CHAPTER 12

# Using Templates

This chapter describes the Controller Template Launch Pad. It is a hub for all controller templates. Templates provide a way to set parameters that you can then apply to multiple devices without having to re-enter the common information. From this Template Launch Pad you can add and apply controller templates, view templates, or make modifications to existing templates. This chapter also includes steps for applying and deleting controller templates and creating or changing access point templates.

**Note** Template information can be overridden on individual devices.

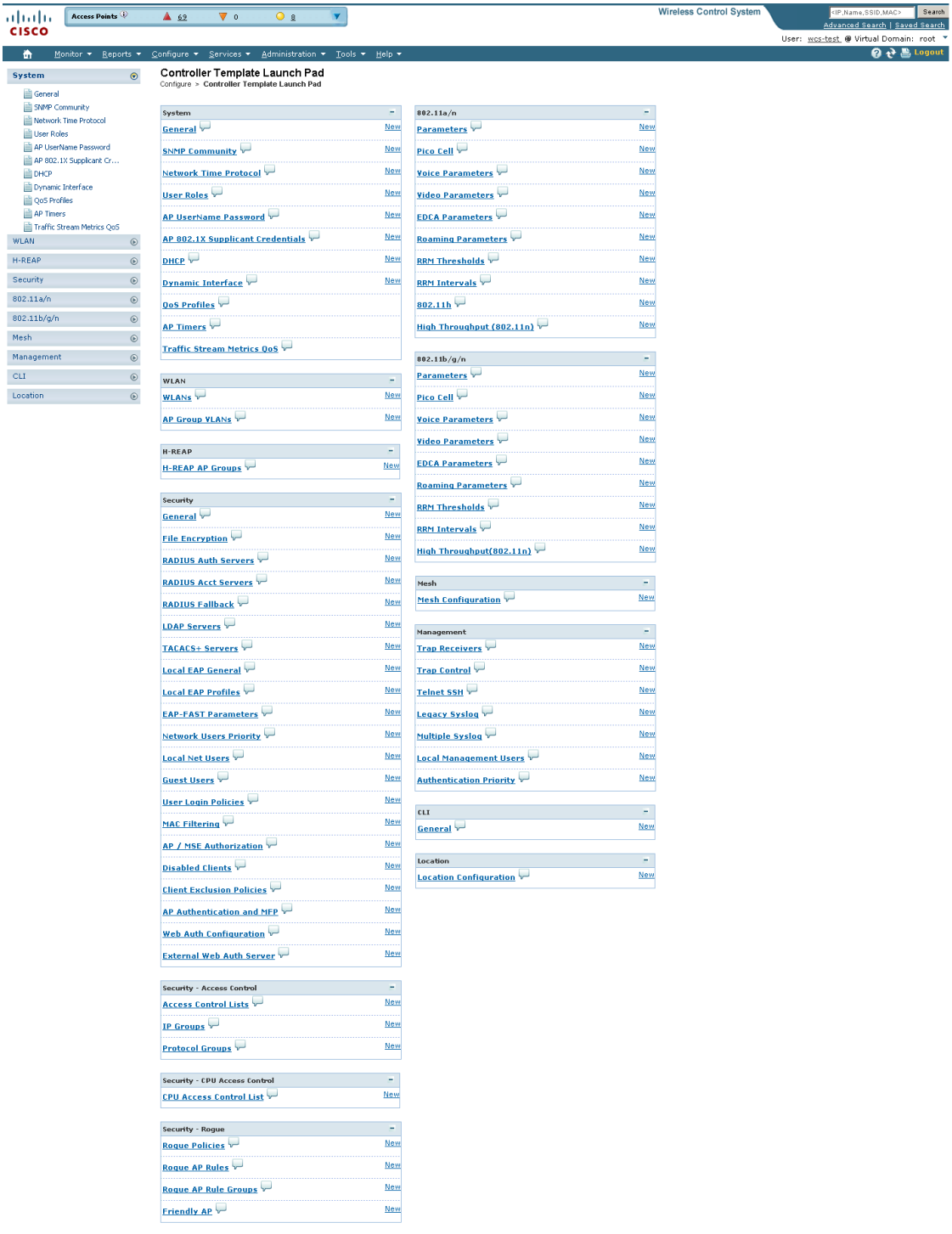
This chapter contains these sections:



## Controller Template Launch Pad

The controller template launch pad appears when you choose **Configure > Controller Template Launch Pad** (see Figure 12-1).

*Figure 12-1 Controller Template Launch Pad*




**Tip** Hold your mouse cursor over the tool tip next to the template type to view more details regarding the template.

# Adding Controller Templates

Follow these steps to add a new controller template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **New** beside the template you want to add.

**Step 3** Enter the template name.

**Step 4** Describe the template.

**Step 5** Click **Save**.

**Note** If you attempt to save a template without a name, the following popup message appears: "Template Name: This attribute is MANDATORY. Please specify it. Make the necessary corrections and try again."

# Configuring Controller Templates

Within this chapter, you can find information on adding or configuring the following controller templates:

# Configuring General Templates

Follow these steps to add a general template or make changes to an existing general template.

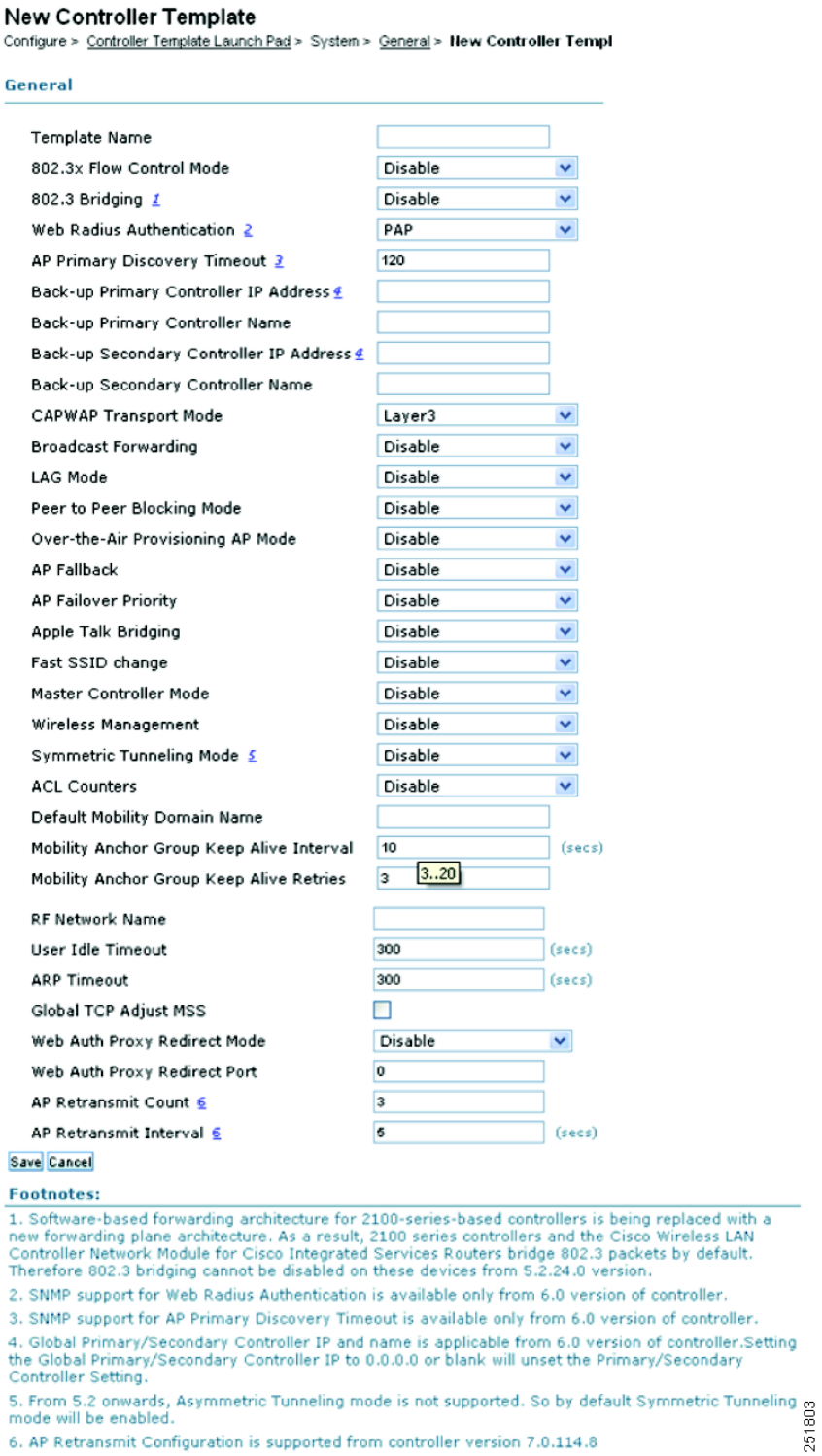
**Step 1** Choose **Configure > Controller Template Launch Pad**.

Click **General** or choose **System > General** from the left sidebar menu. The System > General Template page appears, and the number of controllers and virtual domains the template is applied to automatically populates. The last column shows when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page that displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 2** If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The General template page appears (see Figure 12-2).

***Figure 12-2 System > General Page***



**Step 3** Use the drop-down list to enable or disable flow control mode.

**Step 4** Use the drop-down list to enable or disable 802.3 bridging.

**Note** This 802.3 bridging option is not available for 5500 and 2106 series controllers.

**Step 5** Use the drop-down list to choose the desired Web RADIUS authentication. You can choose to use PAP, CHAP, or MD5-CHAP for authentication between the controller and the client during the user credential exchange.

**Step 6** Specify the number of seconds for the AP Primary Discovery Timeout. The default is 120 seconds, and the valid range is 30 to 3600.

**Step 7** Specify the Primary and Secondary Back-up Controller details (Controller IP Address and Controller Name).

**Step 8** Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the LWAPP or CAPWAP uses IP addresses to communicate with the access points; these IP addresses are collected from a mandatory DHCP server. When set to Layer 2, the lightweight access point uses proprietary code to communicate with the access points.

**Note** The older versions of controllers upto 5.2 will use LWAPP and the new controller version uses CAPWAP protocols.

**Step 9** Choose to enable or disable broadcast forwarding. The default is disabled.

**Step 10** Choose **Enable** or **Disable** from the LAG Mode drop-down list. Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG).

If LAG is enabled on a controller, any dynamic interfaces that you have created are deleted to prevent configuration inconsistencies in the interface database. When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

**Note** Interfaces cannot be created with the Dynamic AP Manager flag set. Also, you cannot create more than one LAG on a controller.

**Step 11** Choose to enable or disable peer-to-peer blocking mode. If you choose Disable, any same-subnet clients communicate through the controller. If you choose Enable, any same-subnet clients communicate through a higher-level router.

**Step 12** At the Over Air AP Provision Mode drop-down list, choose **enable** or **disable**.

**Step 13** At the AP Fallback drop-down list, choose **enable** or **disable**. Enabling fallback causes an access point that lost a primary controller connection to automatically return to service when the primary controller returns.

**Step 14** When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This may cause the controller to reach a saturation point and reject some of the access points. By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points can join the backup controller if the lower priority access points are disjoined. Choose Enable at the AP Failover Priority drop-down list if you want to allow this capability.

**Step 15** Choose to enable or disable Apple Talk bridging.

**Note** This Apple Talk bridging option is not available on 5500 series controllers.

**Step 16** Choose to enable or disable the Fast SSID Change option. If the option is enabled, the client connects instantly to the controller between SSIDs without having much loss of connectivity. Normally, each client is connected to a particular WLAN identified by the SSID. If the client moves out of reach of the connected access point, the client has to reconnect to the controller using a different access point. This normal process consumes some time as the DHCP (Dynamic Host Configuration Protocol) server has to assign an IP address to the client.

**Step 17** Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or operating system code upgrade. You may enable the controller as the master controller from the Master Controller Mode drop-down list.

**Step 18** Choose to enable or disable access to the controller management interface from wireless clients. Because of IPSec operation, management via wireless is only available to operators logging in across WPA or Static WEP. Wireless management is not available to clients attempting to log in via an IPSec WLAN.

**Step 19** Choose to enable or disable symmetric tunneling mode. 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.

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

**Note** For symmetric tunneling to take effect, you must reboot.

**Step 20** Use the drop-down list to enable or disable ACL counters. The values per ACL rule can be viewed for each controller.

**Step 21** Enter the operator-defined RF mobility group name in the Default Mobility Domain Name text box.

**Step 22** At the Mobility Anchor Group Keep Alive Interval, determine the delay between tries for clients attempting to join another access point. 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.

**Note** When you hover over the parameter field with the mouse, the valid range for that field appears.

**Step 23** At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.

**Step 24** Enter the RF network group name between 8 and 19 characters. Radio Resource Management (RRM) neighbor packets are distributed among access points within an RF network group. The Cisco access points only accept RRM neighbor packets sent with this RF network name. The RRM neighbor packets sent with different RF network names are dropped.

**Step 25** Specify the time out for idle clients. The factory default is 300 seconds. When the timeout expires, the client loses authentication, briefly disassociates from the access point, reassociates, and re-authenticates.

**Step 26** Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.

**Step 27** Select the Global TCP Adjust MMS checkbox to start checking the TCP packets originating from the client, for the TCP SYN/ TCP ACK packets and MSS value and reset it to the configured value on the upstream and downstream side.

**Step 28** Choose enable or disable Web Auth Proxy Redirect Mode, if a manual proxy configuration is configured on the client's browser, all web traffic going out from the client will be destined to the PROXY IP and PORT configured on the browser.

**Step 29** Enter the Web Auth Proxy Redirect Port. The default ports are 8080 and 3128. The range is 0 to 65535.

**Step 30** Enter the AP Retransmit Count and Intervals. The AP Retransmit Count default value is 5 and the range is from 3 to 8. The AP Retransmit Interval default value is 3. The range is 2 to 5.

**Step 31** Click **Save**.

# Configuring an NTP Server Template

Follow these steps to add an NTP template or make modifications to an existing NTP template. NTP is used to synchronize computer clocks on the internet.

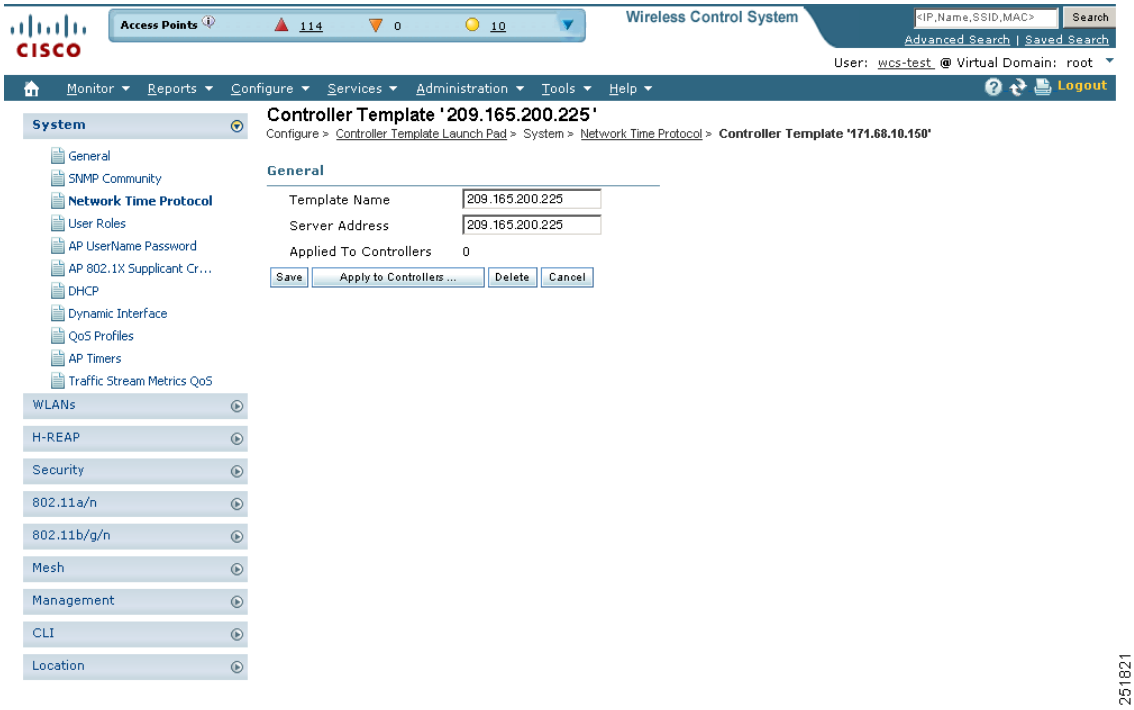
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Network Time Protocol** or choose **System > Network Time Protocol** from the left sidebar menu. The System > NTP Server Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens the Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens to an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Network Time Protocol template page appears (see Figure 12-3).

*Figure 12-3 NTP Servers Template*




**Step 4** Enter the NTP server IP address.

**Step 5** Click **Save**.

# Configuring AP 802.1X Supplicant Credentials

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. All access points that are currently joined to the controller and any that join in the future are included. Follow these steps to add or modify an existing AP 802.1X Supplicant Credentials template.

**Note** If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See "Configuring Access Points" section on page 9-17 for more information.

**Step 1** Choose **Configure > Controller Templates Launch Pad**.

**Step 2** Click **AP 802.1X Supplicant Credentials** or choose **System > AP 802.1X Supplicant Credentials** from the left sidebar menu. The AP 802.1X Supplicant Credentials Templates page displays all currently saved AP 802.1X Supplicant Credentials templates. It also displays the number of controllers and virtual domains to which each template is applied.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** Click a template name to open the Controller Template list page. From there, you can edit the current template parameters.

**Step 4** Click **Save**.

# Configuring DHCP Template

Follow these steps to add a DHCP template or make modifications to an existing DHCP template.

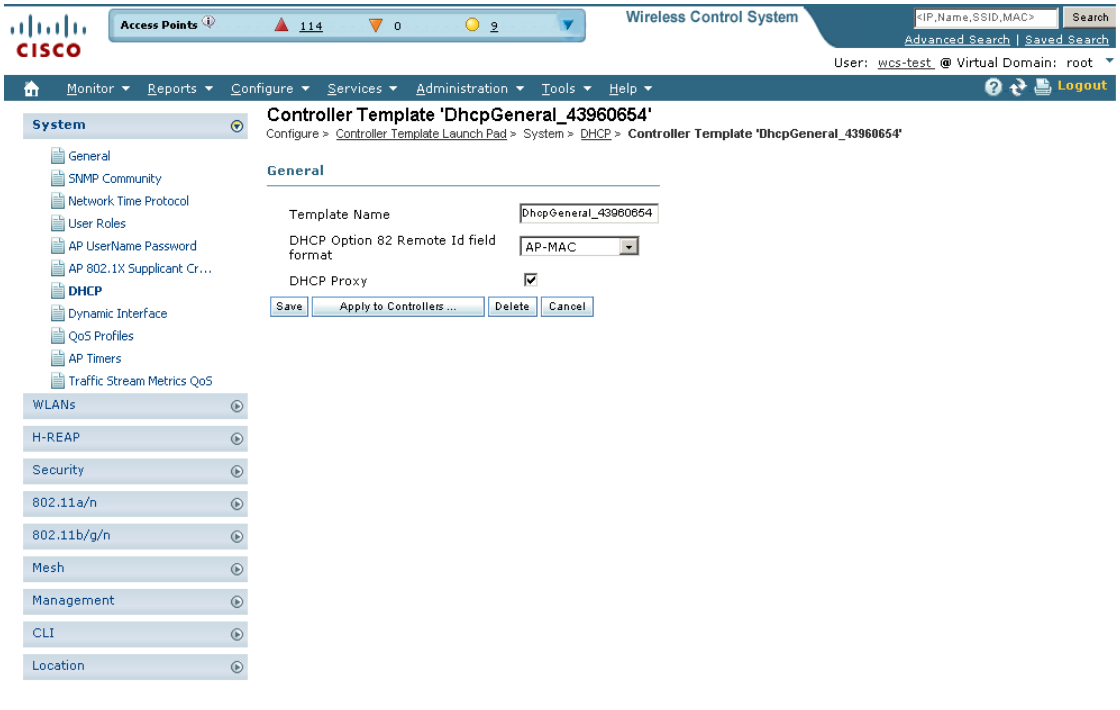
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **DHCP** or choose **System > DHCP** from the left sidebar menu. The System > DHCP Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The DHCP template page appears (see Figure 12-4).

*Figure 12-4 DHCP Template Page*




**Step 4** You can enable or disable DHCP proxy on a global basis rather than on a WLAN basis. When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the WLAN or on the WLAN itself. DHCP proxy is enabled by default.

**Step 5** Click **Save**.

# Configuring Dynamic Interface Templates

Follow these steps to add a dynamic interface template or make modifications to an existing interface configuration.

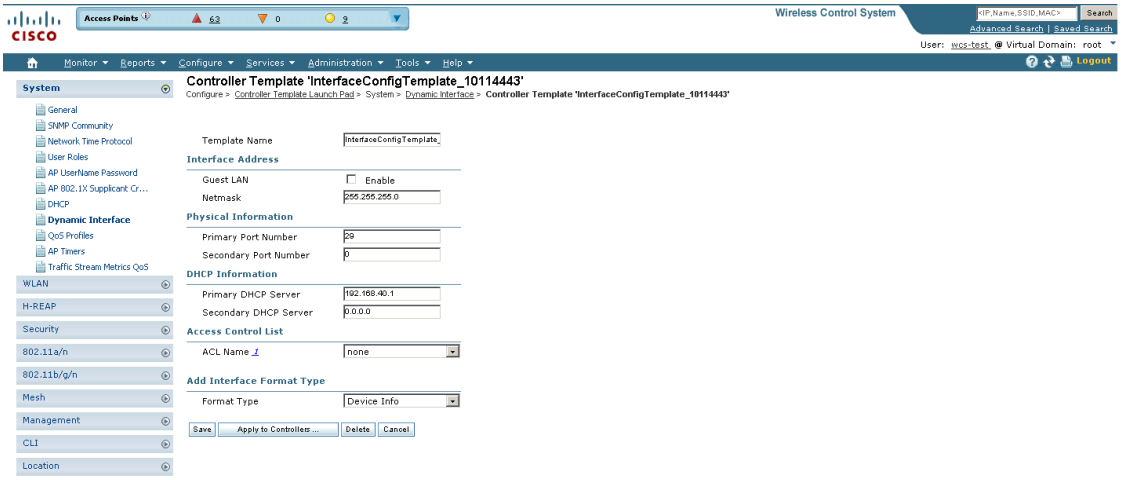
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Dynamic Interface** or choose **System > Dynamic Interface** from the left sidebar menu. The System > Dynamic Interface Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Dynamic Interface template page appears (see Figure 12-5).

*Figure 12-5 Dynamic Interface Template*




251795

**Step 4** Select the Guest LAN check box to mark the interface as wired.

**Step 5** Enter the net mask address of the interface.

**Step 6** Enter which port is currently used by the interface.

**Step 7** Enter a secondary port to be used by the interface when the primary port is down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN Controller transfers the interfaces back to the primary port.

**Note** Primary and secondary port numbers are present only in the Cisco 4400 Series Wireless LAN Controllers.

**Step 8** Enter the IP address of the primary DHCP server.

**Step 9** Enter the IP address of the secondary DHCP server.

**Step 10** From the ACL Name drop-down list, choose a name from the list of defined names.

**Step 11** From the Add Format Type drop-down list in the Add Interface Format Type section, choose either Device Info or File. If you choose device info, you must configure the device specific parameters for each controller. If you choose File, you must configure CSV device specific parameters (Interface Name, VLAN Identifier, Quarantine VLAN Identifier, IP Address, and Gateway) for all the managed controllers specified in the CSV file (see Table 12-1). If you choose Device Info, continue to Step 12.

The sample CSV files are as follows:

*Table 12-1 Sample CSV Files*

| ip_address | interface_name | vlan_id | quarantine_ vlan_id | interface_ ip_address | gateway |
|---|---|---|---|---|---|
| 209.165.200.224 | dyn-1 | 1 | 2 | 209.165.200.228 | 209.165.200.229 |
| 209.165.200.225 | interface-1 | 4 | 2 | 209.165.200.230 | 209.165.200.231 |

*Table 12-1 Sample CSV Files*

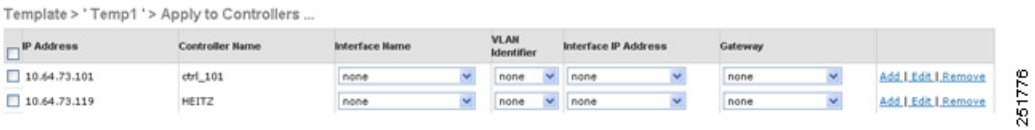
| ip_address | interface_name | vlan_id | quarantine_ vlan_id | interface_ ip_address | gateway |
|---|---|---|---|---|---|
| 209.165.200.226 | interface-2 | 5 | 3 | 209.165.200.232 | 209.165.200.233 |
| 209.165.200.227 | dyna-2 | 2 | 3 | 209.165.200.234 | 209.165.200.235 |

The first row of the CSV file is used to describe the columns included. The CSV files can contain the following fields:

- ip_address
- interface_name
- vlan_id
- quarantine_vlan_id
- interface_ip_address
- gateway

**Step 12** If you choose Apply to Controllers, you advance to the Apply To page where you can configure device-specific parameters for each controller (see Figure 12-6).

*Figure 12-6 Apply To Page*




**Step 13** Use the **Add** and **Remove** options to configure device specific parameters for each controllers. If you click **Edit**, a dialog box appears with the current parameter input.

**Step 14** Make the necessary changes in the dialog box, and click **OK**.

**Note** If you change the interface parameters, the WLANs are temporarily disabled, so, you may lose connectivity for some clients. Any changes to the interface parameters are saved only after you successfully apply them to the controller(s).

**Note** If you remove an interface here, it is removed only from this template and NOT from the controllers.

# Configuring QoS Templates

Follow these steps to modify the quality of service (QoS) profiles.

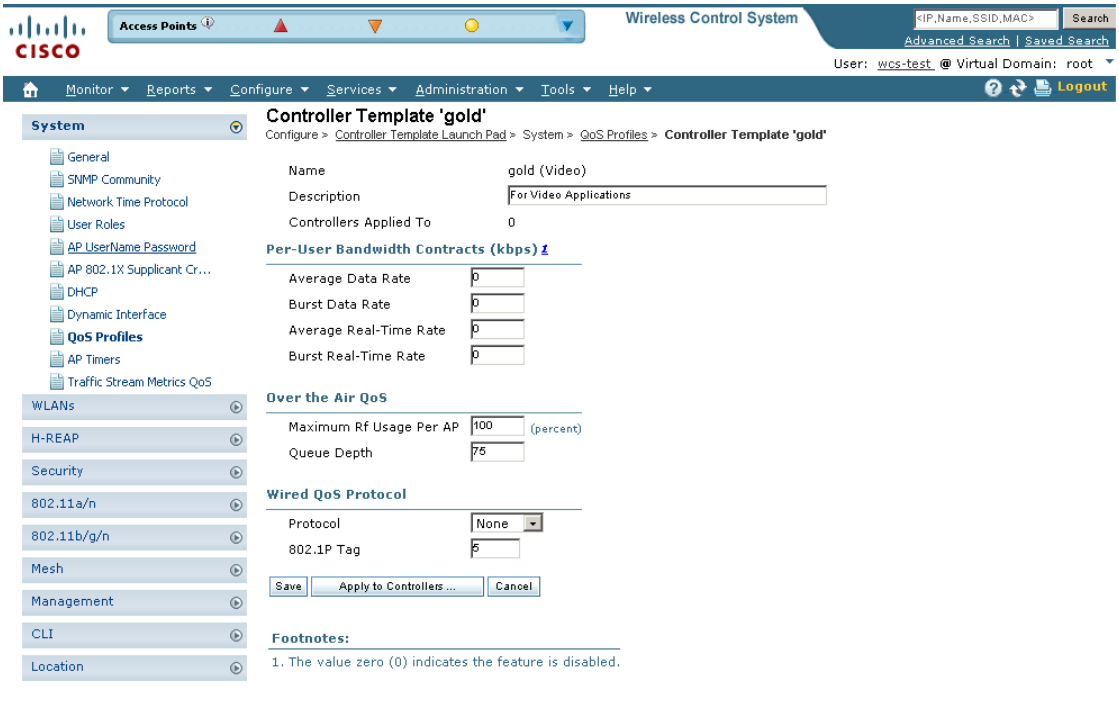
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **QoS Profiles** or choose **System > QoS Profile**s from the left sidebar menu. The System > QoS Profiles page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to edit the bronze, gold, platinum, or silver QoS profile, click in the Name column for the profile you want to edit. The Edit QoS Profile Template page appears (see Figure 12-7).

***Figure 12-7 Edit QoS Profile Template Page***




**Step 4** Set the following values in the Per-User Bandwidth Contracts portion of the page. All have a default of 0 or Off.

- Average Data Rate - The average data rate for non-UDP traffic.
- Burst Data Rate - The peak data rate for non-UDP traffic.
- Average Real-time Rate - The average data rate for UDP traffic.
- Burst Real-time Rate - The peak data rate for UDP traffic.

**Step 5** Set the following values for the Over-the-Air QoS portion of the page.

- Maximum QoS RF Usage per AP - The maximum air bandwidth available to clients. The default is 100%.
- QoS Queue Depth - The depth of queue for a class of client. The packets with a greater value are dropped at the access point.

**Step 6** Set the following values in the Wired QoS Protocol portion of the page.

- Wired QoS Protocol - Choose 802.1P to activate 802.1P priority tags or None to deactivate 802.1P priority flags.
- 802.1P Tag - Choose 802.1P priority tag for a wired connection from 0 to 7. This tag is used for traffic and CAPWAP packets.

**Step 7** Click **Save**.

# Configuring AP Timers

Some advanced timer configuration for HREAP and local mode is available for the controller on WCS. Follow these steps to configure a template for advanced timers.

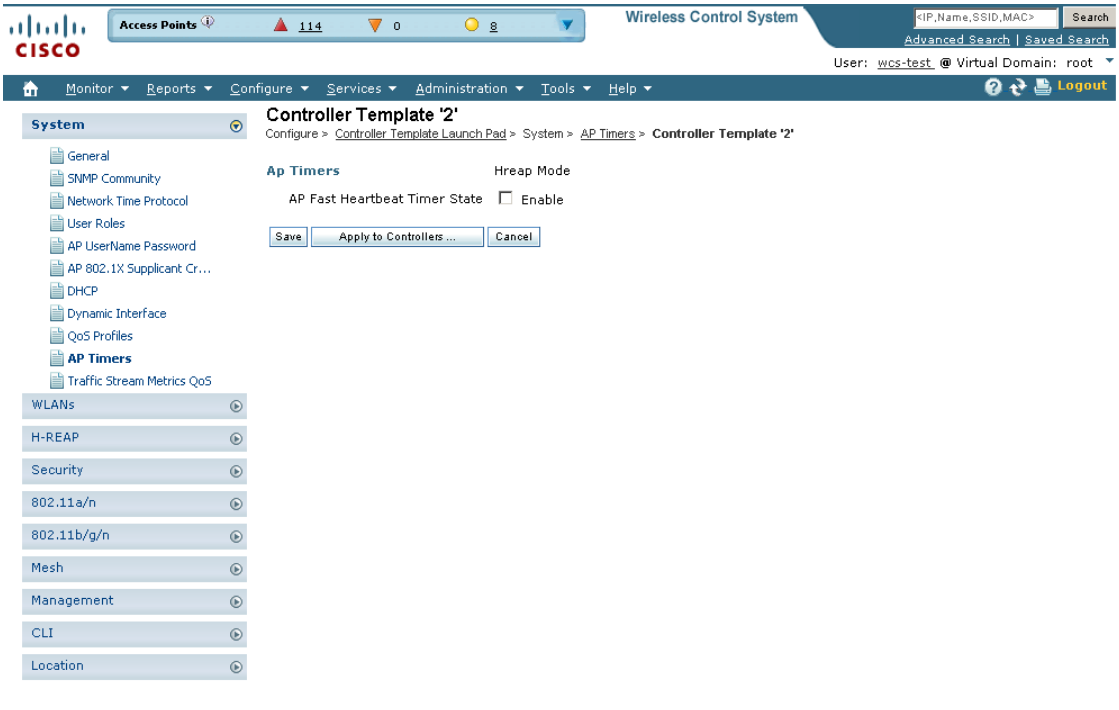
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **AP Timers** or choose **System > AP Timers** from the left sidebar menu. The System > AP Timers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** To reduce the controller failure detection time, click **Local Mode** (see Figure 12-8). You can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 1 and 10 seconds.

*Figure 12-8 AP Timers Page*




**Step 4** Click **HREAP Mode**. You can then configure the HREAP timeout value. Check the AP Primary Discovery Timeout check box to enable the timeout value. Enter a value between 30 and 3600 seconds.

**Step 5** Click **Save**.

# Configuring a Traffic Stream Metrics QoS Template

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and informs you of the QoS of the wireless LAN. These statistics are different than the end-to-end statistics provided by VoIP systems. End-to-end statistics provide information on packet loss and latency covering all the links comprising the call path. However, traffic stream metrics are statistics for only the WLAN segment of the call. Because of this, system administrators can quickly determine whether audio problems are being caused by the WLAN or by other network elements participating in a call. By observing which access points have impaired QoS, system administrators can quickly determine the physical area where the problem is occurring. This is important when lack of radio coverage or excessive interference is the root problem.

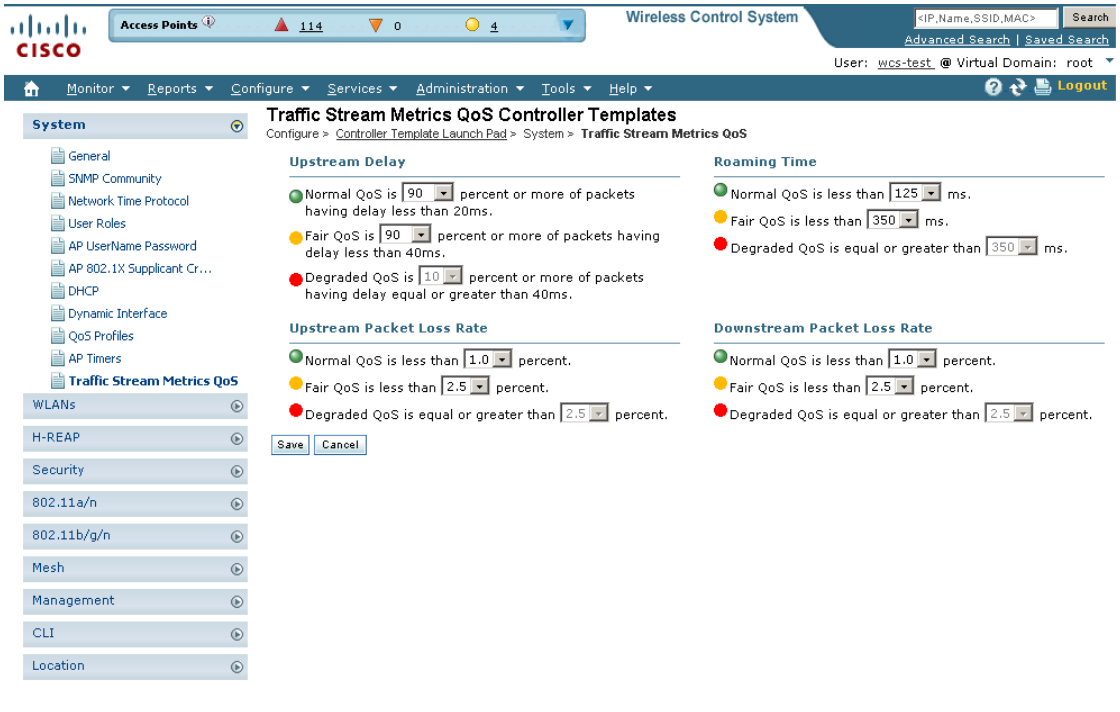
Four QoS values (packet latency, packet jitter, packet loss, and roaming time), which can affect the audio quality of voice calls, are monitored. All the wireless LAN components participate in this process. Access points and clients measure the metrics, access points collect the measurements and then send them to the controller. The access points update the controller with traffic stream metric information every 90 seconds, and 10 minutes of data is stored at one time. Cisco WCS queries the controller for the metrics and displays them in the Traffic Stream Metrics QoS Status. These metrics are compared to threshold values to determine their status level and if any of the statistics are displaying a status level of fair (yellow) or degraded (red), the administrator investigates the QoS of the wireless LAN.

For the access points to collect measurement values, traffic stream metrics must be enabled on the controller.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Traffic Stream Metrics QoS** or choose **System > Traffic Stream Metrics QoS** from the left sidebar menu. The System > Traffic Stream Metrics QoS Status page appears (see Figure 12-9).

***Figure 12-9 Traffic Stream Metrics QoS Status Template***




The Traffic Stream Metrics QoS Status Configuration page shows several QoS values. An administrator can monitor voice and video quality of the following:

- Upstream delay
- Upstream packet loss rate
- Roaming time
- Downstream packet loss rate
- Downstream delay

Packet Loss Rate (PLR) affects the intelligibility of voice. Packet delay can affect both the intelligibility and conversational quality of the connection. Excessive roaming time produces undesired gaps in audio.

There are three levels of measurement:

- Normal: Normal QoS (green)
- Fair: Fair QoS (yellow)
- Degraded: Degraded QoS (red)

System administrators should employ some judgement when setting the green, yellow, and red alarm levels. Some factors to consider are:

- Environmental factors including interference and radio coverage which can affect PLR.
- End-user expectations and system administrator requirements for audio quality on mobile devices (lower audio quality can permit greater PLR).
- Different codec types used by the phones have different tolerance for packet loss.
- Not all calls will be mobile-to-mobile; therefore, some have less stringent PLR requirements for the wireless LAN.

# Configuring WLAN Templates

WLAN templates allow you to define various WLAN profiles for application to different controllers.

In WCS software release 4.0.96.0 and later releases, you can configure multiple WLANs with the same SSID. This feature enables you to assign different Layer 2 security policies within the same wireless LAN. Unlike previous release where profile name was used as the unique identifier, the template name is now the unique identifier with software release 5.1.

These restrictions apply when configuring multiple WLANs with the same SSID:

- WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes. These are the available Layer 2 security policies:
  - None (open WLAN)
  - Static WEP or 802.1
  - CKIP
  - WPA/WPA2
- Broadcast SSID must be enabled on the WLANs that share an SSID so that the access points can generate probe responses for these WLANs.
- Hybrid-REAP access points do not support multiple SSIDs.

Follow these steps to add a WLAN template or make modifications to an existing WLAN template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

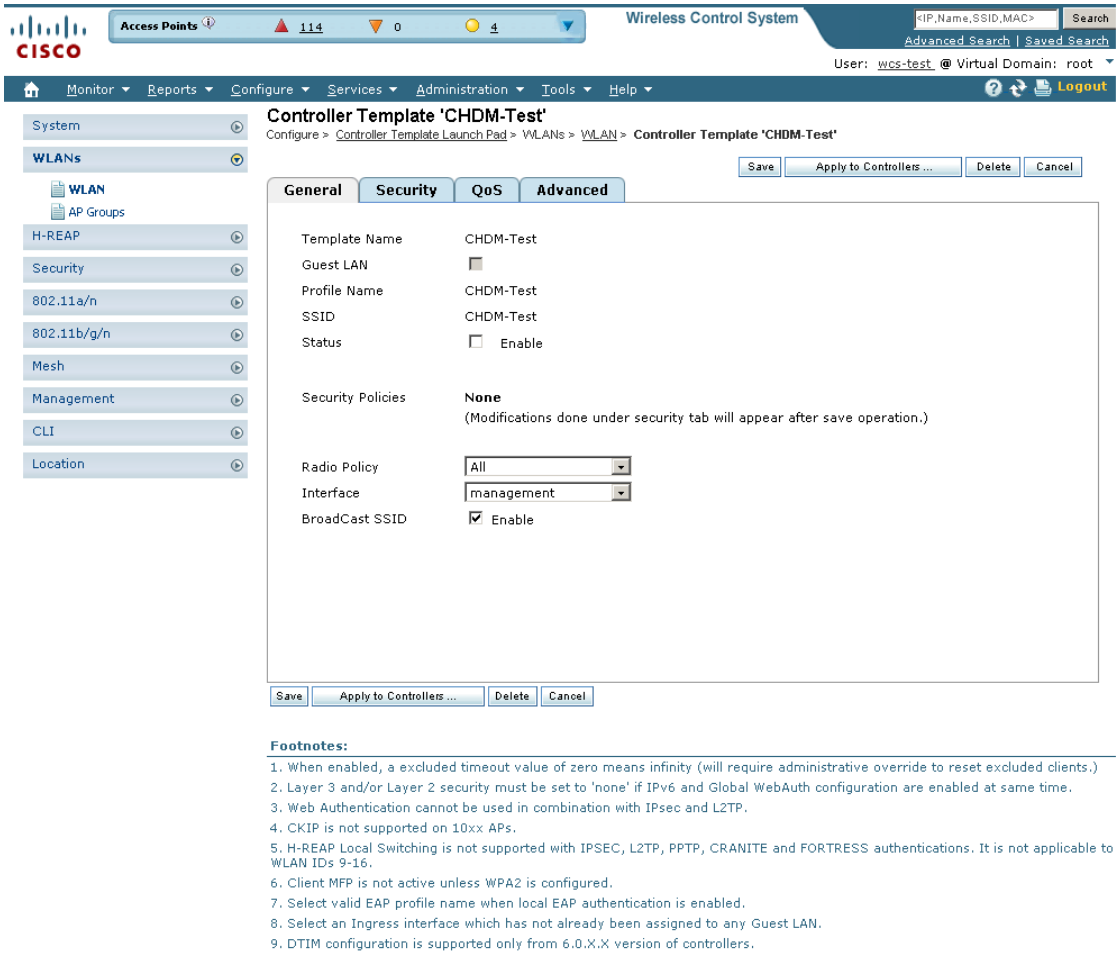
**Step 2** Click **WLAN** or choose **WLANs > WLAN** from the left sidebar menu. The WLAN Template page appears with a summary of all existing defined WLANs. The following information headings are used to define the WLANs listed on the WLAN Template General page:

- Template Name—The user-defined name of the template. Clicking the name displays parameters for this template.
- Profile Name—User-defined profile name used to distinguish WLANs with the same SSID.
- SSID—Displays the name of the WLAN.
- WLAN/Guest LAN—Determines if guest LAN or WLAN.
- Security Policies—Indicates what security policy is chosen. None indicates no 802.1X.
- WLAN Status—Determines whether the WLAN is enabled or not.

- Applied to Controllers—The number of controllers the WLAN template is applied to. The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status.
- Applied to Virtual Domains—The number of virtual domains the WLAN template is applied to. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.
- Last Saved At—Indicates when the template was last saved.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The WLAN template page appears (see Figure 12-10).

***Figure 12-10 WLAN Template***




**Step 4** Specify if you want guests users to have wired guest access from an Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room and accounts are added to the network using the Lobby Ambassador portal. (See the "Creating Guest User Accounts" section on page 7-10).

**Step 5** Enter a name in the Profile Name text box that identifies the WLAN or the guest LAN. Do not use any spaces in the name entered.

**Step 6** Enter the name of the WLAN SSID. An SSID is not required for a guest LAN.

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes.

**Step 7** Check the **Enable** check box for the Status parameter.

**Step 8** Use the Radio Policy drop-down list to set the WLAN policy to apply to All (802.11a/b/g/n), 802.11a only, 802.11g only, 802.11b/g only, or 802.11a/g only.

**Step 9** Use the Interface drop-down list to choose the available names of interfaces created by the Controller > Interfaces module.

**Step 10** From the Egress Interface drop-down list, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 10-52. This provides a path out of the controller for wired guest client traffic.

**Step 11** From the Ingress Interface drop-down list, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 10-51. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

**Step 12** Click **Broadcast SSID** to activate SSID broadcasts for this WLAN.

**Step 13** Click **Save**.

**Step 14** To further configure the WLAN template, choose from the following:

- Click the **Security** tab to establish which AAA can override the default servers on this WLAN and to establish the security mode for Layer 2 and 3. Continue to the "Security" section on page 12-20.
- Click the **QoS** tab to establish which quality of service is expected for this WLAN. Continue to the "QoS" section on page 12-28.
- Click the **Advanced** tab to configure any other details about the WLAN, such as DHCP assignments and management frame protection. Continue to the "Advanced" section on page 12-29.

## Security

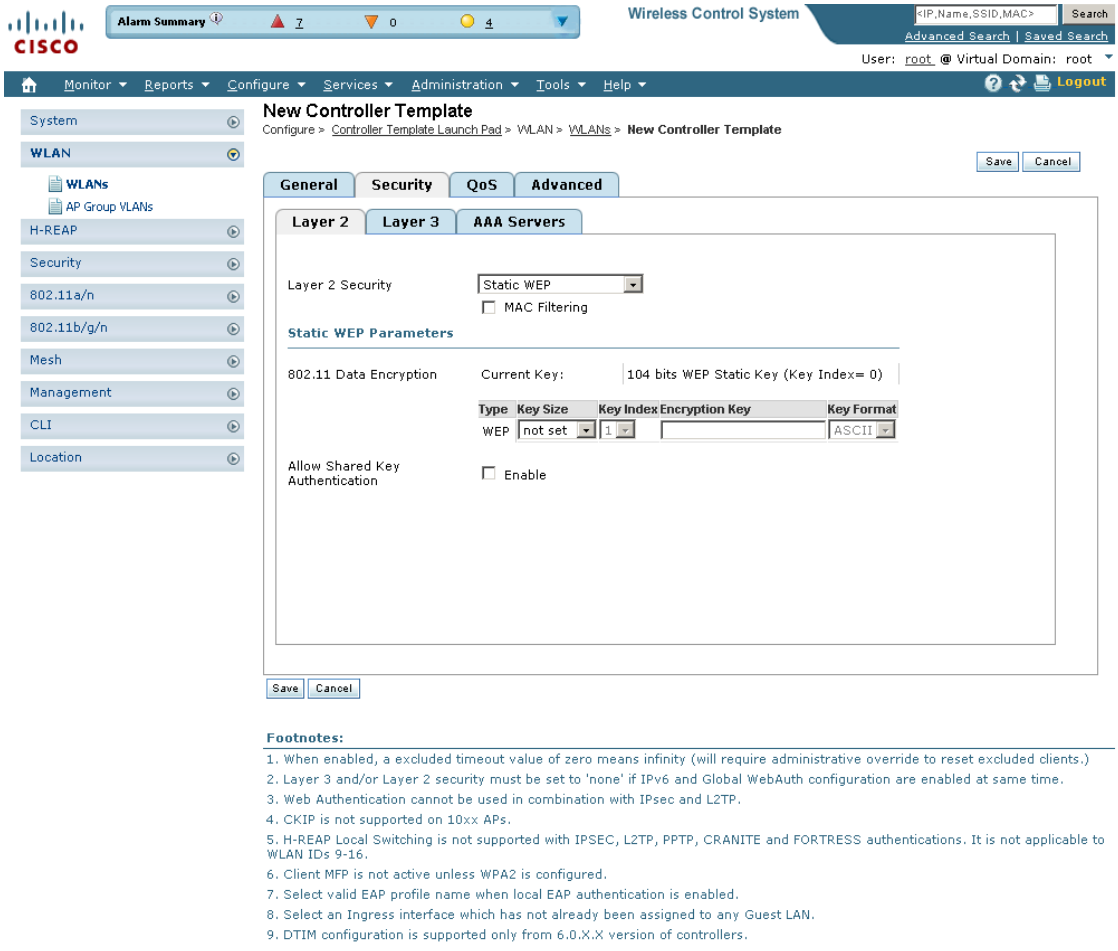
After choosing Security, you have an additional three tabs: Layer 2, Layer 3, and AAA Servers.

### Layer 2

When you choose the Layer 2 tab, the page as shown in Figure 12-11 appears.

**Note** The screen contains different views depending on what option is chosen in the Layer 2 Security drop-down list.

*Figure 12-11 Layer 2 Page*




**Step 1** Use the Layer 2 Security drop-down list to choose None, 802.1X, Static WEP, Static WEP-802.1X, WPA + WPA2, or CKIP as described in the table below.

*Table 12-2 Layer 2 Security Options*

| Parameter | Description |
|---|---|
| None | No Layer 2 security selected. |
| 802.1X | WEP 802.1X data encryption type (Note 1):<br>40/64 bit key.<br>104 bit key.<br>152 bit key. |

*Table 12-2 Layer 2 Security Options (continued)*

| Parameter | Description |
|---|---|
| Static WEP | Static WEP encryption parameters:<br>Key sizes: Not set, 40/64, 104, and 152 bit key sizes.<br>Key Index: 1 to 4 (Note 2).<br>Encryption Key: Encryption key required.<br>Key Format: ASCII or HEX.<br>Allowed Shared Key Authentication—Select the check box to enable.<br>**Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device. |
| Static WEP-802.1X | Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X parameters are displayed at the bottom of the page.<br>Static WEP encryption parameters:<br>Key sizes: Not set, 40/64, 104, and 152 bit key sizes.<br>Key index: 1 to 4 (Note 2).<br>Encryption Key: Enter encryption key.<br>Key Format: ASCII or HEX.<br>Allowed Shared Key Authentication—Select the check box to enable.<br>802.1 Data Encryption: 40/64 bit key, 104 bit key, 152 bit key. |

*Table 12-2 Layer 2 Security Options (continued)*

| Parameter | Description |
|---|---|
| WPA+WPA2 | Use this setting to enable WPA, WPA2, or both. See the WPA1 and WPA2 parameters displayed in the page when WPA+WPA2 is selected. WPA enables Wi-Fi Protected Access with TKIP-MIC Data Encryption or AES. When WPA+WPA2 is selected, you can use Cisco Centralized Key Management (CCKM) authentication key management, which allows fast exchange when a client roams from one access point to another.<br><br>When WPA+WPA2 is selected as the Layer 2 security policy, and Pre-shared Key is enabled, then neither CCKM or 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time. |
| CKIP | Cisco Key Integrity Protocol (CKIP). A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WLAN.<br><br>**Note** CKIP is not supported on 10xx APs.<br><br>When selected, these CKIP parameters are displayed.<br><br>Key size: Not set, 40, or 104.<br><br>Key Index: 1 to 4<br><br>Encryption Key: Specify encryption key.<br><br>Key Format: ASCII or HEX.<br><br>**Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.<br><br>MMH Mode: Select the check box to enable.<br><br>Key Permutation: Select the check box to enable. |

**Step 2** Check the **MAC Filtering** check box if you want to filter clients by MAC address.

**Note** The ability to join a controller without specification within a MAC filter list is only supported on mesh access points.

**Note** For releases prior to 4.1.82.0, mesh access points do not join the controller unless they are defined in the MAC filter list.

You may want to disable the MAC filter list to allow newly added access points to join the controller. Before enabling the MAC filter list again, you should enter the MAC addresses of the new access points.

**Step 3** Choose the desired type of authentication key management. The choices are 802.1X, CCKM, or PSK.

**Note** If you choose PSK, you must enter the shared key and type (ASCII or hexadecimal).

**Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

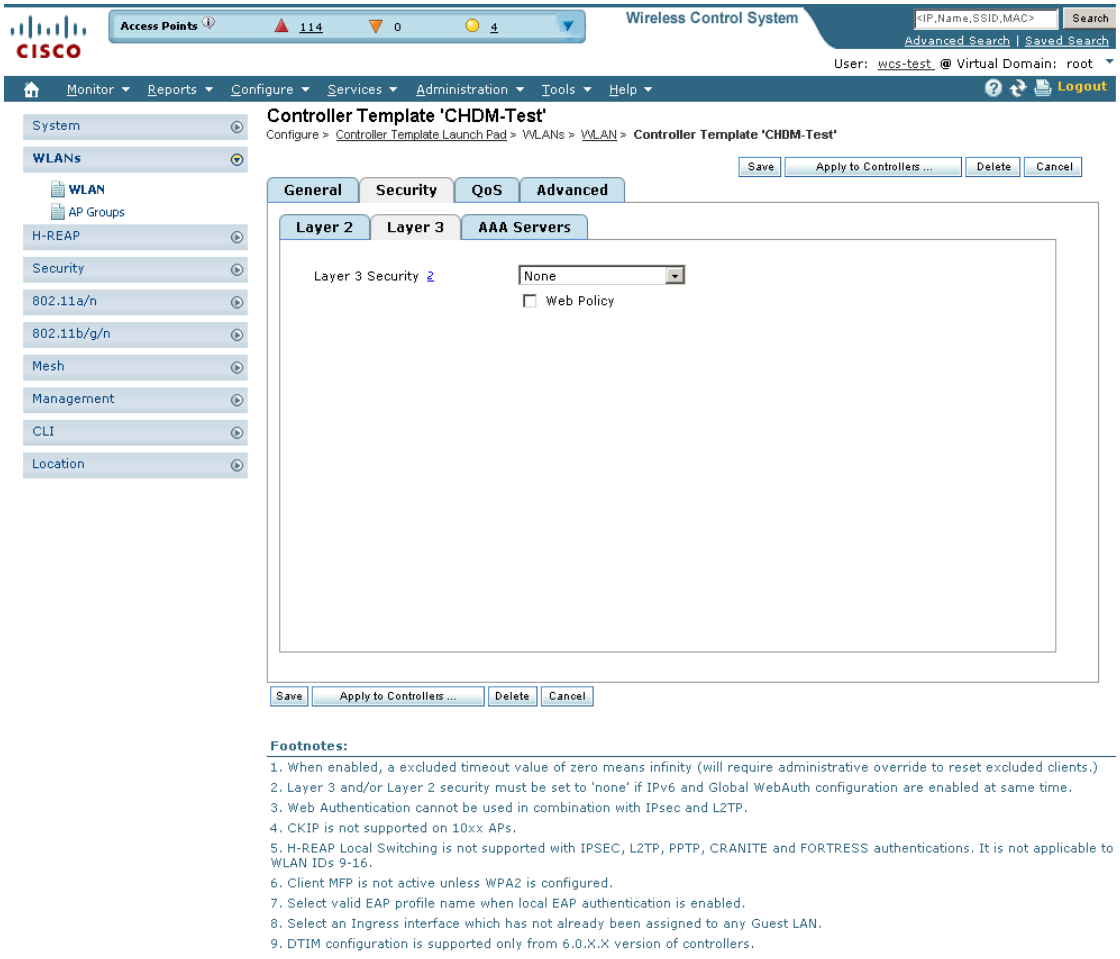
**Step 4** Click **Save**.

## Layer 3

When you choose the Layer 3 tab, the page shown in Figure 12-12 appears.

**Note** The screen contains different views depending on what option is chosen in the Layer 3 Security drop-down list.

*Figure 12-12 Layer 3 Page*




Follow these steps to configure the Layer 3 tab.

**Step 1** Use the Layer 3 security drop-down list to choose between None and VPN Pass Through. The page parameters change according to the selection you make. If you choose VPN pass through, you must enter the VPN gateway address.

**Note** The VPN passthrough option is not available for the 2106 or 5500 series controllers.

**Step 2** You can modify the default static WEP (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source.

**a.** To change the static WEP to passthrough, check the **Web Policy** check box and the **Passthrough** option. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Check this check box if you want users to be prompted for their email address when attempting to connect to the network.

b. To specify custom web authentication pages, unselect the Global WebAuth Configuration **Enable** check box.

1. When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

   Default Internal—Displays the default web login page for the controller. This is the default value.

   Customized Web Auth—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

   These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For specifics on downloading custom pages, refer to the "Downloading Customized Web Authentication" section on page 3-48.

   External—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

   **Note** External web auth is not supported for 2106 and 5500 series controllers.

   You can select specific RADIUS or LDAP servers to provide external authentication in the **Security > AAA** page. To do so, continue with Step 4.

**Note** The RADIUS and LDAP servers must be already configured to have selectable options in the Security > AAA page. You can configure these servers in the RADIUS Authentication Servers page and TACACS+ Authentication Servers page.

**Step 3** If you selected External as the Web Authentication Type in Step 2, click **Security > AAA** and choose up to three RADIUS and LDAP servers using the drop-down lists.

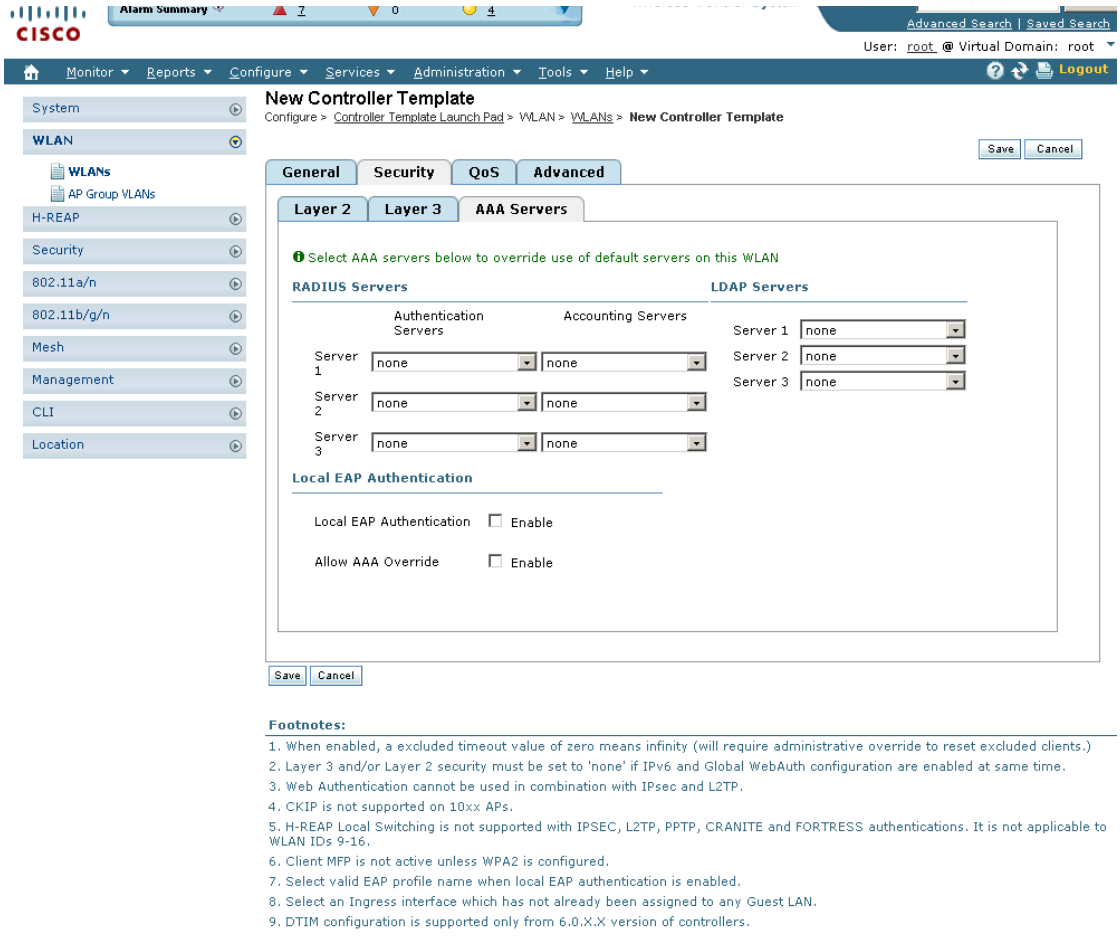
**Step 4** Click **Save**.

**Step 5** Repeat this process if a second (anchor) controller is being used in the network.

## AAA Servers

When you choose the AAA Servers tab, the page shown in Figure 12-13 appears.

*Figure 12-13 AAA Servers Page*




Follow these steps to configure the AAA Servers tab.

**Step 1** Use the drop-down lists in the RADIUS and LDAP servers section to choose authentication and accounting servers. This selects the default RADIUS server for the specified WLAN and overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority and so on.

If no LDAP servers are chosen here, WCS uses the default LDAP server order from the database.

**Step 2** Click the Local EAP Authentication check box if you have an EAP profile already configured that you want to enable. Local EAP is an authentication method that allows users and wireless clients to locally authenticate. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

**Step 3** When AAA Override is enabled, and a client has conflicting AAA and controller WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system also uses QoS and ACL provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as identity networking.)

For instance, if the corporate WLAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.

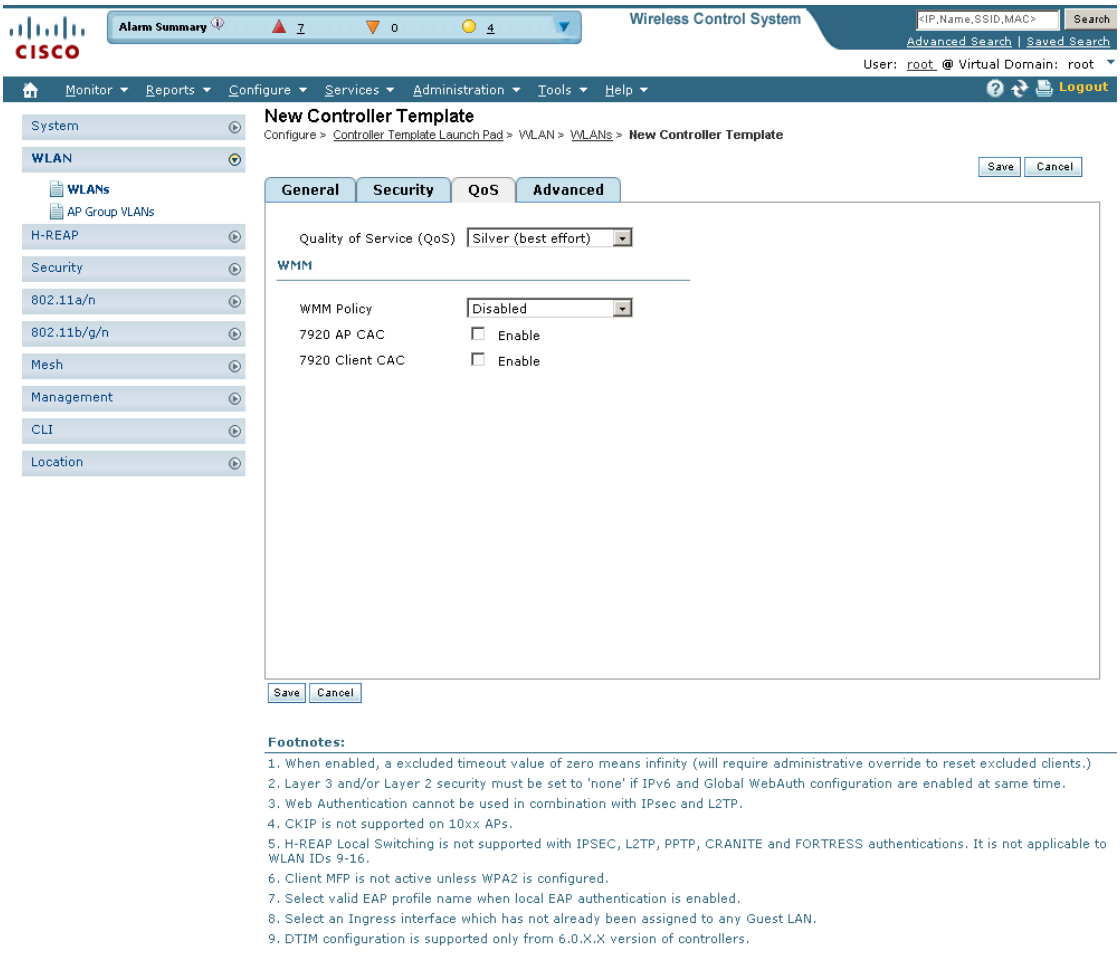
The AAA override values may come from a RADIUS server, for example.

**Step 4** Click **Save**.

## QoS

When you select the QoS tab from the WLAN Template page, the page as shown in Figure 12-14 appears.

***Figure 12-14 QoS Page***



Follow these steps to configure the QoS tab.

**Step 1** Use the QoS drop-down list to choose Platinum (voice), Gold (video), Silver (best effort), or Bronze (background). Services such as VoIP should be set to gold while non-discriminating services such as text messaging can be set to bronze.

**Step 2** Use the WMM Policy drop-down list to choose Disabled, Allowed (so clients can communicate with the WLAN), or Required to make it mandatory for clients to have WMM enabled for communication.

**Step 3** Click the **7920 AP CAC** check box if you want to enable support on Cisco 7920 phones.

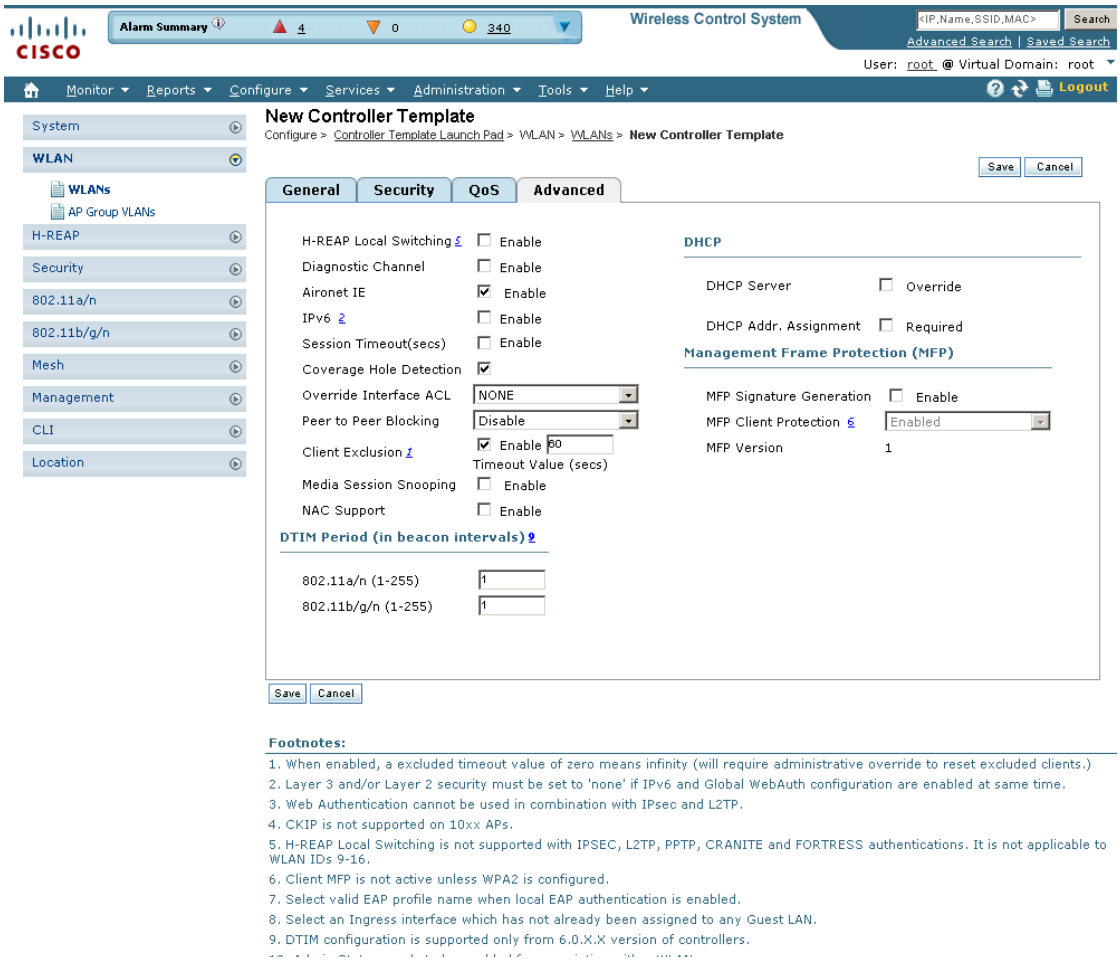
**Step 4** If you want WLAN to support older versions of the software on 7920 phones, click to enable the **7920 Client CAC** check box. The CAC limit is set on the access point for newer versions of software.

**Step 5** Click **Save**.

## Advanced

When you click the Advanced tab in the WLAN Template page, the page shown in Figure 12-15 appears.

***Figure 12-15 Advanced Page***



**Step 1** Click the check box if you want to enable Hybrid REAP local switching. For more information on Hybrid REAP, see the "Configuring Hybrid REAP" section on page 15-4. If you enable it, the hybrid-REAP access point handles client authentication and switches client data packets locally.

H-REAP local switching is only applicable to the Cisco 1130/1240/1250 series access points. It is not supported with L2TP or PPTP authentications, and it is not applicable to WLAN IDs 9-16.

**Step 2** Choose to enable the diagnostic channel feature or leave it disabled. The diagnostic channel feature allows you to troubleshoot problems regarding client communication with a WLAN. When initiated by a client having difficulties, the diagnostic channel provides the most robust communication methods with the fewest obstacles to communication.

**Step 3** Check the Aironet IE check box if you want to enable support for Aironet information elements (IEs) for this WLAN. If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

**Step 4** Click to enable IPv6. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.

**Step 5** At the Session Timeout parameter, set the maximum time a client session can continue before requiring reauthorization.

**Step 6** Choose to enable or disable coverage hold detection(CHD) on this WLAN. By default CHD is enabled on all WLANs on the controller. If you disable CHD on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where highly mobile guests are connected to your network for short periods of time.

**Step 7** A list of defined access control lists (ACLs) is provided at the Override Interface ACL drop-down list. (See the "Configuring Access Control List Templates" section on page 12-69 for steps on defining ACLs.) Upon choosing an ACL from the list, the WLAN associates the ACL to the WLAN. Selecting an ACL is optional, and the default for this parameter is None.

**Step 8** You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. At the Peer to Peer Blocking drop-down list, choose one of the following:

- Disable—Peer-to-peer blocking is disabled, and traffic is bridged locally whenever possible.
- Drop—The packet is discarded.
- Forward Up Stream—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet.

If H-REAP local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is grayed out.

**Note** Peer-to-peer blocking does not apply to multicast traffic.

**Step 9** Click the check box if you want to enable automatic client exclusion. If you enable client exclusion, you must also set the Timeout Value in seconds for disabled client machines. Client machines are excluded by MAC address, and their status can be observed. A timeout setting of 0 indicates that administrative control is required to re-enable the client.

**Note** When session timeout is not set, it implies that an excluded client remains and will not timeout from the excluded state. It does not imply that the exclusion feature is disabled.

**Step 10** Click to enable Media Session Snooping. This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and WCS. It can be enabled or disabled per WLAN.

When media session snooping is enabled, the access point radios that advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.

**Step 11** Check the NAC Support check box if you want to enable it. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing. See the "Configuring NAC Out-of-Band Integration" section on page 10-45 for more information.

**Step 12** When you click the check box to override DHCP server, another parameter appears where you can enter the IP address of your DHCP server. For some WLAN configurations, this is required. Three valid configurations are as follows:

- DHCP Required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server.
- DHCP is not required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server or use a static IP address.
- DHCP not required and DHCP server IP address 0.0.0.0 - All WLAN clients are forced to use a static IP address. All DHCP requests are dropped.

You cannot choose to require a DHCP address assignment and then enter a DHCP server IP address.

**Step 13** If the MFP Signature Generation check box is checked, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. Signature generation makes sure that changes to the transmitted management frames by an intruder are detected and reported.

**Step 14** At the MFP Client Protection drop-down list, choose Optional, Disabled, or Required for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable.

**Note** Client-side MFP is only available for those WLANs configured to support Cisco Compatible Extensions (version 5 or later) clients, and WPA2 must first be configured.

**Step 15** Enter a value between 1 and 255 beacon intervals in the 802.11a/n DTIM Period portion of the page. The controller sends a DTIM packet on the 802.11a/n radio for this WLAN based on what is entered as an interval.

**Step 16** Enter a value between 1 and 255 beacon intervals in the 802.11b/g/n DTIM Period portion of the page. The controller sends a DTIM packet on the 802.11b/g/n radio for this WLAN based on what is entered as an interval.

**Note** DTIM configuration is not appropriate for guest LANs.

**Step 17** Click **Save**.

# Configuring WLAN AP Groups

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits include more effective management of load balancing and bandwidth allocation.

Follow these steps to configure WLAN AP Groups.

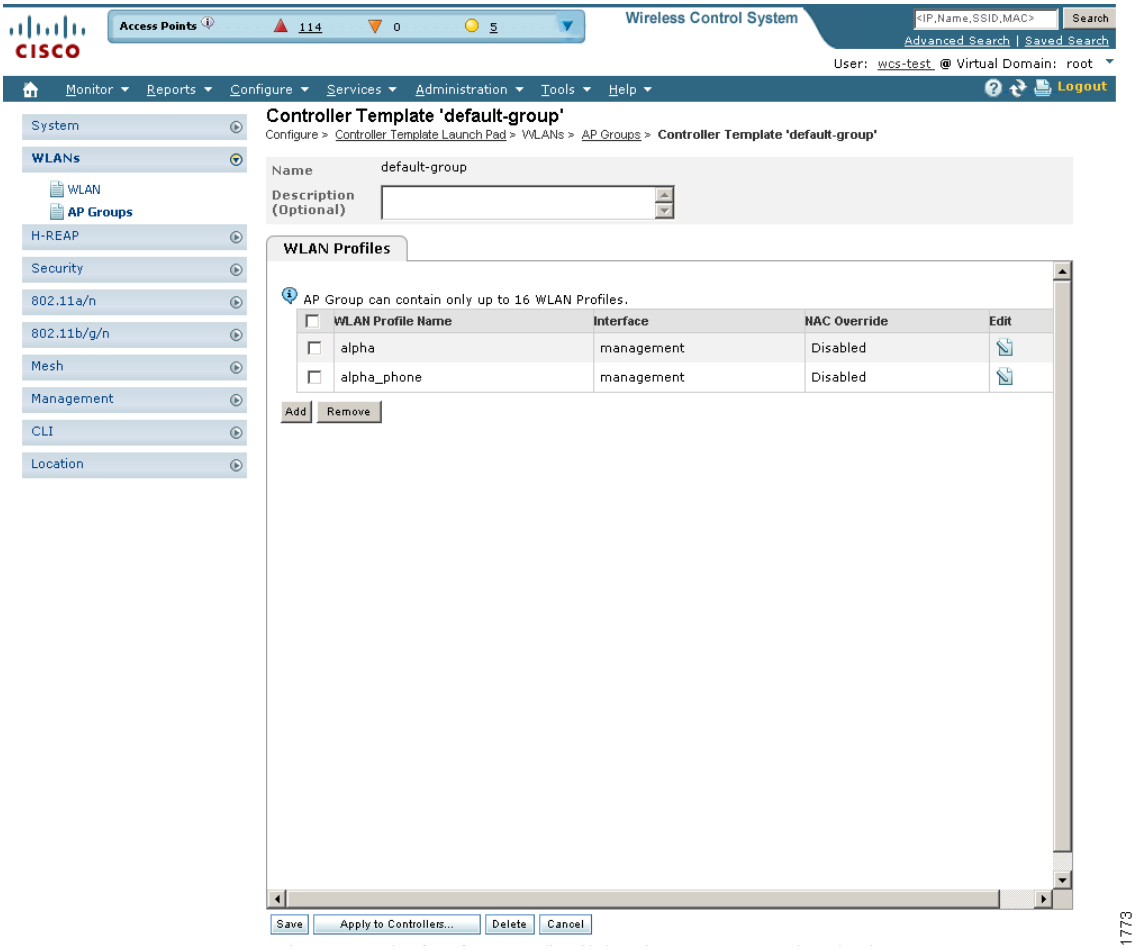
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **AP Groups** or choose **WLAN > AP Groups** from the left sidebar menu. The WLAN > AP Groups page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP Groups template page appears (see Figure 12-16).

*Figure 12-16 WLAN AP Groups*



This page displays a summary of the AP groups configured on your network. From here you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Click the check box in the WLAN Profile Name column and click Remove to delete WLAN profiles.

## Adding Access Point Groups

Follow these steps to add a new access point group.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **AP Group VLANs** or choose **WLAN > AP Group VLANs** from the left sidebar menu.

**Note** AP Groups (for 5.2 and above controllers) are referred to as AP Group VLANs for controllers prior to 5.2.

**Step 3** Choose **Add Template** from the Select a command drop-down list, and click **Go**.

**Step 4** Enter a name and group description for the access point group.

**Note** The group description is optional.

**Step 5** Click the **WLAN Profile** check box.

**Note** To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles display in the drop-down list.

**Note** Each access point is limited to sixteen WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

**Note** The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

**Step 6** Type a WLAN profile name or select one from the WLAN Profile Name drop-down list.

**Step 7** Enter an interface or select one from the Interface drop-down list.

**Note** To display all available interfaces, delete the current interface from the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces display in the drop-down list.

**Step 8** Click the **NAC Override** check box, if applicable. NAC override is disabled by default.

**Step 9** When access points and WLAN profiles are added, click **Add**.

**Note** After saving, click the edit icon on the WLAN Profiles tab to edit the WLAN profile information.

## Deleting Access Point Groups

Follow these steps to delete an access point group.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **AP Groups** or choose **WLAN > AP Groups** from the left sidebar menu.

**Step 3** Click **Remove**.

# Configuring H-REAP AP Groups

Hybrid REAP enables you to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of hybrid-REAP access points per location, but you can organize and group the access points per floor and limit them to 25 or so per building, since it is likely the branch offices share the same configuration.

Follow these steps to set up an H-REAP AP group.

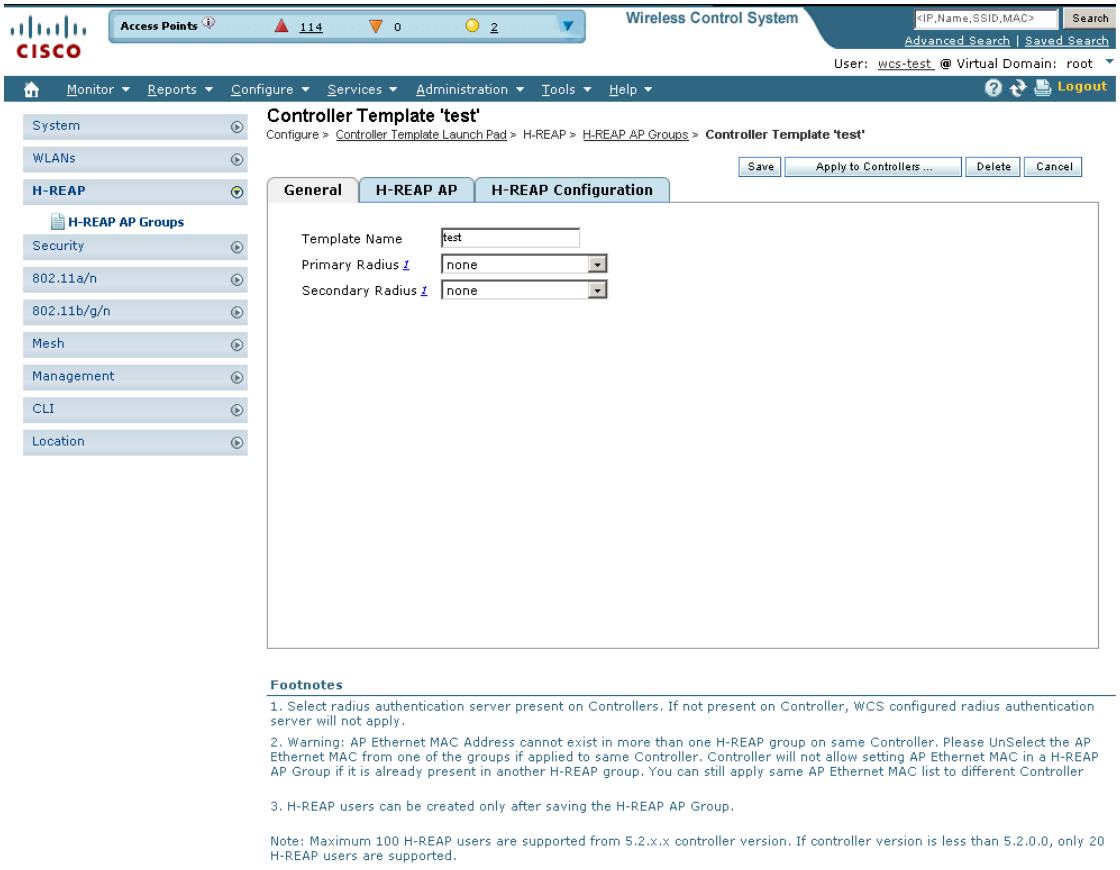
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **H-REAP AP Groups** or choose **H-REAP > H-REAP AP Groups** from the left sidebar menu. The H-REAP > H-REAP AP Groups page appears. It displays the primary and secondary RADIUS, as well as the number of controllers and virtual domains that the template is applied to, which automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The General tab of the H-REAP AP Groups page appears (see Figure 12-17).

*Figure 12-17 AP Groups H-REAP Template*




**Step 4** The Template Name parameter shows the group name assigned to the HREAP access point group.

**Step 5** Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply. A value of 10 indicates that the primary RADIUS server is not configured for this group.

**Step 6** Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply. A value of 0 indicates that the primary RADIUS server is not configured for this group.

**Step 7** If you want to add an access point to the group, click the **H-REAP AP** tab.

**Step 8** An access point Ethernet MAC address cannot exist in more than one H-REAP group on the same controller. If more than one group is applied to the same controller, click the **Ethernet MAC** check box to unselect an access point from one of the groups. You should save this change or apply it to controllers.

**Step 9** Click **Add AP**. The H-REAP AP Group page appears.

**Step 10** Click the **H-REAP Configuration** tab to enable local authentication for a hybrid REAP group.

**Note** Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None** on the General tab.

**Step 11** Select the **H-REAP Local Authentication** check box to enable local authentication for this hybrid-REAP group. The default value is unselected.

**Note** When you attempt to use this feature, a warning message indicates that it is a licensed feature.

**Step 12** To allow a hybrid-REAP access point to authenticate clients using LEAP, check the **LEAP** check box. Otherwise, to allow a hybrid-REAP access point to authenticate clients using EAP-FAST, check the **EAP-FAST** check box.

**Step 13** Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key and Confirm EAP-FAST Key text box. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, check the **Auto key generation** check box.

**Step 14** In the EAP-FAST Key text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

**Step 15** In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

**Step 16** In the EAP-FAST Pac Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.

**Step 17** Click **Submit**.

# Configuring a File Encryption Template

This page enables you to add a file encryption template or make modifications to an existing file encryption template.

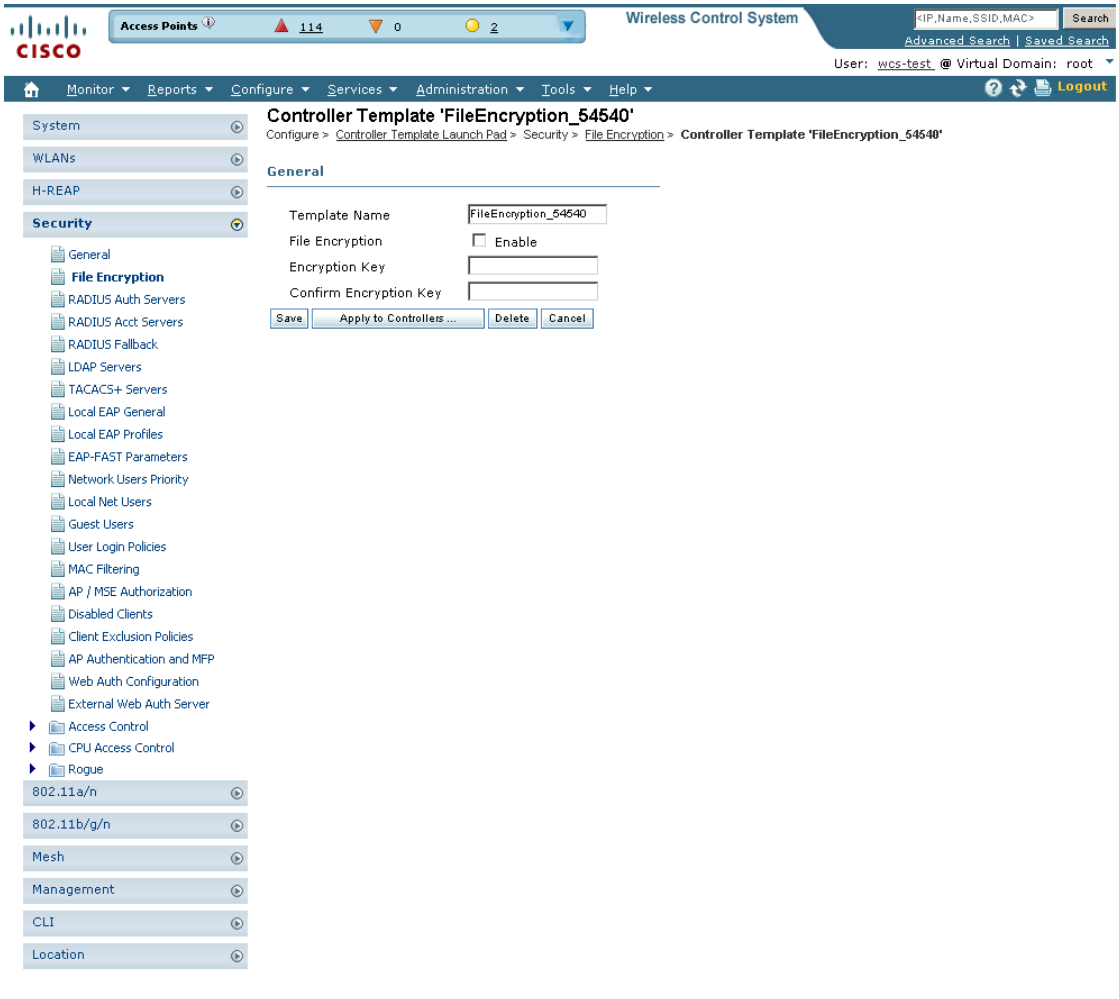
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **File Encryption** or choose **Security > File Encryption** from the left sidebar menu. The Security > File Encryption page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The File Encryption template page appears (see Figure 12-18).

*Figure 12-18 File Encryption Template*




**Step 4** Check if you want to enable file encryption.

**Step 5** Enter an encryption key text string of exactly 16 ASCII characters.

**Step 6** Retype the encryption key.

**Step 7** Click **Save**.

# Configuring a RADIUS Authentication Template

This page allows you to add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

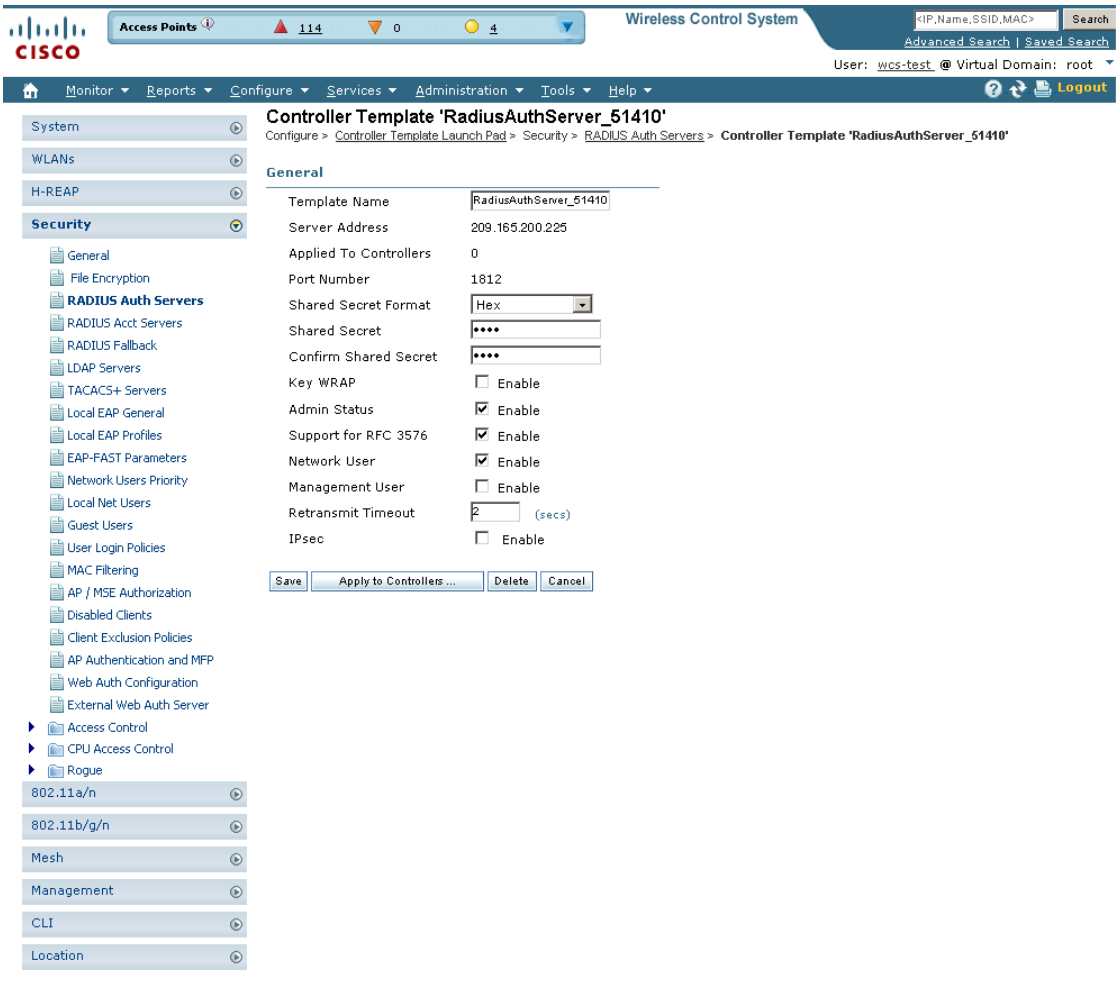
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **RADIUS Auth Servers** or choose **Security > RADIUS Auth Servers** from the left sidebar menu. The Security > RADIUS Auth Servers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The IP address of the RADIUS server and the port number and admin status for the interface protocol is also displayed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Auth Servers template page appears (see Figure 12-19).

***Figure 12-19 RADIUS Authentication Server Template***




**Step 4** Use the Shared Secret Format drop-down list to choose either ASCII or hex shared secret format.

**Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

**Step 5** Enter the RADIUS shared secret used by your specified server.

**Step 6** Click if you want to enable key wrap. If this option is enabled, the authentication request is sent to RADIUS servers that have key encryption key (KEK) and message authenticator code keys (MACK) configured. Also, when enabled, the parameters below appear:

- Shared Secret Format: Determine whether ASCII or hexadecimal.

  **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

- KEK Shared Secret: Enter KEK shared secret.
- MACK Shared Secret: Enter MACK shared secret.

**Note** Each time the controller is notified with the shared secret, the existing shared secret is overwritten with the new shared secret.

**Step 7** Click if you want to enable administration privileges.

**Step 8** Click if you want to enable support for RFC 3576. RFC 3576 is an extension to the Remote Authentication Dial In User Service (RADIUS) protocol. It allows dynamic changes to a user session and includes support for disconnecting users and changing authorizations applicable to a user session. With these authorizations, support is provided for Disconnect and Change-of-Authorization (CoA) messages. Disconnect messages immediately terminate a user session, whereas CoA messages modify session authorization attributes such as data filters.

**Step 9** Click if you want to enable network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.

**Step 10** Click if you want to enable management authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user.

**Step 11** Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller. You can specify a value between 2 and 30 seconds.

**Step 12** If you click to enable the IP security mechanism, additional IP security parameters are added to the page, and Steps 13 to 19 are required. If you disable it, click **Save** and skip Steps 13 to 19.

**Step 13** Use the drop-down list to choose which IP security authentication protocol to use. The options are HMAC-SHA1, HMAC-MD5, and None.

Message Authentication Codes (MAC) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions and can be used in combination with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

**Step 14** Set the IP security encryption mechanism to use. Options are as follows:

- DES—Data Encryption Standard is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
- Triple DES—Data Encryption Standard that applies three keys in succession.
- AES 128 CBC—Advanced Encryption Standard uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Clock Chaining (CBC) mode.
- None—No IP security encryption mechanism.

**Step 15** The Internet Key Exchange (IKE) authentication is not an editable text box. Internet Key Exchange protocol (IKE) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how data should be protected. IKE keeps track of connections by assigning a bundle of security associations (SAs) to each connection.

**Step 16** Use the IKE phase 1 drop-down list to choose either aggressive or main. This sets the IKE protocol. IKE phase 1 is used to negotiate how IKE is protected. Aggressive mode passes more information in fewer packets, with the benefit of a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.

**Step 17** At the Lifetime parameter, set the timeout interval (in seconds) when the session expires.

**Step 18** Set the IKE Diffie Hellman group. The options are group 1 (768 bits), group 2 (1024 bits), or group 5 (1536 bits). Diffie-Hellman techniques are used by two devices to generate a symmetric key where you can publicly exchange values and generate the same symmetric key.

Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size.

**Step 19** Click **Save**.

# Configuring a RADIUS Accounting Template

This page allows you to add a RADIUS accounting template or make modifications to an existing RADIUS accounting template.

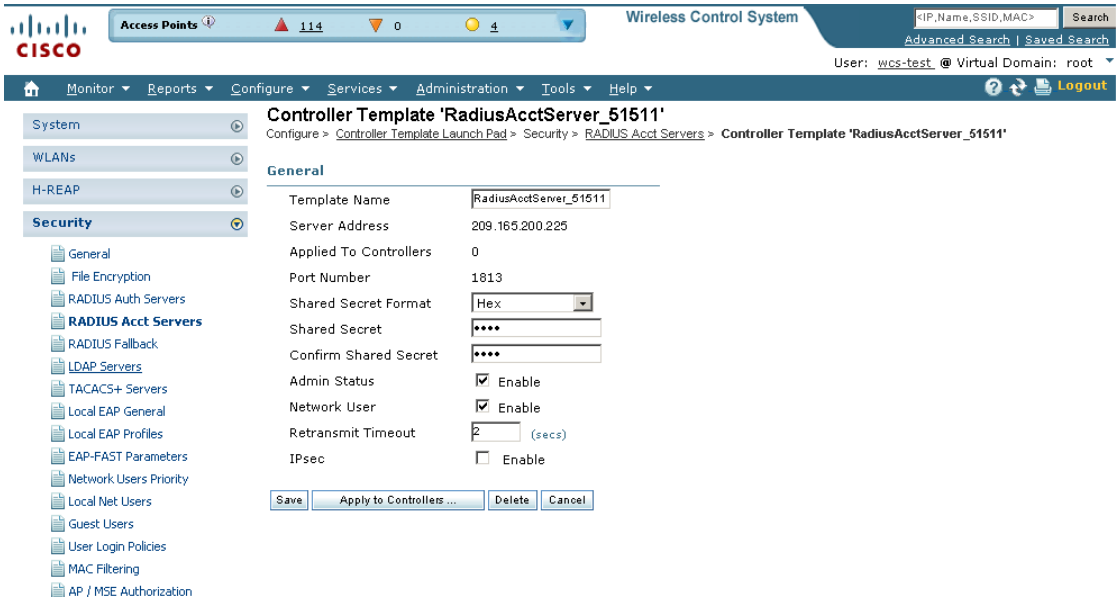
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **RADIUS Acct Servers** or choose **Security > RADIUS Acct Servers** from the left sidebar menu. The Security > RADIUS Acct Servers page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The IP address of the RADIUS server and the port number and admin status for the interface protocols are also displayed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Accounting Server template page appears (see Figure 12-20).

*Figure 12-20 RADIUS Accounting Server Templates*




**Step 4** Use the Shared Secret Format drop-down list to choose either ASCII or hexadecimal.

**Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

**Step 5** Enter the RADIUS shared secret used by your specified server.

**Step 6** Retype the shared secret.

**Step 7** Click if you want to establish administrative privileges for the server.

**Step 8** Click if you want to enable the network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.

**Step 9** Specify the time in seconds after which the RADIUS authentication request will timeout and a retransmission by the controller will occur. You can specify a value between 2 and 30 seconds.

**Step 10** Click **Save**.

# Configuring a RADIUS Fallback Template

This page allows you to add a RADIUS fallback template or make modifications to an existing RADIUS fallback template.

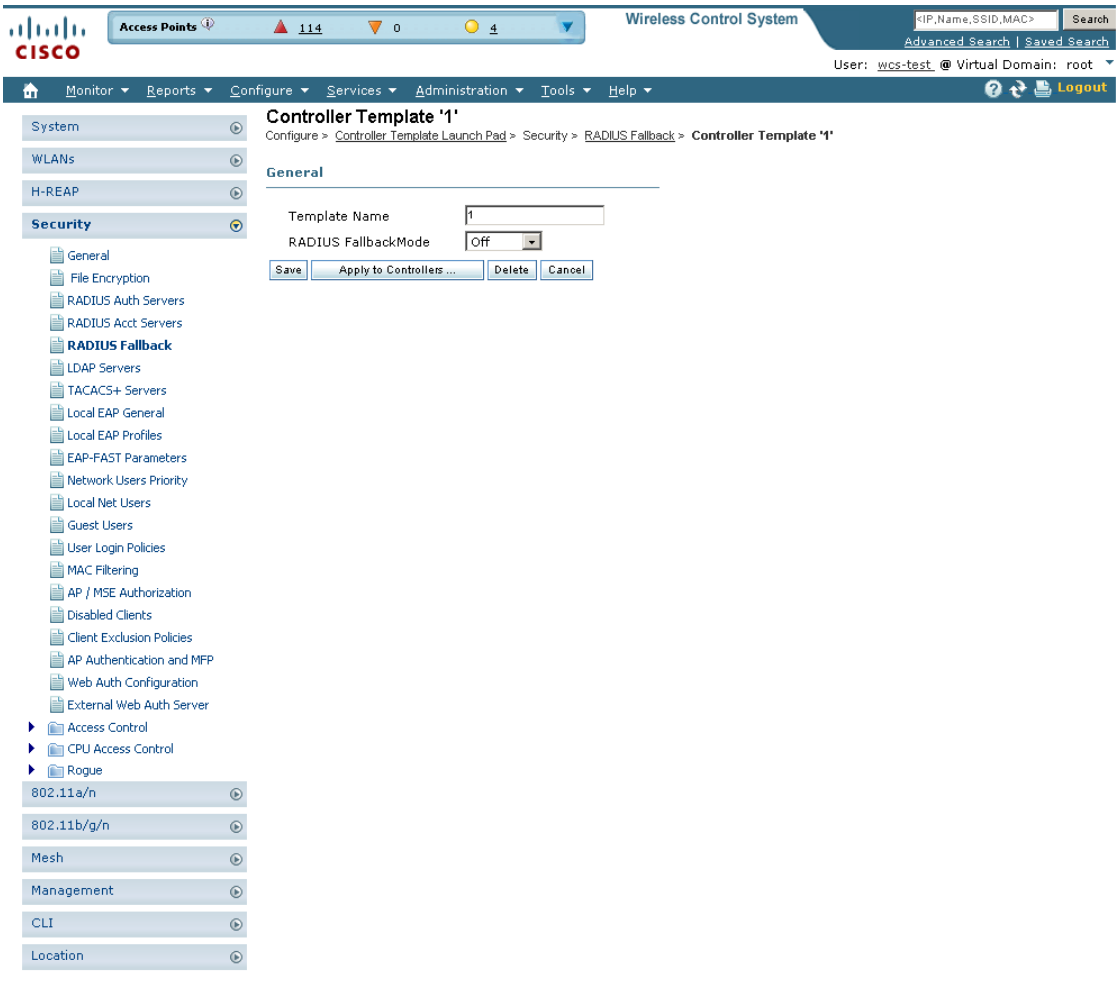
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **RADIUS Fallback** or choose **Security > RADIUS Fallback** from the left sidebar menu. The Security > RADIUS Fallback page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The RADIUS Fallback template page appears (see Figure 12-21).

***Figure 12-21 RADIUS Fallback Page***




**Step 4** From the RADIUS Fallback Mode drop-down list, choose **Off**, **Passive**, or **Active**.

- Off—Disables fallback.
- Passive—You must enter a time interval.
- Active—You must enter a username and time interval.

**Step 5** Click **Save**.

# Configuring a LDAP Server Template

This section explains how to configure a Lightweight Directory Access Protocol (LDAP) server as a backend database, similar to a RADIUS or local user database. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP may use an LDAP server as its backend database to retrieve user credentials. Follow these steps to add an LDAP server template or make modifications to an existing LDAP server template.

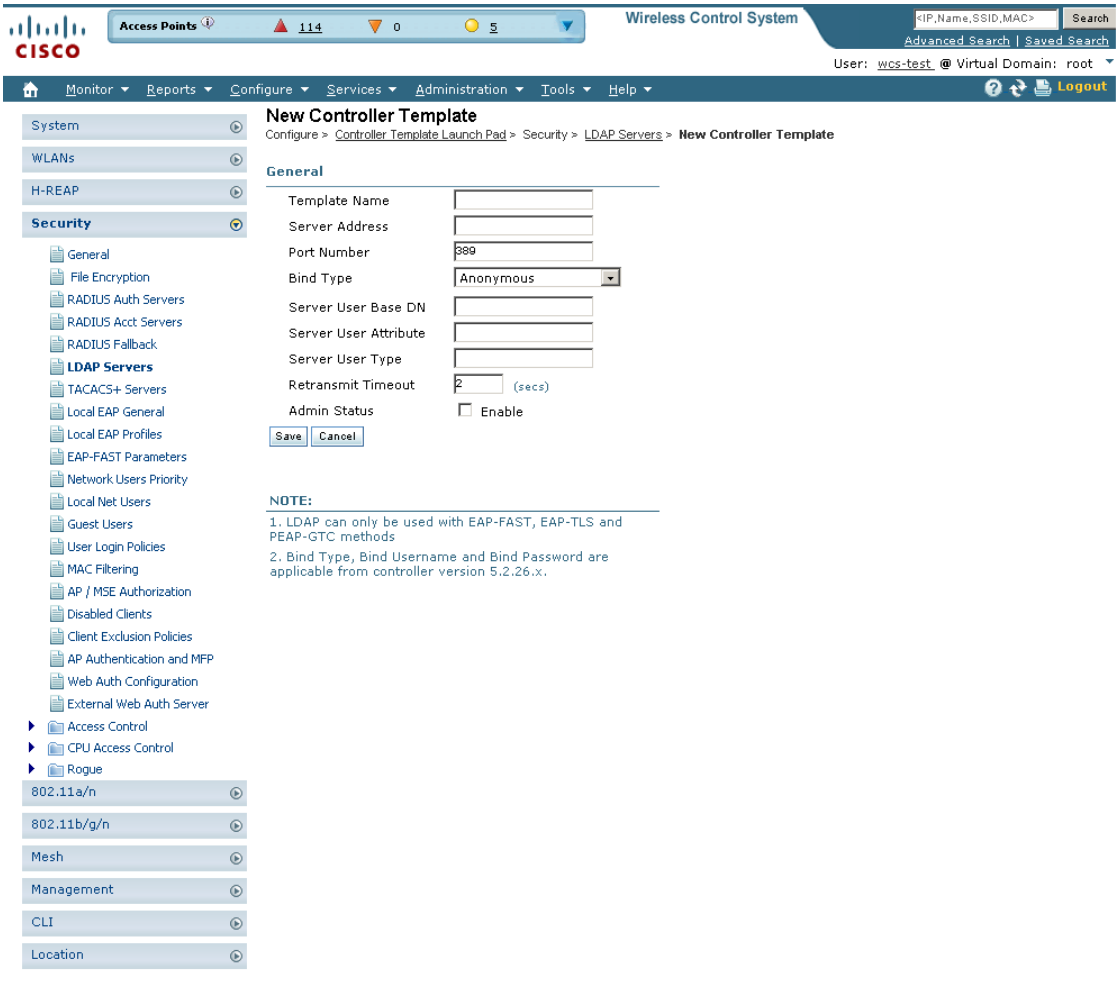
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **LDAP Servers** or choose **Security > LDAP Servers** from the left sidebar menu. The Security > LDAP Servers page appear. The IP address of the LDAP server and the port number for the interface protocols are displayed. Also, the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The LDAP Server template page appears (see Figure 12-22).

*Figure 12-22 LDAP Server Template*




**Step 4** The port number of the controller to which the access point is connected.

**Step 5** From the Bind Type drop-down list, choose **Authenticated** or **Anonymous**. If you choose Authenticated, you must enter a bind username and password as well. A bind is a socket opening that performs a lookup. Anonymous bind requests are rejected.

**Step 6** In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

**Step 7** In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.

**Step 8** In the Server User Type text box, enter the ObjectType attribute that identifies the user.

**Step 9** In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

**Step 10** Select the **Admin Status** check box if you want the LDAP server to have administrative privileges.

**Step 11** Click **Save**.

# Configuring a TACACS+ Server Template

This page allows you to add a TACACS+ server or make modifications to an existing TACACS+ server template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

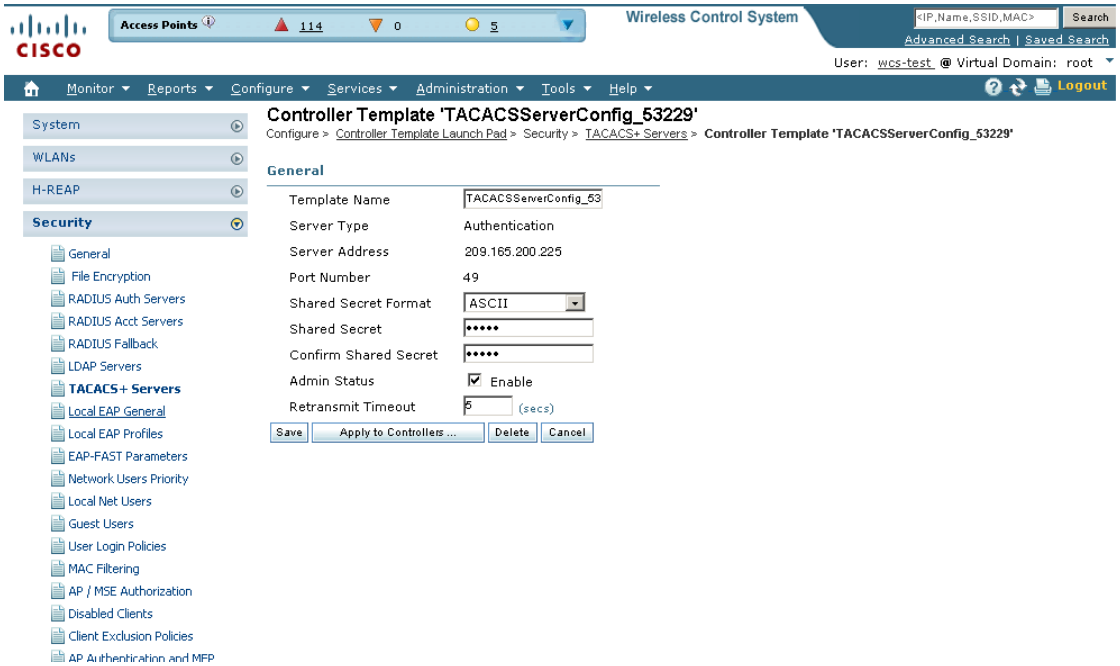
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **TACACS+ Server** or choose **Security > TACACS+ Server** from the left sidebar menu. The Security > TACACS+ Servers page appears. The IP address and the port number and admin of the TACACS+ template are displayed. Also, the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The TACACS+ Servers template page appears (see Figure 12-23).

***Figure 12-23 TACACS+ Server Template***




**Step 4** Select the server type. The choices are authentication, authorization, or accounting.

**Step 5** Use the drop-down list to choose either ASCII or hex shared secret format.

**Note** Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC (and WCS). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.

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

**Step 7** Re-enter the shared secret in the Confirm Shared Secret text box.

**Step 8** Check the Admin Status check box if you want the TACACS+ server to have administrative privileges.

**Step 9** Specify the time in seconds after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

**Step 10** Click **Save**.

# Configuring a Local EAP General Template

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.

**Note** If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

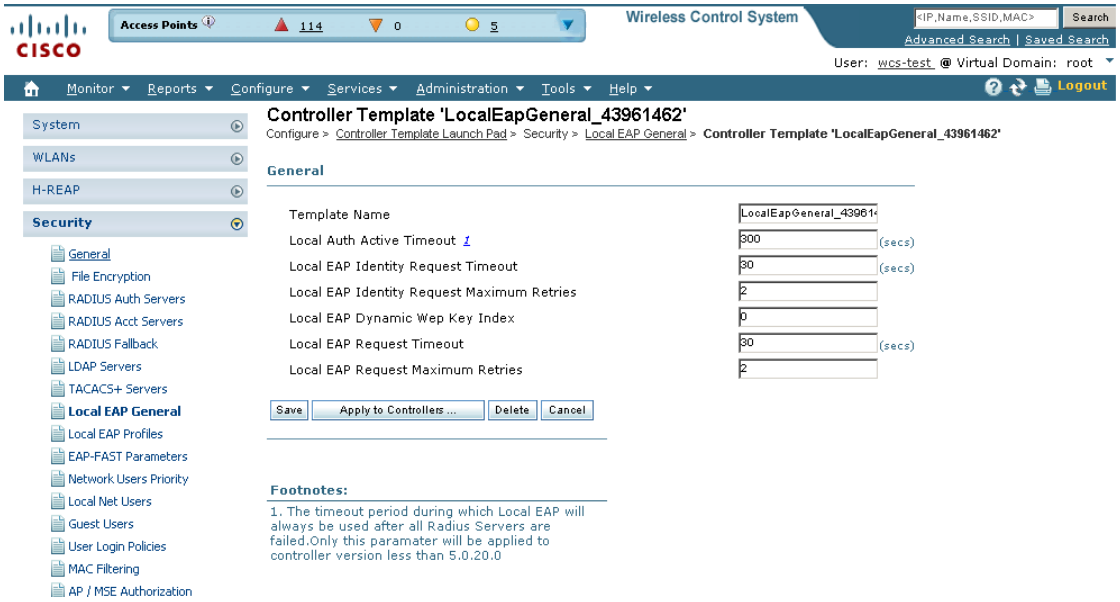
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Local EAP General** or choose **Security > Local EAP General** from the left sidebar menu. The Security > Local EAP General page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local EAP General controller template page appears (see Figure 12-24).

*Figure 12-24 Local EAP General Template*




**Step 4** In the Local Auth Active Timeout text box, enter the amount of time (in seconds) that the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fail. The valid range is 1 to 3600 seconds, and the default setting is 1000 seconds.

**Step 5** The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones. You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. The recommended and default timeout on the Cisco ACS server is 20 seconds.

**Note** Roaming fails if these values are not set the same across multiple controllers.

- Local EAP Identify Request Timeout =1
- Local EAP Identity Request Maximum Retries=20
- Local EAP Dynamic WEP Key Index=0
- Local EAP Request Timeout=20
- Local EAP Request Maximum Retries=2

**Step 6** Click **Save**.

# Configuring a Local EAP Profile Template

This page allows you to add a local EAP profile template or make modifications to an existing template. Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable

local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.

**Note** The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

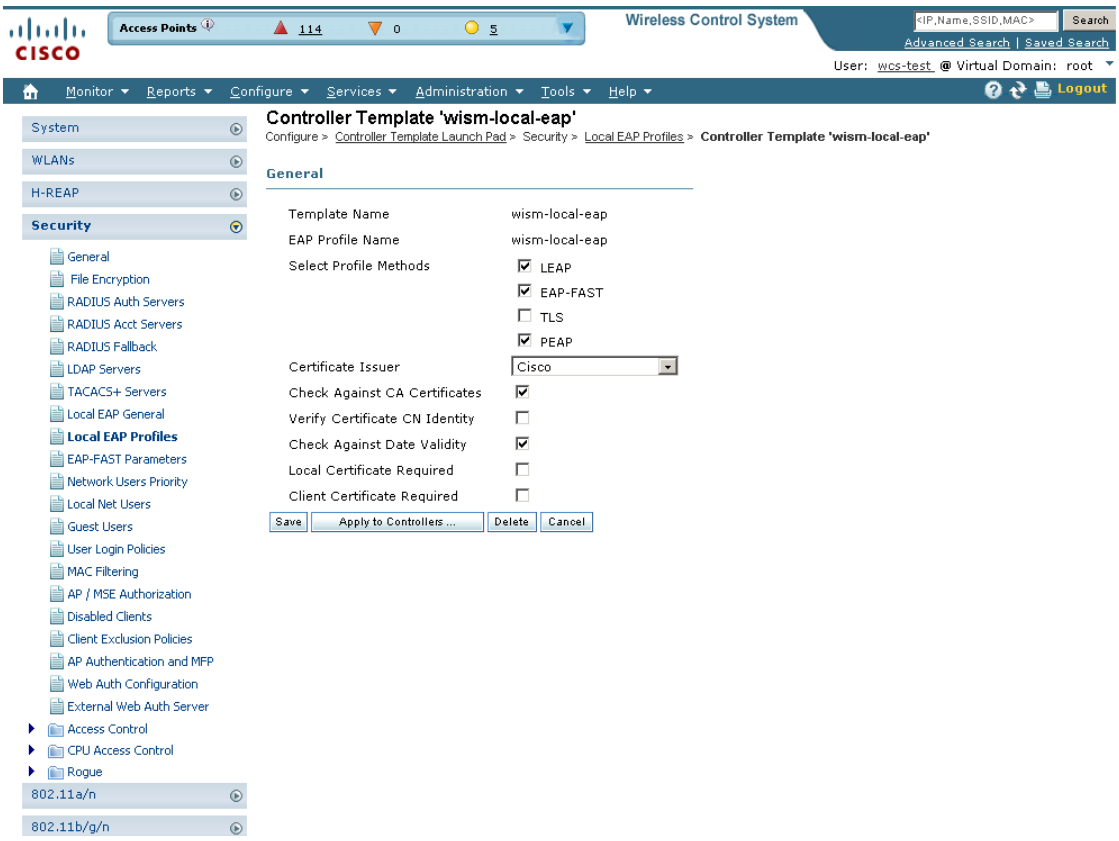
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Local EAP Profiles** or choose **Security > Local EAP Profiles** from the left sidebar menu. The Security > Local EAP Profiles page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. It also shows the EAP profile name and indicates whether LEAP, EAP-FAST, TLS, or PEAP is used. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local EAP Profiles template page appears (see Figure 12-25).

***Figure 12-25 Local EAP Profiles Template***



**Step 4** Each EAP profile must be associated with an authentication type(s). Choose the desired authentication type from the choices below:

- LEAP — This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST — This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS — This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—This authentication type is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

**Step 5** Use the Certificate Issuer drop-down list to determine whether Cisco or another vendor issued the certificate for authentication. Only EAP-FAST and TLS require a certificate.

**Step 6** If you want the incoming certificate from the client to be validated against the certificate authority (CA) certificates on the controller, check the **Check Against CA Certificates** check box.

**Step 7** If you want the common name (CN) in the incoming certificate to be validated against the CA certificates' CN on the controller, check the **Verify Certificate CN Identity** check box.

**Step 8** If you want the controller to verify that the incoming device certificate is still valid and has not expired, check the **Check Against Date Validity** check box.

**Step 9** If a local certificate is required, click the check box.

**Step 10** If a client certificate is required, click the check box.

**Step 11** Click **Save**.

**Step 12** Follow these steps to enable local EAP:

a. Choose **WLAN > WLAN Configuration** from the left sidebar menu.

b. Click the profile name of the desired WLAN.

c. Click the **Security > AAA Servers** tab to access the AAA Servers page.

d. Check the **Local EAP Authentication** check box to enable local EAP for this WLAN.

**Step 13** Click **Save**.

# Configuring an EAP-FAST Template

This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point. This page allows you to add an EAP-FAST template or make modifications to an existing EAP-FAST template.

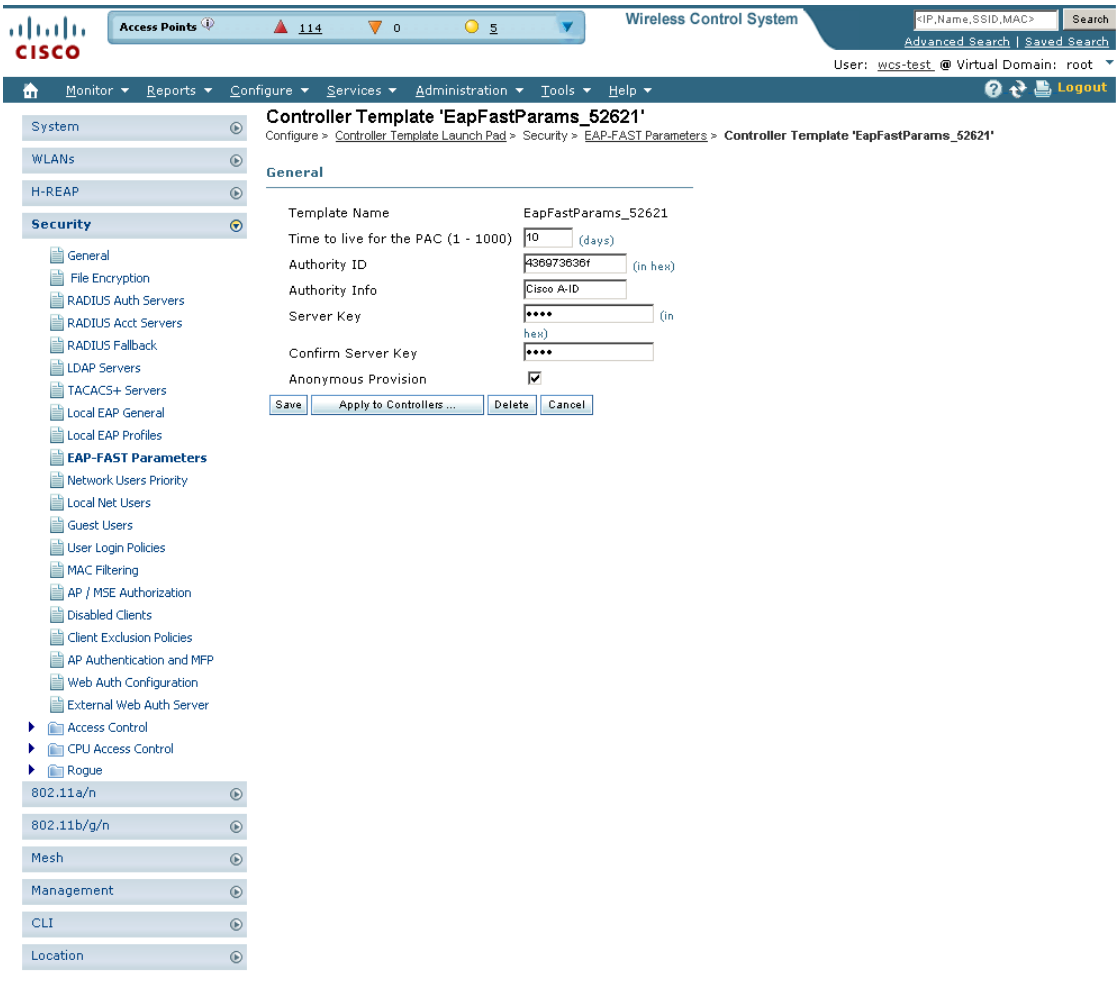
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **EAP-FAST Parameters** or choose **Security > EAP-FAST Parameters** from the left sidebar menu. The Security > EAP-FAST Parameters page appears. The number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The EAP-FAST Parameters template page appears (see Figure 12-26).

***Figure 12-26 EAP-FAST Parameters Template***




**Step 4** In the Time to Live for the PAC text box, enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.

**Step 5** In the Authority ID text box, enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.

**Step 6** In the Authority ID text box, enter the ID for the authority identifier of the local EAP-FAST server.

**Step 7** In the Authority Info text box, enter the authority identifier of the local EAP-FAST server in text format.

**Step 8** In the Server Key and Confirm Server Key fields, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

**Step 9** If you want to enable anonymous provisioning, check the **Anonymous Provision** check box. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned.

**Step 10** Click **Save**.

# Configuring Network User Credential Retrieval Priority Templates

You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add or make modifications to an existing network user credential retrieval priority template.

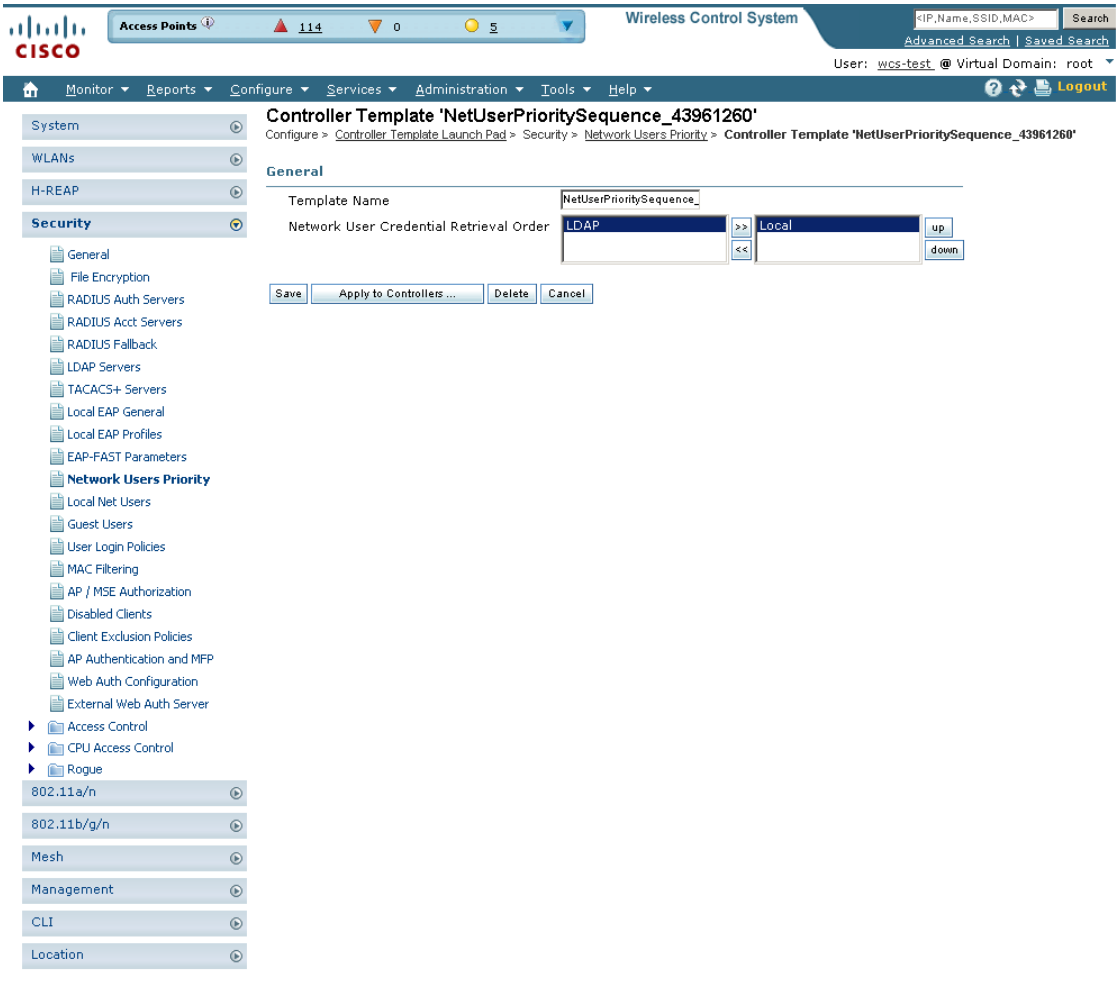
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Network Users Priority** or choose **Security > Network Users Priority** from the left sidebar menu. The Security > Network User Credential Retrieval Priority page appears. The network retrieval order and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Network Users Priority template page appears (see Figure 12-27).

*Figure 12-27 Network User Credential Retrieval Priority Order Template*




**Step 4** Use the left and right pointing arrows to include or disclude network user credentials in the right page.

**Step 5** Use the up and down buttons to determine the order credentials are tried.

**Step 6** Click **Save**.

# Configuring a Local Network Users Template

With this template, you can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP may use the local user database as its backend database to retrieve user credentials. This page allows you to add or make modifications to an existing local network user template. You must create a local net user and define a password when logging in as a web authentication client.

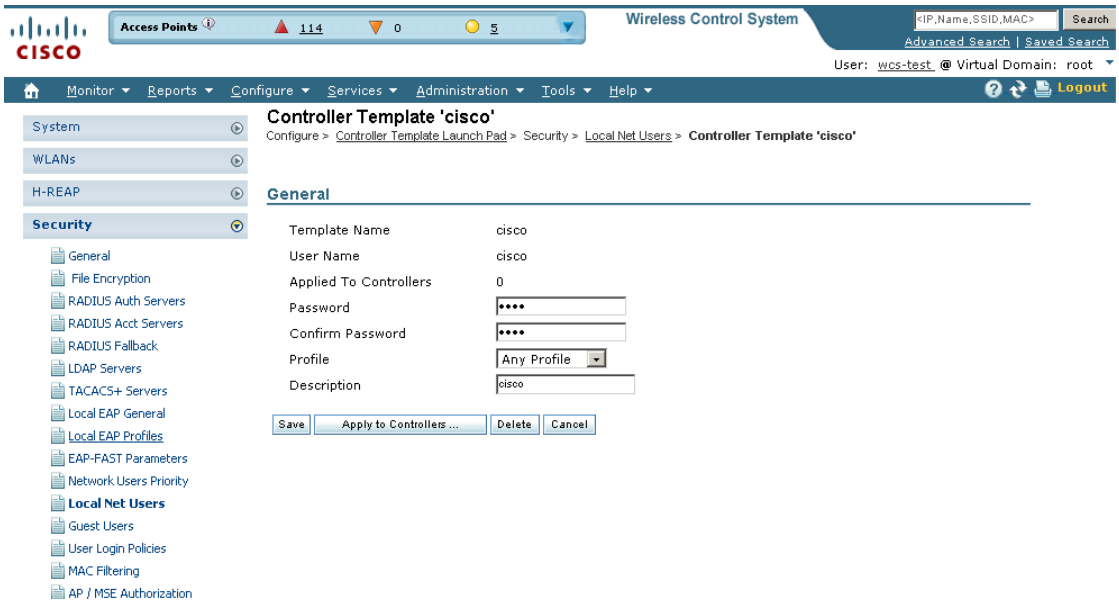
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Local Net Users** or choose **Security > Local Net Users** from the left sidebar menu. The Security > Local Net Users page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local Net Users template page appears (see Figure 12-28).

***Figure 12-28 Local Net Users Template***




**Step 4** If you keep Import from File enabled, you need to enter a file path or click the Browse button to navigate to the file path. Then continue to Step 11. If you disable the import, continue to Step 5.

**Note** You can only import a.csv file. Any other file formats are not supported.

The first row in the file is the header. The data in the header is not read by the Cisco WCS. The header can either be blank or filled. The Cisco WCS reads data from the second row onwards.

**Step 5** Enter a username and password.It is mandatory to fill the Username and Password fields in all the rows.

**Step 6** Enter a profile. The Profile column if left blank (or filled in with *any profile*) means a client on any profile can use this account.

**Step 7** Enter a description of the profile.

**Step 8** Use the drop-down list to choose the SSID which this local user is applied to or choose the *any SSID* option.

**Step 9** Enter a user-defined description of this interface. Skip to Step11.

**Step 10** If you want to override the existing template parameter, click to enable this parameter.

**Step 11** Click **Save**.

# Configuring Guest User Templates

This page allows you to add a guest user template or make modifications to an existing guest user template. The purpose of a guest user account is to provide a user account for a limited amount of time. A Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires. See the "Creating Guest User Accounts" section on page 7-10 for further information on guest access.

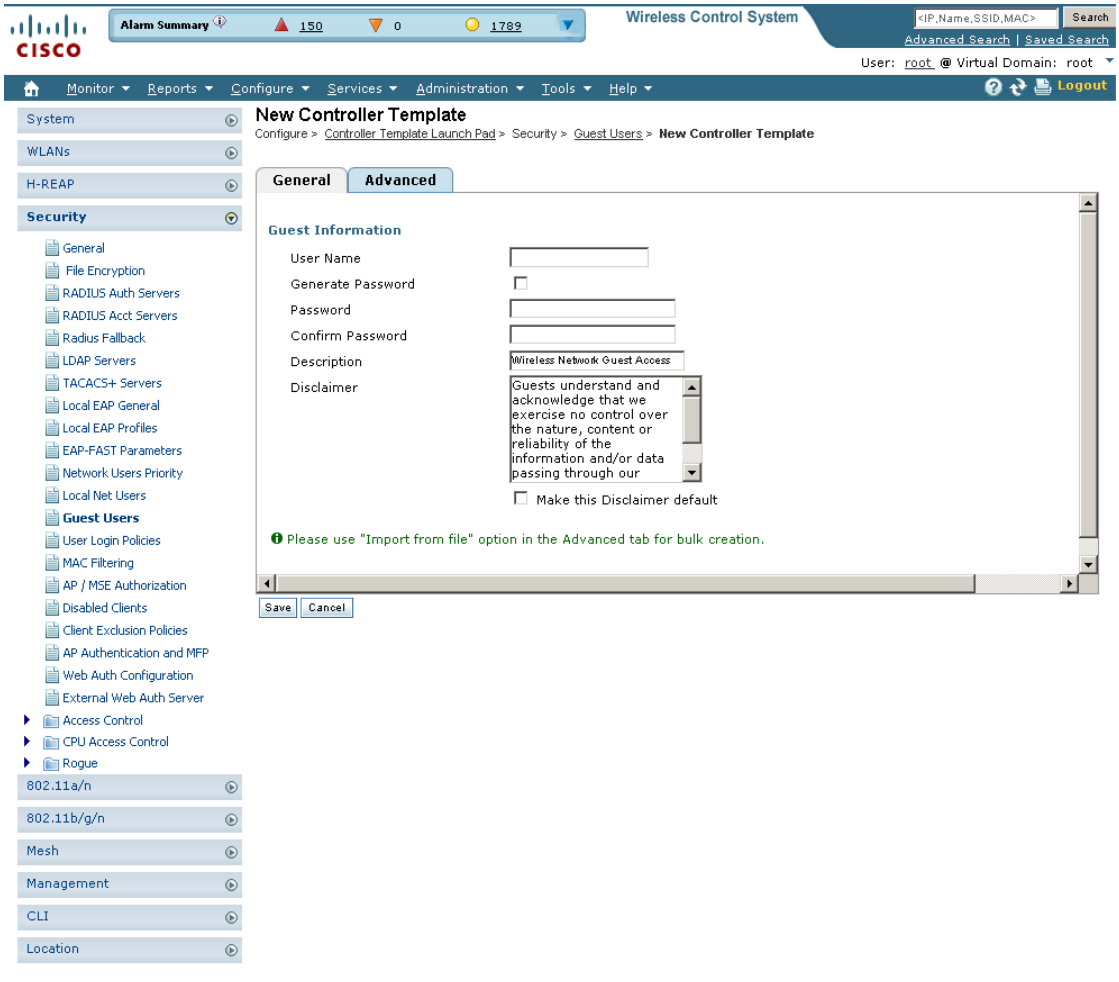
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Guest Users** or choose **Security > Guest Users** from the left sidebar menu.The Security > Guest User page appears.

**Note** To reduce clutter, WCS does not show expired templates by default. You can specify which guest users to filter based on their status (active, scheduled, expired, not active, or none). Use the Select a Status Filter drop-down list to determine the filter criteria.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Guest Users template page appears (see Figure 12-29).

*Figure 12-29 Guest User Template*




**Step 4** Enter a guest name. Maximum size is 24 characters.

**Step 5** Enter a password for this username.

**Step 6** Click the **Advanced** tab.

**Step 7** Use the Profile drop-down list to choose the guest user to connect to.

**Step 8** Choose a user role for the guest user from the drop-down list. User roles are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).

User Role is used to manage the amount of bandwidth allocated to specific users within the network.

**Step 9** Define how long the guest user account will be active by choosing either the Limited or Unlimited Lifetime option.

- For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours).
- When Unlimited is chosen, there is no expiration date for the guest account.

**Step 10** Choose the area (indoor, outdoor), controller list, or config group to which the guest user traffic is limited from the Apply to drop-down list.

If you choose the controller list option, a list of controller IP addresses appears.

**Step 11** (Optionally) Modify the default guest user description on the General tab if necessary.

**Step 12** (Optionally) Modify the Disclaimer text on the General tab, if necessary. If you want the supplied text to be the default, click the **Make this Disclaimer default** check box.

**Step 13** Click **Save**.

# Configuring a User Login Policies Template

This page allows you to add a user login template or make modifications to an existing user login policies template. On this template you set the maximum number of concurrent logins that each single user can have.

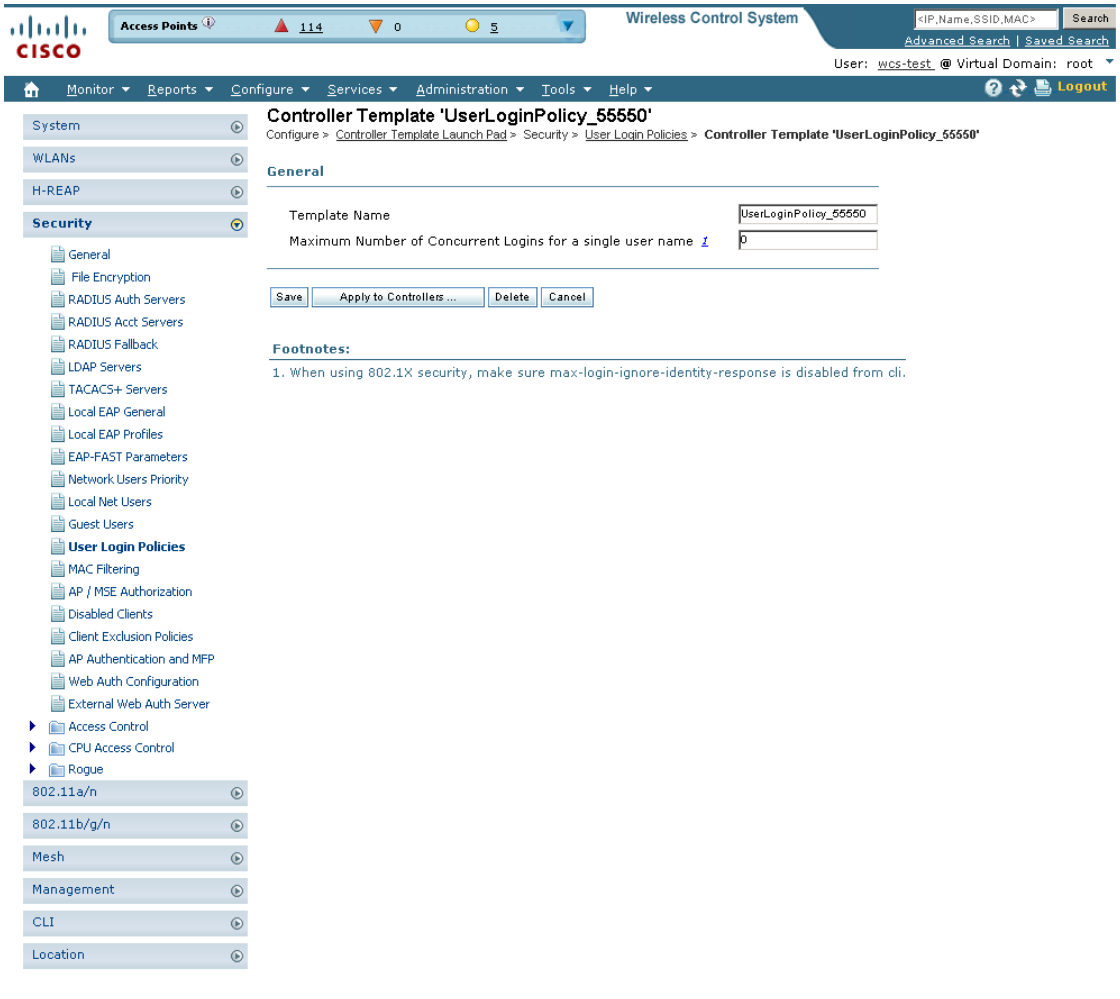
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **User Login Policies** or choose **Security > User Login Policies** from the left sidebar menu. The Security > User Login Policies page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The User Login Policies template page appears (see Figure 12-30).

*Figure 12-30 User Login Policies Template*




**Step 4** You can adjust the maximum number of concurrent logins each single user can have.

**Step 5** Click **Save** to keep this template.

# Configuring a MAC Filter Template

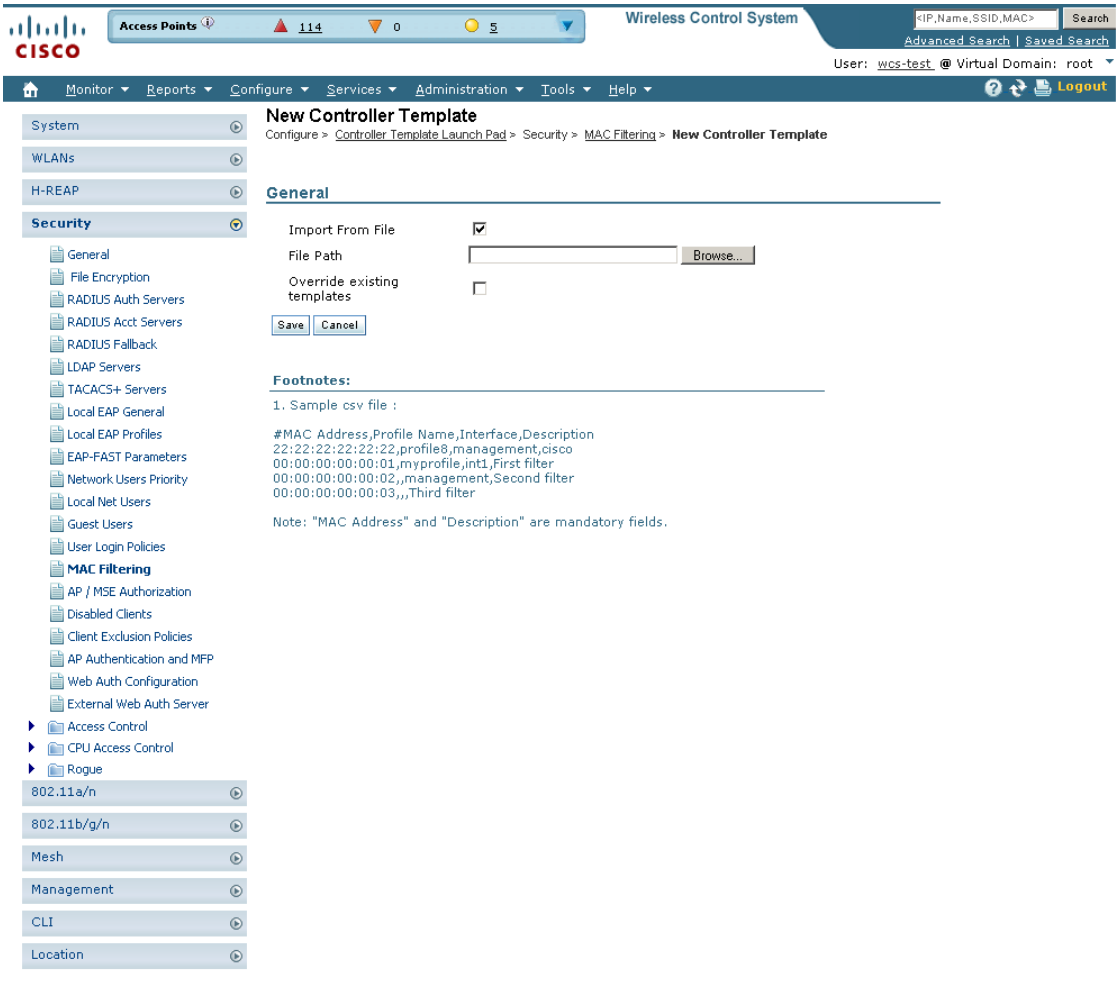
This page allows you to add a MAC filter template or make modifications to an existing MAC filter template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **MAC Filtering** or choose **Security > MAC Filtering** from the left sidebar menu. The Security > MAC Filtering page appears.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The MAC Filtering template page appears (see Figure 12-31).

*Figure 12-31 MAC Filter Templates*




**Step 4** If you keep Import From File enabled, you need to enter a file path or click the Browse button to navigate to the file path. The import file must be a CSV file with MAC address, profile name, interface, and description (such as 00:11:22:33:44:55,Profile1,management,test filter). If you disable Import from File, continue to Step 5. Otherwise, skip to Step 8.

The client MAC address appears.

**Step 5** Choose the profile name to which this MAC filter is applied or choose the **any Profile** option.

**Step 6** Use the drop-down list to choose from the available interface names.

**Step 7** Enter a user-defined description of this interface. Skip to Step 9.

**Step 8** If you want to override the existing template parameter, click to enable this parameter.

**Step 9** Click **Save**.

# Configuring an Access Point or MSE Authorization

Follow these steps to add an MSE authorization or make changes to an existing access point or MSE authorization template. These templates are devised for Cisco 11xx/12xx series access points converted from Cisco IOS to lightweight access points or for 1030 access points connecting in bridge mode. See the *Cisco Location Appliance Configuration Guide* for further information.

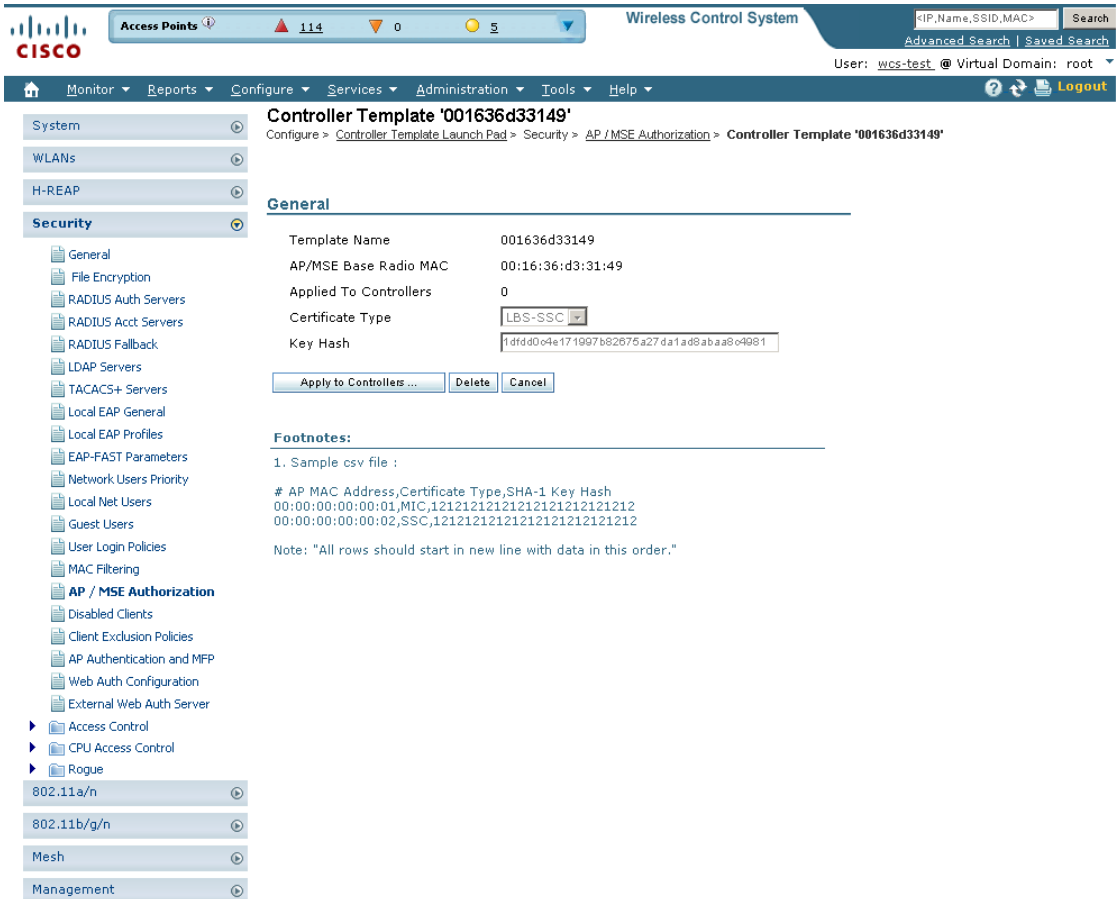
**Step 1** Choose **Configure > Controller Template Launch Pad.**

**Step 2** Click **AP/MSE Authorization** or choose **Security > AP/MSE Authorization** from the left sidebar menu. The Security > AP/LBS Authorization Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also shows the Base Radio MAC and the certificate type and key. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP/MSE Authorization template page appears (see Figure 12-32).

***Figure 12-32 AP/MSE Authorization Templates***



**Step 4** Select the **Import from File** check box if you want to import a file containing access point MAC addresses.

**Note** You can only import a .csv file. The .csv file format parallels the fields in the GUI and therefore includes access point base radio MAC, Type, Certificate Type (MIC or SSC), and key hash (such as 00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx). Any other file formats are not supported.

**Step 5** Enter the file path from where you want to import the file.

**Step 6** Click **Save**.

# Configuring a Manually Disabled Client Template

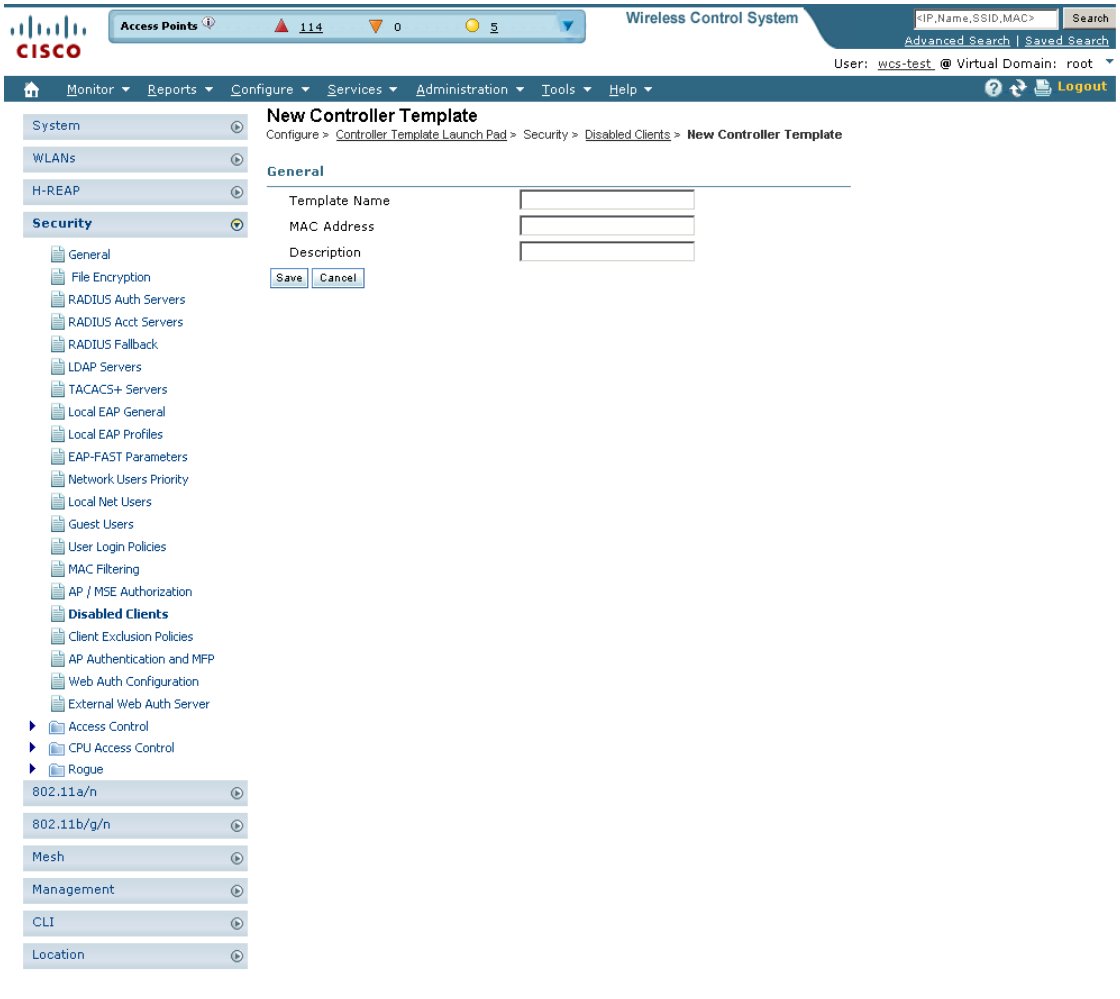
This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Disable Clients** or choose **Security > Disabled Clients** from the left sidebar menu. The Security > Disabled Clients page appears.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Manually Disabled template page appears (see Figure 12-33).

*Figure 12-33 Manually Disabled Clients Template*




**Step 4** Enter the MAC address of the client you want to disable.

**Step 5** Enter a description of the client you are setting to disabled.

**Step 6** Click **Save**.

# Configuring a Client Exclusion Policies Template

Follow these steps to add a client exclusion policies template or modify an existing client exclusion policies template.

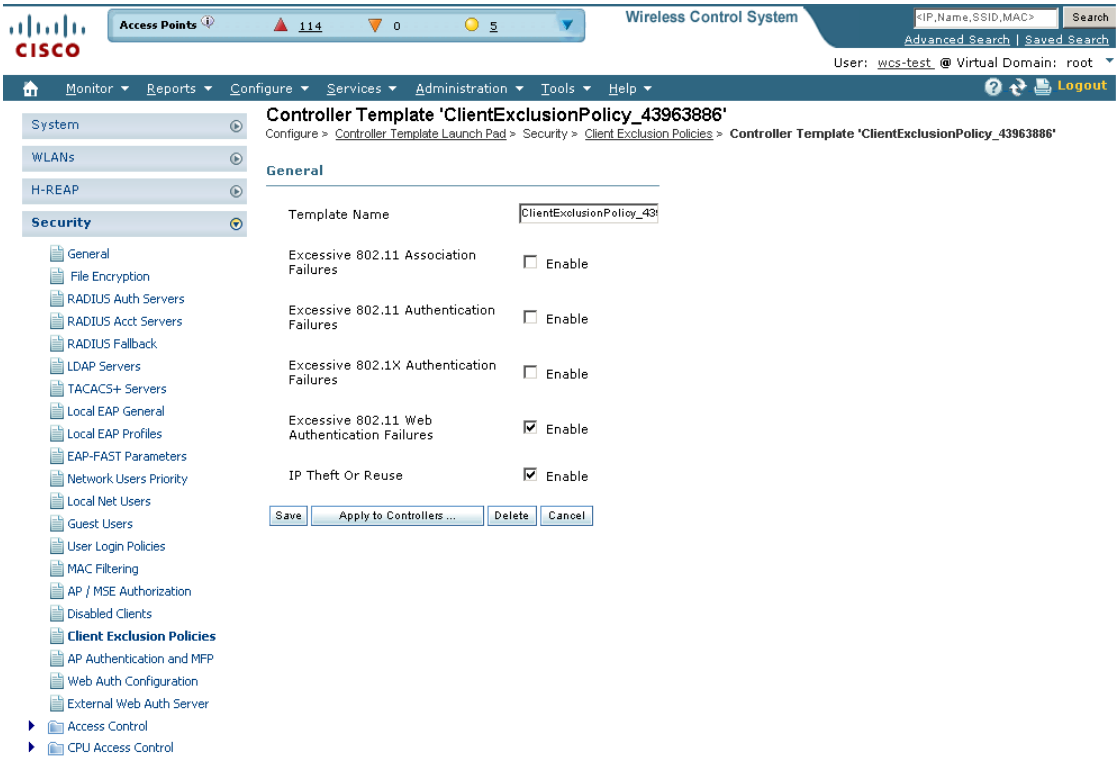
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Client Exclusion Policies** or choose **Security > Client Exclusion Policies** from the left sidebar menu. The Security > Client Exclusion Policies page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Client Exclusion Policies template page appears (see Figure 12-34).

***Figure 12-34 Policies Template***




**Step 4** Edit a client exclusion policies template by configuring its parameters.

***Table 12-3 Policies Template Parameters***

| Parameter | Description |
|---|---|
| Template Name | Enter a name for the client exclusion policy. |
| Excessive 802.11 Association Failures | Enable to exclude clients with excessive 802.11 association failures. |
| Excessive 802.11 Authentication Failures | Enable to exclude clients with excessive 802.11 authentication failures. |
| Excessive 802.1X Authentication Failures | Enable to exclude clients with excessive 802.1X authentication failures. |

*Table 12-3 (continued) Policies Template Parameters*

| Parameter | Description |
|---|---|
| Excessive 802.11 Web Authentication Failures | Enable to exclude clients with excessive 802.11 web authentication failures. |
| IP Theft or Reuse | Enable to exclude clients exhibiting IP theft or reuse symptoms. |

**Step 5** Click **Save**.

# Configuring an Access Point Authentication and MFP Template

Management frame protection (MFP) provides for the authentication of 802.11 management frames by the wireless network infrastructure. Management frames can be protected in order to detect adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy. An access point must be a member of a WDS to transmit MFP frames.

When MFP detection is enabled, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system.

Follow these steps to add or make modifications for the access point authentication and management frame protection (MFP) template.

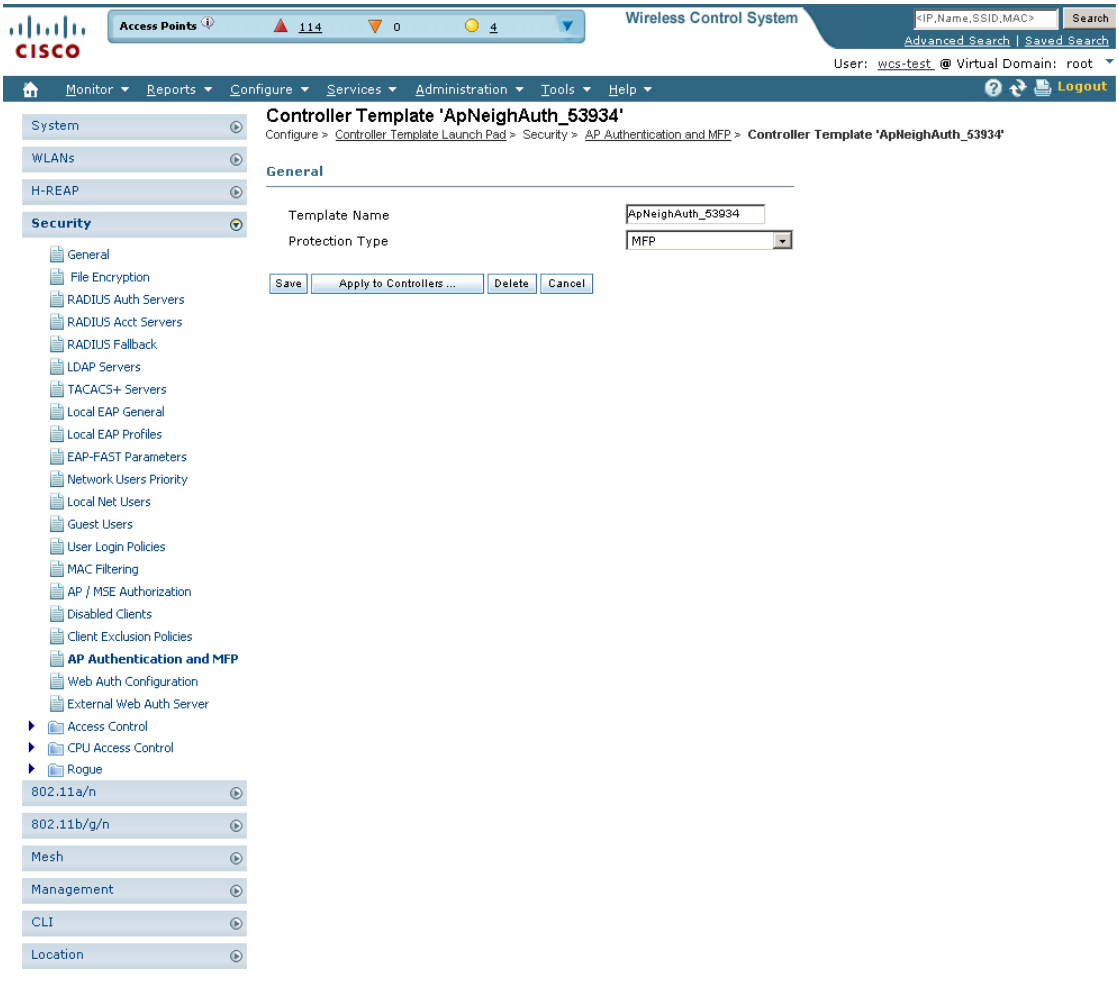
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **AP Authentication and MFP** or choose **Security > AP Authentication and MFP** from the left sidebar menu. The Security > AP Authentication Policy Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP Authentication and MFP template page appears (see Figure 12-35).

*Figure 12-35 AP Authentication Policy Template*




**Step 4** From the Protection Type drop-down list, choose one of the following authentication policies:

- None: No access point authentication policy.
- AP Authentication: Apply authentication policy.
- MFP: Apply management frame protection.

Alarm trigger threshold appears only when AP authentication is selected as a protection type. Set the number of hits from an alien access point to ignore before raising an alarm.

The valid range is from 1 to 255. The default value is 255.

**Step 5** Click **Save**.

# Configuring a Web Authentication Template

With web authentication, guests are automatically redirected to a web authentication page when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or

encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts may be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. You can use this template to replace the Web authentication page provided on the controller.

Follow these steps to add or make modifications to an existing web authentication template.

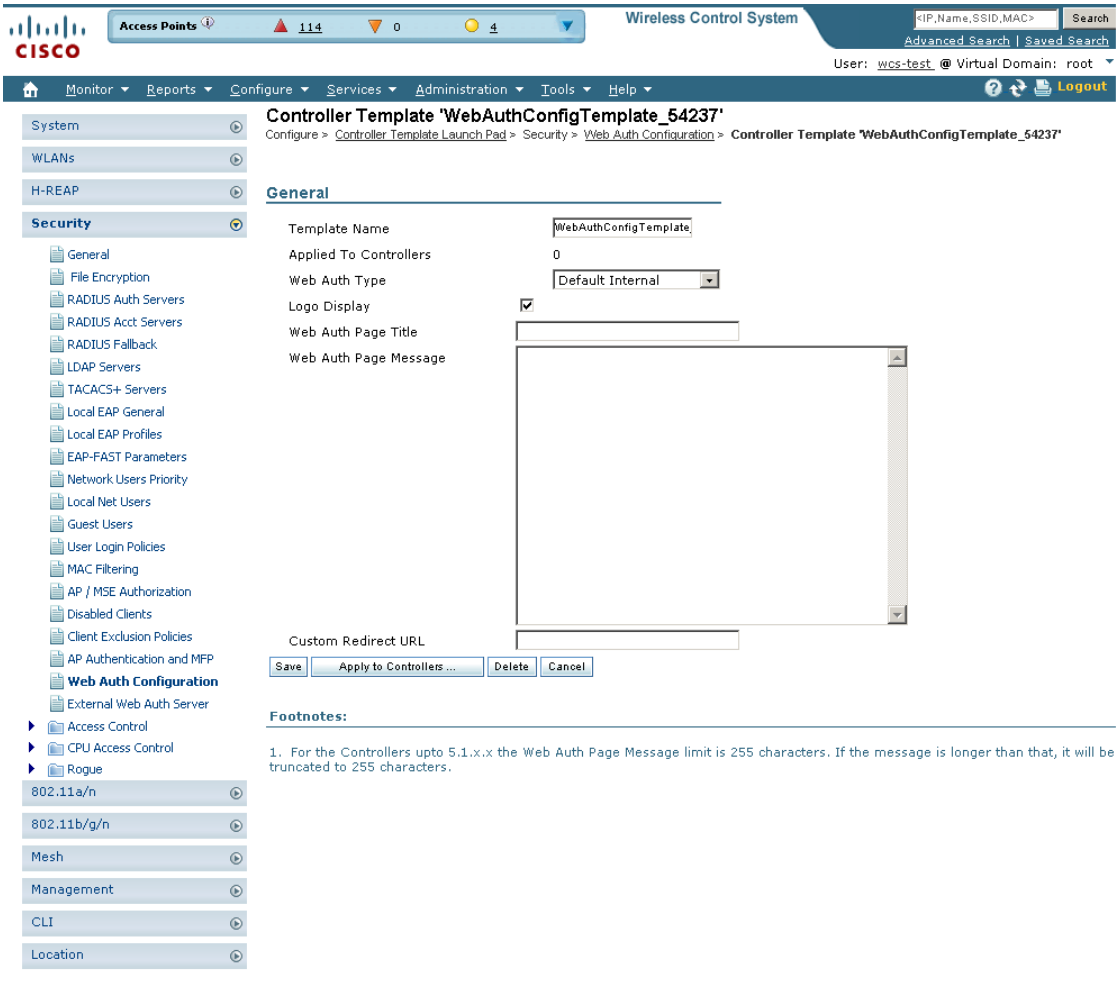
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Web Auth Configuration** or choose **Security > Web Auth Configuration** from the left sidebar menu. The Security > Web Authentication page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Web Authentication template page appears (see Figure 12-36).

*Figure 12-36 Web Authentication Configuration Template*




**Step 4** Choose the appropriate web authentication type from the drop-down list. The choices are default internal, customized web authentication, or external.

- If you choose default internal, you can still alter the page title, message, and redirect URL, as well as whether the logo appears. Continue to Step 5.
- If you choose customized web authentication, click **Save** and apply this template to the controller. You are prompted to download the web authentication bundle.

**Note** Before you can choose customized web authentication, you must first download the bundle by going to **Config > Controller** and choose **Download Customized Web Authentication** from the Select a command drop-down list, and click **Go**.

- If you choose external, you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.

**Step 5** Click to enable Logo Display if you want your company logo displayed.

**Step 6** Enter the title you want displayed on the Web authentication page.

**Step 7** Enter the message you want displayed on the Web authentication page.

**Step 8** Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.

**Step 9** Click **Save**.

## Downloading a Customized Web Authentication Page

You can download a customized Web authentication page to the controller. With a customized web page, you can establish a username and password for user web access.

When downloading customized web authentication, you must follow these strict guidelines:

- Provide a username.
- Provide a password.
- Retain a redirect URL as a hidden input item after extracting from the original URL.
- Extract the action URL and set aside from the original URL.
- Include scripts to decode the return status code.
- All paths used in the main page should be of relative type.

Perform the required following steps before downloading:

**Step 1** Download the sample login.html bundle file from the server. The .html file is shown in Figure 12-37. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

***Figure 12-37 Login.html***


**Step 2** Edit the login.html file and save it as a .tar or .zip file.

**Note** You can change the text of the Submit button to read Accept terms and conditions and Submit.

**Step 3** Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add *IP address of TFTP server*).
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco WCS because WCS's built-in TFTP server and third-party TFTP server use the same communication port.

**Step 4** Download the .tar or .zip file to the controller(s).

**Note** The controller allows you to download up to 1 MB of a .tar file containing the pages and image files required for the Web authentication display. The 1 MB limit includes the total size of uncompressed files in the bundle.

You can now continue with the download.

**Step 5** Copy the file to the default directory on your TFTP server.

**Step 6** Choose **Configure > Controllers**.

**Step 7** Choose a controller by clicking the URL for the corresponding IP address. If you select more than one IP address, the customized Web authentication page is downloaded to multiple controllers.

**Step 8** From the left sidebar menu, choose **System > Commands**.

**Step 9** From the Upload/Download Commands drop-down list, choose **Download Customized Web Auth, and click Go**.

**Step 10** The IP address of the controller to receive the bundle and the current status are displayed.

**Step 11** Choose **local machine** from the File is Located On parameter. If you know the filename and path relative to the server's root directory, you can also select TFTP server.

**Note** For a local machine download, either .zip or .tar file options exists, but the WCS does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files would be specified.

**Step 12** Enter the maximum number of times the controller should attempt to download the file in the Maximum Retries parameter.

**Step 13** Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout parameter.

**Step 14** The 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.

**Step 15** Click **OK**.

If the transfer times out, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the administrator's workstation to WCS's own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the WCS server's TFTP directory, and the download web page now automatically populates the filename.

**Step 16** Click the **Click here to download a sample tar file** link to get an option to open or save the login.tar file.

**Step 17** After completing the download, you are directed to the new page and able to authenticate.

# Configuring External Web Auth Server

You can create or modify an External Web Auth Server template by following these steps:

**Step 1** Choose **Configure > Controller Templates Launch Pad**.

**Step 2** Click **External Web Auth Server** or choose **Security > External Web Auth Server** from the left sidebar menu. The External Web Auth Server Controller Templates page displays all currently saved External Web Auth Server templates. It also displays the number of controllers and virtual domains to which each template is applied.

**Step 3** Click a template name to open the Controller Template list page. From here, you can edit the current template parameters.

# Configuring Access Control List Templates

You can create or modify an ACL template for configuring the type of traffic that is allowed, by protocol, direction, and the source or destination of the traffic.

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs can be applied to data traffic to and from wireless clients or to all traffic destined for the controller central processing unit (CPU) and can now support reusable grouped IP addresses and reusable protocols. After ACLs are configured in the template, they can be applied to the management interface, the AP-manager interface, or any of the dynamic interfaces for client data traffic; to the network processing unit (NPU) interface for traffic to the controller CPU; or to a WAN. Follow these steps to add or modify an existing ACL template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Access Control Lists** or choose **Security > Access Control > Access Control Lists** in the left sidebar menu. The Security > Access Control List page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

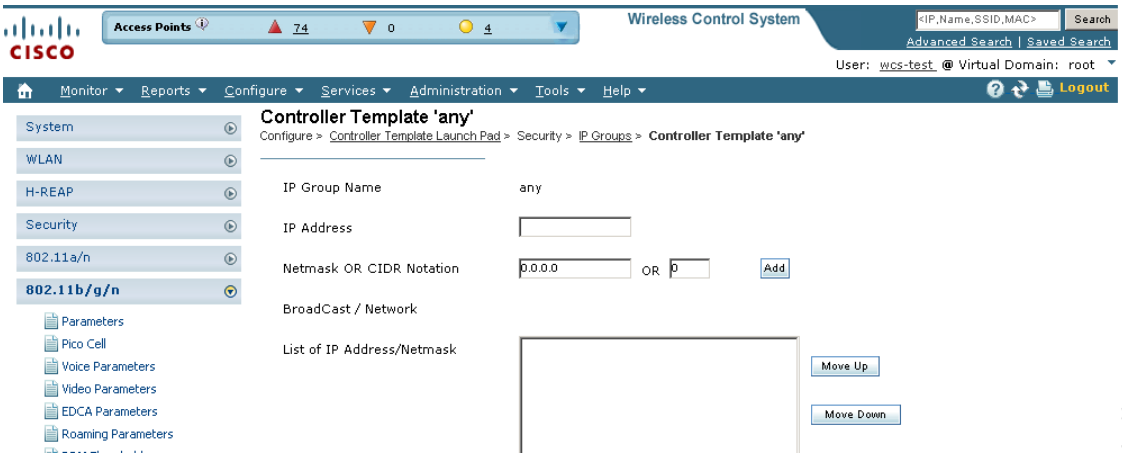
The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** To create reusable grouped IP addresses and protocols, choose **Access Control > IP Groups** from the left sidebar menu.

**Step 4** All the IP address groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose **Add IP Group** from the Select a command drop-down list, and click **Go**. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens (see Figure 12-38).

**Note** For the IP address of any, an *any* group is predefined.

***Figure 12-38 IP Groups Controller Template***




**Step 5** On the ACL IP Groups details page you can edit the current IP group parameters.

- IP Group Name
- IP Address
- Netmask OR CIDR Notation—Enter the Netmask or CIDR Notation and then click **Add**. The list of IP addresses or Netmasks appears in the List of IP Address/Netmasks text box.

  CIDR notation allows you to add a large number of clients that exist in a subnet range by configuring a single client object.

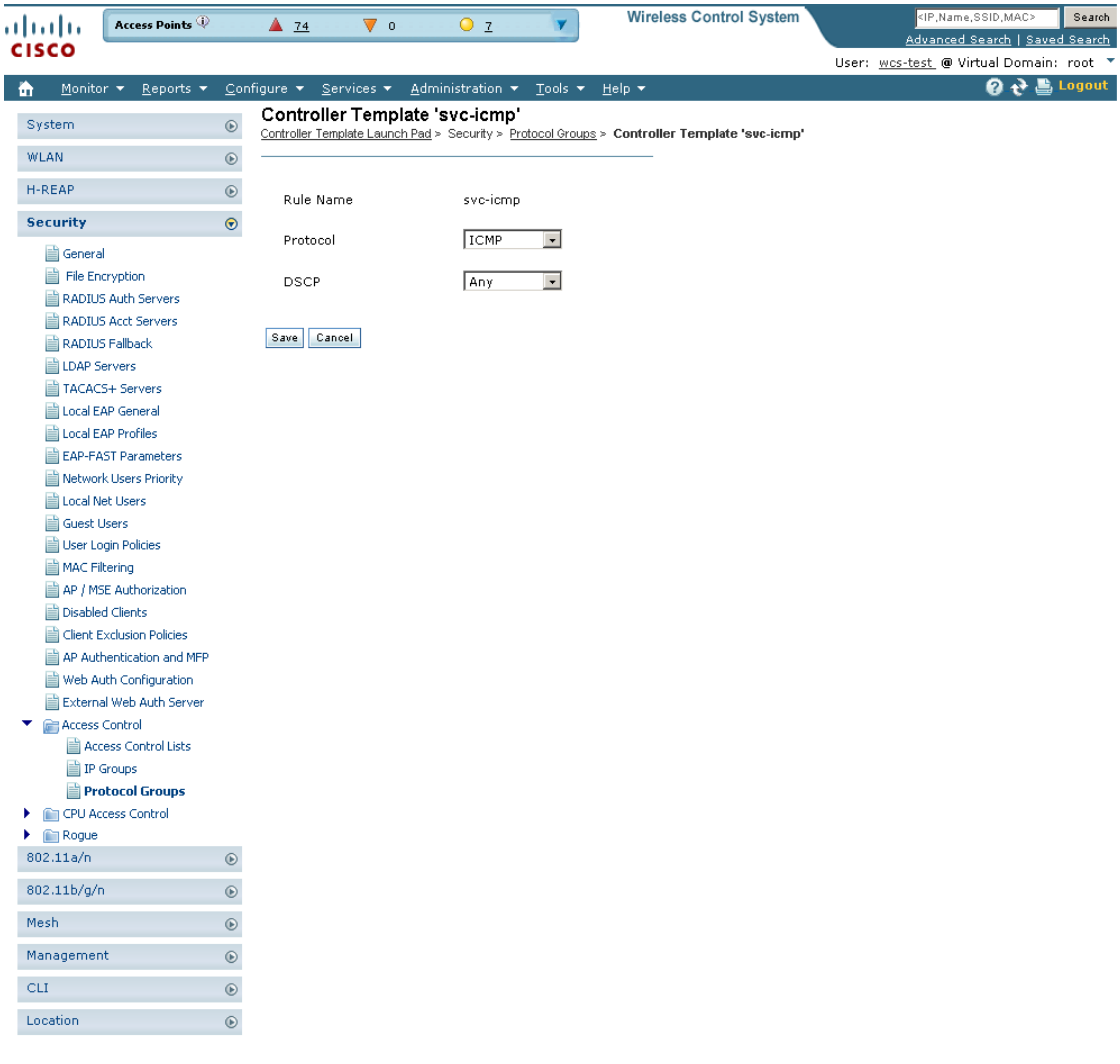
  Netmask allows you to set the subnet mask in dotted decimal notation rather than the CIDR notation for the IP address property.

  - Netmask—A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
  - CIDR—Classless InterDomain Routing. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks.
- BroadCast/Network
- List of IP Addresses/Netmasks—Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or Netmask.

**Step 6** To define an additional protocol that is not a standard predefined one, choose **Access Control > Protocol Groups** from the left sidebar menu. The protocol groups with their source and destination port and DSCP are displayed.

**Step 7** To create a new protocol group, choose **Add Protocol Group** from the Select a command drop-down list, and click **Go**. To view or modify an existing protocol group, click the URL of the group. The Protocol Groups page appears (see Figure 12-39).

*Figure 12-39 Protocol Groups Controller Template*




**Step 8** The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the parameters of a rule, the action for this rule is exercised.

**Step 9** Choose a protocol from the drop-down list:

- Any—All protocols
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP—Internet Protocol

- Eth Over IP—Ethernet over Internet Protocol
- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

**Step 10** Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.

- Source Port—Specify the source of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.
- Dest Port—Specify the destination of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

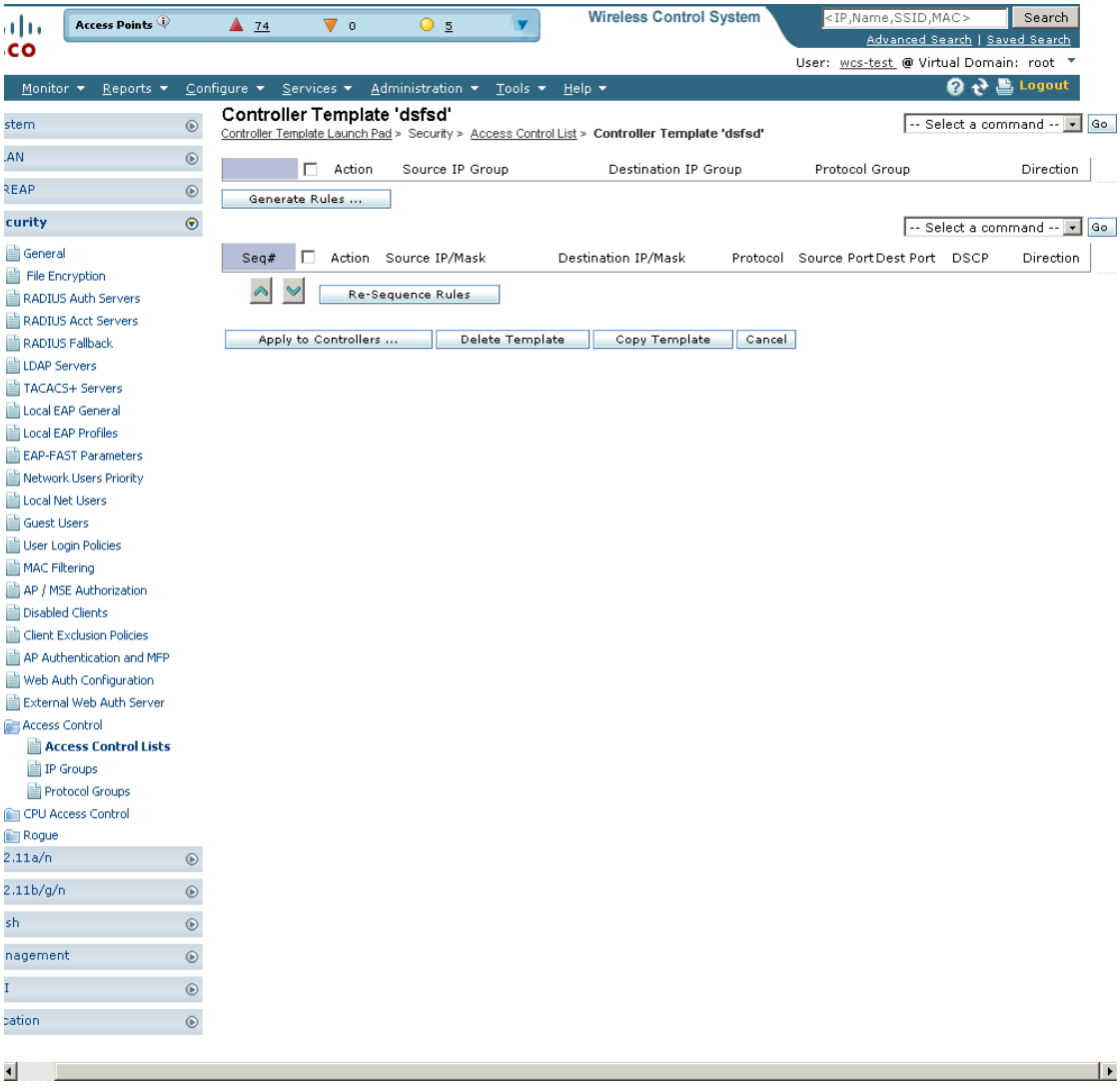
**Step 11** In the DSCP (Differentiated Services Code Point) drop-down list, choose **any** or **specific**. If you choose specific, enter the DSCP (range of 0 to 255).

**Note** DSCP is a packet header code that can be used to define the quality of service across the Internet.

**Step 12** Click **Save**.

**Step 13** You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All ACL mappings appear on the top of the page, and all ACL rules appear on the bottom (see Figure 12-40).

*Figure 12-40 Access Control List Rule Mapping*




**Step 14** To define a new mapping, choose **Add Rule Mappings** from the Select a command drop-down list. The Add Rule Mapping page appears.

**Step 15** Choose the desired IP address groups, protocol groups, direction, and action, and click **Add**. The new mappings will populate the bottom table.

**Step 16** Click **Save**.

**Step 17** You can now automatically generate rules from the rule mappings you created. Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

Existing ACL templates are duplicated into a new ACL template. This duplication clones all the ACL rules and mappings defined in the source ACL template.

# Configuring a CPU Access Control List (ACL) Template

The existing ACLs established in the "Configuring Access Control List Templates" section on page 12-69 is used to set traffic controls between the central processing unit (CPU) and network processing unit (NPU). Follow these steps to add or modify an existing CPU ACL template.

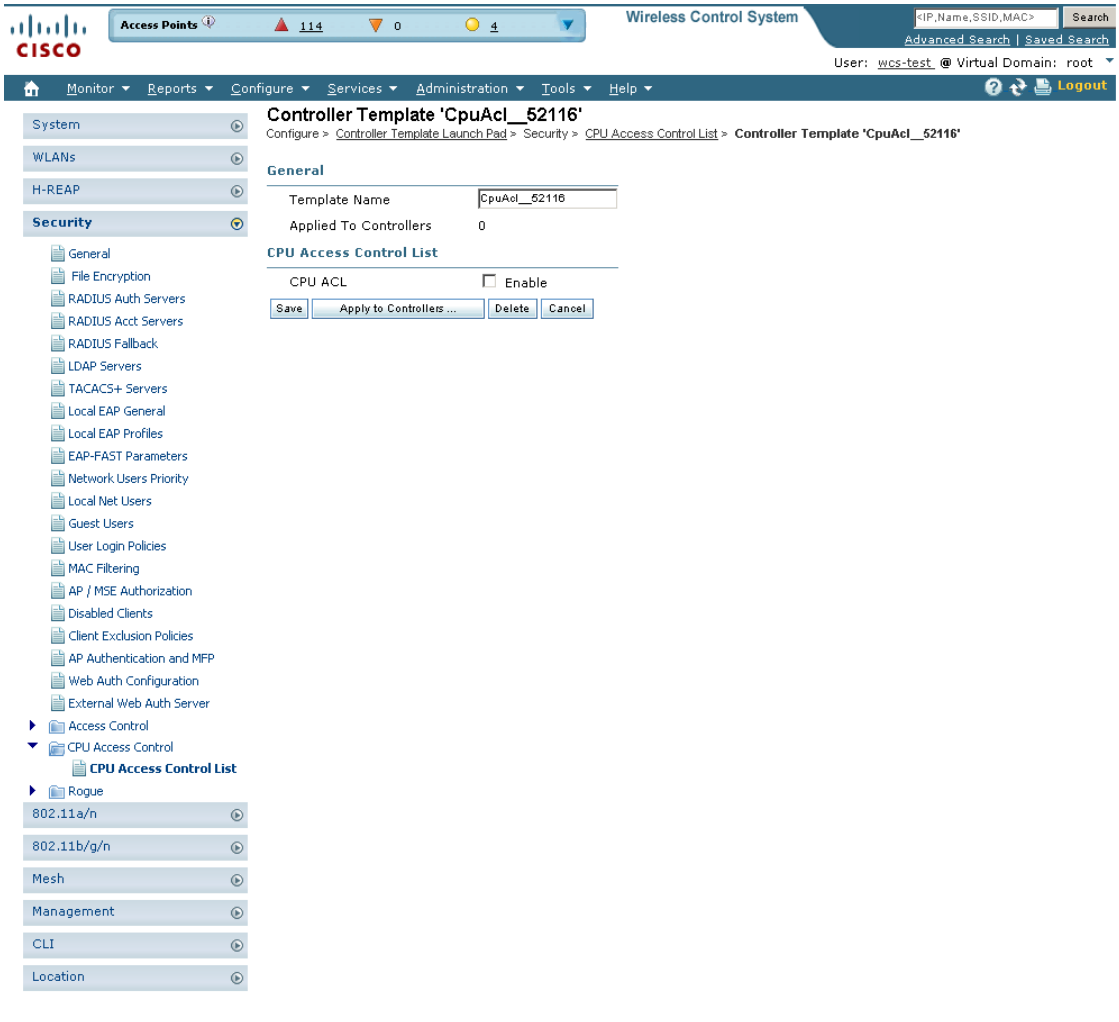
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **CPU Access Control Lists** or choose **Security > CPU Access Control > CPU Access Control List** from the left sidebar menu. The Security > CPU Access Control List page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The CPU Access Control List template page appears (see Figure 12-41).

*Figure 12-41 CPU Access Control List Template*




**Step 4** If you click the check box to enable CPU ACL, two more parameters appear. When CPU ACL is enabled and applied on the controller, WCS displays the details of the CPU ACL against that controller.

**Step 5** From the ACL Name drop-down list, choose a name from the list of defined names.

**Step 6** From the CPU ACL Mode drop-down list, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.

**Step 7** Click **Save**.

# Configuring a Rogue Policies Template

This page enables you to configure the rogue policy (for access points and clients) applied to the controller. Follow these steps to add or modify an existing template.

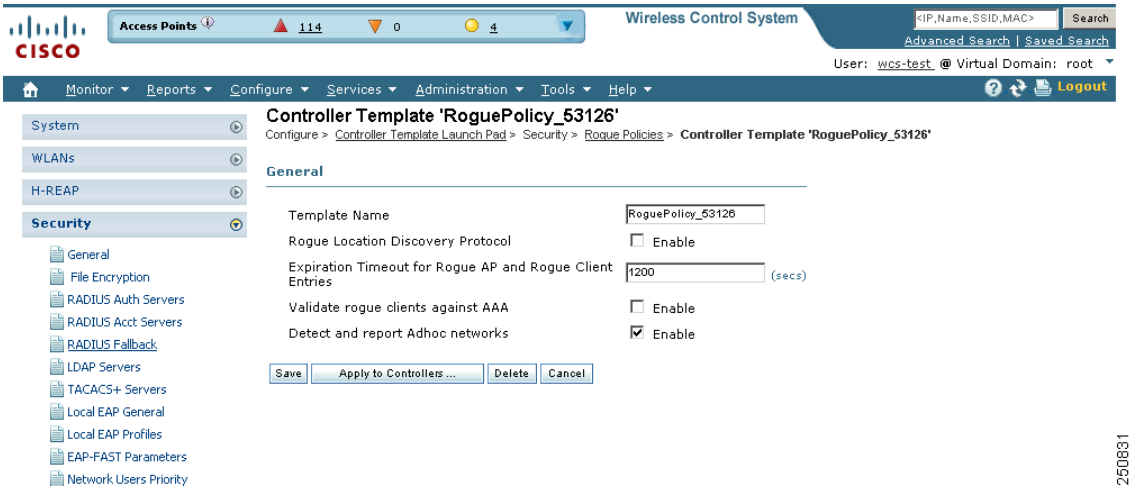
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Rogue Policies** or choose **Security > Rogue > Rogue Policies** from the left sidebar menu. The Security > Rogue Policy Setup page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Rogue Policies template page appears (see Figure 12-42).

***Figure 12-42 Rogue Policy Setup Template***




**Step 4** Determine whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:

- Disable—Disables RLDP on all access points.
- All APs—Enables RLDP on all access points.
- Monitor Mode APs—Enables RLDP only on access points in monitor mode.

**Note** With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

**Step 5** Set the expiration timeout (in seconds) for rogue access point entries.

**Step 6** Check the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

**Step 7** Check the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.

**Step 8** Click **Save**.

# Configuring a Rogue AP Rules Template

Rogue access point rules allow you to define rules to automatically classify rogue access points. WCS applies the rogue access point classification rules to the controllers. These rules can limit a rogue's appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

**Note** Rogue access point rules also help reduce false alarms.

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configure > Controller Template Launch Pad> Security > Rogue > Rogue AP Rules**. If you want to view rogue access point rules, refer to the "Viewing or Editing Rogue Access Point Rules" section on page 9-36.

**Note** Rogue classes include the following types:
Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

Follow these steps to add or create a new classification rule template for rogue access points.

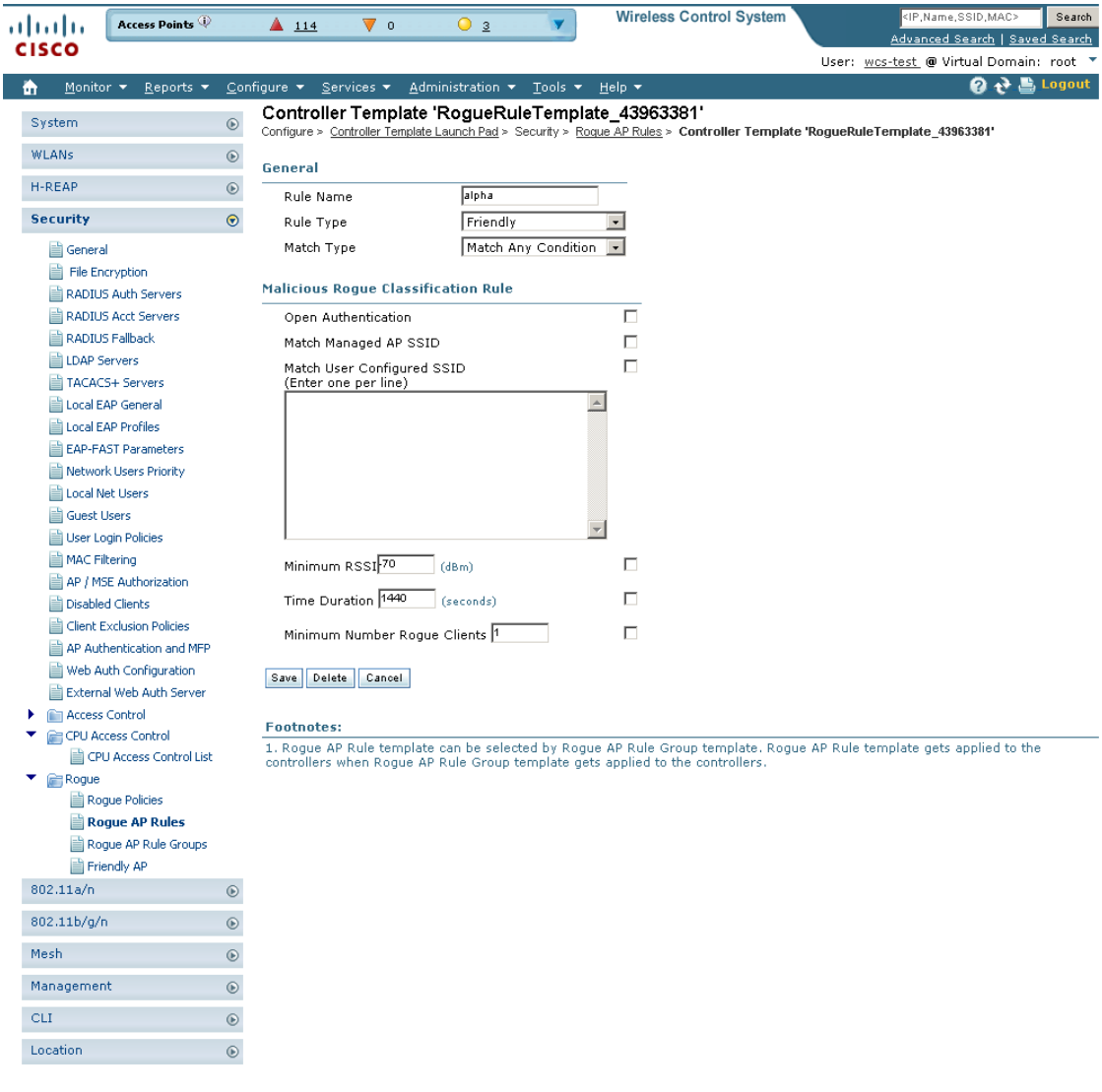
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** From the left sidebar menu, choose **Security > Rogue > Rogue AP Rules**. The Rogue AP Rules Controller Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** From the Select a command drop-down list, choose **Add Classification Rule**, and click **Go**. The Rogue AP Rules > New Template page appears (see Figure 12-43). To modify an existing rogue access point rules template or to apply a current template to the controllers, choose **Configure > Controller Template Launch Pad > Security > Rogue > Rogue AP Rules**, and click a template name.

*Figure 12-43 Rogue AP Rules > New Template Page*




**Step 4** In the General portion of the page, enter the following parameters:

- Rule Name—Enter a name for the rule in the text box.
- Rule Type—Choose **Malicious** or **Friendly** from the drop-down list. A rogue is considered malicious if a detected access point matches the user-defined malicious rules or has been manually moved from the Friendly AP category. A rogue is considered friendly if it is a known, acknowledged, or trusted access point or a detected access point that matches the user-defined Friendly rules.
- Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.

**Step 5** In the Malicious Rogue Classification Rule portion of the page, enter the following parameters.

- Open Authentication—Choose the check box to enable open authentication.
- Match Managed AP SSID—Choose the check box to enable the matching of a Managed AP SSID.

**Note** Managed SSIDs are the SSIDs configured for the WLAN and known to the system

- Match User Configured SSID—Choose the check box to enable the matching of User Configured SSIDs.

**Note** User Configured SSIDs are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

- Minimum RSSI—Choose the check box to enable the Minimum RSSI threshold limit.

**Note** Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

- Time Duration—Choose the check box to enable the Time Duration limit.

**Note** Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

- Minimum Number Rogue Clients—Choose the check box to enable the Minimum Number Rogue Clients limit. Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

**Step 6** Click **Save**.

# Configuring a Rogue AP Rule Groups Template

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers. Follow these steps to view current rogue access point rule group templates or create a new rule group.

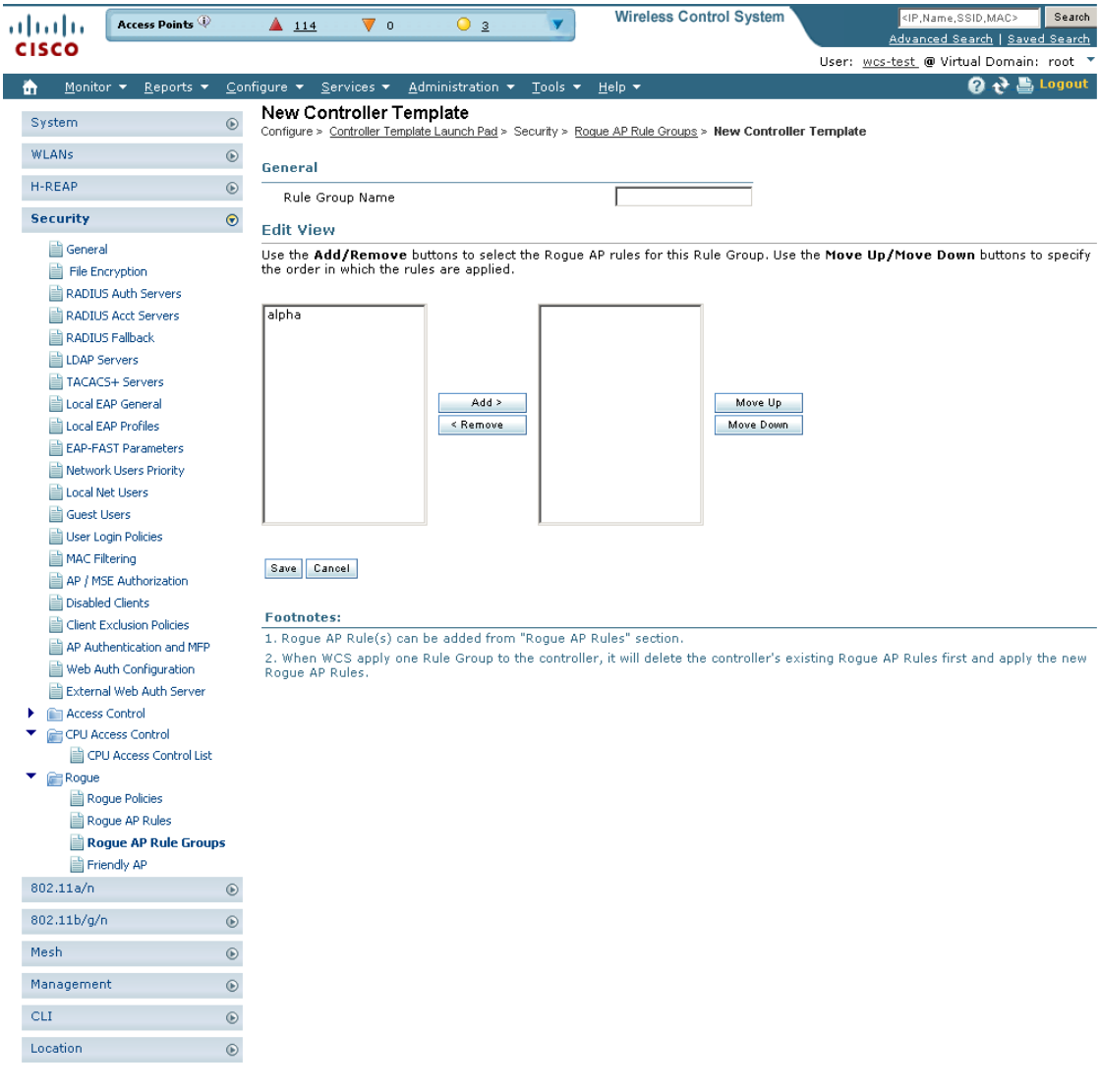
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Rogue AP Rule Groups** or choose **Security > Rogue > Rogue AP Rule Groups** from the left sidebar menu.

**Step 3** From the Select a command drop-down list, click **Add Rogue Rule Group**.

**Step 4** Click **Go**. The Rogue AP Rule Groups > New Template page appears (see Figure 12-44).

*Figure 12-44 Rogue AP Rule Groups > New Template*




**Note** To modify an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Template Launch Pad > Security > Rogue > Rogue AP Rule Groups** and click a template name. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

**Step 5** Enter a name for the rule group in the General portion of the page.

**Step 6** To add a Rogue AP rule, click to highlight the rule in the left column. Click **Add** to move the rule to the right column.

**Note** Rogue access point rules can be added from the Rogue Access Point Rules section. See the "Configuring a Rogue AP Rules Template" section on page 12-77 for more information.

**Step 7** To remove a rogue access point rule, click to highlight the rule in the right column. Click **Remove** to move the rule to the left column.

**Step 8** Use the **Move Up/Move Down** buttons to specify the order in which the rules apply. Highlight the desired rule and click **Move Up** or **Move Down** to move it higher or lower in the current list.

**Step 9** Click **Save** to confirm the rogue access point rule list.

**Step 10** Click **Cancel** to close the page without making any changes to the current list.

**Note** To view and edit the rules applied to a controller, choose **Configure > Controller** and click the controller name.

# Configuring a Friendly Access Point Template

This template allows you to import friendly internal access points. Importing these friendly access points prevents non-lightweight access points from being falsely identified as rogues.

**Note** *Friendly Internal* access points were previously referred to as *Known APs*.

Follow these steps to view or edit the current list of friendly access points. The friendly access point screen identifies the access point's MAC address, status, any comments, and whether or not the alarm is suppressed for this access point.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

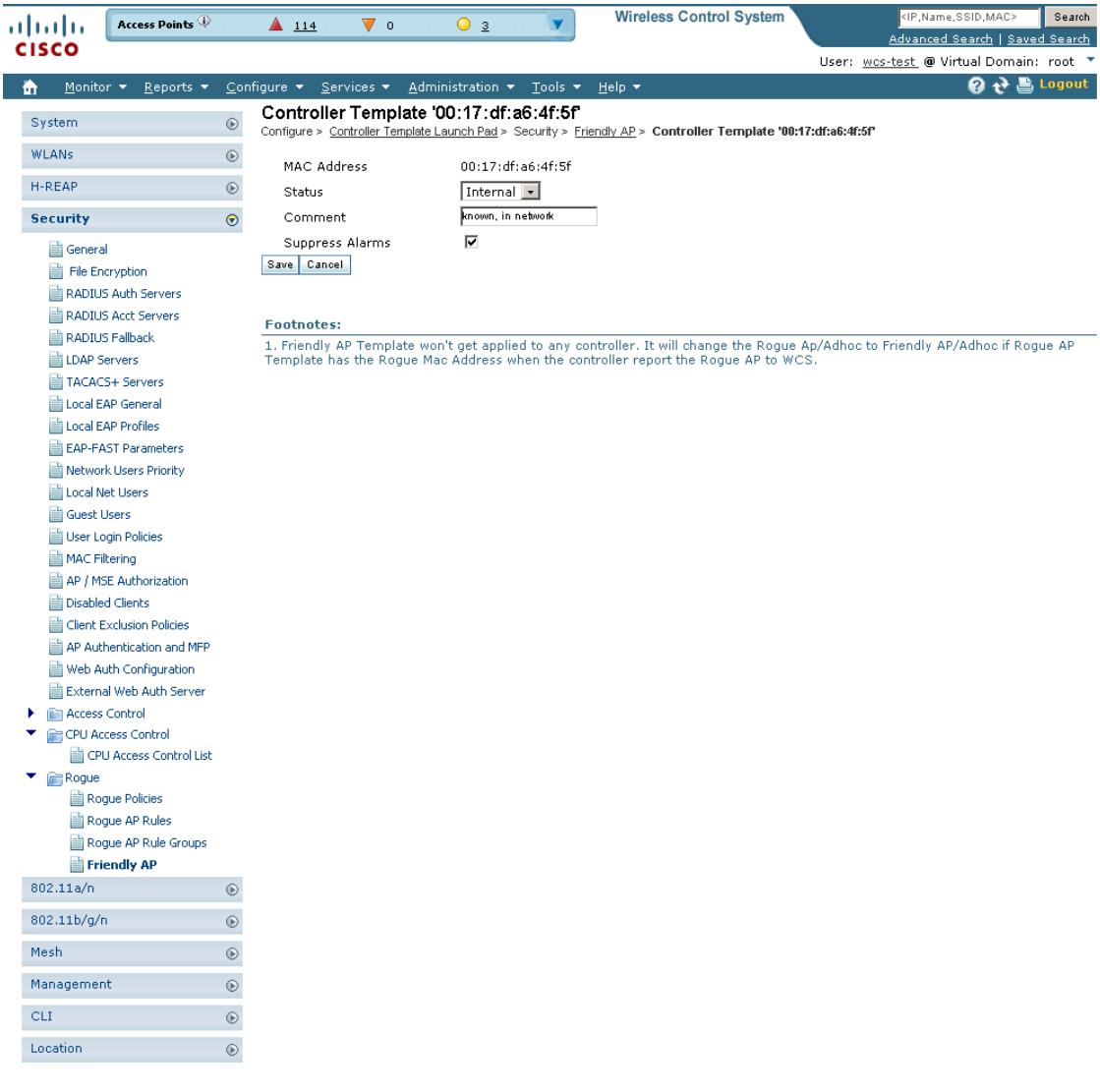
**Step 2** Click **Friendly AP** or choose **Security > Rogue > Friendly AP** from the left sidebar menu.

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

**Step 4** Click **Go**. The Friendly AP page appears (see Figure 12-45).

**Note** To modify an existing friendly access point, choose **Configure > Controller Template Launch Pad > Security > Rogue > Friendly Internal** and click the access point's MAC address. Make the necessary changes to the access point and click **Save**.

*Figure 12-45 Friendly AP > Add Friendly AP Page*




**Step 5** Friendly access points can be added by either importing the access point or manually entering the access point information:

- To import an access point using the Import feature,
  - Choose the **Import from File** check box.
  - Enter the file path or use the **Browse** button to navigate to the correct file.
- To manually add an access point,
  - Deselect the **Import from File** check box.
  - Enter the MAC address for the access point.

**Note** Use a line break to separate MAC addresses. For example, you could enter the MAC addresses as follows:
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46

- Choose **Internal** access point from the Status drop-down list.
- Enter a comment regarding this access point, if necessary.
- Check the **Suppress Alarms** check box to suppress all alarms for this access point.

- Click **Save** to confirm this access point or **Cancel** to close the page without adding the access point to the list.

# Configuring Radio Templates (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify radio templates.

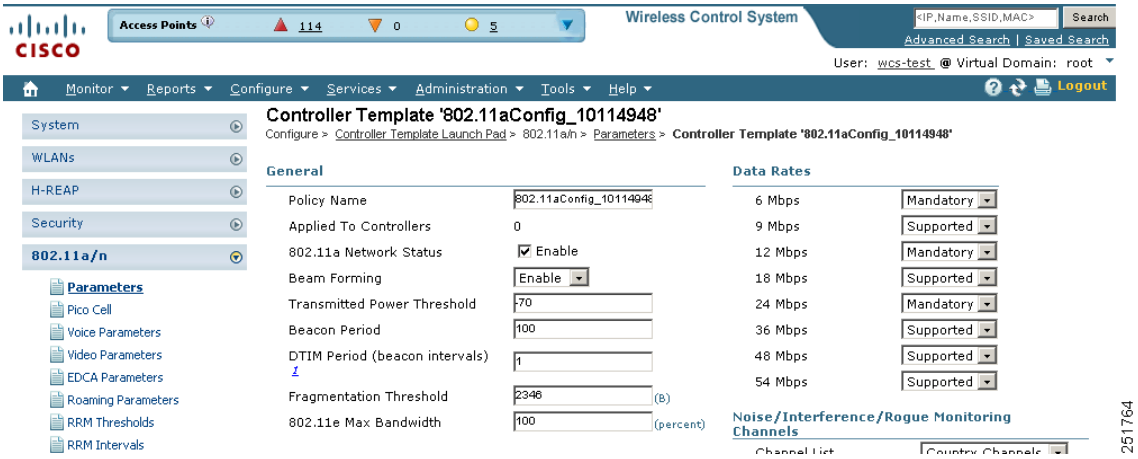
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Parameters** or choose either **802.11a/n > Parameters or 802.11b/g/n > Parameters** from the left sidebar menu. The 802.11a/n or b/g/n Parameters Template page appears and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the 802.11 network status and the channel and power mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n Parameters template page appears (see Figure 12-46).

*Figure 12-46 802.11a/n Parameters Template*




**Step 4** Click the check box if you want to enable 802.11a/n or b/g/n network status.

**Step 5** Use the ClientLink drop-down list to enable Clientlink on all access point 802.11a/n radios which support ClientLink. Otherwise, choose **Disable**.

**Step 6** Enter a transmitted power threshold between -50 and -80.

**Step 7** Enter the amount of time between beacons in kilomicroseconds. The valid range is from 20 to 1000 milliseconds.

**Step 8** Enter the number of beacon intervals that may elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count text box is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMS let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

**Step 9** At the Fragmentation Threshold parameter, determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

**Step 10** Enter the percentage for 802.11e maximum bandwidth.

**Step 11** Click if you want short preamble enabled.

**Step 12** At the Dynamic Assignment drop-down list, choose one of three modes:

- Automatic - The transmit power is periodically updated for all access points that permit this operation.
- On Demand - Transmit power is updated when the Assign Now button is selected.
- Disabled - No dynamic transmit power assignments occur, and values are set to their global default.

**Step 13** Determine if you want to enable Dynamic Tx Power Control. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

**Step 14** The Assignment Mode drop-down list has three dynamic channel modes:

- Automatic - The channel assignment is periodically updated for all access points that permit this operation. This is also the default mode.
- On Demand - Channel assignments are updated when desired.
- OFF - No dynamic channel assignments occur, and values are set to their global default.

**Step 15** At the Avoid Foreign AP Interference check box, click if you want to enable it. Enable this parameter to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Disable this parameter to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.

**Step 16** Select the **Avoid Cisco AP Load** check box if you want it enabled. Enable this bandwidth-sensing parameter to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Disable this parameter to have RRM ignore this value.

In certain circumstances and with denser deployments, there may not be enough channels to properly create perfect channel re-use. In these circumstances, RRM can assign better re-use patterns to those access points that carry more traffic load.

**Step 17** Select the **Avoid non 802.11 Noise** check box if you want to enable it. Enable this noise-monitoring parameter to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Disable this parameter to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM may adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.

**Step 18** The Signal Strength Contribution check box is always enabled (not configurable). constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel re-use. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.

**Step 19** The client and controller negotiate data rates between them. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate may communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported in order to associate. For each rate, a drop-down list of Mandatory or Supported is available. Each data rate can also be set to Disabled to match client settings.

**Step 20** At the Channel List drop-down list in the Noise/Interference/Rogue Monitoring Channels section, choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

**Step 21** The Cisco Compatible Extension's location measurement interval can only be changed when measurement mode is enabled to broadcast radio measurement requests. When enabled, this enhances the location accuracy of clients.

**Step 22** Click **Save**.

# Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify either 802.11a/n or 802.11b/g/n voice parameters, such as call admission control and traffic stream metrics.

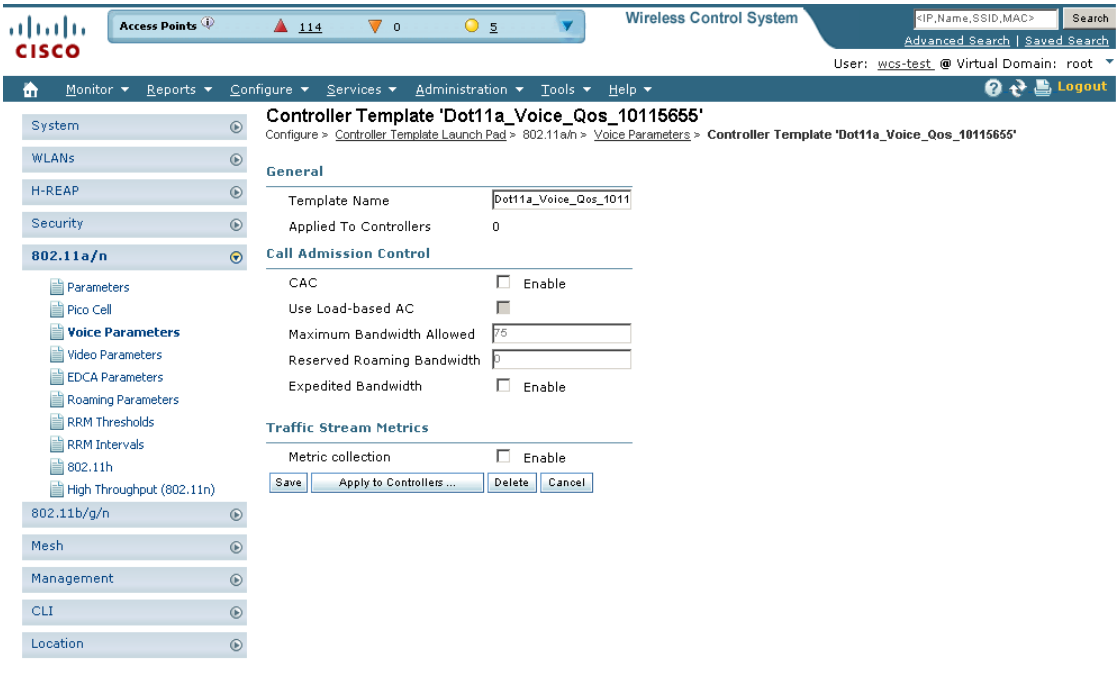
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Voice Parameters** or choose either **802.11a/n > Voice Parameters** or **802.11b/g/n > Voice Parameters**. The 802.11a/n or 802.11b/g/n Voice Parameters page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the maximum bandwidth allowed and the reserved roaming bandwidth. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n Voice Parameters template page appears (see Figure 12-47).

***Figure 12-47 802.11b/g/n Voice Parameters Template***




**Step 4** For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity. Click the check box to enable CAC.

**Step 5** Load-based AC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based AC also covers the additional bandwidth consumption resulting from PHY and channel impairment. To enable load-based AC for this radio band, check the Use Load-based AC check box.

**Step 6** Enter the percentage of maximum bandwidth allowed.

**Step 7** Enter the percentage of reserved roaming bandwidth.

**Step 8** Click if you want to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is Cisco Compatible Extensions (version 5) compliant so that a TSPEC request is given higher priority.

**Step 9** Click the check box if you want to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data in every 90 seconds from the 802.11b/g/n interfaces of all associated access points. For VoIP and video, this feature should be enabled.

**Step 10** Click **Save**.

# Configuring a Video Parameter Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify an 802.11a/n or 802.11b/g/n video parameter template.

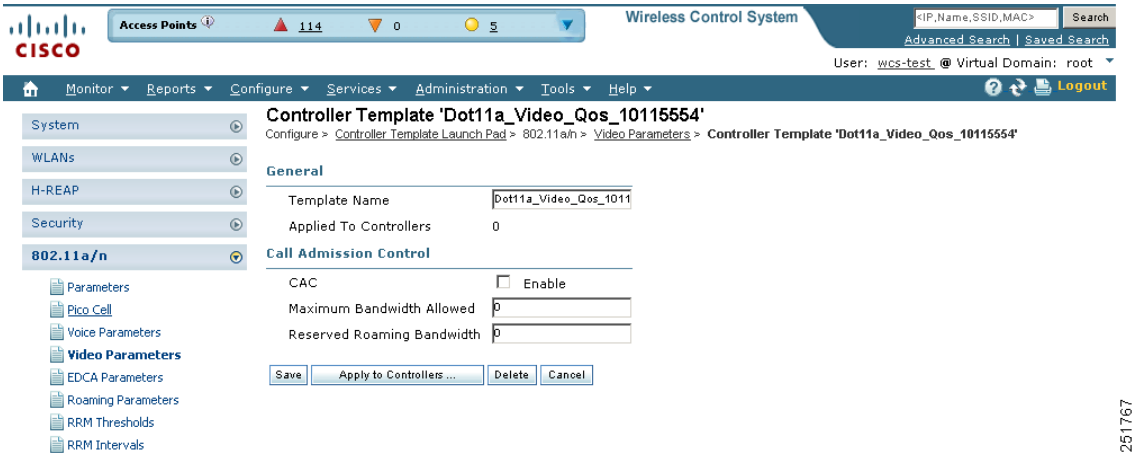
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Video Parameters** or choose either **802.11a/n > Video Parameters** or **802.11b/g/n > Video Parameters**. The 802.11a/n or 802.11b/g/n Video Parameters page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the maximum bandwidth allowed and the reserved roaming bandwidth. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n Video Parameters template page appears (see Figure 12-48).

*Figure 12-48 802.11a/n Video Parameters Template*




**Step 4** For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keeps the maximum allowed number of calls to an acceptable quantity. Click the check box to enable CAC.

**Step 5** Enter the percentage of maximum bandwidth allowed.

**Step 6** Enter the percentage of reserved roaming bandwidth.

**Step 7** Click **Save**.

# Configuring EDCA Parameters through a Controller Template

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic. Follow these steps to add or configure 802.11a/n or 802.11b/g/n EDCA parameters through a controller template:

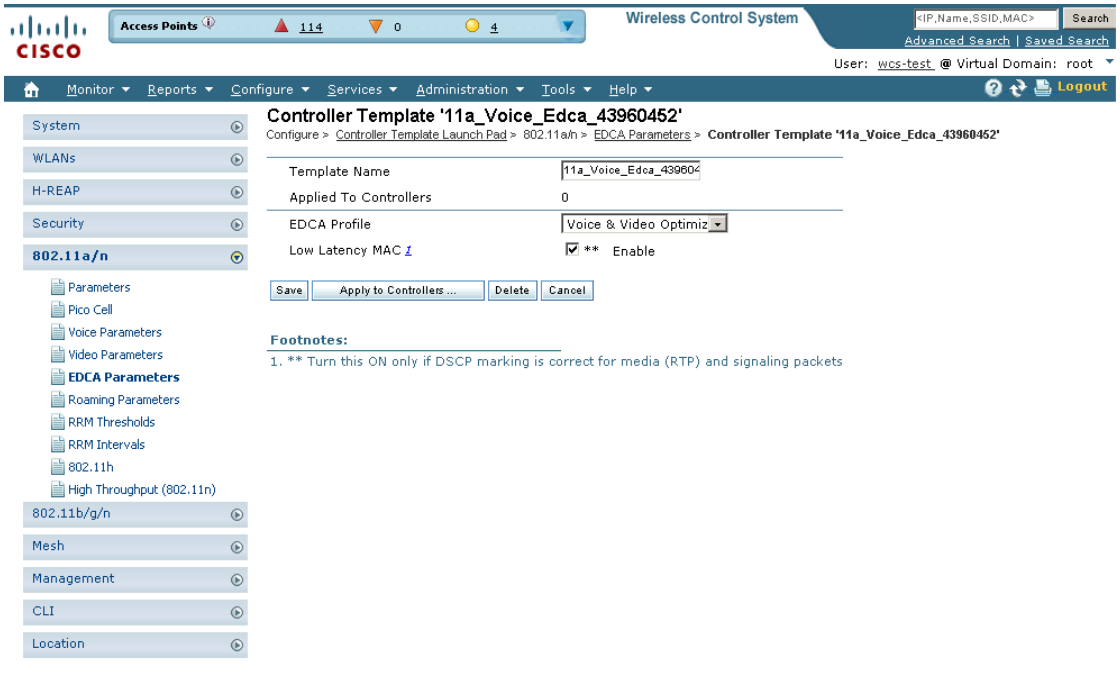
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **EDCA Parameters** or choose **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters** from the left sidebar menu. The EDCA Parameters Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the EDCP profile and the low latency MAC. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n EDCA Parameters template page appears (see Figure 12-49).

*Figure 12-49 802.11a EDCA Parameters*




**Step 4** Choose one of the following options from the **EDCA Profile** drop-down list:

- WMM—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- Spectralink Voice Priority—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
- Voice Optimized—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.
- Voice & Video Optimized —Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.

**Note** Video services must be deployed with admission control (ACM). Video services without ACM are not supported.

**Note** You must shut down radio interface before configuring EDCA Parameters.

**Step 5** Click the **Low Latency MAC** check box to enable this feature.

**Note** Cisco recommends never to enable Low Latency MAC if serving voice clients.

# Configuring a Roaming Parameters Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify an existing roaming parameter template.

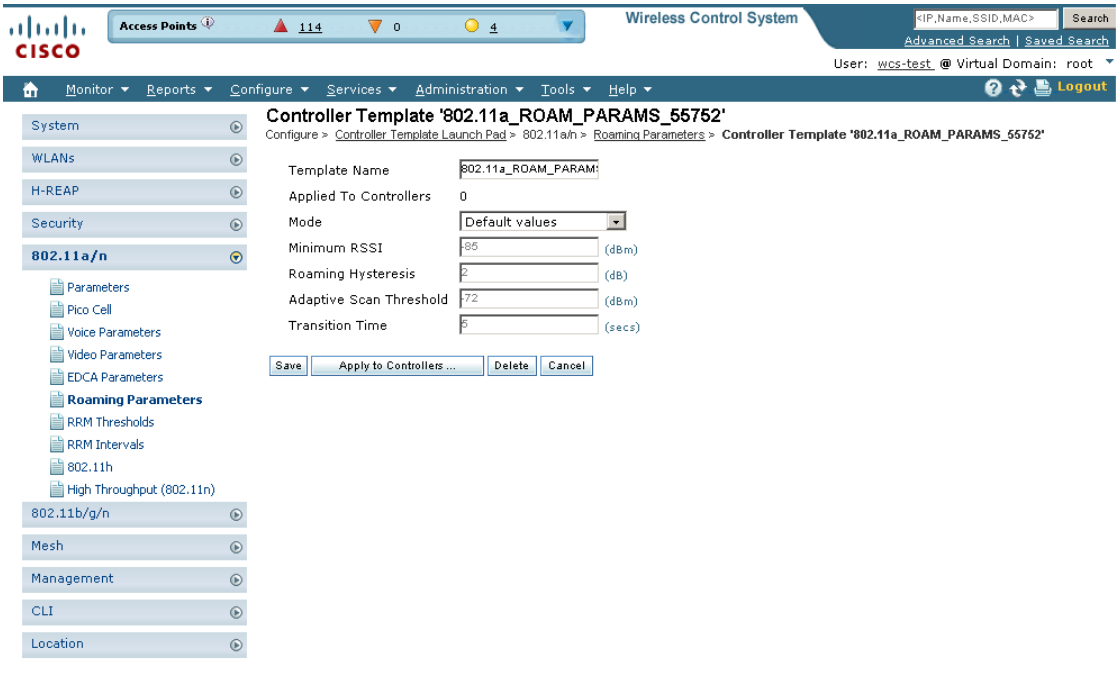
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Roaming Parameters** or choose **802.11a/n > Roaming Parameters** or **802.11b/g/n > Roaming Parameters** from the left sidebar menu. The Roaming Parameters Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the minimum RSSI, roaming hysteresis, adaptive scan threshold, and transition time. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n Roaming Parameters template page appears (see Figure 12-50).

***Figure 12-50 802.11 Roaming Parameters Template***




**Step 4** Use the Mode drop-down list to choose one of the configurable modes: default values and custom values. When the default values option is chosen, the roaming parameters are unavailable with the default values displayed in the text boxes. When the custom values option is selected, the roaming parameters can be edited in the text boxes. To edit the parameters, continue to Step 5.

**Step 5** In the Minimum RSSI field, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Range: -80 to -90 dBm

Default: -85 dBm

**Step 6** In the Roaming Hysteresis field, enter a value to indicate how strong the signal strength of a neighboring access point must be for the client to roam to it. This parameter is intended to reduce the amount of "ping ponging" between access points if the client is physically located on or near the border between two access points.

Range: 2 to 4 dB

Default: 3 dB

**Step 7** In the Adaptive Scan Threshold field, enter the RSSI value from a client's associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

Range: -70 to -77 dB

Default: -72 dB

**Step 8** In the Transition Time field, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

Range: 1 to 10 seconds

Default: 5 seconds

**Step 9** Click **Save**.

# Configuring an RRM Threshold Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or make modifications to an 802.11a/n or 802.11b/g/n RRM threshold template.

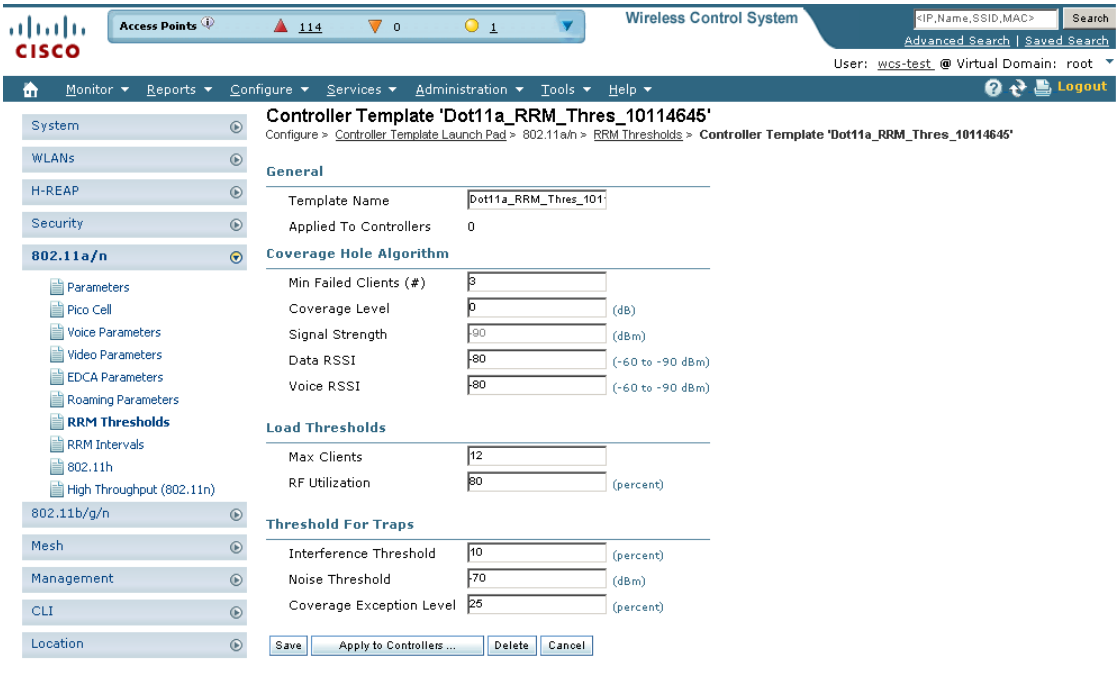
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **RRM Thresholds** or choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**. The 802.11a/n or 802.11b/g/n RRM Thresholds Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the interference and noise threshold, maximum clients, and RF utilization. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n RRM Threshold template page appears (see Figure 12-51).

***Figure 12-51 802.11b/g/n RRM Thresholds Template***




**Step 4** Enter the minimum number of failed clients currently associated with the controller.

**Step 5** Enter the target range of coverage threshold.

**Step 6** Enter the Data RSSI (–60 to –90 dBm). This number indicates the value for the minimum received signal strength indicator (RSSI) for data required for the client to associate to an access point.

**Note** You must disable the 802.11a/n or 802.11b/g/n network before applying these RRM threshold parameters.

**Step 7** Enter the Voice RSSI (–60 to –90 dBM). This number indicates the value for the minimum received signal strength indicator (RSSI) required for voice for the client to associate to an access point.

**Step 8** Enter the maximum number of failed clients that are currently associated with the controller.

**Step 9** At the RF Utilization parameter, enter the percentage of threshold for either 802.11a/n or 802.11b/g/n.

**Step 10** Enter an interference threshold percentage.

**Step 11** Enter a noise threshold between -127 and 0 dBm. When the controller is outside of this threshold, it sends an alarm to WCS.

**Step 12** Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

**Step 13** Click **Save**.

# Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or make modifications to an 802.11a/n or 802.11b/g/n RRM interval template.

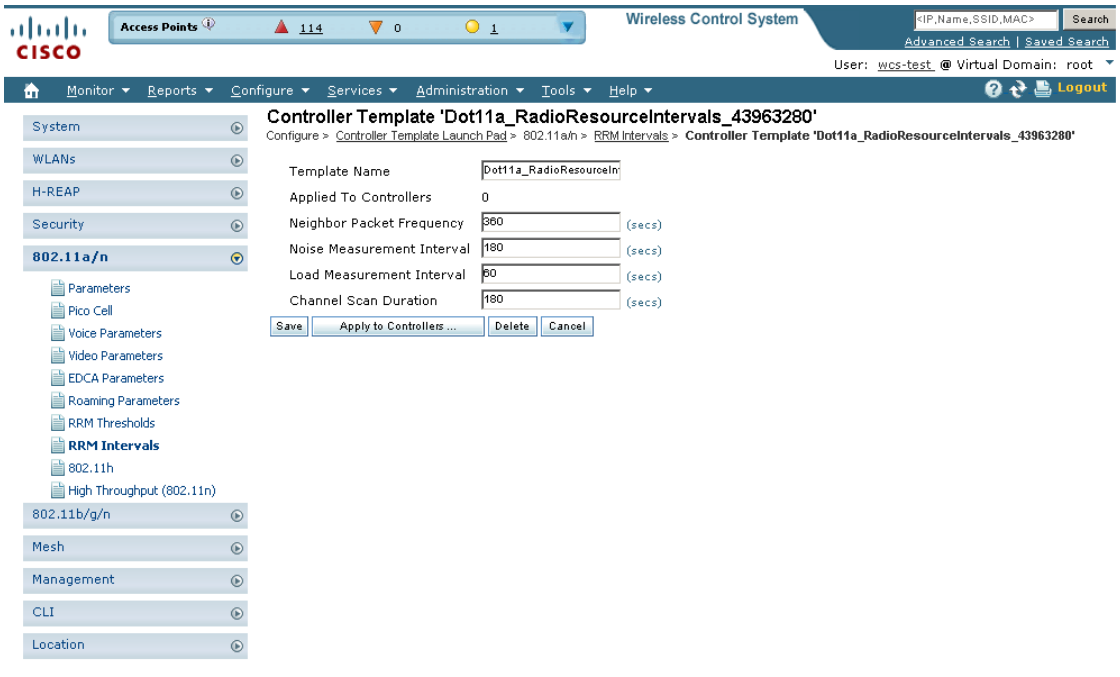
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click RRM Intervals or choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals** from the left sidebar menu. The 802.11a/n or 802.11b/g/n RRM Threshold Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the neighbor packet frequency, noise measurement interval, and load measurement interval. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n RRM Intervals template page appears (see Figure 12-52).

***Figure 12-52 802.11a/n RRM Intervals Template***



**Step 4** At the Neighbor Packet Frequency parameter, enter the interval at which you want strength measurements taken for each access point. The default is 300 seconds.

**Step 5** Enter the interval at which you want noise and interference measurements taken for each access point. The default is 300 seconds.

**Step 6** Enter the interval at which you want load measurements taken for each access point. The default is 300 seconds.

**Step 7** At the Coverage Measurement Interval parameter, enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

**Step 8** Click **Save**.

# Configuring an 802.11h Template

802.11h informs client devices about channel changes and can limit the client device's transmit power. Create or modify a template for configuration 802.11h parameters (such as power constraint and channel controller announcement) and applying these settings to multiple controllers. Follow these steps to add or modify an 802.11h template.

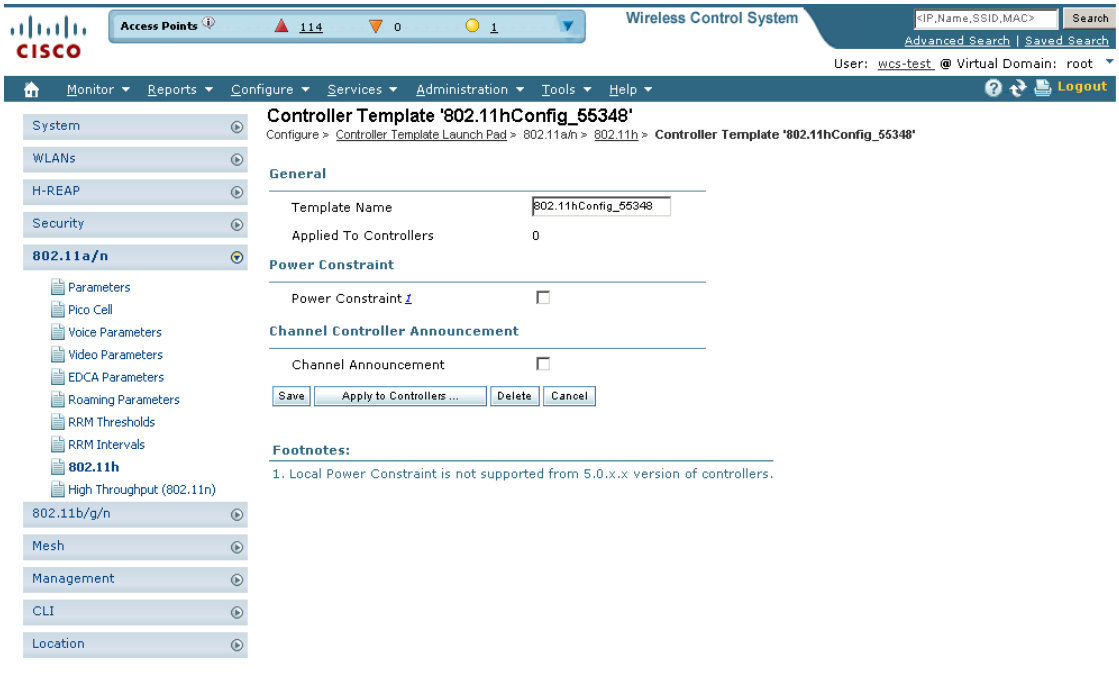
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **802.11h** or choose **802.11a/n > 802.11h** from the left sidebar menu.The 802.11h Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the local power constraint and channel announcement quiet mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11h template page appears (see Figure 12-53).

*Figure 12-53 802.11h Template*




**Step 4** Check the **Power Constraint** check box if you want the access point to stop transmission on the current channel.

**Step 5** Check the **Channel Announcement** check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

**Step 6** Click **Save**.

# Configuring a High Throughput Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add or modify to an 802.11a/n or 802.11b/g/n high throughput template.

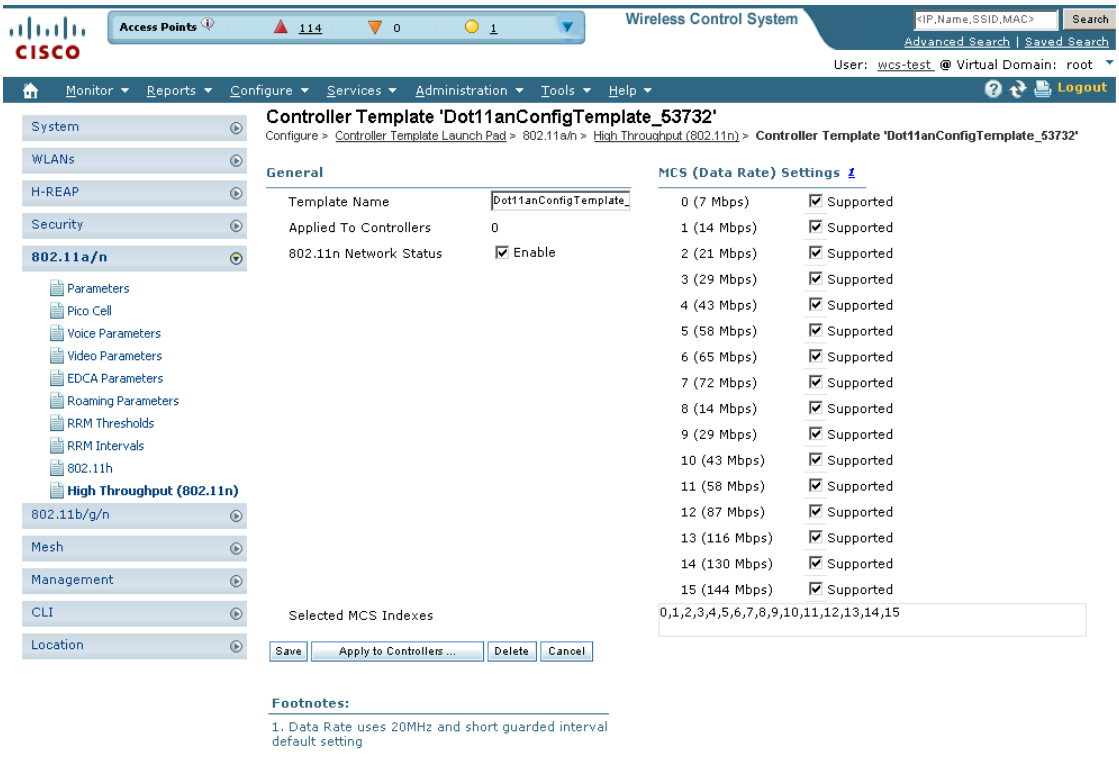
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **High Throughput (802.11n)** or choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput** from the left sidebar menu. The 802.11n Parameters for 2.4 GHz or 802.11n Parameters for 5 GHz template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the 802.11n network status. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11a/n or 802.11b/g/n High Throughput template page appears (see Figure 12-54).

***Figure 12-54 802.11n Parameters for 2.4GHz Template***




**Step 4** Click the **802.11n Network Status Enabled** check box to enable high throughput.

**Step 5** In the MCS (Data Rate) Settings column, choose which level of data rate you want supported. Modulation coding schemes (MCS) are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

**Note** When you select the **Supported** check box, the chosen numbers appear in the Selected MCS Indexes page.

**Step 6** Click **Save**.

# Configuring CleanAir Controller Templates (for 802.11a/n or 802.11b/g/n)

Create or modify a template for configuring CleanAir parameters for the 802.11a/n or 802.11 b/g/n radio. You can configure the template to enable or disable CleanAir, reporting and alarms for the controllers. You can also configure the type of interfering devices to include for reporting and alarms.

- Editing Existing CleanAir Controller Templates (802.11a/n or 802.11 b/g/n)

- Adding a New CleanAir Controller Template (802.11a/n or 802.11 b/g/n)

## Editing Existing CleanAir Controller Templates (802.11a/n or 802.11 b/g/n)

To make changes to an existing CleanAir controller, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** From the left sidebar menu, choose **802.11a/n > CleanAir** or **802.11b/g/n > CleanAir**. The 802.11a/n or 802.11b/g/n CleanAir Controller Templates page displays all currently saved 802.11a/n or 802.11b/g/n CleanAir templates. It also displays and the number of controllers and virtual domains to which each template is applied.

**Step 3** Click a template name to open the Controller Template list page. From here, you can edit the current template parameters.

**Note** See Adding a New CleanAir Controller Template (802.11a/n or 802.11 b/g/n) for information on 802.11a/n or 802.11b/g/n CleanAir template parameters.

### Command Buttons

- Save—Click to save the current template.
- Apply to Controllers—Click to apply the current template to controllers. In the Apply to Controllers page, select the applicable controllers, and click OK. See "Applying Controller Templates" for more information.
- Delete—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- Cancel—Click to cancel the current template creation or changes to the current template.

## Adding a New CleanAir Controller Template (802.11a/n or 802.11 b/g/n)

To add a new template with 802.11a/n or 802.11b/g/n CleanAir information for a controller, follow these steps:

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** From the left sidebar menu, choose **802.11a/n > CleanAir** or **802.11b/g/n > CleanAir**. The 802.11a/n or 802.11b/g/n CleanAir Controller Templates page displays all currently saved 802.11a/n or 802.11b/g/n CleanAir templates. It also displays and the number of controllers and virtual domains to which each template is applied.

**Step 3** From the **Select a Command** drop-down list, choose **Add a Template**, and click **Go**.

The **New Controller Template** page appears.

**Step 4** Add or modify the following parameters:

- Template Name—Enter the template name.
- CleanAir—Select the check box to enable CleanAir functionality on the 802.11 b/g/n network, or unselect to prevent the controller from detecting spectrum interference.

**Note** If CleanAir is enabled, the Reporting Configuration and Alarm Configuration sections appear.

- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report Interferers—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is checked.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.
- Alarm Configuration—This section enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.
  - Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.
  - Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is unselected.
  - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

**Step 5** Click **Save**. Once saved, the template displays in the Template List page. In the Template List page, you can apply this template to controllers. See "Adding Controller Templates" for more information.

# Configuring a Mesh Template

You can configure an access point to establish a connection with the controller. Follow these steps to add or modify a mesh template.

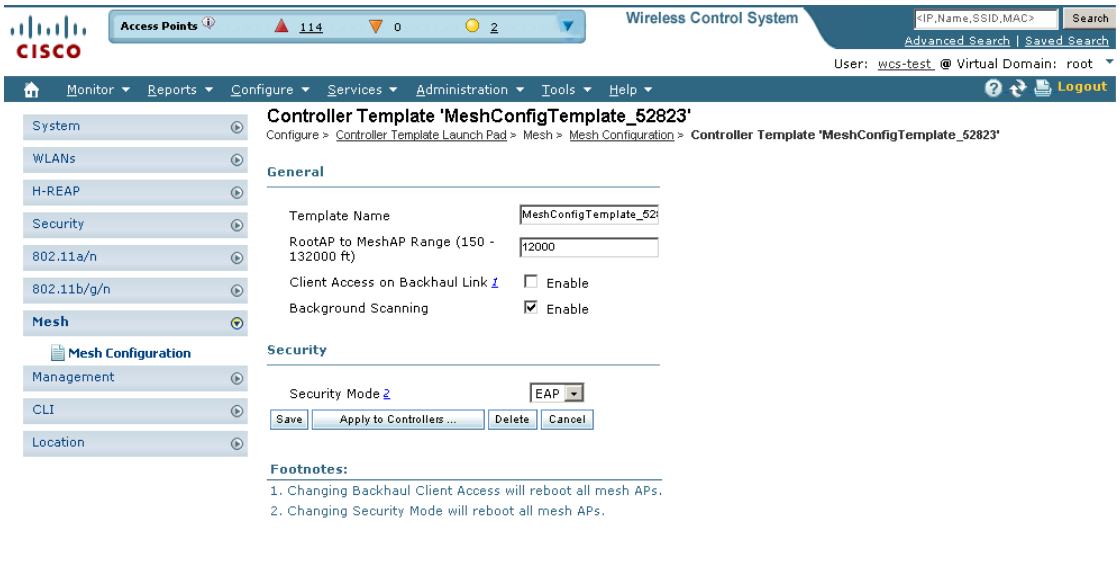
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Mesh Configuration** or choose **Mesh > Mesh Configuration** from the left sidebar menu. The Mesh Configuration Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the rootAP to MeshAP range, the client access on backhaul link, and security mode. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Mesh Configuration template page appears (see Figure 12-55).

***Figure 12-55 Mesh Configuration Template***




**Step 4** The Root AP to Mesh AP Range is 12,000 feet by default. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global parameter applies to all access points when they join the controller and all existing access points in the network.

**Step 5** The **Client Access on Backhaul Link** check box is not checked by default. When this option is enabled, mesh access points can associate with 802.11a/n wireless clients over the 802.11a/n backhaul. This client association is in addition to the existing communication on the 802.11a/n backhaul between the root and mesh access points.

**Note** This feature applies only to access points with two radios.

**Step 6** The **Mesh DCA Channels** check box is not selected by default. Select this option to enable backhaul channel deselection on the Controller using the DCA channel list configured in the Controller. Any change to the channels in the Controller DCA list is pushed to the associated access points. This feature applies only to the 1524SB mesh access points. For more information on this feature, see the *Controller Configuration Guide*

**Step 7** Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. See the "Background Scanning on 1510s in Mesh Networks" section on page 10-63 for further information.

**Step 8** From the Security Mode drop-down list, choose **EAP** (Extensible Authentication Protocol) or **PSK** (Pre-Shared Key).

**Step 9** Click **Save**.

# Configuring a Trap Receiver Template

Follow these steps to add or modify a trap receiver template. If you have monitoring devices on your network that receive SNMP traps, you may want to add a trap receiver template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Trap Receivers** or choose **Management > Trap Receivers** from the left sidebar menu.

**Step 3** The Management > Trap Receiver page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the IP address and admin status. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 4** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Trap Receivers template page appears (see Figure 12-56).

***Figure 12-56 Trap Receiver Template***


**Step 5** Enter the IP address of the server.

**Step 6** Click to enable the admin status if you want SNMP traps to be sent to the receiver.

**Step 7** Click **Save**.

# Configuring a Trap Control Template

Follow these steps to add or modify a trap control template.

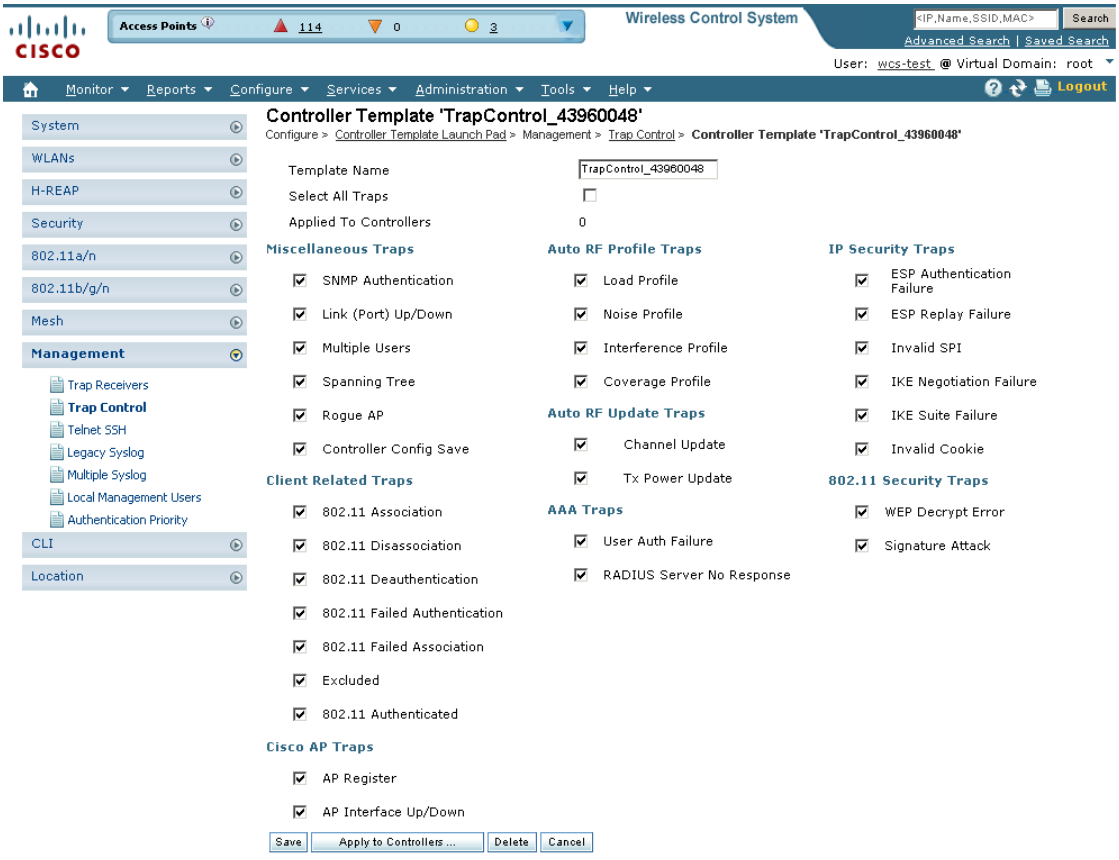
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Trap Control** or choose **Management > Trap Control** from the left sidebar menu. The Management > Trap Control page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the link port up or down and rogue AP. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Trap Control template page appears (see Figure 12-57).

*Figure 12-57 Trap Controls Template*




**Step 4** Check the appropriate check box to enable any of the following miscellaneous traps:

- SNMP Authentication - The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.
- Link (Port) Up/Down - Link changes states from up or down.
- Multiple Users - Two users log in with the same login ID.
- Spanning Tree - Spanning Tree traps. See the STP specification for descriptions of individual parameters.
- Rogue AP - Whenever a rogue access point is detected or when a rogue access point was detected earlier and no longer exists, this trap is sent with its MAC address.
- Controller Config Save - Notification sent when the configuration is modified.

**Step 5** Check the appropriate check box to enable any of the following client-related traps:

- 802.11 Association - A trap is sent when a client is associated to a WLAN. This trap does not guarantee that the client is authenticated.
- 802.11 Disassociation - The disassociate notification is sent when the client sends a disassociation frame.

- 802.11 Deauthentication - The deauthenticate notification is sent when the client sends a deauthentication frame.
- 802.11 Failed Authentication - The authenticate failure notification is sent when the client sends an authentication frame with a status code other than successful.
- 802.11 Failed Association - The associate failure notification is sent when the client sends an association frame with a status code other than successful.
- Excluded - The associate failure notification is sent when a client is excluded.

**Step 6** Check the appropriate check box to enable any of the following access point traps:

- AP Register - Notification sent when an access point associates or disassociates with the controller.
- AP Interface Up/Down - Notification sent when access point interface (802.11a/n or 802.11b/g/n) status goes up or down.

**Step 7** Check the appropriate check box to enable any of the following auto RF profile traps:

- Load Profile - Notification sent when Load Profile state changes between PASS and FAIL.
- Noise Profile - Notification sent when Noise Profile state changes between PASS and FAIL.
- Interference Profile - Notification sent when Interference Profile state changes between PASS and FAIL.
- Coverage Profile - Notification sent when Coverage Profile state changes between PASS and FAIL.

**Step 8** Check the appropriate check box to enable any of the following auto RF update traps:

- Channel Update - Notification sent when access point's dynamic channel algorithm is updated.
- Tx Power Update - Notification sent when access point's dynamic transmit power algorithm is updated.

**Step 9** Check the appropriate check box to enable any of the following AAA traps:

- User Auth Failure - This trap is to inform you that a client RADIUS authentication failure has occurred.
- RADIUS Server No Response - This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

**Step 10** Check the appropriate check box to enable the following IP security traps:

- ESP Authentication Failure
- ESP Replay Failure
- Invalid SPI
- IKE Negotiation Failure
- IKE Suite Failure
- Invalid Cookie

**Step 11** Check the appropriate check box to enable the following 802.11 security trap:

- WEP Decrypt Error - Notification sent when the controller detects a WEP decrypting error.
- Signature Attack

**Step 12** Click **Save**.

# Configuring a Telnet SSH Template

Follow these steps to add or modify a Telnet SSH configuration template.

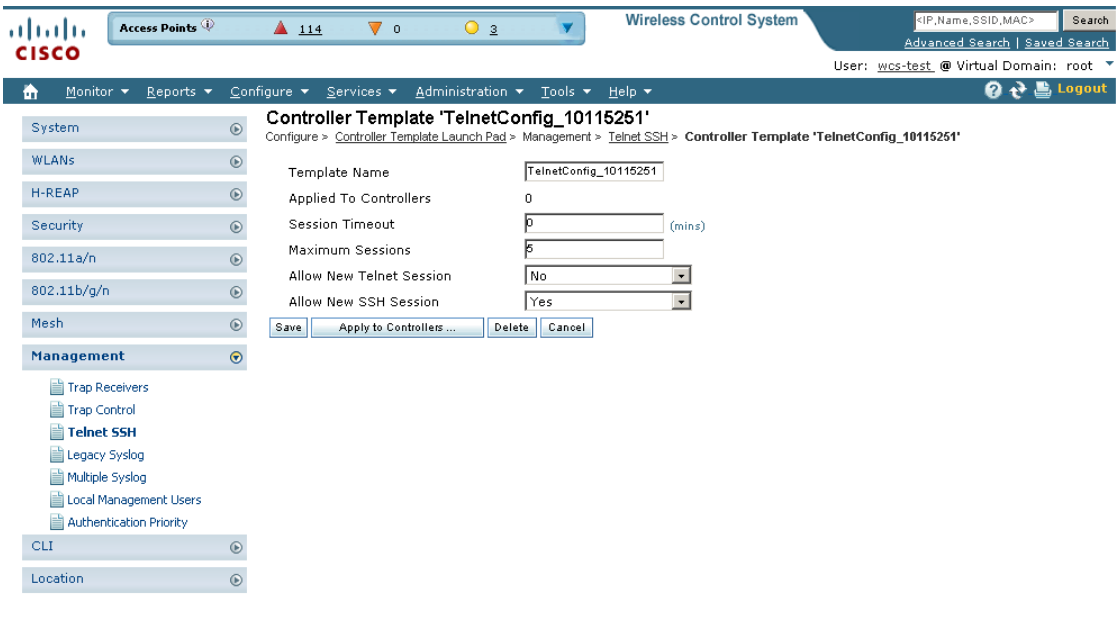
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Telnet SSH** or choose **Management > Telnet SSH** from the left sidebar menu. The Management > Telnet SSH Configuration page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the session timeout, maximum sessions, and whether Telnet or SSH sessions are allowed. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Telnet SSH template page appears (see Figure 12-58).

***Figure 12-58 Telnet SSH Configuration Template***




**Step 4** Enter the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The valid range is 0 to 160, and the default is 5.

**Step 5** At the Maximum Sessions parameter, enter the number of simultaneous Telnet sessions allowed. The valid range is 0 to 5, and the default is 5. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port.

**Step 6** Use the Allow New Telnet Session drop-down list to determine if you want new Telnet sessions allowed on the DS port. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port. The default is no.

**Step 7** Use the Allow New SSH Session drop-down list to determine if you want Secure Shell Telnet sessions allowed. The default is yes.

**Step 8** Click **Save**.

# Configuring a Legacy Syslog Template

Follow these steps to add or modify a legacy syslog configuration template.

**Note** Legacy Syslog applies to controllers earlier than version 5.0.6.0

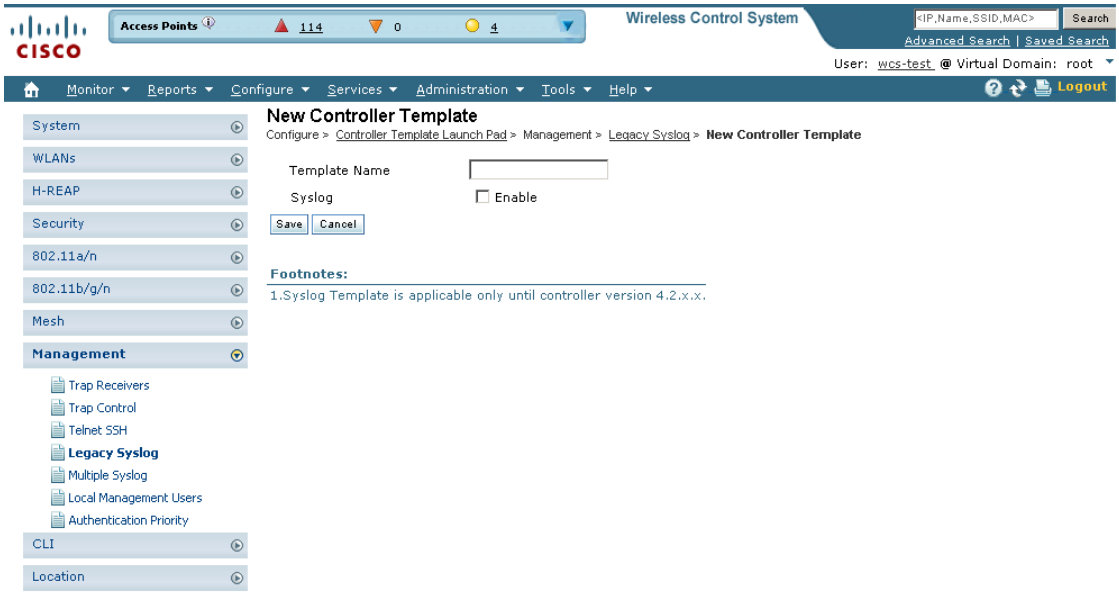
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click Legacy Syslog or choose **Management > Legacy Syslog** from the left sidebar menu. The Management > Legacy Syslog page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Legacy Syslog template page appears (see Figure 12-59).

***Figure 12-59 Syslog Configuration Template***




**Step 4** Enter a template name. The number of controllers to which this template is applied is displayed.

**Step 5** Click to enable syslog. When you do, a Syslog Host IP Address parameter appears.

**Step 6** Click **Save**.

# Configuring a Multiple Syslog Template

Follow these steps to add or modify a multiple syslog configuration template.

**Note** You can enter up to three syslog server templates.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Multiple Syslog** or choose **Management > Multiple Syslog** from the left sidebar menu. The Management > Multiple Syslog page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the syslog server address. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Multiple Syslog template page appears (see Figure 12-60).

***Figure 12-60 Syslog Server Template Page***


**Step 4** Enter a template name and a syslog server IP address.

**Step 5** Click **Save**.

# Configuring a Local Management User Template

Follow these steps to add or modify a local management user template.

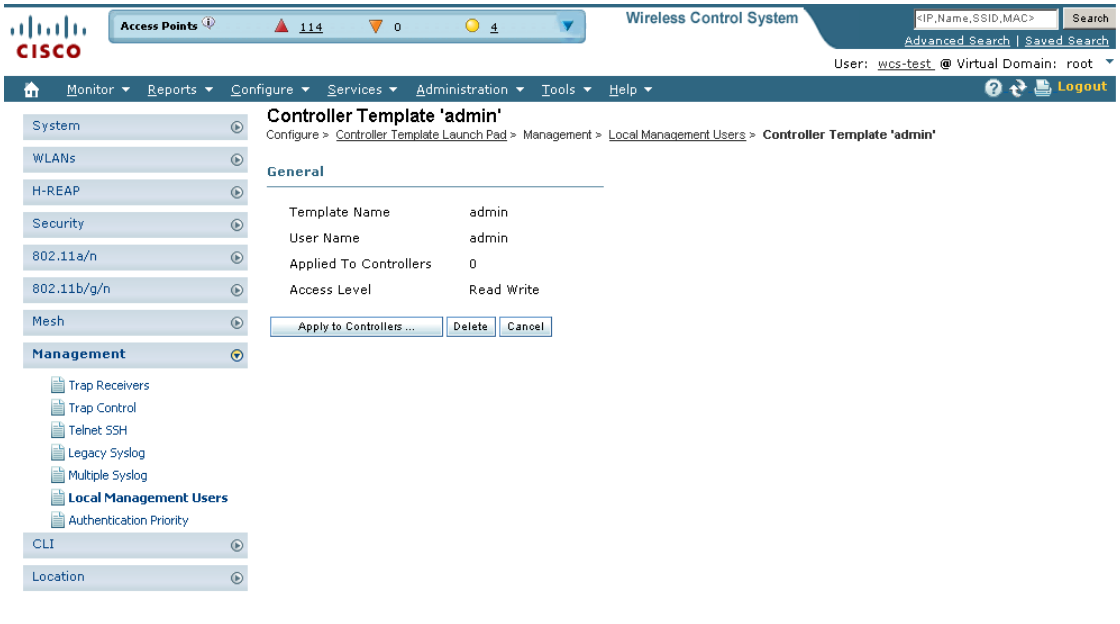
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Local Management Users** or choose **Management > Local Management Users** from the left sidebar menu. The Management > Local Management Users Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the user name and access level. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local Management Users template page appears (see Figure 12-61).

***Figure 12-61 Local Management Users Template***




**Step 4** Enter a template name

**Step 5** Enter a template username.

**Step 6** Enter a password for this local management user template.

**Step 7** Re-enter the password.

**Step 8** Use the Access Level drop-down list to choose either Read Only or Read Write.

**Step 9** Click **Save**.

# Configuring a User Authentication Priority Template

Management user authentication priority templates control the order in which authentication servers are used to authenticate a controller's management users. Follow these steps to add a user authentication priority template or make modifications to an existing template.

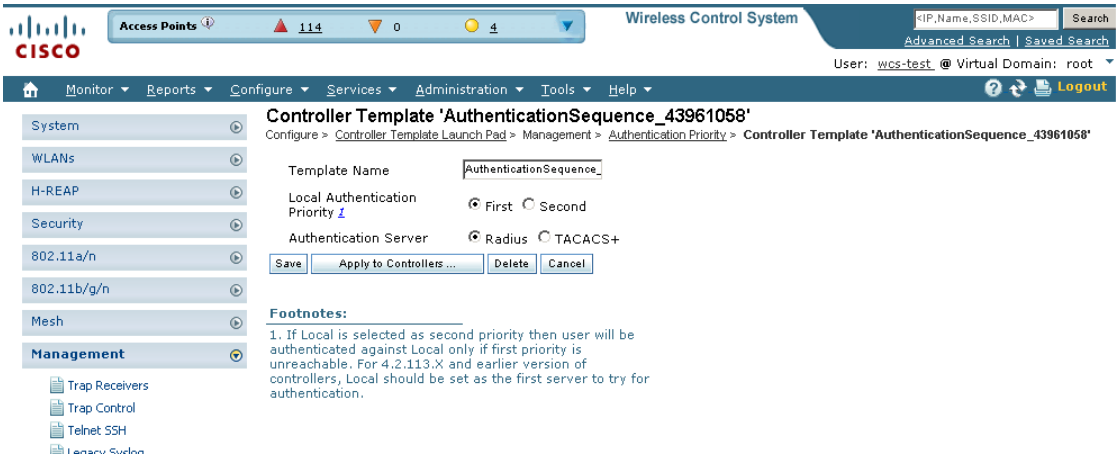
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Authentication Priority** or choose **Management > Authentication Priority** from the left sidebar menu. The Management > Local Management Users Template appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the authentication priority list. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Local Management Users template page appears (see Figure 12-62).

***Figure 12-62 User Authentication Priority Template***




**Step 4** Enter a template name.

**Step 5** The local server is tried first. Choose either **RADIUS** or **TACACS+** to try if local authentication fails.

**Step 6** Click **Save**.

# Applying a Set of CLI Commands

You can create templates containing a set of CLI commands and apply them to one or more controllers from WCS. These templates are meant for provisioning features in multiple controllers for which there is no SNMP support or custom WCS user interface. The template contents are simply a command array of strings. No support for substitution variables, conditionals, and the like exist.

The CLI sessions to the device are established based on user preferences. The default protocol is SSH. See the "CLI Session" section on page 18-41 for information on setting protocol user preferences.

Follow these steps to add or modify a CLI template.

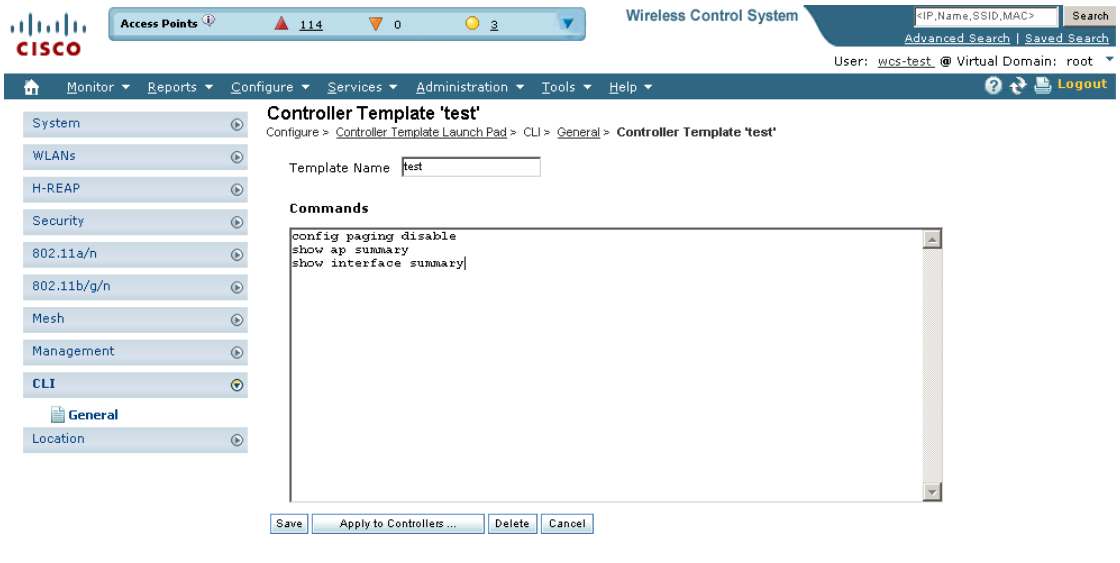
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **CLI > General** or choose **CLI > General** from the left sidebar menu. The CLI > General page appears, and the number of controllers that the template is applied to automatically populates.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Command Line Interface General template page appears (see Figure 12-63).

***Figure 12-63 Command Line Interface Template***




**Step 4** If you are adding a new template, provide a name that you are giving to this string of commands. If you are making modifications to an existing template, the Template Name field cannot be modified.

**Step 5** In the Commands page, enter the series of CLI commands.

**Step 6** Click **Save** to save the CLI commands to the WCS database without applying to the selected controllers or **Apply to Controllers** to save the commands to the WCS database as well as apply to the selected controllers. If you click Apply to Controllers, choose the IP address of the controller to which you want to apply the template.

**Note** When the template is applied to the selected controllers, a status screen appears. If an error occurred while you applied the template, an error message is displayed. You can click the icon in the Session Output column to get the entire session output.

**Note** If the Controller Telnet credentials check fails or the Controller CLI template fails with invalid username and password even though the correct username and password are configured on the controller, check whether the controller has exceeded the number of CLI connections it can accept. If the connections have exceeded the maximum limit, then either increase the maximum allowed CLI sessions or terminate any pre-existing CLI sessions on the controller, and then retry the operation.

# Configuring Location Settings

Follow these steps to add or modify a location setting template.

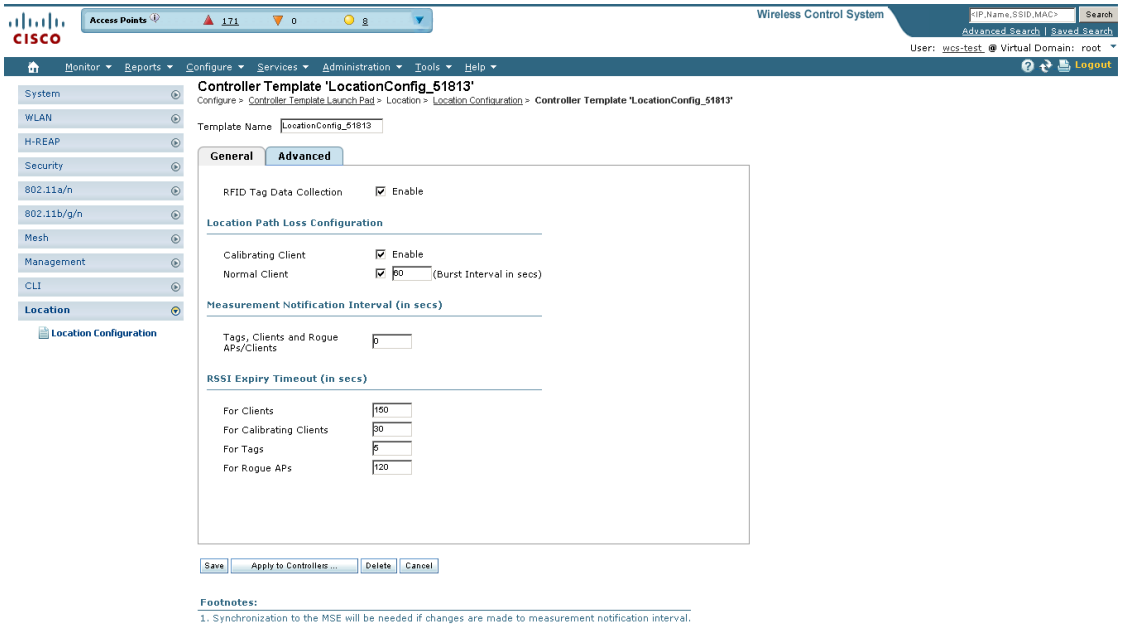
**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click **Location > Location Configuration** or choose **Location > Location Configuration** from the left sidebar menu. The Location > Location Configuration page appears, and the number of controllers that the template is applied to automatically populates.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, click **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The template page appears (see Figure 12-64).

*Figure 12-64 Location Configuration Template*




**Step 4** Check the **RFID Tag Data Collection** check box to enable tag collection. Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers.

**Step 5** Check the **Calibrating Client** check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

**Note** To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced page.

**Step 6** Check the **Normal Client** check box to have a non-calibrating client. No S36 or S60 requests are transmitted to the client.

**Step 7** Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue APs/clients).

**Step 8** Enter the number of seconds after which RSSI measurements for clients should be discarded.

**Step 9** Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.

**Step 10** Enter the number of seconds after which RSSI measurements for tags should be discarded.

**Step 11** Enter the number of seconds after which RSSI measurement for rogue access points should be discarded.

**Step 12** Click the **Advanced** tab.

**Step 13** Enter a value in seconds to set the RFID tag data timeout setting.

**Step 14** Check the **Calibrating Client Multiband** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the general panel.

**Step 15** Click **Save**.

# Applying Controller Templates

You can apply a controller template to a controller.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Using the left sidebar menu, choose the category of templates to apply. A list of devices is shown.

**Step 3** Click the Template Name for the template that you want to apply to the controller.

**Step 4** Click **Apply to Controllers** to open the Apply to Controllers page.

**Note** In the Configure > Controllers page, you can see which templates are applied to controllers. See the "Displaying Templates Applied to Controller" section on page 10-10 for further information. You can also discover templates in the Configure > Controllers page. See the "Discovering Templates from Controllers" section on page 10-9 for more information.

**Step 5** Choose between applying the template directly to a controller or to all controllers in a selected configuration group.

To apply the template directly to a controller(s), follow these steps:

a. Select the **Apply to controllers selected directly** radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).

b. Check the check box for each controller to which you want to apply the template.

**Note** Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a. Select the **Apply to controllers in the selected Config Groups** radio button. The Apply to Controllers page list the name of each configuration group along with the mobility group name and the number of controllers included.

b. Check the check box for each configuration group to which you want to apply the template.

**Note** Configuration groups which have no controllers cannot be selected to apply the templates.

**Step 6** Click **OK**.

## Deleting a Controller Template

Follow these steps to delete a controller template.

**Step 1** Choose **Configure > Controller Template Launch Pad**.

**Step 2** Click the template type to open its template list page.

**Step 3** Click the check box(es) of the template(s) that you want to delete.

**Step 4** From the Select a command drop-down list, choose **Delete Templates**, and click **Go**.

**Step 5** Click **OK** to confirm the deletion. If this template is applied to controllers, the Remove Template Confirmation page opens and lists all controllers to which this template is currently applied.

**Step 6** Check the check box of each controller from which you want to remove the template.

**Step 7** Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

# Configure AP Configuration Templates

This menu provides access to the access point templates summary details. Use the selector area to access and configure the respective templates details.

**Note** Select a template name to view or edit parameters for current access point templates. View the applicable steps in "Configuring Lightweight Access Point Templates" for more information on access point template parameters.

- <CrossRef>Configure Lightweight Access Point Templates
- Configure Autonomous Access Point Templates
- Applying or Scheduling Lightweight or Autonomous AP Templates

## Configure Lightweight Access Point Templates

This section includes the following topics:

- Adding Lightweight Access Point Templates
- Configuring Lightweight Access Point Templates

### Adding Lightweight Access Point Templates

Follow these steps to add a new lightweight access point template.

**Step 1** Choose **Configure > AP Configuration Templates > Lightweight AP**.

**Step 2** Choose **Add Template** from the Select a command drop-down list, and click **Go**.

**Step 3** Enter the template name.

**Step 4** Describe the template.

**Step 5** Click **Save**.

## Configuring Lightweight Access Point Templates

Follow these steps to configure a template of access point information that you can apply to one or more access points.

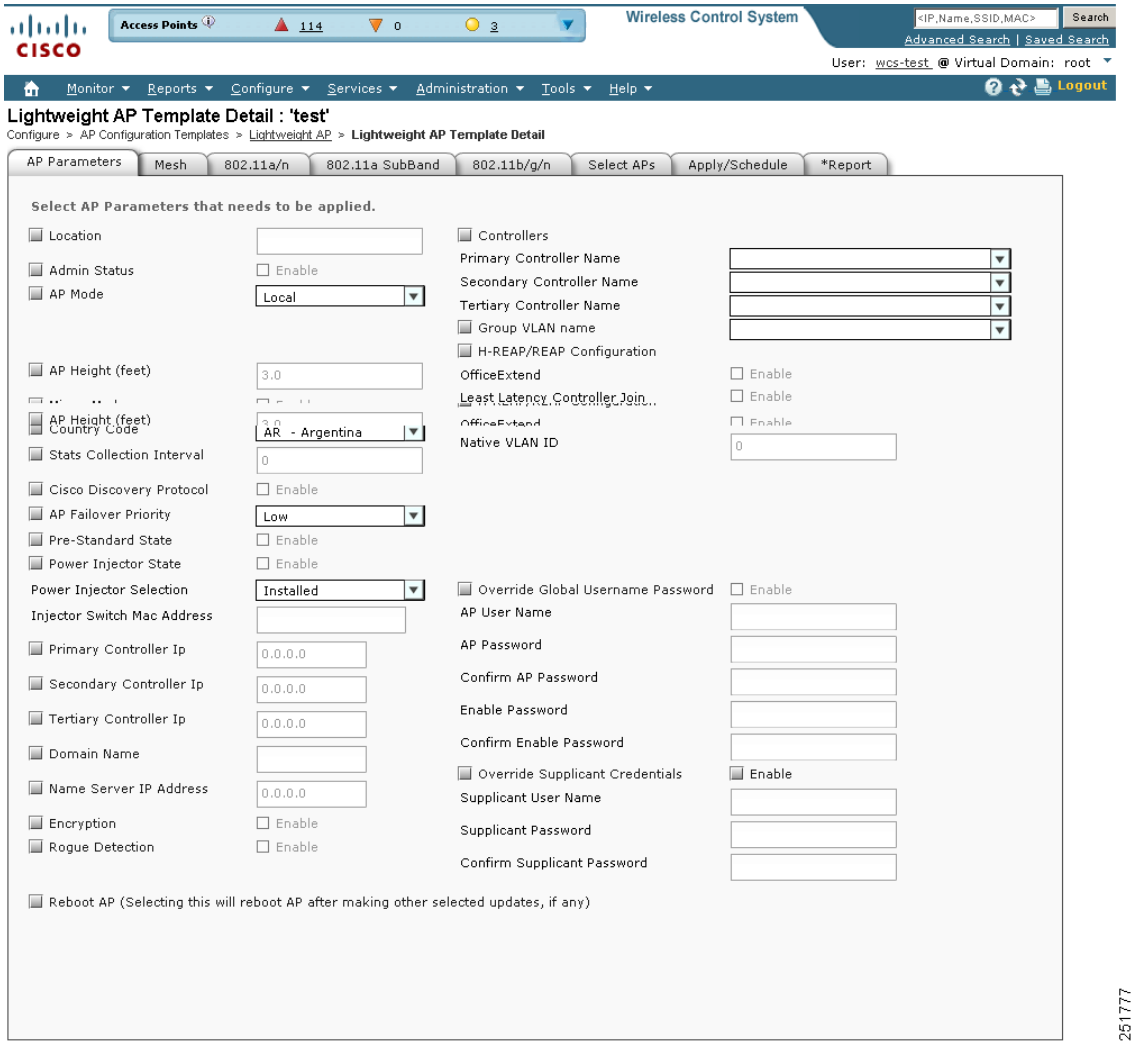
**Step 1** Choose **Configure > AP Configuration Template > Lightweight AP**.

**Step 2** In the Template Name column, click the template name you want to configure.

**Note** Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the Autonomous AP. If this check box is not selected, any errors encountered while applying a command in the template to a Autonomous AP causes the rest of the commands to be not applied.

**Step 3** Click the **AP Parameters** tab. The AP/Radio Templates page appears (see Figure 12-65) if you chose Lightweight AP. If you chose Autonomous AP, the heading is Command Line Interface Templates.

*Figure 12-65 AP/Radio Templates*




**Step 4** Select the Location check box and enter the access point location.

**Step 5** Select both the **Admin Status** and **Enabled** check box to enable access point administrative status.

**Note** In order to conserve energy, access points can be turned off at specified times during non-working hours. Select the **Enabled** check box to allow access points to be turned on or off.

**Step 6** Select the **AP Mode** check box and use the drop-down list to set the operational mode of the access point as follows:

- Local - Default
- Monitor - Monitor mode only.

**Note** Select Monitor to enable this access point template for Cisco Adaptive wIPS. Once Monitor is selected, select the Enhanced WIPS Engine check box and the Enabled check box. Then select the AP Monitor Mode Optimization check box and WIPS from the AP Monitor Mode Optimization drop-down list. You cannot use monitor mode optimization if wIPS is disabled. For more information on Cisco Adaptive wIPS, see the "wIPS" section on page 13-1 for more information.

- H-REAP/REAP - Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.

**Note** H-REAP must be selected in order to configure an OfficeExtend access point. When the AP mode is H-REAP, H-REAP configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join. See the "Configuring Hybrid REAP" section on page 15-4 for further information.

- Rogue Detector - Monitors the rogue access points but does not transmit or contain rogue access points.
- Bridge

**Note** Changing the AP mode reboots the access point.

- Sniffer - The access point performs an inspection on a given channel. It captures and forwards all the packets from the client on that channel to a remote machine that runs airopeek (a packet analyzer for IEEE 802.11 wireless LANs). It includes information on timestamp, signal strength, packet size, and so on. If you choose Sniffer as an operation mode, you are required to enter a channel and server IP address on the AP/Radio Templates 802.11b/g/n or 802.11a/n parameters tab.

**Note** The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see http://www.wildpackets.com/support/legacy/airopeek/overview.

**Step 7** Select the **Enhanced wIPS engine** and the **Enabled** check box to enable.

**Step 8** Select **None** or **wIPS** from the AP Monitor Mode Optimization drop-down list. You cannot choose wIPS if wIPS was not enabled in Step 7.

**Step 9** Enter the access point height in feet. The height defaults to the floor height. The height must be greater than 3 feet and must not exceed the floor height. The specified height is applied to all selected access points in the template.

**Note** To change the height for a specific access point, go to **Monitor > Maps > Floor > Position Access Points**.

**Step 10** You must click both the **Mirror Mode** and **Enabled** check box to enable access point mirroring mode.

**Step 11** Click the check box to enable the country code drop-down list. For this access point, choose a country code selection to allow. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country's regulations.

**Note** Access points may not operate properly if they are not designed for use in your country. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country's regulatory domain. For a complete list of country codes supported per product, refer to:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

**Note** Changing the country code may cause the access point to reboot.

**Step 12** Click to enable **Stats Collection Interval** and then enter the collection period (in seconds) for access point statistics.

**Step 13** Click the **Cisco Discovery Protocol check box** and click **Enable** to allow CDP on a single access point or all access points. CDP is a device discovery protocol that runs on all Cisco manufactured equipment (such as routers, bridges, communication servers, and so on).

**Step 14** By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is overloaded, the higher-priority access points join the backup controller and disjoin the lower priority access points. Set the AP Failover Priority setting to low, medium, high, or critical.

**Step 15** Choose pre-standard state if the access point is powered by a high power Cisco switch. Otherwise, it should be disabled.

**Step 16** You can now manipulate power injector settings through WCS without having to go directly to the controllers. If the Power Injector State is checked, use the Power Injector Selection drop-down list to choose from the possible values of unknown, installed, override, or foreign. If you choose foreign, you must enter the Injector Switch MAC address.

**Step 17** Click the **Primary**, **Secondary**, or **Tertiary Controller IP** check box, and enter the appropriate IP addresses.

**Step 18** Domain Name Server IP and Domain Name can be configured only on access points which have static IP.

**Step 19** Check the check box to enable rogue detection. See the "Rogue Access Point Location, Tagging, and Containment" section on page 16-21.

**Step 20** Check the **Encryption** check box to enable encryption.

**Note** DTLS data encryption is enabled automatically for OfficeExtend access points.

**Step 21** (MESH ONLY) Enter a bridge group name (up to 10 characters).

**Note** Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other. For mesh access points to communicate, they must have the same bridge group name. For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another. For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

**Step 22** (MESH ONLY) Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

**Note** This data rate is shared between the mesh access points and is fixed for the whole mesh network. Do NOT change the data rate for a deployed mesh networking solution.

**Step 23** (MESH ONLY) Choose the **Enable** option from the Ethernet Bridging drop-down list to enable Ethernet bridging for the mesh access point.

**Step 24** Check the **SSH Access** check box to enable SSH access.

**Step 25** Check the **Telnet Access** check box to enable Telnet access.

**Note** An OfficeExtend access point may be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.

**Step 26** Click the check box if you want to enable link latency. You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for hybrid-REAP access points, for which the link could be a slow or unreliable WAN connection. See "Configuring Link Latency Settings for Access Points" section on page 9-40 for more information.

**Note** Link latency is supported for use only with hybrid-REAP access points in connected mode. Hybrid-REAP access points in standalone mode are not supported.

**Step 27** Check the **Reboot AP** check box to enable a reboot of the access point after making any other updates.

**Step 28** Select **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point's failover priority. The default priority is low.

**Step 29** Choose the **Controllers** check box to enable the drop-down lists for the primary, secondary, and tertiary controller names.

**Step 30** Choose the appropriate group VLAN name from the drop-down lists.

**Step 31** Check the check box to enable H-REAP configuration (including VLAN support, native VLAN ID, and profile name VLAN mappings).

- OfficeExtend—The default is Enabled.

**Note** Clearing the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the access point's personal SSID, click **Reset Personal SSID** at the bottom of the access point details page.

**Note** Then VLAN support should be pushed to the controller before sending the WLAN profile mappings.

**Note** When you select Enable for the OfficeExtend AP, several configuration changes automatically occur including: encryption and link latency are enabled; rogue detection, SSH access, and Telnet access are disabled.

**Note** When you enable the OfficeExtend access point, you must configure at least one primary, secondary, and tertiary controller (including name and IP address).

**Step 32** When Least Latency Controller Join is enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

**Note** The access point only performs this search once— when it initially joins the controller. It does not recalculate the primary, secondary, and tertiary controllers' latency measurements once joined to see if the measurements have changed.

**Step 33** The SSID-VLAN Mappings section lists all the SSIDs of the controllers which are currently enabled for HREAP local switching. You can edit the number of VLANs from which the clients will get an IP address by clicking the check box and adjusting the value.

**Step 34** Enter a native VLAN ID between the range of 1 to 4094. If you are changing the mode to REAP and if the access point is not already in REAP mode, then all other REAP parameters are not applied on the access point.

**Step 35** In the System > AP Username Password page, you can set global credentials for all access points to inherit as they join a controller. These established credentials are displayed in the lower right of the AP Parameters tab page. If you want to override the global credentials for this particular access point, select the **Override Global Username Password** check box. You can then enter a unique username, password, and enable password that you want to assign to this access point.

**Step 36** Select the **Override Supplicant Credentials** check box to override supplicant credentials. If selected, enter a new supplicant username and password. Confirm the supplicant password. See "Configuring AP 802.1X Supplicant Credentials" section on page 12-9 for more information on supplicant credentials.

**Step 37** Click the **Mesh** tab.

**Step 38** To assign this access point to a bridge group, enter a name for the group in the Bridge Group Name field. The name can be up to 10 characters.

**Note** Bridge groups are used to logically group the mesh access points to avoid having two networks on the same channel communicating with each other. For mesh access points to communicate, they must have the same bridge group name.

**Note** For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another. For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

**Step 39** Choose a data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

**Note** The data rate is shared between the mesh access points and is fixed for the whole mesh network.

**Note** Do NOT change the data rate for a deployed mesh networking solution.

**Step 40** Choose **Enabled** or **Disabled** from the Ethernet Bridging drop-down list.

**Step 41** Use the Role drop-down list to choose MAP or RAP. Choose MAP (MeshAP) if the 1520 series access point has a wireless connection to the controller. Choose RAP (RootAP) if the 1520 series access point has a wired connection to the controller.

**Note** At least one mesh access point must be set to RootAP in the mesh network.

**Step 42** Click the **Select APs** tab. Use the drop-down list to apply the parameters by controller, floor area, outdoor area, or all. Click **Apply**.

**Note** When you apply the template to the access point, WCS checks to see if the access point supports REAP mode and displays the application status accordingly. Clicking Apply saves and applies the template parameters to the selected access points. After applying a report, it appears in the Apply Report tab.

# Configure Autonomous Access Point Templates

The Configuring > Autonomous Access Point Templates page allows you to configure CLI templates for autonomous access points.

- Configuring a New Autonomous Access Point Template
- Applying an AP Configuration Template to an Autonomous Access Point

## Configuring a New Autonomous Access Point Template

To configure a new autonomous access point template, follow these steps:

**Step 1** Choose **Configure > AP Configuration Templates > Autonomous AP**.

**Step 2** From the **Select a Command** drop-down menu, choose **Add Template**.

**Step 3** Click **GO**.

**Step 4** Enter a **Template Name**.

**Step 5** Enter the applicable CLI commands.

**Step 6** Click **Save**.

## Applying an AP Configuration Template to an Autonomous Access Point

To apply an AP configuration template to an autonomous access point, follow these steps:

**Step 1** Choose **Configure > AP Configuration Templates > Autonomous AP**.

**Step 2** Click the template name link to select a template and apply it to the an autonomous access point. The Autonomous AP Template page appears.

**Step 3** Enter a **Template Name**.

**Step 4** Enter the applicable CLI commands.

**Step 5** Click **Save**.

**Step 6** Click **Apply to Autonomous Access Points**. The Apply to Autonomous Access Points page appears.

**Step 7** Select the desired autonomous access point.

**Step 8** Click **OK**.

**Note** Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the Autonomous AP. If this check box is not selected, any errors encountered while applying a command in the template to a Autonomous AP causes the rest of the commands to be not applied.

# Applying or Scheduling Lightweight or Autonomous AP Templates

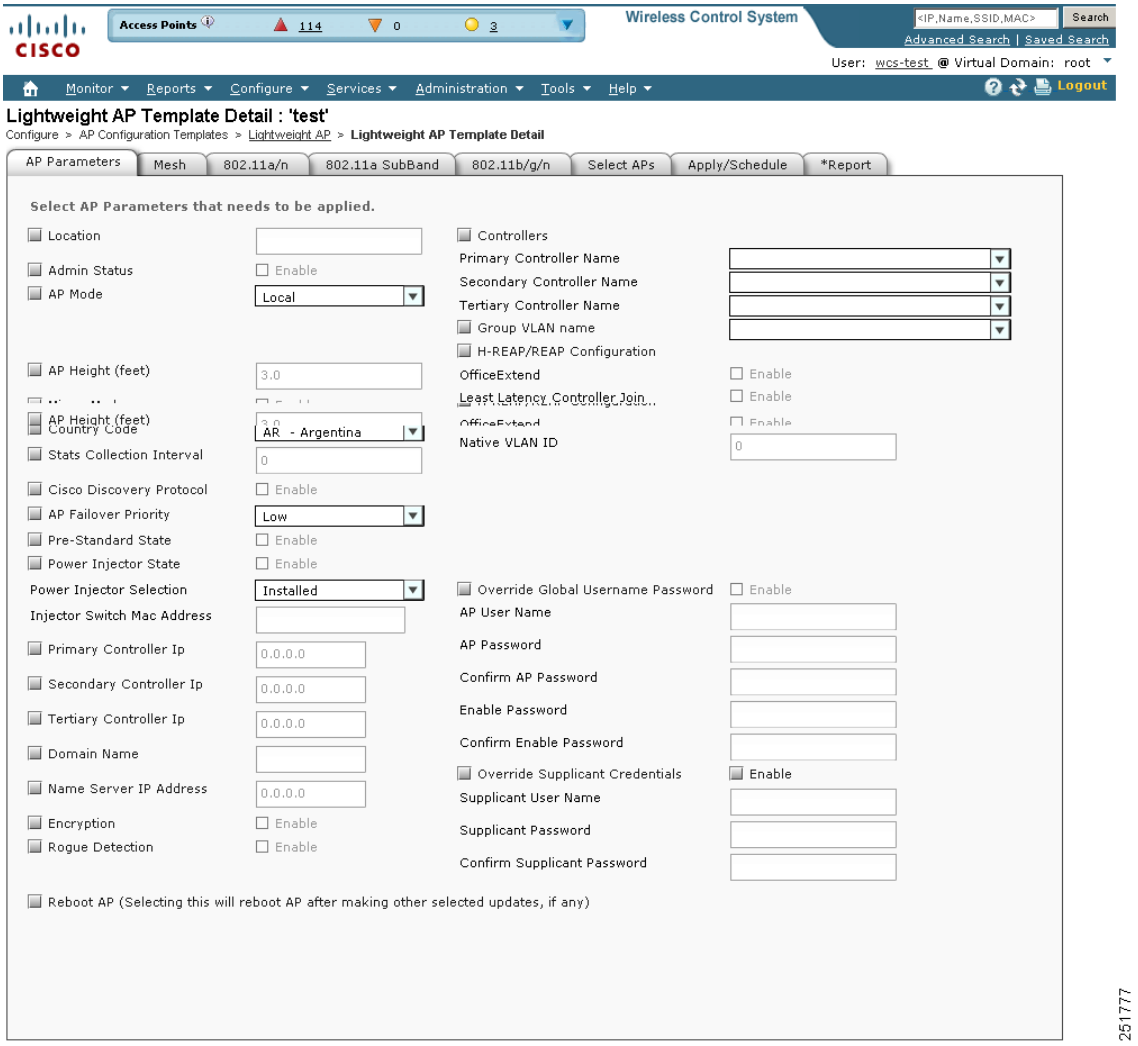
Follow these steps to apply the autonomous access point and lightweight radio templates to all the controllers in a config group.

**Step 1** Choose **Configure > AP Configuration Templates > Lightweight AP** or **Autonomous AP**.

**Step 2** Under Template Name, choose the access point template to which you want to add a schedule.

**Step 3** Click the **Apply/Schedule** tab to access this page (see Figure 12-66).

*Figure 12-66 Apply/Schedule Tab*




**Step 4** Click **Apply** to start the provisioning of access point and radio templates to all the controllers. After you apply, you can leave this page or log out of Cisco WCS. The process continues, and you can return later to this page and view a report.

A report is generated and appears in the Recent Apply Report page. It shows which templates were successfully applied to each of the controllers.

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

**Step 5** 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 6** Enter a starting date in the text box or use the calendar icon to choose a start date.

**Step 7** Choose the starting time using the hours and minutes drop-down lists.

**Step 8** Determine how often you want the provisioning of the template to occur. The choices are no recurrence, hourly, daily, or weekly. You can also specify a certain number of days in the Every ___ Days field.

**Step 9** Click **Schedule** to start the provisioning at the scheduled time.

# Configuring Scheduled Configuration Tasks

The Scheduled Configuration Tasks feature allows you to view, modify, and delete scheduled access point template and configuration group tasks. To access the Scheduled Configuration Tasks page, choose **Configure > Scheduled Configuration Tasks**.

- AP Template Tasks
- Config Group Tasks
- Viewing WLAN Configuration Scheduled Task Results
- Download Software

## AP Template Tasks

The AP Template Tasks page allows you to view, modify, delete, enable, or disable current access point template tasks. To access the AP Template Tasks page and view current access point template tasks, choose **Configure > Scheduled Configuration Tasks**.

- Modifying a Current AP Template Task, page 12-123
- Viewing AP Status Report for the Scheduled Task, page 12-123
- Enabling or Disabling a Current AP Template Task, page 12-124
- Viewing an AP Template Task History, page 12-124
- Deleting a Current AP Template Task, page 12-124

### Modifying a Current AP Template Task

To modify a current access point template task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** Choose the template name of the applicable task.

**Step 3** In the AP Radio/Template page, click the **Apply/Schedule** tab.

**Step 4** Make any necessary changes to the current schedule or AP template parameters and click **Schedule**.

### Viewing AP Status Report for the Scheduled Task

The AP Status Report for the scheduled task includes the following information:

- AP Name—Lists all of the access points included in the scheduled access point template task.
- Ethernet MAC—Indicates the ethernet MAC addresses for the applicable access points.
- Controller—Indicates the associated controller for each of the applicable access points.
- Map—Displays the map location for the applicable access points.

- Status—Indicates whether the access point template has been successfully applied or not. The possible states are not initiated, success, failure, partial failure, and not reachable.
- Task Execution Time—Indicates the execution time of the scheduled task for the applicable access point.

To view the status report for the access points included in the scheduled task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** Choose the AP Status Report for the applicable task.

### Enabling or Disabling a Current AP Template Task

To enable or disable a current access point template task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** Choose the check box of the scheduled task to be enabled or disabled.

**Step 3** From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

**Step 4** Click **Go**.

### Viewing an AP Template Task History

To view previously scheduled task reports, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** Choose the check box of the applicable scheduled task.

**Step 3** From the Select a command drop-down list, choose **View History**.

**Step 4** Click **Go**.

### Deleting a Current AP Template Task

To delete a scheduled access point template task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** Choose the check box of the applicable scheduled task.

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

**Step 4** Click **Go**.

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

# Config Group Tasks

The Config Group Tasks page allows you to view, modify, delete, enable, or disable current configuration group tasks.

A config group allows controllers to spawn across multiple config groups. A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes the controller from the other mobility group if the controller is already a mobility group member.

To access the Config Group Tasks page and view current config group tasks, choose **Configure > Scheduled Configuration Tasks > ConfigGroup**.


- Modifying a Current AP Template Task, page 12-123
- Viewing Controller Status Report for the Scheduled Task, page 12-125
- Enabling or Disabling a Current Config Group Task, page 12-125
- Viewing a Config Group Task History, page 12-126
- Deleting a Current Config Group Task, page 12-126


## Modifying a Current Config Group Task

To modify a current configuration group task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

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

**Step 3** Choose the group name of the applicable task.

**Step 4** In the Config Groups page, click the **Apply/Schedule** tab.

**Step 5** Make any necessary changes to the current schedule and click **Schedule**.

## Viewing Controller Status Report for the Scheduled Task

The Controller Status Report for the scheduled task includes the task execution results of templates applied to the controller.

To view the controller status report, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

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

**Step 3** Choose the Controller Status Report for the applicable task.

## Enabling or Disabling a Current Config Group Task

To enable or disable a current configuration group task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

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

**Step 3** Choose the check box of the scheduled task to be enabled or disabled.

**Step 4** From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

**Step 5** Click **Go**.

### Viewing a Config Group Task History

To view previous scheduled task reports, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

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

**Step 3** Choose the check box of the applicable scheduled task.

**Step 4** From the Select a command drop-down list, choose **View History**.

**Step 5** Click **Go**.

### Deleting a Current Config Group Task

To delete a scheduled configuration group task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

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

**Step 3** Choose the check box of the applicable scheduled tasks.

**Step 4** From the Select a command drop-down list, choose **Delete Task(s)**.

**Step 5** Click **Go**.

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

## Viewing WLAN Configuration Scheduled Task Results

**Note** There is no drop-down command list provided for WLAN Configuration.

To view and manage all scheduled WLAN tasks in WCS, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** From the left sidebar, choose **WLAN Configuration** to open the WLAN Configuration Task List page.

**Step 3** If scheduled configuration tasks are available, the WLAN Configuration Task List page contains the following parameters:

- Schedule Task Name—The user-defined name of the new scheduled task.
- Schedule—Indicates the status of the scheduled task.

- WLAN Status—Indicates the status of the WLAN.
- Controller IP Address—Indicates the IP address of the controller.
- Last Run Time—Indicates the date and time of the most recent scheduled task.
- Next Scheduled Run—Indicates the date and time of the next scheduled task.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.

**Step 4** Select the Task Name link to open the WLAN Schedule Detail page. From this page, you can modify the date and time of the scheduled task. See "Managing WLAN Status Schedules"for more information.

**Step 5** Select the check box of the scheduled task and use the Select a command drop-down list located in the WLAN Configuration Task List page to enable, disable, or delete selected tasks.

- Enable Schedule—Enable the task if its schedule is disabled on the server.
- Disable Schedule—Disable the running scheduled task on the server. Once disabled, the task will not run at the scheduled time. You can re-enable the task at a later time.
- View History—View the execution results for individual WLAN tasks including reasons for any failures.
- Delete Task(s)—Delete the selected task from the WCS server.

# Download Software

By using this feature you can schedule tasks for downloading software to controllers. The Download Software Tasks page allows you to add, delete, view, enable, or disable scheduled download software tasks. To access the Download Software Tasks page and view current download software tasks, choose **Configure > Scheduled Configuration Tasks > Download Software**.

The Download Software Tasks list page displays the following information:

- Task Name—Specifies the template name.
- Image Name—Specifies the image file name.
- Download Type—Specifies the download type.
- Selected Controllers—Specifies the number of controllers that you have selected.
- Schedule Run—Specifies the time at which the task is scheduled to run.
- Reboot Type—Specifies the reboot type.
- Status—Indicates one of the following task statuses:
  - Not initiated—The task is yet to start the download software and will start at the scheduled time. When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.
  - Disabled—The task is disabled and will not run at the scheduled time. This is the default state for a task when it is created without selecting any controllers. When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.
  - Expired—The task did not run at the scheduled time (may be due to the WCS server was down). When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.

- Enabled—The task is yet to start the download software and will start at the scheduled time. When the task is in this state, you can click the Task Name or Selected Controllers link to edit the task.
- In progress—The task is currently downloading the software to the selected controllers. When the task is in this state, you cannot edit it.
- Success—The task has completed the download software to the selected controllers successfully. When the task is in this state, you cannot edit it.
- Failure—The task failed to download software to all the controllers. You can check the detailed status about the failures by using the View Scheduled Run Results command. When the task is in this state, you cannot edit it.
- Partial Success—The task failed to download software to a subset of selected controllers. You can check the detailed status about the failures by using the View Scheduled Run Results command. When the task is in this state, you cannot edit it.

From the Select a command drop-down list, the following functions can be performed:

- Add a Download Software Task
- Modify a Download Software Task
- Select Controllers for Download Software Task
- View Download Software Results
- Delete a Download Software Task
- Enable or Disable a Download Software Task

### Add a Download Software Task

To add a download software task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** From the left sidebar menu, choose **Download Software** to open the Download Software Task List page.

**Step 3** From the Select a command drop-down list, choose **Add Download Software Task**.

**Step 4** Click **Go**. The New Download Software Task page appears.

**Step 5** Configure the following information:

- General
  - Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Schedule Details
  - Download Type—Select the download type. Select the **Download software to controller** check box to schedule download software to controller or select the **Pre-download software to APs** check box to schedule the pre-download software to APs. If you select Download software to controller, specify the image details.

**Note** The pre-download option is displayed only when all selected controllers are using the version 7.0.x.x or later.

**Note** To see Image Predownload status per AP, enable the task in the Administration > Background Task > AP Image Predownload Task page and run an AP Image Predownload report from the Report Launch Pad.

- Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

  **Note** Reboot Type Automatic can be set when only Download software to controller option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Select the time from the hours and minutes drop-down lists.
- Reboot date/time—This option appears only if you select the reboot type as "Scheduled". Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Select the time from the hours and minutes drop-down lists.

**Note** Schedule enough time (at least 30mins) between Download and Reboot so that all APs can complete the software pre-download.

**Note** If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller will not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- Notification (Optional)—Enter the e-mail address of recipient to send notifications via e-mail.

  **Note** To receive email notifications, configure the WCS mail server in the Administration > Settings > Mail Server Configuration page.

- Image Details—Specify the TFTP or FTP Server Information:

**Note** Complete these details if you selected the Download software to controller option under Schedule Details.

TFTP—Specify the TFTP Server Information:

- From the **File is Located on** drop-down list, choose **Local machine** or **TFTP server**.

  **Note** If you choose TFTP server, select the Default Server or add a New server using the Server Name drop-down list.

- Specify the IP address of the TFTP server. This is automatically populated if the default server is selected.
- Specify the local file name or click **Browse** to navigate to the appropriate file.

- If you selected TFTP server previously, specify the File Name.

FTP—Specify the FTP Server Information:

- FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button.
- From the File is Located on parameter, choose **Local machine** or **FTP server**.

**Note** If you choose FTP server, select the Default Server or add a New server using the **Server Name** drop-down list.

- Specify the IP address of the FTP server. This is automatically populated if the default server is selected.
- Specify the local file name or click **Browse** to navigate to the appropriate file.
- If you selected FTP server previously, specify the File Name.

**Step 6** Click **Save**.

## Modify a Download Software Task

To modify a download software task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** From the left sidebar menu, choose **Download Software**.

**Step 3** Select the Task Name link to open the **Download Software Task** page.

**Step 4** Make any necessary changes.

**Note** Any changes in Download Type (Download/Pre-download) or Server Type (FTP/TFTP) for the task in 'Enabled' state will set the task to 'Disabled' state and all the existing controllers will be disassociated from the task.

**Step 5** Click **Save**.

## Select Controllers for Download Software Task

This page lists all the supported controllers that can be selected for the scheduled image download/pre-download task.

To select a controller for scheduled image download, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** From the left sidebar menu, choose **Download Software**.

**Step 3** Click the Controller to open the **Download Software Task** details page.

**Step 4** In the Download Software Task details page, Click **Select Controller** to view the controller list.

**Note** The Select Controllers page can also be accessed from Configure > Scheduled Configuration Tasks > Download Software. Click the hyperlink under the Select Controller column for any download task which is in Enabled, Disabled or in the Expired state.

**Note** If the pre-download option is chosen for the task, then the controllers with software version 7.0.x.x or later only will be listed.

**Note** Controllers with Reachability Status '**Unreachable**' cannot be selected for Download Software Task.

**Step 5** Select the controllers for the scheduled image download task.

**Step 6** Make any necessary changes.

**Step 7** Click **Save**.

### View Download Software Results

To view the Schedule Run Results report, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** From the left sidebar menu, select **Download Software**.

**Step 3** Select the **Task Name** check box.

**Step 4** From the Select a command drop-down list, choose **Schedule Run Results**.

**Step 5** Select the controller for which you want to view the report.

**Step 6** Click **Go**. The Schedule Run Results page provides the information:

- IP Address—The IP address of the controller to which the software to be downloaded.
- Controller Name—Name of the controller.
- Scheduled Run Time—Scheduled time of the download process.
- Last Updated Time—Last update time of the schedule download status (or result).
- Transfer Status—Current download status of the image in controller. For example, Not Initiated, Wrong file Type, Writing the code into flash, Transfer Successful.
- Reboot Status—Reboot status of the controller. For example, NA (if the reboot type is “Manual”), Reboot failed, Reboot Successful.
- Details—Detailed status about the download and reboot process.

### Delete a Download Software Task

To delete a scheduled download software task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** From the left sidebar menu, choose **Download Software**.

**Step 3** Select the check box of the applicable scheduled task.

**Step 4** From the Select a command drop-down list, choose **Delete Download Software Task**.

**Step 5** Click **Go**.

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

### Enable or Disable a Download Software Task

To enable or disable a download software task, follow these steps:

**Step 1** Choose **Configure > Scheduled Configuration Tasks**.

**Step 2** From the left sidebar menu, choose **Download Software**.

**Step 3** Select the check box of the scheduled task to be enabled or disabled.

**Step 4** From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

**Step 5** Click **Go**.

## Configuring Radio Templates

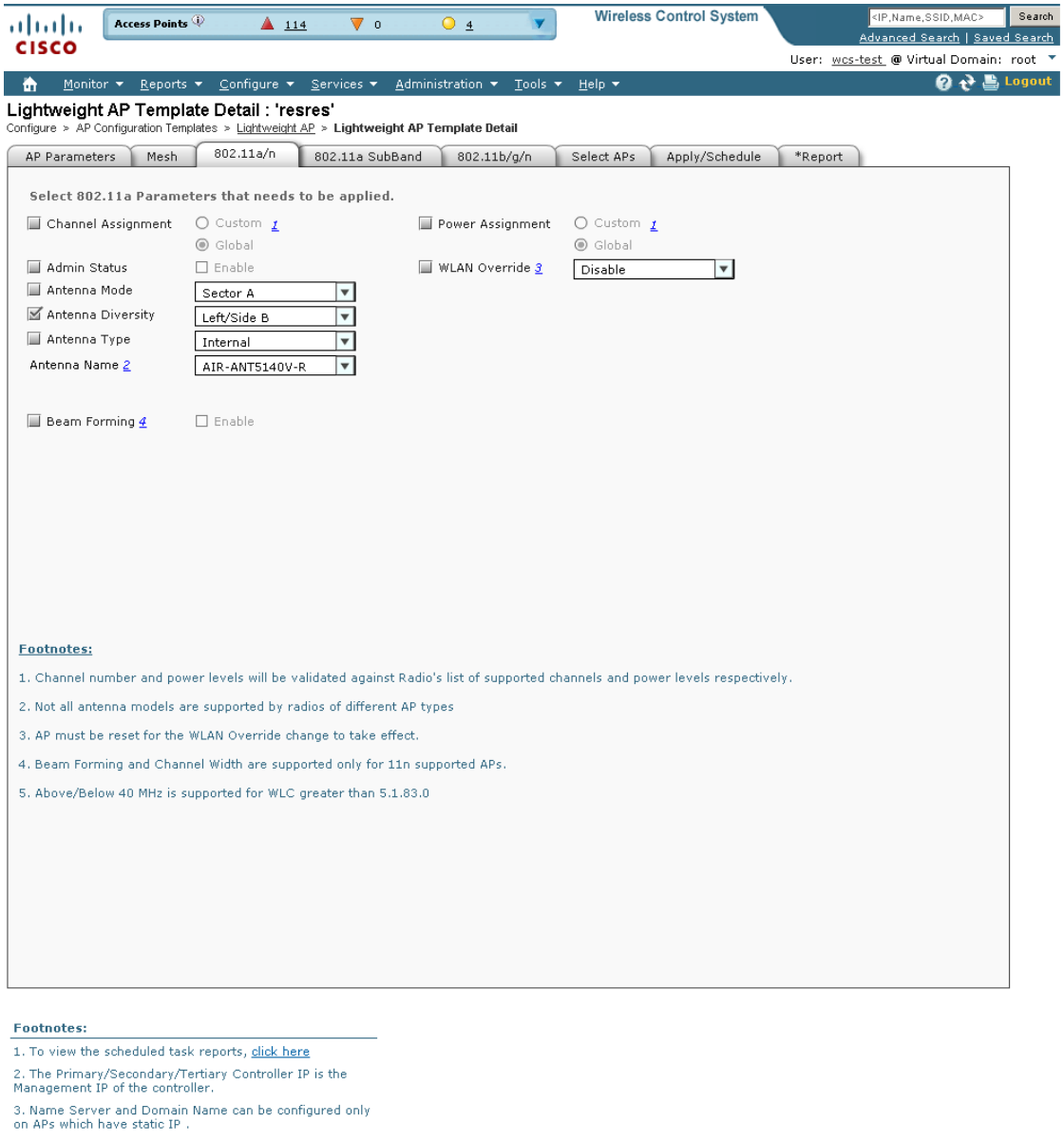
This page allows you to configure a template of radio information that you can apply to one or more access points.

**Step 1** Choose **Configure > AP Configuration Templates > Lightweight AP**.

**Step 2** From the Template Name column, click the template name you want to configure.

**Step 3** Click the **802.11a/n or 802.11b/g/n** tab. The AP/Radio Templates page appears (see Figure 12-67).

*Figure 12-67 802.11a/n Parameters*




**Step 4** Click the Channel Assignment check box to enable it. To choose a specific channel, click **Custom** and use the drop-down to designate the channel number. Otherwise, click **Global**.

**Note** The channel assignment is validated the radio's list of supported channels.

**Step 5** Click both the **Admin Status** and **Enabled** check box to enable access point administrative status.

**Step 6** Use the Antenna Mode drop-down list to choose the antenna model. The choices are omni, sector A, and sector B.

**Note** Not all antenna models are supported by radios of different access point types.

**Step 7** For external antennas, choose one of the following:

- Enabled—Use this setting to enable diversity on both the left and right connectors of the access point.
- Left/Side B—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector.
- Right/Side A—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector.

For internal antennas, choose one of the following:

- Enabled—Use this setting to enable diversity on both Side A and Side B.
- Left/Side B—Use this setting to enable diversity on Side B (rear antenna) only.
- Right/Side A—Use this setting to enable diversity on Side A (front antenna) only.

**Step 8** Click to enable Antenna Type and use the drop-down list to specify if the antenna is external or internal.

**Step 9** Use the Antenna Name drop-down list to determine whether the antenna is a Kodiak directional, AIR-ANT1000, CUSH-S5157WP, etc.

**Step 10** Select the Power Assignment check box and choose the power level currently being used to transmit data. (Some PHYs also use this value to determine the receiver sensitivity requirements.) If you choose Global, the power level is assigned by dynamic algorithm. If you choose Custom, you can select a value using the drop-down list. Power level 1is the maximum.

**Step 11** Enable or disable WLAN override for this access point. When you enable WLAN override, the operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, choose WLANs to enable WLAN operation and deselect WLANs to disallow WLAN operation for this access point 802.11b/g Cisco Radio.

**Note** The access point must be reset for the WLAN override change to take effect.

**Step 12** Enable or disable ClientLink for the access point radios per interface. This feature is only supported for legacy OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

**Note** The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

**Step 13** Select the **CleanAir** check box for controllers whose version is 7.0 (for CleanAir supported APs).

**Step 14** Select the **Enable** check box to enable CleanAir.

# Selecting Access Points

After you have completed the radio template configuration, you must pick the access point to which these attributes are applied. Follow these steps to select access points.

**Step 1** Click the **Select APs** tab.

**Step 2** Use one of the search criterias to choose the access points and click **Search**. For example, you can search for access points that this template was last saved or search by controller name, by floor area, etc. The search criterias change based on the selection you choose.

The AP name, ethernet MAC, controller and map information appears.

**Step 3** Click the check box in the AP Name column and select to which access points you want the access point and radio parameters applied. You can also click the **Select All** or **Unselect All** options.

**Step 4** Click **Save** to save the parameter selection or click **Apply** to save and apply the access point and radio parameters to the selected access points.

## Applying the Report

After access points are selected and applied, click the **Apply Report** tab.