CHAPTER 11

Using Templates

This chapter describes how to add and apply templates. Templates allow you to set fields that you can then apply to multiple devices without having to reenter the common information. This chapter contains the following sections:

Information About Templates

The Controller Template Launch Pad is a hub for all controller templates. 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.

Accessing the Controller Template Launch Pad

To access the Controller Template Launch Pad, choose **Configure > Controller Template Launch Pad**.

The controller template launch pad provides access to all the NCS templates from a single page. From this page, you can view current controller templates or create and save new templates.

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

Adding Controller Templates

To add a new controller template, follow these steps:

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.

> **Note** Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 Provide a description of the template.

Step 5 Click **Save**.

Deleting Controller Templates

To delete a controller template, follow these steps:

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

Step 2 Click the template type to open its template list page.

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

Step 4 From the Select a command drop-down list, choose **Delete Templates**.

Step 5 Click **Go**.

Step 6 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 7 Select the check box of each controller from which you want to remove the template.

Step 8 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

Applying Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

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

Step 2 From the left sidebar menu, choose the category of templates to apply.

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.

Step 5 Select the check box for each controller to which you want to apply the template.

Note To select all controllers, select the check box that appears at the left most corner of the controllers table.

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.

Step 6 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 (or controllers), 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. Select 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 lists the name of each configuration group along with the mobility group name and the number of controllers included.

b. Select 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 7 You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

Note This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

Step 8 Click **Save**.

Note You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose **Apply Templates** from the Select a command drop-down list, and click **Go** to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click **OK**.

Configuring Controller Templates

This section contains the following topics:

Configuring System Templates

This section contains the following topics:

- Configuring a Global CDP Configuration Template, page 11-12
- Configuring DHCP Templates, page 11-14
- Configuring Dynamic Interface Templates, page 11-14
- Configuring Controller System Interface Groups, page 9-42
- Configuring QoS Templates, page 11-17
- Configuring AP Timers Templates, page 11-19
- Configuring a Traffic Stream Metrics QoS Template, page 11-20

Configuring General Templates

To add a general template or make changes to an existing general template, follow these steps:

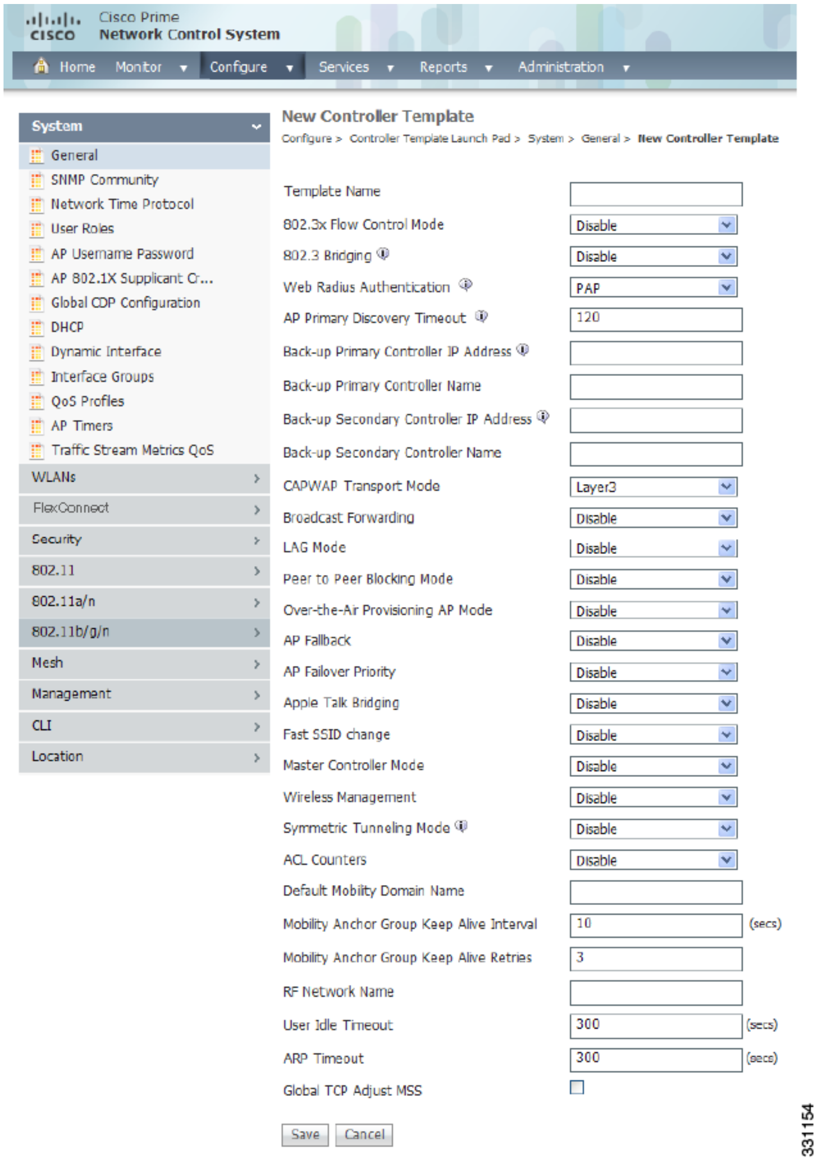
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 11-1).

Figure 11-1 System > General Page



New Controller Template

Configure > Controller Template Launch Pad > System > General > New Controller Template

Template Name	
802.3x Flow Control Mode	Disable
802.3 Bridging	Disable
Web Radius Authentication	PAP
AP Primary Discovery Timeout	120
Back-up Primary Controller IP Address	
Back-up Primary Controller Name	
Back-up Secondary Controller IP Address	
Back-up Secondary Controller Name	
CAPWAP Transport Mode	Layer3
Broadcast Forwarding	Disable
LAG Mode	Disable
Peer to Peer Blocking Mode	Disable
Over-the-Air Provisioning AP Mode	Disable
AP Fallback	Disable
AP Failover Priority	Disable
Apple Talk Bridging	Disable
Fast SSID change	Disable
Master Controller Mode	Disable
Wireless Management	Disable
Symmetric Tunneling Mode	Disable
ACL Counters	Disable
Default Mobility Domain Name	
Mobility Anchor Group Keep Alive Interval	10 (secs)
Mobility Anchor Group Keep Alive Retries	3
RF Network Name	
User Idle Timeout	300 (secs)
ARP Timeout	300 (secs)
Global TCP Adjust MSS	□

Step 3 Use the 802.3x Flow Control Mode drop-down list to enable or disable flow control mode.

Step 4 Use the 802.3x Bridging 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 Web RADIUS Authentication 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 Back-up primary and secondary controller details (controller IP address and controller name).

Step 8 Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the lightweight access point 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 Controllers through Release 5.2 use LWAPP and the new controller release uses CAPWAP.

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

Step 13 From 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 might 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** from the AP Failover Priority drop-down list if you want to allow this capability.

Step 15 Choose to enable or disable AppleTalk bridging.

Note This AppleTalk 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 might want to 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 Forwarding (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 ACL Counters 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 your mouse cursor over the field, the valid range of values appear.

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** check box 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 browser of the client; all web traffic going out from the client is destined for 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 SNMP Community Controller Templates

Create or modify a template for configuring SNMP communities on controllers. Communities can have read-only or read-write privileges using SNMP v1, v2, or v3.

To add a new template with SNMP community information for a controller, follow these steps:

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

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

Step 3 Configure the following fields:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Community Name
- Confirm Community Name—Retype the community name.
- IP Address—The IP address of the server.
- Netmask
- Access Mode—Choose **Read Only** or **Read Write** from the drop-down list.
  - Read Only—Cannot be edited.
  - Read Write—Can be edited.
- Admin Status—Select the check box to enable this template and also to enable the Update Discover Community option.
- Update Discover Community—Select the check box to update the SNMP version as v2. This updates the Read/Write Community as the template community name for the applied controllers.

Note If the Access Mode option is configured as Read Only, then the NCS has only read access to the controller after applying this template.

Step 4 Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 11-2 for more information.

Note If a template is applied successfully and the Update Discover Community option is enabled, then the applied community name is updated in the NCS database for that applied controller. Also, the NCS uses that community name for further communication with that controller.

Configuring an NTP Server Template

Note NTP is used to synchronize computer clocks on the Internet.

To add an NTP template or make modifications to an existing NTP template, follow these steps:

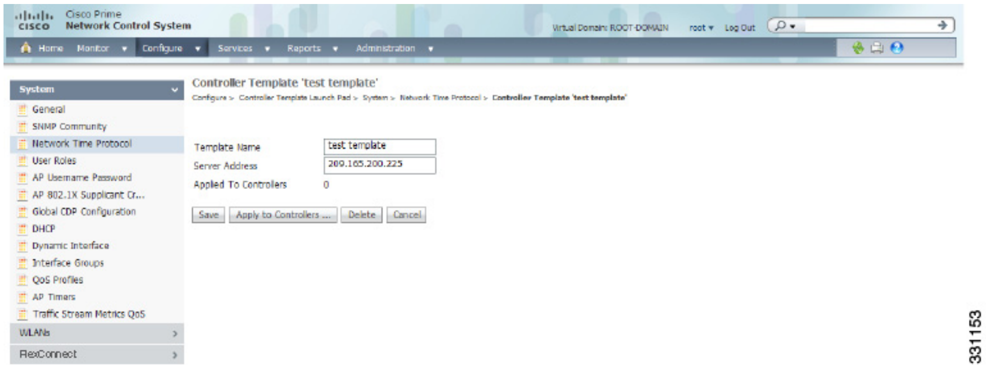
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-2).

Figure 11-2 NTP Servers Template



Controller Template 'test template'

Configure > Controller Template Launch Pad > System > Network Time Protocol > Controller Template 'test template'

Template Name: test template
Server Address: 209.165.200.225
Applied To Controllers: 0

Step 4 Enter the NTP server IP address.

Step 5 Click **Save**.

Configuring User Roles Controller Templates

This section describes how to create or modify a template for configuring user roles. User roles determine how much bandwidth the network can use. Four QoS levels (Platinum, Bronze, Gold, and Silver) are available for the bandwidth distribution to Guest Users. Guest Users are associated with predefined roles (Contractor, Customer, Partner, Vendor, Visitor, Other) with respective bandwidth configured by the Admin. These roles can be applied when adding a new Guest User. See the "Configuring a Guest User Template" section on page 11-59 for more information on adding Guest Users.

To add a new template with User Roles information for a controller, follow these steps:

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

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

Step 3 Configure the following fields:

- Role Name
- Average Data Rate—The average data rate for non-UDP (User Datagram Protocol) 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 4 Click **Save**. Once saved, the template displays in the Template List page. From the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 11-2 for more information.

Configuring AP Username Password Controller Templates

Create or modify a template for setting an access point username and password. All access points inherit the password as they join the controller and these credentials are used to log into the access point via the console or Telnet/SSH.

Note See the "Configuring a Global Access Point Password" section on page 9-60 for more information regarding global passwords.

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis. See the "Configuring AP Configuration Templates" section on page 11-136 to see where the global password is displayed and how it can be overridden on a per-access point basis.

Also, in controller software Release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To add a new template with AP Username Password information for a controller, follow these steps:

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

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

Step 3 Configure the following fields:

- AP Username—Type the username that you want to be inherited by all access point that join the controller.
- AP Password—Type the password that you want to be inherited by all access point that join the controller.
- Confirm Password—Retype the access point password.
- Enable Password

Note For Cisco IOS access points, you must also enter and confirm an enable password.

- Confirm Enable Password

Step 4 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 the "Applying Controller Templates" section on page 11-2 for more information.

Note See the "Configuring a Global Access Point Password" section on page 9-60 for more information regarding global passwords.

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.

To add or modify an existing AP 802.1X Supplicant Credentials template, follow these steps:

Note If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See the "Configuring Access Points" section on page 9-161 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 fields.

Step 4 Click **Save**.

Configuring a Global CDP Configuration Template

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the Ethernet and radio ports of the bridge by default.

To configure a Global CDP Configuration template, follow these steps:

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

Step 2 Click **Global CDP Configuration** or choose **System > Global CDP Configuration** from the left sidebar menu. The Global CDP Configuration Templates page displays all currently saved Global CDP Configuration templates.

Step 3 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 Global CDP Configuration template page appears.

Step 4 Enter the new CDP template name.

Step 5 In the Global CDP group box of the page, configure the following fields:

- CDP on controller—Choose enable or disable CDP on the controller.

  Note This configuration cannot be applied on WiSM2 controllers.

- Global CDP on APs—Choose to enable or disable CDP on the access points.
- Refresh-time Interval (seconds)—At the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.
- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 6 In the CDP for Ethernet Interfaces group box of the page, select the slots of Ethernet interfaces for which you want to enable CDP.

Note CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7 In the CDP for Radio Interfaces group box of the page, select the slots of Radio interfaces for which you want to enable CDP.

Note CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 8 Click **Save**.

Note The Global Interface CDP configuration is applied only to the APs for which the CDP is enabled at AP level.

Configuring DHCP Templates

To add a DHCP template or make modifications to an existing DHCP template, follow these steps:

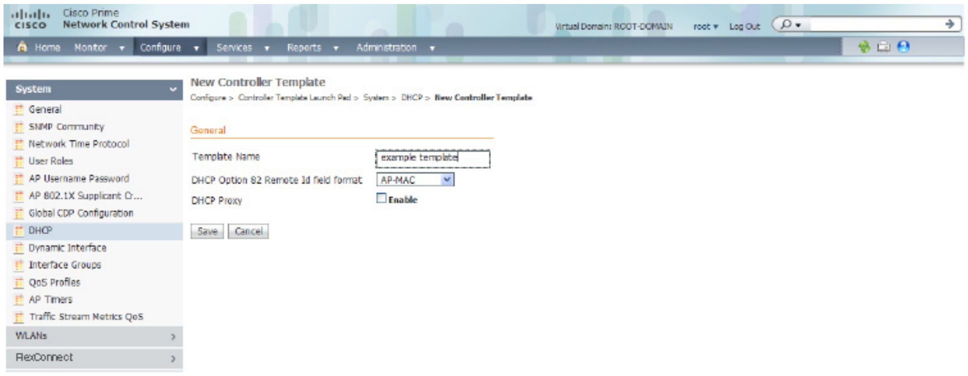
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-3).

Figure 11-3 DHCP Template Page



New Controller Template

Configure > Controller Template Launch Pad > System > DHCP > **New Controller Template**

General

Template Name: example template

DHCP Option 82 Remote Id field format: AP-MAC

DHCP Proxy: ☐ Enable

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 Enter the DHCP Timeou,t in seconds, after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds.

Note DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6 Click **Save**.

Configuring Dynamic Interface Templates

To add a dynamic interface template or make modifications to an existing interface configuration, follow these steps:

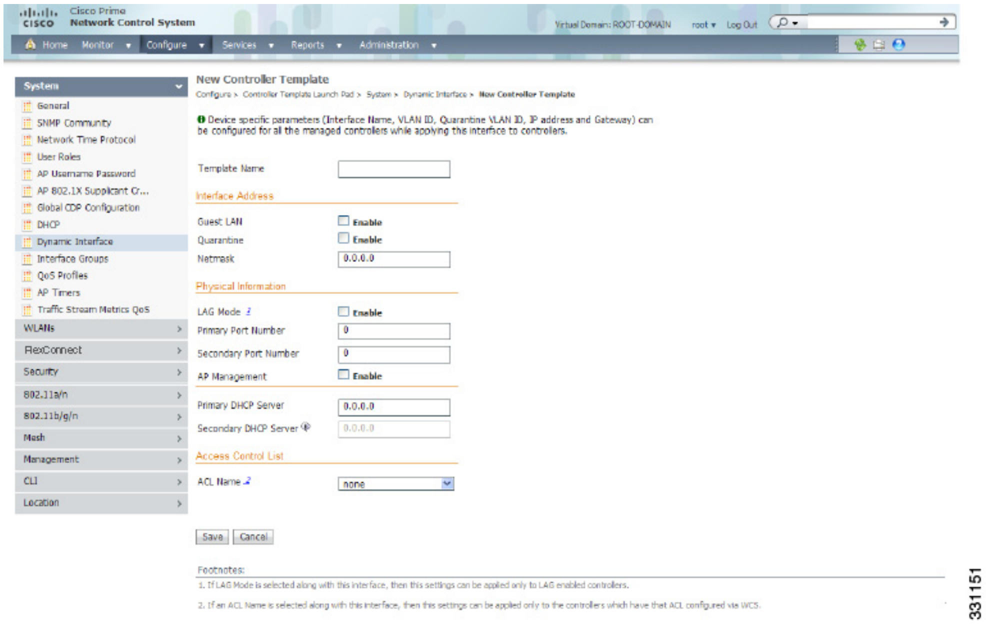
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-4).

Figure 11-4 Dynamic Interface Template



New Controller Template

Configure > Controller Template Launch Pad > System > Dynamic Interface > **New Controller Template**

Device specific parameters (Interface Name, VLAN ID, Quarantine VLAN ID, IP address and Gateway) can be configured for all the managed controllers while applying this interface to controllers.

Template Name

Interface Address

Guest LAN □ Enable

Quarantine □ Enable

Netmask 0.0.0.0

Physical Information

LAG Mode [1] □ Enable

Primary Port Number 0

Secondary Port Number 0

AP Management □ Enable

Primary DHCP Server 0.0.0.0

Secondary DHCP Server 0.0.0.0

Access Control List

ACL Name [2] none

Footnotes:

1. If LAG Mode is selected along with this interface, then this settings can be applied only to LAG enabled controllers.

2. If an ACL Name is selected along with this interface, then this settings can be applied only to the controllers which have that ACL configured via WCS.

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 the port 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 group box, choose either **Device Info** or **File**. If you choose device info, you must configure the device-specific fields for each controller. If you choose File, you must configure CSV device-specific fields (Interface Name, VLAN Identifier, Quarantine VLAN Identifier, IP Address, and Gateway) for all the managed controllers specified in the CSV file (see Table 11-1). If you choose Device Info, continue to Step 12.

The sample CSV files are as follows.

Table 11-1 Sample CSV Files

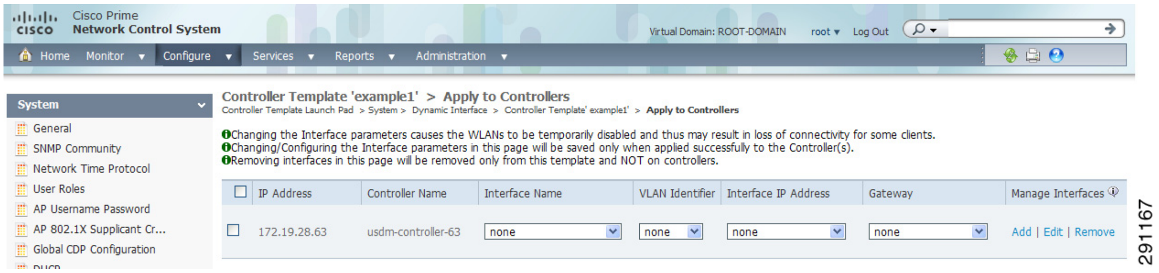
ip_address	interface_name	vlan_id	quarantine_ vlan_id	interface_ ip_address	gateway
209.165.200.224	dyn-1	1	2	209.165.200.228	209.165.200.229
209.165.200.225	interface-1	4	2	209.165.200.230	209.165.200.231
209.165.200.226	interface-2	5	3	209.165.200.232	209.165.200.233
209.165.200.227	dyna-2	2	3	209.165.200.234	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 fields for each controller (see Figure 11-5).

Figure 11-5 Apply To Page



Controller Template 'example1' > Apply to Controllers

Controller Template Launch Pad > System > Dynamic Interface > Controller Template' example1' > **Apply to Controllers**

Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.
Changing/Configuring the Interface parameters in this page will be saved only when applied successfully to the Controller(s).
Removing interfaces in this page will be removed only from this template and NOT on controllers.

☐	IP Address	Controller Name	Interface Name	VLAN Identifier	Interface IP Address	Gateway	Manage Interfaces
☐	172.19.28.63	usdm-controller-63	none ▾	none ▾	none ▾	none ▾	Add | Edit | Remove

Step 13 Use the **Add** and **Remove** options to configure device specific fields 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 fields, the WLANs are temporarily disabled, therefore you might lose connectivity for some clients. Any changes to the interface fields 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.

Applying a Dynamic Interface Template to Controllers

To apply a Dynamic Interface template to a controller, follow these steps:

Step 1 In the Dynamic Interface controller template page, click **Apply to Controllers**.

Step 2 Use the Manage Interfaces options to configure device-specific fields:

- Add—Click **Add** to open the Add Interface dialog box. Enter an interface name, VLAN identifier, IP address, and gateway. When all fields are entered, click **Done**.
- Edit—Click **Edit** to make changes to current interfaces.
- Remove—Click **Remove** to delete a current interface.

Step 3 Select a check box for each controller to which you want to apply this template.

Step 4 Click **Apply**.

Note Changing the Interface fields causes the WLANs to be temporarily disabled and might result in loss of connectivity for some clients.

Note Interface field changes or configurations made on this page are saved only when applied successfully to the controller(s).

Note Interfaces removed from this page are removed only from this template and not from controllers.

Note See the "Configuring Dynamic Interface Templates" section on page 11-14 for more information on Dynamic Interface controller templates.

Configuring QoS Templates

To modify the quality of service (QoS) profiles, follow these steps:

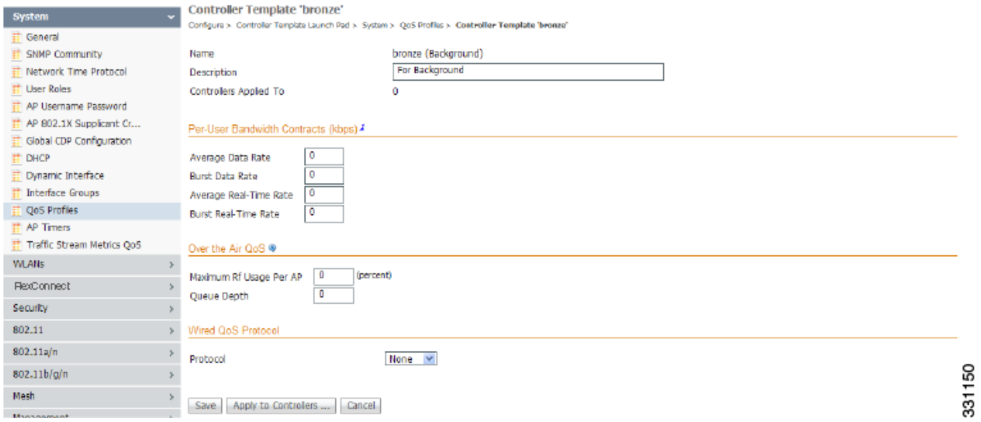
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **QoS Profiles** or choose **System > QoS Profiles** 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 11-6).

Figure 11-6 Edit QoS Profile Template Page



Controller Template 'bronze'

Configure > Controller Template Launch Pad > System > QoS Profiles > **Controller Template 'bronze'**

Name bronze (Background)

Description For Background

Controllers Applied To 0

Per-User Bandwidth Contracts (kbps)

Average Data Rate 0

Burst Data Rate 0

Average Real-Time Rate 0

Burst Real-Time Rate 0

Over the Air QoS

Maximum Rf Usage Per AP 0 (percent)

Queue Depth 0

Wired QoS Protocol

Protocol None

Step 4 Set the following values in the Per-User Bandwidth Contracts group box. 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 in the Over-the-Air QoS group box.

- 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.

Note The Air QoS configurations are applicable for controller Release 7.0 and earlier.

Step 6 Set the following values in the Wired QoS Protocol group box.

- 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 Templates

Some advanced timer configuration for FlexConnect and local mode is available for the controller on the NCS.

To configure a template for AP timers, follow these steps:

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.

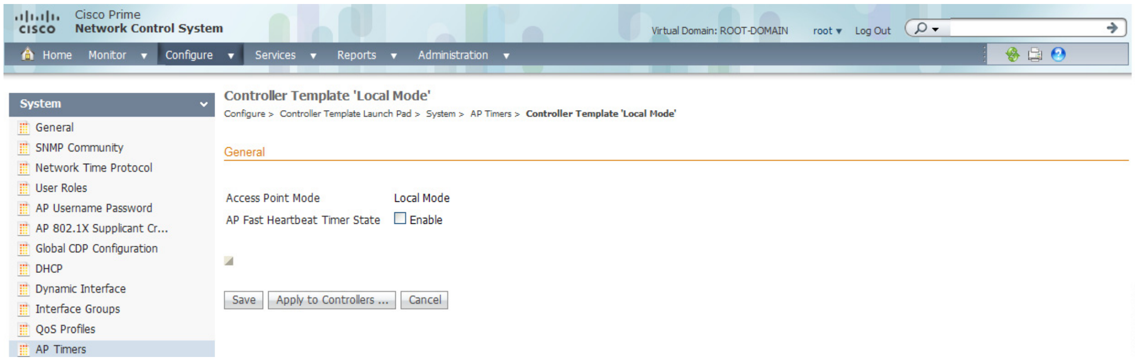
The values in the Access Point Mode column are links. When you click a link, the Controller Template *access point mode* page appears. The Access Point Mode is automatically populated (see Figure 11-7).

Step 3 Select the **AP Fast Heartbeat Timer State** check box to enable AP Fast Heartbeat Timeout.

Step 4 Enter an AP Fast Heartbeat Timeout value. The valid range is 1 to 15 seconds. The default is 10 seconds. The recommended timeout values are:

- 10 to 15 seconds for 7500 series controllers.
- 10 to 15 seconds for 5500 series controllers Release 7.0.98.0 and earlier.
- 1 to 10 seconds for 5500 series controllers Release 7.0.98.0 and later.
- 1 to10 seconds for other controllers.

Figure 11-7 AP Timers Page



Controller Template 'Local Mode'

Configure > Controller Template Launch Pad > System > AP Timers > **Controller Template 'Local Mode'**

General

Access Point Mode Local Mode

AP Fast Heartbeat Timer State □ Enable

Step 5 Click **Save**.

Configuring an Interface Group Template

The interface group template page allows you to select list of interfaces and form a group.

Note You cannot create interfaces using this page.

To configure an interface group template, follow these steps:

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

Step 2 Click **Interface Groups** or choose **System > Interface Groups** from the left sidebar menu. The System > Interface Groups page appears.

Step 3 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 New Controller template page appears.

Step 4 Specify the following details:

- Name—Interface Group name.
- Description(optional)—A more detailed description of the interface group.
- Quarantine—Indicates the type of interfaces that can be added to an interface group. If this option is enabled, you can add interfaces with quarantine VLAN ID set. If this options is disabled, you can add interfaces with quarantine VLAN ID not set.

Step 5 Selected Controllers/Interfaces that you want to add to the group.

Step 6 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. The NCS 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.

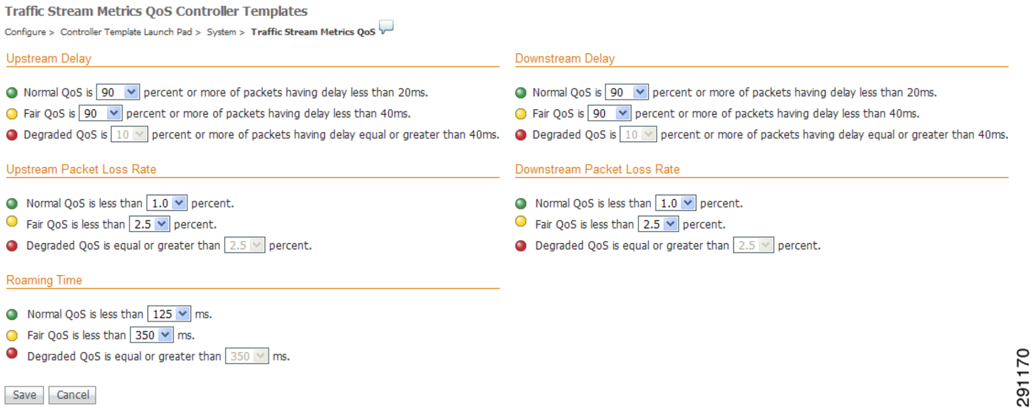
For the access points to collect measurement values, traffic stream metrics must be enabled on the controller.

To configure a Traffic Stream Metrics QoS template, follow these steps:

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 Traffic Stream Metrics QoS Controller Templates page appears (see Figure 11-8).

Figure 11-8 Traffic Stream Metrics QoS Status Template



Traffic Stream Metrics QoS Controller Templates

Configure > Controller Template Launch Pad > System > **Traffic Stream Metrics QoS**

Upstream Delay

- ● Normal QoS is 90 percent or more of packets having delay less than 20ms.
- ● Fair QoS is 90 percent or more of packets having delay less than 40ms.
- ● Degraded QoS is 10 percent or more of packets having delay equal or greater than 40ms.

Upstream Packet Loss Rate

- ● Normal QoS is less than 1.0 percent.
- ● Fair QoS is less than 2.5 percent.
- ● Degraded QoS is equal or greater than 2.5 percent.

Roaming Time

- ● Normal QoS is less than 125 ms.
- ● Fair QoS is less than 350 ms.
- ● Degraded QoS is equal or greater than 350 ms.

Downstream Delay

- ● Normal QoS is 90 percent or more of packets having delay less than 20ms.
- ● Fair QoS is 90 percent or more of packets having delay less than 40ms.
- ● Degraded QoS is 10 percent or more of packets having delay equal or greater than 40ms.

Downstream Packet Loss Rate

- ● Normal QoS is less than 1.0 percent.
- ● Fair QoS is less than 2.5 percent.
- ● Degraded QoS is equal or greater than 2.5 percent.

The Traffic Stream Metrics QoS Controller 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 are mobile-to-mobile; therefore, some have less stringent PLR requirements for the wireless LAN.

Configuring WLAN Templates

This section contains the following topics:

- Configuring WLAN Templates, page 11-22

- Configuring WLAN AP Groups Templates, page 11-38

Configuring WLAN Templates

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

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.
- FlexConnect access points do not support multiple SSIDs.

To add a WLAN template or make modifications to an existing WLAN template, follow these steps:

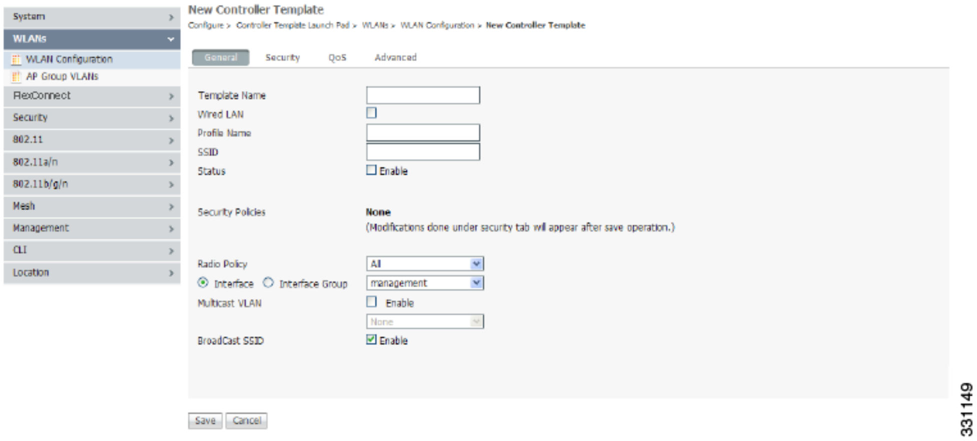
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **WLAN** or choose **WLANs > WLAN Configuration** 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 in the WLAN Template General page:

- Template Name—The user-defined name of the template. Clicking the name displays fields 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, choose **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 11-9).

Figure 11-9 WLAN Template



New Controller Template

Configure > Controller Template Launch Pad > WLANs > WLAN Configuration > **New Controller Template**

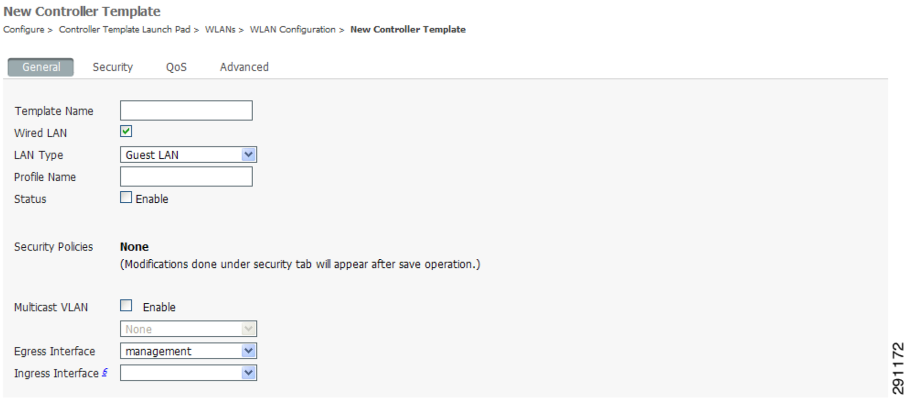
Template Name
Wired LAN □
Profile Name
SSID
Status □ Enable

Security Policies **None**
(Modifications done under security tab will appear after save operation.)

Radio Policy All
● Interface ○ Interface Group management
Multicast VLAN □ Enable
None
BroadCast SSID ☑ Enable

Step 4 Select the **Wired LAN** check box to indicate whether or not this WLAN is a wired LAN.

Figure 11-10 WLAN Template



New Controller Template

Configure > Controller Template Launch Pad > WLANs > WLAN Configuration > **New Controller Template**

Template Name
Wired LAN ☑
LAN Type Guest LAN
Profile Name
Status □ Enable

Security Policies **None**
(Modifications done under security tab will appear after save operation.)

Multicast VLAN □ Enable
None
Egress Interface management
Ingress Interface

Note Specify if you want guest 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).

Note The Egress or Ingress interface configurations are applicable for Wired LAN only.

Step 5 Use the **Type** drop-down list to select the type of the wired LAN.

- Guest LAN—Indicates that this wired LAN is a Guest LAN.

  Note If you selected the Guest LAN option, you need to select an Ingress interface which has not already been assigned to any Guest LAN.

- Remote LAN—Indicates that this wired LAN is a Remote LAN.

Step 6 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 7 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 8 Select the **Enable** check box for the Status field.

Step 9 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 10 Use the Interface/Interface Group drop-down list to choose the available names of interfaces created by the Controller > Interfaces module.

Step 11 From the Egress Interface drop-down list, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 9-49. This provides a path out of the controller for wired guest client traffic.

Step 12 From the Ingress Interface drop-down list, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 9-49. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 13 Select the **Enable** check box to enable the multicast VLAN feature.

Step 14 From the Multicast VLAN Interface drop-down list, choose the appropriate interface name. This list is automatically populated when you enable the multicast VLAN feature.

Step 15 Click **Broadcast SSID** to activate SSID broadcasts for this WLAN.

Step 16 Click **Save**.

Step 17 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 Tab" section on page 11-24.
- Click the **QoS** tab to establish which quality of service is expected for this WLAN. Continue to the "QoS Tab" section on page 11-32.
- Click the **Advanced** tab to configure any other details about the WLAN, such as DHCP assignments and management frame protection. Continue to the "Advanced Tab" section on page 11-33.

Security Tab

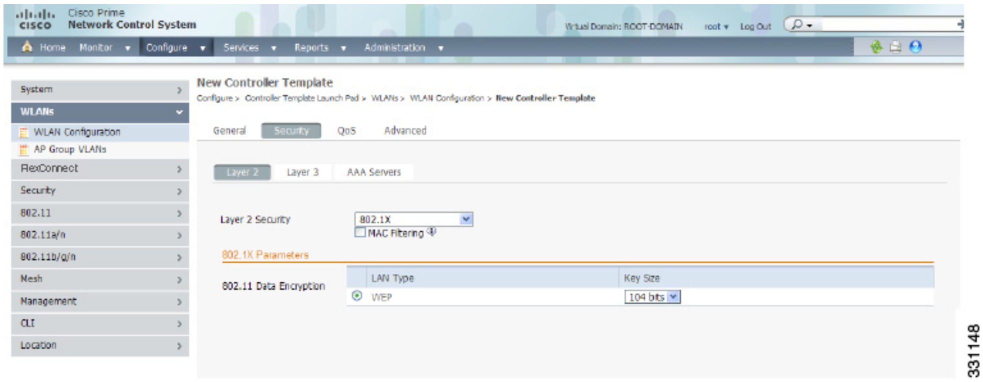
After choosing Security, you have an additional three tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2 Tab

When you click the Layer 2 tab, the Layer 2 tab appears (see Figure 11-11).

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

Figure 11-11 Layer 2 Tab



Layer 2 Security: 802.1X

□ MAC Filtering

802.1X Parameters

802.11 Data Encryption	LAN Type	Key Size
	● WEP	104 bits

To configure the Layer 2 tab, follow these steps:

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 Table 11-2.

Table 11-2 Layer 2 Security Options

Field	**Description**
None	No Layer 2 security selected. • FT Enable—Select the check box to enable Fast Transition (FT) between access points. **Note** Fast transition is not supported with FlexConnect mode. – Over the DS—Select the check box to enable or disable the fast transition over a distributed system. – Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100. **Note** To enable Over the DS or Reassociation Timeout, you must enable fast transition.
802.1X	WEP 802.1X data encryption type (Note 1): 40/64 bit key. 104 bit key. 152 bit key.

Table 11-2 Layer 2 Security Options (continued)

Field	Description
Static WEP	Static WEP encryption fields: Key sizes: Not set, 40/64, 104, and 152 bit key sizes. Key Index: 1 to 4 (Note 2). Encryption Key: Encryption key required. Key Format: ASCII or HEX. Allowed Shared Key Authentication—Select the check box to enable shared key authentication. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). 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 fields are displayed at the bottom of the page. Static WEP encryption fields: Key sizes: Not set, 40/64, 104, and 152 bit key sizes. Key index: 1 to 4 (Note 2). Encryption Key: Enter encryption key. Key Format: ASCII or HEX. Allowed Shared Key Authentication—Select the check box to enable. 802.1 Data Encryption: 40/64 bit key, 104 bit key, 152 bit key.

Table 11-2 Layer 2 Security Options (continued)

Field	Description
WPA+WPA2	Use this setting to enable WPA, WPA2, or both. 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. When WPA+WPA2 is selected as the Layer 2 security policy and preshared key is enabled, neither CCKM nor 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time. • Mac Filtering—Enables MAC address filtering. **Note** Mac Filtering and Max-Clients are not supported with FlexConnect local authentication. • FT Enable—Select the check box to enable fast transition between access points. **Note** Fast transition is not supported with FlexConnect mode. – Over the DS—Select the check box to enable the fast transition over a distributed system. – Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100. **Note** To enable Over the DS or Reassociation Timeout, enable fast transition. WPA+WPA2 parameters: • WPA1—Select the check box to enable WPA1. • WPA2—Select the check box to enable WPA2. Authentication Key Management: • FT802.1X—Select the check box to enable FT802.1X. • 802.1X—Select the check box to enable 802.1X. • CCKM—Select the check box to enable CCKM. • PSK—Select the check box to enable PSK. • FTPSK—Select the check box to enable FTPSK. **Note** Enable WPA2 and fast transition to set FT802.1X or FTPSK.

Table 11-2 Layer 2 Security Options (continued)

Field	Description
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. **Note** CKIP is not supported on 10xx APs. When selected, these CKIP fields are displayed. Key size: Not set, 40, or 104. Key Index: 1 to 4 Encryption Key: Specify encryption key. Key Format: ASCII or HEX. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). 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. MMH Mode: Select the check box to enable. Key Permutation: Select the check box to enable.

Step 2 Select 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 might 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 the NCS). 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.

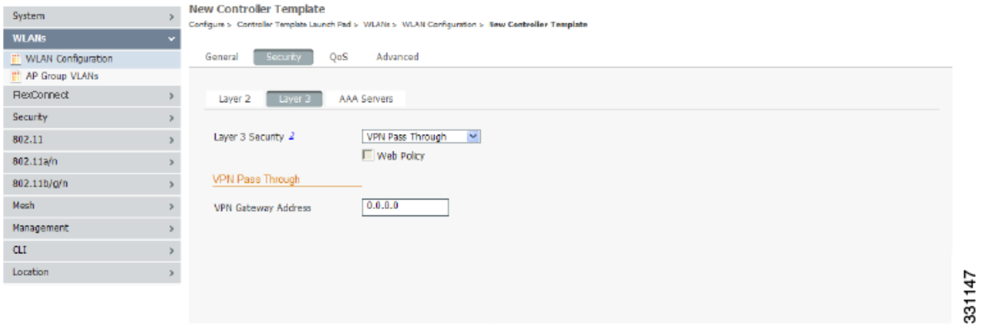
Step 4 Click **Save**.

Layer 3 Tab

When you click the Layer 3 tab, the Layer 3 tab appears (see Figure 11-12).

Note The tab contains different views depending on the option you chose from the Layer 3 Security drop-down list.

Figure 11-12 Layer 3 Tab



New Controller Template

Configure > Controller Template Launch Pad > WLANs > WLAN Configuration > New Controller Template

Layer 3 Security: VPN Pass Through

□ Web Policy

VPN Pass Through

VPN Gateway Address: 0.0.0.0

To configure the Layer 3 tab, follow these steps:

Step 1 Use the Layer 3 security drop-down list to choose between None and VPN Pass Through. The page fields 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, select the **Web Policy** check box and choose the Passthrough option from the drop-down list. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b. Choose the **WebAuth on MAC Filter Failure** option so that when clients fail on MAC filter, they are automatically switched to webAuth.

Note The WebAuth on Mac Filter Failure option works only when the Layer 2 Mac Filtering option is enabled.

c. 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, see the "Downloading Customized Web Authentication" section on page 3-42.

   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, choose **Security > AAA**, and choose up to three RADIUS and LDAP servers using the drop-down lists.

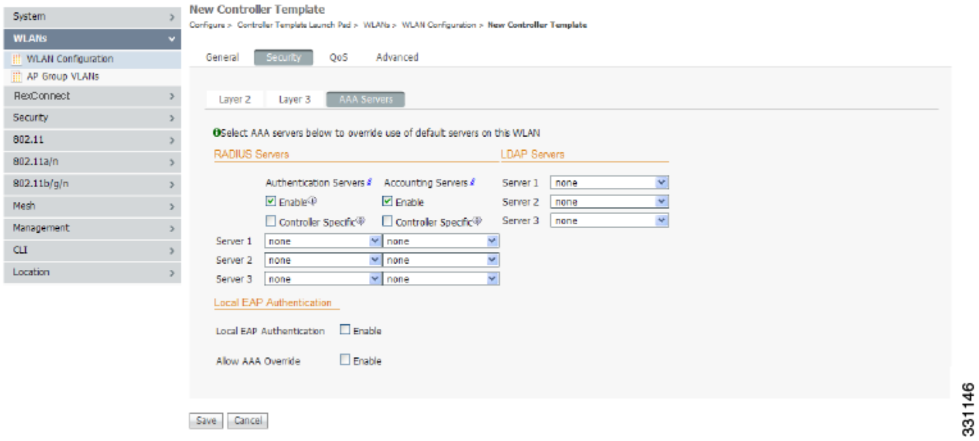
Step 4 Click **Save**.

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

AAA Servers

When you click the AAA Servers tab, the AAA Servers tab appears (see Figure 11-13).

Figure 11-13 AAA Servers Tab



Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

	Authentication Servers	Accounting Servers
	☑ Enable	☑ Enable
	□ Controller Specific	□ Controller Specific
Server 1	none	none
Server 2	none	none
Server 3	none	none

LDAP Servers

Server 1	none
Server 2	none
Server 3	none

Local EAP Authentication

Local EAP Authentication □ Enable

Allow AAA Override □ Enable

To configure the AAA Servers tab, follow these steps:

Step 1 Select the **Radius Server Overwrite Interface** check box to send the client authentication request through the dynamic interface which is set on the WLAN. When you enable the Radius Server Overwrite Interface option, the WLC sources all radius traffic for a WLAN using the dynamic interface configured on that WLAN.

Note You cannot enable Radius Server Overwrite Interface when Diagnostic Channel is enabled.

Note The Radius Server Overwrite Interface option is supported in controller Release 7.0.x and later.

Step 2 Select the **Enable** check boxes, then 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, the NCS uses the default LDAP server order from the database.

Step 3 Select the **Interim Update** check box if you want to enable interim update for RADIUS Server Accounting. If you have selected this check box, specify the Interim Interval value. The range is 180 to 3600 seconds, and the default value is 0.

Note The Interim Interval can be entered only when Interim Update is enabled.

Step 4 Select 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 5 When AAA Override is enabled, and a client has conflicting AAA and controller WLAN authentication fields, 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.

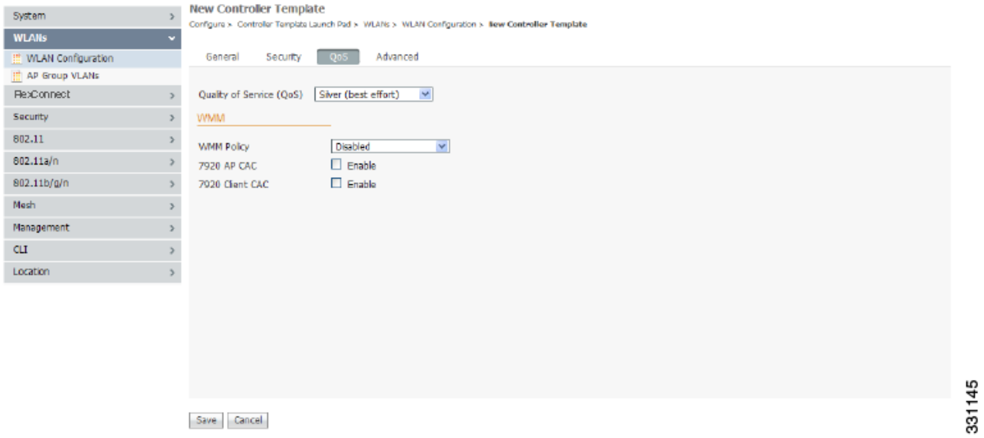
The AAA override values might come from a RADIUS server, for example.

Step 6 Click **Save**.

QoS Tab

When you click the QoS tab in the WLAN Template page, the QoS tab appears (see Figure 11-14).

Figure 11-14 QoS Tab



New Controller Template

Configure > Controller Template Launch Pad > WLANs > WLAN Configuration > New Controller Template

Quality of Service (QoS) Silver (best effort)

WMM

WMM Policy Disabled

7920 AP CAC □ Enable

7920 Client CAC □ Enable

To configure the QoS fields, follow these steps:

Step 1 From the QoS drop-down list, 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 From the WMM Policy drop-down list, 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 Select the **7920 AP CAC** check box if you want to enable support on Cisco 7920 phones.

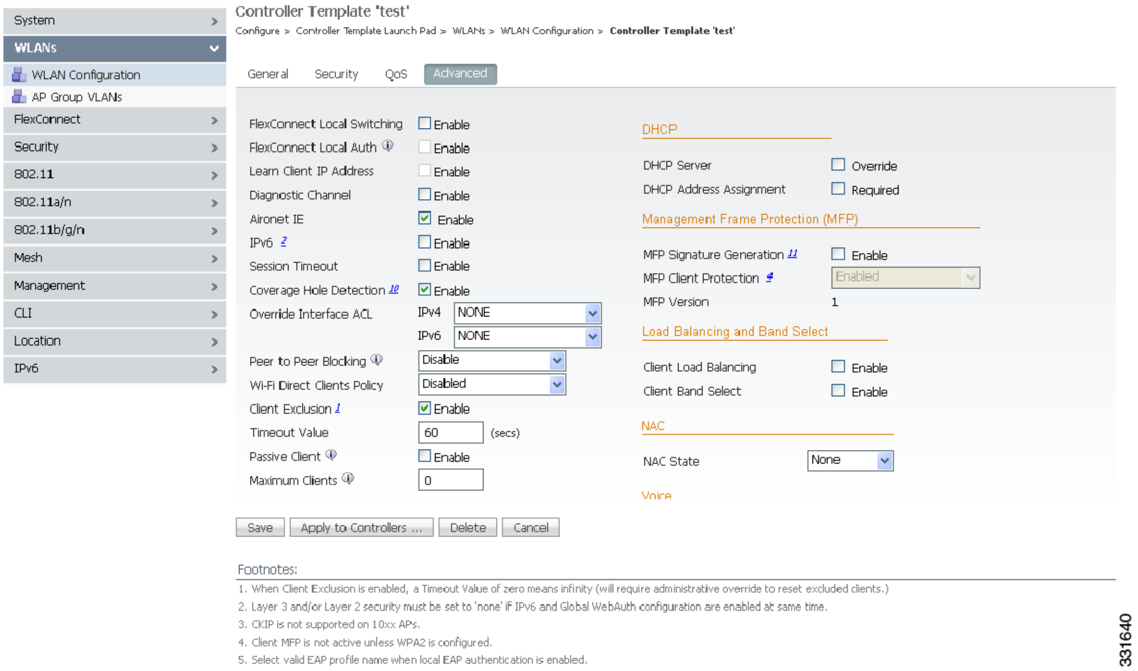
Step 4 If you want WLAN to support older versions of the software on 7920 phones, select the **7920 Client CAC** check box to enable it. The CAC limit is set on the access point for newer versions of software.

Step 5 Click **Save**.

Advanced Tab

When you click the Advanced tab in the WLAN Template page, the Advanced tab appears (see Figure 11-15).

Figure 11-15 Advanced Tab



Controller Template 'test'

Configure > Controller Template Launch Pad > WLANs > WLAN Configuration > **Controller Template 'test'**

FlexConnect Local Switching □ Enable
FlexConnect Local Auth □ Enable
Learn Client IP Address □ Enable
Diagnostic Channel □ Enable
Aironet IE ☑ Enable
IPv6 [2] □ Enable
Session Timeout □ Enable
Coverage Hole Detection [10] ☑ Enable
Override Interface ACL IPv4 NONE
IPv6 NONE
Peer to Peer Blocking Disable
Wi-Fi Direct Clients Policy Disabled
Client Exclusion [1] ☑ Enable
Timeout Value 60 (secs)
Passive Client □ Enable
Maximum Clients 0

DHCP
DHCP Server □ Override
DHCP Address Assignment □ Required

Management Frame Protection (MFP)
MFP Signature Generation [11] □ Enable
MFP Client Protection [4] Enabled
MFP Version 1

Load Balancing and Band Select
Client Load Balancing □ Enable
Client Band Select □ Enable

NAC
NAC State None

Voice

Footnotes:
1. When Client Exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients.)
2. Layer 3 and/or Layer 2 security must be set to 'none' if IPv6 and Global WebAuth configuration are enabled at same time.
3. CKIP is not supported on 10xx APs.
4. Client MFP is not active unless WPA2 is configured.
5. Select valid EAP profile name when local EAP authentication is enabled.

Step 1 Select the **FlexConnect local switching** check box if you want to enable FlexConnect local switching. For more information on FlexConnect, see the "Configuring FlexConnect" section on page 12-4. If you enable it, the FlexConnect access point handles client authentication and switches client data packets locally.

FlexConnect 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 Select the **FlexConnect Local Auth** check box if you want to enable FlexConnect local authentication.

Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office.

Note Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.

Local authentication is not supported in the following scenarios:

- Guest Authentication cannot be performed on a FlexConnect local authentication enabled WLAN.

- RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN.
- Local radius is not supported.
- Once the client has been authenticated, roaming is supported after the WLC and the other FlexConnects in the group are updated with the client information.

Step 3 When you enable hybrid-REAP local switching, the Learn Client IP Address check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.

Step 4 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 5 Select 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 6 Select the **IPv6** check box. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.

Step 7 Select the **Session Timeout** check box to set the maximum time a client session can continue before requiring reauthorization.

Step 8 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 9 The Override Interface drop-down lists provides a list of defined access control lists (ACLs). (See the "Configuring an Access Control List Template" section on page 11-72 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 field is None.

Step 10 You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. From 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.

Note For controller Release 7.2.x and later, the Forward Up Stream is same as Drop for locally switched clients.

If FlexConnect local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is dimmed.

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

Step 11 From the Wi-Fi Direct Clients Policy drop-down list, choose one of the following options:

- **Disabled**—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients. The default is Disabled.
- **Allow**—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN.
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN.

Note The Wi-Fi Direct Clients Policy is applicable to WLANs that have APs in local mode only.

Note The Wi-Fi Direct Clients Policy is applicable for controller Release 7.2.x. and later.

Step 12 Select the check box if you want to enable automatic client exclusion.

Step 13 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 reenable the client.

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

Step 14 Enter the maximum number of clients to be associated in a WLAN in the Maximum Clients text box. The valid range is from 0 to 7000. The default value is 0.

Note A value of 0 allows unlimited number of clients to be associated with a WLAN.

Step 15 Enable dynamic anchoring of static IP clients by selecting the **Static IP Tunneling** check box.

Step 16 Select the **Media Session Snooping** check box. This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and the NCS. 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 17 Select the **KTS based CAC** check box to enable KTS based CAC support per WLAN.

WLC supports TSPEC based CAC and SIP based CAC. But there are certain phones that work with different protocols for CAC, which are based on the KTS (Key Telephone System). For supporting CAC with KTS-based SIP clients, WLC should understand and process the bandwidth request message from those clients to allocate the required bandwidth on the AP radio, in addition to handling and sending certain other messages, as part of this protocol.

Note The KTS CAC configuration is only supported by Cisco 5508, 7500, WISM2, and 2500 controllers that run controller software Release 7.2.x. This feature is not supported by Cisco 4400 series controllers.

Step 18 NAC State—From the **NAC State** drop-down list, choose **SNMP NAC** or **Radius NAC**. SIP errors that are discovered generate traps that appear on the client troubleshooting and alarms screens. 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 "NAC Integration" section on page 9-44 for more information.

Step 19 Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitor access points, or other access points in the same location that do not have this WLAN assigned.

Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

Set the Scan Defer Priority by clicking the priority argument and Set the time in milliseconds in the Scan Defer Interval text box. Valid values are 0 through 60000. The default value is 100 milliseconds.

Step 20 In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings might be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. We recommend a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients.

Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 21 When you select the check box to override DHCP server, another field 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 22 If the MFP Signature Generation check box is selected, 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 23 From the MFP Client Protection drop-down list, choose **Enabled**, **Disabled**, or **Required** for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable.

Note The Enabled parameter is the same as the Optional parameter that you choose from the MFP Client Protection drop-down list in the WLC graphical user interface.

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 24 Enter a value between 1 and 255 beacon intervals in the 802.11a/n DTIM Period group box 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 25 Enter a value between 1 and 255 beacon intervals in the 802.11b/g/n DTIM Period group box 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 The DTIM configuration is not appropriate for guest LANs.

Step 26 Select the **Client Profiling** check box to enable or disable profiling of all the clients that are associated with the WLAN.

Note Client Profiling is not supported with FlexConnect local authentication.

Note Client Profiling is configurable only when you select the DHCP Address Assignment check box.

Step 27 Click **Save**.

Configuring WLAN AP Groups Templates

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.

To configure WLAN AP Groups, follow these steps:

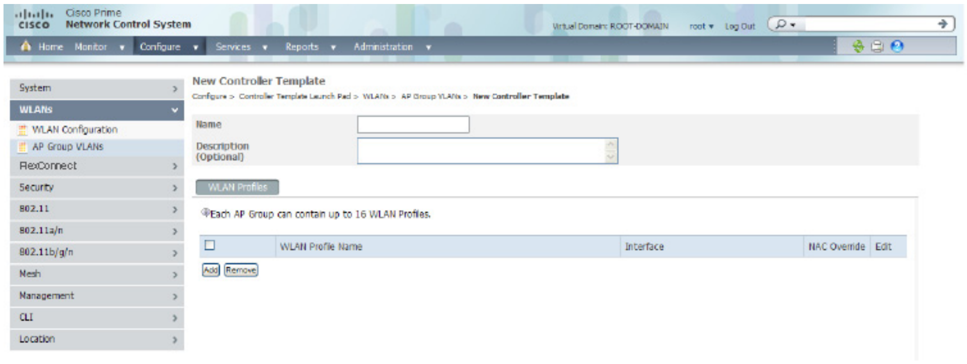
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-16).

Figure 11-16 WLAN AP Groups



New Controller Template

Configure > Controller Template Launch Pad > WLANs > AP Group VLANs > **New Controller Template**

Name

Description (Optional)

Each AP Group can contain up to 16 WLAN Profiles.

□	WLAN Profile Name	Interface	NAC Override	Edit

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

Note The maximum characters that you can enter in the Description text box is 256.

Adding Access Point Groups

You can create or modify a template for dividing the WLAN profiles into AP groups.

To add a new access point group, follow these steps:

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 controllers Release 5.2 and later) 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 If you want to add a WLAN profile, click the **WLAN Profiles** tab and configure the following fields:

a. Click **Add**.

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 appear in the drop-down list.

Note Each access point is limited to 16 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).

b. Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

c. Enter an interface/interface group or choose one from the Interface/Interface Group 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 appear in the drop-down list.

d. Select the **NAC Override** check box, if applicable. The NAC override feature is disabled by default.

e. When access points and WLAN profiles are added, click **Save**.

Step 6 If you want to add a RF profile, click the **RF Profiles** tab, and configure the following fields:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
- 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
- When RF profiles are added, click **Save**.

Note Click the **Click here** link to add a new RF profile. See the "Configuring RF Profiles Templates (802.11)" section on page 11-91 for more information.

Deleting Access Point Groups

To delete an access point group, follow these steps:

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 FlexConnect Templates

This section contains the following topics:

- Configuring FlexConnect AP Groups Templates, page 11-40
- Configuring FlexConnect Users, page 11-43

Configuring FlexConnect AP Groups Templates

FlexConnect 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 FlexConnect access points per location, but you can organize and group the access points per floor and limit them to 25 or so per building, because it is likely the branch offices share the same configuration.

To set up an FlexConnect AP group, follow these steps:

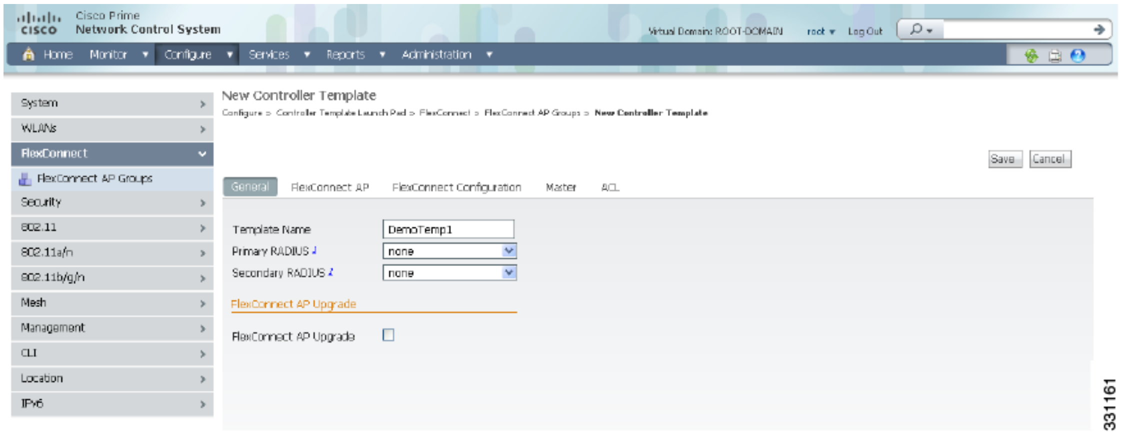
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **FlexConnect AP Groups** or choose **FlexConnect > FlexConnect AP Groups** from the left sidebar menu. The FlexConnect > FlexConnect 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, 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 tab of the FlexConnect AP Groups page appears (see Figure 11-17).

Figure 11-17 AP Groups FlexConnect Template



New Controller Template

Configure > Controller Template Launch Pad > FlexConnect > FlexConnect AP Groups > **New Controller Template**

Template Name	DemoTemp1
Primary RADIUS	none
Secondary RADIUS	none

FlexConnect AP Upgrade

FlexConnect AP Upgrade □

Step 4 The Template Name field shows the group name assigned to the FlexConnect 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 NCS 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 NCS 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 **FlexConnect AP** tab.

Step 8 An access point Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. If more than one group is applied to the same controller, select 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 FlexConnect AP Group page appears.

Step 10 Click the **FlexConnect Configuration** tab to enable local authentication for a FlexConnect group.

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

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

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

Note You can click the **Users configured in the group** link that appears at the bottom of the page to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group.

Step 12 To allow a FlexConnect access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select 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 boxes. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select 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 Authority Info text box, enter the authority information of the EAP-FAST server.

Step 17 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.

Note The EAP-FAST options are available only if you select the **EAP-FAST** check box in Step 12.

Step 18 Click the **Image Upgrade** tab and configure the following:

- FlexConnect AP Upgrade—Select the check box if you want to upgrade the FlexConnect access points.
- Slave Maximum Retry Count—Enter the maximum retries for the slave to undertake to start the download from the master in the FlexConnect group. This option is available only if you select the FlexConnect AP Upgrade check box.

Note You are allowed to add an access point as a master access point only if the FlexConnect AP Upgrade check box is enabled on the General tab.

Step 19 Click the **VLAN-ACL Mapping** tab to view, add, edit, or remove a VLAN ACL mapping.

a. Click **Add**.

b. Enter a VLAN ID. The valid VLAN ID range is 1—4094.

c. From the Ingress ACL drop-down list, choose an Ingress ACL.

d. From the Egress AC drop-down list, choose an Egress ACL.

e. Click **Save**.

Step 20 Click the **WLAN-ACL Mapping** tab to view, add, edit, or remove a WLAN ACL mapping.

a. Click **Add**.

b. From the WLAN Profile Name drop-down list, choose a WLAN profile.

c. From the WebAuth ACL drop-down list, choose a WebAuth ACL.

d. Click **Save**.

Note You can add up to a maximum of 16 WebAuth ACLs.

Step 21 Click the **WebPolicy ACL** tab to view, add, edit, or remove a WebPolicy ACL mapping.

a. Click **Add**.

b. From the Web-Policy ACL drop-down list, choose a WebPolicy ACL.

c. Click **Save**.

Note You can add up to a maximum of 16 Web-Policy ACLs.

Step 22 Click **Save**.

Configuring FlexConnect Users

Note You can create FlexConnect users only after you save the FlexConnect AP Group.

Note Maximum 100 FlexConnect users are supported in controller Release 5.2.x.x and later. If controller Release 5.2.0.0, and earlier supports only 20 FlexConnect users.

To configure a FlexConnect user, follow these steps:

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

Step 2 Click **FlexConnect AP Groups** or choose **FlexConnect > FlexConnect AP Groups** from the left sidebar menu. The FlexConnect > FlexConnect AP Groups page appears.

Step 3 Click the **FlexConnect Configuration** tab to enable local authentication for a FlexConnect group.

Step 4 Select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group.

Step 5 Click the **Users configured in the group** link. The FlexConnect Users page appears.

Step 6 If you want to add a new user, choose **Add User** from the Select a command drop-down list, and click **Go**. The **Add User** page appears.

Step 7 In the User Name text box, enter the FlexConnect username.

Step 8 In the Password text box, enter the password.

Step 9 Reenter the password in the Confirm Password text box.

Step 10 Click **Save**.

Note To delete a FlexConnect User, choose a user from the FlexConnect Users list, and then click **Delete**.

Configuring Security Templates

This section contains the following topics:

Configuring a General Security Controller Template

To add a new template with general security information for a controller, follow these steps:

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

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

Step 3 Configure the following fields:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Maximum Local Database Entries (on next reboot)—Enter the maximum number of allowed database entries. This amount becomes effective on the next reboot.

Step 4 Click **Save**. Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the "Applying Controller Templates" section on page 11-2 for more information.

Configuring a File Encryption Template

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

To configure a File Encryption template, follow these steps:

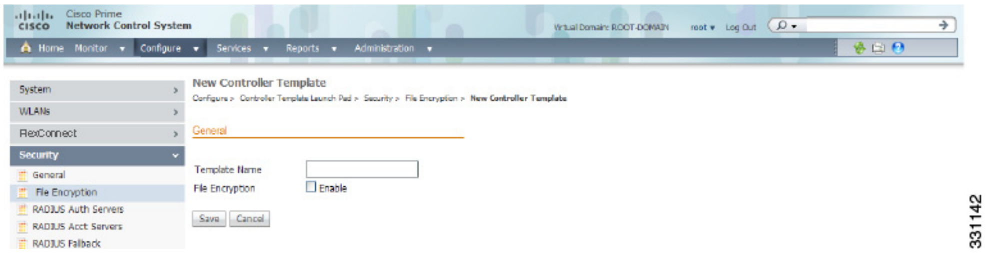
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-18).

Figure 11-18 File Encryption Template



New Controller Template

Configure > Controller Template Launch Pad > Security > File Encryption > New Controller Template

General

Template Name

File Encryption □ Enable

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.

To configure a RADIUS Authentication template, follow these steps:

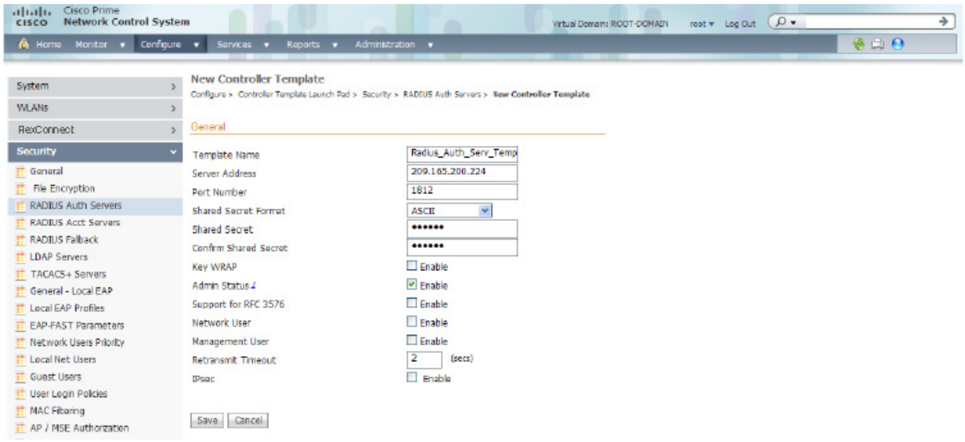
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-19).

Figure 11-19 RADIUS Authentication Server Template



New Controller Template

Configure > Controller Template Launch Pad > Security > RADIUS Auth Servers > New Controller Template

General

Template Name	Radius_Auth_Serv_Temp
Server Address	209.165.200.224
Port Number	1812
Shared Secret Format	ASCII
Shared Secret	••••••
Confirm Shared Secret	••••••
Key WRAP	□ Enable
Admin Status	☑ Enable
Support for RFC 3576	□ Enable
Network User	□ Enable
Management User	□ Enable
Retransmit Timeout	2 (secs)
IPsec	□ Enable

Step 4 From the Shared Secret Format drop-down list, choose either **ASCII** or **hex**.

Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). 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 Select the check box if you want to enable key wrap. If this check box is enabled, the authentication request is sent to RADIUS servers that have following key encryption key (KEK) and message authenticator code keys (MACK) configured. When enabled, the following fields appear:

- Shared Secret Format: Enter ASCII or hexadecimal.

Note Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the NCS). 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 the event a discovered template is applied to another device.

- KEK Shared Secret: Enter the KEK shared secret.
- MACK Shared Secret: Enter the 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 fields 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. The 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 field, 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.

To configure a RADIUS Accounting template, follow these steps:

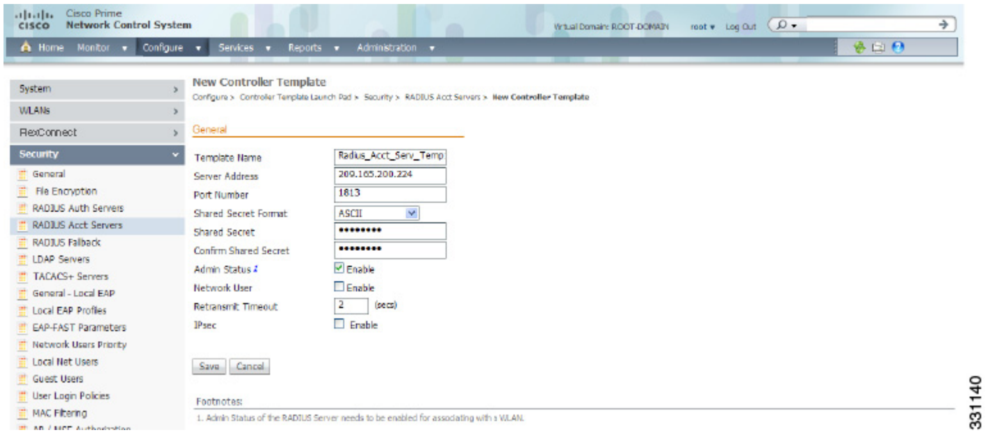
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-20).

Figure 11-20 RADIUS Accounting Server Templates



New Controller Template

Configure > Controller Template Launch Pad > Security > RADIUS Acct Servers > New Controller Template

General

Template Name	Radius_Acct_Serv_Temp
Server Address	209.165.200.224
Port Number	1813
Shared Secret Format	ASCII
Shared Secret	••••••••
Confirm Shared Secret	••••••••
Admin Status [1]	☑ Enable
Network User	□ Enable
Retransmit Timeout	2 (secs)
IPsec	□ Enable

Footnotes:
1. Admin Status of the RADIUS Server needs to be enabled for associating with a WLAN.

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 the NCS). 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 times out and a retransmission by the controller occurs. 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.

To configuring a RADIUS Fallback template, follow these steps:

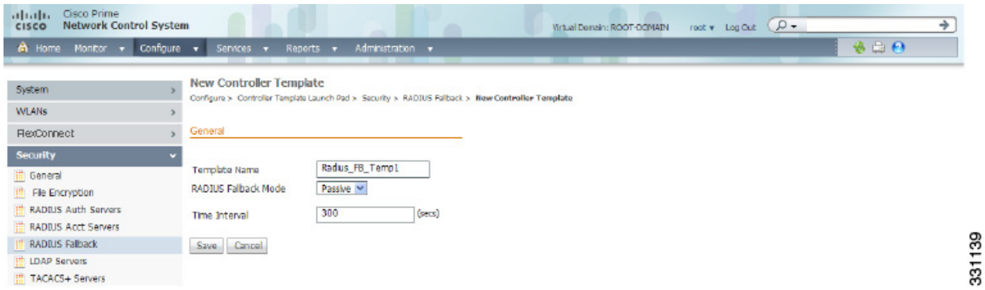
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-21).

Figure 11-21 RADIUS Fallback Page



New Controller Template

Configure > Controller Template Launch Pad > Security > RADIUS Fallback > New Controller Template

General

Template Name: Radius_FB_Temp1
RADIUS Fallback Mode: Passive
Time Interval: 300 (secs)

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 an 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 might use an LDAP server as its backend database to retrieve user credentials.

To add an LDAP server template or make modifications to an existing LDAP server template, follow these steps:

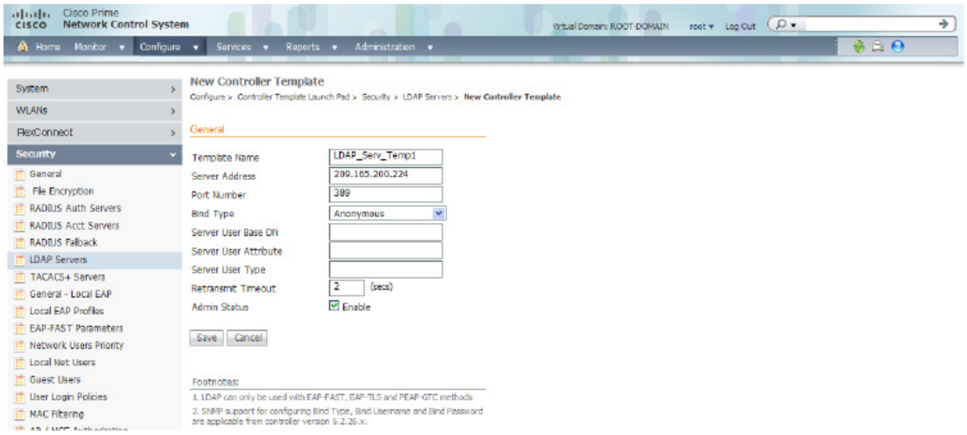
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-22).

Figure 11-22 LDAP Server Template



New Controller Template

Configure > Controller Template Launch Pad > Security > LDAP Servers > **New Controller Template**

General

Template Name	LDAP_Serv_Temp1
Server Address	209.165.200.224
Port Number	389
Bind Type	Anonymous
Server User Base DN	
Server User Attribute	
Server User Type	
Retransmit Timeout	2 (secs)
Admin Status	☑ Enable

Save Cancel

Footnotes:

1. LDAP can only be used with EAP-FAST, EAP-TLS and PEAP-GTC methods
2. SNMP support for configuring Bind Type, Bind Username and Bind Password are applicable from controller version 5.2.26.x.

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.

To configure a TACACS+ Server template, follow these steps:

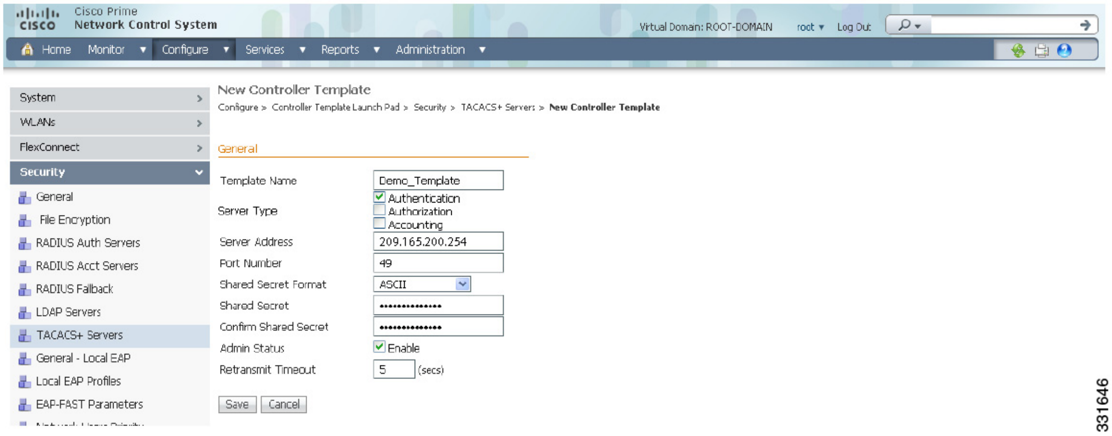
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-23).

Figure 11-23 TACACS+ Server Template



New Controller Template

Configure > Controller Template Launch Pad > Security > TACACS+ Servers > **New Controller Template**

General

Template Name	Demo_Template
Server Type	☑ Authentication □ Authorization □ Accounting
Server Address	209.165.200.254
Port Number	49
Shared Secret Format	ASCII
Shared Secret	••••••••••••••
Confirm Shared Secret	••••••••••••••
Admin Status	☑ Enable
Retransmit Timeout	5 (secs)

Save Cancel

Step 4 Select one or more server types by selecting their respective check boxes. The following server types are available:

- **authentication**—Server for user authentication/authorization.
- **authorization**—Server for user authorization only.
- **accounting**—Server for RADIUS user accounting.

Step 5 Enter the IP address of the server.

Step 6 Enter the port number of the server. The default is 49.

Step 7 From the drop-down list, choose either **ASCII** or **hex**.

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

Step 8 Enter the TACACS+ shared secret used by your specified server in the Shared Secret text box.

Step 9 Reenter the shared secret in the Confirm Shared Secret text box.

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

Step 11 In the Retransmit Timeout text box, enter the time, in seconds, after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Step 12 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.

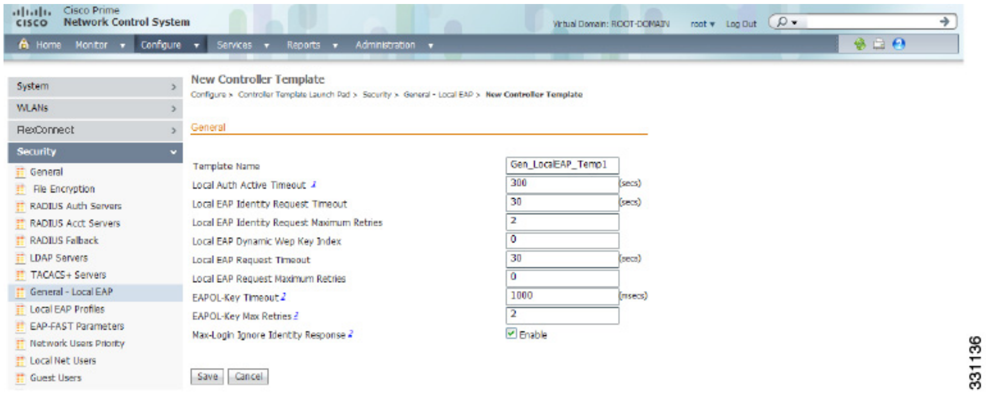
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-24).

Figure 11-24 Local EAP General Template



New Controller Template

Configure > Controller Template Launch Pad > Security > General - Local EAP > **New Controller Template**

General

Template Name	Gen_LocalEAP_Temp1
Local Auth Active Timeout	300 (secs)
Local EAP Identity Request Timeout	30 (secs)
Local EAP Identity Request Maximum Retries	2
Local EAP Dynamic Wep Key Index	0
Local EAP Request Timeout	30 (secs)
Local EAP Request Maximum Retries	0
EAPOL-Key Timeout	1000 (msecs)
EAPOL-Key Max Retries	2
Max-Login Ignore Identity Response	☑ Enable

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.

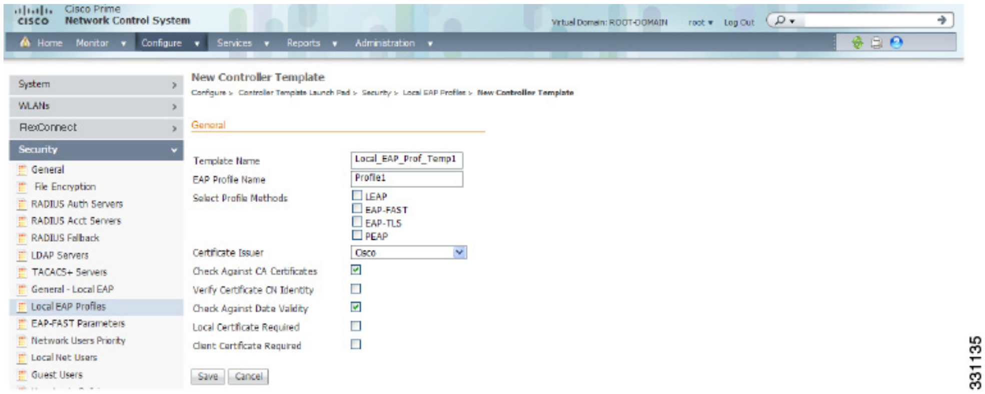
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-25).

Figure 11-25 Local EAP Profiles Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Local EAP Profiles > New Controller Template

General

Template Name: Local_EAP_Prof_Temp1

EAP Profile Name: Profile1

Select Profile Methods: □ LEAP □ EAP-FAST □ EAP-TLS □ PEAP

Certificate Issuer: Cisco

Check Against CA Certificates: ☑

Verify Certificate CN Identity: □

Check Against Date Validity: ☑

Local Certificate Required: □

Client Certificate Required: □

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

- 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, select the **Check Against CA Certificates** check box.

Step 7 If you want the (CN) in the incoming certificate to be validated against the common name of the CA certificate, select 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, select the **Check Against Date Validity** check box.

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

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

Step 11 Click **Save**.

Step 12 To enable local EAP, follow these steps:

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

b. Click the profile name of the desired WLAN.

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

d. Select 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.

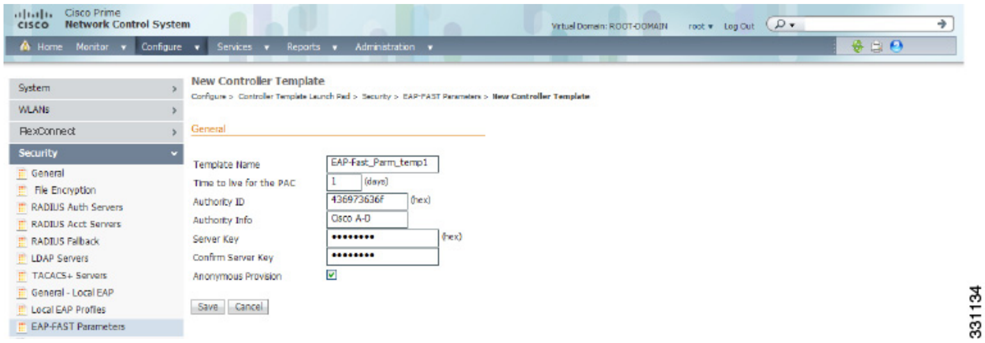
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-26).

Figure 11-26 EAP-FAST Parameters Template



New Controller Template

Configure > Controller Template Launch Pad > Security > EAP-FAST Parameters > New Controller Template

General

Template Name	EAP-Fast_Parm_temp1
Time to live for the PAC	1 (days)
Authority ID	436973636f (hex)
Authority Info	Cisco A-D
Server Key	•••••••• (hex)
Confirm Server Key	••••••••
Anonymous Provision	☑

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 Info text box, enter the authority identifier of the local EAP-FAST server in text format.

Step 7 In the Server Key and Confirm Server Key text boxes, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

Step 8 If you want to enable anonymous provisioning, select 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 9 Click **Save**.

Configuring a Network User Priority Template

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.

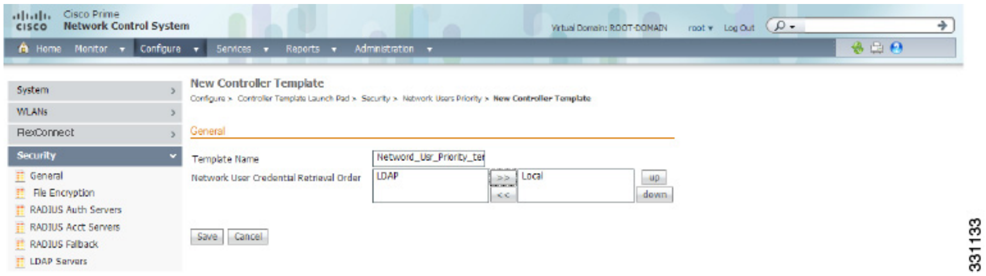
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-27).

Figure 11-27 Network User Credential Retrieval Priority Order Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Network Users Priority > **New Controller Template**

General

Template Name: Netword_Usr_Priority_ter

Network User Credential Retrieval Order: LDAP | Local

Step 4 Use the left and right pointing arrows to include or exclude 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 might 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.

To configure a Local Network Users template, follow these steps:

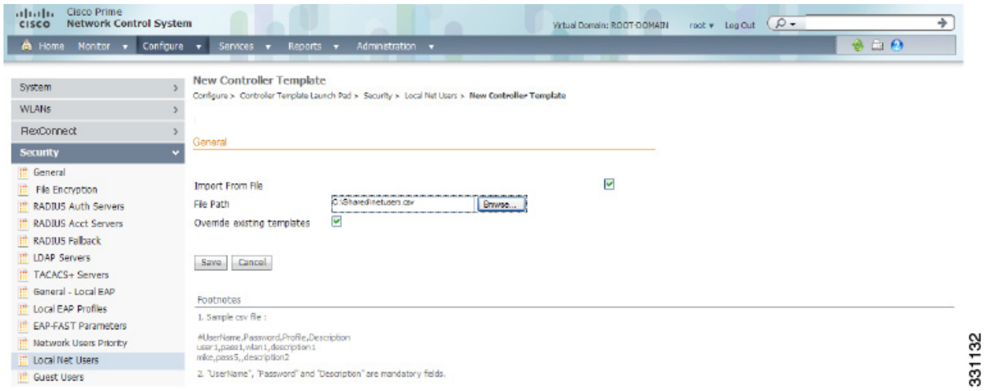
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-28).

Figure 11-28 Local Net Users Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Local Net Users > **New Controller Template**

General

Import From File ☑

File Path C:\Shared\netusers.csv

Override existing templates ☑

Footnotes

1. Sample csv file :

```
#UserName,Password,Profile,Description
user1,pass1,wlan1,description1
mike,pass5,,description2
```

2. "UserName", "Password" and "Description" are mandatory fields.

Step 4 If you keep Import from File enabled, you need to enter a file path or click **Browse** 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 NCS. The header can either be blank or filled. The NCS 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 Step 11.

Step 10 If you want to override the existing template, select the **Override existing templates** check box.

Step 11 Click **Save**.

Guest User Templates

Choose **Configure > Controller Template Launch Pad > Security > Guest Users** to access the Guest Users list page.

Note To reduce clutter, the NCS 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.

Note Click the **Edit View** link to add, remove, or reorder columns in the Guest Users table.

Configuring a Guest User Template

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.

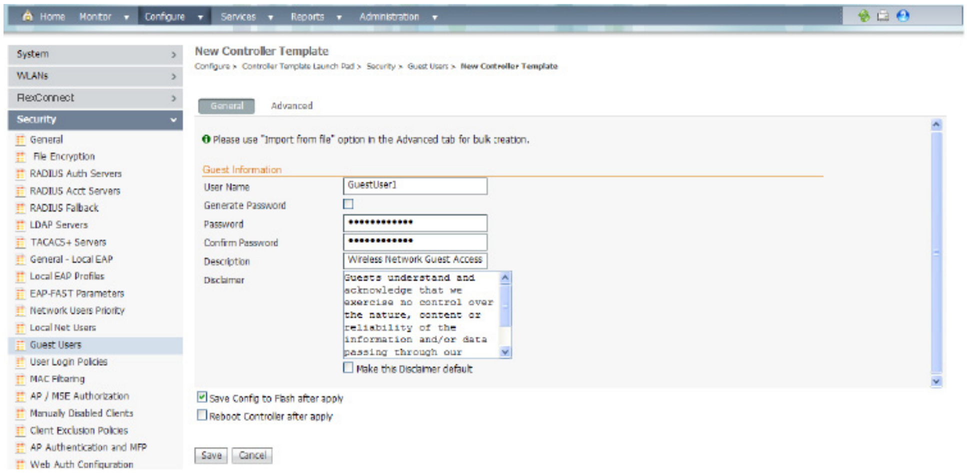
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, the NCS 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, choose **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 11-29).

Figure 11-29 Guest User Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Guest Users > New Controller Template

Please use "Import from file" option in the Advanced tab for bulk creation.

Guest Information

User Name	GuestUser1
Generate Password	□
Password	••••••••••••
Confirm Password	••••••••••••
Description	Wireless Network Guest Access
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our
	□ Make this Disclaimer default

☑ Save Config to Flash after apply

□ Reboot Controller after apply

Step 4 Enter a guest username in the User Name text box. The maximum size is 24 characters.

Step 5 Enter a password for this username in the Password text box.

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 access of the guest (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 remains 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 (Optional) Modify the default guest user description on the General tab if necessary.

Step 12 (Optional) Modify the Disclaimer text on the General tab, if necessary. If you want the supplied text to be the default, select 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.

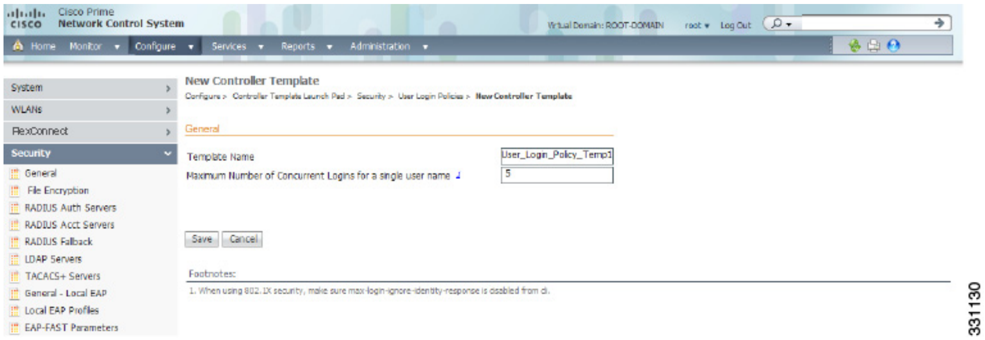
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-30).

Figure 11-30 User Login Policies Template



New Controller Template

Configure > Controller Template Launch Pad > Security > User Login Policies > New Controller Template

General

Template Name: User_Login_Policy_Temp1

Maximum Number of Concurrent Logins for a single user name [1]: 5

Footnotes:

1. When using 802.1X security, make sure max-login-ignore-identity-response is disabled from cli.

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

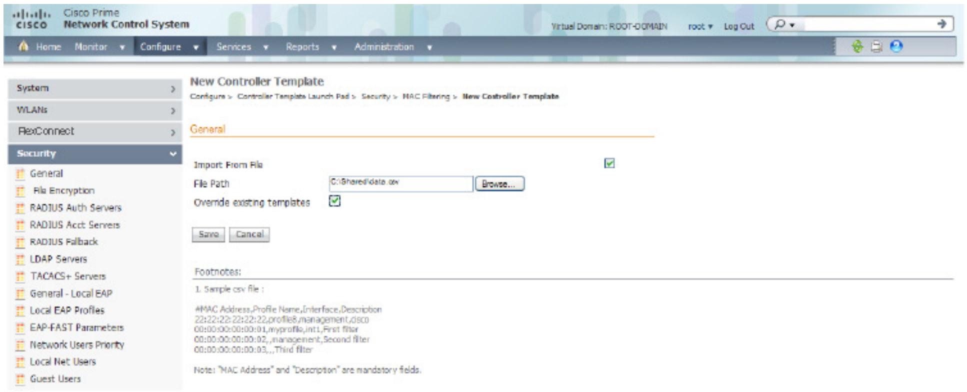
This page allows you to add a MAC filter template or make modifications to an existing MAC filter template.

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, choose **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 11-31).

Figure 11-31 MAC Filter Templates



New Controller Template

Configure > Controller Template Launch Pad > Security > MAC Filtering > **New Controller Template**

General

Import From File ☑

File Path C:\Shared\data.csv

Override existing templates ☑

Footnotes:

1. Sample csv file :

```
#MAC Address,Profile Name,Interface,Description
22:22:22:22:22:22,profile8,management,cisco
00:00:00:00:00:01,myprofile,int1,First filter
00:00:00:00:00:02,,management,Second filter
00:00:00:00:00:03,,,Third filter
```

Note: "MAC Address" and "Description" are mandatory fields.

Step 4 If you keep Import From File enabled, you must enter a file path or click **Browse** 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 unselect the Import from File check box, 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, select the **Override existing templates** check box.

Step 9 Click **Save**.

Note You cannot use MAC address in the broadcast range.

Configuring an Access Point or MSE Authorization Template

To add an MSE authorization or make changes to an existing access point or MSE authorization template, follow these steps:

Note 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 Mobility Services Engine Configuration Guide* for further information.

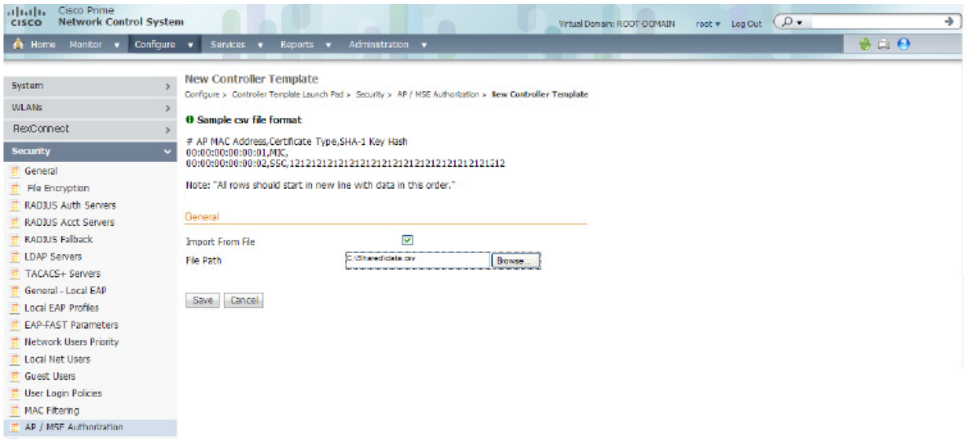
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **AP/MSE Authorization** or choose **Security > AP/MSE Authorization** from the left sidebar menu. The Security > AP/LBS Authorization Template page 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, choose **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 11-32).

Figure 11-32 AP/MSE Authorization Templates



New Controller Template

Configure > Controller Template Launch Pad > Security > AP / MSE Authorization > New Controller Template

Sample csv file format

```
# AP MAC Address,Certificate Type,SHA-1 Key Hash
00:00:00:00:00:01,MIC,
00:00:00:00:00:02,SSC,1212121212121212121212121212121212121212
```

Note: "All rows should start in new line with data in this order."

General

Import From File ☑

File Path C:\Shared\data.csv

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 desired file path or click **Browse** to import the file.

Step 6 Click **Save**.

Note You cannot use MAC address in the broadcast range.

Configuring a Manually Disabled Client Template

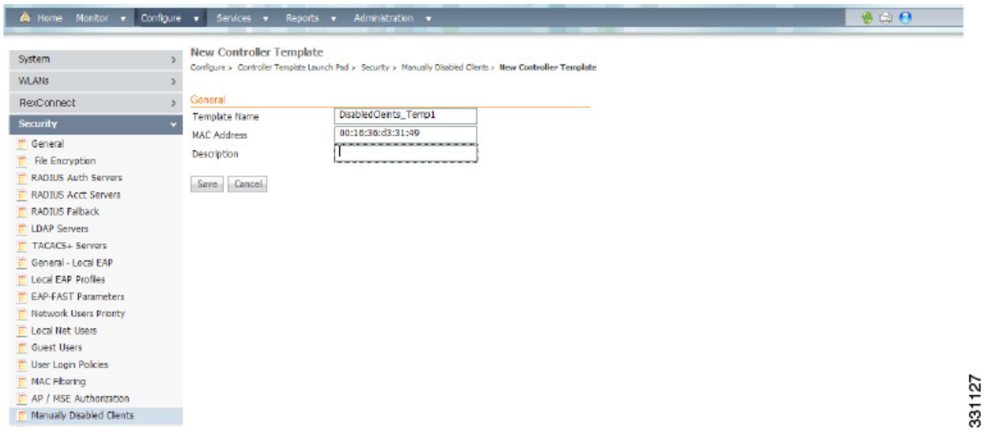
This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

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, choose **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 11-33).

Figure 11-33 Manually Disabled Clients Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Manually Disabled Clients > **New Controller Template**

General

Template Name: DisabledClients_Temp1

MAC Address: 00:16:36:d3:31:49

Description:

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**.

Note You cannot use a MAC address in the broadcast range.

Configuring a Client Exclusion Policies Template

To add a client exclusion policies template or modify an existing client exclusion policies template, follow these steps:

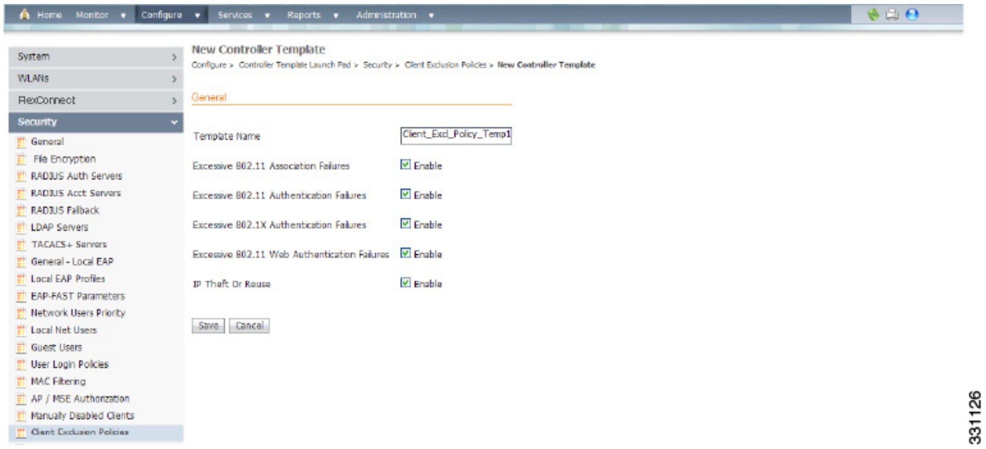
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-34).

Figure 11-34 Policies Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Client Exclusion Policies > New Controller Template

General

Template Name: Client_Excl_Policy_Temp1

Excessive 802.11 Association Failures ☑ Enable

Excessive 802.11 Authentication Failures ☑ Enable

Excessive 802.1X Authentication Failures ☑ Enable

Excessive 802.11 Web Authentication Failures ☑ Enable

IP Theft Or Reuse ☑ Enable

Step 4 Edit a client exclusion policies template by configuring its field (see Table 11-3).

Table 11-3 Policies Template Fields

Field	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.
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 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.

To add or make modifications for the access point authentication and management frame protection (MFP) template, follow these steps:

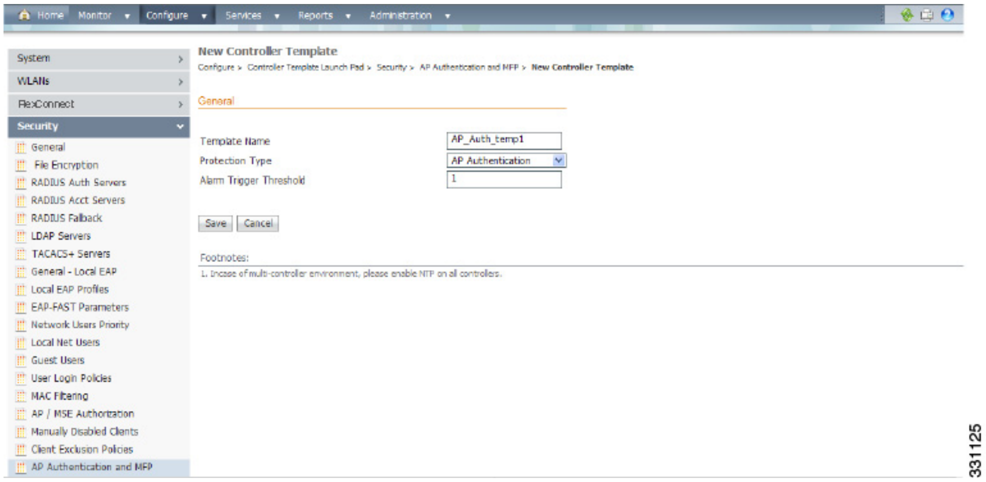
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 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, choose **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 11-35).

Figure 11-35 AP Authentication Policy Template



New Controller Template

Configure > Controller Template Launch Pad > Security > AP Authentication and MFP > New Controller Template

General

Template Name: AP_Auth_temp1

Protection Type: AP Authentication

Alarm Trigger Threshold: 1

Footnotes:

1. Incase of multi-controller environment, please enable NTP on all controllers.

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 might 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.

To add or make modifications to an existing web authentication template, follow these steps:

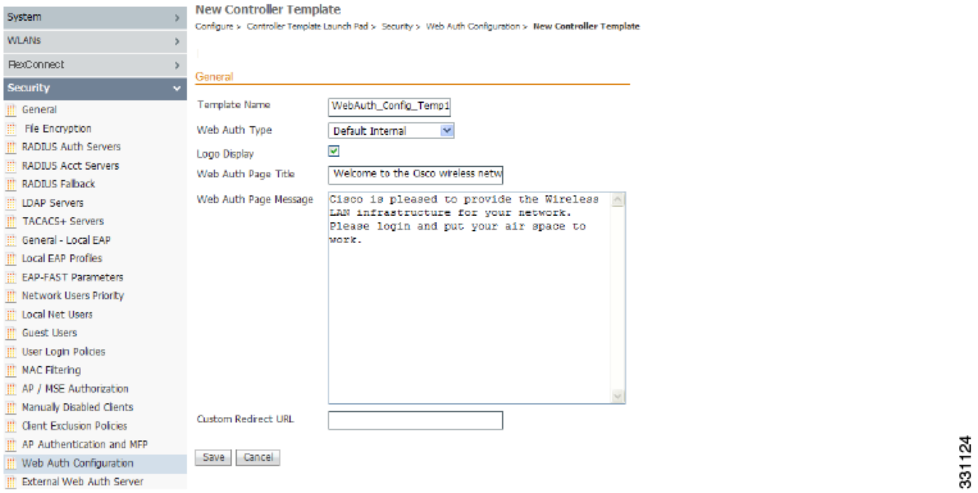
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-36).

Figure 11-36 Web Authentication Configuration Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Web Auth Configuration > **New Controller Template**

General

Template Name	WebAuth_Config_Templ
Web Auth Type	Default Internal
Logo Display	☑
Web Auth Page Title	Welcome to the Cisco wireless netw
Web Auth Page Message	Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.
Custom Redirect URL	

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 is directed to the company home page.

Step 5 Select the **Logo Display** check box 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.

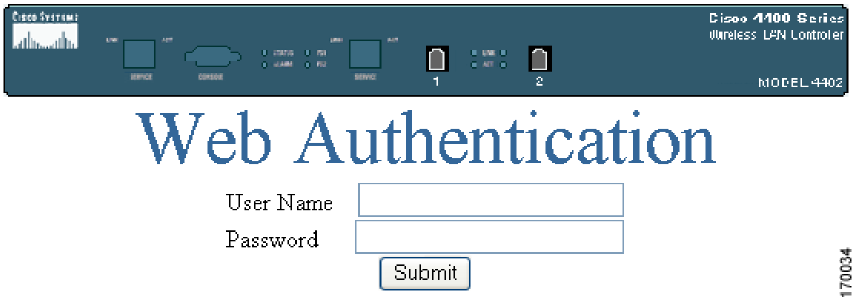
When downloading customized web authentication, you must follow these strict guidelines:

- 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.

Before downloading, follow these steps:

Step 1 Download the sample login.html bundle file from the server. The .html file is shown in Figure 11-37. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 11-37 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 NCS because the built-in TFTP server of the NCS 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 field. If you know the filename and path relative to the root directory of the server, you can also select TFTP server.

Note For a local machine download, either .zip or .tar file options exists, but the NCS 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 field.

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

Step 14 The files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** 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 field, and the server filename is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of the NCS. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of the NCS server, 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 an External Web Auth Server Template

To create or modify an External Web Auth Server template, follow 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. In this page, you can edit the current template fields.

Configuring a Security Password Policy Template

This page enables you to determine your security password policy.

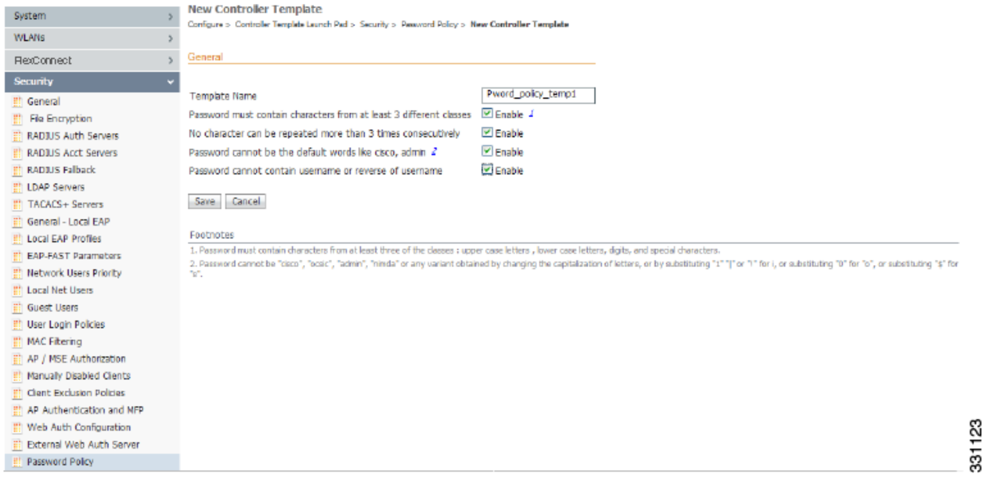
To add or make modifications to an existing password policy template, follow these steps:

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

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

Step 3 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 Password Policy template page appears (see Figure 11-38).

Figure 11-38 Password Policy Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Password Policy > New Controller Template

General

Template Name: Pword_policy_temp1

Password must contain characters from at least 3 different classes ☑ Enable [1]

No character can be repeated more than 3 times consecutively ☑ Enable

Password cannot be the default words like cisco, admin [2] ☑ Enable

Password cannot contain username or reverse of username ☑ Enable

Footnotes

1. Password must contain characters from at least three of the classes : upper case letters , lower case letters, digits, and special characters.

2. Password cannot be "cisco", "ocsic", "admin", "nimda" or any variant obtained by changing the capitalization of letters, or by substituting "1" "|" or "!" for i, or substituting "0" for "o", or substituting "$" for "s".

Step 4 Enter the template name.

Step 5 You can enable or disable the following settings:

- Password must contain characters from at least 3 different classes such as uppercase letters, lowercase letters, digits, and special characters.
- No character can be repeated more than 3 times consecutively.
- Password cannot be the default words like cisco, admin.

Note Password cannot be “cisco”, “ocsic”, “admin”, “nimda’ or any variant obtained by changing the capitalization of letters, or by substituting ‘1” “|” or “!” for i, or substituting “0” for “o”, or substituting “$” for “s”.

- Password cannot contain username or reverse of username.

Step 6 Click **Save**.

Configuring Security - Access Control Templates

This section contains the following topics:

- Configuring an Access Control List Template, page 11-72
- Configuring a FlexConnect Access Control List Template, page 11-75
- Configuring an ACL IP Groups Template, page 11-76
- Configuring an ACL Protocol Groups Template, page 11-77

Configuring an Access Control List Template

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.

This release of the NCS provides support to IPv6 ACLs.

To add or modify an existing ACL template, follow these steps:

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 If you want to add a new Access Control List template, choose **Add Template** from the Select a command drop-down list, and click **Go**. The New Controller Template page appears. In this page, specify the following fields:

- Access Control List Name—User-defined name of the template.
- ACL Type—Choose either **IPv4** or **IPv6**.

Note IPv6 ACL is supported from controller Release 7.2.x.

Step 4 To create reusable grouped IP addresses and protocols, choose **Access Control > IP Groups** from the left sidebar menu.

Step 5 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.

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

Step 6 In the ACL IP Groups details page you can edit the current IP group fields.

- 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.

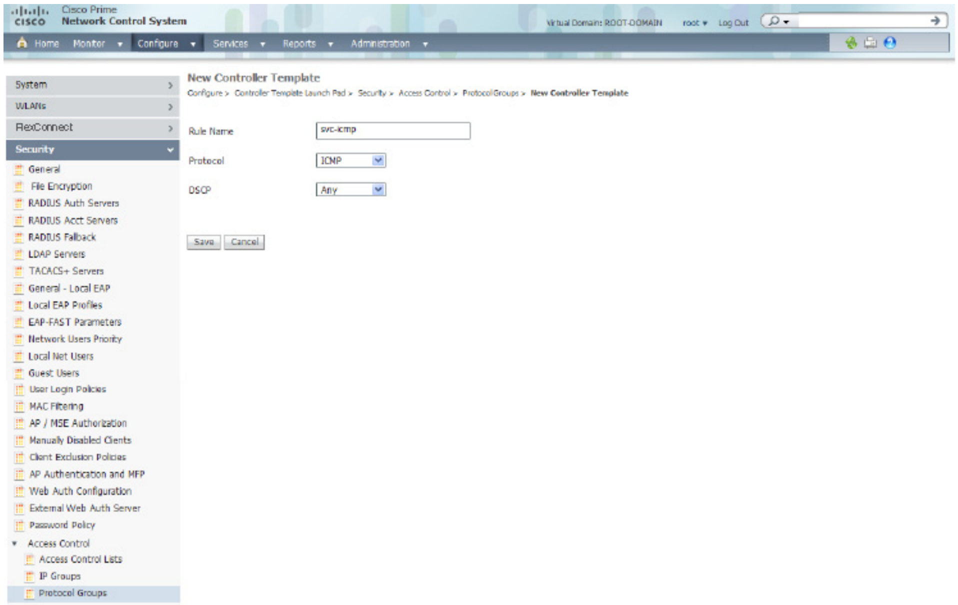
  - Netmask—A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service.
  - CIDR—Classless InterDomain Routing. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks.

- 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 7 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 8 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 11-39).

Figure 11-39 Protocol Groups Controller Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Access Control > Protocol Groups > New Controller Template

Rule Name: svc-icmp

Protocol: ICMP

DSCP: Any

Step 9 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 10 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 11 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 12 From 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 13 Click **Save**.

Step 14 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.

Step 15 To define a new mapping, choose **Add Rule Mappings** from the Select a command drop-down list. The Add Rule Mapping page appears.

Step 16 Configure the following fields:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Direction—Any, Inbound (from client) or Outbound (to client).
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 17 Click **Add**. The new mappings populate the bottom table.

Step 18 Click **Save**.

Step 19 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 FlexConnect Access Control List Template

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

Note The FlexConnect ACLs do not support IPv6 addresses.

This section contains the following topics:

- Configuring and Applying a FlexConnect Access Control List, page 11-75
- Deleting a FlexConnect Access Control List, page 11-76

Configuring and Applying a FlexConnect Access Control List

To configure and apply an Access Control List template to a Controller, follow these steps:

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

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > Access Control > FlexConnect ACLs**.

Step 4 From the Select a command drop-down list, choose **Add a Template**.

Step 5 Click **Go**.

The New Controller Template page appears.

Step 6 Enter a name for the new FlexConnect ACL in the **FlexConnect ACL Name** text box.

Step 7 Click **Save**.

A FlexConnect ACL template is created. 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 FlexConnect ACL mappings appear on the top of the page, and all FlexConnect ACL rules appear in the bottom.

Step 8 From the Select a command drop-down list, choose **Add Rule Mappings**, and click **Go**.

Step 9 The FlexConnect ACL IP Protocol Map page appears.

Step 10 Configure the following fields:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 11 Click **Add**. The new mappings populate the bottom table.

Step 12 Click **Save**.

Step 13 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 FlexConnect ACL templates are duplicated into a new FlexConnect ACL template. This duplication clones all the FlexConnect ACL rules and mappings defined in the source FlexConnect ACL template.

Step 14 From the Select a command drop-down list in the FlexConnect ACL page, choose **Apply Templates**.

The Apply to Controllers page appears.

Step 15 Select **Save Config to Flash after apply** check box to save the configuration to Flash after applying the FlexConnect ACL to the controller.

Step 16 Select **Reboot Controller after apply** to reboot the controller once the FlexConnect ACL is applied. This check box is available only when you select the Save Config to Flash after apply check box.

Step 17 Select one or more controllers and click **OK** to apply the FlexConnect ACL template.

The FlexConnect ACL that you created appears in Configure > Controller Template Launch Pad > <*IP Address*> > Security > Access Control > FlexConnect ACLs.

Deleting a FlexConnect Access Control List

To delete a FlexConnect ACL, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > FlexConnect ACLs**.

Step 4 From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.

Step 5 From the Select a command drop-down list, choose **Delete FlexConnect ACLs**.

Step 6 Click **Go**.

Configuring an ACL IP Groups Template

To create reusable grouped IP addresses, follow these steps:

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

Step 2 Choose **Security > Access Control > IP Groups** from the left sidebar menu.

Step 3 All the IP address including IPv4 and IPv6 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 or Add IPv6 Group** from the Select a command drop-down list, and click **Go**.

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

Note For the IPv6 address of any, an *any* group is predefined with an IP address type as IPv6.

Step 4 Configure the following fields:

- IP Group Name
- IP Address—For IP Group, enter an IPv4 address format. For IPv6 groups, enter an IPv6 address format.
- 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 Addresses/Netmasks text box.

  Note These fields are not applicable for IPv6 groups.

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

  Netmask allows the user 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

  Note These fields are not applicable for IPv6 groups.

- Prefix Length—Prefix for IPv6 addresses, ranging from 0 to 128.
- 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 an IP address or Netmask.

Step 5 Click **Save**. Once saved, the IP Group appears in the Template List page.

You can 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 in the top of the page, and all ACL rules appear in the bottom. See the "Configuring an Access Control List Template" section on page 11-72 for more information.

See the "Configuring an ACL Protocol Groups Template" section on page 11-77 for information on defining Protocol Groups.

Configuring an ACL Protocol Groups Template

To define an additional protocol that is not a standard predefined one, follow these steps:

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

Step 2 Choose **Access Control > Protocol Groups** from the left sidebar menu.

Step 3 Configure the following fields:

- Rule Name—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 fields of a rule, the action for this rule is exercised.

  Note See the "Configuring an Access Control List Template" section on page 11-72 for more information on ACLs.

- Protocol—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/)
- Source Port—Can be 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—Destination port. If TCP or UDP is selected, can be 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.
- DSCP (Differentiated Services Code Point)—Choose Any or Specific from the drop-down list. If Specific is selected, enter the DSCP (range of 0 through 255).

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

Step 4 Click **Save**. Once saved, the IP Group displays in the Template List page.

You can 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 in the top of the page, and all ACL rules appear in the bottom. See the "Configuring an Access Control List Template" section on page 11-72 for more information.

See the "Configuring an ACL IP Groups Template" section on page 11-76 for information on defining IP Groups.

Configuring Security - CPU Access Control List Templates

Note CPU ACL configuration with IPv6 is not supported in this release becuase all IP addresses of controllers on interfaces use IPv4 except the virtual interface.

Configuring a CPU Access Control List (ACL) Template

The existing ACLs established in the "Configuring an Access Control List Template" section on page 11-72 is used to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

To add or modify an existing CPU ACL template, follow these steps:

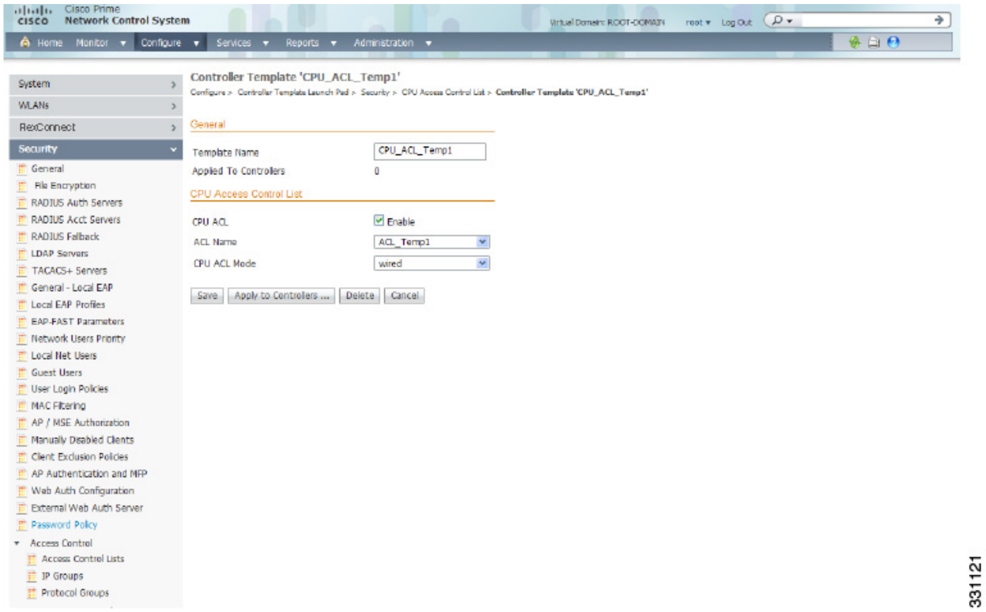
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-40).

Figure 11-40 CPU Access Control List Template



Controller Template 'CPU_ACL_Temp1'

Configure > Controller Template Launch Pad > Security > CPU Access Control List > Controller Template 'CPU_ACL_Temp1'

General

Template Name: CPU_ACL_Temp1

Applied To Controllers: 0

CPU Access Control List

CPU ACL: ☑ Enable

ACL Name: ACL_Temp1

CPU ACL Mode: wired

Step 4 If you select the check box to enable CPU ACL, two more fields appear. When CPU ACL is enabled and applied on the controller, the NCS 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 Security - Rogue Templates

This section contains the following topics:

- Configuring a Rogue Policies Template, page 11-80
- Configuring a Rogue AP Rules Template, page 11-82
- Configuring a Rogue AP Rule Groups Template, page 11-84
- Configuring a Friendly Access Point Template, page 11-86

Configuring a Rogue Policies Template

This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

To add or modify an existing template, follow these steps:

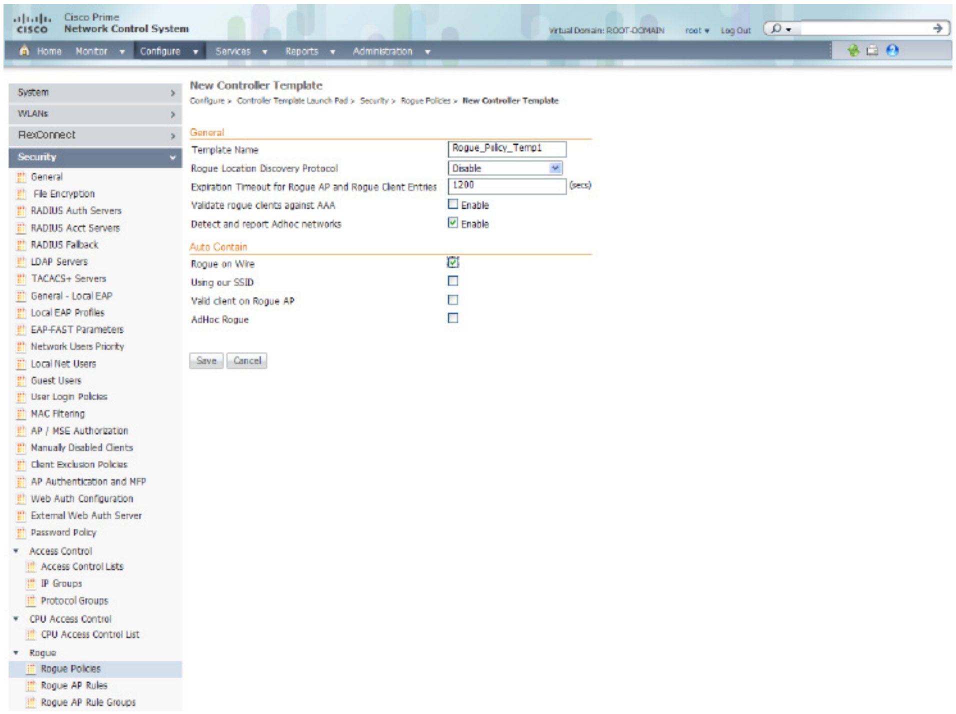
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-41).

Figure 11-41 Rogue Policy Setup Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Rogue Policies > **New Controller Template**

General

Template Name	Rogue_Policy_Temp1
Rogue Location Discovery Protocol	Disable
Expiration Timeout for Rogue AP and Rogue Client Entries	1200 (secs)
Validate rogue clients against AAA	□ Enable
Detect and report Adhoc networks	☑ Enable

Auto Contain

Rogue on Wire	☑
Using our SSID	□
Valid client on Rogue AP	□
AdHoc Rogue	□

Save Cancel

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 In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.

Step 7 In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.

Note There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

Step 8 In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

Step 9 Select the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

Step 10 Select the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.

Step 11 Click **Save**.

Configuring a Rogue AP Rules Template

Rogue access point rules allow you to define rules to automatically classify rogue access points. The NCS applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue 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, see the "Viewing or Editing Rogue Access Point Rules" section on page 9-199.

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.

To add or create a new classification rule template for rogue access points, follow these steps:

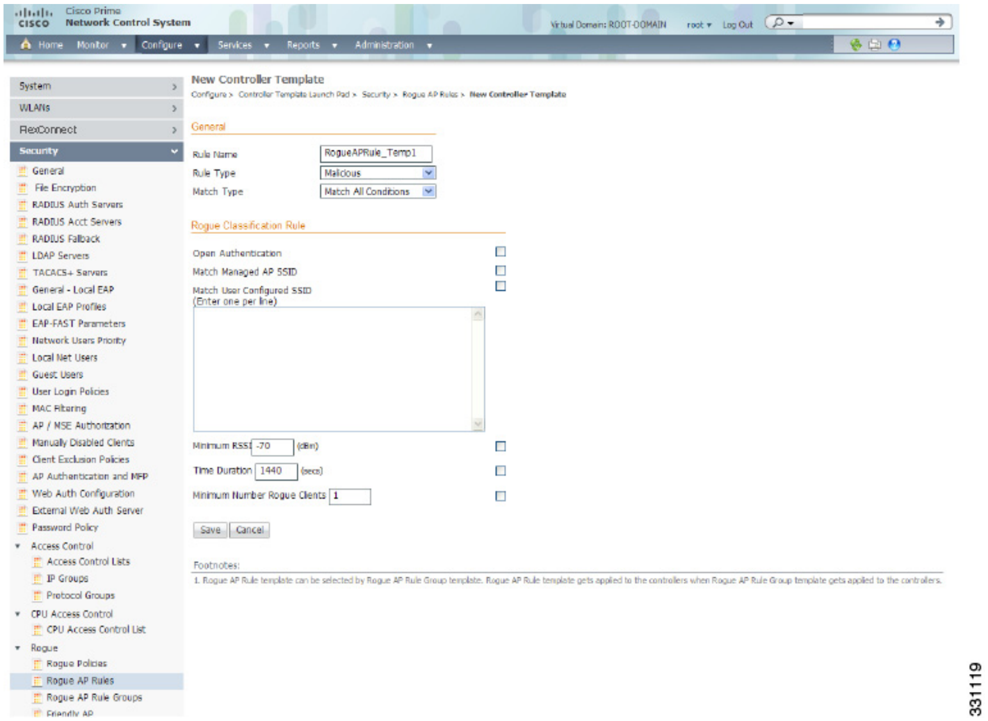
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 11-42). 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 11-42 Rogue AP Rules > New Template Page



New Controller Template

Configure > Controller Template Launch Pad > Security > Rogue AP Rules > New Controller Template

General

Rule Name: RogueAPRule_Temp1

Rule Type: Malicious

Match Type: Match All Conditions

Rogue Classification Rule

Open Authentication ☐

Match Managed AP SSID ☐

Match User Configured SSID ☐
(Enter one per line)

Minimum RSSI -70 (dBm) ☐

Time Duration 1440 (secs) ☐

Minimum Number Rogue Clients 1 ☐

Footnotes:

1. Rogue AP Rule template can be selected by Rogue AP Rule Group template. Rogue AP Rule template gets applied to the controllers when Rogue AP Rule Group template gets applied to the controllers.

Step 4 In the General group box, configure the following fields:

- 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 group box of the page, configure the following fields.

- Open Authentication—Select the check box to enable open authentication.
- Match Managed AP SSID—Select 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—Select 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—Select 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—Select 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—Select 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.

To view current rogue access point rule group templates or create a new rule group, follow these steps:

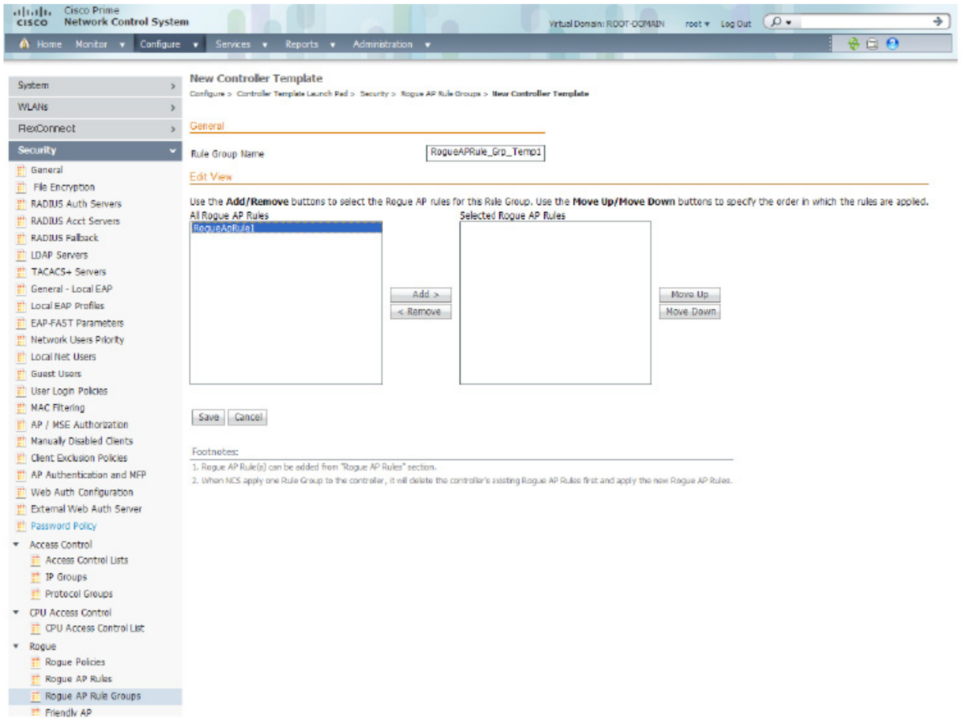
Step 1 Choose **Configure > Controller Template Launch Pad**.

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 11-43).

Figure 11-43 Rogue AP Rule Groups > New Template



New Controller Template

Configure > Controller Template Launch Pad > Security > Rogue AP Rule Groups > **New Controller Template**

General

Rule Group Name: RogueAPRule_Grp_Temp1

Edit View

Use the **Add/Remove** buttons to select the Rogue AP rules for this Rule Group. Use the **Move Up/Move Down** buttons to specify the order in which the rules are applied.

All Rogue AP Rules: RogueApRule1

Selected Rogue AP Rules:

Footnotes:

1. Rogue AP Rule(s) can be added from "Rogue AP Rules" section.
2. When NCS apply one Rule Group to the controller, it will delete the controller's existing Rogue AP Rules first and apply the new Rogue AP Rules.

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 group box 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 11-82 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*.

Note The Friendly AP page identifies the MAC address of an access point, status, any comments, and whether or not the alarm is suppressed for this access point.

To view or edit the current list of friendly access points, follow these steps:

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

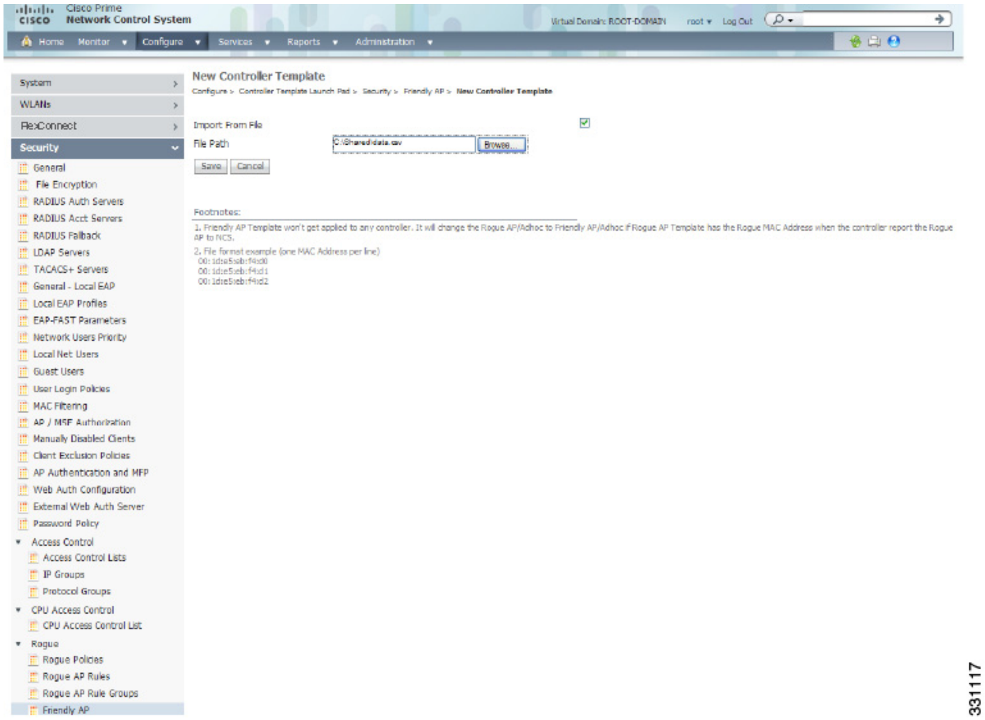
Step 2 Click **Friendly AP** or choose **Security > Rogue > Friendly AP** from the left sidebar menu.

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

Step 4 Click **Go**. The Friendly AP page appears (see Figure 11-44).

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

Figure 11-44 Friendly AP > Add Friendly AP Page



New Controller Template

Configure > Controller Template Launch Pad > Security > Friendly AP > **New Controller Template**

Import From File ☑

File Path: C:\Shared\data.csv

Footnotes:

1. Friendly AP Template won't get applied to any controller. It will change the Rogue AP/Adhoc to Friendly AP/Adhoc if Rogue AP Template has the Rogue MAC Address when the controller report the Rogue AP to NCS.

2. File format example (one MAC Address per line)
00:1d:e5:eb:f4:d0
00:1d:e5:eb:f4:d1
00:1d:e5:eb:f4:d2

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 do the following:
  - Select the **Import from File** check box.
  - Enter the file path or click **Browse** to navigate to the correct file.

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

- To manually add an access point, do the following:
  - Unselect the **Import from File** check box.
  - Enter the MAC address for the access point.
  - Choose **Internal** access point from the Status drop-down list.
  - Enter a comment regarding this access point, if necessary.
  - Select 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 Ignored Rogue AP Templates

The Ignored Rogue AP Template page allows you to create or modify a template for importing ignored access points. Access points in the Ignored AP list are not identified as rogues.

Note An Ignored Rogue AP template does not get applied to any controller. It suppresses the Rogue AP/Adhoc alarm if Ignored Rogue AP Template has the Rogue MAC Address when the controller reports the Rogue AP to the NCS and this MAC address is added to the Rogue AP Ignore-List on the controller.

To add or edit the Ignored Rogue access points, follow these steps:

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

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

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

Step 4 Click **Go**. The Ignored Rogue AP page appears.

Step 5 The Ignored Rogue access points can be added by either importing the access point or manually entering the access point information:

- To import an ignored rogue access point using the Import feature:
  - Select the **Import from File** check box.
  - Enter the file path or use the **Browse** button to navigate to the correct file. The import file must be a CSV file with MAC address (one MAC Address per line).

    Note For example, enter the MAC addresses as follows:
    00:00:11:22:33:44
    00:00:11:22:33:45
    00:00:11:22:33:46

- To manually add an ignored rogue access point:
  - Unselect the **Import from File** check box.
  - Enter the MAC address and comment for the rogue access point.
- Click **Save** to confirm this access point or **Cancel** to close the page without adding the ignored rogue access point to the list.

Note To modify an existing friendly access point, choose **Configure > Controller Template Launch Pad > Security > Rogue >Ignored Rogue AP**, and click the MAC address of the ignored rogue access point. Make the necessary changes, and click **Save**.

Note If you remove the MAC address from the Ignored AP list, the MAC address is removed from the Rogue AP Ignore-List on the controller.

Configuring 802.11 Templates

This section contains the following topics:

- Configuring Load Balancing Templates, page 11-89
- Configuring Band Selection Templates, page 11-89
- Configuring Media Parameters Controller Templates (802.11a/n), page 11-95

Configuring Load Balancing Templates

To configure load balancing templates, follow these steps:

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

Step 2 Click **Load Balancing** or choose **802.11 > Load Balancing** from the left sidebar menu. The Load Balancing page appears.

Step 3 Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing page + client associations on AP with lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 4 Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

Step 5 Click **Save**.

Configuring Band Selection Templates

To configure band selection templates, follow these steps:

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

Step 2 Click **Band Select** or choose **802.11 > Band Select** from the left sidebar menu. The Band Select page appears.

Step 3 Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 4 Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 5 Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 7 Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 8 Click **Save**.

Configuring Preferred Call Templates

This page enables you to create or modify a template for configuring Preferred Call.

To add or modify preferred call templates, follow these steps:

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

Step 2 Click **Preferred Call** or choose **802.11 > Preferred Call** from the left sidebar menu. The Preferred Call Controller Templates page appears.

Step 3 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 New Controller Template page appears.

Step 4 Configure the following Preferred Call parameters:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Number Id—Enter a value to identify the preferred number. You can have a maximum of six preferred call numbers. The valid range is from 1 to 6. The default value is 1.
- Preferred Number—Enter the preferred call number.

Step 5 Click **Save**.

Configuring Media Stream for Controller Templates (802.11)

To configure the media stream for a controller template for an 802.11 Radio, follow these steps:

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

Step 2 In the **802.11** group box, click **New** beside Media Stream. The New Controller Template page appears.

Step 3 In the General group box, specify an appropriate name for the template.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 In the Media Stream Configuration group box, specify the following fields:

- Media Stream Name
- Multicast Destination Start IP—Start IP address of the media stream to be multicast.
- Multicast Destination End IP—End IP address of the media stream to be multicast.

Note Start IP and End IP can be IPv4 or IPv6 multicast address from controller Release 7.2.x.

- Maximum Expected Bandwidth—Maximum bandwidth that a media stream can use.

Step 5 In the Resource Reservation Control (RRC) Parameters group box, specify the following fields:

- Average Packet Size—Average packet size that a media stream can use.
- RRC Periodical Update—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
- RRC Priority—Priority of RRC with the highest at 1 and the lowest at 8.
- Traffic Profile Violation—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
- Policy—Appears if the media stream is admitted or denied.

Step 6 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring RF Profiles Templates (802.11)

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller template for an 802.11 Radio, follow these steps:

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

Step 2 Click **RF Profiles** or choose either **802.11 > RF Profiles** from the left sidebar menu. The RF Profiles page appears.

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

Step 4 Click **Go**. The New Controller template page appears.

Step 5 Configure the following information:

- General
  - Template Name—User-defined name for the template.
  - Profile Name—User-defined name for the current profile.
  - Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.
- TPC (Transmit Power Control)
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. Range: -10 to 30 dBm Default: -10 dBm.

- Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. Range: -10 to 30 dBm Default: 30 dBm.
- Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold.
- Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.

- Data Rates—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

  For each data rate, choose one of these options:
  - Mandatory—Clients must support this data rate to associate to an access point on the controller.
  - Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
  - Disabled—The clients specify the data rates used for communication.

Step 6 Click **Save**.

Configuring Radio Templates (802.11a/n)

This section contains the following topics:

- Configuring 802.11a/n Parameters Templates, page 11-92
- Configuring Media Parameters Controller Templates (802.11a/n), page 11-95
- Configuring EDCA Parameters Through a Controller Template (802.11a/n), page 11-96
- Configuring a Roaming Parameters Template (802.11a/n), page 11-98
- Configuring an 802.11h Template, page 11-99
- Configuring a High Throughput Template (802.11a/n), page 11-100
- Configuring CleanAir Controller Templates (802.11a/n), page 11-101

Configuring 802.11a/n Parameters Templates

To add or modify radio templates, follow these steps:

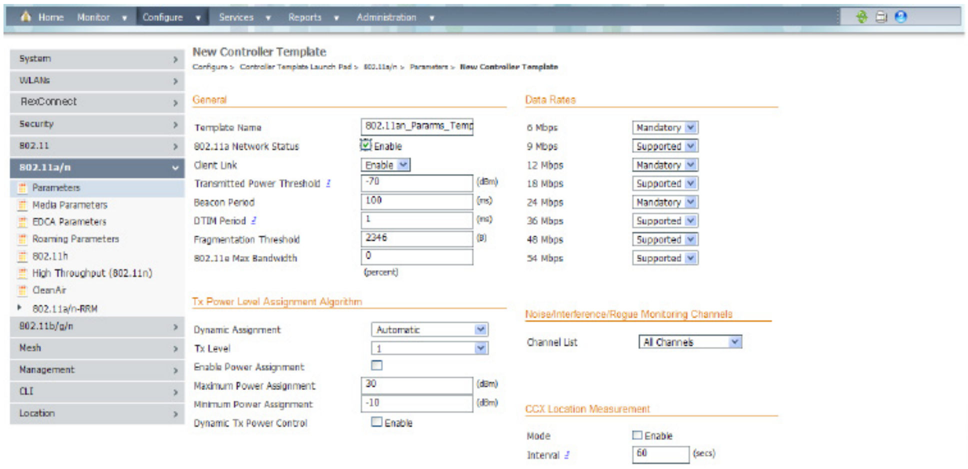
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Parameters** or choose either **802.11a/n > Parameters** from the left sidebar menu. The 802.11a/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, choose **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 Parameters template page appears (see Figure 11-45).

Figure 11-45 802.11a/n Parameters Template



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > Parameters > New Controller Template

General

Template Name: 802.11an_Params_Temp
802.11a Network Status: ☑ Enable
Client Link: Enable
Transmitted Power Threshold: -70 (dBm)
Beacon Period: 100 (ms)
DTIM Period: 1 (ms)
Fragmentation Threshold: 2346 (B)
802.11e Max Bandwidth: 0 (percent)

Tx Power Level Assignment Algorithm

Dynamic Assignment: Automatic
Tx Level: 1
Enable Power Assignment: □
Maximum Power Assignment: 30 (dBm)
Minimum Power Assignment: -10 (dBm)
Dynamic Tx Power Control: □ Enable

Data Rates

6 Mbps: Mandatory
9 Mbps: Supported
12 Mbps: Mandatory
18 Mbps: Supported
24 Mbps: Mandatory
36 Mbps: Supported
48 Mbps: Supported
54 Mbps: Supported

Noise/Interference/Rogue Monitoring Channels

Channel List: All Channels

CCX Location Measurement

Mode: □ Enable
Interval: 60 (secs)

Step 4 Select the check box if you want to enable 802.11a/n network status.

Step 5 Use the ClientLink drop-down list to enable Clientlink on all access point 802.11a/n radios that 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 might 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 In the Fragmentation Threshold field, 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 From 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 Select the **Avoid Foreign AP Interference** check box if you want to enable it. Enable this field to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This Radio Resource Management (RRM) field monitors foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might 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 RRM bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.

In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better reuse 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 RRM noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might 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). RRM constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. 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 to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported 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 From 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 location measurement interval of the Cisco Compatible Extension 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 Media Parameters Controller Templates (802.11a/n)

This page enables you to create or modify a template for configuring 802.11a/n voice fields such as call admission control and traffic stream metrics.

To add a new template with 802.11a/n voice fields information (such as Call Admission Control and traffic stream metrics) for a controller, follow these steps:

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

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

Step 3 Specify an appropriate name for the template.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 On the Voice tab, configure the following fields:

- Admission Control (ACM)—Select the check box to enable admission control.

  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.
- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC 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 CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.
- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP Codec—Specify the codec name you want to use on this radio. The available options are **G.711**, **G.729**, and **User Defined**.
- SIP Call Bandwidth—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
- SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.
- Max Number of Calls per Radio—Specify the maximum number of calls per Radio.

- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which 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 every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 On the Video tab, configure the following fields:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 On the General tab, specify the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click **Save**.

Once saved, the template appears in the Template List page. In the Template List page, you can apply this template to controllers. See the “Applying Controller Templates” section on page 11-2 for more information.

Configuring EDCA Parameters Through a Controller Template (802.11a/n)

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

To add or configure 802.11a/n EDCA parameters through a controller template, follow these steps:

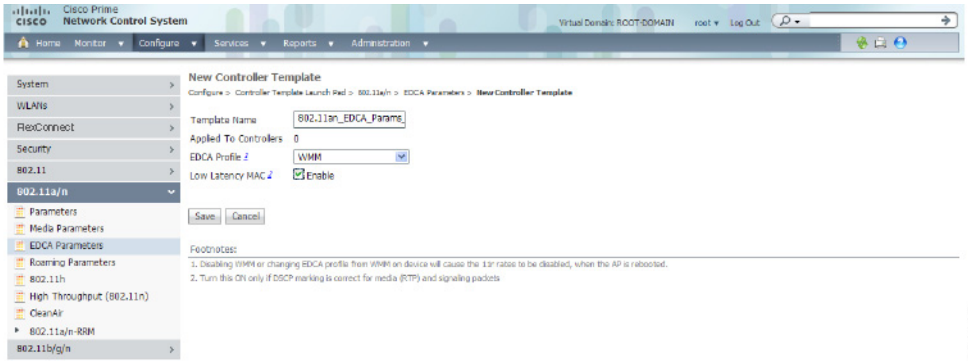
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **EDCA Parameters** or choose **802.11a/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, choose **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 EDCA Parameters template page appears (see Figure 11-46).

Figure 11-46 802.11a EDCA Parameters



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > EDCA Parameters > New Controller Template

Template Name: 802.11an_EDCA_Params_

Applied To Controllers: 0

EDCA Profile [1]: WMM

Low Latency MAC [2]: ☑ Enable

Footnotes:

1. Disabling WMM or changing EDCA profile from WMM on device will cause the 11r rates to be disabled, when the AP is rebooted.
2. Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets

331115

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 Select the **Low Latency MAC** check box to enable this feature.

Note Enable low latency MAC only if all clients on the network are WMM compliant.

Configuring a Roaming Parameters Template (802.11a/n)

To add or modify an existing roaming parameter template, follow these steps:

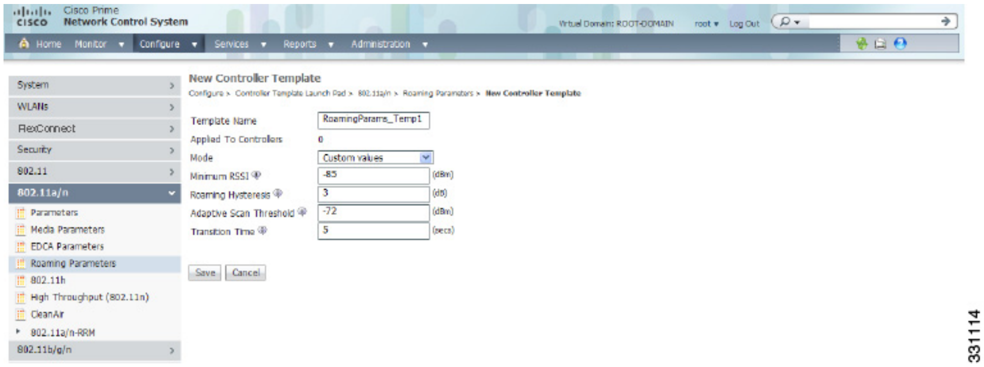
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Roaming Parameters** or choose **802.11a/n > Roaming Parameters** from the left sidebar menu. The Roaming 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 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, choose **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 Roaming Parameters template page appears (see Figure 11-47).

Figure 11-47 802.11a/n Roaming Parameters Template



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > Roaming Parameters > New Controller Template

Template Name	RoamingParams_Temp1	
Applied To Controllers	0	
Mode	Custom values	
Minimum RSSI	-85	(dBm)
Roaming Hysteresis	3	(dB)
Adaptive Scan Threshold	-72	(dBm)
Transition Time	5	(secs)

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 average received signal power of the client 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 field 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: 2 dB

Step 7 In the Adaptive Scan Threshold field, enter the RSSI value from the associated access point of the client, below which the client must be able to roam to a neighboring access point within the specified transition time. This field 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 associated access point of the client 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 802.11h Template

802.11h informs client devices about channel changes and can limit the transmit power of the client device. 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.

To add or modify an 802.11h template, follow these steps:

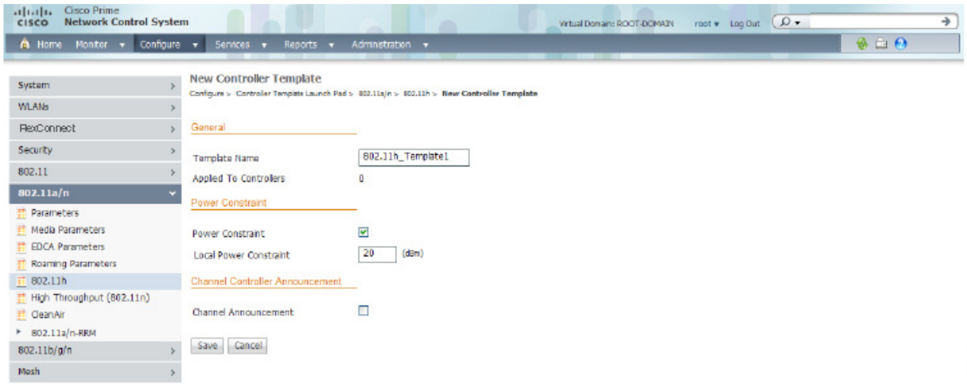
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **802.11h** or choose **802.11a/n > 802.11h** from the left sidebar menu.The 802.11h Template page 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, choose **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 11-48).

Figure 11-48 802.11h Template



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > 802.11h > New Controller Template

General

Template Name: 802.11h_Template1

Applied To Controllers: 0

Power Constraint

Power Constraint: ☑

Local Power Constraint: 20 (dBm)

Channel Controller Announcement

Channel Announcement: □

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

Step 5 Select 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 (802.11a/n)

To add or modify to an 802.11a/n high throughput template, follow these steps:

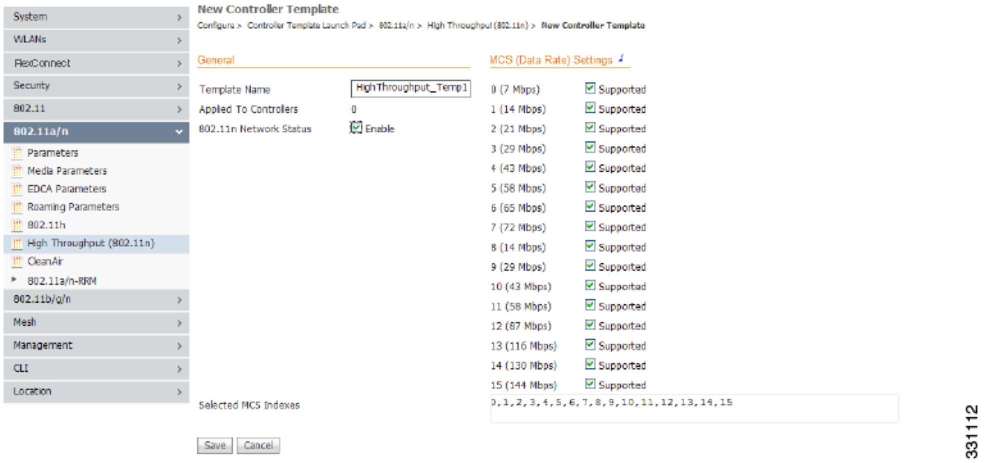
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **High Throughput (802.11n)** or choose **802.11a/n > High Throughput** from the left sidebar menu. The 802.11n Parameters for 2.4 GHz or 802.11n Parameters for 5 GHz 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 802.11n 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, choose **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 High Throughput template page appears (see Figure 11-49).

Figure 11-49 802.11a/n High Throughput Template



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > High Throughput (802.11n) > New Controller Template

General

Template Name: HighThroughput_Temp1

Applied To Controllers: 0

802.11n Network Status: ☑ Enable

MCS (Data Rate) Settings

0 (7 Mbps)	☑ Supported
1 (14 Mbps)	☑ Supported
2 (21 Mbps)	☑ Supported
3 (29 Mbps)	☑ Supported
4 (43 Mbps)	☑ Supported
5 (58 Mbps)	☑ Supported
6 (65 Mbps)	☑ Supported
7 (72 Mbps)	☑ Supported
8 (14 Mbps)	☑ Supported
9 (29 Mbps)	☑ Supported
10 (43 Mbps)	☑ Supported
11 (58 Mbps)	☑ Supported
12 (87 Mbps)	☑ Supported
13 (116 Mbps)	☑ Supported
14 (130 Mbps)	☑ Supported
15 (144 Mbps)	☑ Supported

Selected MCS Indexes: 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Step 4 Select 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 (802.11a/n)

Create or modify a template for configuring CleanAir parameters for the 802.11a/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.

To add a new template with 802.11a/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**. The 802.11a/n CleanAir Controller Templates page displays all currently saved 802.11a/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 Configure the following fields:

- 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 group boxes appear.

- Reporting Configuration—Use the fields in this group box 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 selected.

  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 group box 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 appears in the Template List page. In the Template List page, you can apply this template to controllers. See the "Configuring Controller Templates" section on page 11-4 for more information.

Configuring 802.11a/n RRM Templates

This section contains the following topics:

Configuring an RRM Threshold Template (802.11a/n)

To add or make modifications to an 802.11a/n or 802.11b/g/n RRM threshold template, follow these steps:

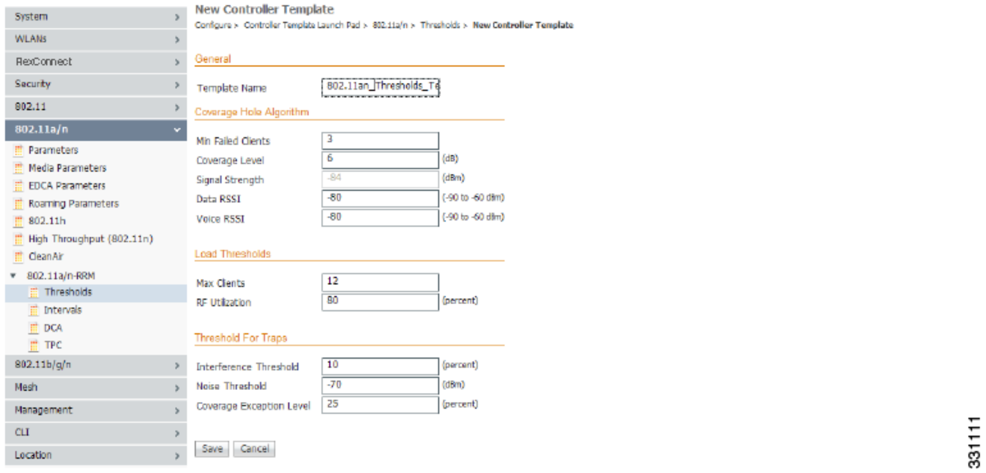
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **RRM Thresholds** or choose **802.11a/n > RRM Thresholds**. The 802.11a/n RRM Thresholds 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 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, choose **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 RRM Threshold template page appears (see Figure 11-50).

Figure 11-50 802.11a/n RRM Thresholds Template



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > Thresholds > New Controller Template

General

Template Name: 802.11an_Thresholds_Te

Coverage Hole Algorithm

Min Failed Clients: 3
Coverage Level: 6 (dB)
Signal Strength: -84 (dBm)
Data RSSI: -80 (-90 to -60 dBm)
Voice RSSI: -80 (-90 to -60 dBm)

Load Thresholds

Max Clients: 12
RF Utilization: 80 (percent)

Threshold For Traps

Interference Threshold: 10 (percent)
Noise Threshold: -70 (dBm)
Coverage Exception Level: 25 (percent)

Save Cancel

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 network before applying these RRM threshold fields.

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 In the RF Utilization text box, enter the percentage of threshold for 802.11a/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 the NCS.

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 (802.11a/n)

To add or make modifications to an 802.11a/n RRM interval template, follow these steps:

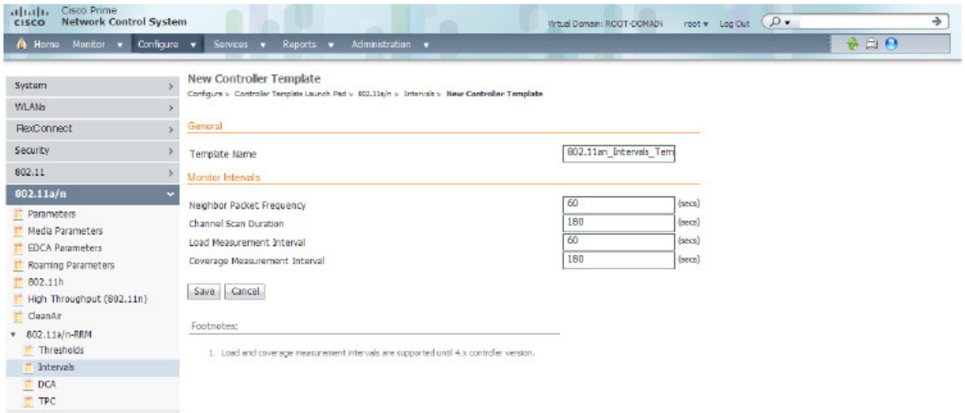
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click RRM Intervals or choose **802.11a/n > RRM Intervals** from the left sidebar menu. The 802.11a/n or 802.11b/g/n RRM Threshold 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 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, choose **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 11-51).

Figure 11-51 802.11a/n RRM Intervals Template



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > Intervals > New Controller Template

General

Template Name: 802.11an_Intervals_Tem

Monitor Intervals

Neighbor Packet Frequency: 60 (secs)
Channel Scan Duration: 180 (secs)
Load Measurement Interval: 60 (secs)
Coverage Measurement Interval: 180 (secs)

Footnotes:

1. Load and coverage measurement intervals are supported until 4.x controller version.

Step 4 In the Neighbor Packet Frequency text box, 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 field, enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 8 Click **Save**.

Configuring an RRM Dynamic Channel Allocation Template (802.11a/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA template, follow these steps:

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

Step 2 Click **DCA** or choose **802.11a/n > DCA**. The 802.11a/n DCS 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, choose **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 TPC template page appears.

Step 4 Configure the following fields:

- Template Name—Enter the template name.
- **Assignment Mode**—From 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 you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Select the **Avoid Foreign AP Interference** check box to enable it. Enable this check box 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. Unselect this check box to have RRM ignore this interference.

  In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might 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.
- Select the **Avoid Cisco AP Load** check box if you want it enabled. Enable this bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value.

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

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

  In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might 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.
- The Signal Strength Contribution check box is always enabled (not configurable). This constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.
- Enable or disable event-driven Radio Resource Management (RRM) using the following fields. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.
  - Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 5 Click **Save**.

Configuring an RRM Transmit Power Control Template (802.11a/n)

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access points according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11a/n RRM TPC template, follow these steps:

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

Step 2 Click **TPC** or choose **802.11a/n > TPC**. The 802.11a/n TPC 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, choose **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 TPC template page appears.

Step 4 Configure the following fields:

- Template Name—Enter the template name in the text box.
- TPC Version—Choose TPCv1 or TPCv2.

Note The TPCv2 option is applicable only for those controllers running Release 7.2.x or later.

- Dynamic Assignment—From 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 you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring Radio Templates (802.11b/g/n)

This section contains the following topics:

- Configuring 802.11b/g/n Parameters Templates, page 11-108
- Configuring Media Parameters Controller Templates (802.11b/g/n), page 11-110
- Configuring EDCA Parameters Controller Templates (802.11b/g/n), page 11-112
- Configuring Roaming Parameters Controller Templates (802.11b/g/n), page 11-113
- Configuring High Throughput (802.11n) Controller Templates (802.11b/g/n), page 11-114
- Configuring CleanAir Controller Templates (802.11 b/g/n), page 11-115

- Configuring 802.11b/g/n RRM Templates, page 11-116

Configuring 802.11b/g/n Parameters Templates

Create or modify a template for configuring 802.11b/g/n parameters (such as power and channel status, data rates, channel list, and CCX location measurement) and/or applying these settings to controller(s).

To add a new template with 802.11b/g/n parameters information for a controller, follow these steps:

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

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

Step 3 Configure the following General parameters:

- Policy Name—Security policy in force.
- 802.11b/g Network Status
- Beam Forming—Choose **Enable** or **Disable** from the drop-down list.

Note Beam forming refers to a general signal processing technique used to control the directionality of the reception or transmission of a signal.

- Transmitted Power Threshold—The valid range is from -50 to -80.
- Beacon Period—The rate at which the SSID is broadcast by the access point (the amount of time between beacons). The valid range is from 100 to 600 milliseconds.
- DTIM Period—The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field 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.

Note DTIM period is not applicable in controller Release 5.0.0.0 and later.

- Fragmentation Threshold—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. The default value is 2346.
- 802.11e Max Bandwidth—Percentage for 802.11e max bandwidth. The default value is 100.

Step 4 Configure the following 802.11b/g Power Status parameters:

- Dynamic Assignment—From the Dynamic Assignment drop-down list, choose any one of the following dynamic transmit power assignment modes.
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur and values are set to their global default. The default is Automatic.

Note The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

- Dynamic Tx Power Control—Select this check box to enable DTPC support. If this option is enabled, the transmit power level of the radio is advertised in the beacons and the probe responses.

Step 5 Configure the following 802.11b/g Channel Status parameters:

- Assignment Mode—From the Assignment Mode drop-down list, choose any one of the following dynamic channel assignment modes.
  - **Automatic**—The channel assignment is periodically updated for all access points that permit this operation.
  - **On Demand**—Channel assignments are updated when desired.
  - **Disabled**—No dynamic channel assignments occur and values are set to their global default.

  Note The default is Automatic.

- Avoid Foreign AP Interference—Enable this Radio Resource Management (RRM) foreign 802.11 interference-monitoring parameter to have Radio Resource Management consider interference from foreign (non-Cisco access points outside the RF/mobility domain) access points when assigning channels to Cisco access points.

  Disable this field to have Radio Resource Management ignore this interference.

  Note In certain circumstances with significant interference energy (dB) and load (utilization) from Foreign access points, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in Cisco access points close to the Foreign access points to increase capacity and reduce variability for the Cisco WLAN Solution.

- Avoid Cisco AP Load—Enable this Radio Resource Management (RRM) bandwidth-sensing parameter to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points.

  Disable this field to have Radio Resource Management ignore this value.

  Note In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel re-use. In these circumstances, Radio Resource Management can assign better re-use patterns to those APs that carry more traffic load.

- Avoid non 802.11 Noise—Enable this Radio Resource Management (RRM) noise-monitoring field to have access points avoid channels that have interference from non-Access Point sources, such as microwave ovens or Bluetooth devices.

  Disable this field to have Radio Resource Management ignore this interference.

Note In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability for the Cisco WLAN Solution.

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

Step 6 Configure the Data Rate parameters.

The data rates set are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. But it is not required that a client be able to use all the rates marked Supported to associate 6, 9, 12, 18, 24, 36, 48, 54 Mbps. For each rate, a drop-down list selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

Step 7 Configure the Noise/Interference/Rogue Monitoring Channels parameters.

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 among a set of managed devices connected to the controller.

Step 8 Configure the CCX Location Measurement parameters:

- Mode—Enable or disable the broadcast radio measurement request. When enabled, this enhances the location accuracy of clients.
- Interval—Interval in seconds between requests.

Note Cisco Compatible Extension location measurement interval can be changed only when measurement mode is enabled.

Step 9 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring Media Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n voice parameters such as Call Admission Control and traffic stream metrics.

To add a new template with 802.11b/g/n voice parameters information (such as Call Admission Control and traffic stream metrics) for a controller, follow these steps:

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

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

Step 3 Specify an appropriate name for the template.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 On the Voice tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

  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.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  Load-based CAC 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 CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

- Maximum Bandwidth Allowed—Enter the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Enter the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Choose the codec name you want to use on this radio from the SIP Codec drop-don list. The available options are G.711, G.729, and User Defined.
- SIP Call Bandwidth—Enter the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
- SIP Sample Interval—Enter the sample interval in milliseconds that the codec must operate in.
- Max Number of Calls per Radio—Enter the maximum number of calls per radio.
- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which 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 every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 On the Video tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 On the General tab, specify the following field:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring EDCA Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring 802.11b/g/n EDCA parameters. EDCA parameters designate pre-configured profiles at the MAC layer for voice and video.

To add a new template with 802.11b/g/n EDCA parameters information for a controller, follow these steps:

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

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

Step 3 Configure the following parameters:

- Template Name

  Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- EDCA Profile—Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

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

- Streaming MAC—Only enable streaming MAC if all clients on the network are WMM compliant.

Step 4 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring Roaming Parameters Controller Templates (802.11b/g/n)

Create or modify a template for configuring roaming parameters for 802.11b/g/n radios.

To add a new template with 802.11b/g/n Roaming parameters information for a controller, follow these steps:

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

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

Step 3 Configure the following parameters:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Mode—Choose **Default Values** or **Custom Values** from the drop-down list.
  - Default Values—The roaming parameters are unavailable and the default values are displayed.
  - Custom Values—The following roaming parameters can be edited.
- Minimum RSSI—Enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.

  If the client 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
- Roaming Hysteresis—Enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it. This field 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: 2 dB
- Adaptive Scan Threshold—Enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This field 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

- Transition Time—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 associated access point is below the scan threshold.
  - Range: 1 to 10 seconds
  - Default: 5 seconds

Note 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.

Step 4 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring High Throughput (802.11n) Controller Templates (802.11b/g/n)

Create or modify a template for configuring high-throughput parameters such as MCS (data rate) settings and indexes and for applying these 802.11n settings to multiple controllers.

To add a new template with High Throughput (802.11n) information for a controller, follow these steps:

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

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

Step 3 Configure the following fields:

- Template Name

  Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- 802.11n Network Status—Select the check box to enable high throughput.
- MCS (Data Rate) Settings—Choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate.

  Note As a default, 20 MHz and short guarded interval are used.

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

Step 4 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring CleanAir Controller Templates (802.11 b/g/n)

Create or modify a template for configuring CleanAir parameters for the 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.

To add a new template with 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 **802.11b/g/n > CleanAir**. The 802.11b/g/n CleanAir Controller Templates page displays all currently saved 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 Configure the following fields:

- Template Name—Enter the template name in the text box.
- 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. The default value is selected.

Note If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.

- Reporting Configuration—Use the parameters in this group box 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 selected.
  - 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 group box 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 text box 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 unselected 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 the "Adding Controller Templates" section on page 11-2 for more information.

Configuring 802.11b/g/n RRM Templates

This section contains the following topics:

- Configuring RRM Thresholds Controller Templates (802.11b/g/n), page 11-116
- Configuring RRM Intervals Controller Templates (802.11b/g/n), page 11-117
- Configuring an RRM Dynamic Channel Allocation Template (802.11b/g/n), page 11-118
- Configuring an RRM Transmit Power Control Template (802.11b/g/n), page 11-119

Configuring RRM Thresholds Controller Templates (802.11b/g/n)

Create or modify a template for setting various RRM thresholds such as load, interference, noise, and coverage.

To add a new template with 802.11b/g/n RRM thresholds information for a controller, follow these steps:

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

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

Step 3 Add or modify the following template name.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 Configure the following Coverage Hole Algorithm parameters:

- Min. Failed Clients (#)—Enter the minimum number of failed clients currently associated with the controller.
- Coverage Level—Enter the target range of coverage threshold (dB).

- Signal Strength—When the Coverage Level field is adjusted, the value of the Signal Strength (dBm) automatically reflects this change. The Signal Strength field provides information regarding what the signal strength is when adjusting the coverage level.
- Data RSSI—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.
- Voice RSSI—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 5 Configure the following Load Thresholds parameters:

- Max. Clients—Enter the maximum number of clients able to be associated with the controller.
- RF Utilization—Enter the percentage of threshold for this radio type.

Step 6 Configure the following Threshold for Traps parameters:

- Interference Threshold—Enter an interference threshold between 0 and 100 percent.
- Noise Threshold—Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to the NCS.
- Coverage Exception Level—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 7 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring RRM Intervals Controller Templates (802.11b/g/n)

Create or modify a template for configuring RRM intervals for 802.11b/g/n radios.

To add a new template with 802.11b/g/n RRM intervals information for a controller, follow these steps:

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

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

Step 3 Configure the following parameters:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Neighbor Packet Frequency—Enter at which interval you want strength measurements taken for each access point. The default is 300 seconds.
- Noise Measurement Interval—Enter at which interval you want noise and interference measurements taken for each access point. The default is 180 seconds.
- Load Measurement Interval—Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.

- Channel Scan Duration—Enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 4 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 the "Applying Controller Templates" section on page 11-2 for more information.

Configuring an RRM Dynamic Channel Allocation Template (802.11b/g/n)

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels, which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11b/g/n RRM DCA template, follow these steps:

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

Step 2 Click **DCA** or choose **802.11b/g/n > DCA**. The 802.11b/g/n DCS 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, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11b/g/n TPC template page appears.

Step 4 Configure the following parameters:

- Template Name—Enter the template name.
- Assignment Mode—From 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 you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Select the **Avoid Foreign AP Interference** check box to enable it. Enable this field 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. Unselect this check box to have RRM ignore this interference.

In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might 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.

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

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

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

  In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might 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.

- 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.

- Enable or disable event-driven Radio Resource Management (RRM) using the following parameters. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.
  - Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 5 Click **Save**.

Configuring an RRM Transmit Power Control Template (802.11b/g/n)

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of an access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points.

This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11b/g/n RRM TPC template, follow these steps:

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

Step 2 Click **TPC** or choose **802.11b/g/n > TPC**. The 802.11b/g/n TPC 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, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The 802.11b/g/n TPC template page appears.

Step 4 Configure the following parameters:

- Template Name—Enter the template name in the text box.
- TPC Version—Choose TPCv1 or TPCv2 from the drop-down list.

Note The TPCv2 option is applicable only for those controller Release 7.2.x or later.

- Dynamic Assignment—From 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 you click **Assign Now**.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring Mesh Templates

Configuring Mesh Setting Templates

You can configure an access point to establish a connection with the controller.

To add or modify a mesh template, follow these steps:

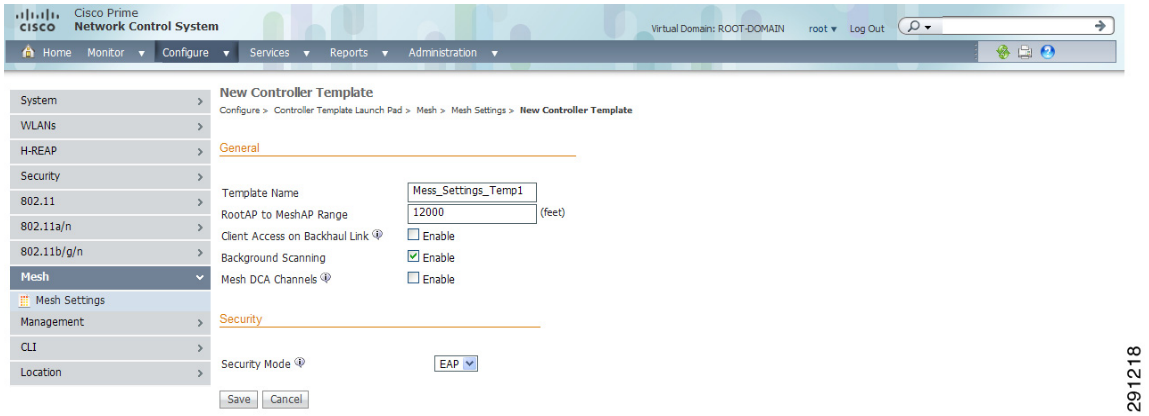
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-52).

Figure 11-52 Mesh Configuration Template



New Controller Template

Configure > Controller Template Launch Pad > Mesh > Mesh Settings > **New Controller Template**

General

Template Name: Mess_Settings_Temp1

RootAP to MeshAP Range: 12000 (feet)

Client Access on Backhaul Link: □ Enable

Background Scanning: ☑ Enable

Mesh DCA Channels: □ Enable

Security

Security Mode: EAP

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 field 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 selected 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 9-54 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 Management Templates

This section contains the following topics:

- Configuring Trap Receiver Templates, page 11-122
- Configuring Trap Control Templates, page 11-123
- Configuring Telnet SSH Templates, page 11-125
- Configuring Legacy Syslog Templates, page 11-126
- Configuring Multiple Syslog Templates, page 11-127
- Configuring Local Management User Templates, page 11-128
- Configuring User Authentication Priority Templates, page 11-129

Configuring Trap Receiver Templates

If you have monitoring devices on your network that receive SNMP traps, you might want to add a trap receiver template.

To add or modify a trap receiver template, follow these steps:

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

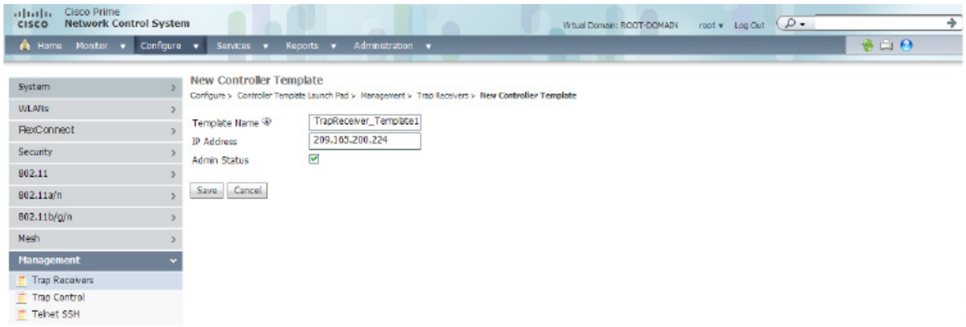
Step 2 Click **Trap Receivers** or choose **Management > Trap Receivers** from the left sidebar menu.

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, choose **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 11-53).

Figure 11-53 Trap Receivers Template



New Controller Template

Configure > Controller Template Launch Pad > Management > Trap Receivers > New Controller Template

Template Name: TrapReceiver_Template1

IP Address: 209.165.200.224

Admin Status: ☑

Step 5 Enter the IP address of the server in the text box.

Step 6 Select the **Admin Status** check box to enable the administrator status if you want SNMP traps to be sent to the receiver.

Step 7 Click **Save**.

Configuring Trap Control Templates

To add or modify a trap control template, follow these steps:

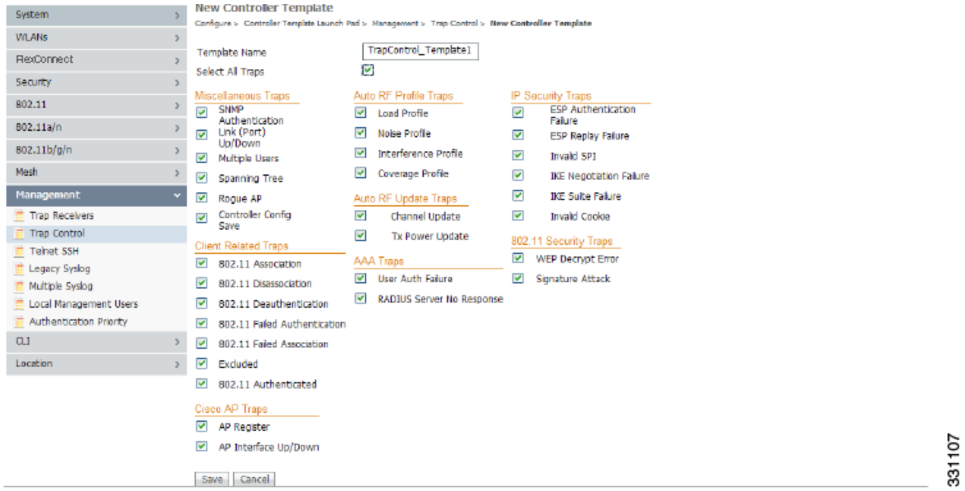
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-54).

Figure 11-54 Trap Control Template



New Controller Template

Configure > Controller Template Launch Pad > Management > Trap Control > **New Controller Template**

Template Name: TrapControl_Template1

Select All Traps ☑

Miscellaneous Traps

- ☑ SNMP Authentication
- ☑ Link (Port) Up/Down
- ☑ Multiple Users
- ☑ Spanning Tree
- ☑ Rogue AP
- ☑ Controller Config Save

Client Related Traps

- ☑ 802.11 Association
- ☑ 802.11 Disassociation
- ☑ 802.11 Deauthentication
- ☑ 802.11 Failed Authentication
- ☑ 802.11 Failed Association
- ☑ Excluded
- ☑ 802.11 Authenticated

Cisco AP Traps

- ☑ AP Register
- ☑ AP Interface Up/Down

Auto RF Profile Traps

- ☑ Load Profile
- ☑ Noise Profile
- ☑ Interference Profile
- ☑ Coverage Profile

Auto RF Update Traps

- ☑ Channel Update
- ☑ Tx Power Update

AAA Traps

- ☑ User Auth Failure
- ☑ RADIUS Server No Response

IP Security Traps

- ☑ ESP Authentication Failure
- ☑ ESP Replay Failure
- ☑ Invalid SPI
- ☑ IKE Negotiation Failure
- ☑ IKE Suite Failure
- ☑ Invalid Cookie

802.11 Security Traps

- ☑ WEP Decrypt Error
- ☑ Signature Attack

Step 4 Select 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 Select 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 Select 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 Select 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 Select the appropriate check box to enable any of the following auto RF update traps:

- Channel Update—Notification sent when the dynamic channel algorithm of an access point is updated.
- Tx Power Update—Notification sent when the dynamic transmit power algorithm of an access point is updated.

Step 9 Select 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 Select 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 Select 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 Telnet SSH Templates

To add or modify a Telnet SSH configuration template, follow these steps:

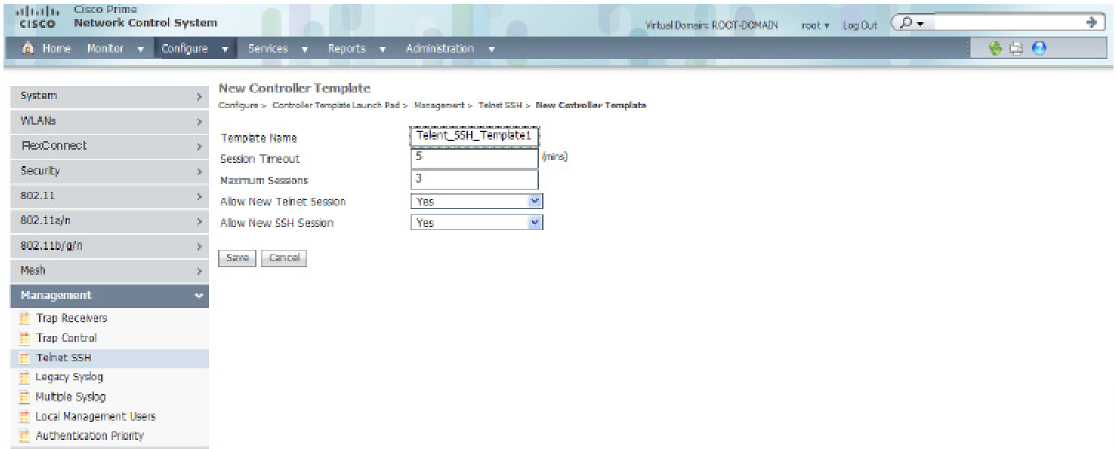
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-55).

Figure 11-55 Telnet SSH Template



New Controller Template

Configure > Controller Template Launch Pad > Management > Telnet SSH > New Controller Template

Template Name: Telent_SSH_Template1
Session Timeout: 5 (mins)
Maximum Sessions: 3
Allow New Telnet Session: Yes
Allow New SSH Session: Yes

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 field, 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 Legacy Syslog Templates

To add or modify a legacy syslog configuration template, follow these steps:

Note Legacy Syslog applies to controllers Release 5.0.6.0 and earlier.

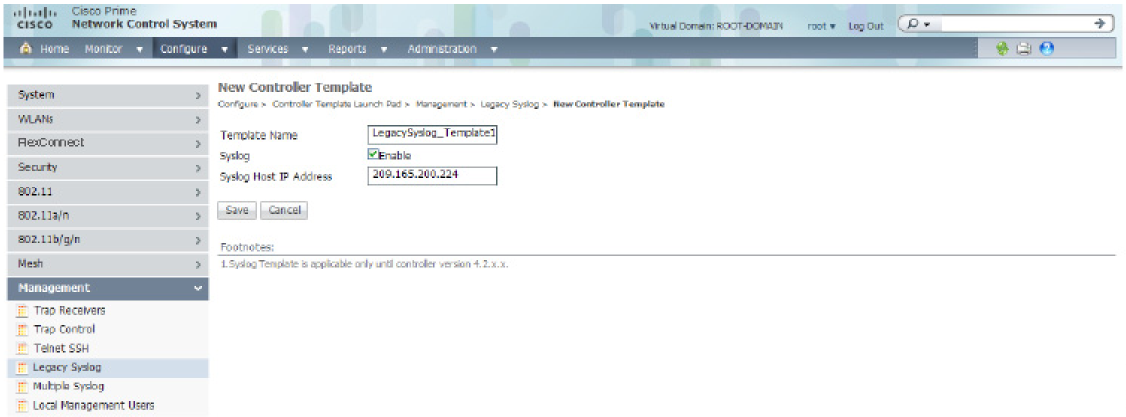
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-56).

Figure 11-56 Legacy Syslog Template



New Controller Template

Configure > Controller Template Launch Pad > Management > Legacy Syslog > New Controller Template

Template Name: LegacySyslog_Template1

Syslog: ☑ Enable

Syslog Host IP Address: 209.165.200.224

Footnotes:

1.Syslog Template is applicable only until controller version 4.2.x.x.

Step 4 Enter a template name. The number of controllers to which this template is applied is displayed.

Step 5 Select the **Syslog** check box to enable syslog. When you do, a Syslog Host IP Address text box appears.

Step 6 Click **Save**.

Configuring Multiple Syslog Templates

To add or modify a multiple syslog configuration template, follow these steps:

Note You can enter up to three syslog server templates.

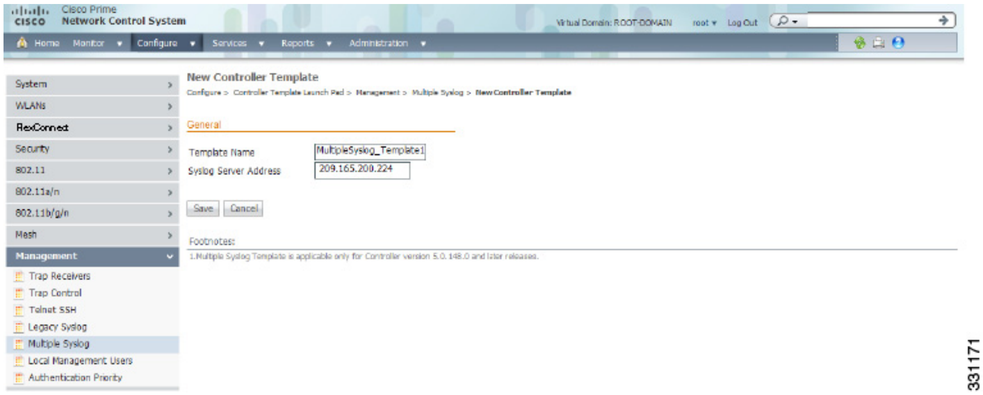
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-57).

Figure 11-57 Multiple Syslog Template Page



New Controller Template

Template Name: MultipleSyslog_Template1

Syslog Server Address: 209.165.200.224

Footnotes:
1.Multiple Syslog Template is applicable only for Controller version 5.0.148.0 and later releases.

Step 4 Enter a template name and a syslog server IP address in the text boxes.

Step 5 Click **Save**.

Configuring Local Management User Templates

To add or modify a local management user template, follow these steps:

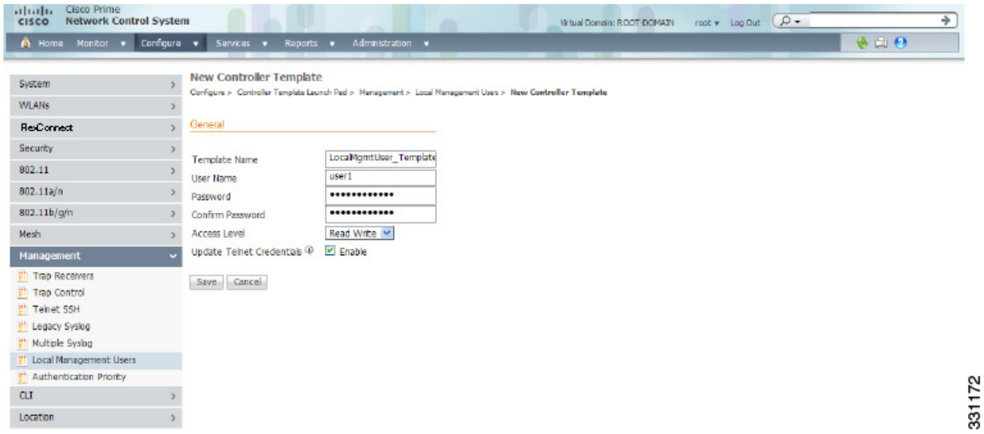
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Local Management Users** or choose **Management > Local Management Users** from the left sidebar menu. The Management > Local Management Users Template page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the username 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, choose **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 11-58).

Figure 11-58 Local Management Users Template



New Controller Template

Configure > Controller Template Launch Pad > Management > Local Management Users > New Controller Template

General

Template Name: LocalMgmtUser_Template

User Name: user1

Password: ••••••••••••

Confirm Password: ••••••••••••

Access Level: Read Write

Update Telnet Credentials: ☑ Enable

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 Reenter the password.

Step 8 Use the Access Level drop-down list to choose either **Read Only** or **Read Write**.

Step 9 Select the **Update Telnet Credentials** check box to update the user credentials in the NCS for Telnet/SSH access.

Note If the template is applied successfully and the Update Telnet Credentials option is enabled, the applied management user credentials are used in the NCS for Telnet/SSH credentials to that applied controller.

Step 10 Click **Save**.

Configuring User Authentication Priority Templates

Management user authentication priority templates control the order in which authentication servers are used to authenticate the management users of a controller.

To add a user authentication priority template or make modifications to an existing template, follow these steps:

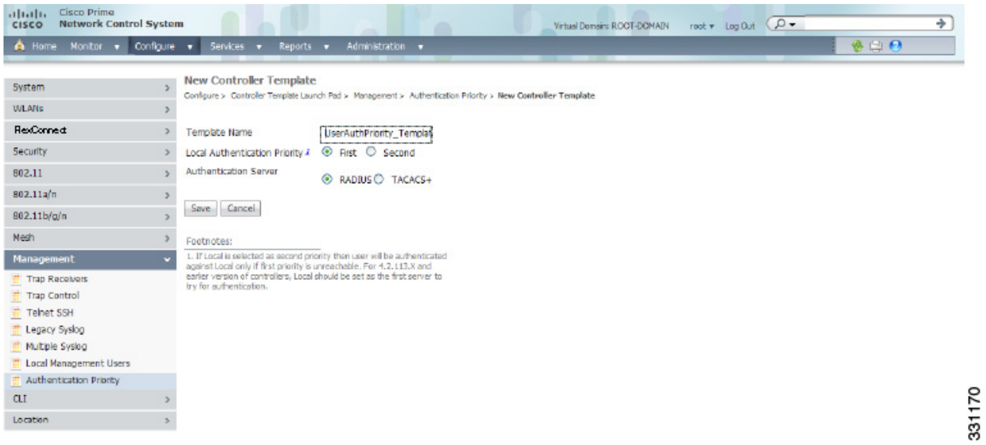
Step 1 Choose **Configure > Controller Template Launch Pad**.

Step 2 Click **Authentication Priority** or choose **Management > Authentication Priority** from the left sidebar menu. The Management > Local Management Users Template page 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, choose **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 11-59).

Figure 11-59 User Authentication Priority Template



New Controller Template

Configure > Controller Template Launch Pad > Management > Authentication Priority > New Controller Template

Template Name: UserAuthPriority_Templat

Local Authentication Priority[1]: ● First ○ Second

Authentication Server: ● RADIUS ○ TACACS+

Footnotes:

1. If Local is selected as second priority then user will be authenticated against Local only if first priority is unreachable. For 4.2.113.X and earlier version of controllers, Local should be set as the first server to try for authentication.

Step 4 Enter a template name.

Step 5 The local server is tried first. Choose either **RADIUS** or **TACACS+** from the drop-down list to try if local authentication fails.

Step 6 Click **Save**.

Configuring CLI Templates

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 the NCS. These templates are meant for provisioning features in multiple controllers for which there is no SNMP support or custom NCS 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 "Configuring Protocols for CLI Sessions" section on page 15-58 for information on setting protocol user preferences.

To add or modify a CLI template, follow these steps:

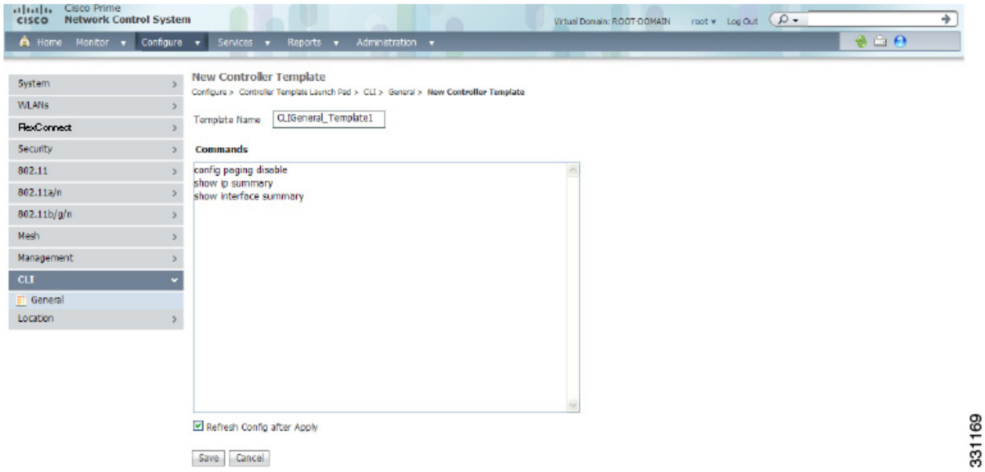
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **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 11-60).

Figure 11-60 Command-Line Interface Template



New Controller Template

Configure > Controller Template Launch Pad > CLI > General > **New Controller Template**

Template Name: CLIGeneral_Template1

Commands

```
config paging disable
show ip summary
show interface summary
```

☑ Refresh Config after Apply

Step 4 If you are adding a new template, provide a name that you are giving to this string of commands in the text box. If you are making modifications to an existing template, the Template Name text box cannot be modified.

Step 5 In the Commands page, enter the series of CLI commands.

Step 6 Select the **Refresh Config after Apply** check box to perform a refresh config on the controller after the CLI template is applied successfully.

Step 7 Click **Save** to save the CLI commands to the NCS database without applying to the selected controllers or **Apply to Controllers** to save the commands to the NCS 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 Configuration Templates

To add or modify a location setting template, follow these steps:

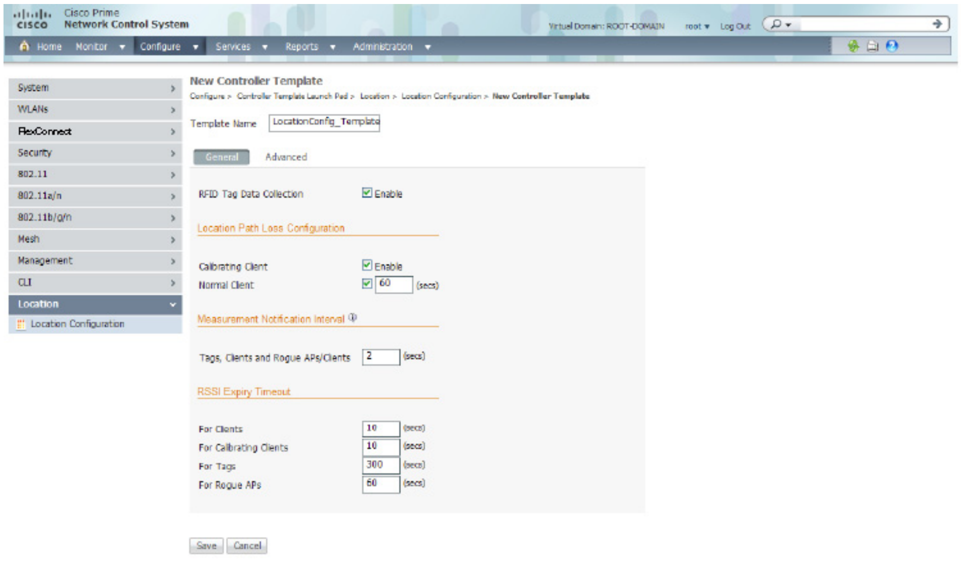
Step 1 Choose **Configure > Controller Template Launch Pad**.

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, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The Location Configuration template page appears (see Figure 11-61).

Figure 11-61 Location Configuration Template



New Controller Template

Configure > Controller Template Launch Pad > Location > Location Configuration > New Controller Template

Template Name: LocationConfig_Template

RFID Tag Data Collection ☑ Enable

Location Path Loss Configuration

Calibrating Client ☑ Enable

Normal Client ☑ 60 (secs)

Measurement Notification Interval

Tags, Clients and Rogue APs/Clients 2 (secs)

RSSI Expiry Timeout

For Clients 10 (secs)

For Calibrating Clients 10 (secs)

For Tags 300 (secs)

For Rogue APs 60 (secs)

Step 4 Select the **RFID Tag Data Collection** check box to enable tag collection. Before the mobility services engine 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 Select 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 Select the **Normal Client** check box to have a non-calibrating client. No S36 requests are transmitted to the client.

Note S36 and S60 are client drivers compatible with specific Cisco Compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see the following URL:
http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml

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 Select the **Calibrating Client Multiband** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled in the General group box.

Step 15 Click **Save**.

Configuring IPv6 Templates

This section contains the following topics:

- Configuring Neighbor Binding Timers Templates, page 11-133
- Configuring RA Throttle Policy Templates, page 11-135
- Configuring RA Guard Templates, page 11-136

Configuring Neighbor Binding Timers Templates

You can create or modify a template for configuring IPv6 Router Neighbor Binding Timers such as Down Lifetime, Reachable Lifetime, State Lifetime, and corresponding intervals.

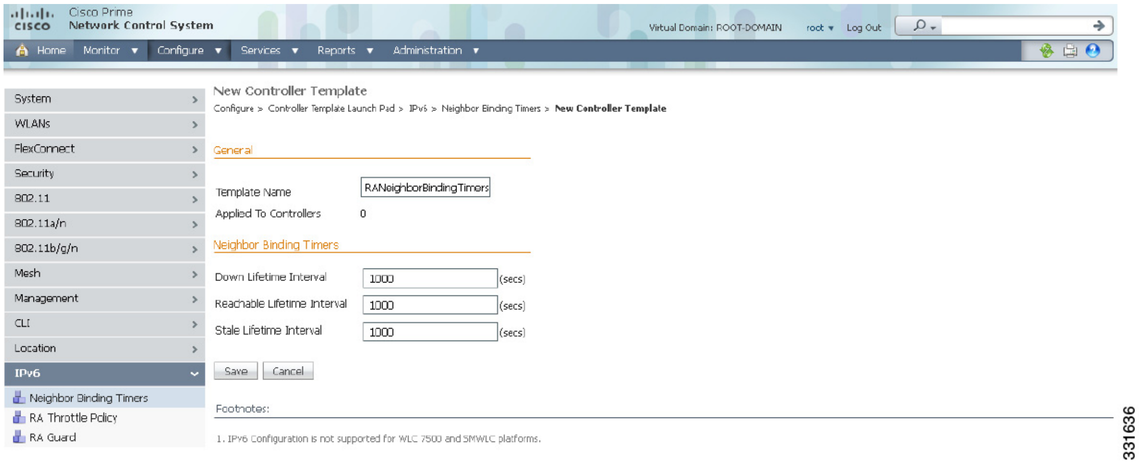
To configure a Neighbor Binding Timers template, follow these steps:

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

Step 2 Click **Neighbor Binding Timers** or choose **IPv6 > Neighbor Binding Timers** from the left sidebar menu. The IPv6 > Neighbor Binding Timers page appears.

Step 3 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 Neighbor Binding Timers template page appears (see Figure 11-61).

Figure 11-62 Neighbor Binding Timers Template



New Controller Template

Configure > Controller Template Launch Pad > IPv6 > Neighbor Binding Timers > **New Controller Template**

General

Template Name: RANeighborBindingTimers

Applied To Controllers: 0

Neighbor Binding Timers

Down Lifetime Interval: 1000 (secs)

Reachable Lifetime Interval: 1000 (secs)

Stale Lifetime Interval: 1000 (secs)

Footnotes:

1. IPv6 Configuration is not supported for WLC 7500 and SMWLC platforms.

Step 4 Enter a template name in the text box.

Step 5 If you want to enable the down lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Down Lifetime Interval text box. This indicates the maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.The range is 0 to 86,400 seconds, and the default value is 0.

Step 6 If you want to enable the reachable lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Reachable Lifetime Interval text box. This indicates the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale.The range is 0 to 86,400 seconds, and the default value is 0.

Step 7 If you want to enable the stale lifetime, select the **Enable** check box. If you have selected this check box, specify the value in the Stale Lifetime Interval text box. This indicates the maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.The range is 0 to 86,400 seconds, and the default value is 0.

Step 8 Click **Save**.

Configuring RA Throttle Policy Templates

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network. You can create or modify a template for configuring IPv6 Router Advertisement parameters such as RA Throttle Policy, Throttle Period, and other options.

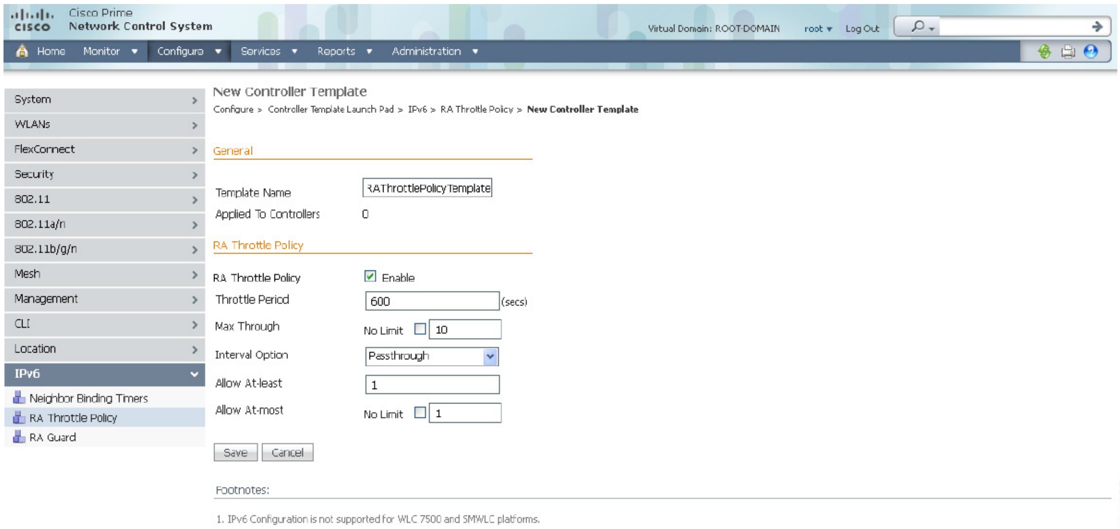
To configure a RA Throttle Policy template, follow these steps:

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

Step 2 Click **RA Throttle Policy** or choose **IPv6 > RA Throttle Policy** from the left sidebar menu. The IPv6 > RA Throttle Policy page appears.

Step 3 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 RA Throttle Policy template page appears (see Figure 11-61).

Figure 11-63 RA Throttle Policy Template



New Controller Template

Configure > Controller Template Launch Pad > IPv6 > RA Throttle Policy > **New Controller Template**

General

Template Name: RAThrottlePolicyTemplate

Applied To Controllers: 0

RA Throttle Policy

RA Throttle Policy: ☑ Enable

Throttle Period: 600 (secs)

Max Through: No Limit ☐ 10

Interval Option: Passthrough

Allow At-least: 1

Allow At-most: No Limit ☐ 1

Footnotes:

1. IPv6 Configuration is not supported for WLC 7500 and SMWLC platforms.

Step 4 Enter a template name in the text box.

Step 5 If you want to enable the down lifetime, select the **Enable** check box. If you have selected this check box, configure the following parameters:

- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
- Max Through—The number of RA that passes through over a period in seconds.
- Interval Option—Indicates the behavior in case of RA with an interval option.
- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum number of RA not throttled per router.

Step 6 Click **Save**.

Configuring RA Guard Templates

RA Guard is a Unified Wireless solution used to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can create or modify a template for configuring IPv6 Router Advertisement parameters.

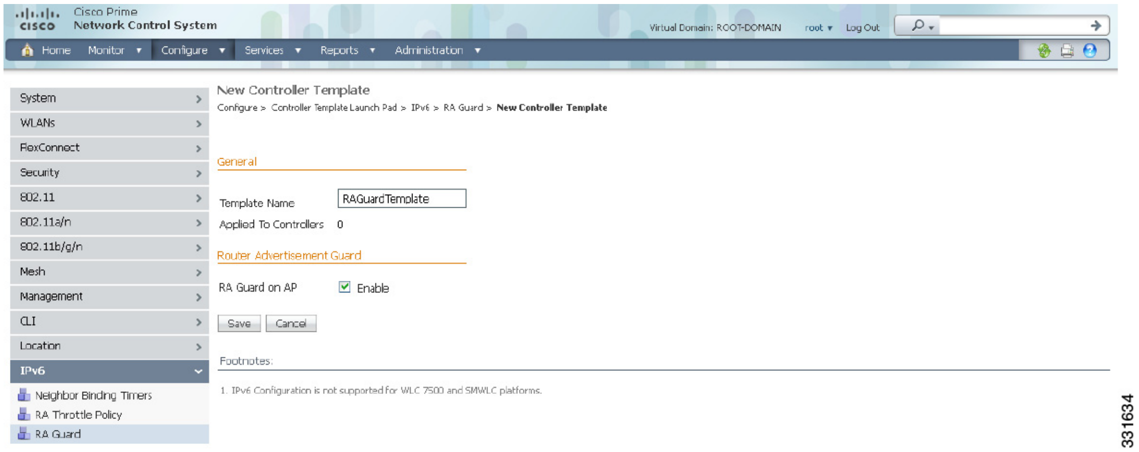
To configure an RA Guard template, follow these steps:

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

Step 2 Click **RA Guard** or choose **IPv6 > RA Guard** from the left sidebar menu. The IPv6 > RA Guard page appears.

Step 3 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 RA Guard template page appears (see Figure 11-61).

Figure 11-64 RA Guard Template



New Controller Template

Configure > Controller Template Launch Pad > IPv6 > RA Guard > **New Controller Template**

General

Template Name: RAGuardTemplate

Applied To Controllers: 0

Router Advertisement Guard

RA Guard on AP ☑ Enable

Footnotes:

1. IPv6 Configuration is not supported for WLC 7500 and SMWLC platforms.

Step 4 Enter a template name in the text box.

Step 5 If you want to enable the Router Advertisement Guard, select the **Enable** check box.

Step 6 Click **Save**.

Configuring AP Configuration Templates

This menu provides access to the access point templates summary details. Use the selector group box to access and configure the respective templates details.

Note Select the template name to view or edit parameters for current access point templates. View the applicable steps in Configuring a New Lightweight Access Point Template, page 11-137 for more information on access point template parameters.

This section contains the following topics:

- Configuring Lightweight Access Point Templates, page 11-137
- Configuring Autonomous Access Point Templates, page 11-146

Configuring Lightweight Access Point Templates

This section contains the following topics:

- Configuring a New Lightweight Access Point Template, page 11-137
- Editing a Current Lightweight Access Point Template, page 11-145

Configuring a New Lightweight Access Point Template

To configure a new Lightweight Access Point template, follow these steps:

Step 1 Choose **Configure > Lightweight AP Configuration Templates**.

Step 2 From the Select a command drop-down list, choose **Add Template**.

Step 3 Click **Go**.

Step 4 Enter a template name in the text box.

Step 5 Enter a template description in the text box.

Step 6 Click **Save**.

Step 7 Once loaded, the Lightweight AP Template Detail page appears. This section describes the Lightweight AP Template Detail page and contains the following topics:

- AP Parameters Tab, page 11-137
- Mesh Tab, page 11-141
- 802.11a/n Tab, page 11-141
- 802.11a SubBand Tab, page 11-142
- 802.11b/g/n Tab, page 11-142
- CDP Tab, page 11-143
- FlexConnect Tab, page 11-143
- Select APs Tab, page 11-144
- Apply/Schedule Tab, page 11-144
- Report Tab, page 11-145

AP Parameters Tab

Select the check box of the access point parameters that must be applied.

- Location—Enter the location in the Location text box.
- Admin Status—Select the **Admin and Enabled** check box to enable administrative status.

Note 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.

- AP Mode—From the drop-down list, choose one of the following:
  - **Local**—Default
  - **Monitor**—Monitor mode only.

    Note Choose **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 choose WIPS from the AP Monitor Mode Optimization drop-down list. For more information on Cisco Adaptive wIPS, see the "Configuring wIPS Profiles" section on page 9-237, or the "wIPS Policy Alarm Encyclopedia" section on page 18-1, and the "NCS Services" section on page 16-1.

  - FlexConnect—Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.

    Note FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join. See the "Configuring FlexConnect" section on page 12-4 for more information.

  - Rogue Detector—Monitors the rogue access points but does not transmit or contain rogue access points.
  - Bridge
  - Sniffer—The access point "sniffs" the air 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.

  - SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

    Note This option is displayed only if the access point is CleanAir-capable.

Note Changing the AP mode reboots the access point.

- Enhanced wIPS Engine—Select the **Enhanced wIPS engine** and the **Enabled** check box to enable.
- AP Monitor Mode Optimization—Choose **None** or **wIPS** from the drop-down list.
- AP Height (feet)—Enter the height of the access point (in feet) in the text box.
- Mirror Mode—Select the **Enabled** check box to enable mirror mode.
- Country Code—Select the appropriate country code from the drop-down list.

Note Changing the country code might cause the access point to reboot.

- Stats Collection Interval—Enter the stats collection interval in the text box.
- Cisco Discovery Protocol—Select the **Enabled** check box to enable Cisco Discovery Protocol.
- AP Failover Priority—Choose **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point failover priority. The default priority is low. See the "Setting AP Failover Priority" section on page 9-162 for more information.
- Pre-Standard 802.3af switches.
- Power Injector State—When enabled, this allows you to manipulate power injector settings through the NCS without having to go directly to the controllers. If the Enable Power Injector State is selected, power injector options appear.
- Power Injector Selection—Choose **installed** or **override** from the drop-down list.
- Injector Switch MAC Address—Enter the MAC address of the injector switch.
- Primary, Secondary, and Tertiary Controller IP—The Primary/Secondary/Tertiary Controller IP is the Management IP of the controller.
- Domain Name
- Domain Name Server IP Address—Domain Name Server IP and Domain Name can be configured only on APs which have static IP.
- Encryption—Select the **Encryption** check box to enable encryption.

Note Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients.

Note DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license. Encryption is not available for all access point models.

Note Enabling encryption might impair performance.

- Rogue Detection—Select the check box to enable rogue detection. See the "Rogue Access Point Location, Tagging, and Containment" section on page 3-13 for more information on rogue detection.

Note Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see *Cisco Wireless LAN Controller Configuration Guide*.

- SSH Access—Select the **SSH Access** check box to enable SSH access.
- Telnet Access—Select the **Telnet Access** check box to enable Telnet access.

Note An OfficeExtend access point might 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.

- 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 FlexConnect access points, for which the link could be a slow or unreliable WAN connection. See the "Configuring Link Latency Settings for Access Points" section on page 9-213 for more information.

Note Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

- Reboot AP—Select the check box to enable a reboot of the access point after making any other updates.
- TCP Adjust MSS—Select the **TCP Adjust MSS** check box to enable TCP to adjust MSS.
- AP Failover Priority—Choose **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point failover priority. The default priority is low. See the "Setting AP Failover Priority" section on page 9-162 for more information.
- Controllers—Select the **Controllers** check box to enable the drop-down lists for the primary, secondary, and tertiary controller names.
- Group VLAN name—Choose the appropriate group VLAN name from the drop-down list.
- Override Global Username Password—Select the check box to enable an override for the global username/password. Enter and confirm the new access point username and password in the appropriate text boxes. See the "Configuring a Global Access Point Password" section on page 9-60 for more information on a global username and password.

Note 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 Parameter tab page.

- Override Supplicant Credentials—Select the **Override Supplicant Credentials** check box to prevent this access point from inheriting the authentication username and password from the controller. The default value is unselected. The Override Supplicant Credentials option is supported in controller Release 6.0 and later.
  - In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

Mesh Tab

Use the Mesh tab to set the following parameters for mesh access points:

- Bridge Group Name—Enter a bridge group name (up to 10 characters) in the text box.

  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.

  Note 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.

- Data Rate (Mbps)—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.

  Note Do not change the data rate for a deployed mesh networking solution.

- Ethernet Bridging—Select the **Enable** check box. From the Ethernet Bridging drop-down list, enable Ethernet bridging for the mesh access point.
- Role—Choose the role of the mesh access point from the drop-down list (**MAP** or **RAP**). The default setting is MAP.

  Note An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

802.11a/n Tab

Select the check boxes of the 802.11a/n parameters that must be applied:

- Channel Assignment
- Admin Status
- Antenna Mode
- Antenna Diversity
- Antenna Name

- Power Assignment
- WLAN Override
- 11n Antenna Selection
- CleanAir

802.11a SubBand Tab

Select the 802.11a Sub Band options (for either 4.9 or 5.8 parameters) that must be applied:

Note Options are disabled unless the check box to the left of the field is selected.

- Admin Status
- Channel Assignment—Select the check box and then choose the appropriate channel from the drop-down list.

  Note The channel number is validated against the radio list of supported channels.

- Power Assignment—Select the check box and then choose the appropriate power level from the drop-down list.

  Note The power level is validated against the radio list of supported power levels.

- WLAN Override—Select the check box and then choose **Disable** or **Enable** from the drop-down list.

  Note The access point must be reset for the WLAN override change to take effect.

- Antenna Type—Select the check box and then choose the antenna type from the drop-down list.
- Antenna Name—Select the **Antenna Type** check box and then choose the applicable antenna name from the drop-down list.

  Note Not all antenna models are supported by radios of different access point types.

802.11b/g/n Tab

Select the check box of the 802.11b/g/n parameters that must be applied:

- Channel Assignment
- Admin Status
- Antenna Mode
- Antenna Diversity
- Antenna Name
- Power Assignment
- WLAN Override

- Tracking Optimized Monitor Mode
- 11n Antenna Selection
- CleanAir

CDP Tab

- In the Cisco Discovery Protocol on Ethernet Interfaces group box, select the check boxes for the slots of Ethernet interfaces for which you want to enable CDP.
- In the Cisco Discovery Protocol on Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

FlexConnect Tab

- FlexConnect Configuration—Select the check box to enable FlexConnect configuration (including VLAN support, native VLAN ID, and profile name VLAN mappings).

  Note These options are only available for access points in FlexConnect mode.

  - OfficeExtend—The default is Enabled.

    Note Unselecting 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 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 personal SSID, click Reset Personal SSID at the bottom of the access point details page. See the "Restoring Factory Defaults" section on page 9-34 for more information.

    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).

  - Least Latency Controller Join—When 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 latency measurements of primary, secondary, and tertiary controllers once joined to see if the measurements have changed.

  - VLAN Support
  - Native VLAN ID

Note The valid native VLAN ID range is 1—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.

Click the **Show/Add VLAN ACL Mapping** link to add or delete a VLAN ID and map it to Ingress ACL and Egress ACL.

- VLAN ID ACL Mapping—Enter a VLAN ID and choose the Ingress and Egress ACLs from the drop-down list boxes to map to the VLAN ID specified.

Click the **Show/Add WebAuth ACL Mapping** link to add or delete a WLAN Profile and WebAuth ACL mapping.

- WLAN Profile to ACL Mapping— Choose the WLAN Profile and WebAuth ACL from the drop-down list boxes to add a WebAuth ACL mapping.

Click the **Show/Add WebPolciy ACL** link to add or delete a Web Policy ACL.

Select APs Tab

Use the Search APs drop-down list to search for Last Applied AP(s), Scheduled AP(s), All, All Mesh MAP AP(s), All Mesh RAP AP(s), By Controller (choose the controller from the drop-down list), By Controller Name (choose the controller name from the drop-down list), By Floor Area (choose the campus, building, and floor area from the drop-down lists), By Outdoor Area (choose the campus and the outdoor area from the drop-down lists), By Model (choose the model from the drop-down list), By AP MAC Address (enter the MAC address), By AP Name (enter the complete AP name or starting characters of the AP name), and By AP IP Address Range (enter the IP address).

Note The input text for IP address search can be of two formats X.X.X.* or X.X.X.[0-255]. For example, 10.10.10.* or 10.10.10.[20-50] searches the APs in 10.10.10.10 to 10.10.10.50 IP address range.

Note The All Applied APs and Scheduled APs search filters list the last 24 hours AP data.

Note The AP(s) unassigned to Map(s) search filter lists the APs that have not yet been assigned to any maps.

- Click **Save** to save the parameters selections.
- Click **Apply** to save and apply the AP/Radio parameters to the selected access points from the search.

Apply/Schedule Tab

Allows you to save the current template, apply the current template immediately, or schedule the current template to start the provisioning at the applicable time.

- Save—Click **Save** to save the current template configuration.
- Apply—Click **Apply** to save the template and start the provisioning of the template to selected access points.

Note This provisioning process continues until completed even if you leave the page and log out of the NCS.

- Schedule—Allows you to configure and start the provisioning at a scheduled time.
  - Enable schedule—Select the **Enable schedule** check box to activate the scheduling function.
  - Start Date—Enter a starting date in the text box or use the calendar icon to select a start date.
  - Start Time—Select the starting time using the hours and minutes drop-down lists.
  - Recurrence—Select from no recurrence, hourly, daily, or weekly to determine how often this provisioning occurs. Enter how often (in days) the provisioning is to occur.
  - Schedule—Click **Schedule** to start the provisioning at the scheduled time.

Report Tab

Displays all recently applied reports including the apply status and the date and time the apply was initiated. The following information is provided for each individual access point:

- Status—Indicates success, partial failure, failure, or not initiated. For failed or partially failed provisioning, click **Details** to view the failure details (including what failed and why it failed).
- Ethernet MAC—Indicates the Ethernet MAC address for the applicable access point.
- Controller—Indicates the controller IP address for the applicable access point.
- Map—Identifies a map location for the access point.

Note Click the **click here** link at the bottom of the Report page to view scheduled task reports.

Editing a Current Lightweight Access Point Template

To edit a current Lightweight Access Point Template, follow these steps:

Step 1 Choose **Configure > Lightweight AP Configuration Templates**.

Step 2 Click the applicable template in the Template Name column.

Step 3 Edit the necessary parameters on the following tabs:

- AP Parameters—Select the check box of the access point parameters that must be applied.
- Mesh
- 802.11a/n Parameters—Select the check box of the 802.11a/n parameters that must be applied.
- 802.11b/g/n Parameters—Select the check box of the 802.11b/g/n parameters that must be applied.
- Select APs
  - Use the Search APs drop-down list to search for Last Applied APs, All APs, All MAP(s), or All RAP(s).
  - Click **Save** to save the parameters selections.

- Click **Apply** to save and apply the AP/Radio parameters to the selected access points from the search.
- Apply Report—Displays the reports from the applied template.

Configuring Autonomous Access Point Templates

The Configuring > Autonomous Access Point Templates page allows you to configure CLI templates for autonomous access points.

This section contains the following topics:

- Configuring a New Autonomous Access Point Template, page 11-146
- Applying an AP Configuration Template to an Autonomous Access Point, page 11-146
- Editing Current Autonomous AP Migration Templates, page 11-150

Configuring a New Autonomous Access Point Template

To configure a new Autonomous Access Point template, follow these steps:

Step 1 Choose **Configure > Autonomous AP Configuration Templates**.

Step 2 From the Select a command drop-down list, choose **Add Template**.

Step 3 Click **Go**.

Step 4 Enter a Template Name.

Step 5 Enter the applicable CLI commands.

Note Do not include any show commands in the CLI commands text box. The show commands are not supported.

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 > Autonomous AP Configuration Templates**.

Step 2 Click the template name link to select a template and apply it to the an autonomous access point. The New Autonomous AP Configuration 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.

Viewing Template Results

To view the results when you apply an Autonomous AP Configuration template to an 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 Configuration 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**. The Template Results page appears. The following parameters appear:

- IP Address —IP address of the access point.
- AP Name—The name of the access point.
- Apply Status—Indicates success, failure, initiated or not initiated.
- Operation Status—Displays the operational status: Success or Failure.
- Reason—Indicates the reasons for failure.
- Session Output

Configuring Switch Location Configuration Templates

You can configure the location template for a switch using the Switch Location Configuration template.

To configure a location template for a switch, follow these steps:

Step 1 Choose **NCS > Configure > Switch Location Configuration Template**.

The Switch Location Configuration template page appears.

Step 2 From the Select a command drop-down list, choose **Add Template**, and click **Go**.

The New Template page appears.

Table 11-4 lists the fields in the New Template page.

Field	Description
General	
Template Name	Name of the template.
Map Location	
Campus	Choose a campus for the map location for a switch/switch port.
Building	Choose a building for the map location for a switch/switch port.
Floor	Choose a floor for the map location for a switch/switch port.
Import	Imports the civic information for the campus, building, and floor selected.
ELIN and Civic Location	
ELIN	The Emergency Location Identification Number.
Civic Address tab	The available civic address information for the switch/switch port.
Advanced tab	Detailed information about the switch/switch port location.
NMSP	Select or unselect this check box to enable or disable NMSP for the switch.
Buttons	
Save	Saves the template.
Cancel	Discards the template creation.

Configuring Autonomous AP Migration Templates

This section contains the following topic:

Migrating an Autonomous Access Point to a Lightweight Access Point, page 11-148**Migrating an Autonomous Access Point to a Lightweight Access Point**

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to lightweight access points. The migration utility is available in the Configure > Autonomous AP Migration Templates page where existing templates are listed.

The Autonomous AP Migration Templates list page displays the following information:

- Name—The template name.
- Description—The description of template.
- AP Count—The number of autonomous access points selected for migration.
- Schedule Run—The time at which the task is scheduled to run.

- Status—Indicates one of the following task statuses:
  - Not initiated—The template is yet to start the migration and starts at the scheduled time.
  - Disabled—The template is disabled and does not run at the scheduled time. This is the default state for a template when it is created without selecting any autonomous access points.
  - Expired—The template did not run at the scheduled time (this might be due to the NCS server being down).
  - Enabled—The template is yet to start the migration and starts at the scheduled time.
  - In progress—The template is currently converting the selected autonomous access points to CAPWAP.
  - Success—The template has completed the migration of autonomous access point to CAPWAP successfully.
  - Failure—The template failed to migrate all the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.
  - Partial Success—The template failed to migrate a subset of the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.

Note In any of these states, you can edit the template by clicking the **Name** link.

Note Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

From the Select a command drop-down list, the following functions can be performed:

- Add Template—Allows you to provide necessary information for migration.
- Delete Templates—Allows you to delete a current template.
- View Migration Report—Allows you to view information such as AP address, migration status (in progress or fail), timestamp, and a link to detailed logs.
- View Current Status—Allows you to view the progress of the current migration (updated every three seconds).

Note When you migrate an already-managed autonomous access point to lightweight, its location and antenna information is migrated as well. You do not need to reenter the information. The NCS automatically removes the autonomous access point after migration.

- View Migration Analysis Summary—Lists the pass or fail status as required for an access point conversion. Only those access points with all criteria as pass are eligible for conversion.

Note The Migration Analysis option does not run during discovery by default. If you prefer to run the migration analysis during discovery, choose **Administration > Settings > CLI Session** to enable this option.

Note The NCS also supports the migration of autonomous access point to CAPWAP access point.

Editing Current Autonomous AP Migration Templates

To edit a current migration template, follow these steps:

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Click the migration template in the Name column.

Step 3 Edit the necessary parameters:

- General
  - Name—Indicates the user-defined name of the migration template.
  - Description—Enter a brief description to help you identify the migration template.
- Upgrade Options
  - DHCP Support—Click to enable Dynamic Host Configuration Protocol support. This ensures that after the conversion every access point gets an IP from the DHCP server.
  - Retain AP HostName—Click to enable retention of the same hostname for this access point.

  Note The hostname is retained in the CAPWAP, only when you are migrating the AP to CAPWAP for the first time. It might not be retained if you are upgrading an AP for several times. The CAPWAP access points hostname is set to default if autonomous access points hostname has more than 32 characters.

  Note If you upgrade the access points to LWAPP from 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, 12.3(11)JA3 autonomous images, the converted access points might not retain their Static IP Address, Netmask, Hostname and Default Gateway.

  - Migrate over WANLink—If you enable this option, the *env_vars* file stores the remote TFTP server location. This information is copied to the AP. If this option is not selected, then the NCS internal TFTP server is used to copy the *env_vars* file to AP.
  - DNS Address—Enter the DNS address.
  - Domain Name—Enter the domain name.
- Controller Details

  Note Ensures that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

  - Controller IP
  - AP Manager IP
  - User Name
  - Password

- TFTP Details
  - TFTP Server IP
  - File Path
  - File Name
- Schedule Details
  - Apply Template
  - Notification (Optional)

Step 4 Click **Save**.

Viewing the Migration Analysis Summary

To view the Migration Analysis Summary, follow these steps:

Note You can also view the migration analysis summary by choosing **Tools > Migration Analysis**.

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Choose **View Migration Analysis Summary** from the Select a command drop-down list, and click **Go**. The Migration Analysis Summary page appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green checkmark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version Criteria—Conversion is supported only in Cisco IOS Release 12.3(7)JA excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Adding/Modifying a Migration Template

If you want to add a migration template, choose **Add Template** from the Select a command drop-down list in the Configure > Autonomous AP Migration Templates page.

To modify an existing template, click the template name from the summary list.

Enter or modify the following migration parameters:

General

- Name—User-defined name of this migration template.
- Description—Brief description to help you identify the migration template.

Upgrade Options

- DHCP Support—Ensures that after the conversion every access point gets an IP from the DHCP server.
- Retain AP HostName—Allows you to retain the same hostname for this access point.
- Migrate over WANLink—Increases the default timeouts for the CLI commands executed on the access point.
- DNS Address
- Domain Name

Controller Details

Note Ensure that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

- Controller IP—Enter the IP address of the WLAN controller you are wanting to add to the newly migrated access point.
- AP Manager IP—Specify the controller the access point should join by entering the access point manager IP address.

  Note For SSC-enabled access points, this IP address must be the same as the controller IP field. For MIC-enabled access points, the IP addresses need not match.

- User Name—Enter a valid username for login of the WLAN controller.
- Password—Enter a valid password for this username used during WLAN controller login.

TFTP Details

The NCS provides its own TFTP and FTP server during the installation and setup.

- TFTP Server IP—Enter the IP address of the NCS server.
- File Path—Enter the TFTP directory which was defined during the NCS setup.
- File Name—Enter the CAPWAP conversion file defined in the TFTP directory during the NCS setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).

Schedule Details

This group box enables you to specify scheduling options for migration templates.

- Apply Template—Choose an option by which you want to apply the template for migration.

- Now—Choose this option to run the migration task immediately.
- Schedule for later date/time—If you plan to schedule the migration at a later time, enter the Schedule parameters. Enter a date in the text box, or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists. The report begins running on this data and at this time.

- (Optional) Notification—Enter the e-mail address of recipient to send notifications via e-mail.

Note To receive e-mail notifications, configure the NCS mail server in the Administration > Settings > Mail Server Configuration page.

- Click **Save**.

Once a template is added in the NCS, the following additional buttons appear:

- Select APs—Choosing this option provides a list of autonomous access points in the NCS from which to choose the access points for conversion. Only those access points with migration eligibility as *pass* can be chosen for conversion.
- Select File—To provide CSV information for access points intended for conversion.

Copying a Migration Template

To copy a migration template, follow these steps:

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Select the check box of the template you want to copy, and then choose **Copy Template** from the Select a command drop-down list.

Step 3 Click **Go**.

Step 4 Enter the name for the new template to which you want to copy the current template.

Deleting Migration Templates

To delete migration templates, follow these steps:

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Select the check box(es) of the template(s) you want to delete, and then choose **Delete Templates** from the Select a command drop-down list.

Step 3 Click **Go**.

Step 4 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

Viewing the Current Status of Cisco IOS Access Points

Select **View Current Status** from the Select a command drop-down list in the Autonomous AP Migration Templates page to view the status of Cisco IOS access point migration.

The following information is displayed:

- IP Address—IP address of the access point.
- Status—Current status of the migration.
- Progress—Summary of the migration progress.

Disabling Access Points that are Ineligible

If an autonomous access point is labelled as ineligible for conversion, you can disable it.