions from Learning state to Forwarding state	Switch	⚠
□	A reboot scheduled on the controller "{0}" has been canceled	Controller	ℹ
□	A reboot scheduled on the controller "{0}" has been failed	Controller	ℹ
□	A repeater reset has completed	Switch	ℹ
□	AP Authorization Failure	Access Points	✖
□	AP Detected Duplicate IP	Security	✖
□	AP IP fallback	Access Points	⚠
□	AP associated with controller	Access Points	ℹ
□	AP attempted to join Controller with licensed AP count exceeded	Controller	✖
□	AP big nav DOS attack	Security	✖
□	AP contained as rogue	Access Points	✖
□	AP disassociated from controller	Access Points	✖
□	AP functionality license expired	Controller	✖
□	AP has no radios	Access Points	✖
□	AP impersonation detected	Security	✖
□	AP maximum rogue count exceeded	Access Points	✖
□	AP radio interface down due to configuration changes	Access Points	ℹ
□	AP radio interface down due to failure	Access Points	✖
□	AP reboot reason	Access Points	ℹ
□	AP regulatory domain mismatch	Access Points	✖
□	APPLIANCE_FAN_BAD_OR_MISSING	NCS	▼
□	APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING	NCS	▼

Step 3 Select the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Severity Level drop-down list, choose the new severity level (Critical, Major, Minor, Warning, Informational, Reset to Default).

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the change.

Configuring SNMP Credentials

The SNMP Credentials page allows you to specify credentials to use for tracing the rogue access points. Use this option when you cannot find a specific entry using a number-based entry. When a switch credential is not added to the NCS, you can use SNMP credentials on this page to connect to the switch.

To configure SNMP credentials, follow these steps:

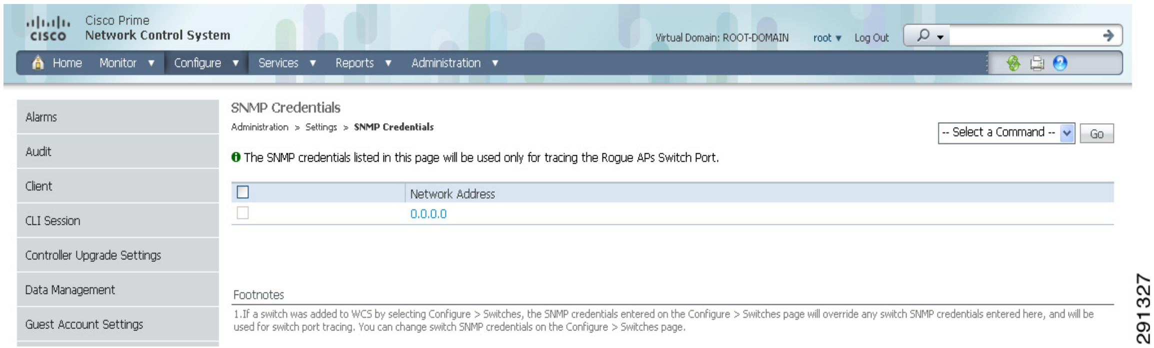
Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**. The SNMP Credentials page appears (see Figure 15-21).

Step 3 To view or edit details about a current SNMP entry, click the **Network Address** link. See the "Viewing Current SNMP Credential Details" section on page 15-73 for more information.

Note The default network address is 0.0.0.0 which indicates the entire network. An SNMP credential is defined per network so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. The default community string is *private* for both read and write. You should update the prepopulated SNMP credential with your own SNMP information.

Figure 15-21 SNMP Credentials Page



SNMP Credentials

Administration > Settings > **SNMP Credentials**

The SNMP credentials listed in this page will be used only for tracing the Rogue APs Switch Port.

□	Network Address
□	0.0.0.0

Footnotes

1.If a switch was added to WCS by selecting Configure > Switches, the SNMP credentials entered on the Configure > Switches page will override any switch SNMP credentials entered here, and will be used for switch port tracing. You can change switch SNMP credentials on the Configure > Switches page.

Step 4 To add a new SNMP entry, choose **Add SNMP Entries** from the Select a command drop-down list, and click **Go**. See the "Adding a New SNMP Credential Entry" section on page 15-74 for more information.

Viewing Current SNMP Credential Details

To view or edit details for current SNMP credentials, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**.

Step 3 Click the Network Address link to open the SNMP Credential Details page. The details page displays the following information:

General Parameters

- Add Format Type—Display only. See the "Adding a New SNMP Credential Entry" section on page 15-74 for more information regarding Add Format Type.
- Network Address
- Network Mask

SNMP Parameters—Select the applicable version(s) for SNMP parameters. The SNMP credentials are validated according to which SNMP version(s) are selected.

Note Enter SNMP parameters for write access, if available. With Display only access parameters, the switch is added but you cannot modify its configuration in the NCS. Device connectivity tests use the SNMP retries and timeout parameters configured in Administration > Settings > SNMP Settings.

- Retries—The number of times that attempts are made to discover the switch.
- Timeout—The session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.
- SNMP v1 Parameters or v2 Parameters—If selected, enter the applicable community in the available text box.
- SNMP v3 Parameters—If selected, configure the following parameters:
  - Username
  - Auth. Type
  - Auth. Password
  - Privacy Type
  - Privacy Password

Note If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non-default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

Step 4 Click **OK** to save changes or **Cancel** to return to the SNMP Credentials page without making any changes to the SNMP credential details.

Adding a New SNMP Credential Entry

To add a new SNMP credential entry, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**.

Step 3 From the Select a command drop-down list, choose **Add SNMP Entries**.

Step 4 Click **Go**. The SNMP Credentials page opens (see Figure 15-21).

Step 5 Choose one of the following:

To manually enter SNMP credential information, leave the Add Format Type drop-down list at SNMP Credential Info. To add multiple network addresses, use a comma between each address. Go to Step 7.

If you want to add multiple switches by importing a CSV file, choose **File** from the Add Format Type drop-down list. The CSV file allows you to generate your own import file and add the devices you want. Go to Step 6.

Step 6 If you chose File, click **Browse** to find the location of the CSV file you want to import. Skip to Step 11.

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory.

Sample File:

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_passw
ord,snmpv3_privacy_type,snmpv3_privacy_password,network_mask
1.1.1.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,255.255.255.0
10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```

The CSV file can contain the following fields:

- ip_address:IP address
- snmp_version:SNMP version
- network_mask:Network mask
- snmp_community:SNMP V1/V2 community
- snmpv3_user_name:SNMP V3 username
- snmpv3_auth_type:SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA
- snmpv3_auth_password:SNMP V3 authorization password
- snmpv3_privacy_type:SNMP V3 privacy type. Can be None or DES or CFB-AES-128
- snmpv3_privacy_password:SNMP V3 privacy password
- snmp_retries:SNMP retries
- snmp_timeout:SNMP timeout

Step 7 If you chose SNMP Credential Info, enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between the string of IP addresses.

Step 8 In the Retries field, enter the number of times that attempts are made to discover the switch.

Step 9 Provide the session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.

Step 10 Select the applicable version(s) for SNMP parameters. The SNMP credentials are validated according to which SNMP version(s) are selected.

- If SNMP v1 Parameters or v2 Parameters is selected, enter the applicable community in the available text box.
- If SNMP v3 Parameters is selected, configure the following parameters:
  - Username
  - Auth. Type
  - Auth. Password
  - Privacy Type
  - Privacy Password

Note If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non-default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

Step 11 Click **OK**.

If the NCS can use the SNMP credential listed to access the switch, the switch is added for later use and appears in the Configure > Ethernet Switches page.

Note If you manually added switches through the Configure > Ethernet Switches page, then switch port tracing uses the credentials from that page, not the ones listed in the SNMP Credentials page. If the manually-added switch credentials have changed, you need to update them from the Configure > Ethernet page.

Configuring SNMP Settings

The SNMP Settings page allows you to configure global SNMP settings from the NCS.

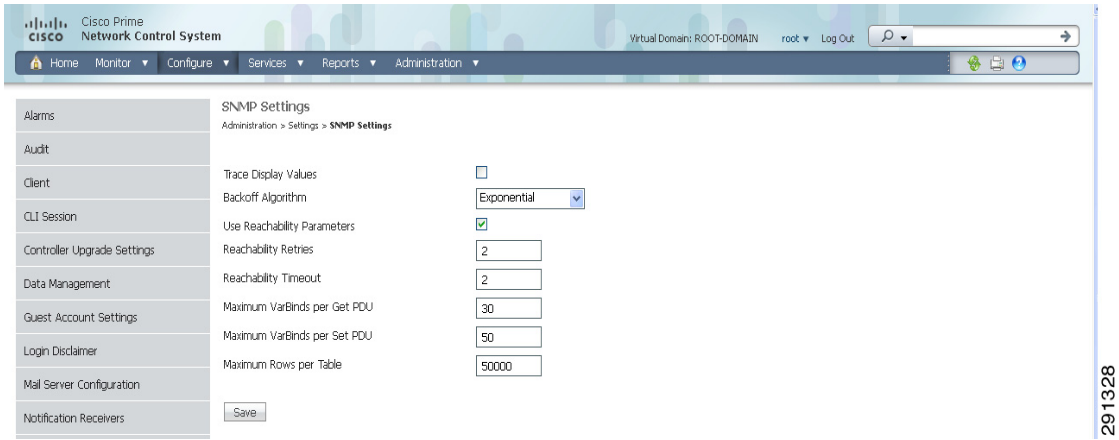
Note Any changes you make on this page affects the NCS globally. The changes are saved across restarts as well as across backups and restores.

To configure global SNMP settings, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **SNMP Settings**. The SNMP Settings page appears (see Figure 15-22).

Figure 15-22 SNMP Settings Page



SNMP Settings

Administration > Settings > **SNMP Settings**

Trace Display Values	□
Backoff Algorithm	Exponential
Use Reachability Parameters	☑
Reachability Retries	2
Reachability Timeout	2
Maximum VarBinds per Get PDU	30
Maximum VarBinds per Set PDU	50
Maximum Rows per Table	50000

Step 3 If the Trace Display Values check box is selected, mediation trace-level logging shows data values fetched from the controller using SNMP. If unselected, the values do not appear.

Note The default is unselected for security reasons.

Step 4 For the Backoff Algorithm, choose either **Exponential** or **Constant Timeout** from the drop-down list. If you choose Exponential (the default value), each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time.

Note Constant Timeout is useful on unreliable networks (such as satellite networks) where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.

Step 5 Determine if you want to use reachability parameters. If selected, the NCS defaults to the global Reachability Retries and Timeout that you configure. If unselected, the NCS always uses the timeout and retries specified per-controller or per-IOS access point. The default is selected.

Note Adjust this setting downward if switch port tracing is taking a long time to complete.

Step 6 For the Reachability Retries field, enter the number of global retries used for determining device reachability. The default number is 2. This field is only available if the Use Reachability Parameters check box is selected.

Note Adjust this setting downward if switch port tracing is taking a long time to complete.

Step 7 For the Reachability Timeout field, enter a global timeout used for determining device reachability. The default number is 2. This field is only available if the Use Reachability Parameters check box is selected.

Step 8 At the Maximum VarBinds per PDU field, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. The default is 100.

Note For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.

Step 9 The maximum rows per table field is configurable and the default value is 50000 rows. The configured value is retained even if you upgrade the NCS version.

Step 10 Click **Save** to confirm these settings.

Configuring Switch Port Tracing

Currently, the NCS provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, the NCS simply gathers the information received from the controllers; but with software Release 5.1, you can now incorporate switch port tracing of Wired Rogue Access Point Switch Ports. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in the NCS log and only for rogue access points, not rogue clients.

Note Rogue Client connected to the Rogue Access point information is used to track the switch port to which the Rogue Access point is connected in the network.

Note If you try to set tracing for a friendly or deleted rogue, a warning message appears.

Note For Switch Port Tracing to successfully trace the switch ports using v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group.

Note See the "Configuring Switch Port Tracing" section on page 15-77 for information on configuring Switch Port Tracing settings.

The Switch Port Trace page allows you to run a trace on detected rogue access points on the wire.

To correctly trace and contain rogue access points, you must correctly provide the following information.

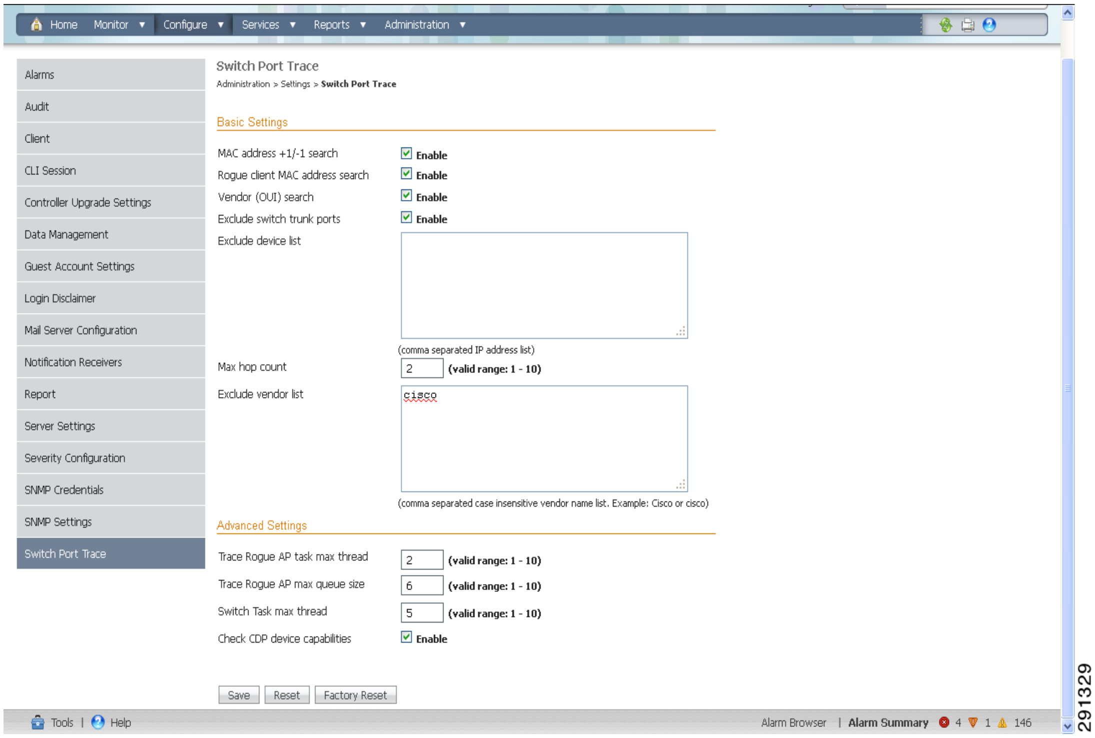
- Reporting APs—A rogue access point has to be reported by one or more managed access points.
- AP CDP Neighbor—Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials—All switches to be traced must have a management IP address and SNMP management enabled. You can add network address based entries instead of only adding individual switches. The correct write community string must be specified to enable/disable switch ports. For tracing, read community strings are sufficient.
- Switch port configuration—Trunking switch ports must be correctly configured. Switch port security must be turned off.
- Only Cisco Ethernet switches are supported.
- Switch VLAN settings must be properly configured.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- You should have some traffic between rogue access points and the Ethernet switch.
- The rogue access point must be connected to a switch within the max hop limit. The default hop count is 2, and the maximum is 10.
- If SNMPv3 is chosen, use the context option and create one for each VLAN, in addition to the one for the main group (which is required for non-VLAN-based MIBs).

To specify options for switch port tracing, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Switch Port Trace** (see Figure 15-23).

Figure 15-23 Switch Port Trace Page



Switch Port Trace

Administration > Settings > **Switch Port Trace**

Basic Settings

MAC address +1/-1 search ☑ **Enable**

Rogue client MAC address search ☑ **Enable**

Vendor (OUI) search ☑ **Enable**

Exclude switch trunk ports ☑ **Enable**

Exclude device list

(comma separated IP address list)

Max hop count 2 **(valid range: 1 - 10)**

Exclude vendor list cisco

(comma separated case insensitive vendor name list. Example: Cisco or cisco)

Advanced Settings

Trace Rogue AP task max thread 2 **(valid range: 1 - 10)**

Trace Rogue AP max queue size 6 **(valid range: 1 - 10)**

Switch Task max thread 5 **(valid range: 1 - 10)**

Check CDP device capabilities ☑ **Enable**

Step 3 Configure the following basic settings as needed:

- MAC address +1/-1 search—Select the check box to enable.

  This search involves the MAC address +1/-1 convention where the wired-side MAC address of the rogue access point is obtained by adding or subtracting the radio MAC address by one.

- Rogue client MAC address search—Select the check box to enable.

  When a rogue access point client exists, the MAC address of the client is added to the searchable MAC address list.

- Vendor (OUI) search—Select the check box to enable. OUI refers to Organizational Unique Identifier search which searches the first 3 bytes in a MAC address.

- Exclude switch trunk ports—Select the check box to exclude switch trunk ports from the switch port trace.

  Note When more than one port is traced for a given MAC address, additional checks are performed to improve accuracy. These checks include: trunk port, non-AP CDP neighbors present on the port, and whether or not the MAC address is the only one on this port.

- Exclude device list—Select the check box to exclude additional devices from the trace. Enter into the device list text box each device that you want to exclude from the switch port trace. Separate each device names with commas.

- Max hop count—Enter the maximum number of hops for this trace. Keep in mind that the greater the hop count, the longer the switch port trace takes to perform.

- Exclude vendor list—Enter in the vendor list text box any vendors that you want to exclude from the switch port trace. Separate vendor names with commas. The vendor list is not case sensitive.

Step 4 Configure the following advanced settings as needed:

- TraceRogueAP task max thread—Switch port tracing uses multiple threads to trace rogue access points. This field indicates the maximum number of rogue access points that can be traced on parallel threads.
- TraceRogueAP max queue size—Switch port tracing maintains a queue to trace rogue access points. Whenever you select a rogue access point for tracing, it is queued for processing. This field indicates the maximum number of entries that you can store in the queue.
- SwitchTask max thread—Switch port tracing uses multiple threads to query switch devices. This field indicates the maximum number of switch devices that you can query on parallel threads.

Note The default value for these parameters should be good for normal operations. These parameters directly impact the performance of switch port tracing and NCS. Unless required, We do not recommend that you alter these parameters.

- Select CDP device capabilities—Select the check box to enable.

Note The NCS uses CDP to discover neighbors during tracing. When the neighbors are verified, the NCS uses the CDP capabilities field to determine whether or not the neighbor device is a valid switch. If the neighbor device is not a valid switch, it is not traced.

Step 5 Click **Save** to confirm changes made. Click **Reset** to return the page to the original settings. Click **Factory Reset** to return settings to the factory defaults.

Establishing Switch Port Tracing

To establish switch port tracing, follow these steps:

Step 1 In the NCS home page, click the **Security** dashboard.

Step 2 In the Rogue APs and Adhoc Rogues section, click the number URL which specifies the number of rogues in the last hour, last 24 hours, or total active.

Step 3 Choose for which rogue you are setting switch port tracking by clicking the URL in the MAC Address column. The Alarms > Rogue AP details page opens.

Step 4 From the Select a command drop-down list, choose **Trace Switch Port**. The Trace Switch Port page opens and NCS runs a switch port trace.

When one or more searchable MAC addresses are available, the NCS uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue switch port.

The SNMP communities for the switches are provided in the "Configuring Switches" section on page 9-200.

See the "Switch Port Tracing Details" section on page 15-81 for additional information on the Switch Port Tracing Details dialog box.

Switch Port Tracing Details

In the Switch Port Tracing Details dialog box, you can enable or disable switch ports, trace switch ports, and view detail status of the access point switch trace. For more information on Switch Port Tracing, see the following topics:

- Configuring Switch Port Tracing—Provides information on configuring switch port trace settings.
- Configuring Switches—Provides information on configuring SNMP switches.
- Configuring SNMP Credentials—Provides information on configuring SNMP switch credentials.

In the Switch Port tracing Details dialog box, do one of the following:

- Click **Enable/Disable Switch Port(s)**—Enables or disables any selected ports.
- Click **Trace Switch Port(s)**—Runs another switch port trace.
- Click **Show Detail Status**—Displays details regarding the switch port traces for this access point.
- Click **Close**.

Switch Port Tracing Troubleshooting

Switch Port Tracing (SPT) works on a best-effort-basis. SPT depends on the following information to correctly trace and contain rogue APs:

- Reporting access points—A rogue access point must be reported by one or more managed access points.
- Access point CDP neighbor—Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials
  - All the switches that need to be traced should have a management IP address and SNMP management enabled.
  - With the new SNMP credential changes, instead of adding the individual switches to the NCS, network address based entries can be added.
  - The new SNMP credential feature has a default entry 0.0.0.0 with default community string as 'private' for both read/write.
  - Correct write community string has to be specified to enable/disable switch ports. For tracing, read community string should be sufficient.
- Switch port configuration
  - Switch ports that are trunking should be correctly configured as trunk ports.
  - Switch port security should be turned off.
- Only Cisco Ethernet switches are supported.

Note The following switches are supported: 3750, 3560, 3750E, 3560E, and 2960.

- Switch VLAN settings should be properly configured.
- CDP protocol should be enabled for all the switches.
- An Ethernet connection should exist between the rogue access point and the Cisco switch.
- There should be some traffic between the rogue access point and the Ethernet switch.
- The rogue access point should be connected to a switch within the max hop limit. Default hop is 2. Max hop is 10.
- If SNMPv3 is used, then make sure you use the context option and create one for each VLAN in addition to the one for the main group (which is required for non-VLAN based MIBs).

Setting User Preferences

Choose Administration > User Preferences to open the User Preferences page. The User Preferences page enables you to control certain display options in the NCS.

Note When the non-root users log into NCS and try to modify the user preferences, the "Permission Denied" message appears, which is an expected behavior.

List Pages

- Items Per List—You can set the number of items, such as controllers or access points, to display in pages that list these items. Choose the number of items to display from the Items Per List Page drop-down list.

User Idle Timeout

- Logout idle user—Select the check box if you want to configure the amount of time, in minutes, that a user session can be idle before the server cancels the session.
- Logout idle user after—Select the maximum number of minutes that a server waits for an idle user. The default value is 60 minutes. The minimum value is 15 minutes. The maximum value is 120 minutes.

Note If the Logout idle user check box is unselected, the user session does not time out.

Alarms

- Refresh Map/Alarms page on new alarm—Select the check box to refresh map and alarm pages each time a new alarm is generated.
- Refresh Alarm count in the Alarm Summary every—Choose the frequency of the Alarm Summary refresh from the drop-down list (every 5, seconds, 15 seconds, 30 seconds, 1 minute, 2 minutes, or 5 minutes).
- Display Alarm Category in Alarm Summary page—Choose the alarm category that you want to display in the minimized Alarm Summary (Alarm Summary, Malicious AP, Unclassified AP, Coverage Holes, Security, Controllers, Access Points, Mobility Services, Mesh Links, NCS, or Performance).

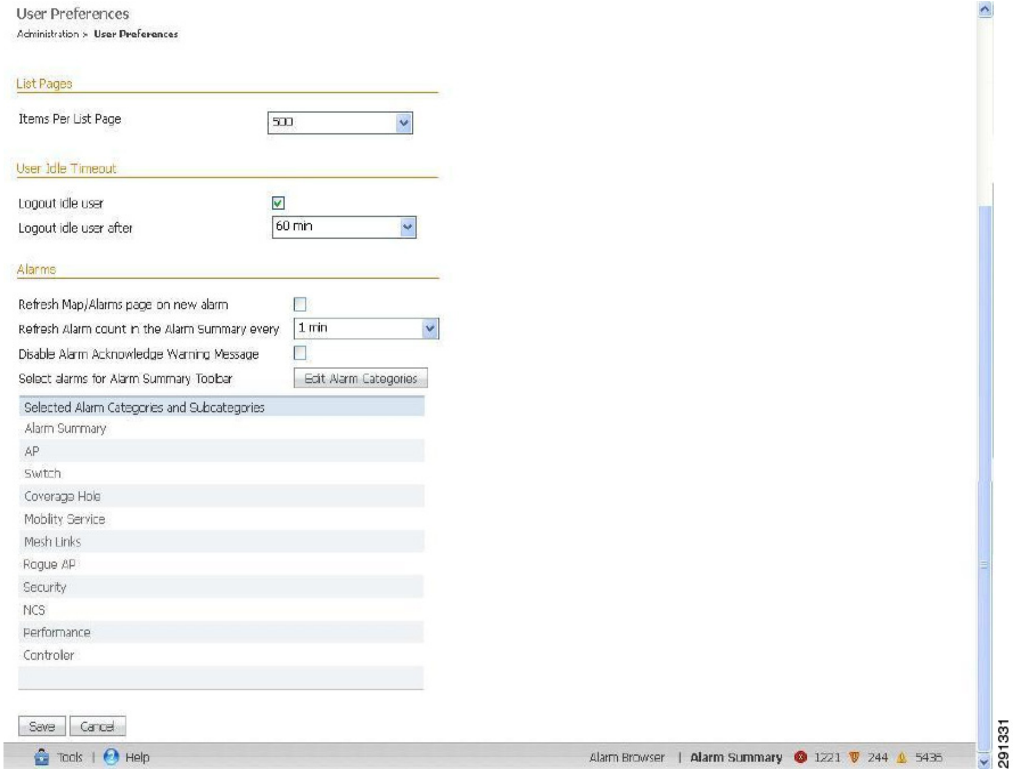
- Disable Alarm Acknowledge Warning Message—When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Select this check box to stop the warning message from displaying.
- Select alarms for Alarm Summary Toolbar—To select alarms for the Alarm Summary Toolbar, click **Edit Alarm Categories** and choose the required alarm categories and subcategories.

This page contains user-specific settings you might want to adjust.

To change the user-specific settings, follow these steps:

Step 1 Choose **Administration > User Preferences**. The User Preferences Page appears (see Figure 15-24).

Figure 15-24 User Preferences Page



User Preferences
Administration > User Preferences

List Pages
Items Per List Page: 500

User Idle Timeout
Logout idle user: ☑
Logout idle user after: 60 min

Alarms
Refresh Map/Alarms page on new alarm: □
Refresh Alarm count in the Alarm Summary every: 1 min
Disable Alarm Acknowledge Warning Message: □
Select alarms for Alarm Summary Toolbar: Edit Alarm Categories

Selected Alarm Categories and Subcategories
Alarm Summary
AP
Switch
Coverage Hole
Mobility Service
Mesh Links
Rogue AP
Security
NCS
Performance
Controller

Step 2 Use the Items Per List Page drop-down list to configure the number of entries shown on a given list page (such as alarms, events, AP list, and so on).

Step 3 Specify how often you want the home page refreshed by selecting the **Refresh home page** check box and choosing a time interval from the Refresh home page every drop-down list.

Step 4 Select the **Logout idle user** check box and configure the Logout idle user after text box, in minutes, that a user session can be idle before the server cancels the session.

Step 5 If you want the maps and alarms page to automatically refresh when a new alarm is raised by the NCS, select the **Refresh Map/Alarms page on new alarm** check box in the Alarms portion of the page.

Step 6 From the Refresh Alarm count in the Alarm Summary every drop-down list choose a time interval to to specify how often to reset.

Step 7 If you do not want the alarm acknowledge warning message to appear, select the **Disable Alarm Acknowledge Warning Message** check box.

Step 8 Click **Edit Alarm Categories** to select the alarm categories to display in the Alarm Summary page.

Step 9 In the Select Alarms page, choose the default category to display from the drop-down list, and select the alarm categories and sub categories to display from the alarm toolbar. Click **Save** to save the alarm category list. The selected alarm category and sub categories appears in the User Preferences page.

Step 10 Click **Save** to save the User Preference settings.

Viewing Appliance Details

This section provides the Appliance details. This section contains the following topics:

- Viewing Appliance Status Details, page 15-84
- Viewing Appliance Interface Details, page 15-85

Viewing Appliance Status Details

To view the appliance status, perform the following steps:

Step 1 Choose **Administration > Appliance**.

Step 2 Choose **Appliance Status** from the left sidebar menu. The Appliance Status page appears (see Figure 15-25) with the following details, see Table 15-5 for more information.

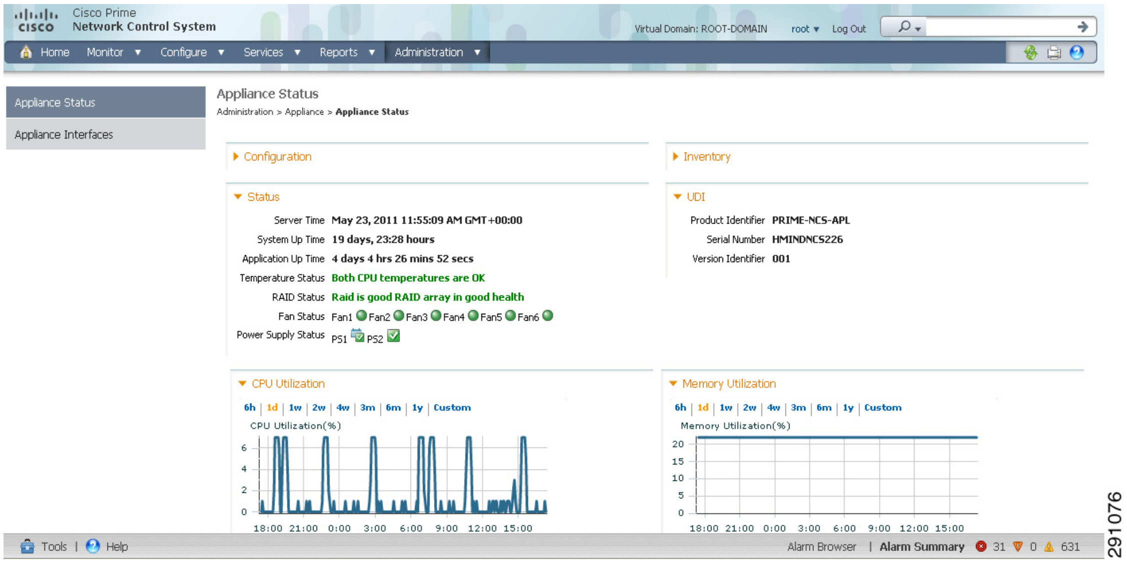
Table 15-5 Appliance Status Details

Field	Description
Configure Details	
Host Name	The hostname of the machine. If the hostname of the user machine is not in DNS, the IP address is displayed.
Domain Name	Domain Name of the server.
Default Gateway	IP address of the default gateway for the network environment in which you belong.
DNS Server(s)	Enter the IP address of the DNS server(s). Each DNS server must be able to update a client DNS entry to match the IP address assigned by this DHCP scope.
NTP Host(s)	Enter the IP address of the NTP server(s).
Status Details	
Server Time	The System time of the server.
System Up Time	It is a measure of the time since the server has been up without any downtime.

Table 15-5 Appliance Status Details (continued)

Field	Description
Application Up Time	It is a measure of the time since the NCS has been up without any downtime.
Temperature Status	The temperature status of the server.
RAID Status	The RAID status of the server.
Fan Status	The status of the cooler fans of the server.
Power Supply Status	The status of the power supply units of the server.
CPU Utilization	CPU Utilization of the server.
Memory Utilization	Memory Utilization of the server.
Inventory Details	Detailed inventory report.
UDI Details	
Product Identifier	The Product ID identifies the type of device.
Serial Number	The Serial Number is an 11 digit number which uniquely identifies a device.
Version Identifier	The VID is the version of the product. Whenever a product has been revised, the VID is incremented.

Figure 15-25 Appliance Status Page



Appliance Status

Administration > Appliance > **Appliance Status**

Server Time	May 23, 2011 11:55:09 AM GMT+00:00
System Up Time	19 days, 23:28 hours
Application Up Time	4 days 4 hrs 26 mins 52 secs
Temperature Status	Both CPU temperatures are OK
RAID Status	Raid is good RAID array in good health
Fan Status	Fan1 ● Fan2 ● Fan3 ● Fan4 ● Fan5 ● Fan6 ●
Power Supply Status	PS1 ✓ PS2 ✓

Product Identifier	PRIME-NCS-APL
Serial Number	HMINDNCS226
Version Identifier	001

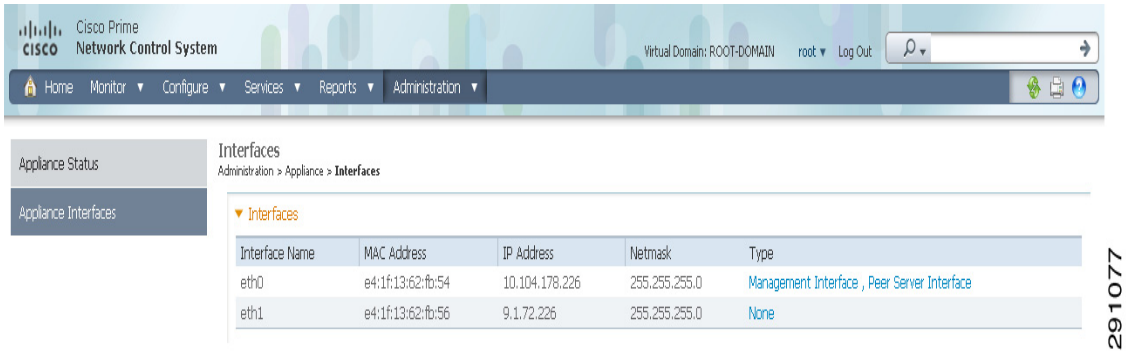
Viewing Appliance Interface Details

To view the Appliance Interface details, follow these steps:

Step 1 Choose **Administration > Appliance**.

Step 2 Choose **Appliance Interface** from the left sidebar menu. The Interfaces page appears (see Figure 15-26).

Figure 15-26 Appliance Interface Details



Interface Name	MAC Address	IP Address	Netmask	Type
eth0	e4:1f:13:62:fb:54	10.104.178.226	255.255.255.0	Management Interface , Peer Server Interface
eth1	e4:1f:13:62:fb:56	9.1.72.226	255.255.255.0	None

Table 15-6 Appliance Interface Details

Field	Description
Interface Name	User-defined name for this interface.
MAC Address	MAC address of the interface.
IP Address	Local network IP address of the interface.
Netmask	A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
Type	Static (Management, Peer, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).

Step 3 Click the **Interface Type** to configure if the interface belongs to peer server or to the management interfaces.

Configuring AAA

This section contains the following topics:

- Configuring AAA in the NCS, page 15-103
- Configuring ACS 4.x, page 15-103
- Configuring ACS 5.x, page 15-113

Configuring AAA Using the NCS

From Administration > AAA, authentication, authorization, and accounting (AAA) can be configured for the NCS. The only username that has permissions to configure NCS AAA is *root* or SuperUser. Any changes to local users accounts are in effect when configured for local mode. If using external authentication, for example RADIUS or TACACS+, the user changes must be done on the remote server.

This section contains the following topics:

Changing Password

Choose **Administration > AAA > Change Password** from the left sidebar menu to access this page.

This page enables you to change the password for current logged in User.

- User—Applies to the logged in User.
- Old Password—Current password.
- New Password—Enter the new password using ASCII characters.
- Confirm password—Reenter the new password.
- Submit—Click **Submit** to confirm password change.

Configuring AAA Mode

Choose **Administration > AAA** > **AAA Mode** from the left sidebar menu to access this page.

This page enables you to configure the authentication mode for all users.

- AAA Mode Settings
  - Local—Authenticate users to a local database.
  - RADIUS—Authenticate users to an external RADIUS server.
  - TACACS+—Authenticate users to an external TACACS+ server.
- Enable fallback to Local—If an external authentication server is down, this provides the option to authenticate users locally. This check box is only available for RADIUS and TACACS+.
  - Choose **ONLY on no server response** or **on auth failure or no server response** from the drop-down list.

See also the "Configuring TACACS+ Servers" section on page 15-95 and the "Configuring RADIUS Servers" section on page 15-98.

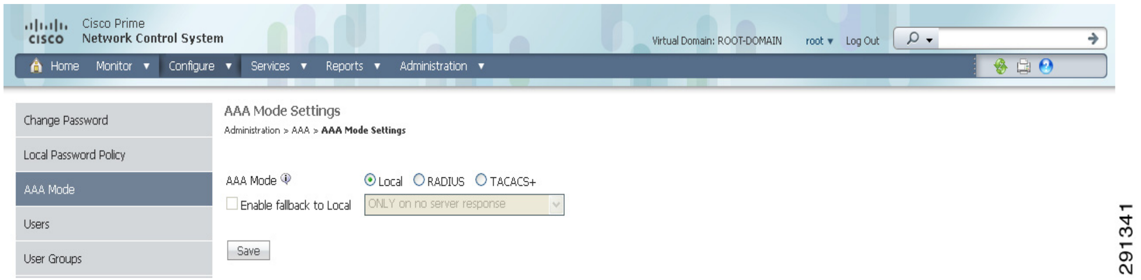
AAA Mode Settings

To choose a AAA mode, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 Choose **AAA Mode** from the left sidebar menu. The AAA Mode Settings page appears (see Figure 15-27).

Figure 15-27 AAA Mode Settings Page



AAA Mode Settings

Administration > AAA > **AAA Mode Settings**

AAA Mode ● Local ○ RADIUS ○ TACACS+

□ Enable fallback to Local ONLY on no server response

Step 3 Choose which AAA mode you want to use. Only one can be selected at a time.

Any changes to local user accounts are effective only when you are configured for local mode (the default). If you use remote authentication, changes to the credentials are made on a remote server. The two remote authentication types are RADIUS and TACACS+. RADIUS requires separate credentials for different locations (East and West Coast). TACACS+ is an effective and secure management framework with a built-in failover mechanism.

Step 4 Select the **Enable Fallback to Local** check box if you want the administrator to use the local database when the external AAA server is down.

> **Note** This check box is unavailable if *Local* was selected as a AAA mode type.

Step 5 Click **OK**.

Configuring Local Password Policy

Choose **Administration > AAA > Local Password Policy** from the left sidebar menu to access this page.This page enables you to determine your local password policy.

You can enable or disable the following policies for your local password:

- Set the minimum length of your password. By default it is set as 8.
- Password cannot be the username or the reverse of the username.
- Password cannot be the word cisco or ocsic (cisco reversed) or any special characters replaced for the same.

- Root password cannot be the word public.
- No character can be repeated more than three time consecutively in the password.
- Password must contain character from three of the character classes: upper case, lower case, digits, and special characters.

Click **Save** to confirm the Local Password Policy changes.

Configuring Users

This section describes how to configure an NCS user. Besides complete access, you can give administrative access with differentiated privileges to certain user groups.

Choose **Administration > AAA > Users** from the left sidebar menu to access this page. You can use this page to view the User details, create a User, delete a User as well as edit User details.

This section contains the following topics:

- Viewing User Details, page 15-89
- Edit Current Users - Passwords and Assigned Groups, page 15-89
- Edit Current Users - Permitted Tasks, page 15-90
- Edit Current Users - Groups Assigned to this User, page 15-90
- Adding a New User, page 15-91
- Add User Name, Password, and Groups, page 15-91
- Assign a Virtual Domain, page 15-92
- Audit User Operations, page 15-92

Viewing User Details

You can view the NCS user details in the Users page. The following information is available in the Administration > AAA > Users page:

- Current User Names
- Member Of—Groups with which the user is associated. Click an item in the Member Of column to view permitted tasks for this user.
- Audit Trail—Click the Audit Trail icon for a specific user to view or clear current audit trails. See the "Audit User Operations" section on page 15-92.

Note The NCS supports a maximum of 25 concurrent User logins at any point in time.

Edit Current Users - Passwords and Assigned Groups

To edit current user account passwords and assigned groups, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Select a specific user from the User Name column.

Step 4 (Optional) Enter and confirm a new password, if necessary.

Step 5 If necessary, make changes to the Groups Assigned to this User check box selections.

Note If the user belongs to Lobby Ambassador, Monitor Lite, North Bound API, or User Assistant group, the user cannot belong to any other group.

Step 6 Select **Submit** to confirm the changes or **Cancel** to close the page without activating any changes.

Edit Current Users - Permitted Tasks

To edit the permitted tasks for this user account, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Select the applicable group(s) from the Member Of column.

Step 4 From the List of Tasks Permitted column, select or deselect the applicable tasks to permit or disallow them.

Note The list of available tasks changes depending on the type of group.

Step 5 Select **Submit** to confirm the changes or **Cancel** to close the page without activating any changes.

Edit Current Users - Groups Assigned to this User

To edit the groups assigned to this user, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Select a specific user from the User Name column.

Step 4 Select the check box(es) of the groups to which this user is assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, North Bound API, or User Assistant group, the user cannot belong to any other group.
Root is only assignable to 'root' user and that assignment cannot be changed.

Note For more information on assigned groups, see Step 7 in the "Adding a New User" section on page 15-91 section.

Step 5 Select **Submit** to confirm the changes or **Cancel** to close the page without activating any changes.

Adding a New User

The Add User page allows the administrator to set up a new user login including username, password, groups assigned to the user, and virtual domains for the user. For more information on assigning virtual domains, see the "Assign a Virtual Domain" section on page 15-92.

Note By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note You must have SuperUser status to access this page.

Add User Name, Password, and Groups

To add a new user, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 From the Select a command drop-down list, choose **Add User**.

Step 4 Click **Go**.

Step 5 Enter a new username.

Step 6 Enter and confirm a password for this account.

Step 7 Select the check box(es) of the groups to which this user is assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, North Bound API, or User Assistant group, the user cannot belong to any other group.

- Admin—Allows users to monitor and configure NCS operations and perform all system administration tasks except administering NCS user accounts and passwords.
- Config Managers—Allows users to monitor and configure NCS operations.
- Lobby Ambassador—Allows guest access for configuration and management only of user accounts. If Lobby Ambassador is selected, a Lobby Ambassador Defaults tab appears. See the "Managing Lobby Ambassador Accounts" section on page 7-17 for more information on setting up a Lobby Ambassador account.
- Monitor Lite—Allows monitoring of assets location.
- North Bound API User—Group used only with NCS Web Service consumers.

Note North Bound API Users cannot be assigned a virtual domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Note You can add a North Bound API User only if you are logged into the ROOT-DOMAIN.

- Root—This group is only assignable to 'root' user and that assignment cannot be changed.

- Super Users—Allows users to monitor and configure NCS operations and perform all system administration tasks including administering NCS user accounts and passwords. Superuser tasks can be changed.
- System Monitoring—Allows users to monitor NCS operations.
- User Assistant—Allows local net user administration only.
- User Defined.

Assign a Virtual Domain

To assign a virtual domain to this user, follow these steps:

Step 1 Select the **Virtual Domains** tab. This page displays all virtual domains available and assigned to this user.

Note The Virtual Domains tab enables the administrator to assign virtual domains for each user. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note North Bound API Users cannot be assigned a virtual domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Step 2 Click to highlight the virtual domain in the Available Virtual Domains list that you want to assign to this user.

Note You can select more than one virtual domain by pressing the Shift or Control key.

Step 3 Click **Add**. The virtual domain moves from the Available Virtual Domains to the Selected Virtual Domains list.

To remove a virtual domain from the Selected Virtual Domains list, click to highlight the domain in the Selected Virtual Domains list and click **Remove**. The virtual domain moves from the Selected Virtual Domains to the Available Virtual Domains list.

Step 4 Select **Submit** or **Cancel** to close the page without adding or editing the current user.

Audit User Operations

To view or clear audit information for this account, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Click the **Audit Trail** icon for the applicable account.

Note You must have SuperUser status to access this page.

This page enables you to view a list of user operations over time.

- User—User login name.
- Operation—Type of operation audited.
- Time—Time operation was audited.
- Status—Success or Failure.
- Reason—Reason is applicable only for failure.
- Configuration Changes—This field provides a Details link if there are any configuration changes. Click the Details link for more information on the configuration changes done by an individual user. The entries list out the change of values for individual parameters between the NCS and controller. For more information on Audit Trail Details, see the "Audit Trail Details Page" section on page 7-10.

Step 4 To clear an audit trail, select the check box for the applicable audit, select Clear Audit Trail from the Select a command drop-down list, click **Go**, and click **OK** to confirm.

Configuring Groups

This page provides you with a list of all current groups and their associated members.

- Group Name—Click a specific group to view or edit the permitted tasks for this group. The available tasks change depending on the type of group. See the "Edit Current Users - Permitted Tasks" section on page 15-90 for more information.
- Members—Click a specific user under the Member column to view or edit that user. See the "Edit Current Users - Passwords and Assigned Groups" section on page 15-89 for more information.
- Audit Trail—Click the Audit Trail icon to view or clear audit for this group. See the "Audit User Operations" section on page 15-92 for more information.
- Export—Click to export the task list associated with this group.

To access the Groups page, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **User Group**.

Note You must have SuperUser status to access this page.

Viewing or Editing User Group Information

To see specific tasks the user is permitted to do within the defined group or make changes to the tasks, follow these steps:

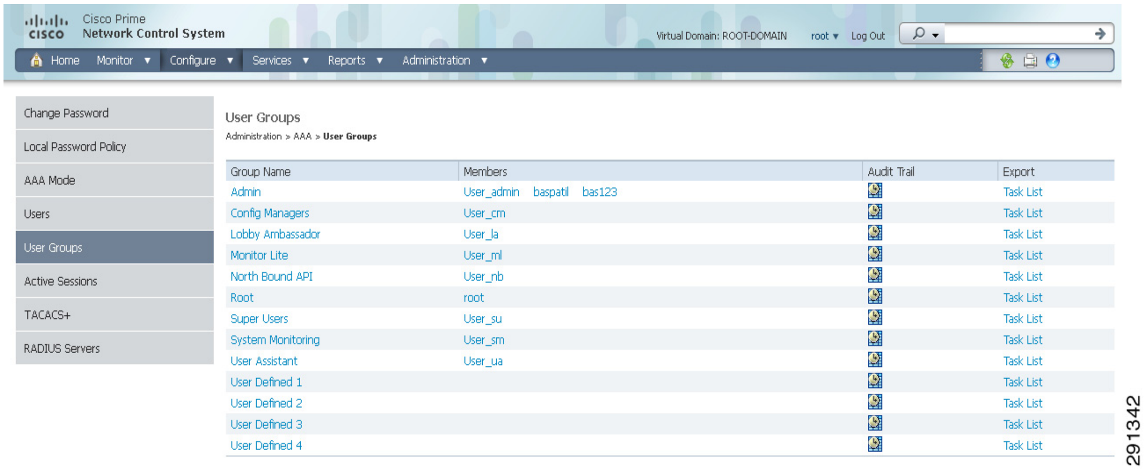
Step 1 Choose **Administration > AAA**.

Step 2 Choose **User Groups** from the left sidebar menu.

Step 3 Click in the **Group Name** column. The Group Detail: *User Group* page appears (see Figure 15-28).

Note The detailed page varies based on what group you choose. Figure 15-28 shows the detailed page of the superuser.

Figure 15-28 Detailed User Groups Page



User Groups

Administration > AAA > **User Groups**

Group Name	Members	Audit Trail	Export
Admin	User_admin baspatil bas123	▣	Task List
Config Managers	User_cm	▣	Task List
Lobby Ambassador	User_la	▣	Task List
Monitor Lite	User_ml	▣	Task List
North Bound API	User_nb	▣	Task List
Root	root	▣	Task List
Super Users	User_su	▣	Task List
System Monitoring	User_sm	▣	Task List
User Assistant	User_ua	▣	Task List
User Defined 1		▣	Task List
User Defined 2		▣	Task List
User Defined 3		▣	Task List
User Defined 4		▣	Task List

You can see the specific tasks the user is permitted to do within the defined group.

Step 4 Click Audit Trail to view the audit trail information for the corresponding User group. For more information on Audit Trail Details, see the "Audit Trail Details Page" section on page 7-10.

Step 5 Make any necessary changes to the tasks.

Table 15-7 Default User Groups

User Group	Description
Admin	Group for NCS Administration.
Config Managers	Group for monitoring and configuration tasks.
Lobby Ambassador	Group to allow Guest user administration only. This Group is not editable.
Monitor Lite	Group to allow monitoring of assets only. Group is not editable.
North Bound API	Group to allow access to North Bound APIs. Group is not editable.
Root	Group for root user. Group is not editable.
Super Users	Group to allow all NCS tasks.
System Monitoring	Group for monitoring only tasks.
User Assistant	Group to allow Local Net user administration only. Group is not editable.
User-Defined 1	User definable group.
User-Defined 2	User definable group.
User-Defined 3	User definable group.
User-Defined 4	User definable group.

Step 6 Click **Submit**.

Viewing Active Sessions

Choose **Administration > AAA > Active Sessions** from the left sidebar menu to open this page.

This page displays a list of users currently logged in. The user highlighted in red represents your current login.

Note You must be logged into a user account with SuperUsers privileges to see active sessions.

If a column heading is a hyperlink, click the heading to sort the list of active sessions in descending or ascending order along that column. The sort direction is toggled each time the hyperlink is clicked.

The Active Sessions page has the following columns:

- Username—The User ID of the User who is logged in.
- IP/Host Name—The IP address or the hostname of the machine on which the browser is running. If the hostname of the user machine is not in DNS, the IP address is displayed.
- Login Time—The time at which the user logged in to the NCS. All times are based on the NCS server machine time.
- Last Access Time—The time at which the user browser accessed the NCS. All times are based on the NCS server machine time.

  Note The time displayed in this column is usually a few seconds behind the current system time because Last Access Time is updated frequently by the updates to the alarm status panel. However, if a user navigates to a non-NCS web page in the same browser, the disparity in time is greater. Alarm counts are not updated when the browser is not displaying NCS web pages.

- Login Method—The login method can be any of the following:
  - Local
  - Radius
  - TACACS+
- User Groups—The list of groups the user belongs to.
- Audit trail icon—Link to page that displays the audit trail (previous login times) for that user.

Configuring TACACS+ Servers

This section describes how to add and delete TACACS+ servers. TACACS+ servers provide an effective and secure management framework with built-in failover mechanisms. If you want to make configuration changes, you must be authenticated.

The TACACS+ page shows the IP address, port, retransmit rate, and authentication type (Password Authentication Protocol (PAP)) or Challenge Handshake Authentication Protocol (CHAP) of the TACACS+ server. The TACACS+ servers are tried based on how they were configured.

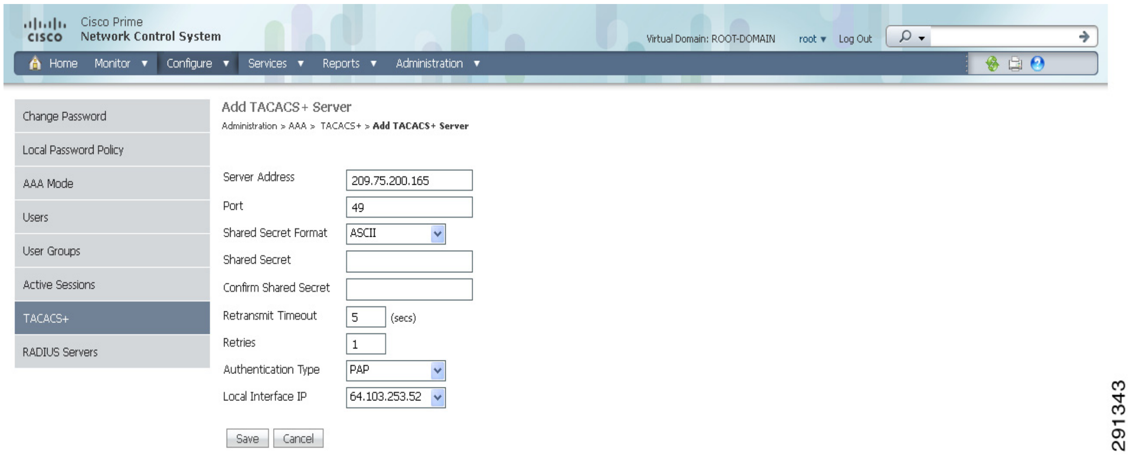
Note To activate TACACS+ servers, you must enable them as described in the "Configuring ACS 4.x" section on page 15-103.

To configure TACACS+, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **TACACS+**. The TACACS+ page appears (see Figure 15-29).

Figure 15-29 TACACS+ Page



Add TACACS+ Server

Administration > AAA > TACACS+ > **Add TACACS+ Server**

Server Address	209.75.200.165
Port	49
Shared Secret Format	ASCII
Shared Secret	
Confirm Shared Secret	
Retransmit Timeout	5 (secs)
Retries	1
Authentication Type	PAP
Local Interface IP	64.103.253.52

Step 3 The TACACS+ page shows the IP address, port, retransmit rate, and authentication type (Password Authentication Protocol (PAP)) or Challenge Handshake Authentication Protocol (CHAP) TACACS+ server. The TACACS+ servers are tried based on how they were configured.

Note If you need to change the order of how TACACS+ servers are tried, delete any irrelevant TACACS+ servers and readd the desired ones in the preferred order.

Step 4 Use the drop-down list in the upper right-hand corner to add or delete TACACS+ servers. You can click an IP address if you want to make changes to the information.

Step 5 The current server address and port are displayed. Use the drop-down list to choose either ASCII or hex shared secret format.

Step 6 Enter the TACACS+ shared secret used by your specified server.

Step 7 Reenter the shared secret in the Confirm Shared Secret text box.

Step 8 Specify the time in seconds after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Step 9 Specify the number of retries that are attempted.

Step 10 In the Authentication Type drop-down list, choose PAP or CHAP protocol.

Step 11 In the Local Interface IP drop-down list, choose an IP address for the interface.

This interface IP address is the same that you specify in the ACS Server for TACACS+.

Step 12 Click **Submit**.

Note The RADIUS/TACACS server IP address and other credentials created in the 7.0.x releases are not migrated to NCS 1.0. You need to add them again after the migration from 7.0.x to NCS 1.0 is complete.

Note See the "Configuring ACS 5.x" section on page 15-113 for more information on Configuring ACS 5.x.

Select a command

- Add TACACS+ Server—See the "Add TACACS+ Server" section on page 15-97.
- Delete TACACS+ Server—Select a server or servers to be deleted, select this command, and click **Go** to delete the server(s) from the database.

Add TACACS+ Server

Choose **Administration > AAA** > **TACACS+** from the left sidebar menu to access this page. From the Select a command drop-down list choose **Add TACACS+ Server**, and click **Go** to access this page.

This page allows you to add a new TACACS+ server to the NCS.

- Server Address—IP address of the TACACS+ server being added.
- Port—Controller port.
- Shared Secret Format—ASCII or Hex.
- Shared Secret—The shared secret that acts as a password to log in to the TACACS+ server.
- Confirm Shared Secret—Reenter TACACS+ server shared secret.
- Retransmit Timeout—Specify retransmission timeout value for a TACACS+ authentication request.
- Retries—Number of retries allowed for authentication request. You can specify a value between 1 and 9.
- Authentication Type—Two authentication protocols are provided. Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Command Buttons

- Submit
- Cancel

Note

- Enable the TACACS+ server with the AAA Mode Settings. See the "Configuring AAA Mode" section on page 15-87.
- You can add only three servers at a time in the NCS.

Configuring RADIUS Servers

This section describes how to add and delete RADIUS servers. You must enable RADIUS servers and have a template set up for them to make configuration changes.

RADIUS provides authentication of users accessing the network. Authentication requests are sent to a RADIUS server that contains all user authentication and network access information. Passwords are encrypted using RADIUS.

In the event the configured RADIUS server(s) is down, NCS falls back to local authentication and authorization if the fallback to local option is configured. See the "Configuring AAA Mode" section on page 15-87.

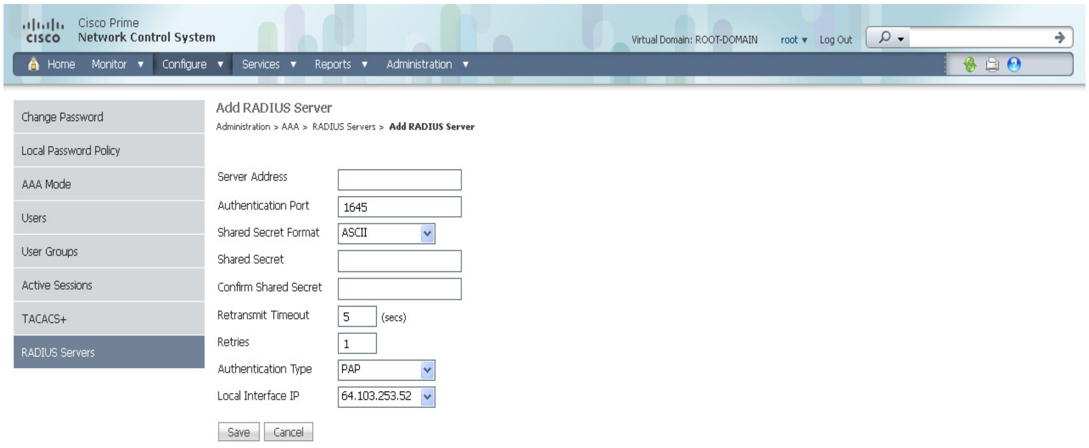
Note To activate RADIUS servers, you must enable them as described in the "Configuring ACS 4.x" section on page 15-103.

To configure a RADIUS server, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **RADIUS**. The RADIUS page appears (see Figure 15-30).

Figure 15-30 RADIUS Page



Add RADIUS Server

Administration > AAA > RADIUS Servers > **Add RADIUS Server**

Server Address	
Authentication Port	1645
Shared Secret Format	ASCII
Shared Secret	
Confirm Shared Secret	
Retransmit Timeout	5 (secs)
Retries	1
Authentication Type	PAP
Local Interface IP	64.103.253.52

Step 3 The RADIUS page shows the server address, authentication port, retransmit timeout value, and authentication type for each RADIUS server that is configured. The RADIUS servers are tried based on how they were configured.

Note If you need to change the order of how RADIUS servers are tried, delete any irrelevant RADIUS servers, and readd the desired ones in the preferred order.

Step 4 Use the drop-down list in the upper right-hand corner to add or delete RADIUS servers. You can click an IP address if you want to make changes to the information.

Step 5 The current authentication port appears. Use the drop-down list to choose either ASCII or hex shared secret format.

Step 6 Enter the RADIUS shared secret used by your specified server.

Step 7 Reenter the shared secret in the Confirm Shared Secret text box.

Step 8 Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller.

Step 9 Specify the number of retries that are attempted.

Step 10 From the Authentication Type drop-down list, choose PAP or CHAP protocol.

Step 11 In the Local Interface IP drop-down list, choose an IP address for the interface.

This interface IP address is the same that you specify in the ACS Server for RADIUS.

Step 12 Click **Submit**.

Select a command

- Add RADIUS Server—See the "Adding RADIUS Server" section on page 15-99.
- Delete RADIUS Server—Select a server or servers to be deleted, select this command, and click **Go** to delete the server(s) from the database.

Adding RADIUS Server

Choose **Administration > AAA > RADIUS** from the left sidebar menu to access this page. From the Select a command drop-down list choose **Add RADIUS Server**, and click **Go** to access this page.

This page allows you to add a new RADIUS server to the NCS.

- Server Address—IP address of the RADIUS server being added.
- Port—Controller port.
- Shared Secret Format—ASCII or Hex.
- Shared Secret—The shared secret that acts as a password to log in to the RADIUS server.
- Confirm Shared Secret—Reenter the RADIUS server shared secret.
- Retransmit Timeout—Specify the retransmission timeout value for a RADIUS authentication request.
- Retries—Number of retries allowed for authentication request. You can specify a value between 1 to 9.

Command Buttons

- Submit
- Cancel

Note

- Enable the RADIUS server with the AAA Mode Settings. See the "Configuring AAA Mode" section on page 15-87.
- You can add only three servers at a time in the NCS.

Authenticating AAA Users Through RADIUS Using Cisco Identity Services Engine (ISE)

You can integrate an NCS with ISE. This section explains the NCS user authentication through Radius protocol using ISE.

This authentication helps you in setting up Users in ISE who are configured locally and not from external sources such as Active Directory and LDAP.

Note Only RADIUS server authentication is supported in ISE.

To authenticate AAA through RADIUS server using ISE, following steps:

Step 1 Add the NCS as a AAA client in ISE. For more information, see the "Adding the NCS as a AAA client in ISE" section on page 15-100.

Step 2 Create a new User group in ISE. For more information, see the "Creating a New User Group in ISE" section on page 15-101.

Step 3 Create a new User in ISE and add that User to the User group created in ISE. For more information, see the "Creating a New User and Adding to a User Group in ISE" section on page 15-101.

Step 4 Create a new Authorization profile. For more information, see the "Creating a New Authorization Profile in ISE" section on page 15-101.

Step 5 Create an Authorization policy rule. For more information, see the "Creating an Authorization Policy Rule in ISE" section on page 15-102.

Step 6 Configure AAA in the NCS. For more information, see the "Configuring AAA in the NCS" section on page 15-103.

Adding the NCS as a AAA client in ISE

To add NCS as a AAA client in ISE, follow these steps:

Step 1 Log in to ISE.

Step 2 Choose **Administration** > **Network Devices**.

Step 3 From the left sidebar menu, click the arrow next to Network Devices to expand that option.

The expanded list shows the already added devices.

Step 4 Click any device to view its details.

Step 5 From the left sidebar menu, click the arrow next to the ⚙▾ icon, and choose the **Add new device** option.

Step 6 In the right pane, enter the following details for the device you want to add:

- Name—Name of the device.
- Description—Device description.
- IP Address—NCS server IP address. For example, enter `209.165.200.225`.

Step 7 Enter the Shared key in the Shared Secret text box.

Click **Save** to add the device.

Creating a New User Group in ISE

You can create a new user group in ISE. This helps you to classify different privileged NCS users and also create authorization policy rules on user groups.

To create a new user group in ISE, follow these steps:

Step 1 Choose **ISE** > **Administration** > **Groups**.

Step 2 From the left sidebar menu, choose **User Identity Groups**.

The User Identity Groups page appears in the right pane.

Step 3 Click **Add**.

The Identity Group details page appears.

Step 4 Enter the name and description for the group.

For example, create a user group *NCS-SystemMonitoring-Group*.

Step 5 Click **Save**.

Creating a New User and Adding to a User Group in ISE

You can create a new user in ISE and map that user to a user group.

To create a new user and map that user to a user group in ISE, follow these steps:

Step 1 Choose **ISE** > **Administration** > **Identity Management** > **Identities**.

Step 2 From the left sidebar menu, choose **Identities** > **Users**.

The Network Access Users page appears in the right pane.

Step 3 Click **Add**.

The Network Access User page appears.

Step 4 Enter the Username, password and reenter password for the user.

For example, create a User *ncs-sysmon*.

Step 5 Choose the required user group from the **User Group** drop-down list, and click **Save**.

The new user is added to the required user group.

Note You can also integrate ISE with external sources such as Active Directory and LDAP.

Creating a New Authorization Profile in ISE

You can create authorization profiles in ISE. To create a new authorization profile, follow these steps:

Step 1 Choose **ISE** > **Policy** > **Policy Elements** > **Results**.

Step 2 From the left sidebar menu, choose **Authorization** > **Authorization Profiles**.

The Standard Authorization Profiles page appears in the right pane.

Step 3 Click **Add**.

The details page appears.

Step 4 Enter the name and description for the profile.

For example, create an authorization profile named *NCS-SystemMonitor*.

Step 5 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.

Step 6 In the Advanced Attribute Settings group box, add the NCS User Group Radius Custom attributes one after another along with virtual domain attributes at the end. Select **cisco - av - pair** and paste the NCS User Group Radius custom attribute next to it. Keep adding one after another. Repeat the same step for virtual domain attributes as well.

Step 7 Save the authorization profile.

Creating an Authorization Policy Rule in ISE

To create an authorization policy rule, follow these steps:

Step 1 Choose **ISE** > **Policy** > **Authorization**.

Step 2 From the Authorization Policy page, choose **Insert New Rule Above** from the Actions drop-down list.

Create a rule which would be used for NCS user login.

Step 3 Enter a name for the rule in the Rule Name text box.

Step 4 Choose the required identity group from the Identity Groups drop-down list.

For Example, choose **NCS-SystemMonitoring-Group**.

For more information on creating Identity User Groups, see the "Creating a New User Group in ISE" section on page 15-101.

Step 5 Choose a permission from the Permissions drop-down list. The permissions are the Authorization profiles.

For Example, choose **NCS-SystemMonitor authorization profile**.

For more information on creating authorization profiles, see the "Creating a New Authorization Profile in ISE" section on page 15-101.

In this example, we define a rule where all users belonging to the NCS System Monitoring Identity Group receive an appropriate authorization policy with system monitoring custom attributes defined.

Step 6 Click **Save** to save the authorization rule.

Note You can also monitor successful and failed authentication using the ISE > Monitor > Authentications option.

Configuring AAA in the NCS

To configure AAA in the NCS, follow these steps:

Step 1 Log in to NCS as *root*.

Step 2 Choose **NCS** > **Administration** > **AAA** > **RADIUS Servers**.

Step 3 Add a new RADIUS Server with the ISE IP address.

For example, enter **`209.165.200.230`**.

Step 4 Click **Save** to save the changes.

Step 5 Choose **ISE** > **Administration** > **AAA** > **AAA Mode Settings**.

The AAA Mode Settings page appears.

Step 6 Select **RADIUS** as the AAA mode.

Step 7 Click **Save**.

The AAA mode is set to RADIUS in the NCS.

Step 8 Log out of the NCS.

Step 9 Log in again to the NCS as a AAA user, defined in ISE.

For example, log in as user *ncs-sysmon*.

For more information on creating users in ISE, see the "Creating a New User and Adding to a User Group in ISE" section on page 15-101.

Configuring ACS 4.x

This section provides instructions for configuring ACS 4.x to work with the NCS.

To import tasks into Cisco Secure ACS server, you must add the NCS to an ACS server (or non-Cisco ACS server). This section contains the following topics:

- Adding the NCS to an ACS Server for Use with TACACS+ Server, page 15-103
- Adding NCS User Groups into ACS for TACACS+, page 15-105
- Adding the NCS to an ACS Server for Use with RADIUS, page 15-108
- Adding NCS User Groups into ACS for RADIUS, page 15-109
- Adding the NCS to a Non-Cisco ACS Server for Use with RADIUS, page 15-112

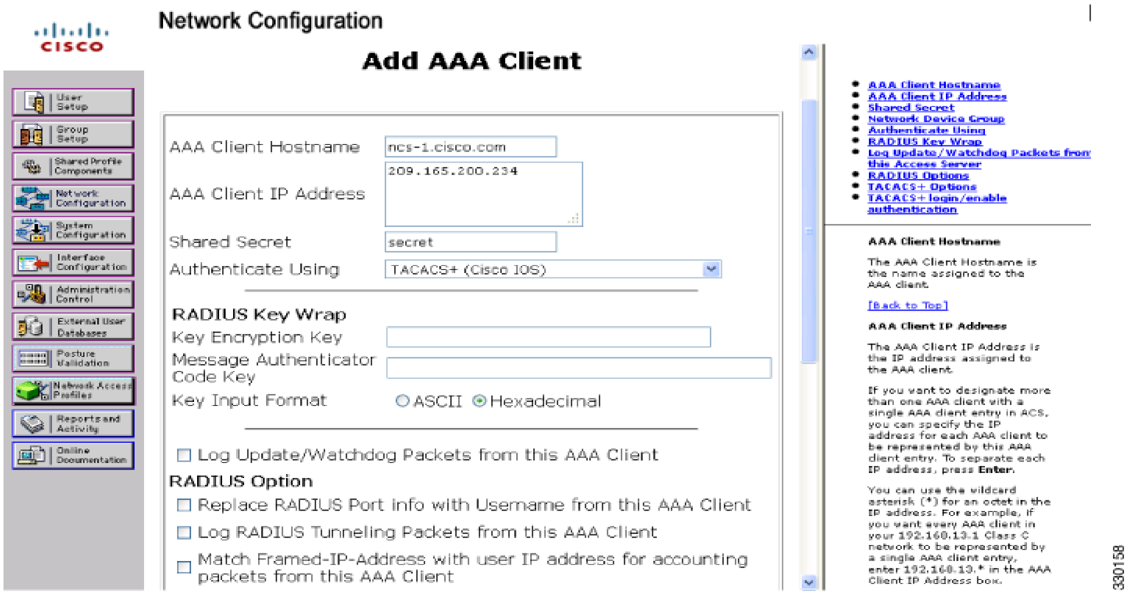
Adding the NCS to an ACS Server for Use with TACACS+ Server

To add the NCS to a TACACS+ server, follow these steps:

Note The instructions and illustrations in this section pertain to ACS Version 4.1 and might vary slightly for other versions or other vendor types. See the CiscoSecure ACS documentation or the documentation for the vendor you are using.

Step 1 Click **Add Entry** in the Network Configuration page of the ACS server (see Figure 15-32).

Figure 15-31 ACS Server Network Configuration Page



Network Configuration

Add AAA Client

AAA Client Hostname: ncs-1.cisco.com

AAA Client IP Address: 209.165.200.234

Shared Secret: secret

Authenticate Using: TACACS+ (Cisco IOS)

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ○ ASCII ● Hexadecimal

□ Log Update/Watchdog Packets from this AAA Client

RADIUS Option

□ Replace RADIUS Port info with Username from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

- AAA Client Hostname
- AAA Client IP Address
- Shared Secret
- Network Device Group
- Authenticate Using
- RADIUS Key Wrap
- Log Update/Watchdog Packets from this Access Server
- RADIUS Options
- TACACS+ Options
- TACACS+ login/enable authentication

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you vant to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the vildcard asterisk (*) for an octet in the IP address. For example, if you vant every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

Step 2 In the AAA Client Hostname text box, enter the NCS hostname.

Step 3 Enter the NCS IP address in the AAA Client IP Address text box.

Ensure the interface that you use for ACS is the same as that is specified in the NCS and it is reacheable.

Step 4 In the Shared Secret text box, enter the shared secret that you want to configure on both the NCS and ACS servers.

Step 5 Choose **TACACS+** in the Authenticate Using drop-down list.

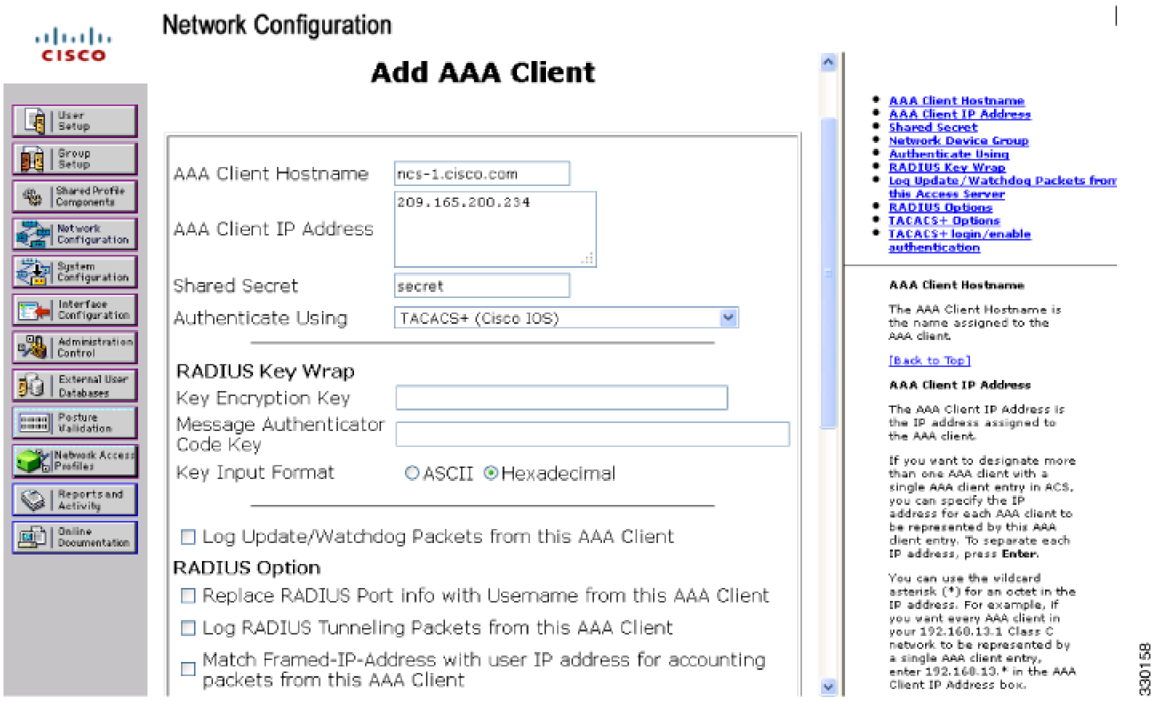
Step 6 Click **Submit + Apply**.

Step 7 From the left sidebar menu, choose **Interface Configuration**.

Step 8 In the Interface Configuration page, click the **TACACS+ (Cisco IOS)** link.

The TACACS+ (Cisco IOS) Interface Configuration page appears (see Figure 15-32).

Figure 15-32 ACS Server Network Configuration Page



Network Configuration

Add AAA Client

AAA Client Hostname: ncs-1.cisco.com

AAA Client IP Address: 209.165.200.234

Shared Secret: secret

Authenticate Using: TACACS+ (Cisco IOS)

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ○ ASCII ● Hexadecimal

□ Log Update/Watchdog Packets from this AAA Client

RADIUS Option

□ Replace RADIUS Port info with Username from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

- AAA Client Hostname
- AAA Client IP Address
- Shared Secret
- Network Device Group
- Authenticate Using
- RADIUS Key Wrap
- Log Update/Watchdog Packets from this Access Server
- RADIUS Options
- TACACS+ Options
- TACACS+ login/enable authentication

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

Step 9 In the New Services portion of the page, add **NCS** in the Service column heading.

Step 10 Enter **HTTP** in the Protocol column heading.

Note HTTP must be in uppercase.

Step 11 Select the check box in front of these entries to enable the new service and protocol.

Note The ACS 4.x configuration is complete only when you specify and enable the NCS service with HTTP protocol.

Step 12 Click **Submit**.

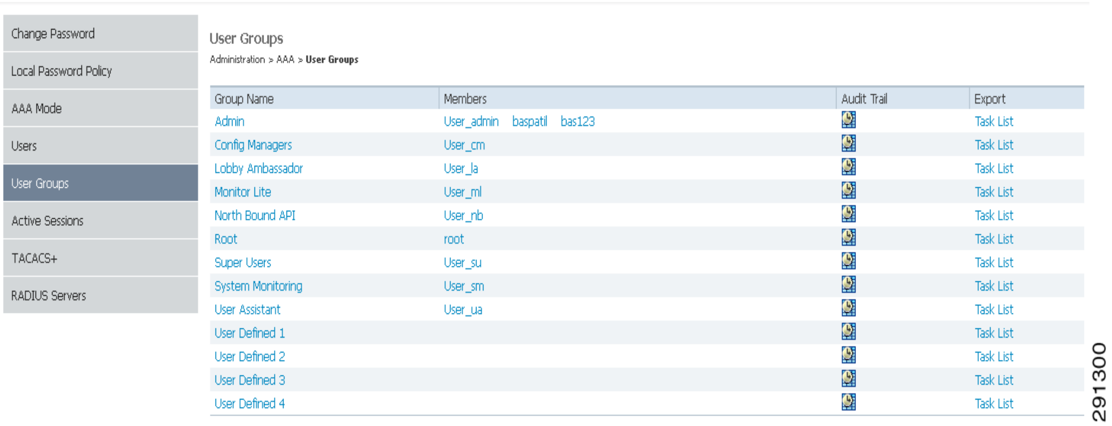
Adding NCS User Groups into ACS for TACACS+

To add NCS User Groups into an ACS Server for use with TACACS+ servers, follow these steps:

Step 1 Log in to the NCS.

Step 2 Choose **Administration > AAA > User Groups**. The User Groups page appears (see Figure 15-33).

Figure 15-33 User Groups Page



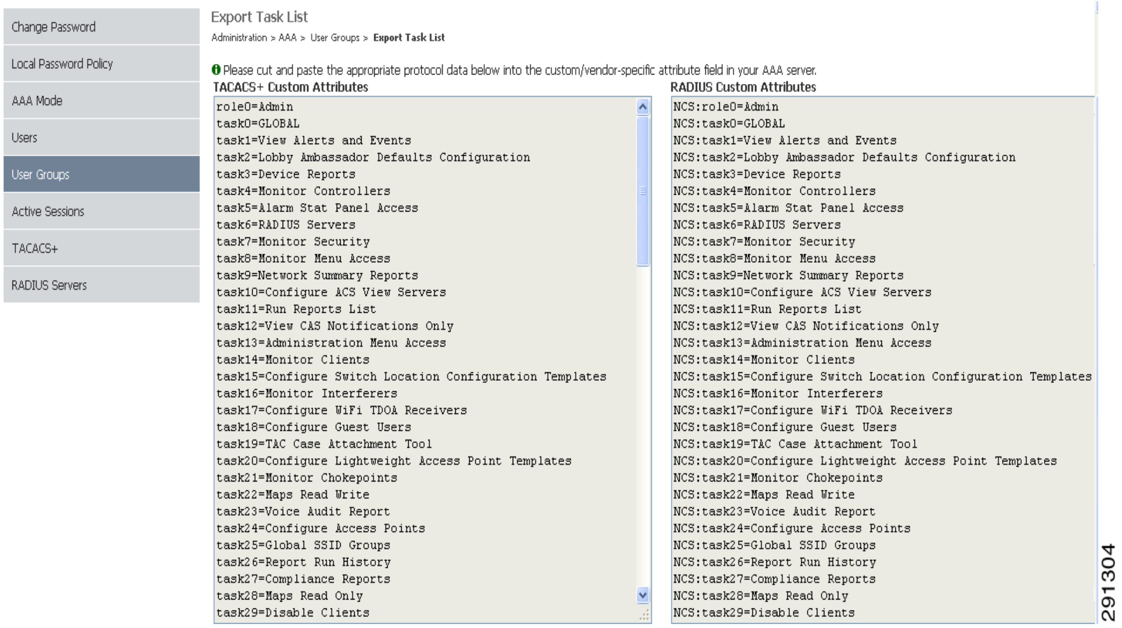
User Groups

Administration > AAA > **User Groups**

Group Name	Members	Audit Trail	Export
Admin	User_admin baspatil bas123		Task List
Config Managers	User_cm		Task List
Lobby Ambassador	User_la		Task List
Monitor Lite	User_ml		Task List
North Bound API	User_nb		Task List
Root	root		Task List
Super Users	User_su		Task List
System Monitoring	User_sm		Task List
User Assistant	User_ua		Task List
User Defined 1			Task List
User Defined 2			Task List
User Defined 3			Task List
User Defined 4			Task List

Step 3 Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears (see Figure 15-34).

Figure 15-34 Export Task List Page



Export Task List

Administration > AAA > User Groups > **Export Task List**

Please cut and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=GLOBAL
task1=View Alerts and Events
task2=Lobby Ambassador Defaults Configuration
task3=Device Reports
task4=Monitor Controllers
task5=Alarm Stat Panel Access
task6=RADIUS Servers
task7=Monitor Security
task8=Monitor Menu Access
task9=Network Summary Reports
task10=Configure ACS View Servers
task11=Run Reports List
task12=View CAS Notifications Only
task13=Administration Menu Access
task14=Monitor Clients
task15=Configure Switch Location Configuration Templates
task16=Monitor Interferers
task17=Configure WiFi TDOA Receivers
task18=Configure Guest Users
task19=TAC Case Attachment Tool
task20=Configure Lightweight Access Point Templates
task21=Monitor Chokepoints
task22=Maps Read Write
task23=Voice Audit Report
task24=Configure Access Points
task25=Global SSID Groups
task26=Report Run History
task27=Compliance Reports
task28=Maps Read Only
task29=Disable Clients
```

RADIUS Custom Attributes

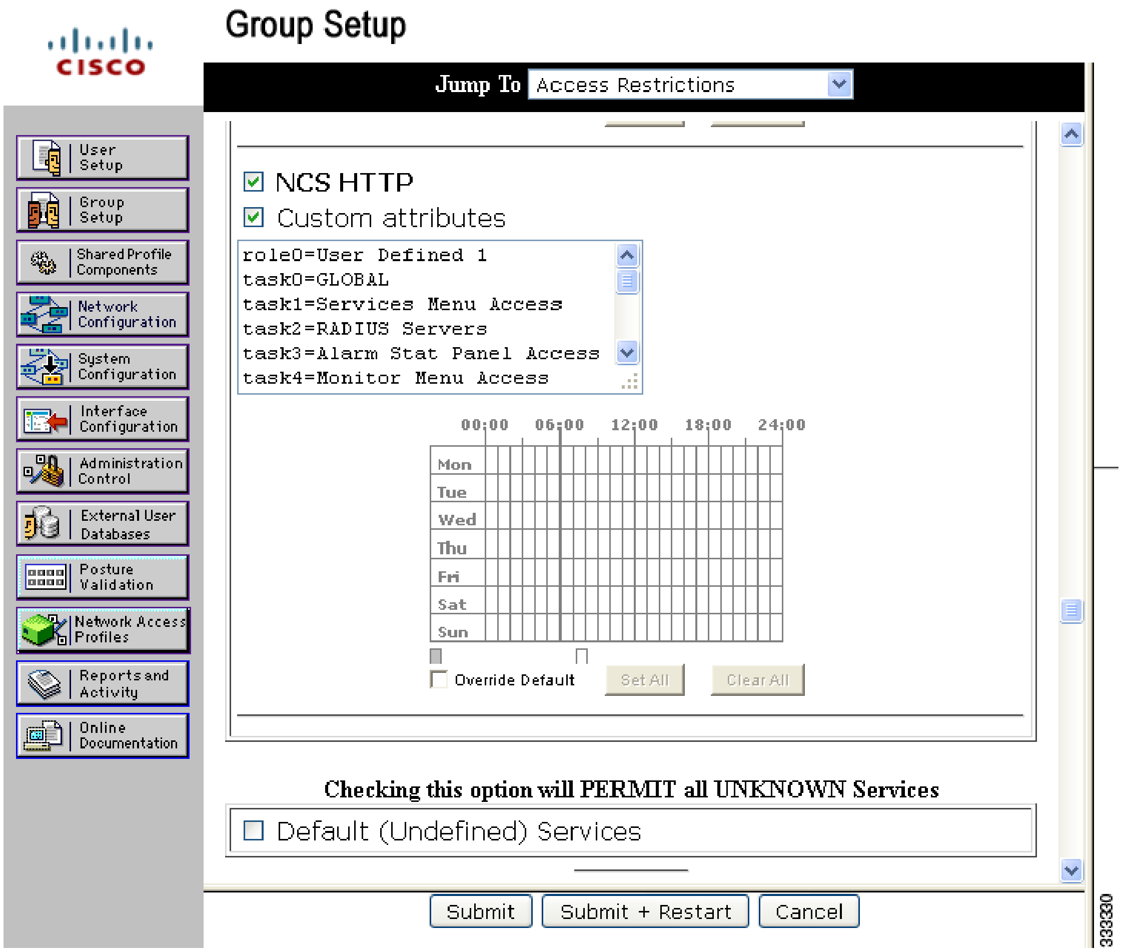
```
NCS:role0=Admin
NCS:task0=GLOBAL
NCS:task1=View Alerts and Events
NCS:task2=Lobby Ambassador Defaults Configuration
NCS:task3=Device Reports
NCS:task4=Monitor Controllers
NCS:task5=Alarm Stat Panel Access
NCS:task6=RADIUS Servers
NCS:task7=Monitor Security
NCS:task8=Monitor Menu Access
NCS:task9=Network Summary Reports
NCS:task10=Configure ACS View Servers
NCS:task11=Run Reports List
NCS:task12=View CAS Notifications Only
NCS:task13=Administration Menu Access
NCS:task14=Monitor Clients
NCS:task15=Configure Switch Location Configuration Templates
NCS:task16=Monitor Interferers
NCS:task17=Configure WiFi TDOA Receivers
NCS:task18=Configure Guest Users
NCS:task19=TAC Case Attachment Tool
NCS:task20=Configure Lightweight Access Point Templates
NCS:task21=Monitor Chokepoints
NCS:task22=Maps Read Write
NCS:task23=Voice Audit Report
NCS:task24=Configure Access Points
NCS:task25=Global SSID Groups
NCS:task26=Report Run History
NCS:task27=Compliance Reports
NCS:task28=Maps Read Only
NCS:task29=Disable Clients
```

Step 4 Highlight the text inside of the TACACS+ Custom Attributes, go to the menu of your browser, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears (see Figure 15-35).

Figure 15-35 Group Setup Page on ACS Server



☑ NCS HTTP

☑ Custom attributes

```
role0=User Defined 1
task0=GLOBAL
task1=Services Menu Access
task2=RADIUS Servers
task3=Alarm Stat Panel Access
task4=Monitor Menu Access
```

Checking this option will PERMIT all UNKNOWN Services

□ Default (Undefined) Services

Step 7 Choose which group to use, and click **Edit Settings**. NCS HTTP appears in the TACACS+ setting.

Step 8 Use Edit > Paste in your browser to place the TACACS+ custom attributes from the NCS into this text box.

Note When you upgrade the NCS, any permissions on the TACACS+ or RADIUS server must be readded.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

Note To enable TACACS+ in the NCS, see the "Configuring TACACS+ Servers" section on page 15-95. For information on configuring ACS view server credentials, see the "Configuring ACS View Server Credentials" section on page 9-247. For information on adding the NCS virtual domains into ACS for TACACS+, see the "Virtual Domain RADIUS and TACACS+ Attributes" section on page 15-49.

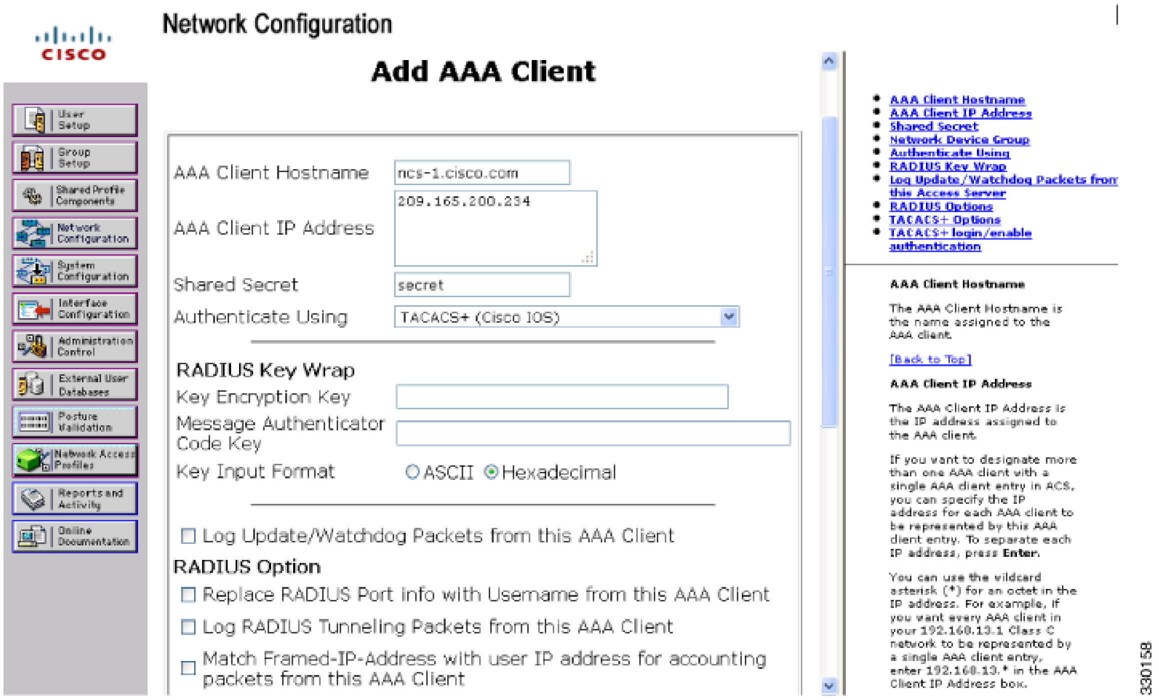
Note From NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the "Configuring a Virtual Domain" section on page 15-41.

Adding the NCS to an ACS Server for Use with RADIUS

To add the NCS to an ACS server for use with RADIUS servers, follow these steps. If you have a non-Cisco ACS server, see the "Adding the NCS to a Non-Cisco ACS Server for Use with RADIUS" section on page 15-112.

Step 1 Go to Network Configuration on the ACS server (see Figure 15-36).

Figure 15-36 Network Configuration Page on ACS Server



Network Configuration

Add AAA Client

AAA Client Hostname	ncs-1.cisco.com
AAA Client IP Address	209.165.200.234
Shared Secret	secret
Authenticate Using	TACACS+ (Cisco IOS)

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ○ ASCII ● Hexadecimal

□ Log Update/Watchdog Packets from this AAA Client

RADIUS Option

□ Replace RADIUS Port info with Username from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

- AAA Client Hostname
- AAA Client IP Address
- Shared Secret
- Network Device Group
- Authenticate Using
- RADIUS Key Wrap
- Log Update/Watchdog Packets from this Access Server
- RADIUS Options
- TACACS+ Options
- TACACS+ login/enable authentication

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

Step 2 Click **Add Entry**.

Step 3 In the AAA Client Hostname text box, enter the NCS hostname.

Step 4 In the AAA Client IP Address text box, enter the NCS IP address.

Note Ensure the interface that you use for ACS is the same you specified in the NCS and it is reachable.

Step 5 In the Shared Secret text box, enter the shared secret that you want to configure on both the NCS and ACS servers.

Step 6 Choose **RADIUS (Cisco IOS/PIX 6.0)** from the Authenticate Using drop-down list.

Step 7 Click **Submit + Apply**.

You can now associate ACS users with this ACS group.

Note To enable RADIUS in the NCS, see the "Configuring RADIUS Servers" section on page 15-98. For information on configuring ACS view server credentials, see the "Configuring ACS View Server Credentials" section on page 9-247.

Note From NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the "Configuring a Virtual Domain" section on page 15-41.

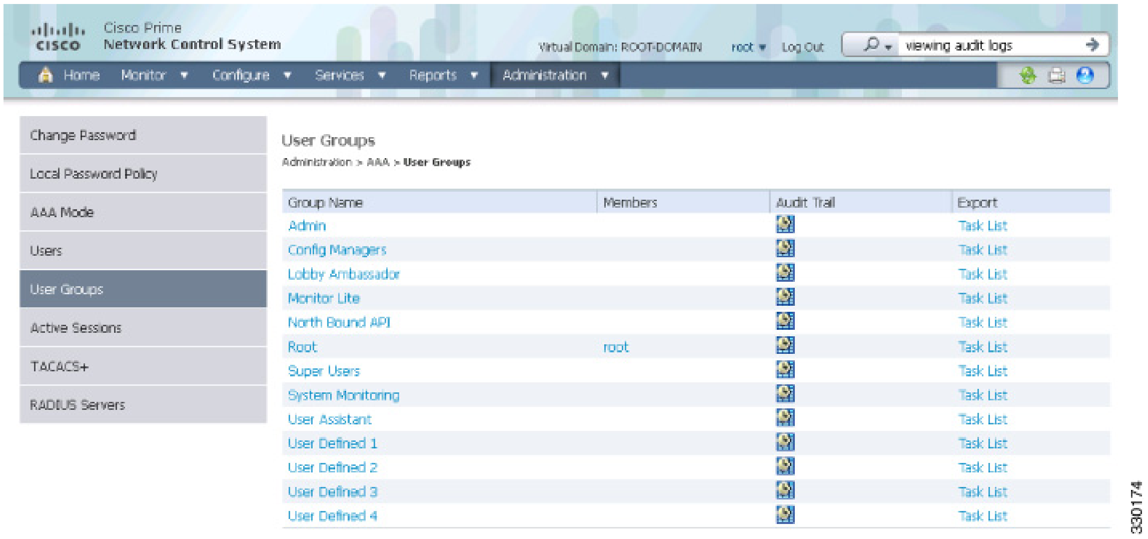
Adding NCS User Groups into ACS for RADIUS

To add NCS user groups into an ACS Server for use with RADIUS servers, follow these steps:

Step 1 Log in to NCS.

Step 2 Choose **Administration > AAA > User Groups**. The All Groups page appears (see Figure 15-37).

Figure 15-37 User Groups Page



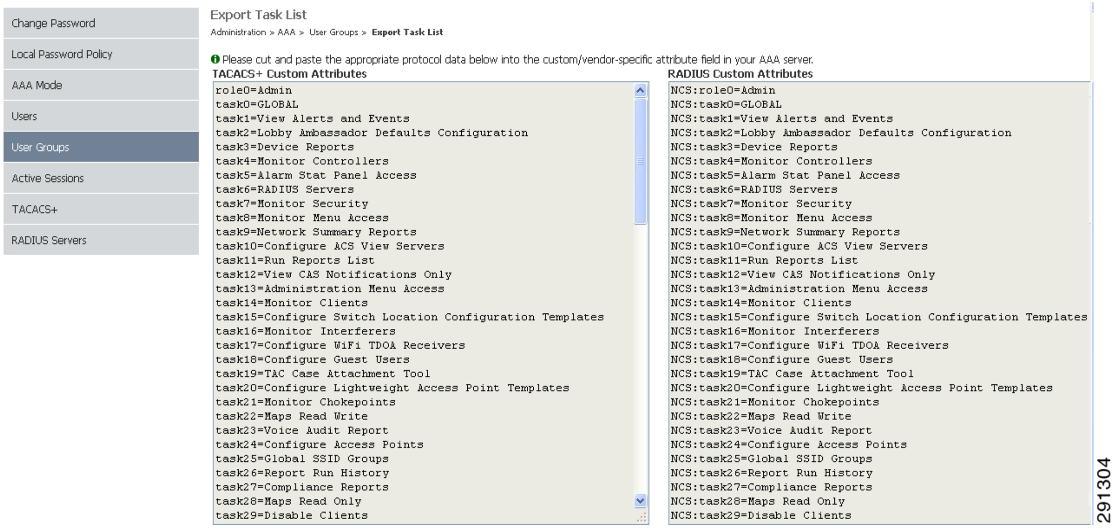
User Groups

Administration > AAA > **User Groups**

Group Name	Members	Audit Trail	Export
Admin			Task List
Config Managers			Task List
Lobby Ambassador			Task List
Monitor Lite			Task List
North Bound API			Task List
Root	root		Task List
Super Users			Task List
System Monitoring			Task List
User Assistant			Task List
User Defined 1			Task List
User Defined 2			Task List
User Defined 3			Task List
User Defined 4			Task List

Step 3 Click the Task List link of the user group that you want to add to ACS. The Export Task List page appears (see Figure 15-38).

Figure 15-38 Export Task List Page



Export Task List

Administration > AAA > User Groups > **Export Task List**

Please cut and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=GLOBAL
task1=View Alerts and Events
task2=Lobby Ambassador Defaults Configuration
task3=Device Reports
task4=Monitor Controllers
task5=Alarm Stat Panel Access
task6=RADIUS Servers
task7=Monitor Security
task8=Monitor Menu Access
task9=Network Summary Reports
task10=Configure ACS View Servers
task11=Run Reports List
task12=View CAS Notifications Only
task13=Administration Menu Access
task14=Monitor Clients
task15=Configure Switch Location Configuration Templates
task16=Monitor Interferers
task17=Configure WiFi TDOA Receivers
task18=Configure Guest Users
task19=TAC Case Attachment Tool
task20=Configure Lightweight Access Point Templates
task21=Monitor Chokepoints
task22=Maps Read Write
task23=Voice Audit Report
task24=Configure Access Points
task25=Global SSID Groups
task26=Report Run History
task27=Compliance Reports
task28=Maps Read Only
task29=Disable Clients
```

RADIUS Custom Attributes

```
NCS:role0=Admin
NCS:task0=GLOBAL
NCS:task1=View Alerts and Events
NCS:task2=Lobby Ambassador Defaults Configuration
NCS:task3=Device Reports
NCS:task4=Monitor Controllers
NCS:task5=Alarm Stat Panel Access
NCS:task6=RADIUS Servers
NCS:task7=Monitor Security
NCS:task8=Monitor Menu Access
NCS:task9=Network Summary Reports
NCS:task10=Configure ACS View Servers
NCS:task11=Run Reports List
NCS:task12=View CAS Notifications Only
NCS:task13=Administration Menu Access
NCS:task14=Monitor Clients
NCS:task15=Configure Switch Location Configuration Templates
NCS:task16=Monitor Interferers
NCS:task17=Configure WiFi TDOA Receivers
NCS:task18=Configure Guest Users
NCS:task19=TAC Case Attachment Tool
NCS:task20=Configure Lightweight Access Point Templates
NCS:task21=Monitor Chokepoints
NCS:task22=Maps Read Write
NCS:task23=Voice Audit Report
NCS:task24=Configure Access Points
NCS:task25=Global SSID Groups
NCS:task26=Report Run History
NCS:task27=Compliance Reports
NCS:task28=Maps Read Only
NCS:task29=Disable Clients
```

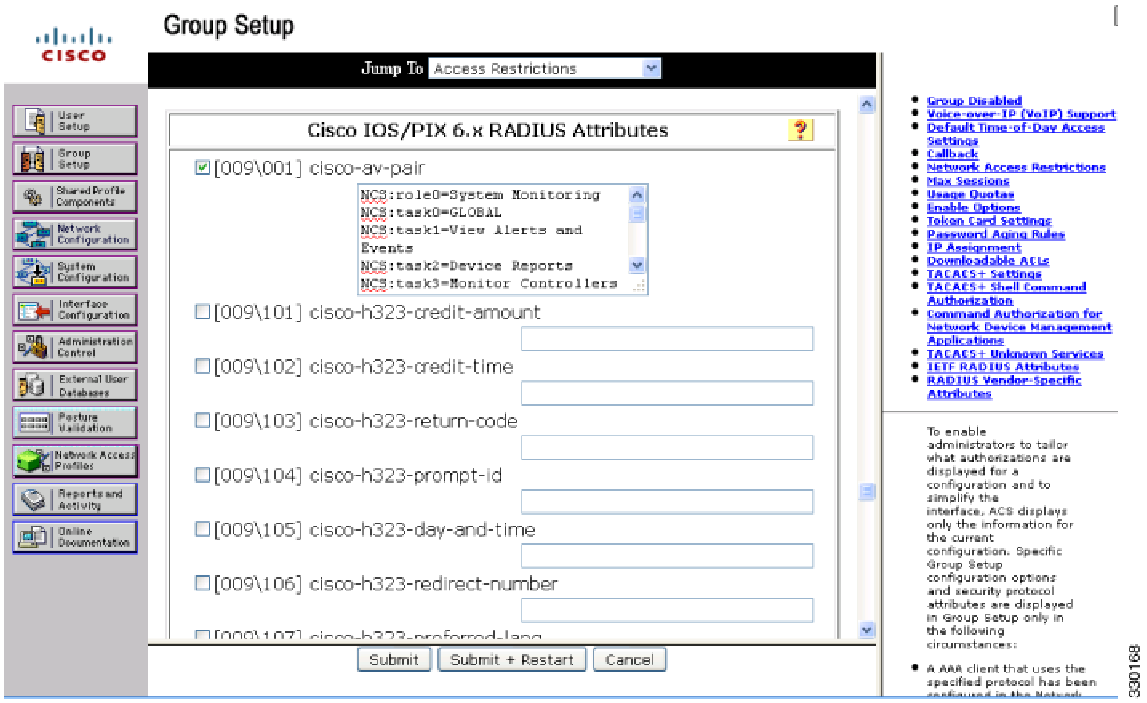
Step 4 Highlight the text inside of the RADIUS Custom Attributes, go to the menu of your browser, and choose **Edit > Copy**.

Note When you upgrade the NCS, any permissions on the TACACS+ or RADIUS server must be readded.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup page appears (see Figure 15-39).

Figure 15-39 Group Setup Page on ACS Server



Group Setup

Jump To: Access Restrictions

Cisco IOS/PIX 6.x RADIUS Attributes

☑ [009\001] cisco-av-pair

```
NCS:role0=System Monitoring
NCS:task0=GLOBAL
NCS:task1=View Alerts and
Events
NCS:task2=Device Reports
NCS:task3=Monitor Controllers
```

□ [009\101] cisco-h323-credit-amount

□ [009\102] cisco-h323-credit-time

□ [009\103] cisco-h323-return-code

□ [009\104] cisco-h323-prompt-id

□ [009\105] cisco-h323-day-and-time

□ [009\106] cisco-h323-redirect-number

□ [009\107] cisco-h323-preferred-lang

- Group Disabled
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:

- A AAA client that uses the specified protocol has been configured in the Network

Step 7 Choose which group to use, and click **Edit Settings**. Find [009\001]cisco-av-pair under Cisco IOS/PIX 6.x RADIUS Attributes.

Step 8 Use Edit > Paste in your browser to place the RADIUS custom attributes from the NCS into this text box.

Note When you upgrade the NCS, any permissions on the TACACS+ or RADIUS server must be readded.

Step 9 Select the check boxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

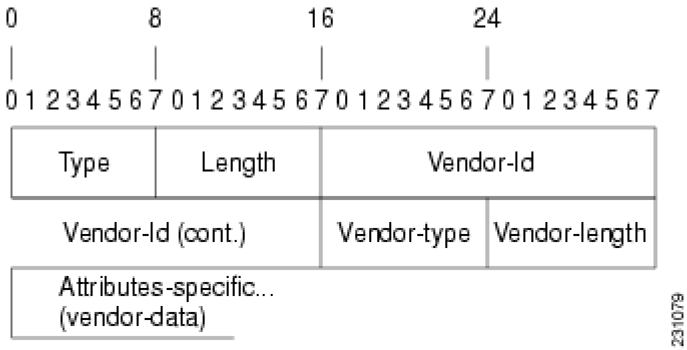
Note To enable RADIUS in the NCS, see the "Configuring RADIUS Servers" section on page 15-98. For information on configuring ACS view server credentials, see the "Configuring ACS View Server Credentials" section on page 9-247. For information on adding NCS virtual domains into ACS for TACACS+, see the "Virtual Domain RADIUS and TACACS+ Attributes" section on page 15-49.

Note From NCS Release 1.0 and later, you are required to add a virtual domain in ACS when exporting the task list to ACS. This might be the default ROOT-DOMAIN virtual domain. For more information on virtual domains, see the "Configuring a Virtual Domain" section on page 15-41.

Adding the NCS to a Non-Cisco ACS Server for Use with RADIUS

When you use a RADIUS server to log in to the NCS, the AAA server sends back an access=accept message with a user group and a list of available tasks, after the username and password were verified. The access=accept message comes back as a fragmented packet because of the large number of tasks in some user groups. You can look in the following file to see the tasks associated with a given user group: C:\Program Files\NCS\webnms\webacs\WEB-INF\security\usergroup-map.xml. The tasks are passed back as a vendor specific attribute (VSA), and the NCS requires authorization information using the VSA (IETF RADIUS attribute number 26). The VSA contains the NCS RADIUS task list information (see Figure 15-40).

Figure 15-40 Extracting Task List



The content of the VSA is as follows:

- Type = 26 (IETF VSA number)
- Vendor Id = 9 (Cisco vendor ID)
- Vendor Type = 1 (Custom attributes)
- Vendor Data = The NCS task information (for example NCS: task0 = Users and Group)

Each line from the NCS RADIUS task list should be sent in its own RADIUS VSA.

In the data portion of the access=access packet, the truncated output sometimes shows only one role sent back for an Admin user group login. The tasks associated with the role start with task0 and increment with task1, task2, and so on. Table 15-8 defines what these attributes in the access=access packet example signify.

```
0000 06 6d 0e 59 07 3d 6a 24 02 47 07 35 d2 12 a4 eb .m.Y.=j$G.5...
0010 a2 5a fa 84 38 20 e4 e2 3a 3a bc e5 1a 20 00 00 .Z..8..::..
0020 00 09 01 1a 57 69 72 65 6c 65 73 73 2d 57 43 53 ....NCS
0030 3a 72 6f 6c 65 30 3d 41 64 6d 69 6e 1a 2b 00 00 :role0=Admin.+...
0040 00 09 01 25 57 69 72 65 6c 65 73 73 2d 57 43 53 ...%NCS
0050 3a 74 61 73 6b 30 3d 55 73 65 72 73 20 61 6e 64 :task0=Users and
0060 20 47 72 6f 75 70 73 1a 27 00 00 00 09 01 21 57 Groups.”....!W
0070 69 72 65 6c 65 73 73 2d 57 43 53 3a 74 61 73 6b NCS:task
0080 31 3d 41 75 64 69 74 20 54 72 61 69 6c 73 xx xx 1=Audit Trails.*
```

Table 15-8 Access=Access Packet Example

Attribute	Description
1a (26 in decimal)	Vendor attribute
2b (43 bytes in decimal)	Length as the total number of bytes to skip and still reach the next TLV (for task0, Users and Groups)
4-byte field	Vendor Cisco 09
01	Cisco AV pair - a TLV for the NCS to read
25 (37 bytes in decimal)	Length
hex text string	NCS:task0=Users and Groups
	The next TLV until the data portion is completely processed.
255.255.255.255	TLV: RADIUS type 8 (framed IP address)
Type 35 (0x19)	A class, which is a string
Type 80 (0x50)	Message authenticator

To troubleshoot, perform the following steps:

- Verify if the RADIUS packet is an access accept.
- Verify the task names for the user group in the access accept.
- Look at the different length fields in the RADIUS packet.

Configuring ACS 5.x

This section provides instructions for configuring ACS 5.x to work with the NCS.

This section contains the following topics:

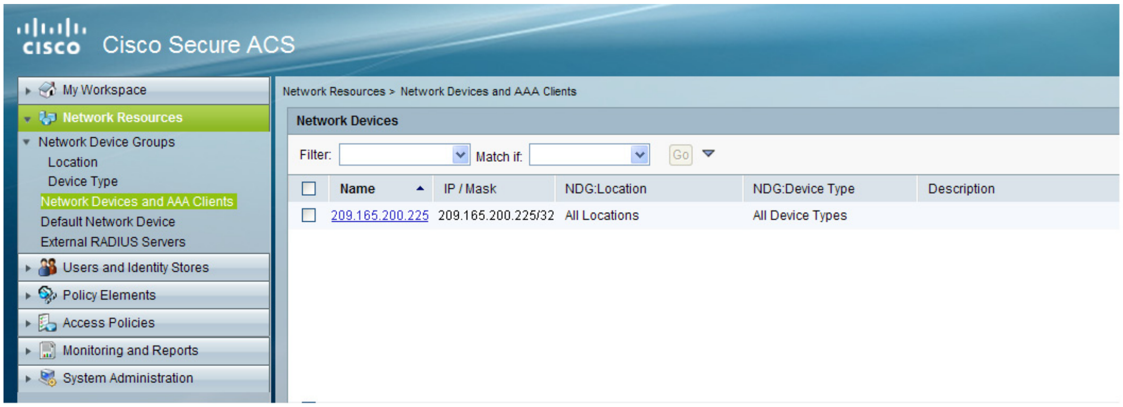
- Creating Network Devices and AAA Clients, page 15-113
- Adding Groups, page 15-114
- Adding Users, page 15-114
- Creating Policy Elements or Authorization Profiles, page 15-115
- Creating Authorization Rules, page 15-117
- Configuring Access Services, page 15-119

Creating Network Devices and AAA Clients

To create Network Devices and AAA Clients, follow these steps:

Step 1 Choose **Network Resources** > **Network Devices and AAA Clients**.

Figure 15-41 Network Devices Page



□	Name	IP / Mask	NDG:Location	NDG:Device Type	Description
□	209.165.200.225	209.165.200.225/32	All Locations	All Device Types	

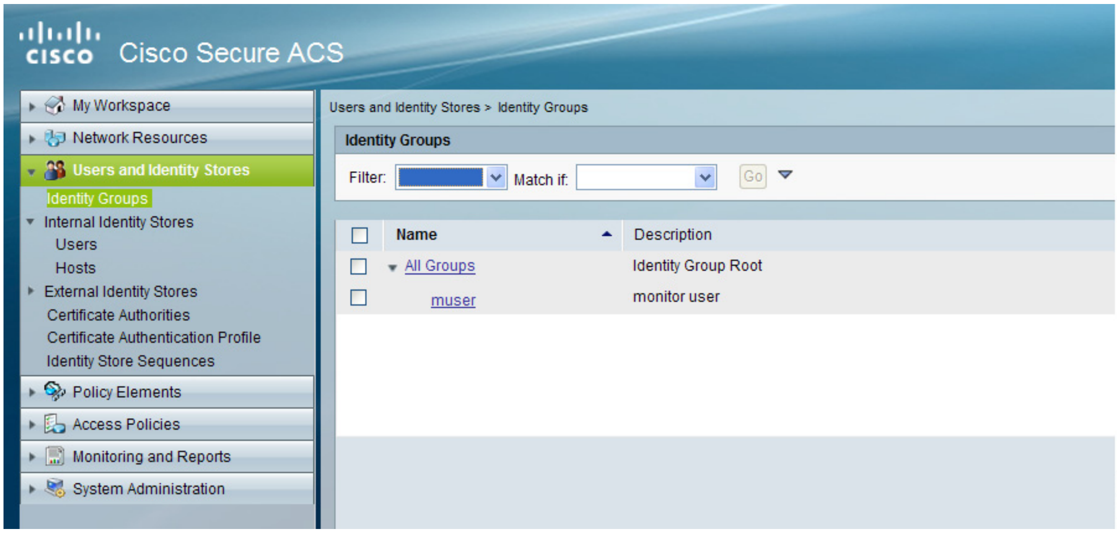
Step 2 Enter an IP address.

Adding Groups

To add groups, follow these steps:

Step 1 Choose **Users and Identity Stores** > **Identity Groups**.

Figure 15-42 Identify Groups Page



□	Name	Description
□	All Groups	Identity Group Root
□	muser	monitor user

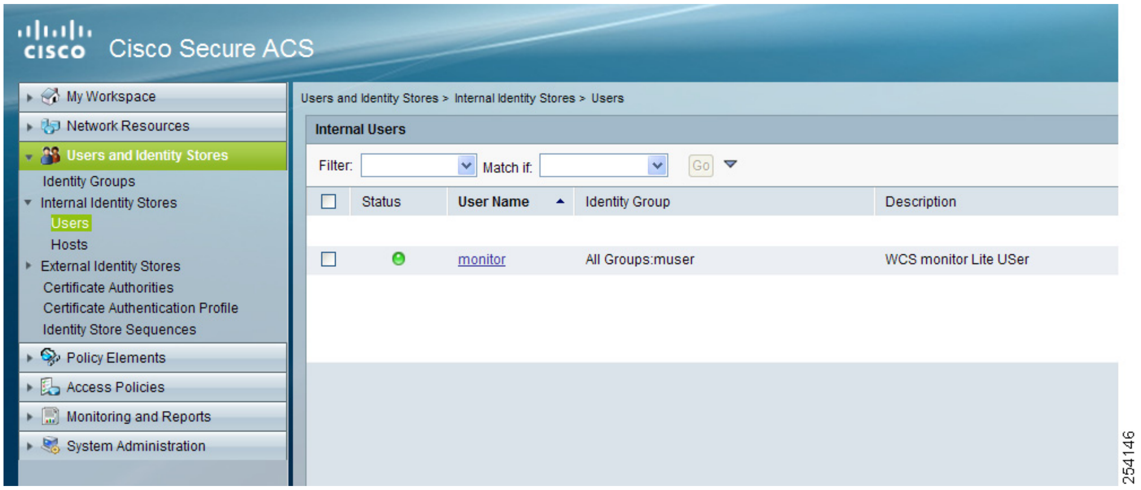
Step 2 Create a Group.

Adding Users

To add users, follow these steps:

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

Figure 15-43 Internal Users Page



Users and Identity Stores > Internal Identity Stores > Users

Internal Users

□	Status	User Name ▲	Identity Group	Description
□	●	monitor	All Groups:muser	WCS monitor Lite USer

Step 2 Add a user, and then map to group to that user.

Creating Policy Elements or Authorization Profiles

This section contains the following topics:

- Creating Policy Elements or Authorization Profiles for RADIUS, page 15-115
- Creating Policy Elements or Authorization Profiles For TACACS, page 15-116

Creating Policy Elements or Authorization Profiles for RADIUS

To create policy elements or authorization profiles for RADIUS, perform the following steps:

Step 1 Choose **Policy Elements** > **Authorization and Permissions** > **Network Access** > **Authorization Profiles**.

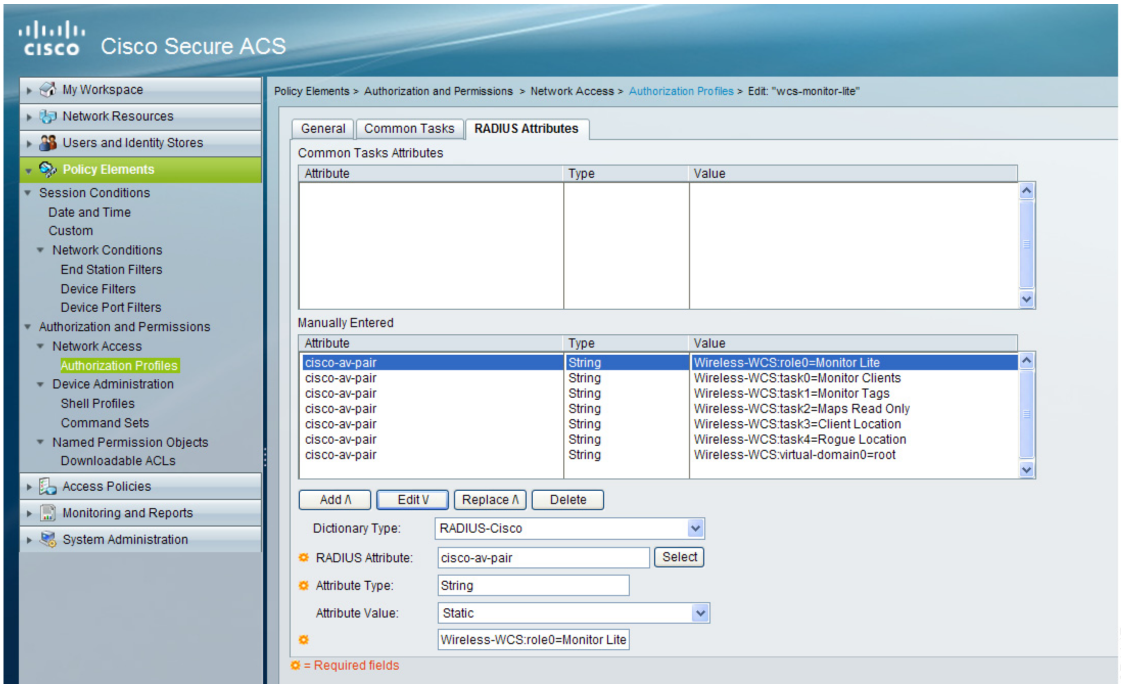
Step 2 Click **Create**.

Step 3 Enter a name and description.

Step 4 Click the **RADIUS Attributes** tab.

Step 5 Add RADIUS attributes one by one (see Figure 15-44).

Figure 15-44 Authorization Profiles Page



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "wcs-monitor-lite"

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
cisco-av-pair	String	Wireless-WCS:role0=Monitor Lite
cisco-av-pair	String	Wireless-WCS:task0=Monitor Clients
cisco-av-pair	String	Wireless-WCS:task1=Monitor Tags
cisco-av-pair	String	Wireless-WCS:task2=Maps Read Only
cisco-av-pair	String	Wireless-WCS:task3=Client Location
cisco-av-pair	String	Wireless-WCS:task4=Rogue Location
cisco-av-pair	String	Wireless-WCS:virtual-domain0=root

Dictionary Type: RADIUS-Cisco

RADIUS Attribute: cisco-av-pair

Attribute Type: String

Attribute Value: Static

Wireless-WCS:role0=Monitor Lite

= Required fields

Step 6 Click **Submit**.

Creating Policy Elements or Authorization Profiles For TACACS

To create policy elements or authorization profiles for TACACS, perform the following steps:

Step 1 Choose **Policy Elements** > **Authorization and Permissions** > **Device Administration** > **Shell Profiles**.

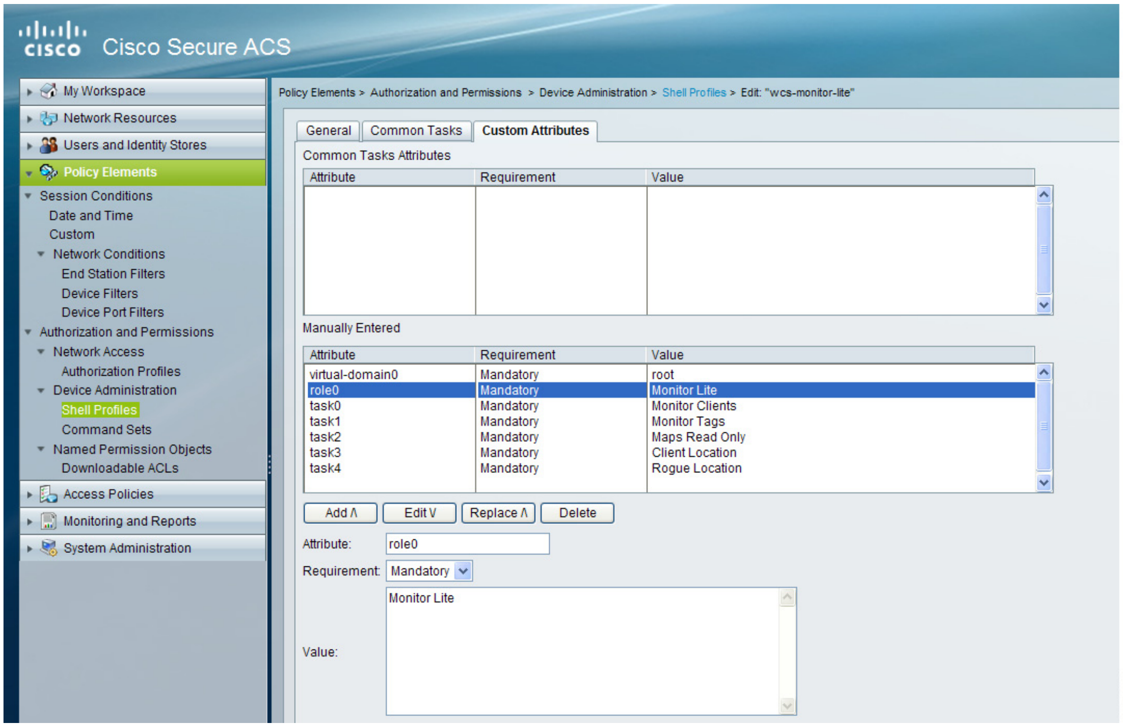
Step 2 Click **Create**.

Step 3 Enter a name and description.

Step 4 Click the **Custom Attributes** tab.

Step 5 Add the TACACS ttributes one by one (see Figure 15-45).

Figure 15-45 Shell Profiles Page



Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "wcs-monitor-lite"

Common Tasks Attributes

Attribute	Requirement	Value

Manually Entered

Attribute	Requirement	Value
virtual-domain0	Mandatory	root
role0	Mandatory	Monitor Lite
task0	Mandatory	Monitor Clients
task1	Mandatory	Monitor Tags
task2	Mandatory	Maps Read Only
task3	Mandatory	Client Location
task4	Mandatory	Rogue Location

Attribute: role0

Requirement: Mandatory

Value: Monitor Lite

Step 6 Click **Submit**.

Creating Authorization Rules

This section provides instructions for configuring authorization for RADIUS and TACACS.

This section contains the following topics:

- "Creating Service Selection Rules for RADIUS" section on page 15-117
- "Creating Service Selection Rules for TACACS" section on page 15-118

Creating Service Selection Rules for RADIUS

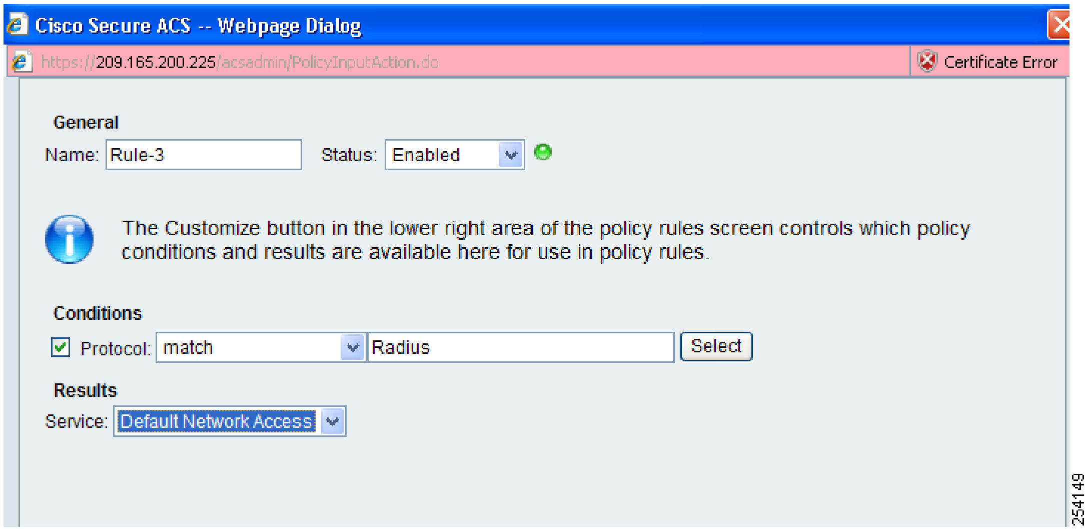
To create service selection rules for RADIUS, perform the following steps:

Step 1 Choose **Access Policies** > **Access Services** > **Service Selection Rules**.

Step 2 Click **Create**.

Step 3 Select the protocol as Radius and choose **Default Network Access** from the Service drop-down list. (see Figure 15-46).

Figure 15-46 Service Selection Page



Cisco Secure ACS -- Webpage Dialog

https://209.165.200.225/acsadmin/PolicyInputAction.do

General

Name: Rule-3 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Protocol: match Radius

Results

Service: Default Network Access

Step 4 Click **OK**.

Creating Service Selection Rules for TACACS

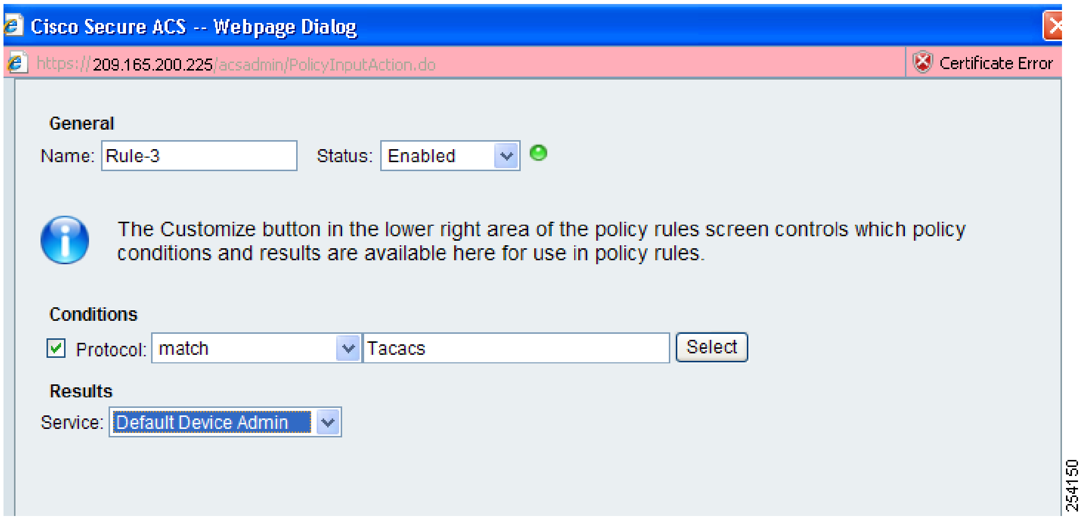
To create service selection rules for TACACS, follow these steps:

Step 1 Choose **Access Policies** > **Access Services** > **Service Selection Rules**.

Step 2 Click **Create**.

Step 3 Select the protocol as TACACS and choose **Default Device Admin** from the Service drop-down list. (see Figure 15-47).

Figure 15-47 Service Selection Page



Cisco Secure ACS -- Webpage Dialog

https://209.165.200.225/acsadmin/PolicyInputAction.do

General

Name: Rule-3 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Protocol: match Tacacs

Results

Service: Default Device Admin

Step 4 Click **OK**.

Configuring Access Services

This section provides instructions for configuring access services for RADIUS and TACACS.

This section contains the following topics:

- Configuring Access Services for RADIUS, page 15-119
- Configuring Access Services for TACACS, page 15-120

Configuring Access Services for RADIUS

To configure access services for RADIUS, perform the following steps:

Step 1 Log in to the ACS 5.x server and choose **Access Policies** > **Access Services** > **Default Network Access**.

Step 2 On the General tab, select the policy structure you want to use. By default, all the three policy structures are selected.

Step 3 From the Allowed Protocols, select the protocols you want to use.

Note You can retain the defaults for identity and group mapping.

Step 4 To create an authorization rule for RADIUS, choose **Access Policies** > **Access Services** > **Default Network Access** > **Authorization** (see Figure 15-48).

Step 5 Click **Create**.

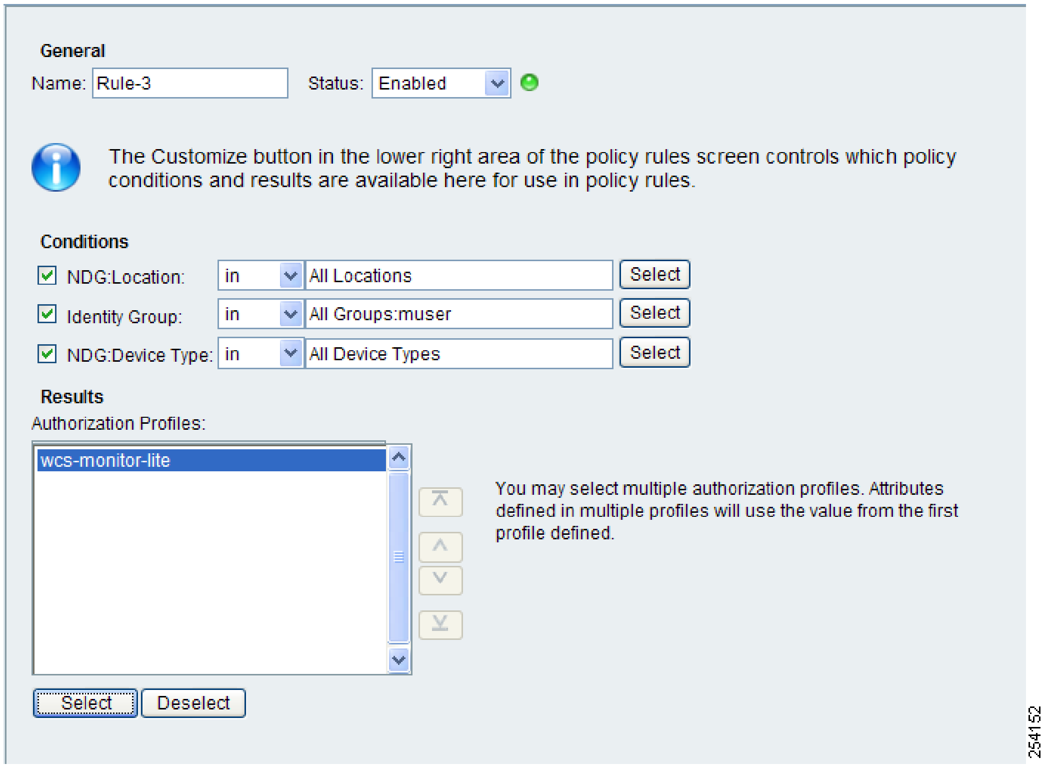
Step 6 In Location, select **All Locations** or you can create a rule based on the location.

Step 7 In Group, select the group that you created earlier.

Step 8 In Device Type, select **All Device Types** or you can create a rule based on the Device Type.

Step 9 In Authorization Profile, select the authorization profile created for RADIUS.

Figure 15-48 Authorization Page



General

Name: Rule-3 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ NDG:Location: in All Locations Select

☑ Identity Group: in All Groups:muser Select

☑ NDG:Device Type: in All Device Types Select

Results

Authorization Profiles:

wcs-monitor-lite

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Step 10 Click **OK**.

Step 11 Click **Save**.

Configuring Access Services for TACACS

To configure access services for TACACS, follow these steps:

Step 1 Choose **Access Policies** > **Access Services** > **Default Device Admin**.

Step 2 On the General tab, select the policy structure you want to use. By default, all the three are selected. Similarly, in Allowed Protocols, select the protocols you want to use.

Note You can retain the defaults for identity and group mapping.

Step 3 To create an authorization rule for TACACS, choose **Access Policies** > **Access Services** > **Default Device Admin** > **Authorization**. (see Figure 15-49).

Step 4 Click **Create**.

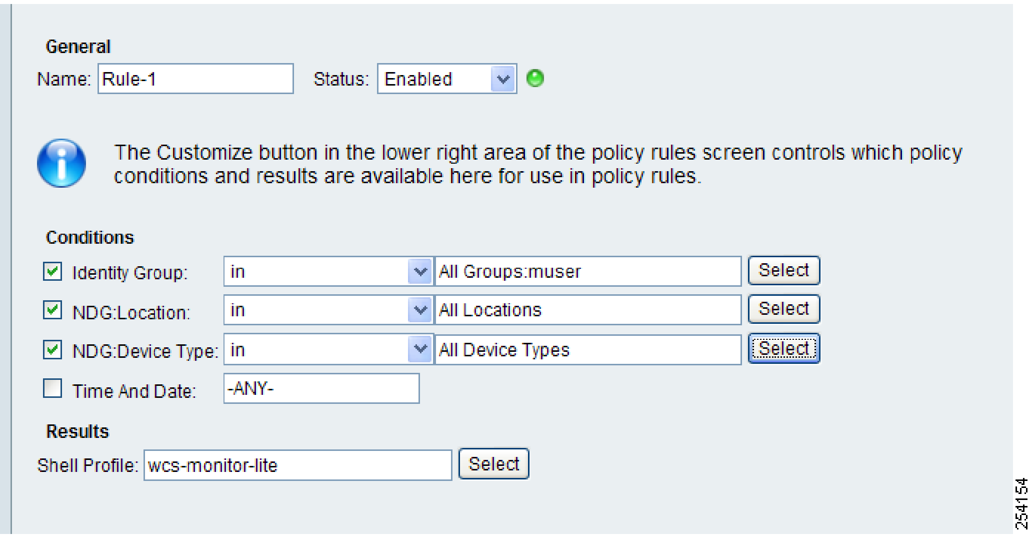
Step 5 In Location, select All Locations or you can create a rule based on the location.

Step 6 In Group, select the group that you created earlier.

Step 7 In Device Type, select All Device Types or you can create a rule based on the Device Type.

Step 8 In Shell Profile, select the shell profile created for TACACS.

Figure 15-49 Authorization Page



General

Name: Rule-1 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Identity Group: in All Groups:muser Select

☑ NDG:Location: in All Locations Select

☑ NDG:Device Type: in All Device Types Select

□ Time And Date: -ANY-

Results

Shell Profile: wcs-monitor-lite Select

Step 9 Click **OK**.

Step 10 Click **Save**.

Establishing Logging Options

Choose **Administration** > **Logging** to access the Administer Logging Options page. The logging for controller syslog information can be done in the Controller > Management > Syslog page. This section describes the log settings that can be configured and contains the following topics:

- General Logging Options, page 15-121
- SNMP Logging Options, page 15-123
- Syslog Options, page 15-124

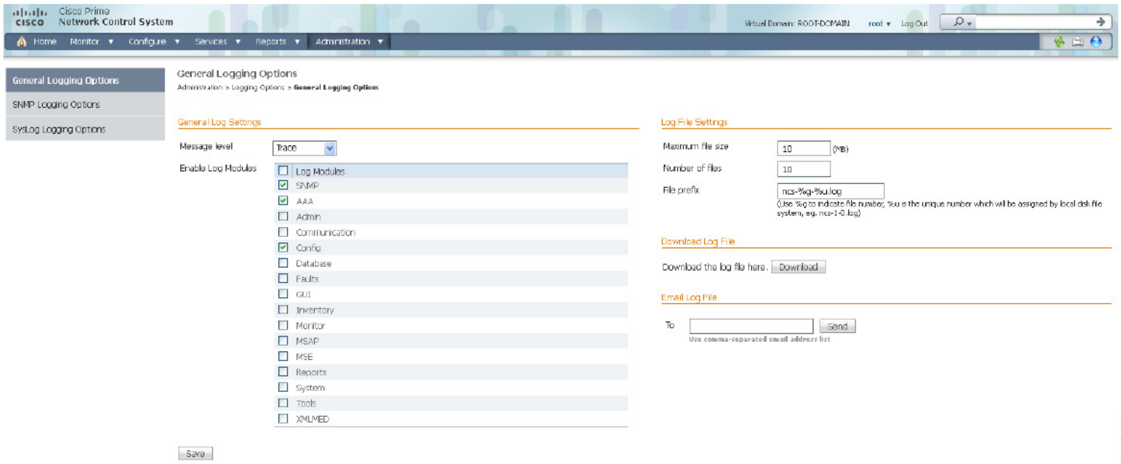
General Logging Options

To enable e-mail logging, follow these steps. The settings you establish are stored and are used by the e-mail server.

Step 1 Choose **Administration > Logging**. The General Logging Options page appears (see Figure 15-50).

Step 2 Choose **General Logging Options** from the left sidebar menu.

Figure 15-50 *General Logging Options Page*



General Logging Options

Administration > Logging Options > **General Logging Options**

General Log Settings

Message level: Trace

Enable Log Modules:

- □ Log Modules
- ☑ SNMP
- ☑ AAA
- □ Admin
- □ Communication
- ☑ Config
- □ Database
- □ Faults
- □ GUI
- □ Inventory
- □ Monitor
- □ MSAP
- □ MSE
- □ Reports
- □ System
- □ Tools
- □ XMLMED

Save

Log File Settings

Maximum file size: 10 (MB)

Number of files: 10

File prefix: ncs-%g-%u.log

(Use %g to indicate file number, %u is the unique number which will be assigned by local disk file system, eg. ncs-1-0.log)

Download Log File

Download the log file here. Download

Email Log File

To: Send

Use comma-separated email address list

Step 3 From the Message level drop-down list, choose **Trace**, **Information**, or **Error**.

Step 4 Select the check boxes within the Enable Log Module group box to enable various administration modules:

- Message Level—Select the minimum level of the messages that are logged including **Error**, **Information**, or **Trace**.
- Enable Log Module—You can enable logging for the following administration modules:
  - Log Modules—Select this check box to select all the modules.
  - SNMP—Captures logs for all SNMP communication between the NCS and controllers.
  - AAA—Captures AAA related logs for the NCS.
  - Admin—Contains Administration based logs, where all the configuration changes performed using the administration console is logged.
  - Communication—Contains logs related to the protocols used in communication.
  - Config—Used to log controller configurations that you make from the NCS.

    Note To get complete controller configuration logs, also enable the General log module.

    Note To get the configuration values that the NCS sends in logs to controllers, enable Trace Display Values (Administration > Settings > SNMP Settings > Trace Display Value).

  - Database—Contains logs to debug important database-related operations in the NCS.

  Note Some functions should be used only for short periods of time during debugging so that the performance is not degraded. For example, trace mode and SNMP meditation should be enabled only during debugging because a lot of log information is generated.

  - Faults—Used by the event and alert subsystem.
  - GUI—Contains generic UI validation logs.

- Inventory—Captures all Inventory-related logs.
- Monitor—Used for Alarms, Spectrum Intelligence, CCXV5, Clients/Tags, Client Radio Measurements, SSO, and Mesh.
- MSE—Used for MSE-related operations such as adding or deleting an MSE and changing parameters on the MSE. It also enables logging for MSE synchronization including NW designs and controllers.
- Reports—Used to log messages related to creating, saving, scheduling, and running reports. This module also contains a list of scheduled and saved reports.
- System—Captures all System-related logs.
- Tools—Contains logs related to different plug-in tools.
- XMLMED—Used to enable trace for the communication between the MSE and NCS.

Step 5 In the Log File Settings portion, enter the following settings. These settings become effective after restarting NCS.

- Max. file size—Maximum number of MBs allowed per log file.
- Number of files—Maximum number of log files allowed.
- File prefix—Log file prefix, which can include the characters "%g" to sequentially number of files.

Step 6 Click **Download** to download the log file to your local machine.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the .zip file is an html file that documents the log files.

Step 7 Enter the E-mail ID or E-mail IDs separated by commas to send the log file.

Note To send the log file in a mail you must have E-mail Server configured.

Step 8 Click **Submit**.

SNMP Logging Options

To enable SNMP Tracing, follow these steps. The settings you establish are stored and are used by the SNMP server.

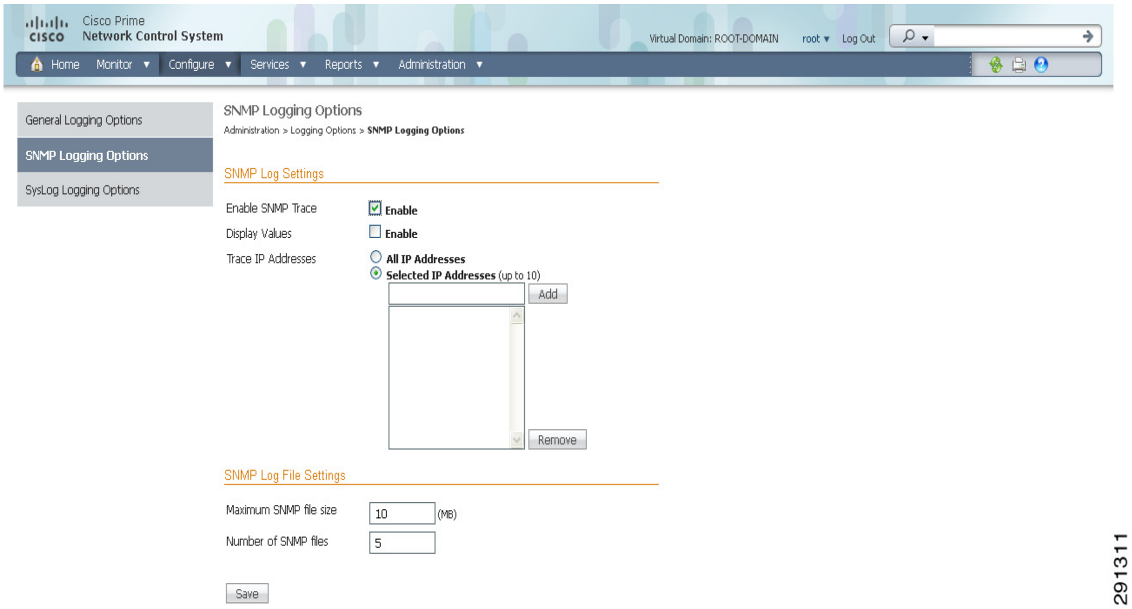
Note SNMP server is nothing but the NCS server which uses these settings for SNMP logging.

Note When you upgrade from WCS Release 7.x to NCS Release 1.1, the settings under Administration > Logging Options > SNMP Logging Options are not retained.

Step 1 Choose A**dministration > Logging**. The Logging Options page appears (see Figure 15-51).

Step 2 Choose the **SNMP Logging Options** from the left sidebar menu.

Figure 15-51 SNMP Logging Options Page



SNMP Logging Options

Administration > Logging Options > **SNMP Logging Options**

SNMP Log Settings

Enable SNMP Trace	☑ **Enable**
Display Values	□ **Enable**
Trace IP Addresses	○ **All IP Addresses** ● **Selected IP Addresses** (up to 10)

SNMP Log File Settings

Maximum SNMP file size	10 (MB)
Number of SNMP files	5

Step 3 Select the **Enable SNMP Trace** check box to enable sending SNMP messages (along with traps) between controller and NCS.

Step 4 Select the **Display Values** check box to see the SNMP Message values.

Step 5 Configure the IP address or IP addresses to trace the SNMP traps. You can add up to a maximum of 10 IP addresses in the text box.

Step 6 You can configure the maximum SNMP file size and the number of SNMP files.

Syslog Options

The Syslog protocol is simply designed to transport event messages from the generating device to the collector. Various devices generate syslog messages for system information and alerts.

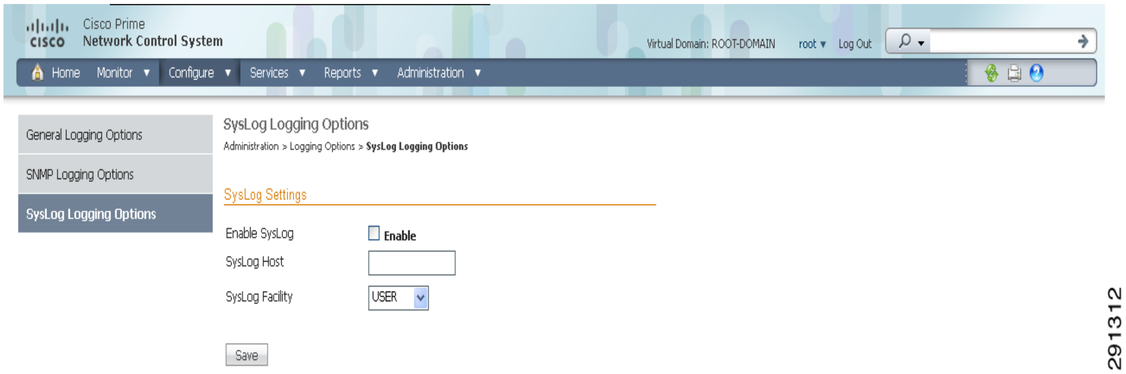
Note When you upgrade from WCS Release 7.x to NCS Release 1.1, the settings under Administration > Logging Options > SysLog Logging Options are not retained.

To configure Syslog for the NCS, follow these steps:

Step 1 Choose A**dministration > Logging**. The Logging Options page appears (see Figure 15-50).

Step 2 Choose the **Syslog Options** from the left sidebar menu.

Figure 15-52 Syslog Options Page



SysLog Logging Options

Administration > Logging Options > **SysLog Logging Options**

SysLog Settings

Enable SysLog □ **Enable**

SysLog Host

SysLog Facility USER

Step 3 Select the **Enable Syslog** check box to enable collecting and processing system logs.

Step 4 Configure the Syslog Server IP address of the interface from which the message is to be transmitted.

Step 5 Choose the **Syslog Facility**. You can choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.

Using Logging Options to Enhance Troubleshooting

The logging page allows you to customize the amount of data the NCS collects to debug an issue. For easily reproduced issues, follow these steps prior to contacting TAC. These steps might create a smoother troubleshooting session:

Step 1 Choose **Administration > Logging**.

Step 2 From the Message Level drop-down list, choose **Trace**.

Step 3 Select each check box to enable all log modules.

Step 4 Reproduce the current problem.

Step 5 Return to the Logging Options page.

Step 6 Click **Download** from the Download Log File section.

Note The logs.zip filename includes a prefix with the host name, date, and time so that you can easily identify the stored log file. Included in the .zip file is an html file that documents the log files.

Step 7 After you have retrieved the logs, choose **Information** from the Message Level drop-down list.

Note Leaving the Message Level at *Trace* can adversely affect performance over a long period of time.

Configuring High Availability

To ensure continued operation in case of failure, the NCS now provides a high availability or failover framework. When an active (primary) NCS fails, a secondary NCS takes over operations (in less than two minutes) for the failed primary NCS and continues to provide service. Upon failover, a peer of the failed primary NCS is activated on the secondary NCS using the local database and files, and the secondary NCS runs a fully functional NCS. While the secondary host is in failover mode, the database and file backups of other primary NCSs continue uninterrupted.

If E-mail Address is specified in the HA configuration, Mail Server must be configured and reachable to succeed in HA configuration.

For more high availability information, see the following sections:

- Guidelines and Limitations for High Availability, page 15-126
- Failover Scenario, page 15-127
- Performing Background Tasks, page 15-1
- High Availability Status, page 15-128
- Configuring High Availability on the Primary NCS, page 15-128
- Deploying High Availability, page 15-130

This section contains the following topics:

- Guidelines and Limitations for High Availability, page 15-126
- Failover Scenario, page 15-127
- High Availability Status, page 15-128
- Configuring High Availability on the Primary NCS, page 15-128
- Deploying High Availability, page 15-130
- Adding a New Primary NCS, page 15-131
- Removing a Primary NCS, page 15-131

Guidelines and Limitations for High Availability

Before initiating failover, you must consider the following prerequisites and limitations:

- You must have the extra hardware identical to the primary NCS to run a standby instance of the NCS.
- The NCS supports High Availability on both the physical and virtual appliance deployment models.
- A reliable high speed wired network must exist between the primary NCS and its backup NCS.
- The primary and secondary NCS must be running the same NCS software release.
- For primary NCS to initiate High Availability with secondary NCS, the status of the secondary NCS services must be running and reachable from the primary NCS. So, you must boot the secondary NCS first and then boot the primary NCS to initiate the High Availability registration.
- Failover should be considered temporary. The failed primary NCS should be restored to normal as soon as possible, and failback is reinitiated. The longer it takes to restore the failed primary NCS, the longer the other NCSs sharing that secondary NCS must run without failover support.
- The latest controller software must be used.

- The primary and secondary host are not required to share the same subnet. They can be geographically separated.
- If a secondary host fails for any reason, all the primary instances are affected, and they run in stand-alone mode without any failover support.
- The ports over which the primary and secondary NCSs communicate must be open (not blocked with network firewalls, application fireways, gateways, and so on). The tomcat port is configurable during installation, and its default port is 8082. You should reserve solid database ports from 1315 to 1319.
- Any access control lists imposed between the primary and secondary NCS must allow traffic to go between the primary and secondary NCSs.
- The primary Prime Infrastructure must have sufficient number of licenses for the devices. When the failover occurs the secondary Prime Infrastructure uses the licenses of the primary Prime Infrastructure for the devices.

NCS 1.x Updates for High Availability

- In NCS Release 1.x, a secondary NCS can only support one primary NCS.
- When high availability is enabled for the first time, the sync up of the servers take a considerable amount of time. The time it would take would be in the order of 30 minutes or more depending on the size of the database.

Failover Scenario

When a failure of a primary NCS is automatically detected, the following events take place:

Note One physical secondary NCS can back many primary devices (NCS).

1. The primary NCS is confirmed as non-functioning (hardware crash, network crash, or the like) by the health monitor on the secondary NCS.
2. If automatic failover has been enabled, NCS is started on the secondary as described in Step 3. If automatic failover is disabled, an e-mail is sent to the administrator asking if they want to manually start failover.
3. The secondary NCS instance is started immediately (using the configuration already in place) and uses the corresponding database of the primary. After a successful failover, the client should point to the newly activated NCS (the secondary NCS). The secondary NCS updates all controllers with its own address as the trap destination.

   Note The redirecting of web traffic to the secondary NCS does not occur automatically. You must use your infrastructure tools to properly configure this redirection.

4. The result of the failover operation is indicated as an event in the Health Monitor UI, or a critical alarm is sent to the administrator and to other NCS instances.

High Availability Status

To view high availability details, follow these steps:

Step 1 Choose **Administration > High Availability**.

Step 2 Choose **HA Status** from the left sidebar menu. The following information is displayed:

- Current status
- Time, state, and description of each event

Table 15-9 provides details about the different statuses of High Availability.

Table 15-9 High Availability Statuses

HA Status	Description
Stand Alone	HA is not configured.
Primary Alone	The primary NCS is alone and not synching with the secondary NCS.
HA Initializing	HA is initializing.
Primary Active	HA is synching with the secondary NCS without issue.
Primary Lost Secondary	The primary NCS has lost connectivity with the secondary NCS.
Primary Failover	A failover is being done to the primary NCS.
Primary Failback	A failback to the primary NCS is being done.
Primary Uncertain	The primary NCS is uncertain about the state of the secondary NCS.
Secondary Alone	The secondary NCS is alone and not synching with the primary NCS.
Secondary Syncing	HA is synching with the primary NCS without issue.
Secondary Active	HA has failed over the primary NCS and the application is running on the secondary NCS and is active.
Secondary Lost Primary	The secondary NCS has lost connectivity with the primary NCS.
Secondary Failover	A failover is being done to the secondary NCS.
Secondary Failback	A failback to the secondary NCS is being done.
Secondary Post Failback	A failback is in the post step.
Secondary Uncertain	The secondary NCS is uncertain about the state of the primary NCS.

Configuring High Availability on the Primary NCS

Note When database transaction logs grow to 1/3 of the database partition disk space, set the database to "Standalone" mode to prevent transaction logs from growing. But it requires a complete *netcopy* next time when the database synchronization occurs.

Follow these steps to configure high availability on the primary NCS. You must specify the NCS role (either standalone, primary, or secondary) during installation. See the "Deploying the NCS Virtual Appliance" section on page 2-5 to see the installation steps.

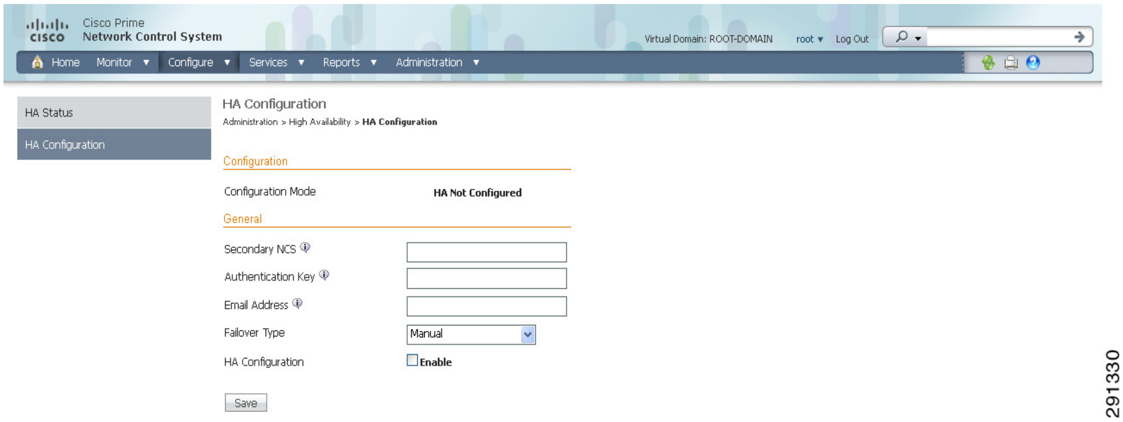
Note

- Before you configure high availability, you must configure a mail server. See the "Configuring the Mail Server" section on page 15-62 for steps on configuring a mail server.
- If you specify an e-mail address in the HA Configuration page then ensure a mail server is configured and reachable.

Step 1 Choose **Administration > High Availability**.

Step 2 Choose **HA Configuration** from the left sidebar menu. The High Availability Configuration page appears (see Figure 15-53).

Figure 15-53 High Availability Configuration Page



HA Configuration

Administration > High Availability > **HA Configuration**

Configuration

Configuration Mode **HA Not Configured**

General

Secondary NCS

Authentication Key

Email Address

Failover Type Manual

HA Configuration □ **Enable**

The current status of high availability is shown in the upper portion of the page. For information about different statuses of High Availability, see Table 15-9.

Step 3 Enter the IP address or hostname of the secondary NCS.

Step 4 Enter the authentication key specified during the installation of the secondary NCS.

Step 5 The default admin e-mail address that you configured in Administration > Settings > E-mail Server is automatically supplied. You can make any necessary changes. Any changes you make to these e-mail addresses must also be entered in the Secondary SMTP Server section of the Administration > Settings > Mail Server page.

Note You must enter an e-mail address when configuring high availability. The NCS tests the e-mail server configuration, and if the test fails (because the mail server cannot connect), the NCS does not allow the high availability configuration.

Step 6 From the Failover Type drop-down list, choose either manual or automatic. If you choose manual, you can trigger the failover operation with a button in the secondary HealthMonitor graphical user interface or with the URL specified in the e-mail which the administrator receives upon failure of the primary NCS. If you choose automatic, the secondary NCS initiates a failover on its own when a failure is detected on the primary.

Step 7 Click **Save** to retain the configuration and enable high availability, or click **Remove** to disable high availability and its settings.

Note The Remove button is only available if high availability is already configured.

At this point, the secondary is either reachable with the database, and files are synchronized between health monitors, or the secondary is unreachable, and an error is returned because secondary installation did not occur.

From the NCS graphical user interface (Administration > High Availability) after high availability has been enabled, you can perform the following functions:

- Update—Use the Update function to make changes to the Report Repository path (Administration > Settings > Report) or FTP/TFTP root directory (Administration > Settings > Server Settings) and to appropriately synchronize the files.
- Delete—Use the Delete operation to decommission the primary NCS from the secondary NCS.
- Cancel—Use the Cancel operation to cancel any modifications you made to the high availability configuration. You are returned to the High Availability Status page after you choose Cancel.

Deploying High Availability

To deploy high availability on an existing NCS installation, follow these steps:

Step 1 Identify and prepare the hardware to run the secondary NCS.

Step 2 Ensure that network connectivity between the primary and secondary NCS is functioning, and all necessary ports are open.

Step 3 Install the secondary NCS with the same version of the NCS that is installed on the primary. See the "Deploying the NCS Virtual Appliance" section on page 2-5.

Step 4 Start the secondary NCS as a standby server. In this mode, the NCS application does not start. At the same time, the Health Monitor is started on the secondary NCS.

Step 5 On every primary NCS that needs to use this secondary NCS, stop the NCS.

Step 6 On the primary host, install the new version of NCS and perform all necessary upgrade steps.

Step 7 Start the primary NCS (as a primary). The Health Monitor also starts.

Step 8 Configure the high availability parameters described in the "Configuring High Availability on the Primary NCS" section on page 15-128.

Step 9 Click **Activate** to activate high availability on the primary. The NCS primary first copies its database to the secondary NCS and then connects to the secondary. The following files are copied over from the primary to the secondary NCS:

- DB password file
- all auto provisioning startup config files
- all domain maps
- all history reports which are generated by scheduled report tasks

High availability deployment is complete. Use https://<ncsip>:8082 to access the HealthMonitor UI. Within the HealthMonitor UI, use the authentication key to log in.

You can change the authentication key in the NCS using the command prompt. To change the authentication key, change the path to the NCS installation directory then to "bin" and enter **hmadmin - authkey** *key*.

To view the current status of the health monitor, enter the **hmadmin [-options] status** command.

Adding a New Primary NCS

To add a new primary NCS to an existing setup, follow these steps. This new primary NCS uses the existing secondary as the failover server.

Step 1 Ensure that network connectivity between the new primary and secondary is functioning and that all necessary ports are open.

Step 2 Make sure that the same NCS release that is loaded on the other primary NCS and secondary NCS is loaded on the new primary NCS.

Step 3 Install the correct version of NCS on the primary NCS.

Step 4 Upgrade the primary NCS. The Health Monitor also starts.

Step 5 Follow the steps in the "Configuring High Availability" section on page 15-126.

Step 6 After the primary NCS connects to the secondary, the Health Monitor on the primary connects to the secondary Health Monitor. They mutually acknowledge each other and start the monitoring.

High availability deployment is now complete.

Removing a Primary NCS

When a primary NCS instance is removed from a group, you must disable the peer database instance on the secondary NCS and remove the Health Monitor for that primary. (To remove the primary NCS from high availability, use the Remove button on the High Availability configuration page.) The secondary NCS disables the database instance and removes the uninstalled primary NCS from its Health Monitor.

Managing Licenses

This section contains the following topics:

- License Center, page 15-132
- Managing NCS Licenses, page 15-139
- Monitoring Controller Licenses, page 15-140
- Managing Mobility Services Engine (MSE) Licenses, page 15-141

License Center

The License Center allows you to manage NCS, wireless LAN controllers, and MSE licenses. The License Center is available from the NCS Administration menu. To view the License Center page, choose **Administration > License Center** (see Figure 15-54).

Note Although NCS and MSE licenses can be fully managed from the License Center, WLC licenses can only be viewed. You must use WLC or CLM to manage WLC licenses.

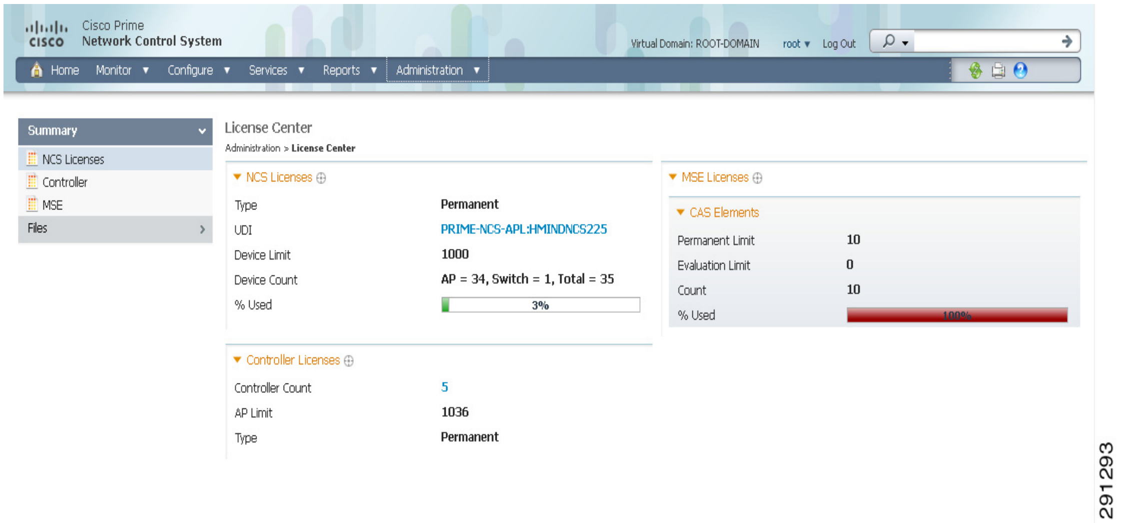
Tip To learn more about the NCS License Center, go to Cisco.com to watch a multimedia presentation. Here you can also find the learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

This section contains the following topics:

- NCS License Information, page 15-132
- WLC Controller License Information, page 15-133
- WLC Controller License Summary, page 15-134
- Mobility Services Engine (MSE) License Information, page 15-136
- Mobility Services Engine (MSE) License Summary, page 15-137

For more information about NCS licenses, see the "NCS Licenses" section on page 1-3.

Figure 15-54 License Center



License Center

Administration > License Center

NCS Licenses

Type	Permanent
UDI	PRIME-NCS-APL:HMINDNCS225
Device Limit	1000
Device Count	AP = 34, Switch = 1, Total = 35
% Used	3%

Controller Licenses

Controller Count	5
AP Limit	1036
Type	Permanent

MSE Licenses

CAS Elements

Permanent Limit	10
Evaluation Limit	0
Count	10
% Used	100%

NCS License Information

The NCS Licenses portion of the License Center page displays the following:

- Feature—The type of license. It can be NCS or DEMO.

- Device Limit—The total number of licensed access points and switches.
- Device Count—The current number of access points and switches using licenses.

Note AP count includes both associated and unassociated access points. When you are near the AP limit, you can delete any unassociated access points to increase available license capacity. For a demo license, you can click the “If you do not have a Product Authorization Key (PAK), please click here for available licenses” link and choose **Wireless Control System Trial License**.

Note Autonomous access points are not counted towards the total device count for your license.

- % Used—The percentage of access points and switches licensed across the NCS. If the percentage drops to 75%, the value appears in red. At this level, a message also appears indicating that both associated and unassociated access points are part of the AP count.
- Type—Permanent if all licenses are permanent. If any licenses are evaluations (or demos), it shows the number of days remaining on the license that has the fewest number of days until expiration.

Note To obtain a new license for the NCS, go to the Product License Registration link

(https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet)

and provide your Product Authorization Key (PAK) and hostname.

Note If you choose **Summary > NCS** from the left sidebar menu, only the NCS license information is displayed.

See the *Cisco Wireless Control System Licensing and Ordering Guide* at this URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd804b4646.html#wp9000156.

It covers selecting the correct SKU, ordering the SKU, installing the software, registering the PAK certificate, and installing the license file on the server.

See the “NCS Licenses” section on page B-1 for more information on licensing enforcement, PAK certificates, license types, and installing and managing NCS licenses.

WLC Controller License Information

The Controller Licensing portion of the License Center page provides the following information for both WPLUS and Base licenses:

- Controller Count—The current number of licensed controllers.

Note Only 5500 series controllers are included in the count. The NCS provides only an inventory view and issues warnings if a license is expiring.

Note Clicking the number in this column is the same as choosing **Summary** > **Controller** from the left sidebar menu, except that it is sorted by the feature you select. This page provides a summary of active controllers.

- AP Limit—The total number of licensed access points.
- Type—The four different types of licenses are as follows:

  Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by the licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license that has the fewest number of days until expiration is shown.
  - Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
  - Grace Period—Licenses are node-locked and metered. These licenses are issued by the licensing portal of Cisco as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

If you need to revoke a license from one controller and install it on another, it is called *rehosting*. You might want to rehost a license to change the purpose of a controller. See Chapter 4, "Performing Maintenance Operations," of the *Cisco Wireless LAN Controller Configuration Guide* for information on rehosting a license.

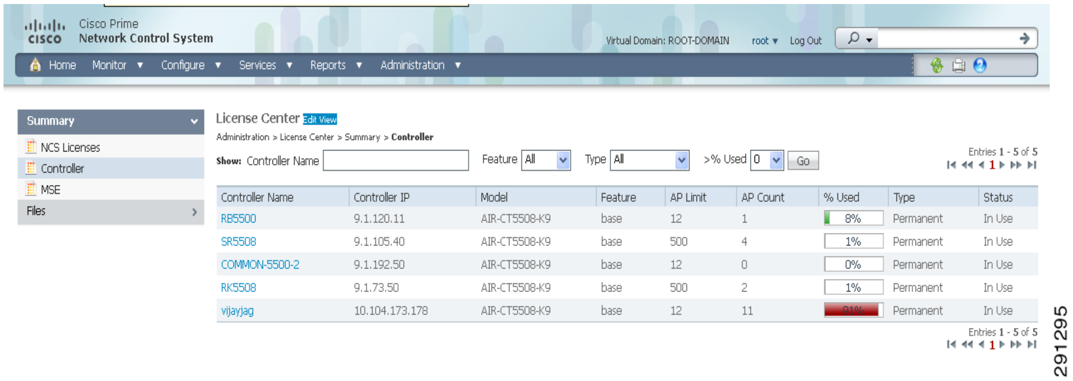
Note The licensing status is updated periodically. To initiate an immediate update, choose **Administration** > **Background Tasks** and run the Controller License Status task.

If your network contains various Cisco licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide. You can download the CLM software and access user documentation at this URL: http://www.cisco.com/go/clm. You can either register a PAK certificate with CLM or with the licensing portal found at the following URL: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet.

WLC Controller License Summary

If you want to see more details about controller licensing, from the left sidebar menu, choose the **Summary > Controller**. The License Center page appears (see Figure 15-55). All currently active licenses on the controller are summarized.

Figure 15-55 License Center (Edit View) Page



License Center

Administration > License Center > Summary > **Controller**

Show: Controller Name Feature All Type All >% Used 0

Controller Name	Controller IP	Model	Feature	AP Limit	AP Count	% Used	Type	Status
RB5500	9.1.120.11	AIR-CT5508-K9	base	12	1	8%	Permanent	In Use
SR5508	9.1.105.40	AIR-CT5508-K9	base	500	4	1%	Permanent	In Use
COMMON-5500-2	9.1.192.50	AIR-CT5508-K9	base	12	0	0%	Permanent	In Use
RK5508	9.1.73.50	AIR-CT5508-K9	base	500	2	1%	Permanent	In Use
vijayjag	10.104.173.178	AIR-CT5508-K9	base	12	11	91%	Permanent	In Use

All licensed controllers and their information in the bulleted list below are displayed. If you want to change how the controller results are displayed, click **Edit View**. In the Edit View page, highlight License Status, and click **Hide** to remove the column from the display.

Above the Controller Summary list is a series of filters that allow you to filter the list by Controller Name, Feature, Type, or Greater Than Percent Used. For example, if you enter 50, the list shows any WLCs that have more than 50% of its licenses used.

Note You can also use the **Advanced Search** link to sort the list of controllers.

- Controller Name—Provides a link to the Files > Controller Files page.
- Controller IP—The IP address of the controller.
- Model—The controller model type.
- Feature—The type of license, either Base or WPLUS. The Base license supports the standard software set, and the WPLUS license supports the premium Wireless Plus (WPLUS) software set. The WPLUS software set provides the standard feature set as well as added functionality for OfficeExtend access points, CAPWAP data encryptions, and enterprise wireless mesh.
- AP Limit—The maximum capacity of access points allowed to join this controller.
- AP Count—The current number of access points using licenses.
- % Used—The percentage of licensed access points that are being used. If the percentage is greater than 75%, the bar appears red to indicate that the limit is being approached.
- Type—The three different types of licenses are as follows:

  Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

- Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
- Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

Note If a license shows as expired, the controller does not stop functioning. Only upon a reboot, the controller with the expired license become inactive.

- Status—In Use, Not in Use, Inactive, or EULA Not Accepted.
  - Inactive—The license level is being used, but this license is not being used.
  - Not In Use—The license level is not being used and this license is not currently recognized.
  - Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
  - Expired Not In Use—The license has expired and can no longer be used.
  - Count Consumed—The ap-count license is In Use.

Mobility Services Engine (MSE) License Information

There are three types of licenses:

- Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
- Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
- Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

The MSE Licenses portion of the License Center page provides information for each service. See (Table 15-10).

Table 15-10 MSE License Information

Field	Description
CAS Elements	
Permanent Limit	The total number of CAS elements with permanent licenses.
Evaluation Limit	The total number of CAS elements with evaluation licenses.

Table 15-10 MSE License Information (continued)

Field	Description
CAS Elements	
Count	The number of CAS elements currently licensed across MSEs.
% Used	The percentage of CAS elements licensed across MSEs.
wIPS Monitor Mode APs	
Permanent Limit	The total number of wIPS Monitor Mode APs with permanent licenses.
Evaluation Limit	The total number of wIPS Monitor Mode APs with evaluation licenses.
Count	The number of wIPS Monitor Mode APs currently licensed across MSEs.
% Used	The percentage of wIPS Monitor Mode APs licensed across MSEs.
Under wIPS Monitor Mode Aps or wIPS Local Mode Aps, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients and tags.	
wIPS Local Mode APs	
Permanent Limit	The total number of wIPS Local Mode APs with permanent licenses.
Evaluation Limit	The total number of wIPS Local Mode APs with evaluation licenses.
Count	The number of wIPS Local Mode APs currently licensed across MSEs.
% Used	The percentage of wIPS Local Mode APs licensed across MSEs.
Under wIPS Monitor Mode APs or wIPS Local Mode APs, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients and tags.	

Note

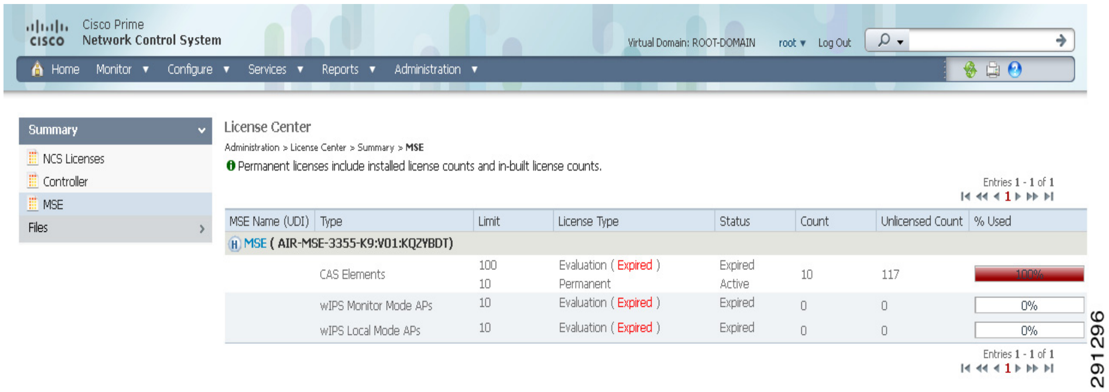
- When a license is deleted, the mobility services engine automatically restarts to load the new license limits.
- If Partner tag engine is up, then the MSE license information consists of information on tag licenses as well.

For more information on MSE licenses, see the "MSE License Overview" section on page 16-90.

Mobility Services Engine (MSE) License Summary

If you want to see more details about MSE licensing, choose **Summary > MSE** from the left sidebar menu. The License Center page appears (see Figure 15-56).

Figure 15-56 License Center Page



License Center

Administration > License Center > Summary > **MSE**

Permanent licenses include installed license counts and in-built license counts.

MSE Name (UDI)	Type	Limit	License Type	Status	Count	Unlicensed Count	% Used
MSE (AIR-MSE-3355-K9:V01:KQZYBDT)							
	CAS Elements	100 10	Evaluation (Expired) Permanent	Expired Active	10	117	100%
	wIPS Monitor Mode APs	10	Evaluation (Expired)	Expired	0	0	0%
	wIPS Local Mode APs	10	Evaluation (Expired)	Expired	0	0	0%

All licensed MSEs are listed in the following columns:

- MSE Name—Provides a link to the MSE license file list page.

Note The icon to the left of the MSE Name/UDI indicates whether the mobility services engine is low-end or high-end.
A high-end mobility services engine (3350) has a higher memory capacity and can track up to 18,000 clients and tags. A low-end mobility services engine (3310) can track up to 2000 clients and tags.

- Type—Specifies the type of MSE.

  Note Under wIPS Monitor Mode APs or wIPS Local Mode APs, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients or tags.

- Limit—Displays the total number of client elements licensed across MSEs.
- Count—Displays the number of client elements that are currently licensed across MSEs.
- Unlicensed Count—Displays the number of client elements that are not licensed.

Note wIPS service does not process the alarms generated from these unlicensed access points.

- % Used—Displays the percentage of clients used across all MSEs.
- License Type—The three different types of licenses are as follows:
  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.

  - Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
- Status
  - Active—License is installed and being used by a feature.
  - Inactive—License is installed but not being used by a feature.
  - Expired—License has expired.
  - Corrupted—License is corrupted.

For more information on MSE licenses, see the "MSE License Overview" section on page 16-90.

Managing NCS Licenses

If you choose Files > NCS Files from the left sidebar menu, you can manage the NCS licenses. This page displays the following information:

- Product Activation Key (PAK)
- Feature
- Access point limit
- Type

This section contains the following topics:

- Adding a New NCS License File, page 15-139
- Deleting an NCS License File, page 15-139

Adding a New NCS License File

To add a new NCS license file, follow these steps:

Step 1 In the License Center > Files > NCS Files page, click **Add**.

Step 2 In the Add a License File dialog box, enter or browse to the applicable license file.

Step 3 Once displayed in the License File text box, click **Upload**.

Deleting an NCS License File

To delete an NCS license file, follow these steps:

Step 1 In the License Center > Files > NCS Files page, select the check box of the NCS license file that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.

Monitoring Controller Licenses

If you choose Files > Controller Files from the left sidebar menu, you can monitor the controller licenses.

Note The NCS does not directly manage controller licenses, rather it simply monitors the licenses. To manage the licenses you can use command-line interface, Web UI, or Cisco License Manager (CLM).

This page displays the following parameters:

- Controller Name
- Controller IP—The IP address of the controller.
- Feature—License features include wplus-ap-count, wplus, base-ap-count, and base.

  For every physical license installed, two license files display in the controller: a feature level license and an ap-count license. For example if you install a “WPlus 500” license on the controller, “wplus” and “wplus-ap-count” features display. There are always two of these features active at any one time that combine to enable the feature level (WPlus or Base) and the AP count.

  Note You can have both a WPlus and Base license, but only one can be active at any given time.

- AP Limit—The maximum capacity of access points allowed to join this controller.
- EULA status—Displays the status of the End User License Agreement and is either Accepted or Not Accepted.
- Comments—User entered comments when the license is installed.
- Type—The four different types of licenses are as follows:
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node locked, their usage is recorded on the device. The number of days left displays for the evaluation license with the fewest number of remaining active license days.
  - Extension—Licenses are node locked and metered. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
  - Grace Period—Licenses are node locked and metered. These licenses are issued by Cisco licensing portal as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

  Note Types other than Permanent display the number of days left until the license expires. Licenses not currently in use do not have their counts reduced until they become “In Use”.

- Status

  - In Use—The license level and the license are in use.
  - Inactive—The license level is being used, but this license is not being used.
  - Not In Use—The license level is not being used and this license is not currently recognized.
  - Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
  - Expired Not In Use—The license has expired and can no longer be used.
  - Count Consumed—The ap-count license is In Use.

Note If you need to filter the list of license files, you can enter a controller name, feature, or type and click **Go**.

Managing Mobility Services Engine (MSE) Licenses

If you choose Files > MSE Files from the left sidebar menu, you can manage the mobility services engine licenses.

This section contains the following topics:

- Registering Product Authorization Keys, page 15-142
- Installing Client and wIPS License Files, page 15-143
- Deleting a Mobility Services Engine License File, page 15-143

The page displays the mobility services engine licenses found and includes the following information:

Note Because tag licenses are added and managed using appropriate vendor applications, tag licenses are not displayed in this page. For more information, see the following URL: http://support.aeroscout.com.
Evaluation (demo) licenses are also not displayed.

Tag licenses are installed using the *AeroScout System Manager* only if the tags are tracked using Partner engine. Otherwise the tags are counted along with the CAS element license.

- MSE License File—Indicates the MSE license.
- MSE—Indicates the MSE name.
- Type—Indicates the type of mobility services engine (client elements, wIPS local mode or wIPS monitor mode access points).
- Limit—Displays the total number of client elements or wIPS monitor mode access points licensed across the mobility services engine.
- License Type—Permanent licenses are the only license types displayed on this page.
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

Registering Product Authorization Keys

You receive a Product Authorization Key (PAK) when you order a client, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for install on the mobility services engine. License files are e-mailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.

Note Tag PAKs are registered with AeroScout. To register your tag PAK, go to this URL: http://www.aeroscout.com/support.

To register a Product Authorization Key (PAK) to obtain a license file for install, follow these steps:

Step 1 Open a browser page and go to www.cisco.com/go/license.

Note You can also access this site by clicking the Product License Registration link located on the License Center page of the NCS.

Step 2 Enter the PAK and click **SUBMIT**.

Step 3 Verify the license purchase. Click **Continue** if correct. The licensee entry page appears.

Note If the license is incorrect, click the **TAC Service Request Tool** link to report the problem.

Step 4 At the Designate Licensee page, enter the mobility service engine UDI in the host ID text box. This is the mobility services engine on which the license is installed.

Note UDI information for a mobility services engine is found in the General Properties group box at Services > Mobility Services Engine > *Device Name* > *System*.

Step 5 Select the **Agreement** check box. Registrant information appears beneath the Agreement check box.

Modify information as necessary.

Note Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.

Step 6 If registrant and end user are not the same person, select the **Licensee (End-User)** check box beneath registrant information and enter the end user information.

Step 7 Click **Continue**. A summary of entered data appears.

Step 8 At the Finish and Submit page, review registrant and end user data. Click **Edit Details** to correct information, if necessary.

Step 9 Click **Submit**. A confirmation page appears.

Installing Client and wIPS License Files

You can install CAS element licenses and wIPS licenses from the NCS.

Note Tag licenses are installed using the *AeroScout System Manager*. For additional information, see the following URL:
http://support.aeroscout.com.

To add a client or wIPS license to the NCS after registering the PAK, follow these steps:

Step 1 Choose **Administration > License Center**.

Step 2 From the left sidebar menu, choose **Files > MSE Files**.

Step 3 In the License Center > Files > MSE Files page, click **Add** to open the Add a License File dialog box.

Step 4 From the MSE Name drop-down list, choose the mobility services engine to which you want to add the license file.

Note Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

Step 5 Enter the license file in the License File text box or browse to the applicable license file.

Step 6 Once displayed in the License File text box, click **Upload**. Newly added license appears in mobility services engine license file list.

Note A Context Aware Service (CAS) restarts if a client or tag license is installed; a wIPS service restarts if a wIPS license is installed.

Note Services must come up before attempting to add or delete another license.

Deleting a Mobility Services Engine License File

To delete a mobility services engine license file, follow these steps:

Step 1 In the License Center > Files > MSE Files page, select the check box of the mobility services engine license file that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.

For more information on licenses, see the "Getting Started" section on page 2-1.