CHAPTER 8

Configuring Mobility Groups

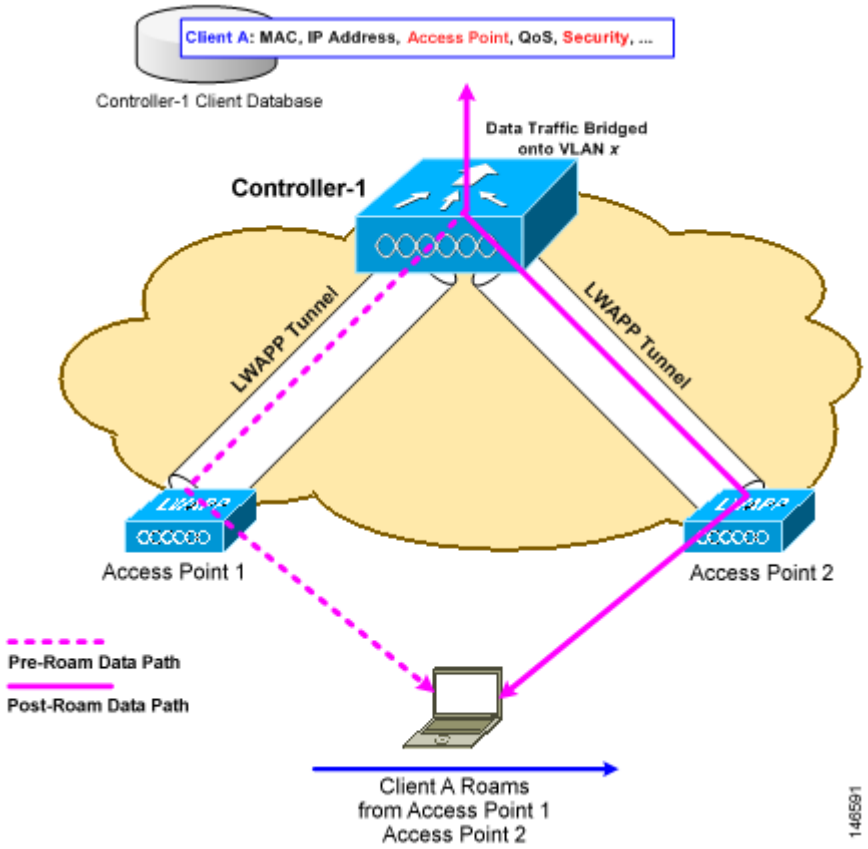
This chapter describes mobility groups and explains how to configure them on WCS. It contains these sections:

Overview of Mobility

Mobility, or *roaming*, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the access point's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLANs, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client. Figure 8-1 illustrates a wireless client roaming from one access point to another when both access points are joined to the same controller.

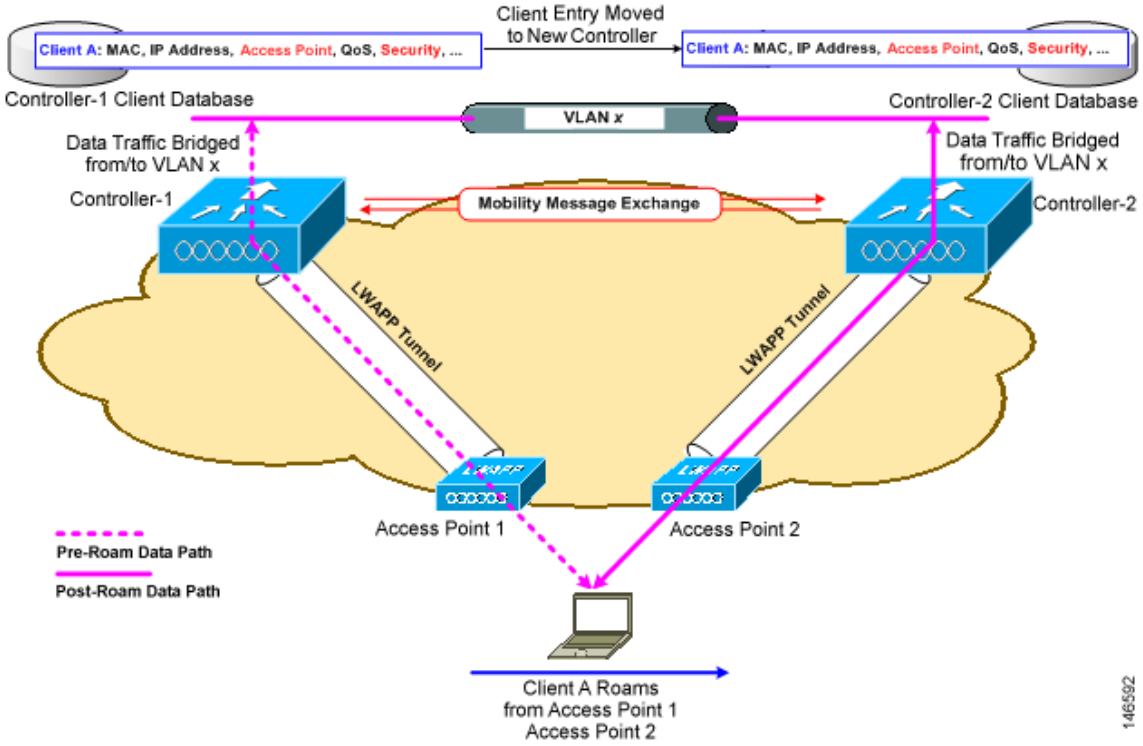
Figure 8-1 Intra-Controller Roaming



When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. The process also varies based on whether the controllers are operating on the same subnet. Figure 8-2 illustrates *inter-controller roaming*, which occurs when the controllers' wireless LAN interfaces are on the same IP subnet.

Figure 8-2 Inter-Controller Roaming

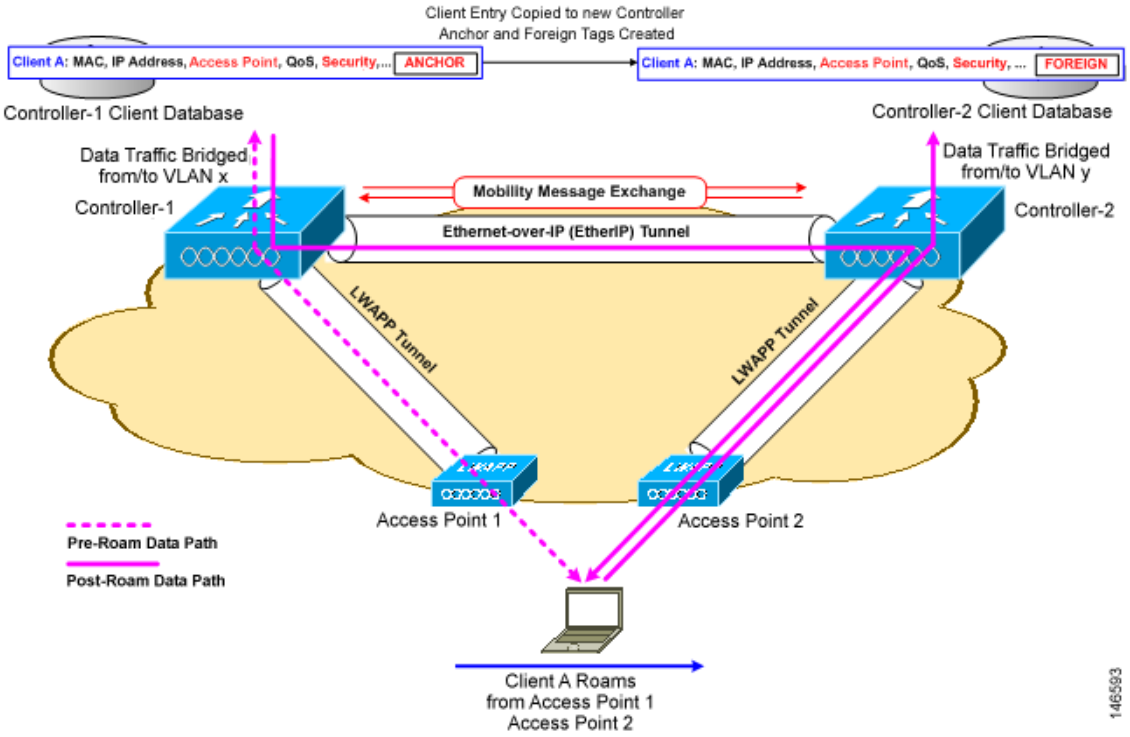


When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains invisible to the user.

Note All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication in order to comply with the IEEE standard.

Figure 8-3 illustrates *inter-subnet roaming*, which occurs when the controllers' wireless LAN interfaces are on different IP subnets.

Figure 8-3 Inter-Subnet Roaming



Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on how the client roams. However, instead of moving the client database entry to the new controller, the original controller marks the client with an "Anchor" entry in its own client database. The database entry is copied to the new controller client database and marked with a "Foreign" entry in the new controller. The roam remains invisible to the wireless client, and the client maintains its original IP address.

After an inter-subnet roam, data flows in an asymmetric traffic path to and from the wireless client. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.

In inter-subnet roaming, WLANs on both anchor and foreign controllers need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients may have network connectivity problems after the handoff.

Note Currently, multicast traffic cannot be passed during inter-subnet roaming. In other words, avoid designing an inter-subnet network for Spectralink phones that need to send multicast traffic while using push to talk.

Note Both inter-controller roaming and inter-subnet roaming require the controllers to be in the same mobility group. See the next two sections for a description of mobility groups and instructions for configuring them.

Symmetric Tunneling

With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has reverse path filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. You enable or disable symmetric tunneling by choosing Configure > Controller and then System > General from the left sidebar menu.

Note All controllers in a mobility group should have the same symmetric tunneling mode.

Note For symmetric tunneling to take effect, a reboot is required.

With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

Refer to the "Configuring General Templates" section on page 11-4 for instructions on configuring this feature within a template.

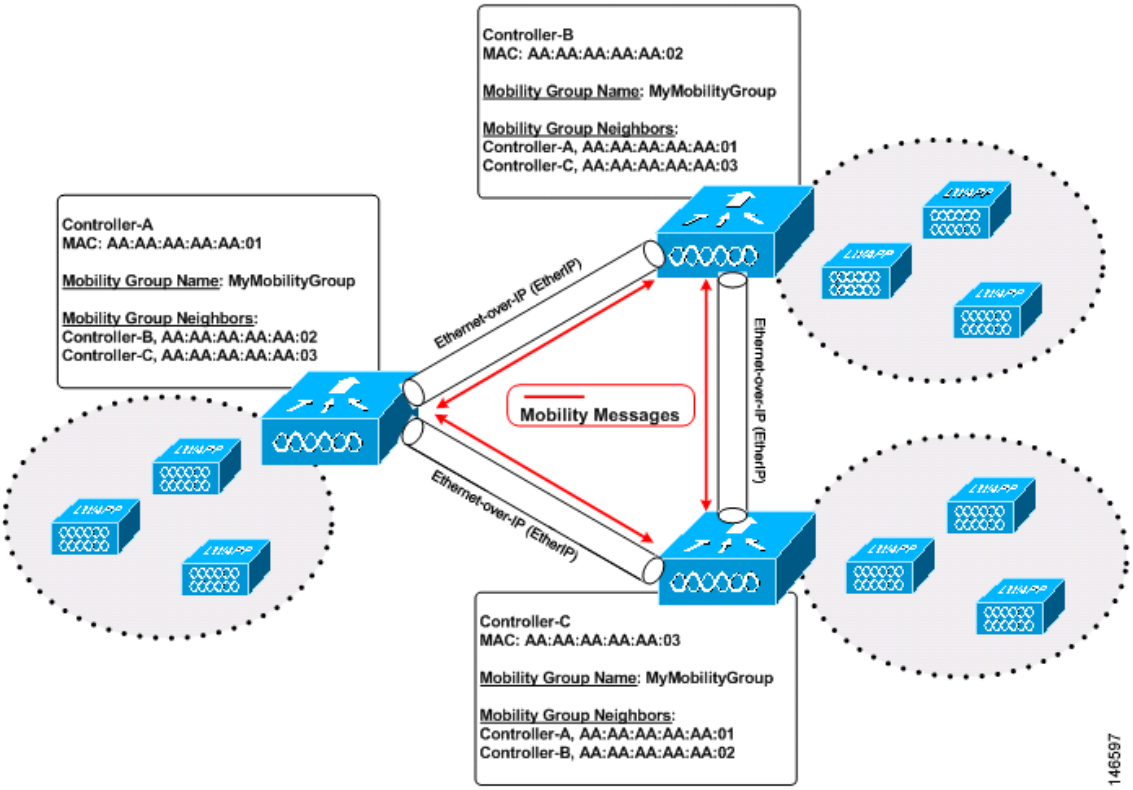
Overview of Mobility Groups

A set of controllers can be configured as a *mobility group* to allow seamless client roaming within a group of controllers. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

Note Clients do not roam across mobility groups.

Figure 8-4 shows an example of a mobility group.

Figure 8-4 A Single Mobility Group



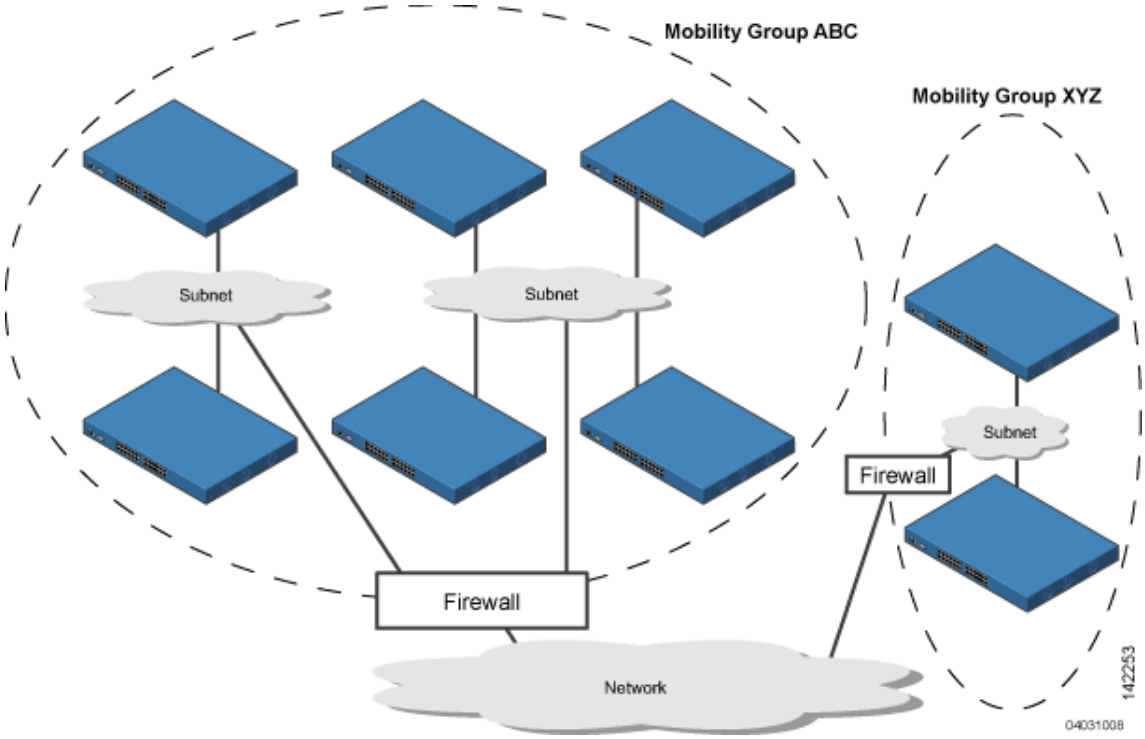
As shown above, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over an LWAPP tunnel.

Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting of 24 4404-100 controllers supports up to 2400 access points (24 * 100 = 2400 access points).
2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group consisting of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless network. Figure 8-5 shows the results of creating distinct mobility group names for two groups of controllers.

Figure 8-5 Two Mobility Groups



The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

Note Clients may roam between access points in different mobility groups, provided they can detect them. However, their session information is not carried between controllers in different mobility groups.

When to Include Controllers in a Mobility Group

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Messaging among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. In WCS and controller software releases 5.0, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list

  The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it. In WCS and controller software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in controller software release 5.0, the controller sends the message only to those members that are in the same group as the controller and then includes all of the other members while sending retries.

- Sending Mobile Announce messages using multicast instead of unicast

  In WCS and controller software releases prior to 5.0, the controller may be configured to use multicast to send the mobile announce messages, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, PMK Update, AP List Update, and IDS Shun) are meant for all members in the group. In WCS and controller software releases 5.0, the controller uses multicast mode to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group containing all the mobility members. To derive the maximum benefit from multicast messaging, Cisco recommends that it be enabled or disabled on all group members.

Configuring Mobility Groups

This section provides instructions for configuring mobility groups.

Note You can also configure mobility groups using the controller. Refer to the *Cisco Wireless LAN Controller Configuration Guide* for instructions.

Prerequisites

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same LWAPP transport mode (Layer 2 or Layer 3).

  Note You can verify and, if necessary, change the LWAPP transport mode on the System > General page.

- IP connectivity must exist between the management interfaces of all devices.

  Note You can verify IP connectivity by pinging the controllers.

- All controllers must be configured with the same mobility group name.

  Note For the Cisco WiSM, both controllers should be configured with the same mobility group name for seamless routing among 300 access points.

- All devices must be configured with the same virtual interface IP address.

Note If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the hand-off does not complete, and the client loses connectivity for a period of time.

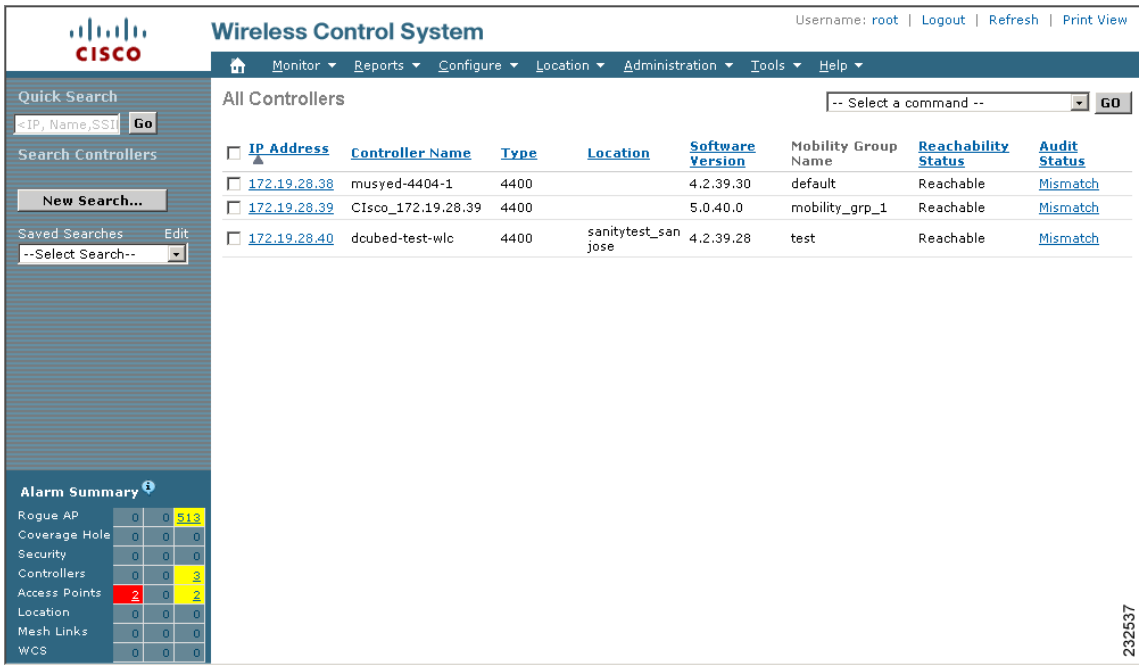
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.

Note You can find the MAC and IP addresses of the other controllers to be included in the mobility group on the Configure > Controllers page.

Follow these steps to add each WLC controller into mobility groups and configure them.

Step 1 Navigate to **Configure > Controllers** (see Figure 8-6).

Figure 8-6 Configure > Controllers



This page shows the list of all the controllers you added in Step 1. The mobility group names and the IP address of each controller that is currently a member of the mobility group is listed.

Step 2 Choose the first controller by clicking on the WLC IP address. You will then access the controller templates interface for the controller you are managing.

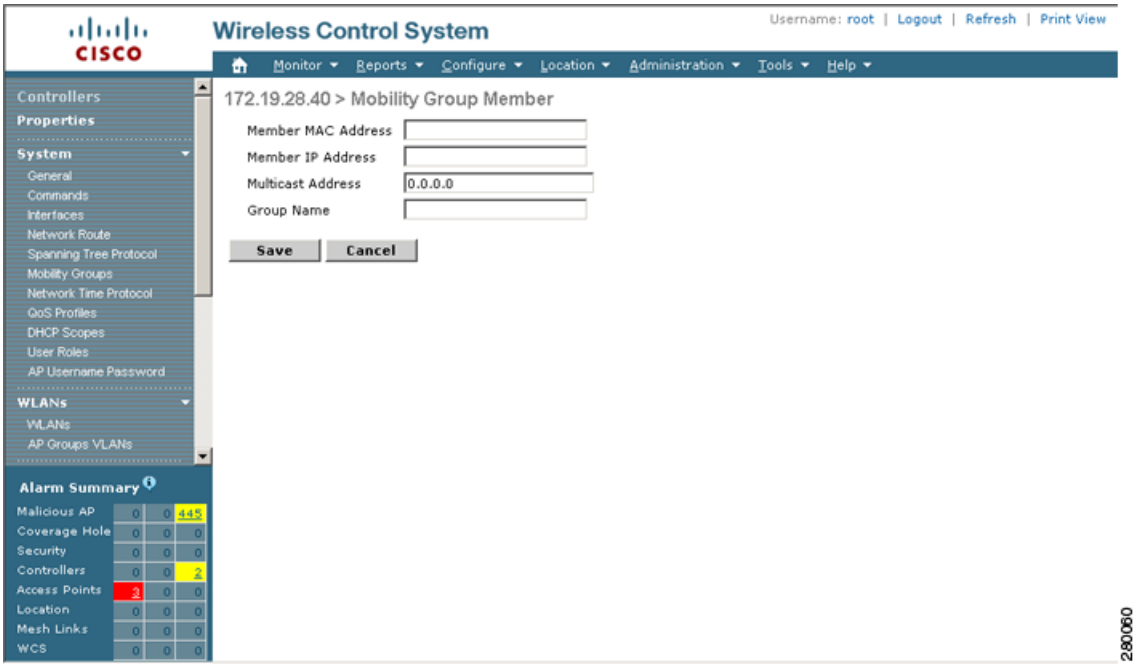
Step 3 Choose **System > Mobility Groups** on the left-hand side. The existing Mobility Group members are listed in the window (see Figure 8-7).

Figure 8-7 Existing Mobility Groups

Step 4 You will see a list of available controllers. From the Select a command drop-down menu in the upper right-hand corner, choose **Add Group Members** and then click **GO**.

Step 5 If no controllers were found to add to the mobility group, you can add the members manually by clicking the "To add members manually to the Mobility Group click here" message. The Mobility Group Member window appears.

Figure 8-8 Mobility Group Member Window



Step 6 In the Member MAC Address field, enter the MAC address of the controller to be added.

Step 7 In the Member IP Address field, enter the management interface IP address of the controller to be added.

Note If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller's management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

Step 8 Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address field. The local mobility member's group address must be the same as the local controller's group address.

Step 9 In the Group Name field, enter the name of the mobility group.

Step 10 Click **Save**.

Step 11 Repeat the above steps for the remaining WLC devices.

Setting the Mobility Scalability Parameters

Follow these steps to set the mobility message parameters.

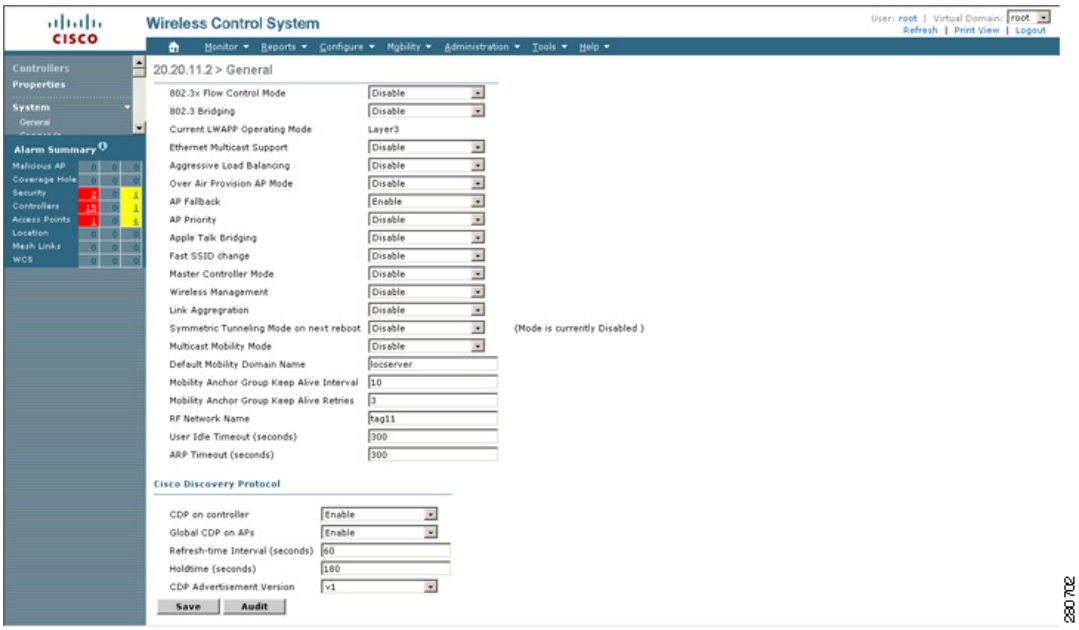
Note You must complete the steps in the "Configuring Mobility Groups" section on page 8-8 prior to setting the mobility scalability parameters.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose an IP address of a controller whose software version is 5.0 or later.

Step 3 Choose **System > General** from the left sidebar menu. The General window as shown in Figure 8-9 appears.

Figure 8-9 System > General Window



Step 4 At the Multicast Mobility Mode parameter, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

Step 5 If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address parameter to begin multicast mobility messaging. You must configure this IP address for the local mobility group, but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

Step 6 Click **Save**.

Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the client's entry point into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as, a lobby, a restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

Note A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controller can have a 4100 series controller or a 4400 series controller as its anchor.

Note The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

Configuring Mobility Anchors

Follow these steps to create a new mobility anchor for a WLAN.

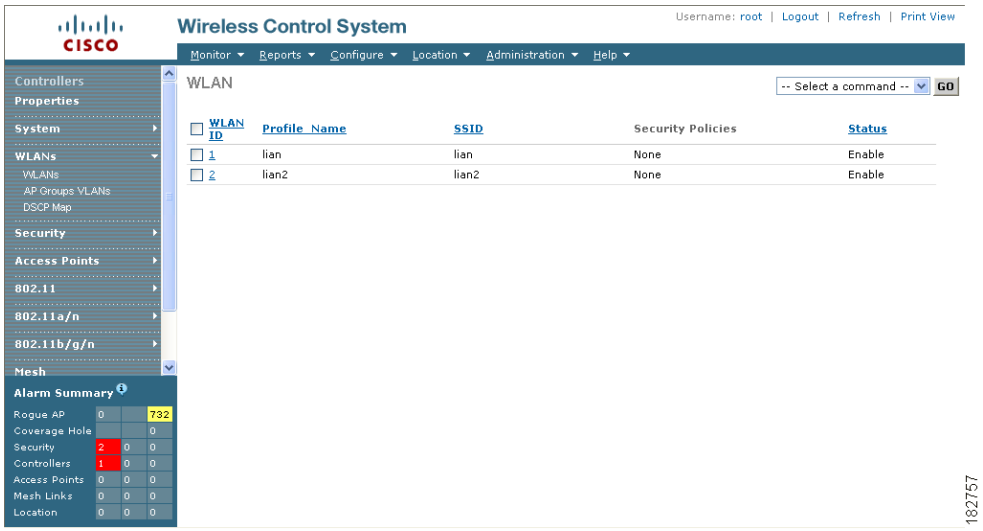
Step 1 Click **Configure > Controllers.**

Step 2 Choose a controller by clicking an IP address.

Step 3 Choose **WLANs > WLANs** from the left sidebar menu.

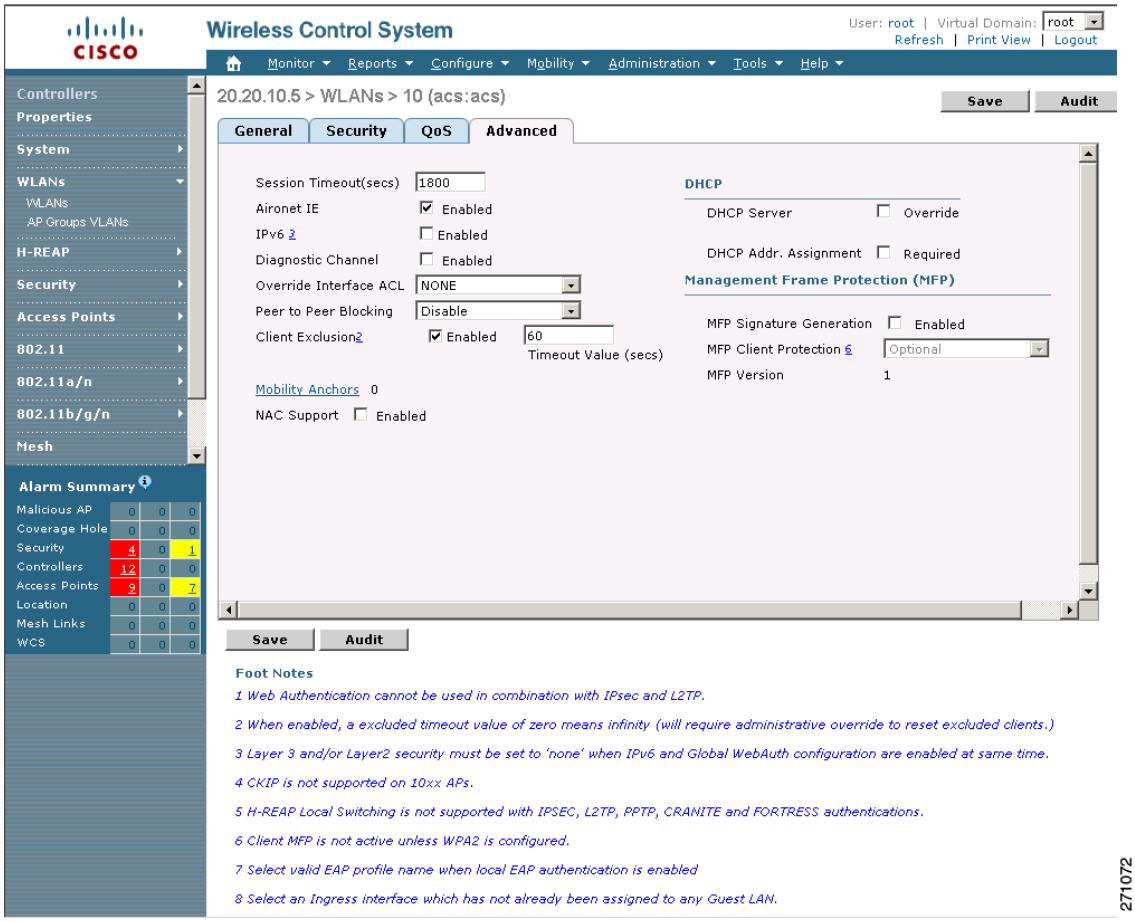
Step 4 Click the desired WLAN ID URL (see Figure 8-10).

Figure 8-10 WLAN Window



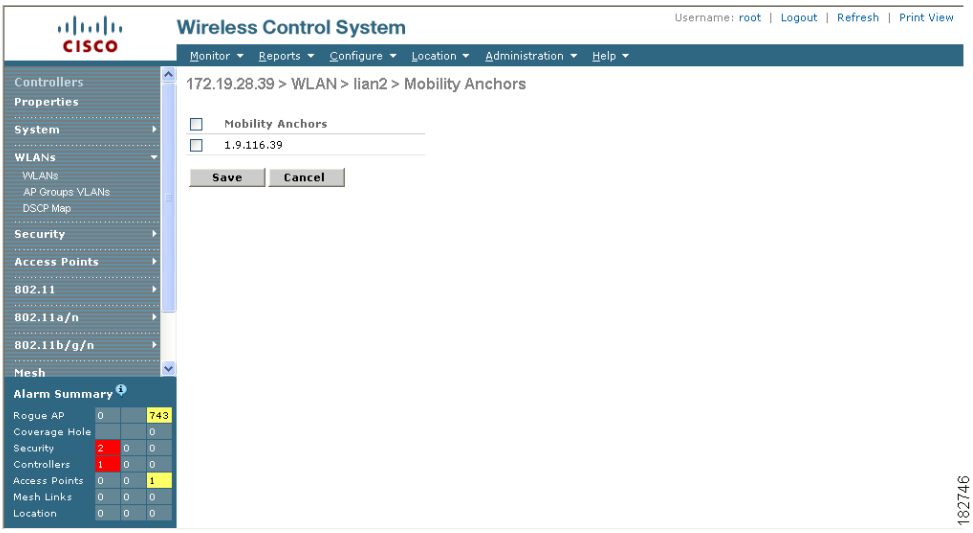
Step 5 After choosing a WLAN ID, a tabbed window appears (see Figure 8-11). Click the **Advanced** tab.

Figure 8-11 Advanced Window



Step 6 Click the **Mobility Anchors** link at the bottom of the page. The Mobility Anchors window appears (see Figure 8-12).

Figure 8-12 Mobility Anchors



Step 7 Check the IP address checkbox of the controller to be designated a mobility anchor and click **Save**.

Step 8 Repeat Step 6 and Step 7 to set any other controllers as anchors for this WLAN.

Step 9 Configure the same set of anchor controllers on every controller in the mobility group.

Configuring Multiple Country Codes

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.

Note 802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, 1) choose Configure > Controllers, 2) select the desired controller you want to disable, 3) choose 802.11a/n or 802.11b/g/n from the left sidebar menu, and then 4) choose Parameters. The Network Status is the first check box.

Follow these steps to add multiple controllers that are defined in a configuration group and then set the DCA channels. To configure multiple country codes outside of a mobility group, refer to the "Setting Multiple Country Codes" section on page 10-3.

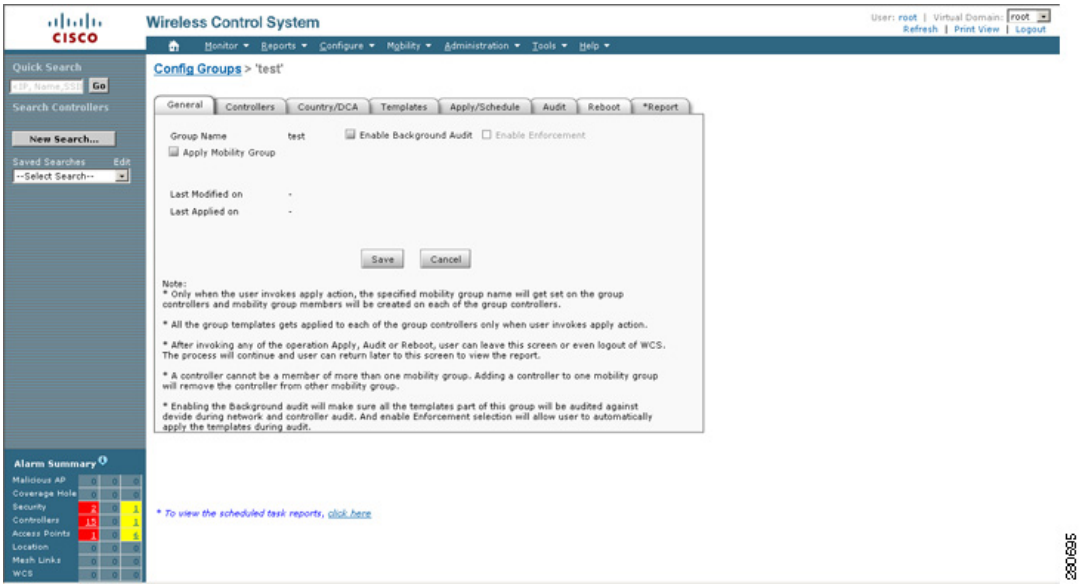
Step 1 Choose **Configure > Config Groups**.

Step 2 Choose **Add Config Groups** from the Select a command drop-down menu.

Step 3 Create a config group by entering the group name and mobility group name.

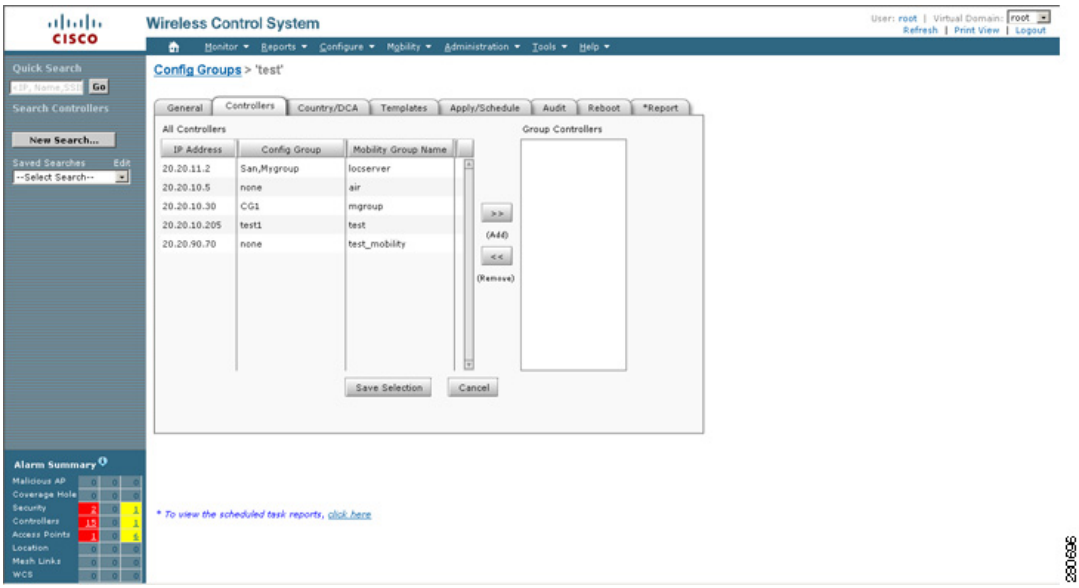
Step 4 Click **Save**. The Config Groups window appears (see Figure 8-13).

Figure 8-13 Config Groups Window



Step 5 Click the **Controllers** tab. The Controllers window appears (see Figure 8-14).

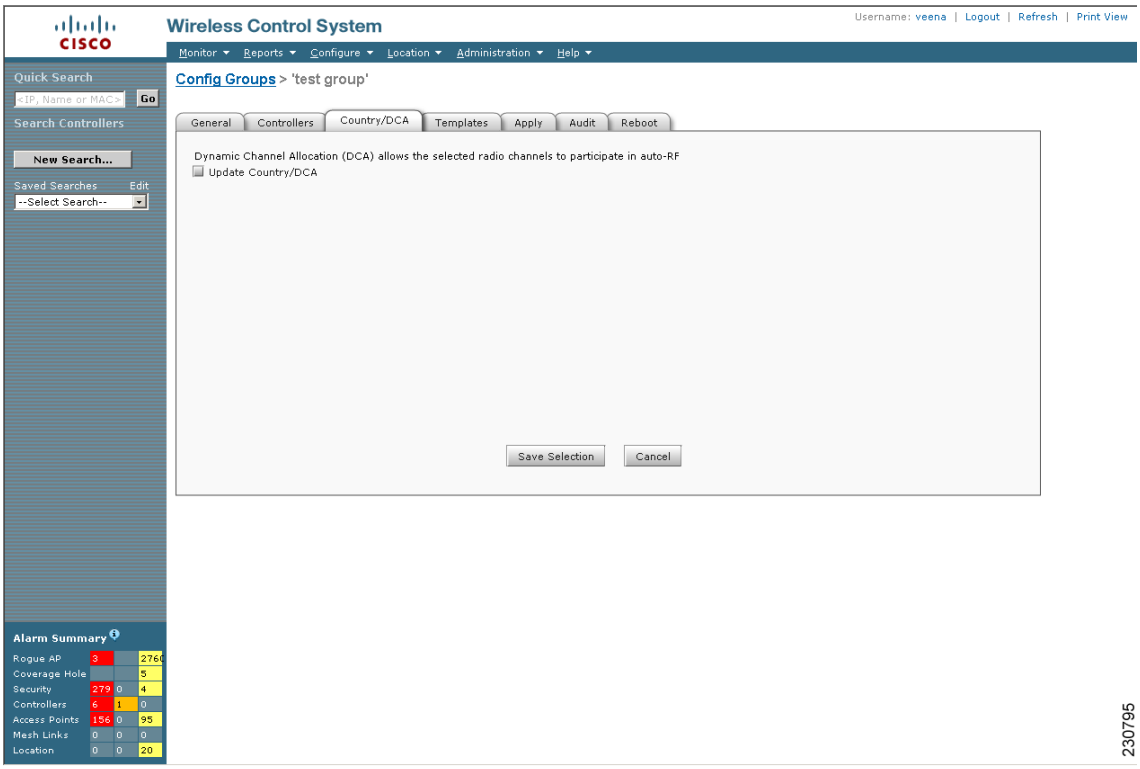
Figure 8-14 Controller Tab



Step 6 Highlight the controllers you want to add and click the **>> Add** button. The controller is added to the Group Controllers window.

Step 7 Click the **Country/DCA** tab. The Country/DCA window appears (see Figure 8-15). Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Figure 8-15 Country/DCA Tab



Step 8 Check the **Update Countries** check box to display a list of countries from which to choose.

Step 9 Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes window. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking **Save Selection.**

Note A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Creating Config Groups

By creating a config group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all the controllers in a group. You can add, delete, or remove config groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected config groups. You can also save the current configuration to nonvolatile (Flash) memory to controllers in selected config groups.

Note A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

For information about applying templates to either individual controllers or controllers in selected Config Groups, refer to Chapter 11, "Using Templates."

By choosing **Configure > Config Groups**, you can view a summary of all config groups in the Cisco WCS database. When you choose **Add Config Groups** from the Select a command drop-down menu, the page displays a table with the following columns:

- Check box: Check to select the config group.
- Group Name: Name of the config group.
- Mobility Group Name: Name of Mobility or WPS Group.
- Controllers: Number of controllers added to Config Group.
- Templates: Number of templates applied to config group.
- Scheduled: Indicates whether or not the provisioning of mobility group, mobility members, and templates has been scheduled.
- Next Scheduled Run: Indicates the date and time of the next scheduled provisioning.
- Last Modified: Date and time config group was last modified.
- Last Applied: Date and time last changes were applied.

Adding New Group

Follow these steps to add a config group.

Step 1 Choose **Configure > Config Groups**.

Step 2 From the Select a command drop-down list, choose **Add Config Group** and click **GO**. The Add New Group window appears.

Step 3 Enter the new config group name. It must be unique across all groups. If Enable Background Audit is selected, the network and controller audits occur for this config group. If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.

Note If the Enable Background Audit option is chosen, the network and controller audit is performed on this config group.

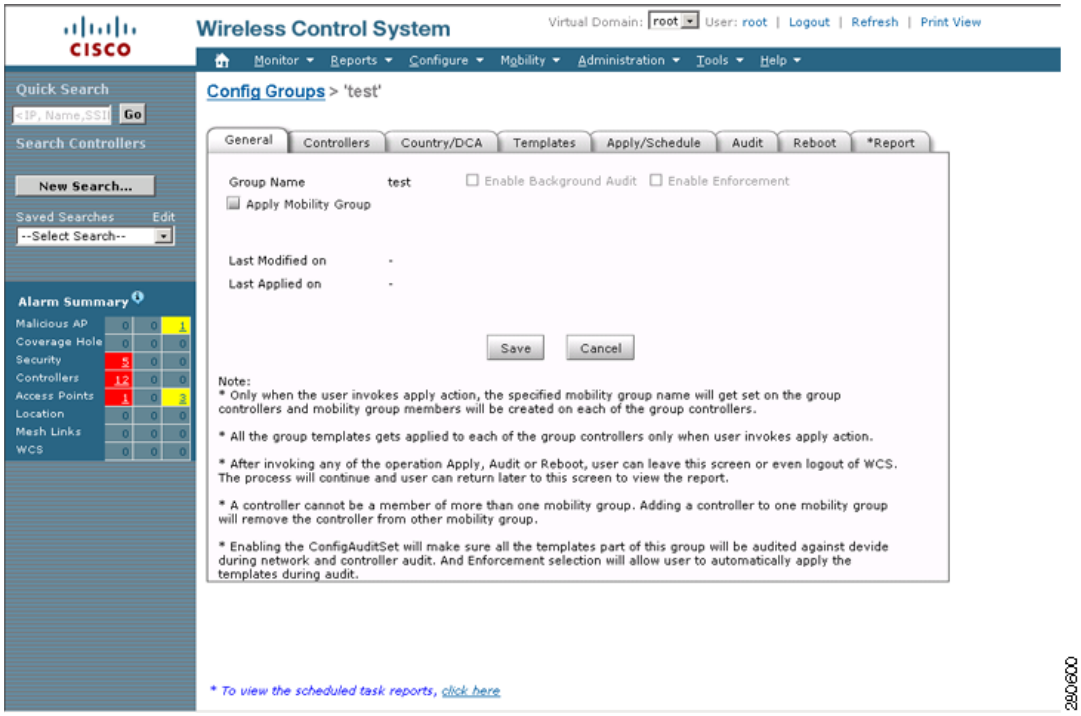
Step 4 Other templates created in WCS can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:

- Select and add later: Click to add template at a later time.
- Copy templates from a controller: Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new config group. Only the templates are copied.

Note The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.

Step 5 Click **Save**. The Config Groups window appears (see Figure 8-16).

Figure 8-16 Config Groups Window



Configuring Config Groups

Follow these steps to configure a config group.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column. The Config Group window shown in Figure 8-16 appears.

Step 2 Click the **General** tab. The following options for the config group appear:

- Group Name: Name of the config group
  - Enable for background audit—If selected, all the templates that are part of this group are audited against the controller during network and controller audits.
  - Enable Enforcement—If selected, the templates are automatically applied during the audit if any discrepancies are found.

Note The audit and enforcement of the config group template happens when the selected audit mode is *Template based audit*.

- Mobility Group Name: Mobility Group Name that is pushed to all controllers in the group. The Mobility Group Name can also be modified here.

Note A controller can be part of multiple config groups.

- Last Modified On: Date and time config group was last modified.
- Last Applied On: Date and time last changes were applied.

Step 3 You must choose the **Apply** tab to distribute the specified mobility group name to the group controllers and to create mobility group members on each of the group controllers.

Step 4 Click **Save**.

Enabling a Background Audit

If you enable a background audit on a config group, all of the templates that are part of this group are audited against the controller during network and controller audits.

This option to enable background audit will be disabled if the audit settings in the audit settings page are set to basic audit. This option is available when the Template based audit setting is chosen.

To change the audit settings, go to Administration > Settings > Audit.

After enable background audit is selected, you can select the **Enforce Configuration** checkbox. This ensures that the templates are automatically applied during the audit if any discrepancies are found.

Adding or Removing Controllers from Config Group

Follow these steps to add or remove controllers from a config group.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Controllers** tab. The columns in the table display the IP address of the controller, the config group name the controller belongs to, and the controller's mobility group name.

Step 3 Click to highlight the row of the controller you want to add to the group.

Step 4 Click the **>>Add** button.

Note If you want to remove a controller from the group, highlight the controller in the Group Controllers box and click the **<< Remove** button.

Step 5 You must choose the **Apply** tab and click the **Apply** button to add or remove the controllers to the config groups.

Step 6 Click the **Save Selection** button.

Adding or Removing Templates from the Config Group

Follow these steps to add or remove templates from the config group.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Templates** tab. The Remaining Templates table displays the item number of all available templates, the template name, and the type and use of the template.

Step 3 Click to highlight the row of the template you want to add to the group.

Step 4 Click the **>> Add** button to move the highlighted template to the Group Templates column.

Note If you want to remove a template from the group, highlight the template in the Remaining Templates box and click the **<< Remove** button.

Step 5 You must choose the **Apply** tab and click the **Apply** button to add or remove the templates to the config groups.

Step 6 Click the **Save Selection** button.

Applying or Scheduling Config Groups

Follow these steps to apply the mobility groups, mobility members, and templates to all the controllers in a config group.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Apply/Schedule** tab to access this page.

Step 3 Click **Apply** to start the provisioning of mobility groups, mobility members, and templates to all the controllers in the config group. After you apply, you can leave this window or log out of Cisco WCS. The process continues, and you can return later to this page and view a report.

Note Do not perform any other config group functions during the apply provisioning.

A report is generated and appears in the Recent Apply Report window. It shows which mobility group, mobility member, or template were successfully applied to each of the controllers.

Note If you want to print the report as shown on the window, you must choose landscape page orientation.

Step 4 The scheduling function allows you to schedule a start day and time for provisioning. Check the enable schedule check box to enable the scheduling feature.

Step 5 Enter a starting date in the text box or use the calendar icon to choose a start date.

Step 6 Choose the starting time using the hours and minutes drop-down menus.

Step 7 Click **Schedule** to start the provisioning at the scheduled time.

Auditing Config Groups

The Config Groups Audit window allows you to verify if the controller's configuration complies with the group templates and mobility group. During the audit, you can leave this screen or logout of Cisco WCS. The process continues, and you can return to this page later to view a report.

Note Do not perform any other config group functions during the audit verification.

Follow these steps to perform a config group audit.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column.

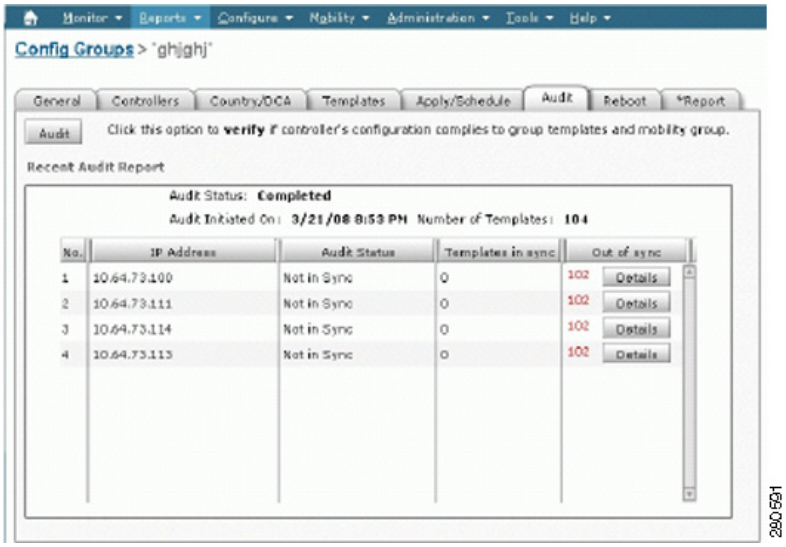
Step 2 Click the **Audit** tab to access this page.

Step 3 Click **Audit** to begin the auditing process (see Figure 8-17).

A report is generated and the current configuration on each controller is compared with that in the config group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

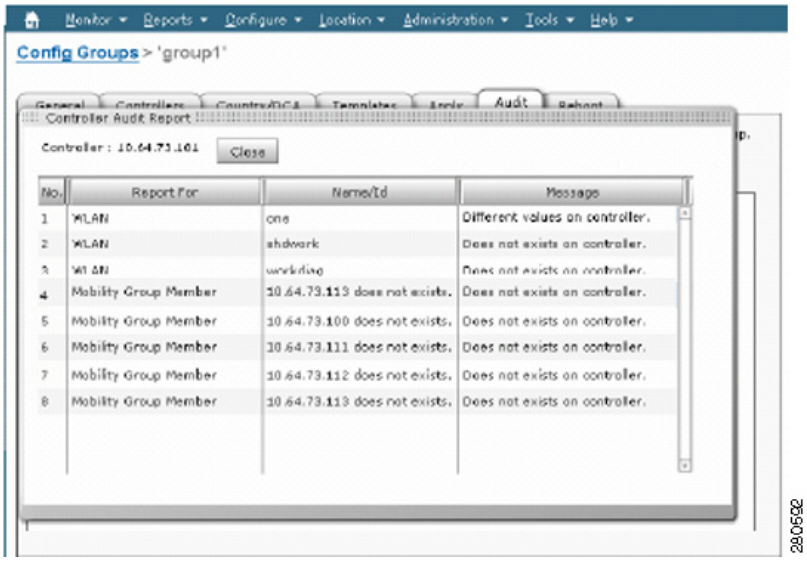
Note This audit does not enforce the WCS configuration to the device. It only identifies the discrepancies.

Figure 8-17 Config Groups Audit Tab



Step 4 Click **Details** to view the Controller Audit Report details (see Figure 8-18).

Figure 8-18 Controller Audit Report Details



Step 5 Double click a line item to open the Attribute Differences window. This window displays the attribute, its value in WCS, and its value in the controller.

Note Click **Retain WCS Value** to push all attributes in the Attribute Differences window to the device.

Step 6 Click **Close** to return to the Controller Audit Report window.

Choosing Basic or Template-based Auditing

You can choose between basic and template-based auditing. The default setting is Basic Audit.

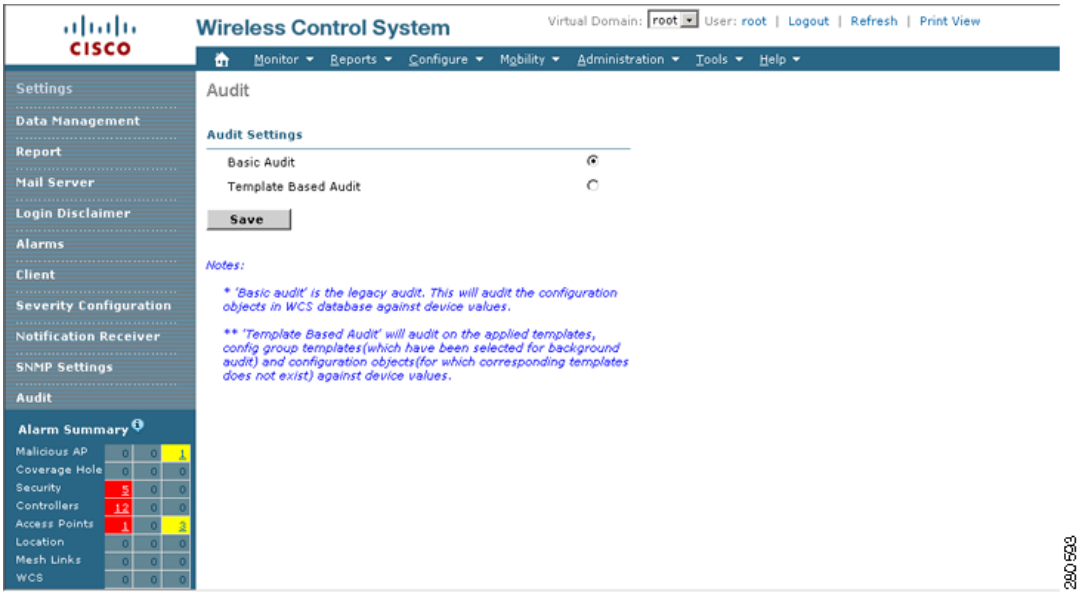
- Basic Audit—Audits the configuration objects in the WCS database against device values. This is the legacy audit. It is selected by default.
- Template-based Audit—Audits on the applied templates, config group templates (which have been selected for the background audit), and configuration audits (for which corresponding templates do not exist) against device values.

Follow these steps to indicate the type of audit you want to perform.

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Audit**. The Audit Setting window appears (see Figure 8-19).

Figure 8-19 Audit Settings Window



Step 3 Choose the radio button for either Basic or Template-Based Audit.

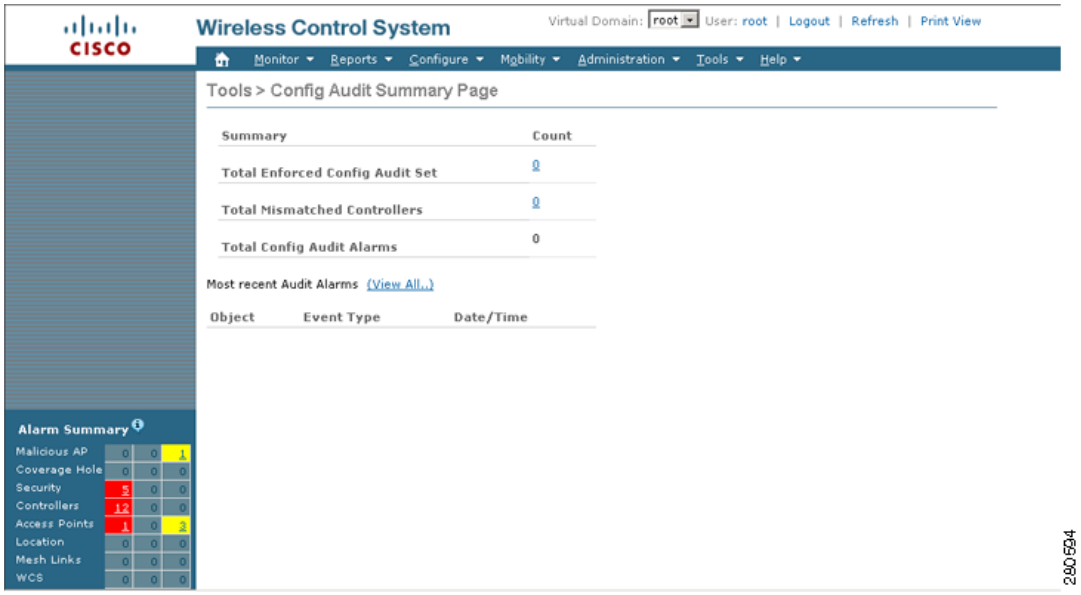
Step 4 Click **Save**.

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

Viewing Configuration Audit Summary

Choose **Tools > Config Audit** to launch the Configuration Audit Summary page (see Figure 8-20).

Figure 8-20 Tools > Config Audit Summary Window



This page provides a summary of the following:

- Config groups enabled for background audit—Identifies the count of config group templates which are configured for Background Audit and enforcement enabled.

  Click the link to launch the Config Group page to view config groups with **Enforce Configuration** enabled.

- Total mismatched controllers—Identifies the number of mismatched controllers. Mismatched controllers indicate that there were configuration differences found between the WCS and the controller during the last audit.

  Click the link to launch the controller list sorted on the mismatched audit status column. Click an item in the Audit Status column to view the audit report for this controller.

- Total config audit alarms—Identifies the number of alarms generated when audit discrepancies are enforced on config groups.

  Click the link to view all config audit alarm details.

  Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view list of discrepancies for each controller.

- Most recent audit alarms—Lists the most recent configuration audit alarms including the object name, event type, and date and time for the audit alarm.

  Click **<View All>** to view the applicable Alarm page which includes all configuration audit alarms.

Rebooting Config Groups

Follow these steps to reboot a config group.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Reboot** tab.

Step 3 Click the **Cascade Reboot** check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.

Step 4 Click **Reboot** to reboot all controllers in the config group at the same time. During the reboot, you can leave this window or logout of Cisco WCS. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report window shows when each controller was rebooted and what the controller status is after the reboot. If WCS is unable to reboot the controller, a failure is shown.

Note If you want to print the report as shown on the window, you must choose landscape page orientation.

Reporting Config Groups

Follow these steps to display all recently applied reports under a specified group name.

Step 1 Choose **Configure > Config Groups**, and click a group name under the Group Name column.

Step 2 Click the **Report** tab. The Recent Apply Report window displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:

- Apply Status—Indicates success, partial success, failure, or not initiated.
- Successful Templates—Indicates the number of successful templates associated with the applicable IP address.
- Failures—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
- Details—Click Details to view the individual failures and associated error messages.

Step 3 If you want to view the scheduled task reports, click the **click here** link at the bottom of the page. You are then redirected to the Configure > Scheduled Configuration Tasks > Config Group menu where you can view reports of the scheduled config groups.

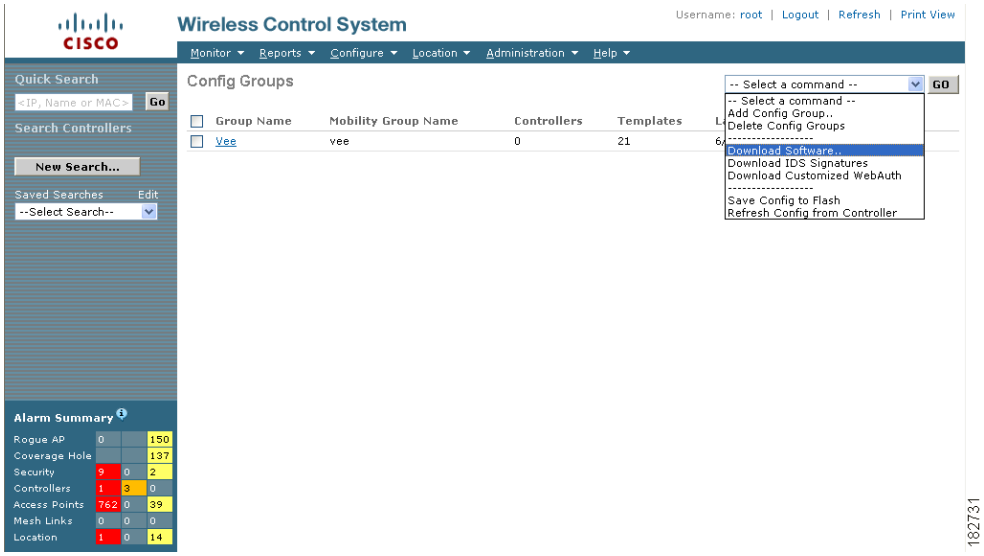
Downloading Software

Follow these steps to download software to all controllers in the selected groups after you have a config group established.

Step 1 From Configure > Config Groups, click the check box to choose one or more config groups names on the Config Groups window.

Step 2 Choose **Download Software** from the Select a command drop-down menu and click **GO** (see Figure 8-21).

Figure 8-21 Download Software Option



Step 3 The Download Software to Controller window appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On parameter.

Step 4 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries parameter.

Step 5 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout parameter.

Step 6 The signature files are uploaded to the c:\tftp directory. Specify the local file name in that directory or use the Browse button to navigate to it. The controller uses this local file name as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated for you and retried.

Step 7 Click **OK**.

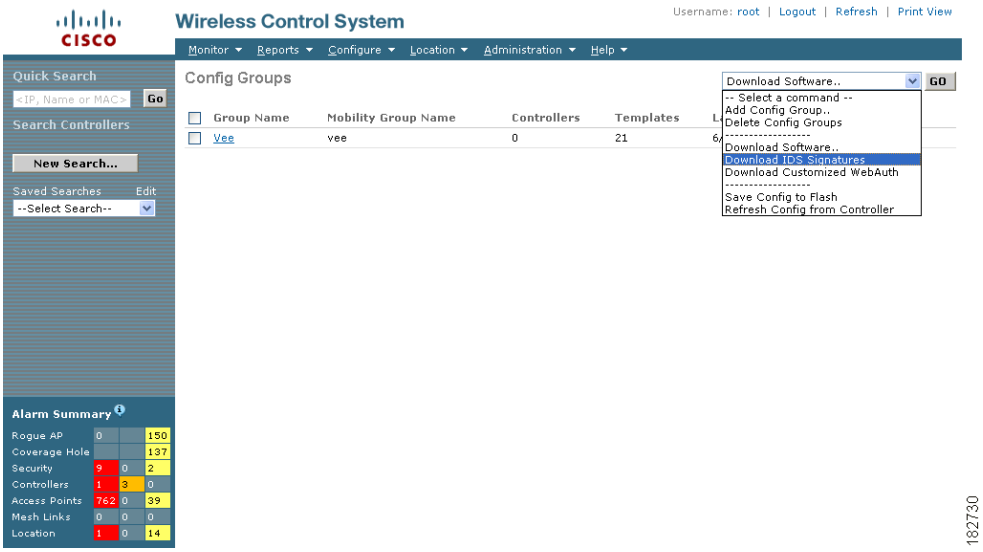
Downloading IDS Signatures

Follow these steps to download intrusion detection system (IDS) signature files from your config group to a local TFTP server.

Step 1 From Configure > Config Groups, click the check box to choose one or more config groups on the Config Groups window.

Step 2 Choose **Download IDS Signature**s from the Select a command drop-down menu and click **GO** (see Figure 8-22).

Figure 8-22 Downloading IDS Signatures Option



Step 3 The Download IDS Signatures to Controller window appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose **local machine** from the File is Located On parameter.

Step 4 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries parameter.

Step 5 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout parameter.

Step 6 The signature files are uploaded to the c:\tftp directory. Specify the local file name in that directory or use the Browse button to navigate to it. The controller uses this local file name as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated for you and retried.

Step 7 Click **OK**.

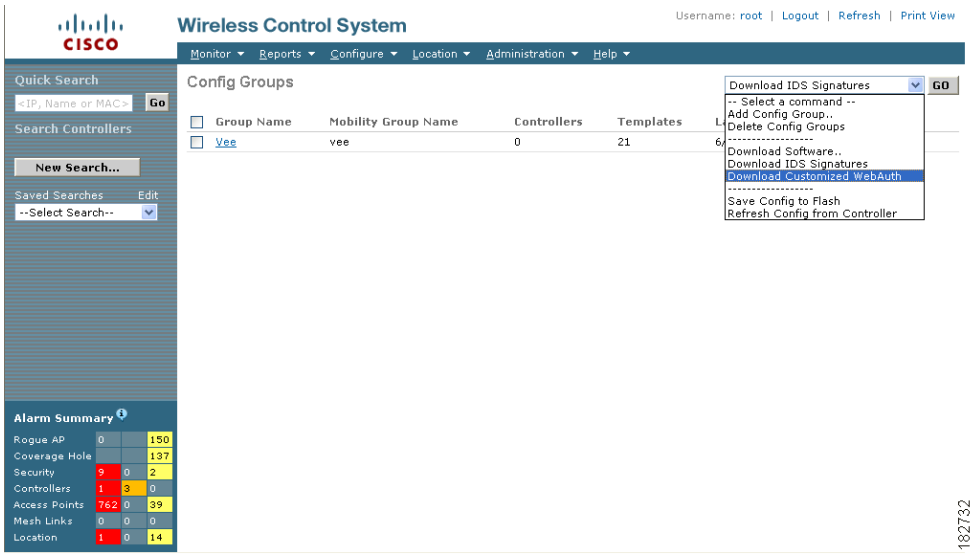
Downloading Customized WebAuth

Follow these steps to download customized web authentication.

Step 1 From Configure > Config Groups, click the check box to choose one or more config groups on the Config Groups window.

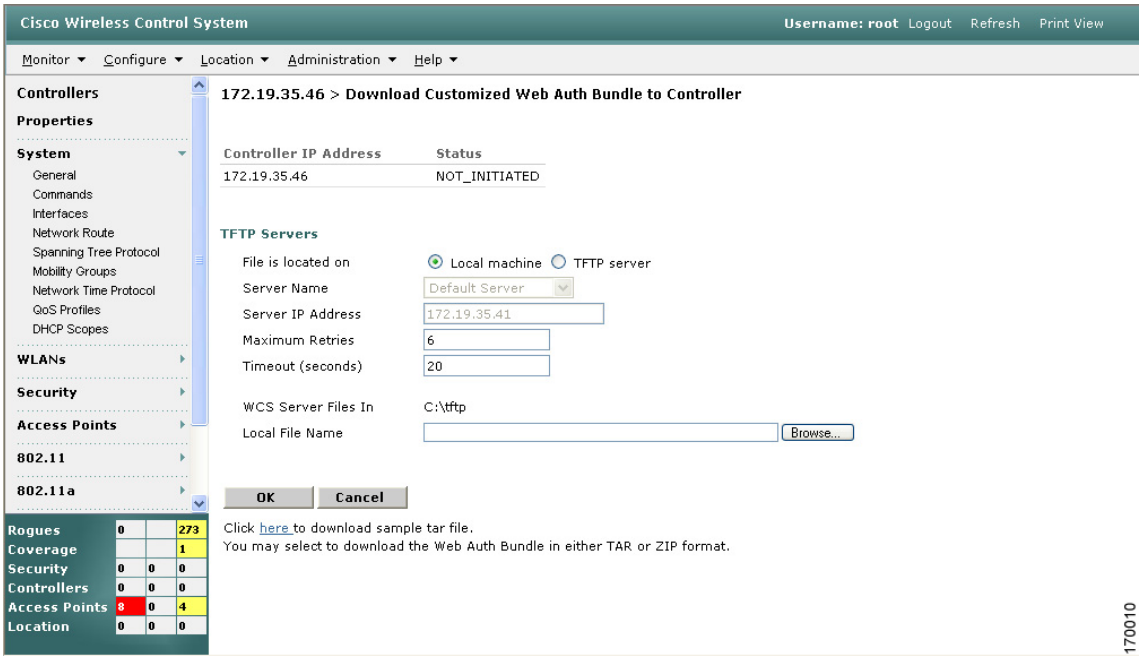
Step 2 Choose **Download Customized WebAuth** from the Select command drop-down menu and click **GO** (see Figure 8-23).

Figure 8-23 Download Customized Web Auth



Step 3 The Download Customized Web Auth Bundle to Controller window appears. The IP address of the controller to receive the bundle and the current status are displayed (see Figure 8-24).

Figure 8-24 Download Customized Web Auth Bundle to Controller



Step 4 Choose **local machine** from the File is Located On parameter.

Step 5 Enter the amount of times the controller should attempt to download the file in the Maximum Retries field.

Step 6 Enter the amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

Step 7 The WCS Server Files In parameter specifies where the WCS server files are located. Specify the local file name in that directory or use the Browse button to navigate to it.

Step 8 Click **OK**.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated for you and retried.