



CHAPTER 11

Using Templates

This chapter describes how to add and apply controller templates. Information on creating (adding) access point templates is also provided.

Templates allow you to set parameters that you can then apply to multiple devices without having to re-enter the common information.



Note

Template information can be overridden on individual devices.

This chapter contains these sections:

- [Adding Controller Templates, page 11-1](#)
- [Applying Controller Templates, page 11-80](#)
- [Adding Access Point Templates, page 11-80](#)
- [Configuring Access Point Templates, page 11-81](#)

Adding Controller Templates

Follow these steps to add a new controller template.

-
- | | |
|---------------|---|
| Step 1 | Choose Configure > Controller Templates . |
| Step 2 | Choose Add Template from the Select a command drop-down menu and click GO . |
| Step 3 | Enter the template name. |
| Step 4 | Provide a description of the template. |
| Step 5 | Click Save . |
-

A summary of the templates that can be added is highlighted below:

- [Configuring an NTP Server Template, page 11-3](#)
- [Configuring General Templates, page 11-4](#)
- [Configuring QoS Templates, page 11-6](#)
- [Configuring a Traffic Stream Metrics QoS Template, page 11-8](#)
- [Configuring WLAN Templates, page 11-9](#)

- [Configuring H-REAP AP Groups, page 11-21](#)
- [Configuring a File Encryption Template, page 11-23](#)
- [Configuring a RADIUS Authentication Template, page 11-24](#)
- [Configuring a RADIUS Accounting Template, page 11-27](#)
- [Configuring a LDAP Server Template, page 11-28](#)
- [Configuring a Local EAP General Template, page 11-30](#)
- [Configuring a Local EAP Profile Template, page 11-31](#)
- [Configuring an EAP-FAST Template, page 11-33](#)
- [Configuring Network User Credential Retrieval Priority Templates, page 11-35](#)
- [Configuring a Local Network Users Template, page 11-35](#)
- [Configuring Guest User Templates, page 11-37](#)
- [Configuring a User Login Policies Template, page 11-38](#)
- [Configuring a MAC Filter Template, page 11-39](#)
- [Configuring an Access Point or LBS Authorization, page 11-40](#)
- [Configuring a Manually Disabled Client Template, page 11-41](#)
- [Configuring a CPU Access Control List \(ACL\) Template, page 11-42](#)
- [Configuring a Rogue Policies Template, page 11-43](#)
- [Configuring a Rogue AP Rules Template, page 11-44](#)
- [Configuring a Rogue AP Rule Groups Template, page 11-46](#)
- [Configuring a Friendly Access Point Template, page 11-48](#)
- [Configuring a Client Exclusion Policies Template, page 11-49](#)
- [Configuring an Access Point Authentication and MFP Template, page 11-51](#)
- [Configuring a Web Authentication Template, page 11-52](#)
- [Configuring Access Control List Templates, page 11-56](#)
- [Configuring a Policy Name Template \(for 802.11a/n or 802.11b/g/n\), page 11-57](#)
- [Configuring High Density Templates, page 11-60](#)
- [Configuring a Voice Parameter Template \(for 802.11a/n or 802.11b/g/n\), page 11-62](#)
- [Configuring EDCA Parameters through a Controller Template, page 11-64](#)
- [Configuring EDCA Parameters through a Controller Template, page 11-64](#)
- [Configuring an RRM Threshold Template \(for 802.11a/n or 802.11b/g/n\), page 11-66](#)
- [Configuring an RRM Interval Template \(for 802.11a/n or 802.11b/g/n\), page 11-68](#)
- [Configuring an 802.11h Template, page 11-69](#)
- [Configuring a High Throughput Template \(for 802.11a/n or 802.11b/g/n\), page 11-70](#)
- [Configuring a Mesh Template, page 11-71](#)
- [Configuring a TFTP Server Template, page 11-72](#)
- [Configuring a Trap Receiver Template, page 11-73](#)
- [Configuring a Trap Control Template, page 11-73](#)
- [Configuring a Telnet SSH Template, page 11-75](#)

- [Configuring a Legacy Syslog Template, page 11-76](#)
- [Configuring a Multiple Syslog Template, page 11-77](#)
- [Configuring a Local Management User Template, page 11-78](#)
- [Configuring a User Authentication Priority Template, page 11-79](#)
- [Configuring Radio Templates, page 11-88](#)

Configuring an NTP Server Template

Follow these steps to add a new network time protocol (NTP) server template to the controller configuration or make modifications to an existing NTP template. NTP is used to synchronize computer clocks on the internet.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** Choose **System > Network Time Protocol** from the left sidebar menu.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To modify an existing template, click to select a template in the Template Name column. The NTP Server Template window appears (see [Figure 11-1](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-1 NTP Servers Template

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Help

NTP Server Templates > Template '171.68.10.150'

General

Template Name: 171.68.10.150

Server Address: 171.68.10.150

No of Controllers Applied To: 0

Save Apply to Controllers ... Delete Cancel

Alarm Summary

Rogue AP	0	150
Coverage Hole	137	
Security	9	2
Controllers	1	0
Access Points	762	40
Mesh Links	0	0
Location	1	14

- Step 4** Enter the NTP server IP address.
- Step 5** Click **Save**.

Configuring General Templates

Follow these steps to add a new template with general information for a controller or make a change to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **System > General**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To modify an existing template, click to select a template in the Template Name column. The General Template window appears (see [Figure 11-2](#)).

Figure 11-2 General Template

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar menu is expanded to 'System' > 'General'. The main content area displays the 'General Template > Template "Switching_23129"' configuration page. The 'General' tab is selected, showing various configuration options for the template. The 'Template Name' is 'Switching_23129'. The '802.3x Flow Control Mode' is set to 'Disable'. The '802.3 Bridging' is set to 'Disable'. The 'LWAPP Transport Mode' is set to 'Layer3'. The 'Aggressive Load Balancing' is set to 'Disable'. The 'Peer to Peer Blocking Mode' is set to 'Disable'. The 'Over Air Provision AP Mode' is set to 'Disable'. The 'AP Fallback' is set to 'Enable'. The 'AP Priority' is set to 'Disable'. The 'Apple Talk Bridging' is set to 'Disable'. The 'Fast SSID change' is set to 'Disable'. The 'Master Controller Mode' is set to 'Disable'. The 'Wireless Management' is set to 'Disable'. The 'Link Aggregation' is set to 'Disable'. The 'Symmetric Tunneling Mode' is set to 'Disable'. The 'Default Mobility Domain Name' is 'air'. The 'Mobility Anchor Group Keep Alive Interval' is '10'. The 'Mobility Anchor Group Keep Alive Retries' is '3'. The 'RF Network Name' is 'air'. The 'User Idle Timeout (seconds)' is '300'. The 'ARP Timeout (seconds)' is '300'. The 'Cisco Discovery Protocol' section shows 'CDP on controller' set to 'Enable', 'Global CDP on APs' set to 'Enable', 'Refresh-time Interval (seconds)' set to '60', 'Holdtime (seconds)' set to '180', and 'CDP Advertisement Version' set to 'v1'. At the bottom, there are buttons for 'Save', 'Apply to Controllers...', 'Delete', and 'Cancel'.

- Step 4** Use the drop-down menu to enable or disable flow control mode.
- Step 5** Use the drop-down menu to enable or disable 802.3 bridging.
- Step 6** Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the LWAPP 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 LWAPP uses proprietary code to communicate with the access points.
- Step 7** At the Ethernet Multicast Support drop-down menu, choose **Disable** to disable multicast support on the controller or **Multicast** to enable multicast support on the controller. Choose **Unicast** if the controller, upon receiving a multicast packet, forwards the packets to all the associated access points. H-REAP supports only unicast mode.
- Step 8** Choose if you want to enable or disable aggressive load balancing.
- Step 9** 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 10** At the Over Air AP Provision Mode drop-down menu, choose enable or disable.

- Step 11** At the AP Fallback drop-down menu, choose enable or disable. Enabling fallback causes an access point which lost a primary controller connection to automatically return to service when the primary controller returns.
- Step 12** Choose to enable or disable Apple talk bridging.
- Step 13** Choose to enable or disable the fast SSID option. If enabled, the client connects instantly to the controller between SSIDs without having appreciable 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 14** Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or OS code upgrade. You may enable the controller as the master controller from the Master Controller Mode drop-down menu.
- Step 15** 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, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPsec WLAN.
- Step 16** Choose to enable or disable link aggregation. 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). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted. This is done to prevent configuration inconsistencies in the interface database.
- Interfaces cannot be created with the “Dynamic AP Manager” flag set.



Note You cannot create more than one LAG on a controller.

The advantages of creating a LAG are as follows:

- It ensures that if one of the links goes down, the traffic is moved to the other links in the LAG. Hence, as long as one of the physical ports is working, the system remains functional.
- It eliminates the need to configure separate backup ports for each interface.
- Multiple AP-manager interfaces are not required since only one logical port is visible to the application.



Note When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

- Step 17** Choose to enable or disable symmetric mobility tunneling. With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has reverse path filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled.

**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 18 Enter the operator-defined RF mobility group name in the Default Mobility Domain Name field.

Step 19 At the Mobility Anchor Group Keep Alive Interval, determine the delay between tries for clients attempting to join another access point. With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

**Note**

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

Step 20 At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.

**Note**

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

Step 21 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 22 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 23 Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.

Step 24 At the CDP on controller drop-down menu, choose if you want to enable CDP on the controller. CDP is a device discovery protocol that runs on all Cisco manufactured equipment (such as routers, bridges, communication servers, and so on).

Step 25 At the Global CDP on APs drop-down menu, choose if you want to enable CDP on the access point.

Step 26 At the Refresh Time Interval parameter, enter the interval at which CDP messages are generated. With the regeneration, the neighbor entries are refreshed.

Step 27 At the Holdtime parameter, enter the time in seconds before the CDP neighbor entry expires.

Step 28 At the CDP Advertisement Version parameter, enter which version of the CDP protocol to use.

Step 29 Click **Save**.

Configuring QoS Templates

Follow these steps to make modifications to the quality of service profiles.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** On the left sidebar menu, choose **System > QoS Profiles**. The QoS Template window appears (see [Figure 11-3](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-3 QoS Profile Template

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor Reports Configure Location Administration Help

Templates

- System
 - General
 - SNMP Community
 - Network Time Protocol
 - QoS Profiles
 - Traffic Stream Metrics QoS
- WLANs
- Security
- Access Control
- 802.11a/n
- 802.11b/g/n
- Mesh

Alarm Summary

Rogue AP	0	150
Coverage Hole	0	137
Security	9	2
Controllers	1	0
Access Points	762	40
Mesh Links	0	0
Location	1	14

Edit QoS Profile Template

Name: gold (Video)

Description: For Video Applications

Controllers Applied To: 8

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 (%)	100
Queue Depth	75

Wired QoS Protocol

Protocol: None

802.1P Tag: 5

Save Apply to Controllers ... Cancel

*The value zero (0) indicates the feature is disabled.

- Step 3** Set the following values in the Per-User Bandwidth Contracts portion of the window. 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 4** Set the following values for the Over-the-Air QoS portion of the window.
- Maximum QoS RF Usage per AP - The maximum air bandwidth available to clients. The default is 100%.
 - QoS Queue Depth - The depth of queue for a class of client. The packets with a greater value are dropped at the access point.
- Step 5** Set the following values in the Wired QoS Protocol portion of the window.
- 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 LWAPP packets.
- 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. Cisco WCS queries the controller for the metrics and displays them in the Traffic Stream Metrics QoS Status. These metrics are compared to threshold values to determine their status level and if any of the statistics are displaying a status level of fair (yellow) or degraded (red), the administrator investigates the QoS of the wireless LAN.

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

-
- Step 1** Choose **Configure > Controller Templates**.
- Step 2** On the left sidebar menu, choose **System > Traffic Stream Metrics QoS**. The Traffic Stream Metrics QoS Status Configuration window appears (see [Figure 11-4](#)).

Figure 11-4 Traffic Stream Metrics QoS Status Template

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor | Reports | **Configure** | Location | Administration | Help

Traffic Stream Metrics QoS Status Configuration

Upstream Delay

- Normal QoS is 95 percent or more of packets having delay less than 20ms.
- Fair QoS is 75 percent or more of packets having delay less than 40ms.
- Degraded QoS is 25 percent or more of packets having delay equal or greater than 40ms.

Upstream Packet Loss Rate

- Normal QoS is less than 1.5 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 Packet Loss Rate

- Normal QoS is less than 2.0 percent.
- Fair QoS is less than 2.5 percent.
- Degraded QoS is equal or greater than 2.5 percent.

Save Cancel

Alarm Summary

Rogue AP	0	150
Coverage Hole	137	
Security	9	2
Controllers	1	0
Access Points	762	40
Mesh Links	0	0
Location	1	14

182755

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

- Upstream delay

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

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

There are three levels of measurement:

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

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

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

Configuring WLAN Templates

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

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

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

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

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

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

Step 2 Choose **WLANs > WLAN** from the left sidebar menu.

The WLAN Template window appears with a summary of all existing defined WLANs. The following information headings are used to define the WLANs listed on the WLAN Template General window (see Figure 11-5).

- Template Name - The user-defined name of the template. Clicking the name displays parameters for this template.
- Profile Name - User-defined profile name used to distinguish WLANs with the same SSID.



Note This heading is not present in software release prior to 4.0.96.0.

- SSID - Displays the name of the WLAN.
- WLAN Status - Sets the status of the WLAN to enabled when checked.
- Security Policies - Determines whether 802.1X is enabled. None indicates no 802.1X.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a URL in the Template Name column. The WLAN Template window appears (see Figure 11-5).

Figure 11-5 WLAN Template

Alarm Summary			
Malicious AP	0	0	0
Coverage Hole	0	0	0
Security	0	0	0
Controllers	0	0	0
Access Points	1	0	2
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

Foot Notes

- 1 When enabled, a excluded 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 Web Authentication cannot be used in combination with IPsec and L2TP.
- 4 CKIP is not supported on 10xx APs.
- 5 H-REAP Local Switching is not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications. It is not applicable to WLAN IDs 9-16.
- 6 Client MFP is not active unless WPA2 is configured.

- Step 4** Wired guest access enables guest users to connect to the guest access network from a wired 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. Wired guest access accounts are added to the network using the Lobby Ambassador portal. (Refer to the [“Creating Guest User Accounts”](#) section on page 7-11).
- Step 5** Enter a name in the Profile Name field that identifies the guest LAN. Do not use any spaces in the name entered.
- Step 6** Check the **Enabled** check box for the Status parameter.
- Step 7** Use the Radio Policy drop-down menu to set the WLAN policy to apply to All (802.11a/b/g/n), 802.11a only, 802.11g only, 802.11b/g/n only, or 802.11a/g/n only.
- Step 8** Use the Interface drop-down menu to choose the available names of interfaces created by the Controller > Interfaces module.
- Step 9** Click **Broadcast SSID** to activate SSID broadcasts for this WLAN.
- Step 10** Click **Save**.
- Step 11** To further configure the WLAN template, choose from the following:
- Click the **Security** tab to establish which AAA can override the default servers on this WLAN and to establish the security mode for Layer 2 and 3. Continue to the [“Security”](#) section on page 11-11.
 - Click the **QoS** tab to establish which quality of service is expected for this WLAN. Continue to the [“QoS”](#) section on page 11-17.
 - Click the **Advanced** tab to configure any other details about the WLAN, such as DHCP assignments and management frame protection. Continue to the [“Advanced”](#) section on page 11-18.
-

Security

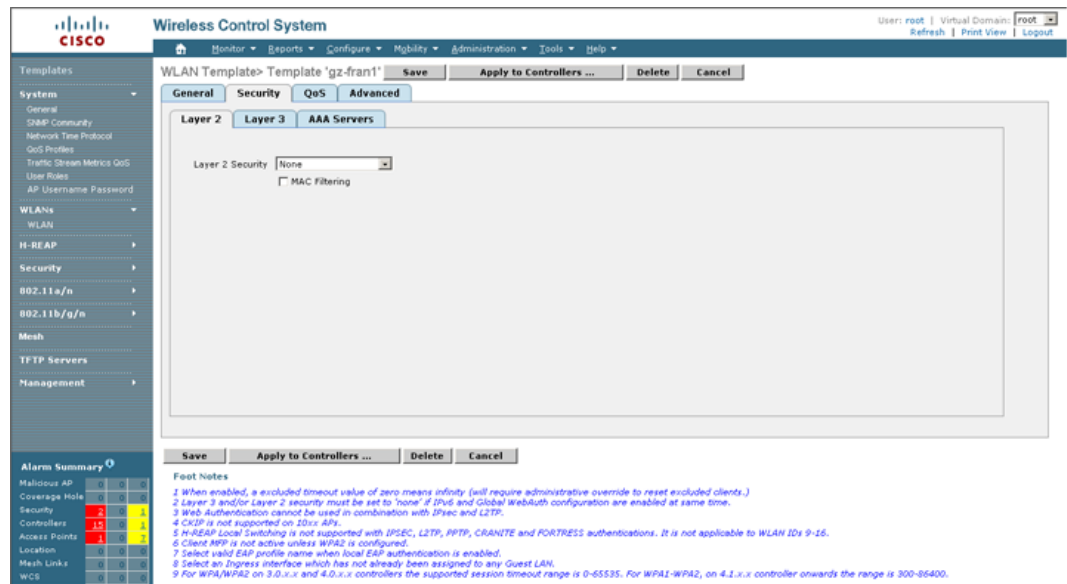
After choosing Security, you have an additional three tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2

When you choose the Layer 2 tab, the window as shown in [Figure 11-6](#) appears.



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

Figure 11-6 Layer 2 Window

Step 1 Use the Layer 2 Security drop-down menu to choose between None, WPA, WPA-2, Static WEP, 802.1X, Cranite, Fortress, Static WEP-802.1X, CKIP, and WPA1 + WPA2 as described in the table below.

Table 11-1 Layer 2 Security Options

Parameter	Description
None	No Layer 2 security selected.
802.1X	WEP 802.1X data encryption type (Note 1): 40/64 bit key. 104/128 bit key. 128/152 bit key.
WPA	This is a 3.2 controller code option and is not supported in 4.0 or later versions.
WPA-2	This is a 3.2 controller code option is not supported in 4.0 or later versions.

Table 11-1 **Layer 2 Security Options (continued)**

Parameter	Description
Static WEP	Static WEP encryption parameters: Key sizes: 40/64, 104/128, and 128/152 bit key sizes. Key Index: 1 to 4 (Note 2). Encryption Key: Encryption key required. Key Format: Select encryption key format in ASCII or HEX. Note Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC. 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.
Cranite	Configure the WLAN to use the FIPS140-2 compliant Cranite Wireless Wall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Cisco Wireless LAN Solution.
Fortress	FIPS 40-2 compliant Layer 2 security feature.
Static WEP-802.1X	Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X parameters are displayed at the bottom of the page. Static WEP encryption parameters: Key sizes: 40/64, 104/128, and 128/152 bit key sizes. Key index: 1 to 4 (Note 2). Encryption Key: Enter encryption key. Key Format: Select encryption key format in ASCII or HEX. WEP 802.1X data encryption type (Note 1): 40/64 bit key. 104-128 bit key. 128/152 bit key.

Table 11-1 **Layer 2 Security Options (continued)**

Parameter	Description
WPA1+WPA2	Use this setting to enable WPA1, WPA2, or both. See the WPA1 and WPA2 parameters displayed on the window when WPA1+WPA2 is selected. WPA1 enables Wi-Fi Protected Access with TKIP-MIC Data Encryption. When WPA1+WPA2 is selected, you can use Cisco's Centralized Key Management (CCKM) authentication key management, which allows fast exchange when a client roams from one access point to another. When WPA1+WPA2 is selected as the Layer 2 security policy, and Pre-shared Key is enabled, then neither CCKM or 802.1X can be enabled. Although, both CCKM and 802.1X can be enabled at the same time.
CKIP	Cisco Key Integrity Protocol (CKIP). A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WLAN. When selected, these CKIP parameters are displayed. Key size: Specify key length. Encryption Key: Specify encryption key. Key Format: ASCII or HEX. Note Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC. 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: Enabled or disabled (check box). Key Permutation: Enabled or disabled (check box).

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

Step 3 If you selected either WPA1 or WPA2 in Step 1, you must specify the type of WPA encryption: either TKIP or AES.

Step 4 Choose the desired type of authentication key management. The choices are 802.1X, CCKM, PSK, or CCKM+802.1X.



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

Step 5 Click **Save**.

Layer 3

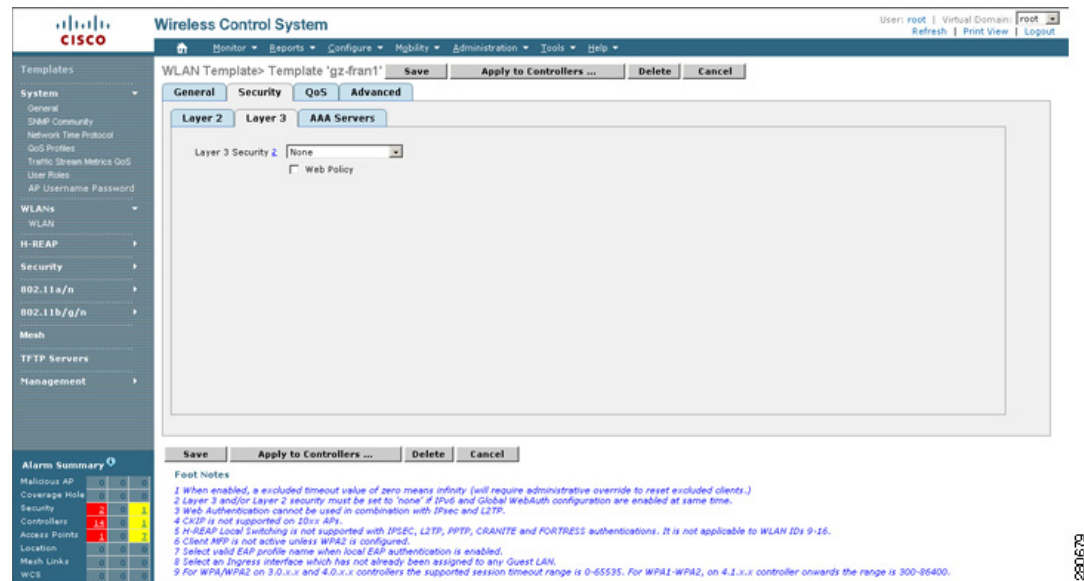
When you choose the Layer 3 tab, the window shown in [Figure 11-7](#) appears.



Note

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

Figure 11-7 Layer 3 Window



Follow these steps to configure the Layer 3 tab.

- Step 1** Use the Layer 3 security drop-down menu to choose between None and VPN Pass Through. The window parameters change according to the selection you make. If you choose VPN pass through, you must enter the VPN gateway address.
- Step 2** You can modify the default security policy (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source.
 - a.** To change the security policy to passthrough, check the **Web Policy** check box and the **Passthrough** option. This option allows users to access the network without entering a username or password.
An *Email Input* check box appears. Check this check box if you want users to be prompted for their email address when attempting to connect to the network.
 - b.** To specify custom web authentication windows, uncheck the Global WebAuth Configuration **Enabled** check box.
 - 1.** When the Web Auth Type drop-down menu appears, choose one of the following options to define the web login page for the wireless guest users:
Internal—Displays the default web login page for the controller. This is the default value.

Customized—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down menus 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 menu if you do not want to display a customized page for that option.

These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For specifics on downloading custom pages, refer to the [“Downloading Customized Web Authentication”](#) section on page 3-17.

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 field.

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



Note

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

- Step 3** If you selected External as the Web Authentication Type in Step 2, click **Security > AAA** and choose up to three RADIUS and LDAP servers using the drop-down menus.
- Step 4** Click **Save**.
- Step 5** Repeat this process if a second (anchor) controller is being used in the network.

AAA Servers

When you choose the AAA Servers tab, the window shown in [Figure 11-8](#) appears.

Figure 11-8 AAA Servers Window

Wireless Control System

User: root | Virtual Domain: root | Refresh | Print View | Logout

WLAN Template> Template 'gz-fran1' Save Apply to Controllers ... Delete Cancel

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

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

RADIUS Servers

	Authentication Servers	Accounting Servers
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 ☐ Enabled

Allow AAA Override ☐ Enabled

Save Apply to Controllers ... Delete Cancel

Foot Notes

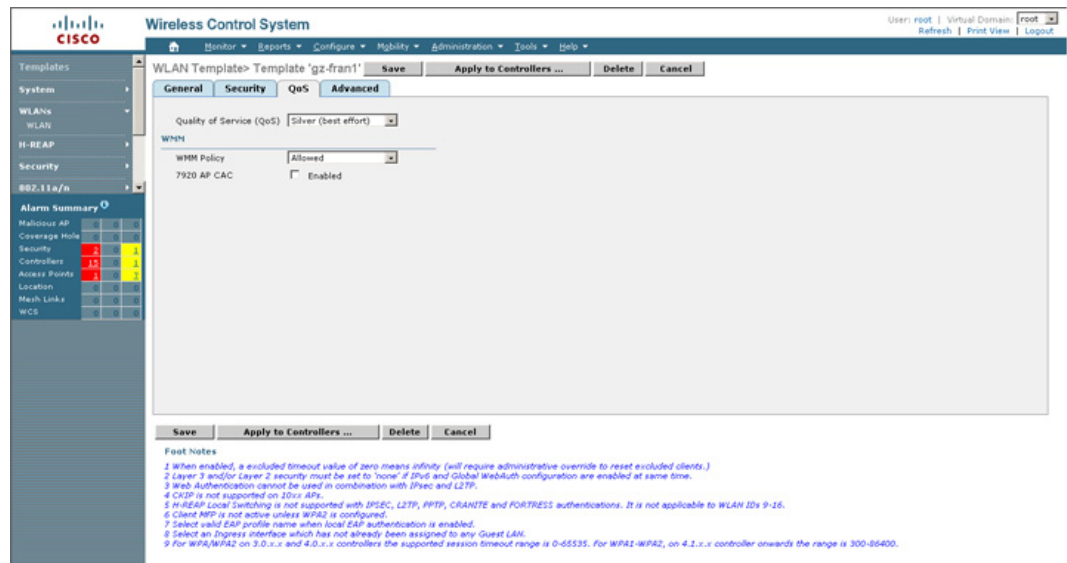
1 When enabled, a excluded timeout value of zero means infinity (will require administrative override to reset excluded clients.)
 2 Layer 3 and/or Layer 2 security must be set to 'none' if IPv6 and Global Webauth configuration are enabled at same time.
 3 Web Authentication cannot be used in combination with IPsec and L2TP.
 4 CoSIP is not supported on 10xx APs.
 5 m-REAP Local Switching is not supported with IPSec, L2TP, PPTP, CRANITE and PORTRESS authentications. It is not applicable to WLAN IDs 9-16.
 6 Client MFP is not active unless WPA2 is configured.
 7 Select valid EAP profile name when local EAP authentication is enabled.
 8 Select an ingress interface which has not already been assigned to any Guest LAN.
 9 For WPA1/WPA2 on 3.0.x.x and 4.0.x.x controllers the supported session timeout range is 0-65535. For WPA1-WPA2, on 4.1.x.x controller onwards the range is 300-86400.

Follow these steps to configure the AAA Servers tab.

-
- Step 1** Use the drop-down menus in the RADIUS and LDAP servers section to choose authentication and accounting servers. This selects the default RADIUS server for the specified WLAN and overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority and so on. If no LDAP servers are chosen here, WCS uses the default LDAP server order from the database.
- Step 2** Click the Local EAP Authentication check box if you have an EAP profile already configured that you want to enable. Local EAP is an authentication method that allows users and wireless clients to locally authenticate. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.
- Step 3** When AAA Override is enabled, and a client has conflicting AAA and controller WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system also uses QoS and ACL provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as identity networking.)
- For instance, if the corporate WLAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.
- When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.
- The AAA override values may come from a RADIUS server, for example.
- Step 4** Click **Save**.
-

QoS

When you select the QoS tab from the WLAN Template window, the window as shown in [Figure 11-9](#) appears.

Figure 11-9 QoS Window

Follow these steps to configure the QoS tab.

- Step 1** Use the QoS drop-down menu to choose Platinum (voice), Gold (video), Silver (best effort), or Bronze (background). Services such as VoIP should be set to gold while non-discriminating services such as text messaging can be set to bronze.
- Step 2** Use the WMM Policy drop-down menu to choose Disabled, Allowed (so clients can communicate with the WLAN), or Required to make it mandatory for clients to have WMM enabled for communication.
- Step 3** Click the **7920 AP CAC** check box if you want to enable support on Cisco 7920 phones.
- Step 4** If you want WLAN to support older versions of the software on 7920 phones, click to enable the **7920 Client CAC** check box. The CAC limit is set on the access point for newer versions of software.
- Step 5** Click **Save**.

Advanced

When you click the Advanced tab on the WLAN Template window, the window shown in [Figure 11-10](#) appears.

Figure 11-10 Advanced Window

Wireless Control System Virtual Domain: root User: root Logout Refresh Print View

Monitor Reports Configure Mobility Administration Tools Help

WLAN> New Template Save Cancel

General Security QoS Advanced

H-REAP Local Switching ☐ Enabled

Diagnostic Channel ☐ Enabled

Aironet IE ☒ Enabled

IPv6 ☐ Enabled

Session Timeout(secs) 0

Override Interface ACL NONE

Peer to Peer Blocking Disable

Client Exclusion ☒ Enabled Timeout Value (secs) 60

NAC Support ☐ Enabled

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)

MFP Signature Generation ☐ Enabled

MFP Client Protection ☐ Optional

MFP Version 1

Save Cancel

Foot Notes

1 When enabled, a excluded 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 Web Authentication cannot be used in combination with IPsec and L2TP.

4 CKIP is not supported on 10xx APs.

5 H-REAP Local Switching is not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications. It is not applicable to WLAN IDs 9-16.

6 Client MFP is not active unless WPA2 is configured.

7 Select valid EAP profile name when local EAP authentication is enabled.

8 Select an Ingress interface which has not already been assigned to any Guest LAN.

9 For WPA/WPA2 on 3.0.x.x and 4.0.x.x controllers the supported session timeout range is 0-65535. For WPA1-WPA2, on 4.1.x.x controller onwards the range is 300-86400.

Step 1 Click the check box if you want to enable Hybrid REAP local switching. For more information on Hybrid REAP, see the [“Configuring Hybrid REAP”](#) section on page 13-4. If you enable it, the hybrid-REAP access point handles client authentication and switches client data packets locally.

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

Step 2 At the Session Timeout parameter, set the maximum time a client session can continue before requiring reauthorization.

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

Step 4 Click if you want to enable IPv6. You can configure IPv6 bridging and IPv4 web auth on the same WLAN. WCS disallows Layer 2 security with IPv6 bridging.



Note Layer 3 security must be set to *None* for this to be enabled.

- Step 5** A list of defined access control lists (ACLs) is provided at the Override Interface ACL drop-down menu. (Refer to the [“Configuring Access Control List Templates”](#) section on page 11-56 for steps on defining ACLs.) Upon choosing an ACL from the list, the WLAN associates the ACL to the WLAN. Selecting an ACL is optional, and the default for this parameter is None.
- Step 6** You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. At the Peer to Peer Blocking drop-down menu, 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—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet.

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



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

- Step 7** Click the check box if you want to enable automatic client exclusion. If you enable client exclusion, you must also set the Timeout Value in seconds for disabled client machines. Client machines are excluded by MAC address, and their status can be observed. A timeout setting of 0 indicates that administrative control is required to re-enable the client.



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

- Step 8** Check the NAC Support check box if you want to enable it. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing. Refer to the [“Configuring NAC Out-of-Band Integration”](#) section on page 10-18 for more information.

- Step 9** When you click the check box to override DHCP server, another parameter appears where you can enter the IP address of your DHCP server. For some WLAN configurations, this is required. Three valid configurations are as follows:

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

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

- Step 10** If the MFP Signature Generation check box is checked, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. Signature generation makes sure that changes to the transmitted management frames by an intruder are detected and reported.
- Step 11** At the MFP Client Protection drop-down menu, choose Optional, Disabled, or Required for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down menu is unavailable.

**Note**

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

Step 12 Click **Save**.

Configuring H-REAP AP Groups

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

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

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

Step 2 From the left sidebar menu, choose **HREAP > HREAP AP Groups**.

Step 3 The Template Name column shows the group names assigned to the HREAP access point groups. If you want to add an additional group, choose **Add HREAP AP Group** from the Select a command drop-down menu.

- or -

To make modifications to an existing template, click to select a template in the Template Name column. The General tab of the HREAP AP Groups template appears (see [Figure 11-11](#)).

Figure 11-11 AP Groups HREAP Template

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor Reports Configure Location Administration Tools Help

Templates

System

Alarm Summary

Malicious AP	0	0	0
Coverage Hole	0	0	0
Security	2	0	0
Controllers	0	0	0
Access Points	2	0	2
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

H-REAP AP Group > New Template

Save Cancel

General H-REAP AP H-REAP Configuration

Template Name

Primary Radius: none

Secondary Radius: none

Foot Notes

1 Select radius authentication server present on Controllers. If not present on Controller, WCS configured radius authentication server will not apply.

* Warning: AP Ethernet Mac Address cannot exist in more than one H-REAP group on same Controller. Please UnSelect the AP Ethernet Mac from one of the groups if applied to same Controller. Controller will not allow setting AP Ethernet Mac in a H-REAP AP Group if it is already present in another H-REAP group. You can still apply same AP Ethernet Mac list to different Controller

- Step 4** The Template Name parameter shows the group name assigned to the HREAP access point group.
- Step 5** Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply. A value of 10 indicates that the primary RADIUS server is not configured for this group.
- Step 6** Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply. A value of 0 indicates that the primary RADIUS server is not configured for this group.
- Step 7** If you want to add an access point to the group, click the **H-REAP AP** tab.
- Step 8** An access point Ethernet MAC address cannot exist in more than one H-REAP group on the same controller. If more than one group is applied to the same controller, click the **Ethernet MAC** check box to unselect an access point from one of the groups. You should save this change or apply it to controllers.
- Step 9** Click **Add AP**. The H-REAP AP Group window appears.
- Step 10** Click the **H-REAP Configuration** tab to enable local authentication for a hybrid REAP group.



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

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



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

- Step 12** To allow a hybrid-REAP access point to authenticate clients using LEAP, check the **LEAP** check box. Otherwise, to allow a hybrid-REAP access point to authenticate clients using EAP-FAST, check the **EAP-FAST** check box.
- Step 13** Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:
- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key and Confirm EAP-FAST Key field. The key must be 32 hexadecimal characters.
 - To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, check the **Auto key generation** check box.
- Step 14** In the EAP-FAST Authority ID field, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
- Step 15** In the EAP-FAST Authority Info field, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
- Step 16** In the EAP-FAST Pac Timeout field, specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.
- Step 17** Click **Submit**.
-

Configuring a File Encryption Template

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

-
- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > File Encryption**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The File Encryption Template appears (see [Figure 11-12](#)).

Figure 11-12 File Encryption Template

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar contains a navigation menu with categories: Templates, System, WLANs, and Security. The 'Security' category is expanded, showing options like File Encryption, RADIUS Auth Servers, and others. The main content area is titled 'File Encryption Template > Template 'FileEncryption_508''. It features a 'General' tab with the following fields: Template Name (FileEncryption_508), File Encryption (a checkbox labeled 'Enabled'), Encryption Key (a text input field), and Confirm Encryption Key (another text input field). At the bottom of the form are four buttons: Save, Apply to Controllers ..., Delete, and Cancel. In the top right corner, there is a user status bar showing 'Username: root' and links for Logout, Refresh, and Print View. At the bottom left, there is an 'Alarm Summary' table.

Alarm Summary			
Rogue AP	0		150
Coverage Hole	0		137
Security	9	0	2
Controllers	1	3	0
Access Points	762	0	40
Mesh Links	0	0	0
Location	1	0	14

- 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 template for RADIUS authentication server information or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** On the left sidebar menu, choose **Security > RADIUS Authentication Servers**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select the template in the Template Name column. The RADIUS Authentication Server Template window appears (see [Figure 11-13](#)), and the number of controllers the template is applied to automatically populates.

The IP address of the RADIUS server and the port number for the interface protocol is also displayed.

Figure 11-13 RADIUS Authentication Server Template

Alarm Summary			
Rogue AP	0	150	
Coverage Hole	137		
Security	9	0	2
Controllers	1	3	0
Access Points	762	0	40
Mesh Links	0	0	0
Location	1	0	14

Step 4 Use the drop-down menu to choose either ASCII or hex shared secret format.

**Note**

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

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

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

- Shared Secret Format: Determine whether ASCII or hexadecimal.

**Note**

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

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

**Note**

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

Step 7 Click if you want to enable administration privileges.

Step 8 Click if you want to enable support for RFC 3576. RFC 3576 is an extension to the Remote Authentication Dial In User Service (RADIUS) protocol. It allows dynamic changes to a user session and includes support for disconnecting users and changing authorizations applicable to a user session.

With these authorizations, support is provided for Disconnect and Change-of-Authorization (CoA) messages. Disconnect messages immediately terminate a user session, whereas CoA messages modify session authorization attributes such as data filters.

- Step 9** Click if you want to enable network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
- Step 10** Click if you want to enable management authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user.
- Step 11** Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller. You can specify a value between 2 and 30 seconds.
- Step 12** If you click to enable the IP security mechanism, additional IP security parameters are added to the window, 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 menu to choose which IP security authentication protocol to use. The options are HMAC-SHA1, HMAC-MD5, and None.

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

- Step 14** Set the IP security encryption mechanism to use. Options are as follows:
- DES—Data Encryption Standard is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
 - Triple DES—Data Encryption Standard that applies three keys in succession.
 - AES 128 CBC—Advanced Encryption Standard uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Block Chaining (CBC) mode.
 - None—No IP security encryption mechanism.
- Step 15** The Internet Key Exchange (IKE) authentication is not an editable field. 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 menu to choose either aggressive or main. This sets the IKE protocol. IKE phase 1 is used to negotiate how IKE is protected. Aggressive mode passes more information in fewer packets, with the benefit of a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.
- Step 17** At the Lifetime parameter, set the timeout interval (in seconds) when the session expires.
- Step 18** Set the IKE Diffie Hellman group. The options are group 1 (768 bits), group 2 (1024 bits), or group 5 (1536 bits). Diffie-Hellman techniques are used by two devices to generate a symmetric key where you can publicly exchange values and generate the same symmetric key.
- Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size.
- Step 19** Click **Save**.
-

Configuring a RADIUS Accounting Template

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > RADIUS Acct Servers**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The RADIUS Accounting Template appears (see [Figure 11-14](#)), and the number of controllers the template is applied to automatically populates. The IP address of the RADIUS server and the port number for the interface protocols are also displayed.

Figure 11-14 RADIUS Accounting Server Templates

Alarm Summary			
Rogue AP	0	150	
Coverage Hole	1	137	
Security	9	0	2
Controllers	1	3	0
Access Points	762	0	40
Mesh Links	0	0	0
Location	1	0	14

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



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

- Step 5** Enter the RADIUS shared secret used by your specified server.
- Step 6** Retype the shared secret.
- Step 7** Click if you want to establish administrative privileges for the server.
- Step 8** Click if you want to enable the network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
- Step 9** Specify the time in seconds after which the RADIUS authentication request will timeout and a retransmission by the controller will occur. You can specify a value between 2 and 30 seconds.

Step 10 Click **Save**.

Configuring a LDAP Server Template

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

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

Step 2 From the left sidebar menu, choose **Security > LDAP Servers**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The LDAP Server Template appears (see [Figure 11-15](#)). The IP address of the LDAP server and the port number for the interface protocols are displayed.

Figure 11-15 LDAP Server Template

Alarm Summary			
Malicious AP	1	0	1
Coverage Hole	0	0	0
Security	8	0	2
Controllers	12	0	1
Access Points	4	0	4
Location	0	0	10
Mesh Links	0	0	0
WCS	0	1	0

Step 4 In the Server User Base DN field, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

Step 5 In the Server User Attribute field, enter the attribute that contains the username in the LDAP server.

Step 6 In the Server User Type field, enter the ObjectType attribute that identifies the user.

Step 7 In the Retransmit Timeout field, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

- Step 8** Check the Admin Status check box if you want the LDAP server to have administrative privileges.
- Step 9** Click **Save**.

Configuring a TACACS+ Server Template

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** On the left sidebar menu, choose **Security > TACACS+ Server**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user in the Template Name column. The TACACS+ Server Template appears (see [Figure 11-16](#)). The IP address and the port number of the TACACS+ template are displayed.

Figure 11-16 TACACS+ Server Template

The screenshot shows the Cisco Wireless Control System (WLC) GUI. The left sidebar has a menu with 'Templates' expanded, showing 'System', 'WLANs', and 'Security'. Under 'Security', 'TACACS+ Servers' is selected. The main content area is titled 'TACACS+ Server > New Template'. It contains a 'General' tab with the following fields: 'Template Name' (text input), 'Server Type' (dropdown menu set to 'Authentication'), 'Server Address' (text input '0.0.0.0'), 'Port Number' (text input '49'), 'Shared Secret Format' (dropdown menu set to 'ASCII'), 'Shared Secret' (text input), 'Confirm Shared Secret' (text input), 'Admin Status' (checkbox labeled 'Enabled'), and 'Retransmit Timeout' (text input '2' followed by 'seconds'). At the bottom are 'Save' and 'Cancel' buttons. The top of the page shows the Cisco logo and 'Wireless Control System' title, with a navigation bar including 'Monitor', 'Reports', 'Configure', 'Location', 'Administration', and 'Help'. The top right corner shows 'Username: root | Logout | Refresh | Print View'.

- Step 4** Select the server type. The choices are authentication, authorization, or accounting.
- Step 5** Use the drop-down menu to choose either ASCII or hex shared secret format.



Note

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

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

- Step 7** Re-enter the shared secret in the Confirm Shared Secret field.
- Step 8** Check the Admin Status check box if you want the TACACS+ server to have administrative privileges.
- Step 9** Specify the time in seconds after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.
- Step 10** Click **Save**.
-

Configuring a Local EAP General Template

This page allows you to specify a timeout value for local EAP. You can then add a template with this timeout value or make changes to an existing 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 Templates**.
- Step 2** From the left sidebar menu, choose **Security > Local EAP General**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Local EAP General Template appears (see [Figure 11-17](#)).

Figure 11-17 **Local EAP General Template**


Wireless System

[Home](#)
[Monitor](#)
[Reports](#)
[Configure](#)
[Location](#)
[Administration](#)
[Tools](#)
[Help](#)

Username: root | [Logout](#) | [Refresh](#) | [Print View](#)

H-REAP AP Groups
Security
 File Encryption
 RADIUS Auth Servers
 RADIUS Acct Servers
 LDAP Servers
 TACACS+ Servers
 Network Access Control
 Local EAP General
 Local EAP Profiles
 EAP-FAST Parameters
 Network Users Priority
 Local Net Users
 Guest Users
 User Login Policies
 MAC Filtering
 AP / LBS Authorization
 Disabled Clients
 Access Control

General > Template'LocalEapGeneral_15252'
General

Template Name	LocalEapGeneral_15252
Local Auth Active Timeout (in secs)	300
Local EAP Identity Request Timeout(in secs)	1
Local EAP Identity Request Maximum Retries	20
Local EAP Dynamic Wep Key Index	0
Local EAP Request Timeout(in secs)	1
Local EAP Request Maximum Retries	20

Save
Apply to Controllers ...
Delete
Cancel

** The timeout period during which Local EAP will always be used after all Radius Servers are failed.Only this parameter will be applied to controller version less than 5.0.20.0*

Alarm Summary

Rogue AP	0	0	322
Coverage Hole	0	0	6
Security	4	0	0
Controllers	0	0	4
Access Points	122	0	13
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

Step 4 In the Local Auth Active Timeout field, 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 new template for the local EAP profile 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 Templates**.
- Step 2** From the left sidebar menu, choose **Security > Local EAP Profiles**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Local EAP Profiles Template appears (see [Figure 11-18](#)).

Figure 11-18 Local EAP Profiles Template

Category	Count
Malicious AP	0
Coverage Hole	0
Security	1
Controllers	1
Access Points	1
Location	0
Mesh Links	0
WCC	0

- Step 4** Each EAP profile must be associated with an authentication type(s). Choose the desired authentication type from the choices below:
- **LEAP** — This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
 - **EAP-FAST** — This authentication type (Flexile 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 Issues drop-down menu to determine whether Cisco or another vendor issued the certificate for authentication. Only EAP-FAST and TLS require a certificate.
- Step 6** If you want the incoming certificate from the client to be validated against the certificate authority (CA) certificates on the controller, check the **Check Against CA Certificates** check box.
- Step 7** If you want the common name (CN) in the incoming certificate to be validated against the CA certificates' CN on the controller, check the **Verify Certificate CN Identity** check box.
- Step 8** If you want the controller to verify that the incoming device certificate is still valid and has not expired, check the **Check Against Date Validity** check box.
- Step 9** If you want the device certificate on the controller to be used for authentication, check the **Local Certificate Required** check box. This certification is applicable only to EAP-FAST.
- Step 10** If you want the wireless clients to send their device certificates to the controller in order to authenticate, check the **Client Certificate Required** check box. This certification is only applicable to EAP-FAST.
- Step 11** Click **Save**.
- Step 12** Follow these steps to enable local EAP:
- a. Choose **WLAN > WLANs** from the left sidebar menu.
 - b. Click the profile name of the desired WLAN.
 - c. Click the **Security > AAA Servers** tab to access the AAA Servers page.
 - d. Check the **Local EAP Authentication** check box to enable local EAP for this WLAN.
- Step 13** Click **Save**.
-

Configuring an EAP-FAST Template

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

-
- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > EAP-FAST Parameters**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The EAP-FAST Parameters Template appears (see [Figure 11-18](#)).

Figure 11-19 EAP-FAST Parameters Template

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor Reports Configure Location Administration Help

EAP-FAST Parameters templates > Template 'EapFastParams_330068'

General

Template Name EapFastParams_330068

Time to live for the PAC 10 (1 - 1000) days

Authority ID Cisco

Authority Info Cisco A-ID

Server Key ••••

Confirm Server Key ••••

Anonymous Provision ☒

Save Apply to Controllers ... Delete Cancel

Alarm Summary

Rogue AP	0	0	759
Coverage Hole	0	0	0
Security	1	0	0
Controllers	4	1	3
Access Points	9	0	14
Location	0	0	4
Mesh Links	0	0	0
WCS	0	0	0

- Step 4** In the Time to Live for the PAC field, 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 field, enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.
- Step 6** In the Authority ID field, enter the ID for the authority identifier of the local EAP-FAST server.
- Step 7** In the Authority Info field, enter the authority identifier of the local EAP-FAST server in text format.
- Step 8** In the Server Key and Confirm Server Key fields, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.
- Step 9** If a local certificate is required, click the check box.
- Step 10** If a client certificate is required, click the check box.
- Step 11** If an anonymous provision is required, click the check box.
- Step 12** If you want to enable anonymous provisioning, check the **Client Authentication 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 13** Click **Save**.

Configuring Network User Credential Retrieval Priority Templates

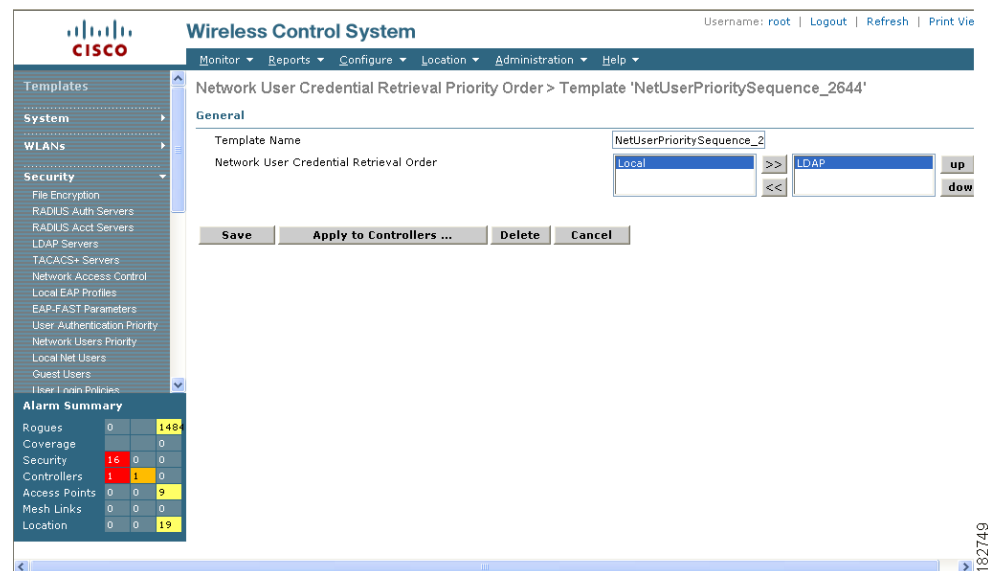
You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add a new template for the network user credential retrieval priority or make modifications to an existing template.

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

Step 2 From the left sidebar menu, choose **Security > Network Users Priority**.

To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Network User Credential Retrieval Priority Template appears (see [Figure 11-20](#)).

Figure 11-20 Network User Credential Retrieval Priority Order Template



Step 3 Use the left and right pointing arrows to include or disclude network user credentials in the right-most window.

Step 4 Use the up and down buttons to determine the order credentials are tried.

Step 5 Click **Save**.

Configuring a Local Network Users Template

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

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

- Step 2** On the left sidebar menu, choose **Security > Local Net Users**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user in the User Name column. The Local Net Users Template appears (see [Figure 11-21](#)).

Figure 11-21 Local Net Users Template

Wireless Control System

User: root | Virtual Domain: root
Refresh | Print View | Logout

Monitor | Reports | Configure | Mobility | Administration | Tools | Help

Local Net Users > Template 'localnet1'

General

Template Name: localnet1
 User Name: localnet1
 No of Controllers Applied To: 0
 Password:
 Confirm Password:
 Profile: Any Profile
 Description: first localnet1

Save Apply to Controllers ... Delete Cancel

Alarm Summary

Malicious AP	0	0	243
Coverage Hole	0	0	0
Security	6	0	2
Controllers	11	0	0
Access Points	3	0	10
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

- Step 4** If you keep Import from File enabled, you need to enter a file path or click the Browse button to navigate to the file path. Then continue to Step 10. If you disable the import, continue to Step 5.



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

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

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

- Step 5** 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 6** Enter a description of the profile.
- Step 7** Use the drop-down menu to choose the SSID which this local user is applied to or choose the *any SSID* option.
- Step 8** Enter a user-defined description of this interface. Skip to Step 10.
- Step 9** If you want to override the existing template parameter, click to enable this parameter.
- Step 10** Click **Save**.

Configuring Guest User Templates

This page allows you to create a new template for guest user information or make modifications to an existing 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. Refer to the [“Creating Guest User Accounts” section on page 7-11](#) for further information on guest access.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > Guest Users**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user in the User Name column. The General Guest User Template window appears (see [Figure 11-22](#)).

Figure 11-22 Guest User Template

- Step 4** Enter a guest name. Maximum size is 24 characters.
- Step 5** Click the **Generate Password** check box if you want a password automatically generated. The Password and Confirm Password parameters are automatically populated. If automatic generation is not enabled, you must supply a password twice.



Note If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unchecked), one password is supplied for a span of days.

- Step 6** Click the **Advanced** tab.
- Step 7** If you want to import multiple users, click the **Import From File** check box.
- Step 8** Click **Browse** to go to the file path where the CSV is located. The Sample CSV file is as follows:
 User Name| Password| Life Time| Description| Disclaimer
 Guest-1,pwd1,864000,Description-1,Disclaimer-1
 Guest-2,pwd2,864000,Description-2,Disclaimer-2



Note Table headings are not required, and description and disclaimer are not mandatory.

- Step 9** Choose a user role for the guest user from the drop-down menu. User roles are predefined by the administrator and are associated with the guests' access (such as contractor, customer, partner, vendor, visitor, and so on).
- User Role is used to manage the amount of bandwidth allocated to specific users within the network.
- Step 10** Define how long the guest user account will be active by choosing either the Limited or Unlimited Lifetime option.
- For the limited option, you choose the period of time that the guest user account is active using the hours and minutes drop-down menus. The default value for Limited is one day (8 hours).
 - When Unlimited is chosen, there is no expiration date for the guest account.
- Step 11** Choose the area (indoor, outdoor), controller list, or config group to which the guest user traffic is limited from the Apply to drop-down menu.
- If you choose the controller list option, a list of controller IP addresses appears. Check the check box next to all controller networks on which guest traffic is allowed.
- Step 12** (Optionally) Modify the default guest user description if necessary.
- Step 13** (Optionally) Modify the Disclaimer text, if necessary. If you want the supplied text to be the default, click the **Make this Disclaimer default** check box.
- Step 14** Click **Save**.
-

Configuring a User Login Policies Template

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

-
- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > User Login Policies**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a user login policy in the Template Name column. The User Login Policies Template window appears (see [Figure 11-23](#)).

Figure 11-23 User Login Policies Template

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Help

Templates

System

WLANS

Security

File Encryption

RADIUS Auth Servers

RADIUS Acct Servers

LDAP Servers

TACACS+ Servers

Network Access Control

Local EAP General

Local EAP Profiles

EAP-FAST Parameters

Network Users Priority

Local Net Users

Guest Users

User Login Policies

MAC Filtering

Alarm Summary

Rogue AP	0	140	0
Coverage Hole	0	0	0
Security	2	0	0
Controllers	0	1	0
Access Points	1	0	2
Mesh Links	0	0	0
Location	0	0	0

User Login Policies Template > Template 'UserLoginPolicy_5192'

General

Template Name: UserLoginPolicy_5192

Maximum Number of Concurrent Logins for a single user name: 0

Save Apply to Controllers ... Delete Cancel

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 new MAC filter template or make modifications to an existing template.

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

Step 2 From the left sidebar menu, choose **Security > MAC Filtering**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a MAC address in the MAC Address column. The MAC Filter Templates window appears (see [Figure 11-24](#)).

Figure 11-24 **MAC Filter Templates**

Wireless Control System User: root | Virtual Domain: root | Refresh | Print View | Logout

MAC Filter Templates > Template 'ba1122334455'

General

Template Name: ba1122334455
 MAC Address: BA:11:22:33:44:55
 No of Controllers Applied To: 0
 Profile Name: Any Profile
 Interface: management
 Description: testing CSCsk47438

Save Apply to Controllers ... Delete Cancel

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

Alarm Summary

Malicious AP	0	0	245
Coverage Hole	0	0	0
Security	6	0	2
Controllers	11	0	0
Access Points	3	0	10
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

- Step 4** If you keep Import From File enabled, you need to enter a file path or click the Browse button to navigate to the file path. The import file must be a CSV file with MAC address, profile name, interface, and description (such as 00:11:22:33:44:55,Profile1,management,test filter). If you disable Import from File, continue to Step 5. Otherwise, skip to Step 9.

The client MAC address appears.

- Step 5** Choose the SSID which this MAC filter is applied to or choose the *any SSID* option.
- Step 6** Use the drop-down menu to choose from the available interface names.
- Step 7** Enter a user-defined description of this interface. Skip to Step 9.
- Step 8** If you want to override the existing template parameter, click to enable this parameter.
- Step 9** Click **Save**.

Configuring an Access Point or LBS Authorization

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

- Step 1** Choose **Configure > Controller Templates**
- Step 2** From the Security selections in the left sidebar menu, choose **AP/LBS authorization**.

- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a MAC address in the AP Base Radio MAC column. The AP/LBS Authorization Template appears (see [Figure 11-25](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-25 AP/LBS Authorization Templates

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar contains a navigation menu with categories: Templates, System, WLANs, H-REAP, and Security. The Security category is expanded, showing options like File Encryption, RADIUS Auth Servers, RADIUS Acct Servers, LDAP Servers, TACACS+ Servers, Local EAP General, Local EAP Profiles, EAP-FAST Parameters, Network Users Priority, Local Net Users, Guest Users, User Login Policies, and MAC Filtering. The main content area is titled 'Wireless Control System' and shows the configuration for 'AP / LBS Authorization Templates > Template '00c09fdf43ee''. The 'General' tab is active, displaying the following fields: Template Name (00c09fdf43ee), AP/LBS Base Radio MAC (00:C0:9F:DF:43:EE), No of Controllers Applied (0), Certificate Type (LBS-SSC), and Key Hash (8044b0e51f88dac13ebcd57f10205569c4ef44bf). At the bottom of the configuration area are three buttons: 'Apply to Controllers ...', 'Delete', and 'Cancel'. An 'Alarm Summary' table is visible at the bottom left of the main area.

Alarm Summary			
Malicious AP	0	0	244
Coverage Hole	0	0	0
Security	5	0	2
Controllers	11	0	0
Access Points	3	0	10
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

- 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, xxx). Any other file formats are not supported.

- Step 5** Enter the file path from where you want to import the file.
- Step 6** Click **Save**.

Configuring a Manually Disabled Client Template

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

- Step 1** Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Disabled Clients**.

To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a disabled client in the Template Name column. The Manually Disabled Clients Template window appears (see [Figure 11-26](#)).

Figure 11-26 Manually Disabled Clients Template

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar contains a navigation menu with categories like Templates, System, WLANs, H-REAP, and Security. The Security section is expanded, showing various security-related options. The main content area displays the 'Manually Disabled Clients > New Template' window. This window includes a 'General' tab with three input fields: 'Template Name', 'MAC Address', and 'Description'. Below these fields are 'Save' and 'Cancel' buttons. At the bottom left of the interface, there is an 'Alarm Summary' table.

Alarm Summary			
Malicious AP	0	0	241
Coverage Hole	0	0	0
Security	6	0	2
Controllers	11	0	0
Access Points	9	0	10
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

Step 3 Enter the MAC address of the client you want to disable.

Step 4 Enter a description of the client you are setting to disabled.

Step 5 Click **Save**.

Configuring a CPU Access Control List (ACL) Template

The existing ACLs established in the “[Configuring Access Control List Templates](#)” section on [page 11-56](#) is used to set traffic controls between the central processing unit (CPU) and network processing unit (NPU). Follow these steps to add a CPU ACL template or make modifications to an existing template.

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

Step 2 Choose **Security > CPU Access Control List** in the left sidebar menu.

Step 3 If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the ACL Name column. The CPU Access Control List Template appears (see [Figure 11-27](#)).

Figure 11-27 CPU Access Control List Template

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Help

CPU Access Control List > Template 'CpuAcl__2440'

General

Template Name: CpuAcl__2440

No of Controllers Applied To: 2

CPU Access Control List

Enable CPU ACL: ☐

Save Apply to Controllers ... Delete Cancel

Alarm Summary

Rogues	0	150
Coverage	13	0
Security	1	0
Controllers	0	0
Access Points	0	11
Mesh Links	0	0
Location	0	19

- Step 4** If you click the check box to enable CPU ACL, two more parameters appear. When CPU ACL is enabled and applied on the controller, WCS displays the details of the CPU ACL against that controller.
- Step 5** From the ACL Name drop-down menu, choose a name from the list of defined names.
- Step 6** From the CPU ACL Mode drop-down menu, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.
- Step 7** Click **Save**.

Configuring a Rogue Policies Template

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > Rogue Policies**.
- Step 3** If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the Template Name column. The Rogue Policy Setup Template appears (see [Figure 11-28](#)).

Figure 11-28 Rogue Policy Setup Template

- Step 4** Check the **Rogue Location Discovery Protocol** to enable the discovery of rogue access points. Rogue Location Discovery Protocol (RLDP) determines whether or not the rogue is connected to the enterprise wired network.



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

- Step 5** Set the expiration timeout (in seconds) for rogue access point entries.
- Step 6** Check the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.
- Step 7** Check the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in adhoc networking.
- Step 8** Click **Save**.

Configuring a Rogue AP Rules Template

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



Note Rogue access point rules also help reduce false alarms.

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configure > Controller Templates > Security > Rogue AP Rules**. If you want to view rogue access point rules, refer to the [“Viewing or Editing Rogue Access Point Rules”](#) section on page 9-17.



Note Rogue classes include the following types:

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

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > Rogue AP Rules**.
- Step 3** From the Select a command drop-down menu, choose **Add Classification Rule** and click **GO**. The Rogue AP Rules > New Template window appears (see [Figure 11-29](#)). To make modifications to an existing rogue access point rules template or to apply a current template to the controllers, choose **Configure > Controller Templates > Security > Rogue AP Rules** and click a template name in the Template Name column.

Figure 11-29 *Rogue AP Rules > New Template Window*

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Tools | Help

Rogue AP Rules > New Template

General

Rule Name:

Rule Type:

Match Type:

Malicious Rogue Classification Rule

Open Authentication ☐

Match Managed AP SSID ☐

Match User Configured SSID (Enter one per line)

Minimum RSSI: dB ☐

Time Duration: seconds ☐

Minimum Number Rogue Clients: ☐

Note: 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 portion of the window, enter the following parameters:

- Rule Name—Enter a name for the rule in the text box.

- Rule Type—Choose **Malicious** or **Friendly** from the drop-down menu. 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 menu.

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

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



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

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



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

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



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

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



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

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

Step 6 Click **Save**.

Configuring a Rogue AP Rule Groups Template

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers.

To view current rogue access point rule groups templates, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups**.

Follow these steps to create a new Rogue AP Rule Groups template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > Rogue AP Rule Groups**.
- Step 3** From the Select a command drop-down menu, click **Add Rogue Rule Group**.
- Step 4** Click **GO**. The Rogue AP Rule Groups > New Template window appears (see [Figure 11-30](#)).

Figure 11-30 *Rogue AP Rule Groups > New Template*

Category	Count	Severity
Malicious AP	0	0
Coverage Hole	0	0
Security	4	0
Controllers	0	2
Access Points	10	0
Location	0	0
Mesh Links	0	0
WCS	0	0



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

- Step 5** Enter a name for the rule group in the General portion of the window.
- 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. Refer to the [“Configuring a Rogue AP Rules Template”](#) section on page 11-44 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 window 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-LWAPP access points from being falsely identified as rogues.

**Note**

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

To view or edit the current list of friendly access points, choose **Configure > Controller Templates > Security > Friendly AP**. The friendly access point screen identifies the access point's MAC address, status, any comments, and whether or not the alarm is suppressed for this access point.

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > Friendly AP**.
- Step 3** From the Select a command drop-down menu, choose **Add Friendly**.
- Step 4** Click **GO**. The Friendly AP window appears (see [Figure 11-31](#)).

**Note**

To make modifications to an existing friendly access point, choose **Configure > Controller Templates > Security > Friendly Internal** and click the access point's MAC address. Make the necessary changes to the access point and click **Save**.

Figure 11-31 Friendly AP > Add Friendly AP Window

Alarm Summary				
Malicious AP	0	0	0	0
Coverage Hole	0	0	0	0
Security	4	0	0	0
Controllers	0	0	2	0
Access Points	10	0	0	0
Location	0	0	0	0
Mesh Links	0	0	0	0
WCS	0	0	0	0

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

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

**Note**

Use a line break to separate MAC addresses. For example, you could enter the MAC addresses as follows:

```
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46
```

- Choose **Internal** access point from the Status drop-down menu.
- Enter a comment regarding this access point, if necessary.
- Check the **Suppress Alarms** check box to suppress all alarms for this access point.
- Click **Save** to confirm this access point or **Cancel** to close the window without adding the access point to the list.

Configuring a Client Exclusion Policies Template

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** Choose **Security > Client Exclusion Policies** in the left sidebar menu.

If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the Template Name column. The Client Exclusion Policies Template appears (see [Figure 11-32](#)).

Figure 11-32 Client Exclusion Policies Template

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor | Reports | **Configure** | Location | Administration | Help

Client Exclusion Policies Template > Template 'ClientExclusionPolicy_316232'

General

Template Name: ClientExclusionPolicy_3162

Excessive 802.11 Association Failures: ☒ Enabled

Excessive 802.11 Authentication Failures: ☒ Enabled

Excessive 802.1X Authentication Failures: ☒ Enabled

Excessive 802.11 Web Authentication Failures: ☒ Enabled

IP Theft Or Reuse: ☒ Enabled

Save Apply to Controllers ... Delete Cancel

Alarm Summary

Rogue AP	0	0	708
Coverage Hole	0	0	0
Security	1	0	0
Controllers	4	1	3
Access Points	9	0	14
Location	0	0	4
Mesh Links	0	0	0
WCS	0	0	0

232536

- Step 3** To edit an existing client exclusion policies template, click its name in the Template Name column to go the Client Exclusion Policies Template window. Create or edit a client exclusion policies template by configuring its parameters.

Table 11-2 Client Exclusion Policies Template Parameters

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

Table 11-2 (continued)*Client Exclusion Policies Template Parameters*

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

Step 4 Click **Save**.

Configuring an Access Point Authentication and MFP Template

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

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

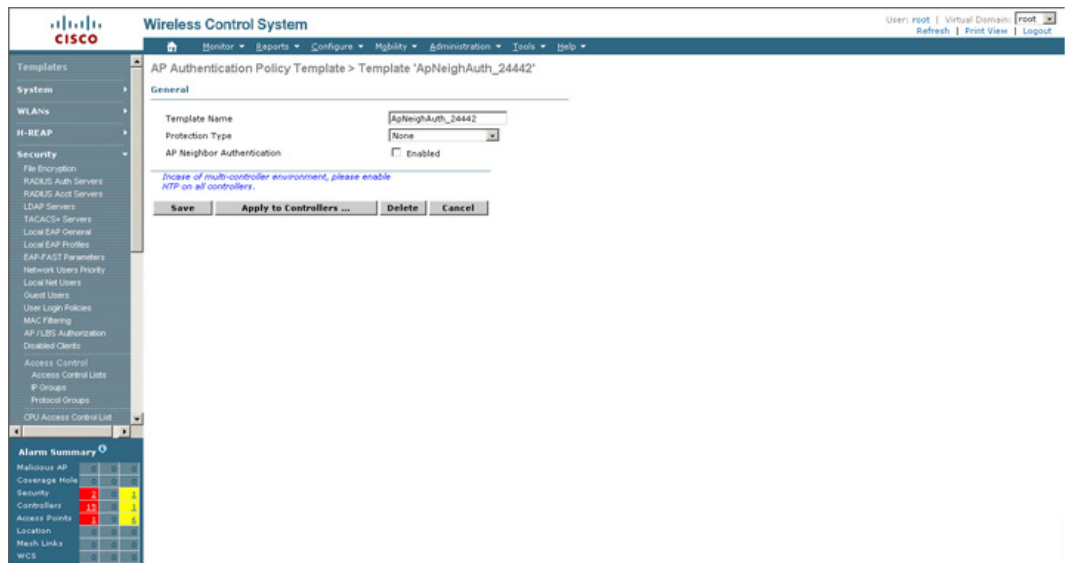
When MFP detection is enabled, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any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

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

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

Step 2 From the left sidebar menu, select **Security > AP Authentication and MFP**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a MAC address in the AP Base Radio MAC column. The AP Authentication Policy Template appears (see [Figure 11-33](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-33 AP Authentication Policy Template

- Step 4** From the Protection Type drop-down menu, choose one of the following authentication policies:
- None: No access point authentication policy.
 - AP Authentication: Apply authentication policy.
 - MFP: Apply management frame protection.
- Step 5** Check to enable AP neighbor authentication. With this feature enabled, the access points sending RRM neighbor packets with different RF network names are reported as rogues.
- Step 6** 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 7** Click **Save**.

Configuring a Web Authentication Template

With web authentication, guests are automatically redirected to a web authentication page when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts may be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. You can use this template to replace the Web authentication page provided on the controller.

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Security > Web Auth Configuration**.

- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Web Authentication Configuration Template window appears (see [Figure 11-34](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-34 Web Authentication Configuration Template

Alarm Summary		
Rogue AP	0	143
Coverage Hole	0	137
Security	9	2
Controllers	1	0
Access Points	766	41
Mesh Links	0	0
Location	1	14

- Step 4** Choose the appropriate web authentication type from the drop-down menu. 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 menu 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 field is `http://www.company.com`, the user would be directed to the company home page.

- Step 5** Click to enable Logo Display if you want your company logo displayed.
- Step 6** Enter the title you want displayed on the Web authentication page.
- Step 7** Enter the message you want displayed on the Web authentication page.
- Step 8** Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this field is `http://www.company.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. A customized web page is created to establish a username and password for user web access.

When downloading customized web authentication, these strict guidelines must be followed:

- A username must be provided.
- A password must be provided.
- A redirect URL must be retained as a hidden input item after extracting from the original URL.
- The action URL must be extracted and set from the original URL.
- Scripts to decode the return status code must be included.
- All paths used in the main page should be of relative type.

Before downloading, the following steps are required:

- Step 1** Download the sample login.html bundle file from the server. The .html file is shown in [Figure 11-35](#). The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 11-35 Login.html



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



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

- Step 3** Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:
- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add *IP address of TFTP server*).
 - If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
 - A third-party TFTP server cannot run on the same computer as the Cisco WCS because WCS's built-in TFTP server and third-party TFTP server use the same communication port.

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

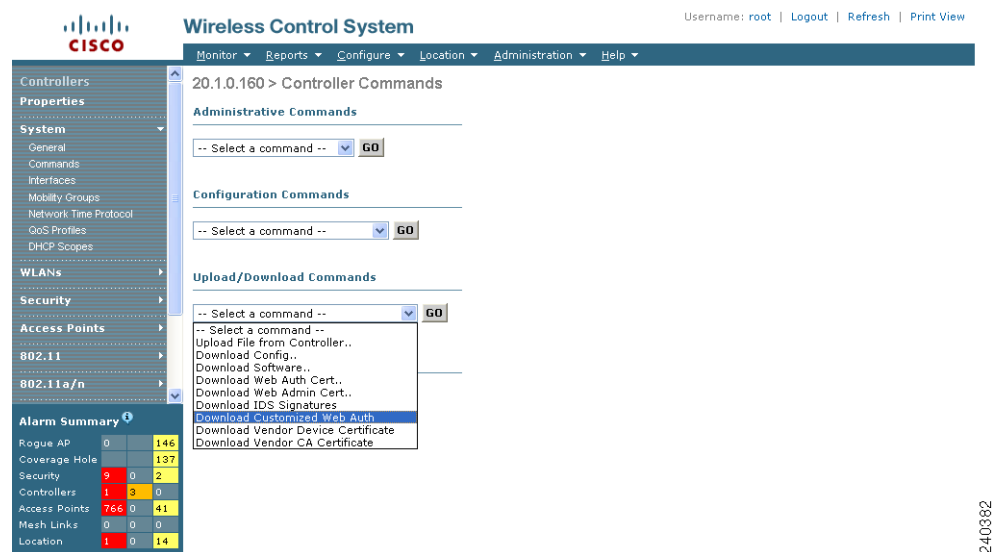
**Note**

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

You can now continue with the download.

- Step 5** Copy the file to the default directory on your TFTP server.
- Step 6** Choose **Configure > Controllers**.
- Step 7** Choose a controller by clicking the URL for the corresponding IP address. If you select more than one IP address, the customized Web authentication page is downloaded to multiple controllers.
- Step 8** From the left sidebar menu, choose **System > Commands**.
- Step 9** From the Upload/Download Commands drop-down menu, 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 (see [Figure 11-36](#)).

Figure 11-36 Download Customized Web Auth Bundle to Controller



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

**Note**

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

- Step 12** Enter the maximum number of times the controller should attempt to download the file in the Maximum Retries parameter.
- Step 13** Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout parameter.

- Step 14** The files are uploaded to the c:\tftp directory. Specify the local file name in that directory or use the Browse button to navigate to it.
- Step 15** Click **OK**.
- If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the administrator's workstation to WCS's own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the WCS server's TFTP directory, and the download web page now automatically populates the filename.
- Step 16** Click the "Click **here** to download a sample tar file" 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 Access Control List Templates

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** Choose **Access Control > Access Control Lists** in the left sidebar menu.
- Step 3** If you want to create a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the ACL Name column. The Access Control List name appears in the window.
- 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 menu and click **GO**. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group window opens.



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

- Step 6** To define an additional protocol that is not a standard predefined one, choose **Access Control > Protocol Groups** from the left sidebar menu. The protocol groups with their source and destination port and DSCP are displayed.
- Step 7** To create a new protocol group, choose **Add Protocol Group** from the Select a command drop-down menu and click **GO**. To view or modify an existing protocol group, click the URL of the group. The Protocol Groups window appears.

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

Step 9 In the Start Port parameter, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL. The rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if rules 1 through 4 are already defined and you add rule 29, it is added as rule 5.

**Note**

If you add or change a sequence number, the operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have sequence numbers 1 through 7 defined and change number 7 to 5, the operating system automatically reassigns sequence 5 to 6 and sequence 6 to 7. Any rules generated can be edited individually and resequenced in the desired order.

Step 10 From the Source Port drop-down menu, specify the source of the packets to which this ACL applies.

Step 11 For the Destination drop-down menu, specify the destination of the packets to which this ACL applies.

Step 12 In the DSCP drop-down menu, choose any or a specific IP address. 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 window, 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 menu. The Add Rule Mapping windows appears.

Step 16 Choose the desired IP address groups, protocol groups, and action and click **Add**. The new mappings will populate the bottom table.

Step 17 Click **Save**.

Step 18 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 Policy Name Template (for 802.11a/n or 802.11b/g/n)

Follow these steps to add a new policy name template for 802.11a/n or 802.11b/g/n or make modifications to an existing template.

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

Step 2 From the left sidebar menu, choose either **802.11a/n > Parameters** or **802.11b/g/n > Parameters**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu. To make modifications to an existing template, click to select a policy name in the Policy Name column. The 802.11a/n or b/g/n Parameters Template window appears (see [Figure 11-37](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-37 802.11a/n Parameters Template

- Step 4** Click the check box if you want to enable 802.11a/n or b/g/n network status.
- Step 5** Enter the amount of time between beacons in kilomicroseconds. The valid range is from 100 to 600 milliseconds.
- Step 6** Enter the number of beacon intervals that may 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.
- Step 7** At the Fragmentation Threshold parameter, determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
- Step 8** Enter the percentage for 802.11e maximum bandwidth.
- Step 9** Click if you want short preamble enabled.
- Step 10** Click the **Pico Cell Mode** check box if you want it enabled. This feature enables automatic operating system parameter reconfiguration, allowing the operating system to function efficiently in pico cell deployments.
- Step 11** Click the **Fast Roaming Mode** check box if you want to enable it. Enabling Cisco's Centralized Key Management (CCKM) authentication key management allows fast exchange when a client roams from one access point to another.
- Step 12** At the Dynamic Assignment drop-down menu, 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 Use the Tx Level drop-down menu to determine the access point's transmit power level. The available options are as follows:

- 1 - Maximum power allowed per country code setting
- 2 - 50% power
- 3 - 25% power
- 4 - 6.25 to 12.5% power
- 5 - 0.195 to 6.25% power



Note 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 menu has three dynamic channel modes:

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

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

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

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

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

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

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

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

- Step 19** Data rates are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it in order to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate may communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported in order to associate. For each rate, a pull-down selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match client settings.
- Step 20** At the Channel List drop-down menu in the Noise/Interference/Rogue Monitoring Channels section, choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.
- Step 21** The Cisco Compatible Extension's location measurement interval can only be changed when measurement mode is enabled to broadcast radio measurement requests. When enabled, this enhances the location accuracy of clients.
- Step 22** Click **Save**.
-

Configuring High Density Templates

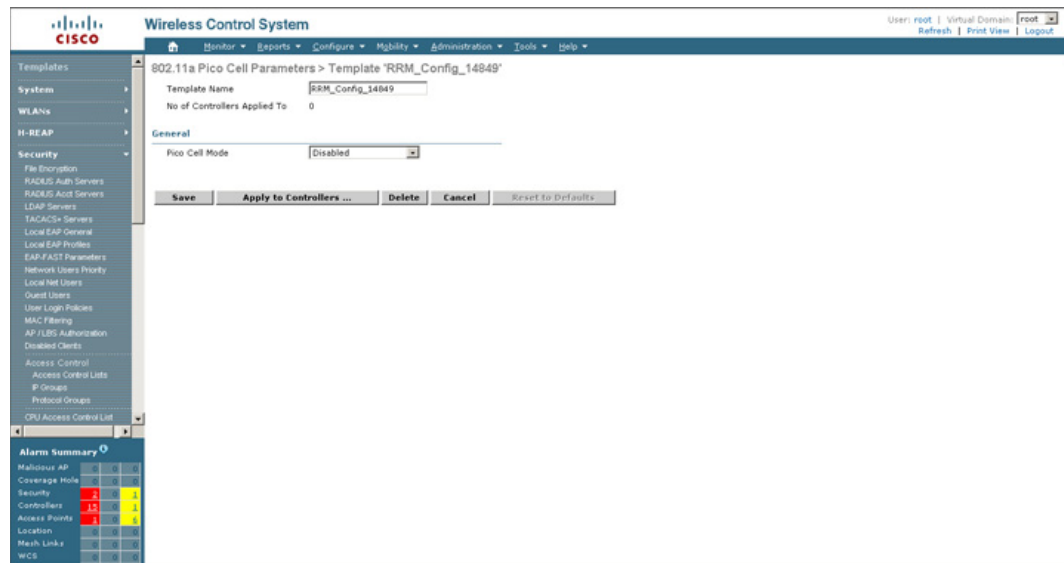
A method to mitigate the inter-cell contention problem in high-density networks is to adjust the access point and client station receiver sensitivity, CCA sensitivity, and transmit power parameters in a relatively cooperative manner. By adjusting these variables, the effective cell size can be reduced, not by lowering the transmit power but by increasing the necessary received power before an access point and client consider the channel sufficiently clear for packet transfer. Follow these steps to add high density on a template or make modifications to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose either **802.11a/n > Parameters**.
- Step 3** In the General portion of this window, you see a Pico Cell Mode parameter. Click the check box to enable pico cell.



Note In order for this check box to have validity, you must have software version 4.1 or later. If you have an earlier version, this check box value is ignored.

- Step 4** Choose **802.11a/n > Pico Cell** from the left sidebar menu. Click which template in the Template Name column you want to modify or choose **Add Template** from the Select a command drop-down menu and click **GO**. The window as shown in [Figure 11-38](#) appears.

Figure 11-38 Pico Cell Parameters Window

Note If the Pico Cell Mode parameter is set to Disabled or V1, the Pico Cell V2 parameters are grayed out.



Note For pico cell V2 to work with Intel 3945 clients, the QBSS feature also has to be enabled (i.e., WMM clients must be set to allowed), and fast roaming cannot be enabled.

Step 5 Go to **802.11a/n > Parameters** and ensure that the 802.11a/n Network Status check box is not enabled.

Step 6 From the Pico Cell Mode drop-down menu, choose **V2**. By choosing V2, the parameters for access point and clients share the same values and make communication symmetrical. This selection also allows you to put in values for Rx sensitivity, CCA sensitivity, and transmit power although the defaulted minimum and maximum values represent the Cisco recommended values for most networks.



Note You can only choose V2 if you have software version 4.1 or later.

Step 7 Set the Rx sensitivity based on the desired receiver sensitivity for 802.11a/n radios. The Current column shows what is currently set on the access point and clients, and the Min and Max columns show the range to which the access points and clients should adapt. Receiver signal strength values falling outside of this range are normally disregarded.

Step 8 Set the CCA sensitivity based on when the access point or client considers the channel clear enough for activity. The current column shows what is currently set on the access point and clients, and Min and Max columns show the range to which the access points and clients should adapt. CCA values falling outside of this range are normally disregarded.

Step 9 Click **Save** to save these values. Before choosing **Reset to Defaults** you must turn off the 802.11 network.

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

Follow these steps to add a template for either 802.11a/n or 802.11b/g/n voice parameters, such as call admission control and traffic stream metrics or make modifications to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose either **802.11a/n > Voice Parameters** or **802.11b/g/n > Voice Parameters**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The 802.11a/n or 802.11b/g/n Voice Parameters window appears (see [Figure 11-39](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-39 802.11b/g/n Voice Parameters Template

The screenshot shows the Cisco Wireless Control System (WCS) configuration page for the 802.11b/g/n Voice Parameters Template. The interface includes a top navigation bar with 'Monitor', 'Reports', 'Configure', 'Location', 'Administration', and 'Help' menus. The left sidebar shows the '802.11b/g/n' section expanded, with 'Voice Parameters' selected. The main content area displays the '802.11b/g Voice Parameters > Template "Voice_Qos_3318"' configuration page. The 'General' section shows the 'Template Name' as 'Voice_Qos_3318' and 'No of Controllers Applied To' as 1. The 'Call Admission Control' section has 'Enable CAC' unchecked, 'Use Load-based AC' checked, 'Maximum Bandwidth Allowed' set to 0, 'Reserved Roaming Bandwidth' set to 0, and 'Enable Expedited Bandwidth' unchecked. The 'Traffic Stream Metrics' section has 'Enable metric collection' unchecked. At the bottom, there are buttons for 'Save', 'Apply to Controllers ...', 'Delete', and 'Cancel'. An 'Alarm Summary' table is visible in the left sidebar.

Alarm Summary			
Rogue AP	0		146
Coverage Hole			0
Security	0	0	0
Controllers	0	0	0
Access Points	23	0	1
Mesh Links	0	0	0
Location	0	0	0

- Step 4** For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity. Click the check box to enable CAC.
- Step 5** Load-based 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. To enable load-based CAC for this radio band, check the Use Load-based AC check box.
- Step 6** Enter the percentage of maximum bandwidth allowed.
- Step 7** Enter the percentage of reserved roaming bandwidth.

- Step 8** Click if you want to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is Cisco Compatible Extensions (version 5) compliant so that a TSPEC request is given higher priority.
- Step 9** Click the check box if you want to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and informs 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/n interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.
- Step 10** Click **Save**.

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

Follow these steps to add a template for either 802.11a/n or 802.11b/g/n video parameters or make modifications to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose either **802.11a/n > Video Parameters** or **802.11b/g/n > Video Parameters**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The 802.11a/n or 802.11b/g/n Video Parameters window appears (see [Figure 11-40](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-40 802.11a/n Video Parameters Template

The screenshot shows the Cisco Wireless Control System interface. The left sidebar menu is expanded to show '802.11b/g/n' parameters, with 'Video Parameters' selected. The main content area displays the configuration for the 'Video_Qos_3141' template. The 'General' section shows the template name and the number of controllers applied to (1). The 'Call Admission Control' section has an 'Enable CAC' checkbox and fields for 'Maximum Bandwidth Allowed' (0) and 'Reserved Roaming Bandwidth' (1). At the bottom, there are buttons for 'Save', 'Apply to Controllers ...', 'Delete', and 'Cancel'. An 'Alarm Summary' table is visible on the left, showing counts for various alarms like Rogue AP, Coverage Hole, Security, Controllers, Access Points, Mesh Links, and Location.

Alarm Summary		
Rogue AP	0	343
Coverage Hole	0	0
Security	6	0
Controllers	0	0
Access Points	0	8
Mesh Links	0	0
Location	0	0

- Step 4** For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keeps the maximum allowed number of calls to an acceptable quantity. Click the check box to enable CAC.
- Step 5** Enter the percentage of maximum bandwidth allowed.

- Step 6** Enter the percentage of reserved roaming bandwidth.
- Step 7** Click **Save**.

Configuring EDCA Parameters through a Controller Template

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, select **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters** to open the EDCA Parameters summary page (see [Figure 11-41](#)).

Figure 11-41 802.11a Pico Cell Parameters

- Step 3** Modify or view a current template by selecting the **Template Name** -or- Create a new template by selecting **Add Template** from the **Select a command** drop-down menu.
- Step 4** Choose one of the following options from the **EDCA Profile** drop-down menu:
- **WMM**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
 - **Spectralink Voice Priority**—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
 - **Voice Optimized**—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.
 - **Voice & Video Optimized**—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.

**Note**

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

**Note**

You must shut down radio interface before configuring EDCA Parameters.

Step 5 Click the **Enable Streaming MAC** checkbox to enable this feature.

**Note**

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

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

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **802.11a/n > Roaming Parameters** or **802.11b/g/n > Roaming Parameters**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the Template Name column. The Roaming Parameters Template appears (see [Figure 11-42](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-42 802.11 Roaming Parameters Template

The screenshot displays the Cisco Wireless Control System (WCS) interface. On the left is a sidebar menu with categories: Templates, System, WLANs, H-REAP, Security, 802.11a/n, 802.11b/g/n, Mesh, TFTP Servers, and Management. The main area is titled '802.11a Roaming Parameters > Template "RoamingParameters"'. It contains several input fields: 'Template Name' (set to 'RoamingParameters'), 'No of Controllers Applied To' (set to 0), 'Mode' (set to 'Default values'), 'Minimum RSSI (dbm)' (set to -85), 'Roaming Hysteresis (db)' (set to 1), 'Adaptive Scan Threshold (dbm)' (set to -72), and 'Transition Time (Sec)' (set to 5). At the bottom of the configuration area are four buttons: 'Save', 'Apply to Controllers ...', 'Delete', and 'Cancel'. In the top right corner, there is a user status bar showing 'User: root | Virtual Domain: root' and a 'Logout' button. An 'Alarm Summary' section is visible at the bottom left of the main area, showing a table with various system metrics.

- Step 4** Use the Mode drop-down menu to choose one of the configurable modes: default values and custom values. When the default values option is chosen, the roaming parameters are unavailable with the default values displayed in the text boxes. When the custom values option is selected, the roaming parameters can be edited in the text boxes. To edit the parameters, continue to Step 5.
- Step 5** In the Minimum RSSI field, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.
- Range:** -80 to -90 dBm
- Default:** -85 dBm
- Step 6** In the Hysteresis field, enter a value to indicate how strong the signal strength of a neighboring access point must be for the client to roam to it. This parameter is intended to reduce the amount of "ping ponging" between access points if the client is physically located on or near the border between two access points.
- Range:** 2 to 4 dB
- Default:** 2 dB
- Step 7** In the Adaptive Scan Threshold field, enter the RSSI value from a client's associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
- Range:** -70 to -77 dB
- Default:** -72 dB
- Step 8** In the Transition Time field, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.
- The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.
- Range:** 1 to 10 seconds
- Default:** 5 seconds
- Step 9** Click **Save**.
-

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

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

-
- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name in the Template Name column. The 802.11a/n or 802.11b/g/n RRM Thresholds Template appears (see Figure 11-43), and the number of controllers the template is applied to automatically populates.

Figure 11-43 802.11b/g/n RRM Thresholds Template

The screenshot displays the Cisco Wireless Control System (WCS) configuration interface for the '802.11b/g/n RRM Thresholds' template. The interface includes a top navigation bar with tabs like Monitor, Reports, Configure, Mobility, Administration, Tools, and Help. A left sidebar contains a tree view of configuration categories, with '802.11b/g/n' currently selected. The main content area is divided into several sections with configuration fields:

- General:** Template Name (1), No of Controllers Applied To (0).
- Coverage Hole Algorithm:** Min Failed Clients (#) (1), Coverage Level (db) (3), Signal Strength (dbm) (-87).
- Load Thresholds:** Max Clients (1), RF Utilization (%) (0).
- Threshold For Traps:** Interference Threshold (%) (0), Noise Threshold (dbm) (0), Coverage Exception Level (%) (0).
- Noise/Interference/Rogue Monitoring Channels:** Channel List (All Channels).

At the bottom left, an 'Alarm Summary' table shows the status of various alarms:

Alarm	On	Off	Clear
Malicious AP	0	0	0
Coverage Hole	0	0	0
Security	0	0	0
Controllers	0	0	0
Access Points	0	0	0
Location	0	0	0
Mesh Links	0	0	0
WCS	1	0	0

Buttons at the bottom include Save, Apply to Controllers..., Delete, and Cancel.

- Step 4** Enter the minimum number of failed clients that are currently associated with the controller.
- Step 5** Enter the desired coverage level. When the measured coverage drops by the percentage configured in the coverage exception level, a coverage hole is generated.
- Step 6** The Signal Strength (dBm) parameter shows the target range of coverage thresholds.
- Step 7** Enter the maximum number of clients currently associated with the controller.
- Step 8** At the RF Utilization parameter, enter the percentage of threshold for either 802.11a/n or 802.11b/g/n.
- Step 9** Enter an interference threshold.
- Step 10** Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to WCS.
- Step 11** 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 12** At the Channel List drop-down menu 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 13** Click **Save**.

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

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name from the Template Name column. The 802.11a/n or 802.11b/g/n RRM Threshold Template appears (see [Figure 11-44](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-44 802.11a/n RRM Intervals Template

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar contains a navigation menu with categories like Templates, System, WLANs, H-REAP, Security, 802.11a/n, 802.11b/g/n, Mesh, TFTP Servers, and Management. The '802.11a/n' category is expanded, and 'RRM Intervals' is selected. The main content area displays the configuration for a specific template named 'RadioResourceIntervals_18595'. The fields are as follows:

Field	Value
Template Name	RadioResourceIntervals_18595
No of Controllers Applied To	0
Neighbor Packet Frequency (sec)	60
Noise Measurement Interval	180
Load Measurement Interval	60
Channel Scan Duration (sec)	180

At the bottom of the configuration area, there are four buttons: 'Save', 'Apply to Controllers...', 'Delete', and 'Cancel'. The 'Add Template' button is highlighted in the top right corner of the configuration area.

- Step 4** In the Neighbor Packet Frequency field, enter (in seconds) how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list. The valid range is 60 to 3600 seconds, and the default value is 60 seconds for 802.11a radios and 180 seconds for 802.11b/g radios.
- Step 5** Enter at which interval you want noise and interference measurements taken for each access point. The default is 300 seconds.
- Step 6** Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.
- Step 7** In the Channel Scan Duration field, enter (in seconds) the sum of the time between scans for each channel within a radio band. The entire scanning process takes 50 ms per channel, per radio and runs at the Channel Scan Duration interval. The time spent listening on each channel is determined by the non-configurable 50-ms scan time and the number of channels to be scanned. For example, in the U.S. all 11 802.11b/g channels are scanned for 50 ms each within the default 180-second interval. So every 16 seconds, 50 ms is spent listening on each scanned channel ($180/11 = \sim 16$ seconds). The Channel Scan Duration parameter determines the interval at which the scanning occurs. The valid range is 60 to 2600 seconds, and the default value is 60 seconds for 802.11a radios and 180 seconds for the 802.11b/g radios.

Step 8 Click **Save**.

Configuring an 802.11h Template

Follow these steps to add an 802.11h template or make modifications to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **802.11a/n > 802.11h**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name from the Template Name column. The 802.11h Template appears (see [Figure 11-45](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-45 802.11h Template

The screenshot shows the Cisco Wireless Control System interface. The left sidebar contains a menu with categories: Templates, System, WLANs, Security, and Alarm Summary. The main content area is titled '802.11h Parameters > Template '802.11hConfig_1''. It includes sections for General, Power Constraint, and Channel Controller Announcement. The General section shows 'Template Name' as '802.11hConfig_1' and 'No of Controllers Applied To' as '8'. The Power Constraint section has a checkbox for 'Power Constraint'. The Channel Controller Announcement section has a checkbox for 'Channel Announcement'. At the bottom, there are buttons for 'Save', 'Apply to Controllers ...', 'Delete', and 'Cancel'. The Alarm Summary section at the bottom left shows various metrics with counts.

Alarm Summary			
Rogue AP	0		140
Coverage Hole			137
Security	9	0	2
Controllers	1	0	0
Access Points	768	0	41
Mesh Links	0	0	0
Location	1	0	14

- Step 4** Check the power constraint check box to enable TPC.
- Step 5** Check the channel announcement check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.
- Step 6** Click **Save**.

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

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template name from the Template Name column. The 802.11n Parameters for 2.4 GHz or 802.11n Parameters for 5 GHz template appears (see [Figure 11-46](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-46 802.11n Parameters for 2.4GHz Template

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Help

802.11n Parameters For 2.4GHz > Template 'Dot11bgnConfigTemplate_9393'

General		MCS (Data Rate) Settings **	
Template Name	Dot11bgnConfigTemplate_9393	1 (7 Mbps)	☐ Supported
No of Controllers Applied To	3	2 (14 Mbps)	☐ Supported
802.11n Network Status	☐ Enabled	3 (21 Mbps)	☐ Supported
		4 (29 Mbps)	☐ Supported
		5 (43 Mbps)	☐ Supported
		6 (58 Mbps)	☐ Supported
		7 (65 Mbps)	☐ Supported
		8 (72 Mbps)	☐ Supported
		9 (14 Mbps)	☐ Supported
		10 (29 Mbps)	☐ Supported
		11 (43 Mbps)	☐ Supported
		12 (58 Mbps)	☐ Supported
		13 (87 Mbps)	☐ Supported
		14 (116 Mbps)	☐ Supported
		15 (130 Mbps)	☐ Supported
		16 (144 Mbps)	☐ Supported

** Data Rate uses 20MHz and short guarded interval default setting

Selected MCS Indexes

Save Apply to Controllers ... Delete Cancel

Alarm Summary

Rogue AP	0	954
Coverage Hole	0	0
Security	0	0
Controllers	0	1
Access Points	19	5
Mesh Links	0	0
Location	0	0

- Step 4** Click the 802.11n Network Status Enabled check box to enable high throughput.
- Step 5** In the MCS (Data Rate) Settings column, choose which level of data rate you want supported. Modulation coding schemes (MCS) are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.



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

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

Configuring a Mesh Template

You can configure an access point to establish a connection with the controller. Follow these steps to add a mesh template or make modifications to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Mesh**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a specific template name. The Mesh Configuration Template window appears (see [Figure 11-47](#)).

Figure 11-47 Mesh Configuration Template

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor | Reports | **Configure** | Location | Administration | Help

Mesh Configuration Template > Template 'MeshConfigTemplate_3290'

General

Template Name: MeshConfigTemplate_3290
 RootAP to MeshAP Range (150 - 13200 ft): 12000
 Enable Client Access on Backhaul Link: ☐

Security

Security Mode: EAP

Save | Apply to Controllers ... | Delete | Cancel

Foot Notes

1 Changing Backhaul Client Access will reboot all mesh APs.
 2 Changing Security Mode will reboot all mesh APs.

Alarm Summary

Rogue AP	0	0	755
Coverage Hole	0	0	0
Security	1	0	0
Controllers	4	1	3
Access Points	2	0	14
Location	0	0	4
Mesh Links	0	0	0
WCS	0	0	0

- Step 4** The Root AP to Mesh AP Range is 12,000 feet by default. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global parameter applies to all access points when they join the controller and all existing access points in the network.
- Step 5** The Mesh Mac Filter is enabled by default. When enabled, this feature secures your network against any rogue access points and does not allow access points to attach if they are not defined in the MAC filter list.

However, if you disable this feature, mesh access points can join the controller.



Note

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

**Note**

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

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

After you check the Enable Mesh MAC Filter check box, the access points reboot and then rejoin the controller if defined in the MAC filter list. Access points that are not defined in the MAC list cannot join the controller.

- Step 6** The Enable Client Access on Backhaul Link check box is not checked by default. When this option is enabled, mesh access points are able to 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 is only applicable to access points with two radios.

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

Configuring a TFTP Server Template

A Trivial File Transfer Protocol (TFTP) server is often available for the download. Keep these guidelines in mind when setting up a TFTP server:

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

Follow these steps to add a new TFTP server template or make modifications to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **TFTP Servers**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a specific template in the TFTP Server Name column. The TFTP Server window appears.
- Step 4** Enter the IP address for the TFTP server.
- Step 5** Click **Save**.

Configuring a Trap Receiver Template

Follow these steps to add a new trap receiver template or make modifications to an existing template. If you have monitoring devices on your network that receive SNMP traps, you may want to add a trap receiver template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Management > Trap Receivers**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a specific template in the Template Name column. The Trap Receiver Template window appears (see [Figure 11-48](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-48 Trap Receiver Template

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar contains a menu with categories: Templates, System, WLANs, Security, and Alarm Summary. The 'Trap Receiver > Template '172.16.32.104'' window is open, displaying the following fields:

Template Name	172.16.32.104
No of Controllers Applied To	0
IP Address	172.16.32.104
Admin Status	☒

At the bottom of the window are four buttons: **Save**, **Apply to Controllers ...**, **Delete**, and **Cancel**.

The Alarm Summary section at the bottom left of the sidebar shows the following data:

Rogue AP	0	132
Coverage Hole	1	137
Security	9	2
Controllers	1	0
Access Points	768	41
Mesh Links	0	0
Location	1	14

- Step 4** Enter the IP address of the server.
- Step 5** Click to enable the admin status if you want SNMP traps to be sent to the receiver.
- Step 6** Click **Save**.

Configuring a Trap Control Template

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

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Management > Trap Control**.

Figure 11-49 **Trap Controls Template**

CISCO

Wireless Control System

Username: root | Logout | Refresh | Print View

Home Monitor Reports Configure Location Administration Help

Trap Controls > Template 'TrapControl_2558'

Template Name:

No of Controllers Applied To: 1

Miscellaneous Traps ☒ SNMP Authentication ☒ Link (Port) Up/Down ☒ Multiple Users ☒ Spanning Tree ☒ Rogue AP ☒ Controller Config Save ☐ 802.11 Association ☒ 802.11 Disassociation ☒ 802.11 Deauthentication ☒ 802.11 Failed Authentication ☒ 802.11 Failed Association ☒ Excluded	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 Decryption Error
--	--	--

Client Related Traps

Alarm Summary

Category	Count	Total
Rogue AP	0	749
Coverage Hole	0	0
Security	1	0
Controllers	4	1
Access Points	9	13
Location	0	4
Mesh Links	0	0
WCS	0	0

Save Apply to Controllers ... Delete Cancel

- **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. Refer to 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.

- 802.11 Disassociation - The disassociate notification is sent when the client sends a disassociation frame.
- 802.11 Deauthentication - The deauthenticate notification is sent when the client sends a deauthentication frame.

- 802.11 Failed Authentication - The authenticate failure notification is sent when the client sends an authentication frame with a status code other than successful.
 - 802.11 Failed Association - The associate failure notification is sent when the client sends an association frame with a status code other than successful.
 - Excluded - The associate failure notification is sent when a client is excluded.
- Step 6** Check the appropriate check box to enable any of the following access point traps:
- AP Register - Notification sent when an access point associates or disassociates with the controller.
 - AP Interface Up/Down - Notification sent when access point interface (802.11a/n or 802.11b/g/n) status goes up or down.
- Step 7** Check the appropriate check box to enable any of the following auto RF profile traps:
- Load Profile - Notification sent when Load Profile state changes between PASS and FAIL.
 - Noise Profile - Notification sent when Noise Profile state changes between PASS and FAIL.
 - Interference Profile - Notification sent when Interference Profile state changes between PASS and FAIL.
 - Coverage Profile - Notification sent when Coverage Profile state changes between PASS and FAIL.
- Step 8** Check the appropriate check box to enable any of the following auto RF update traps:
- Channel Update - Notification sent when access point's dynamic channel algorithm is updated.
 - Tx Power Update - Notification sent when access point's dynamic transmit power algorithm is updated.
- Step 9** Check the appropriate check box to enable any of the following AAA traps:
- User Auth Failure - This trap is to inform you that a client RADIUS authentication failure has occurred.
 - RADIUS Server No Response - This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
- Step 10** Check the appropriate check box to enable the following 802.11 security trap:
- WEP Decrypt Error - Notification sent when the controller detects a WEP decrypting error.
- Step 11** Check the appropriate check box to enable the following WPS trap:
- Rogue Auto Containment - Notification sent when a rogue access point is auto-contained.
- Step 12** Click **Save**.
-

Configuring a Telnet SSH Template

Follow these steps to add a Telnet SSH configuration template or make changes to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Management > Telnet SSH**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Telnet SSH Configuration Template window appears (see [Figure 11-50](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-50 Telnet SSH Configuration Template

The screenshot shows the Cisco Wireless Control System interface. The left sidebar contains a navigation menu with categories: Templates, System, WLANs, Security, and Alarm Summary. The main content area is titled 'Telnet SSH Configuration > Template 'TelnetConfig_13420''. It contains several configuration fields: Template Name (TelnetConfig_13420), No of Controllers Applied To (0), Session Timeout (min) (0), Maximum Sessions (5), Allow New Telnet Session (No), and Allow New SSH Session (Yes). At the bottom of the configuration area are buttons for Save, Apply to Controllers ..., Delete, and Cancel. The Alarm Summary table at the bottom left shows various system metrics.

Alarm Summary			
Rogue AP	0		136
Coverage Hole			137
Security	9	0	2
Controllers	1	3	0
Access Points	768	0	42
Mesh Links	0	0	0
Location	1	0	14

- Step 4** Enter the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The valid range is 0 to 160, and the default is 5.
- Step 5** At the Maximum Sessions parameter, enter the number of simultaneous Telnet sessions allowed. The valid range is 0 to 5, and the default is 5. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port.
- Step 6** Use the Allow New Telnet Session drop-down menu 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 menu to determine if you want Secure Shell Telnet sessions allowed. The default is yes.
- Step 8** Click **Save**.

Configuring a Legacy Syslog Template

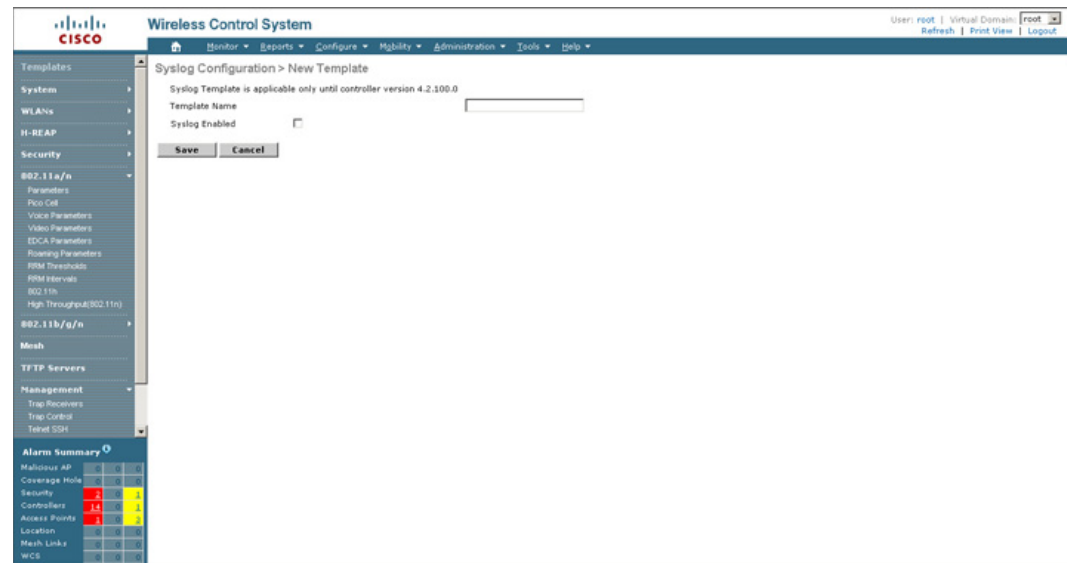
Follow these steps to add a legacy syslog configuration template or make modifications to an existing template.



Note

Legacy Syslog applies to controllers earlier than version 5.0.6.0

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Management > Legacy Syslog**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Legacy Syslog Configuration Template window appears (see [Figure 11-51](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-51 Syslog Configuration Template

- Step 4** Enter a template name. The number of controllers to which this template is applied is displayed.
- Step 5** Click to enable syslog. When you do, a Syslog Host IP Address parameter appears.
- Step 6** Click **Save**.

Configuring a Multiple Syslog Template

Follow these steps to add a multiple syslog configuration template or make modifications to an existing template.



Note You can enter up to three syslog server templates.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Management > Multiple Syslog**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a template in the Template Name column. The Multiple Syslog Configuration Template window appears (see [Figure 11-51](#)), and the number of controllers the template is applied to automatically populates.

Figure 11-52 Syslog Server Template Window

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor Reports Configure Location Administration Tools Help

Syslog Server > New Template

Multiple Syslog Template is applicable only from controller version 5.0.6.0

General

Template Name

Syslog Server Address

Save Cancel

Alarm Summary			
Malicious AP	0	0	276
Coverage Hole	0	0	0
Security	4	2	2
Controllers	6	4	2
Access Points	150	0	21
Location	0	0	0
Mesh Links	0	0	0
WCS	0	1	0

Step 4 Enter a template name and a syslog server IP address.

Step 5 Click **Save**.

Configuring a Local Management User Template

Follow these steps to add a local management user template or make modifications to an existing template.

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

Step 2 From the left sidebar menu, choose **Management > Local Management Users**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a username in the User Name column. The Local Management Users Template appears (see [Figure 11-53](#)).

Figure 11-53 Local Management Users Template

Wireless Control System User: root | Virtual Domain: root
[Refresh](#) | [Print View](#) | [Logout](#)

Monitor | Reports | **Configure** | Mobility | Administration | Tools | Help

Local Management Users > Template 'admin'

General

Template Name: admin
 User Name: admin
 No of Controllers Applied To: 0
 Access Level: Read Write

[Save](#) [Apply to Controllers ...](#) [Delete](#) [Cancel](#)

Alarm Summary

Malicious AP	0	0	237
Coverage Hole	0	0	0
Security	8	0	2
Controllers	11	0	0
Access Points	3	0	3
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

271156

- Step 4** Enter a template name
- Step 5** Enter a template username.
- Step 6** Enter a password for this local management user template.
- Step 7** Re-enter the password.
- Step 8** Use the Access Level drop-down menu to choose either Read Only or Read Write.
- Step 9** Click **Save**.

Configuring a User Authentication Priority Template

Management user authentication priority templates control the order in which authentication servers are used to authenticate a controller's management users. Follow these steps to add a user authentication priority template or make modifications to an existing template.

- Step 1** Choose **Configure > Controller Templates**.
- Step 2** From the left sidebar menu, choose **Management > Authentication Priority**.
- Step 3** To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click to select a username in the Template Name column. The Local Management Users Template appears (Figure 11-54).

Figure 11-54 Authentication Priority Template

- Step 4** Enter a template name.
- Step 5** The local server is tried first. Choose either **RADIUS** or **TACACS+** to try if local authentication fails.
- Step 6** Click **Save**.

Applying Controller Templates

You can apply a controller template to a controller.

- Step 1** Go to **Configure > Controller Templates**.
- Step 2** Using the left sidebar menu, choose the category of templates to apply.
- Step 3** Click the URL from the Template Name column that you want to apply to the controller.
- Step 4** Click the **Apply to Controllers** button.

Adding Access Point Templates

This page allows you to add a new access point template.

- Step 1** Choose **Configure > Access Point Templates**.
- Step 2** Choose **Add Template** from the Select a command drop-down menu and click **GO**.
- Step 3** Enter the template name.
- Step 4** Provide a description of the template.
- Step 5** Click **Save**.

Configuring Access Point Templates

This page allows you to configure a template of access point information that you can apply to one or more access points.

- Step 1** Choose **Configure > Access Point Templates**.
- Step 2** From the Template Name column, click on the template name you want to configure.
- Step 3** Choose the **AP Parameters** tab. The AP/Radio Templates window appears (see [Figure 11-55](#)).

Figure 11-55 AP/Radio Templates

The screenshot shows the Cisco Wireless Control System (WCS) interface. The top navigation bar includes links for Monitor, Reports, Configure, Location, Administration, Tools, and Help. The main content area is titled 'AP/Radio Templates > 'MRS''. Below this, there are tabs for 'AP Parameters', '802.11a/n Parameters', '802.11b/g/n Parameters', 'Select APs', and 'Apply Report'. The 'AP Parameters' tab is active, displaying a list of parameters to be configured. On the left, there is an 'Alarm Summary' table. On the right, there are fields for 'Controllers' and 'Override Global Username Password'.

Alarm Summary				
Malicious AP	0	0	0	442
Coverage Hole	0	0	0	0
Security	0	0	0	0
Controllers	0	0	0	2
Access Points	3	0	0	0
Location	0	0	0	0
Mesh Links	0	0	0	0
WCS	0	0	0	0

Select AP Parameters that needs to be applied.

- ☒ Location
- ☒ Admin Status
- ☒ AP Mode
- ☒ AP Height (feet)
- ☒ Mirror Mode
- ☒ Country Code
- ☒ Stats Collection Interval
- ☒ Cisco Discovery Protocol
- ☒ Bridge Group Name(Mesh APs only)
- ☒ Data Rate(Mesh APs only)
- ☒ Ethernet Bridging(Mesh APs only)
- ☒ Role(Mesh APs only)
- ☐ Enabled
- ☐ H-REAP Configuration
- ☐ VLAN Support
- ☐ Native VLAN ID
- ☐ Override Global Username Password

Reboot AP (Selecting this will reboot AP after making other selected updates, if any)

- Step 4** Click the **Location** check box and enter the access point location.
- Step 5** Click both the **Admin Status** and **Enabled** check box to enable access point administrative status.



Note In order to conserve energy, access points can be turned off at specified times during non-working hours. Choose the **Enabled** check box to allow access points to be turned on/off.

- Step 6** Click the **AP Mode** check box and use the drop-down menu to set the operational mode of the access point as follows:
- Local - Default
 - Monitor - Monitor mode only
 - REAP - Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.

- Rogue Detector - Monitors the rogue access points but does not transmit or contain rogue access points.
- 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/products>.

- Bridge

**Note**

Changing the AP mode reboots the access point.

Step 7 Enter the access point height in feet. The height defaults to the floor height. The height must be greater than 3 feet and must not exceed the floor height. The specified height is applied to all selected access points in the template.

**Note**

To change the height for a specific access point, go to Monitor > Maps > Floor > Position Access Points.

Step 8 You must click both the **Mirror Mode** and **Enabled** check box to enable access point mirroring mode.

Step 9 Click the check box to enable the country code drop-down menu. A list of country codes is returned. For this access point, choose which country code selection to allow. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country’s regulations.

**Note**

Access points may not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country’s regulatory domain. For a complete list of country codes supported per product, refer to http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

**Note**

Changing the country code may cause the access point to reboot.

Step 10 Click to enable **Stats Collection Interval** and then enter the collection period (in seconds) for access point statistics.

Step 11 (Mesh APs only) Choose the bridging option if you want the access point to act as a bridging access point.

Step 12 (Mesh APs only) Use the Data Rate drop-down menu to choose a data rate of 1, 2, 5.5, 6, or 9 Mbps.

- Step 13** (Mesh APs only) Use the Ethernet Bridging drop-down menu to choose to enabled or disabled.
- Step 14** (Mesh APs only) Use the Role drop-down menu to choose MAP or RAP.
- Step 15** Click the **Cisco Discovery Protocol** check box and click **Enabled** to allow CDP on a single access point or all access points. CDP is a device discovery protocol that runs on all Cisco manufactured equipment (such as routers, bridges, communication servers, and so on).
- Step 16** By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is overloaded, the higher-priority access points join the backup controller and disjoin the lower priority access points. Set the AP Failover Priority setting to low, medium, high, or critical.
- Step 17** Click the **Controllers** check box, and then you are required to enter the Primary, Secondary, and Tertiary Controller names.
- Step 18** Click the **Group VLAN Name** check box and then use the drop-down menu to select an established Group VLAN name.
- Step 19** Enable local switching by checking the **H-REAP Configuration** check box. When you enable local switching, any remote access point that advertises this WLAN is able to locally switch data packets (instead of tunneling to the controller).
- Step 20** Check the **VLAN Support** check box to enable it and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN ID** field. This value cannot be zero.

**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.

**Note**

By default, a VLAN is not enabled on the hybrid-REAP access point. Once hybrid REAP is enabled, the access point inherits the VLAN name (interface name) and the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per hybrid-REAP access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

- Step 21** The SSID-VLAN Mappings section lists all the SSIDs of the controllers which are currently enabled for HREAP local switching. You can edit the number of VLANs from which the clients will get an IP address by clicking the check box and adjusting the value.
- Step 22** On the System > AP Username Password window, you can set global credentials for all access points to inherit as they join a controller. These established credentials are displayed in the lower right of the AP Parameters tab window. If you want to override the global credentials for this particular access point, click the **Override Global Username Password** check box. You can then enter a unique username, password, and enable password that you want to assign to this access point.
- Step 23** Save the template.
- Step 24** If the updates require a reboot to be reflected, click to check the **Reboot AP** check box.
- Step 25** Choose the **Select APs** tab. Use the drop-down menu to apply the parameters by controller, floor area, outdoor area, or all. Click **Apply**.

**Note**

When you apply the template to the access point, WCS checks to see if the access point supports REAP mode and displays the application status accordingly. Clicking Apply saves and applies the template parameters to the selected access points. After applying a report, it appears in the Apply Report tab.

Applying or Scheduling Templates

Follow these steps to apply the access point and radio templates to all the controllers in a config group.

- Step 1** Choose **Configure > Access Point Templates**.
- Step 2** Under Template Name, choose the access point template to which you want to add a schedule.
- Step 3** Click the **Apply/Schedule** tab to access this page (see [Figure 11-56](#)).

Figure 11-56 *Apply/Schedule Tab*

Wireless Control System User: root | Virtual Domain: root Refresh Print View Logout

Monitor Reports Configure Mobility Administration Tools Help

AP/Radio Templates > 'test'

AP Parameters Mesh 802.11a/n 802.11a SubBand 802.11b/g/n Select APs **Apply/Schedule** *Report

Save Click 'Save' to save the template.

Apply Click 'Apply' to save the template and start the provisioning of the template to selected APs. This process will continue until completed even if you leave this page and logout from WCS.

Schedule ☒ **Enable schedule**

Start Date
(Current server time: 04/28/2008 08:09:42)

Start Time Hr Min

Recurrence ☐ No Recurrence ☐ Hourly ☒ Daily ☐ Weekly
Every Days(s)

Schedule Click 'Schedule' to save the template and start the provisioning at a scheduled time.

* To view the scheduled task reports, [click here](#)

Alarm Summary

Malicious AP	0	0	211
Coverage Hole	0	0	0
Security	6	0	2
Controllers	11	0	0
Access Points	2	0	2
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

- Step 4** Click **Apply** to start the provisioning of access point and radio templates to all the controllers. After you apply, you can leave this window or log out of Cisco WCS. The process continues, and you can return later to this page and view a report.

A report is generated and appears in the Recent Apply Report window. It shows which templates were successfully applied to each of the controllers.

**Note**

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

- Step 5** The scheduling function allows you to schedule a start day and time for provisioning. Check the **enable schedule** check box to enable the scheduling feature.
- Step 6** Enter a starting date in the text box or use the calendar icon to choose a start date.
- Step 7** Choose the starting time using the hours and minutes drop-down menus.
- Step 8** Determine how often you want the provisioning of the template to occur. The choices are no recurrence, hourly, daily, or weely. You can also specify a certain number of days in the Every ____ Days field.
- Step 9** Click **Schedule** to start the provisioning at the scheduled time.
-

Configuring Scheduled Configuration Tasks

The Scheduled Configuration Tasks feature allows you to view, modify, and delete scheduled access point template and configuration group tasks. To access the Scheduled Configuration Tasks window, choose **Configure > Scheduled Configuration Tasks**.

- [AP Template Tasks](#)
- [Config Group Tasks](#)

AP Template Tasks

The AP Template Tasks window allows you to view, modify, delete, enable, or disable current access point template tasks. To access the AP Template Tasks window and view current access point template tasks, choose **Configure > Scheduled Configuration Tasks**.

- [Modify a Current AP Template Task, page 11-85](#)
- [View AP Status Report for the Scheduled Task, page 11-85](#)
- [Enable or Disable a Current AP Template Task, page 11-86](#)
- [View an AP Template Task History, page 11-86](#)
- [Delete a Current AP Template Task, page 11-86](#)

Modify a Current AP Template Task

To modify a current access point template task, follow these steps:

-
- Step 1** Choose **Configure > Scheduled Configuration Tasks**.
- Step 2** Choose the template name of the applicable task.
- Step 3** From the AP Radio/Template window, choose the **Apply/Schedule** tab.
- Step 4** Make any necessary changes to the current schedule or AP template parameters and click **Schedule**.
-

View AP Status Report for the Scheduled Task

The AP Status Report for the scheduled task includes the following information:

- **AP Name**—Lists all of the access points included in the scheduled access point template task.
- **Ethernet MAC**—Indicates the ethernet MAC addresses for the applicable access points.

- **Controller**—Indicates the associated controller for each of the applicable access points.
- **Map**—Displays the map location for the applicable access points.
- **Status**—Indicates whether the access point template has been successfully applied or not. The possible states are not initiated, success, failure, partial failure, and not reachable.
- **Task Execution Time**—Indicates the execution time of the scheduled task for the applicable access point.

To view the status report for the access points included in the scheduled task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the AP Status Report for the applicable task.

Enable or Disable a Current AP Template Task

To enable or disable a current access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the check box of the scheduled task to be enabled or disabled.

Step 3 From the Select a command drop-down menu, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 4 Click **GO**.

View an AP Template Task History

To view previously scheduled task reports, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the check box of the applicable scheduled task.

Step 3 From the Select a command drop-down menu, choose **View History**.

Step 4 Click **GO**.

Delete a Current AP Template Task

To delete a scheduled access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Choose the check box of the applicable scheduled task.

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

Step 4 Click **GO**.

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

Config Group Tasks

The Config Group Tasks window allows you to view, modify, delete, enable, or disable current configuration group tasks.

A config group allows controllers to spawn across multiple config groups. A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes the controller from the other mobility group if the controller is already a mobility group member.

To access the Config Group Tasks window and view current config group tasks, choose **Configure > Scheduled Configuration Tasks > ConfigGroup**.

- [Modify a Current AP Template Task, page 11-85](#)
- [View Controller Status Report for the Scheduled Task, page 11-87](#)
- [Enable or Disable a Current Config Group Task, page 11-88](#)
- [View a Config Group Task History, page 11-88](#)
- [Delete a Current Config Group Task, page 11-88](#)

Modify a Current Config Group Task

To modify a current configuration group task, follow these steps:

-
- Step 1** Choose **Configure > Scheduled Configuration Tasks**.
- Step 2** From the left sidebar menu, choose **ConfigGroup**.
- Step 3** Choose the group name of the applicable task.
- Step 4** From the Config Groups window, choose the Apply/Schedule tab.
- Step 5** Make any necessary changes to the current schedule and click **Schedule**.
-

View Controller Status Report for the Scheduled Task

The Controller Status Report for the scheduled task includes the task execution results of templates applied to the controller.

To view the controller status report, follow these steps:

-
- Step 1** Choose **Configure > Scheduled Configuration Tasks**.
- Step 2** From the left sidebar menu, choose **ConfigGroup**.
- Step 3** Choose the Controller Status Report for the applicable task.
-

Enable or Disable a Current Config Group Task

To enable or disable a current configuration group task, follow these steps:

-
- Step 1** Choose **Configure > Scheduled Configuration Tasks**.
 - Step 2** From the left sidebar menu, choose **ConfigGroup**.
 - Step 3** Choose the check box of the scheduled task to be enabled or disabled.
 - Step 4** From the Select a command drop-down menu, choose **Enable Schedule** or **Disable Schedule**, as applicable.
 - Step 5** Click **GO**.
-

View a Config Group Task History

To view previous scheduled task reports, follow these steps:

-
- Step 1** Choose **Configure > Scheduled Configuration Tasks**.
 - Step 2** From the left sidebar menu, choose **ConfigGroup**.
 - Step 3** Choose the check box of the applicable scheduled task.
 - Step 4** From the Select a command drop-down menu, choose **View History**.
 - Step 5** Click **GO**.
-

Delete a Current Config Group Task

To delete a scheduled configuration group task, follow these steps:

-
- Step 1** Choose **Configure > Scheduled Configuration Tasks**.
 - Step 2** From the left sidebar menu, choose **ConfigGroup**.
 - Step 3** Choose the check box of the applicable scheduled tasks.
 - Step 4** From the Select a command drop-down menu, choose **Delete Task(s)**.
 - Step 5** Click **GO**.
 - Step 6** Click **OK** to confirm the deletion.
-

Configuring Radio Templates

This page allows you to configure a template of radio information that you can apply to one or more access points.

-
- Step 1** Choose **Configure > Access Point Templates**.
 - Step 2** From the Template Name column, click on the template name you want to configure.

Step 3 Choose the **802.11a/n Parameters** or **802.11b/g/n Parameter** tab. The AP/Radio Templates window appears (see [Figure 11-57](#)).

Figure 11-57 802.11a/n Parameters

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor Reports Configure Location Administration Help

AP/Radio Templates > 'test'

AP Parameters 802.11a/n Parameters 802.11b/g/n Parameters Select APs Apply Report

Select 802.11a Parameters that needs to be applied.

☐ Channel Assignment ☐ Custom * ☒ Global ☐ Power Assignment ☐ Custom * ☒ Global

☐ Admin Status ☒ Enabled ☐ WLAN Override ***

☐ Antenna Mode

☐ Antenna Diversity

☐ Antenna Type

☐ Antenna Name **

* Channel number and power levels will be validated against Radio's list of supported channels and power levels respectively.

** Not all antenna models are supported by radios of different AP types

*** AP must be reset for the WLAN Override change to take effect.

Alarm Summary

Rogue AP	0	0	310
Coverage Hole	0	0	0
Security	17	0	0
Controllers	3	0	3
Access Points	25	0	10
Mesh Links	0	0	0
Location	0	0	0

Step 4 Click the Channel Assignment checkbox to enable it. To choose a specific channel, click **Custom** and use the drop-down to designate the channel. Otherwise, click **Global**.



Note The channel assignment is validated against the radio's list of supported channels.

Step 5 Click both the **Admin Status** and **Enabled** check box to enable access point administrative status.

Step 6 Use the Antenna Mode drop-down menu to choose the antenna model. The choices are omni, sector A, and sector B.



Note Not all antenna models are supported by radios of different access point types.

Step 7 For external antennas, choose one of the following:

- **Enabled**—Use this setting to enable diversity on both the left and right connectors of the access point.
- **Left/Side B**—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector.
- **Right/Side A**—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector.

For internal antennas, choose one of the following:

- **Enabled**—Use this setting to enable diversity on both Side A and Side B.

- Left/Side B—Use this setting to enable diversity on Side B (rear antenna) only.
- Right/Side A—Use this setting to enable diversity on Side A (front antenna) only.

- Step 8** Click to enable Antenna Type and use the drop-down menu to specify if the antenna is external or internal.
- Step 9** Use the Antenna Name drop-down menu to determine whether the antenna is a Kodiak directional, AIR-ANT1000, CUSH-S5157WP, etc.
- Step 10** Check the Power Assignment check box and choose the power level currently being used to transmit data. (Some PHYs also use this value to determine the receiver sensitivity requirements.) If you choose Global, the power level is assigned by dynamic algorithm. If you choose Custom, you can select a value using the drop-down menu. Power level 1 is the maximum.
- Step 11** Enable or disable WLAN override for this access point. When you enable WLAN override, the operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, choose WLANs to enable WLAN operation and deselect WLANs to disallow WLAN operation for this access point 802.11b/g Cisco Radio.



Note The access point must be reset for the WLAN override change to take effect.

Selecting Access Points

After you have completed the radio template configuration, you must pick the access point to which these attributes are applied. Follow these steps to select access points.

- Step 1** Click the **Select APs** tab.
- Step 2** Use one of the search criterias to choose the access points and click **Search**. For example, you can search for access points that this template was last applied to or search by controller name, by floor area, etc. The search criterias change based on the selection you choose.
- The AP name, ethernet MAC, controller and map information appears.
- Step 3** Click the checkbox in the AP Name column and select to which access points you want the access point and radio parameters applied. You can also click the **Select All** or **Unselect All** options.
- Step 4** Click **Save** to save the parameter selection or click **Apply** to save and apply the access point and radio parameters to the selected access points.

Applying the Report

After access points are selected and applied, click the **Apply Report** tab.