CHAPTER 16

Administrative Tasks

This chapter describes administrative tasks to perform with WCS. These tasks include the following:

Running Background Tasks

Choose **Administration > Background Tasks** to view several scheduled tasks. The Background Tasks window appears (see Figure 16-1).

Figure 16-1 Background Tasks Window

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

Performing a Task

Follow these steps to perform a task (such as scheduling an automatic backup of the WCS database).

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

Step 1 Choose **Administration > Background Tasks** to display the Background Tasks page (see Figure 16-1).

Step 2 On this window, perform one of the following:

- Execute the task now.

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

- Enable the task.

  Click the check box of the task you want to enable. From the Select a command drop-down menu, choose **Enable Collection** and click **GO**. The task converts from grayed out to active after enabling is complete.

- Disable the task.

Click the check box of the task you want to disable. From the Select a command drop-down menu, choose **Disable Collection** and click **GO**. The task is grayed out after the disabling is complete.

- View details of a task.

  Click a URL in the Data Set column to view a specific task. The details on that task appear (see the figure in Figure 16-2).

Note For this example, performing a WCS server backup was selected as the task. The screens and fields to enter on the detailed screens vary based on what task you choose.

Figure 16-2 Detailed Background Task Window

Step 3 Check the **Admin Status** check box to enable it.

Step 4 In the Max Backups to Keep field, enter the maximum number of backup files to be saved on the server.

Range: 7 to 50

Default: 7

Note To prevent the WCS 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 field.

Step 5 In the Interval (Days) field, 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 6 In the Time of Day field, enter the back-up start time. It must be in this format: *hh*:*mm AM/PM* (for example: 03:00 AM).

Note Backing up a large database affects the performance of the WCS server. Therefore, Cisco recommends that you schedule backups to run when the WCS server is idle (such as, in the middle of the night).

Step 7 Click **Submit** to save your settings. The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/root/WCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Configuration Sync

Configuration sync is a new task added in software release 5.1. It allows you to poll all configuration data from the controllers. Any audit (such as a network audit, security index calculation, or RRM audit) performed on the polled and database data is secondary to the configuration sync and can only be performed if this configuration sync task is enabled.

Each of the audits can be enabled separately and run independently of the other audits. If a particular audit requires an immediate run, it can be enabled when the Configuration Sync task is run.

Note If you plan to run the configuration sync task daily, you should enable all audits.

Follow these steps to perform a configuration sync.

Step 1 Choose **Administration > Background Tasks** to display the Background Tasks page (see Figure 16-1).

Step 2 On this window, perform one of the following:

- Execute the task now.

  Click the check box of the task you want to execute. From the Select a command drop-down menu, choose **Execute Now** and click **GO**. You see the status change in the Enabled column.

  <OR>

- Enable the task.

  Click the check box of the task you want to enable. From the Select a command drop-down menu, choose **Enable Task** and click **GO**. The task converts from grayed out to active in the Enabled column.

  <OR>

- Disable the task.

  Click the check box of the task you want to disable. From the Select a command drop-down menu, choose **Disable Task** and click **GO**. The task is grayed out 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 window appears (see Figure 16-3).

Figure 16-3 Task > Configuration Sync

Step 4 In this window you can set the interval and time of day for the task and enable the secondary network audit, security index calculation, and RRM audits tasks.

Step 5 Click **Submit.**

Importing Tasks Into ACS

To import tasks into Cisco Secure ACS server, you must add WCS to an ACS server (or non-Cisco ACS server).

Adding WCS to an ACS Server

Follow these steps to add WCS to an ACS server.

Note The instructions and illustrations in this section pertain to ACS version 4.1 and may vary slightly for other versions or other vendor types. Refer to the CiscoSecure ACS documentation or the documentation for the vendor you are using.

Step 1 Click **Add Entry** on the Network Configuration window of the ACS server (see Figure 16-4).

Figure 16-4 ACS Server Network Configuration Window

.

Step 2 In the AAA Client Hostname field, enter the WCS hostname.

Step 3 Enter the WCS IP address into the AAA Client IP Address field.

Step 4 In the Key field, enter the shared secret that you wish to configure on both the WCS and ACS servers.

Step 5 Choose **TACACS+** in the Authenticate Using drop-down menu.

Step 6 Click **Submit + Apply.**

Adding WCS as a TACACS+ Server

Follow these steps to add WCS to a TACACS+ server.

Step 1 Go to the TACACS+ (Cisco IOS) Interface Configuration window (see Figure 16-5).

Figure 16-5 TACACS+ Cisco IOS Interface Configuration Window

Step 2 In the New Services portion of the window, add Wireless-WCS in the Service column heading.

Step 3 Enter HTTP in the Protocol column heading.

Note HTTP must be in uppercase.

Step 4 Click the check box in front of these entries to enable the new service and protocol.

Step 5 Click **Submit**.

Adding WCS UserGroups into ACS for TACACS+

Follow these steps to add WCS UserGroups into an ACS Server for use with TACACS+ servers.

Step 1 Log into WCS.

Step 2 Navigate to Administration > AAA > Groups. The All Groups window appears (see Figure 16-6).

Figure 16-6 All Groups Window

Step 3 Click on the Task List URL (the Export right-most column) of the User Group that you wish to add to ACS. The Export Task List window appears (see Figure 16-7).

Figure 16-7 Export Task List Window

Step 4 Highlight the text inside of the TACACS+ Custom Attributes, go to your browser's menu, and choose Edit > Copy.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup window appears (see Figure 16-8).

Figure 16-8 Group Setup Window on ACS Server

Step 7 Choose which group to use and click **Edit Settings**. Wireless-WCS HTTP appears in the TACACS+ setting.

Step 8 Use your browser's Edit > Paste sequence to place the TACACS+ custom attributes from WCS into this field.

Step 9 Click the checkboxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

Note To enable TACACS+ in WCS, refer to the "Configuring TACACS+ Servers" section on page 16-23. For information on configuring ACS view server credentials, refer to the "Configuring ACS View Server Credentials" section on page 6-34.

Adding WCS to ACS server for Use with RADIUS

Follow these steps to add WCS to an ACS server for use with RADIUS servers. If you have a non-Cisco ACS server, refer to the "Adding WCS to a Non-Cisco ACS Server for Use with RADIUS" section on page 16-14.

Step 1 Go to Network Configuration on the ACS server (see Figure 16-9).

Figure 16-9 Network Configuration Window on ACS Server

Step 2 Click **Add Entry**.

Step 3 In the AAA Client Hostname field, enter the WCS hostname.

Step 4 In the AAA Client IP Address field, enter the WCS IP address.

Step 5 In the Key field, enter the shared secret that you wish to configure on both the WCS and ACS servers.

Step 6 Choose **RADIUS (Cisco IOS/PIX 6.0)** from the Authenticate Using drop-down menu.

Step 7 Click **Submit + Apply.**

You can now associate ACS users with this ACS group.

Note To enable RADIUS in WCS, refer to the "Configuring RADIUS Servers" section on page 16-24. For information on configuring ACS view server credentials, refer to the "Configuring ACS View Server Credentials" section on page 6-34.

Adding WCS UserGroups into ACS for RADIUS

Follow these steps to add WCS UserGroups into an ACS Server for use with RADIUS servers.

Step 1 Log into WCS.

Step 2 Navigate to Administration > AAA > Groups. The All Groups window appears (see Figure 16-10).

Figure 16-10 All Groups Window

Step 3 Click on the Task List URL (the Export right-most column) of the User Group that you wish to add to ACS. The Export Task List window appears (see Figure 16-11).

Figure 16-11 Export Task List Window

Step 4 Highlight the text inside of the RADIUS Custom Attributes, go to your browser's menu, and choose **Edit > Copy**.

Step 5 Log in to ACS.

Step 6 Go to Group Setup. The Group Setup window appears (see Figure 16-12).

Figure 16-12 Group Setup Window on ACS Server

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 your browser's Edit > Paste sequence to place the RADIUS custom attributes from WCS into this field.

Step 9 Click the checkboxes to enable these attributes.

Step 10 Click **Submit + Restart**.

You can now associate ACS users with this ACS group.

Note To enable RADIUS in WCS, refer to the "Configuring RADIUS Servers" section on page 16-24. For information on configuring ACS view server credentials, refer to the "Configuring ACS View Server Credentials" section on page 6-34.

Adding WCS to a Non-Cisco ACS Server for Use with RADIUS

When you use a RADIUS server to log into WCS, the AAA server sends back an access=accept message with a usergroup 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\WCS5.0\webnms\webacs\WEB-INF\security\usergroup-map.xml. The tasks are

passed back as a vendor specific attribute (VSA), and WCS requires authorization information using the VSA (IETF RADIUS attribute number 26). The VSA contains the WCS RADIUS task list information (refer to Figure 16-13).

Figure 16-13 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 WCS task information (for example Wireless-WCS: task0 = Users and Group)

Each line from the WCS 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 16-1 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 ....Wireless-WCS
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 ...%Wireless-WCS
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 Wireless-WCS:task
0080 31 3d 41 75 64 69 74 20 54 72 61 69 6c 73 xx xx 1=Audit Trails.*
```

Table 16-1 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 WCS to read
25 (37 bytes in decimal)	Length

Table 16-1 Access=Access Packet Example (continued)

Attribute	Description
hex text string	Wireless-WCS: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.

Setting AAA Mode

Follow these steps to choose a AAA mode.

Step 1 Choose **Administration > AAA.**

Step 2 Choose **AAA Mode** from the left sidebar menu. The AAA Mode Setting window appears (see Figure 16-14).

Figure 16-14 AAA Mode Settings Window

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 Click the **Fallback to Local** check box if you want the administrator to use the local database when the external AAA server is down.

Note This option is unavailable if *Local* was selected as a AAA mode type.

Step 5 Click **OK**.

Auto Provisioning

Auto provisioning allows WCS to automatically configure a new or replace a current wireless LAN controller. The WCS auto provisioning feature can simplify deployments for customers with a large number of controllers.

Note For auto provisioning privileges, you must have Admin, Root, or SuperUser status.

Note To allow or disallow auto provisioning privileges to a user, edit the permitted tasks using the Administration > AAA > Groups > <group name> List of Tasks Permitted section of WCS. Select or deselect the check box to allow or disallow these privileges.

Follow these steps to configure auto provisioning.

Step 1 Choose **Configure > Auto Provisioning**. The Auto Provisioning Filter List window appears (see Figure 16-15).

Figure 16-15 Auto Provisioning Filter List

Step 2 Choose **Auto Provisioning Device Management** from the left sidebar menu. This allows you to create and edit auto provisioning filters which define the list of allowable devices to be auto provisioned or auto monitored by WCS.

Note Auto provisioning startup files generated by WCS are kept in the TFTP root directory. This directory is not backed up as part of the WCS backup; therefore, if data is restored on to another machine, the startup files will not get restored. You must manually backup the TFTP folder to preserve the auto provisioning startup files.

You cannot use a template to replicate the configuration on a second controller during auto provisioning. The dynamic interfaces must be created separately so that any WLAN or AP groups (or any other key format values) that are mapped to dynamic interfaces function as expected. Regardless of which format (ASCII or hexadecimal) you choose, for security reasons, only ASCII is visible on WLC.

Step 3 The Auto Provisioning Filter List window displays the following information:

- Filter Name: Name of the filter
- Filter Enable: Indicates whether or not the filter is enabled.

Note Only enabled filters can participate in the auto provisioning process.

- Filter Mode: Indicates the search mode for this filter (host name, MAC address, or serial number).
- Config Group Name: Indicates the configuration group name.

Step 4 From the Select a command drop-down menu, you can choose to add or delete a filter or list some or all filter device information. If you choose to add a new filter, continue to Step 5.

Step 5 From the Select a command drop-down menu, choose **Add Filter**.

Step 6 Click **GO**. The Auto Provisioning Filters > New Filter window appears (see Figure 16-16).

Figure 16-16 Auto Provisioning Filters > New Filter

Step 7 Configure the following information:

- General
  - Enable Filter: Click the check box to enable the new filter.

    Note Only enabled filters can participate in the Auto Provisioning process.

  - Filter Name: Enter a filter name.
- Filter Properties
  - Monitor Only: When contacted by WCS during the auto provisioning process, the WLC defined in this filter is managed, but not configured, by WCS.
  - Filter Mode: From the drop-down menu, choose **Host Name**, **MAC Address**, and **Serial Number** to indicate the search mode for this filter.
  - Config Group Name: From the drop-down menu, choose a **Config Group Name**.

    Note An empty config group with no controllers defined must be created so that all config groups appear in the drop-down list.

- Filter Member Management - Add Member
  - Input Type: From the drop-down menu, choose **Single Device** or **CSV file**.

    If Single Device is selected, enter the Host Name, Management Interface IP Address, Management Interface Netmask, Management Interface Gateway, LAG, AP manager interface IP address, AP manager interface network mask, AP manager interface gateway IP address, and DHCP information.

If CSV File is chosen, enter the CSV file or use the **Browse** button to navigate to the applicable CSV File. An example of a valid CSV file (with MAC address filter mode) is as follows:

```
deviceId, LAG, managementIP, managementNetmask, managementGateway, apManagerIP,
apManagerNetmask, apManagerGateway, dhcpServerIP
00:0B:85:46:F2:60, true, 1.9.116.39, 255.255.255.0, 1.9.116.1, 2.9.116.39,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:61, true, 1.9.116.40, 255.255.255.0, 1.9.116.1, 2.9.116.40,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:62, false, 1.9.116.41, 255.255.255.0, 1.9.116.1, 2.9.116.41,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:63, false, 1.9.116.42, 255.255.255.0, 1.9.116.1, 2.9.116.42,
255.255.255.0, 2.9.116.1, 2.9.116.250
00:0B:85:46:F2:64, false, 1.9.116.43, 255.255.255.0, 1.9.116.1, 2.9.116.43,
255.255.255.0, 2.9.116.1, 2.9.116.250
```

The first line in the CSV file must be keyword "deviceId, LAG, managementIP, managementNetmask, managementGateway, apManagerIP, apManagerNetmask, apManagerGateway, dhcpServerIp."

Each of the following lines should contain nine tokens as follows, separated by commas:

1st token can be host name, MAC address, or serial number depending on the selected filter mode.

2nd token is the controller's LAG configuration (true/false).

3rd token is the controller's management interface IP address.

4th token is the controller's management interface network mask.

5th token is the controller's management interface gateway IP.

6th token is the controller's AP Manager interface IP address.

7th token is the controller's AP Manager interface network mask.

8th token is the controller's AP Manager interface Gateway IP.

9th token is the controller's DHCP IP address.

- Host Name
- LAG Configuration: Enabled or Disabled.
- Management Interface IP Address
- Management Interface Netmask
- Management Interface Gateway
- AP Manager Interface IP Address
- AP Manager Interface Netmask
- AP Manager Interface Gateway
- DHCP IP Address

Step 8 Click **Submit**.

Viewing Detailed Auto Provisioning Device Information

To view detailed information about auto provisioning devices, choose **List Filters Device Info** or **List All Filters Device Info** from the Select a command drop-down menu. The Detailed Auto Provisioning Device window appears (see Figure 16-17). The filter name, its device ID, and the IP address, netmask, and gateway address are provided.

The status displays as idle, trap received, failed in trap processing, failed in applying templates, failed in discovery switch, managed, managed partially applied templates, or unknown error.

Figure 16-17 Detailed Auto Provisioning Device Information

Editing a Current Auto Provisioning Filter

Follow these steps to edit a current auto provisioning filter.

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Click the Filter Name of the filter you want to edit.

Step 3 Make the necessary changes to the current filter parameters.

Step 4 Click **Submit**.

Deleting an Auto Provisioning Filter

Follow these steps to delete an auto provisioning filter.

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Choose the check box of the file you want to delete.

Step 3 From the Select a command drop-down menu, choose **Delete Filter(s)**.

Step 4 Click **GO**.

Step 5 Click **OK** to confirm the deletion.

Viewing Details of an Auto Provisioned Filter

To view details for an individual auto provisioning filter, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 Choose the check box of the filter you want to view.

Step 3 From the Select a command drop-down menu, choose **List Filter(s) Device Info**.

Step 4 Click **GO**.

The following information is provided for the selected filter.

Table 16-2 List Filter(s) Device Information

Parameter	Description
Filter Name	Indicates the filter name.
Device ID	Indicates the device ID.
Interface IP	Indicates the management interface IP address of the controller.
Interface Netmask	Indicates the netmask mask of the management interface of the controller.
Interface Gateway	Indicates the netmask gateway of the management interface of the controller.
Status	
Timestamp	

Setting Auto Provisioning

The Primary Search Key Setting provides the ability to set the matching criteria search order.

To indicate the Search Key Order, follow these steps:

Step 1 Choose **Configure > Auto Provisioning**.

Step 2 From the left sidebar menu, choose **Auto Provisioning Setting**. The Auto Provisioning Primary Search Key Setting appears.

Step 3 Click to highlight the applicable search key.

Step 4 Use the **Move Up** or **Move Down** buttons to move the Search Key to a higher or lower priority.

Step 5 Click **Save** to confirm or Cancel to cancel the changes.

Turning Password Rules On or Off

You have the ability to customize the various password rules to meet your criteria. Follow these steps to customize the password rules.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Local Password Policy**. The password rules are displayed individually, and each has a check box in front of it.

Step 3 Click the check boxes to enable the rules you want. The rules are as follows:

Note All rules are on by default.

- Password minimum length is 8 characters (the length configurable).
- Password cannot contain username or the reverse of the username.
- Password cannot be cisco or ocsic (Cisco reversed).
- Root password cannot be *public*.
- No character can be repeated more than three times consecutively in the password.
- Password must contain characters from three of the character classes: uppercase, lowercase, digits, and special characters.

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.

Note In order to activate TACACS+ servers, you must enable them as described in the "Importing Tasks Into ACS" section on page 16-5.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **TACACS+**. The TACACS+ window appears (see Figure 16-18).

Figure 16-18 TACACS+ Window

Step 3 The TACACS+ window shows the TACACS+ server's IP address, port, retransmit rate, and authentication type (Password Authentication Protocol (PAP)) or Challenge Handshake Authentication Protocol (CHAP). 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 re-add the desired ones in the preferred order.

Step 4 Use the drop-down menu in the upper right-hand corner to add or delete TACACS+ servers. You can click on 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 menu to choose either ASCII or hex shared secret format.

Step 6 Enter the TACACS+ shared secret used by your specified server.

Step 7 Re-enter the shared secret in the Confirm Shared Secret field.

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 will be attempted.

Step 10 In the Authentication Type drop-down menu, choose a protocol: PAP or CHAP.

Step 11 Click **Submit**.

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 in order to make configuration changes.

Note In order to activate RADIUS servers, you must enable them as described in the "Importing Tasks Into ACS" section on page 16-5.

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **RADIUS**. The RADIUS window appears (see Figure 16-19).

Figure 16-19 RADIUS Window

Step 3 The RADIUS window 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 re-add the desired ones in the preferred order.

Step 4 Use the drop-down menu in the upper right-hand corner to add or delete RADIUS servers. You can click on an IP address if you want to make changes to the information. When you click on a particular IP address, the window shown in Figure 16-20 appears.

Figure 16-20 RADIUS Server Detailed Window

Step 5 The current authentication port is displayed. Use the drop-down menu to choose either ASCII or hex shared secret format.

Step 6 Enter the RADIUS shared secret used by your specified server.

Step 7 Re-enter the shared secret in the Confirm Shared Secret field.

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 will be attempted.

Step 10 In the Authentication Type drop-down menu, choose a protocol: PAP or CHAP.

Step 11 Click **Submit**.

Establishing Logging Options

Use **Administration > Logging** to access the Administer Logging Options page. This logging function is related only to WCS logging and not syslog information. The logging for controller syslog information can be done on the Controller > Management > Syslog window.

Follow the steps below to enable e-mail logging. The settings you establish are stored and are used by the e-mail server.

Step 1 Choose A**dministration > Logging.** The Logging Options menu appears (see Figure 16-21).

Figure 16-21 Logging Options Window

Step 2 Choose a message level option of Trace, Information, or Error in the General portion of the window.

Step 3 Click the check boxes within the Log Modules portion of the window to enable various administration modules (such as performance, status, object, configuration, monitor, fault analysis, SNMP mediation, general, location servers, XML mediation, asynchronous, and portal).

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.

Performing Data Management Tasks

Within the Settings window, you can determine what data to generate for reports and e-mails. Choose **Administration > Settings** in the left sidebar menu. Three choices appear.

- Refer to the "Data Management" section on page 16-28 to establish trends for hourly, daily, and weekly data periods.
- Refer to the "Report" section on page 16-29 to designate where the scheduled reports will reside and for how long.
- Refer to the "Mail Server" section on page 16-29 to set the primary and secondary SMTP server host and port.
- Refer to the "Login Disclaimer" section on page 16-31 to enter disclaimer information.
- Refer to the "Alarms" section on page 16-31 to specify how to handle old alarms and how to display assigned and acknowledged alarms in the Alarm Summary window.
- Refer to the "Client" section on page 16-32 to enable client troubleshooting on a diagnostic channel.
- Refer to the "Severity Configurations" section on page 16-32 to configure the severity level for newly-generated alarms.

- Refer to the "Notification Receiver" section on page 16-32 to configure parameters for notification support of guest access functionality.
- Refer to the "SNMP Settings" section on page 16-33 to configure global SNMP settings from WCS.
- Refer to "Audit" section on page 16-34 to configure audit information.
- Refer to the "Auto Refresh" section on page 16-34 for information on controller upgrade settings.

Data Management

Follow the steps below to manage data aggregation on an hourly, daily, and weekly basis.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Data Management**. The Data Management window appears (see Figure 16-22).

Figure 16-22 Data Management Window

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

Step 4 Specify the number of days to keep the daily data. The valid range is 7 to 31.

Step 5 Specify the number of weeks to keep the weekly data. The valid range is 2 to 10.

Step 6 Specify the number of days to retain the audit data before purging. The limit is 90 days, and the minimum cleanup interval is 7 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**.

Report

Follow the steps below to indicate where the scheduled reports will reside and for how many days.

Step 1 Choose **Administration > Setting**.

Step 2 From the left sidebar menu, choose **Report**. The Report window appears (see Figure 16-23).

Figure 16-23 Report Window

Step 3 Enter the location on the WCS server where you want the scheduled reports to reside on the server.

Step 4 Specify the number of days the file will stay in the repository.

Step 5 Click **Save**.

Mail Server

You can configure global e-mail parameters to use when sending e-mails from WCS reports, alarm notifications, and so on. This mail server page allows you to configure e-mail parameters at a single place to avoid re-entering the information each time you need it. The Mail Server window allows you to set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail address(es). Follow these steps to configure global e-mail parameters.

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

Step 1 Choose **Administration > Setting**.

From the left sidebar menu, choose **Mail Server**. The window in Figure 16-24 appears.

Figure 16-24 Mail Server Configuration Window

The Mail Server window allows you to set the primary and secondary SMTP server host and port, the sender's e-mail address, and the recipient's e-mail address. From this window, you can configure e-mail parameters without having to visit multiple places.

You must designate the primary mail server, and the secondary one is used only if the primary fails. SMTP authorization is also supported for both primary and secondary mail servers. Follow the steps below to configure the mail server.

Step 1 Enter the host name of the primary SMTP server.

Step 2 The SMTP port is set to 25 by default, but you can change it if your mail server is using a non-default port.

Step 3 Enter the designated username if SMTP authorization is turned on for this mail server.

Step 4 Provide a password for logging on to the SMTP server and enter it for the Password and Confirm Password parameter.

Step 5 Provide the same information for the secondary SMTP server (only if a secondary mail server is available). The secondary server is used only if the primary fails.

Step 6 The From field in the Sender and Receivers portion of the window is populated with *WCS@<WCS server IP address>*. You can change it to a different sender.

Step 7 Enter the recipient's e-mail address(es) in the To field. The e-mail address you provide serves as the default values for other functional areas, such as alarms or reports. Multiple e-mail addresses can be added and should be separated by a comma.

Note If you make global changes to the recipient e-mail address(es) in Step 7, they are disregarded if e-mail notifications were set.

You are required to set the primary SMTP mail server and the From address fields.

Step 8 Click the **Test** button to send a test e-mail using the parameters you configured. The results of the test operation are shown on the same screen. The test feature checks the connectivity to both primary and secondary mail servers by sending an e-mail with a "WCS test e-mail" subject line.

Step 9 If the test results were satisfactory, click **Save**.

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**.

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

Step 4 Click **Save**.

Alarms

This Alarms page allows you to manage the following:

- The handling of old alarms.
- The display of assigned and acknowledged alarms in the Alarm Summary window.

To access this window, follow these steps:

Step 1 Choose **Administration > Settings**.

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

Step 3 In the Cleanup of Old Alarms section, check the check box to enable the deletion of old alarms.

Step 4 Enter the number of days after which old alarms are deleted.

Step 5 In the Alarm Summary Window section, check the check box to hide acknowledged and assigned alarms on the Alarm Summary window. This preference applies only to the Alarm Summary window. A quick search or alarms for any entity show alarms regardless of the acknowledged or assigned state specified here. The default is to hide acknowledged alarms.

Client

From the Settings > Client window, you can enable automatic client troubleshooting on a diagnostic channel. Refer to the "WLAN Client Troubleshooting" section on page 6-20 for further information on client troubleshooting. Follow these steps:

Step 1 Choose **Administration > Settings**.

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

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

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

Step 4 Click **Save**.

Severity Configurations

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 > Setting**.

Step 2 Choose **Severity Configuration** from the left sidebar menu.

Step 3 Choose the check box of the alarm condition for which you want to change the severity level.

Step 4 From the **Configure Severity Level** drop-down menu, 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.

Notification Receiver

The Notification Receiver page allows you to configure parameters for notification support of guest access functionality.

Follow these steps to configure notification receiver parameters:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Notification Receiver**.

Step 3 Enter the Notification Type parameter including Port Number and Community.

Note The Notification Type automatically defaults to SNMP.

Step 4 Click **Submit** to confirm the Notification Receiver information.

SNMP Settings

The SNMP Settings window allows you to configure global SNMP settings from WCS.

Note Any changes made on this screen take effect globally for WCS and are saved across restarts as well as across backups and restores.

Follow these steps to configure global SNMP settings.

Step 1 Choose **Administration > Settings**.

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

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

Note The default is unchecked for security reasons.

Step 4 For the Backoff Algorithm, choose either **Exponential** or **Constant Timeout** from the drop-down menu. 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 WCS defaults to the global Reachability Retries and Timeout that you configure. If unchecked, WCS always uses the timeout and retries specified per-controller or per-IOS access point. The default is checked.

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

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

Step 8 At the Maximum VarBinds per PDU parameter, 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 Click **Save** to confirm these settings.

Audit

The Controller Audit Report displays the following information depending on the type of audit selected in Administration > Settings > Audit:

- Applied template discrepancies (Template Based Audit only)
- Config group template discrepancies (Template Based Audit only)
- Total enforcements for config groups with background audit enabled (Template based Audit only)
  - If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from WCS.
- Failed for config groups with background audit enabled (Template Based Audit only)
  - If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view the failures returned from the device.
- Other WCS discrepancies

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

Note You can audit a controller by selecting **Audit Now** from the Select a command drop-down menu in the Configure > Controllers window or by clicking **Audit Now** directly from the Controller Audit report. See the "Viewing Audit Status (for Controllers)" section on page 10-5.

Auto Refresh

The Auto Refresh page allows you to automatically upgrade the controller. Follow these steps to perform an automatic refresh.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Controller Upgrade Settings** (see Figure 16-25).

Figure 16-25 Controller Upgrade Settings

Step 3 Check the Auto refresh After Upgrade check box to automatically restore the config whenever there is a change in the WLC image.

Step 4 Click **Save**.

Setting User Preferences

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

Step 1 Choose **Administration > User Preferences**. The User Preferences Window appears (see Figure 16-26).

Figure 16-26 User Preferences Window

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

Step 3 If you want the maps and alarms page to automatically refresh when a new alarm is raised by WCS, click the check box in the Alarms portion of the window.

Step 4 Use the drop-down menu to indicate how often you want the alarm count refreshed in the Alarm summary window on the left panel.

Step 5 Click **Save**.