CHAPTER 9

Configuring Access Points

This chapter describes how to configure access points in the Cisco WCS database. This chapter contains the following sections:

Setting AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This may cause the controller to reach a saturation point and reject some of the access points.

By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points are allowed to join the backup controller by disjoining the lower priority access points.

To configure priority settings for access points, you must first enable the AP Priority feature. To enable the AP Priority feature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > General**.

Step 4 From the AP Priority drop-down, choose **Enabled**.

To then configure an access point's priority, follow these steps:

Step 1 Choose **Configure > Access Points > <AP Name>**.

Step 2 From the AP Priority drop-down menu, choose the applicable priority (Low, Medium, High, Critical).

Note The default priority is Low.

Configuring Global Credentials for Access Points

Cisco autonomous access points are shipped from the factory with "Cisco" as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the access point's console port.

In WCS and controller software releases prior to 5.0, you can set the access point enable password only for access points that are currently connected to the controller. In WCS and controller software release 5.0, you can set a global username, password, and enable password that all access points inherit as they join a controller. This includes all access points that are currently joined to the controller and any that join in the future. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis and assign a unique username, password, and enable password. Refer to the "Configuring Access Point Templates" section on page 11-81 to see where the global password is displayed and how it can be overridden on a per-access point basis.

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

Note These controller software release 5.0 features are supported on all access points that have been converted to lightweight mode, except the 1100 series. VxWorks access points are not supported.

The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.

Note You need to keep careful track of the credentials used by the access points. Otherwise, you might not be able to log into an access point's console port. If necessary, you can clear the access point configuration to return the access point username and password to the default setting.

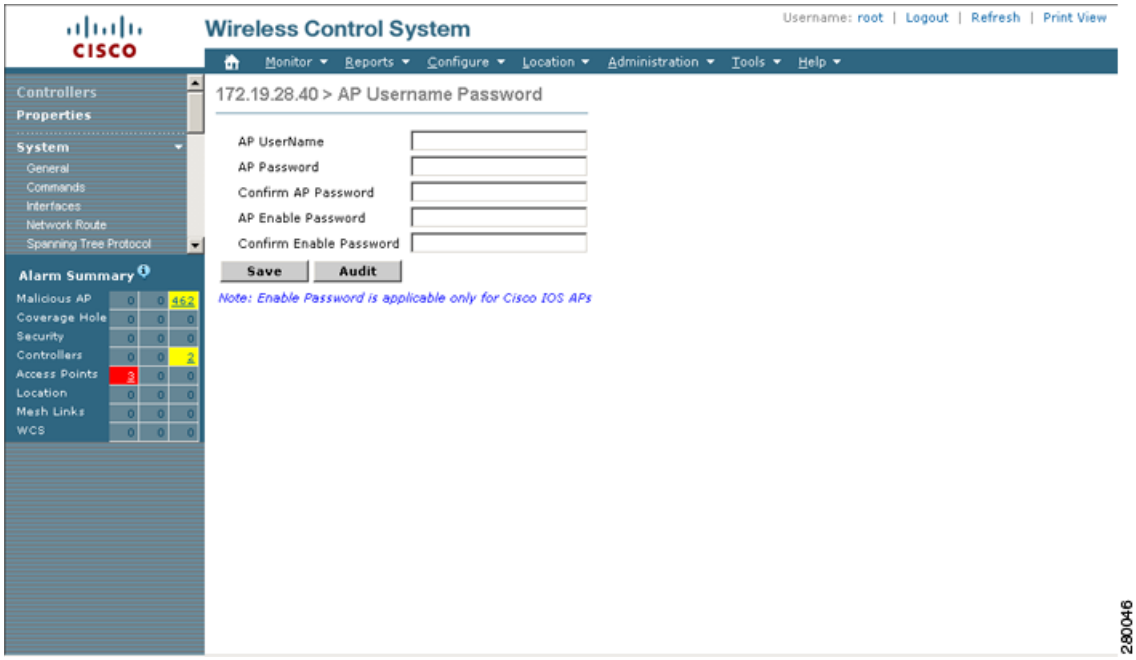
Follow these steps to establish a global username and password.

Step 1 Choose **Configure > Controllers** or **Configure > Access Points**.

Step 2 Choose an IP address of a controller with software release 5.0 or later or choose an access point associated with software release 5.0 or later.

Step 3 Choose **System > AP Username Password** from the left sidebar menu. The AP Username Password window appears (see Figure 9-1).

Figure 9-1 AP Username Password Window



Step 4 In the AP Username field, enter the username that is to be inherited by all access points that join the controller.

Step 5 In the AP Password field, enter the password that is to be inherited by all access points that join the controller. Re-enter in the Confirm AP Password field.

Step 6 For Cisco autonomous access points, you must also enter and confirm an enable password. In the AP Enable Password field, enter the enable password that is to be inherited by all access points that join the controller. Re-enter in the Confirm Enable Password field.

Step 7 Click **Save**.

Autonomous to LWAPP Migration Support

The autonomous to LWAPP migration support feature provides a common application (WCS) from which you can perform basic monitoring of autonomous access points along with current LWAPP access points. The following autonomous access points are supported:

- Cisco Aironet 1100 Access Point
- Cisco Aironet 1130 Access Point
- Cisco Aironet 1200 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1310 Bridge
- Cisco Aironet 1410 Bridge

You may also choose to convert autonomous access points to LWAPP.

From WCS, the following functions are available when managing autonomous access points:

- Adding Autonomous Access Points to WCS
- Configuring autonomous access points
- Viewing Autonomous Access Points in WCS
- Monitoring associated alarms
- Performing an autonomous access point background task
  - Checks the status of autonomous access points managed by WCS.
  - Generates a critical alarm when an unreachable autonomous access point is detected.
  - See Background Task for more information
- Running reports on autonomous access points
  - See Reports > Inventory Reports and Reports > Client Reports > Client Count for more information
- Supporting autonomous access points in Work Group Bridge (WGB) mode
- Migrating autonomous access points to LWAPP access points

Adding Autonomous Access Points to WCS

From WCS, the following methods are available for adding autonomous access points:

- Add autonomous access points by Device information (IP addresses and credentials).
- Add autonomous access points by CSV file.

Adding Autonomous Access Points by Device Information

Autonomous access points can be added to WCS by device information using comma-separated IP addresses and credentials.

To add autonomous access points using device information, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the Select a command drop-down menu, choose **Add Autonomous APs**.

Step 3 Click **GO**.

Step 4 Select **Device Info** from the Add Format Type drop-down list.

Step 5 Enter comma-separated IP addresses of autonomous access points.

Step 6 Enter the SNMP parameters including version number, number of retries, and timeout in seconds.

Step 7 Enter Telnet credentials for migration (optional).

Note The Telnet credentials are required to convert the access points from autonomous to unified.

Note If the autonomous access point already exists, WCS updates the credentials (SNMP and Telnet) to the existing device.

Step 8 Click **OK**.

Adding Autonomous Access Points by CSV File

Autonomous access points can be added to WCS using a CSV file exported from WLSE.

To add autonomous access points using a CSV file, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the **Select a Command** drop-down menu, choose **Add Autonomous APs**.

Step 3 Click **GO**.

Step 4 Select **File** from the **Add Format Type** drop-down list.

Step 5 Enter or browse to the applicable CSV file.

Note The CSV file has the same format as Adding Controllers but includes additional (optional) columns such as telnet_username, telnet_password, and enable_password.

Step 6 Click **OK**.

To remove an autonomous access point from WCS:

Step 1 Select the check box(es) of the appropriate access point(s).

Step 2 Select **Remove APs** from the **Select a Command** drop-down list.

Viewing Autonomous Access Points in WCS

Once added, the autonomous access points can be viewed on the **Monitor > Access Points** page.

Click the autonomous access point to view more detailed information such as:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in **Monitor > Maps**.

They can be added to a floor area by choosing **Monitor Maps > <floor area>** and selecting **Add Access Points** from the **Select a Command** drop-down list**.**

Work Group Bridge (WGB) Mode

Wireless Group Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to an LWAPP access point. The WGB and its wired clients are listed as client in WCS.

Choose **Monitor > WGBs** to view a list of all WCS clients that are in WGBs. Click a User to view detailed information regarding a specific WGB and its wired clients.

Note The WCS provides WGB client information for the autonomous access point whether or not it is managed by the WCS. If the WGB access point is also managed by the WCS, WCS provides basic monitoring functions for the access point similar to other autonomous access points.

Autonomous Access Point to LWAPP Access Point Migration

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to LWAPP access points. The migration utility is available from the **Configure > Migration Templates** page where existing templates are listed.

From the **Select a command** drop-down list, the following functions can be performed:

- Add Template—Allows you to provide necessary information for migration.
- Delete Templates—Allows you to delete a current template.
- View Migration Report—Allows you to view information such as AP address, migration status, timestamp, and a link to detailed logs.
- View Current Status—Allows you to view the progress of the current migration (updated every three seconds).

Note When migrating an already-managed autonomous access point to LWAPP, its location and antenna information is migrated as well. You do not need to re-input the information. WCS automatically removes the autonomous access point after migration.

Adding/Modifying a Migration Template

To add a new template, select **Add Template** from the **Select a command** drop-down list.

To modify an existing template, click the template name from the summary list.

Enter or modify the following migration parameters:

General

- Template Name—User-defined name of this migration template.
- Description—Brief description to help you identify the migration template.

Upgrade Options

- DHCP Support—Ensures that after the conversion every access point gets an IP from the DHCP server.

- Retain AP HostName—Allows you to retain the same hostname for this access point.
- Migrate over WAN Link—Increases the default timeouts for the CLI commands executed on the access point.
- DNS Address
- Domain Name

Controller Details

Note Ensures that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

- Controller IP—Enter the IP address of the WLAN controller you are wanting to add to the newly migrated access point.
- User Name—Enter a valid username for login of the WLAN controller.
- Password—Enter a valid password for this username used during WLAN controller login.

TFTP Details

When you installed and set up WCS, it provided its own TFTP and FTP server.

- TFTP Server IP—Enter the IP address of the WCS server.
- File Path—Enter the TFTP directory which was defined during WCS setup.
- File Name—Enter the LWAPP conversion file defined in the TFTP directory during WCS setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).

Once a template is added in WCS, the following additional buttons appear:

- **Select AP**s—Selecting this option provides a list of autonomous access points in WCS from which to choose the access points for conversion.
- **Select File**—To provide CSV information for access points intended for conversion.

Configuring Access Points

Choose **Configure > Access Points** to see a summary of all access points in the Cisco WCS database. The summary information includes the following:

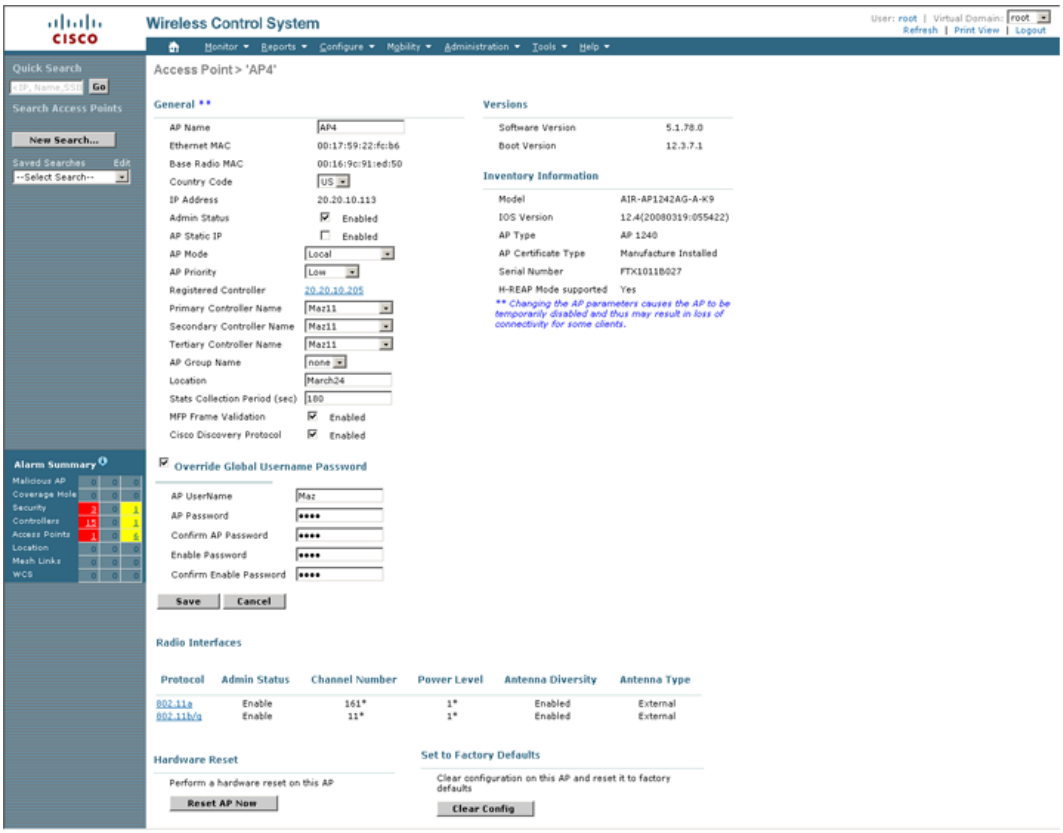
- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

Note If you hover over the Audit Status value, the time of the last audit is displayed.

Step 1 Click the link under AP Name to see detailed information about that access point name. The following window appears (see Figure 9-2).

Figure 9-2 Detailed Access Point Information

.



Note There is no need to add access points to the Cisco WCS database. The operating system software automatically detects and adds an access point to the Cisco WCS database as it associates with existing controllers in the Cisco WCS database.

Some of the parameters on the window are supplied.

- The General portion displays the Ethernet MAC, the Base Radio MAC, and IP Address.
- The Versions portion of the window displays the software and boot version.
- The Inventory Information portion displays the model, IOS version, and serial number and type of the access point, provides which certificate type is required, and determines whether H-REAP mode is supported or not.
- The Radio Interfaces portion provides the current status of the 802.11a/n and 802.11b/g/n radios such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

Follow the steps below to set the configurable parameters.

Step 2 Enter the name assigned to the access point.

Step 3 Use the drop-down menu to choose a country code to establish multiple country support. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that the access point complies with your country's regulations. Consider the following when setting the country code:

- You can configure up to 20 countries per controller.
- Because only one auto-RF engine and one list of available channels exist, configuring multiple countries limits the channels available to auto-RF in the common channels. A common channel is one that is legal in each and every configured country.
- When you configure access points for multiple countries, the auto-RF channels are limited to the highest power level available in every configured country. A particular access point may be set to exceed these limitations (or you may manually set the levels in excess of these limitations), but auto-RF does not automatically choose a non-common channel or raise the power level beyond that available in all countries.

Note Access points may not operate properly if they are not designed for use in your country of operation. For example, an (-A) access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Europe (-E). 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/warp/public/779/smbiz/wireless/approvals.html.

Step 4 If you want to enable the access point for administrative purposes, check the **Enabled** check box.

Step 5 If you click **Enabled** at the AP Static IP check box, a static IP address is always assigned to the access point rather than getting an IP address dynamically upon reboot.

Step 6 Choose the role of the access point from the AP Mode drop-down menu. No reboot is required after the mode is changed *except* when monitor mode is selected. You are notified of the reboot when you click **Save**. The available modes are as follows:

- Local — This is the normal operation of the access point and the default AP Mode choice. With this mode, data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.
- Monitor — This is radio receive only mode and allows the access point to scan all configured channels every 12 seconds. Only deauthentication packets are sent in the air with an access point configured this way. A monitor mode access point detects rogues, but it cannot connect to a suspicious rogue as a client to prepare for the sending of RLDP packets.

Note You can expand the monitor mode for tags to include location calculation by enabling the location optimized monitor mode (LOMM) feature. When LOMM is enabled, you can specify which four channels within the 2.4GHz band (802.11b/g radio) of an access point to use to monitor tags. This allows you to focus channel scans on only those channels for which tags are traditionally found (such as channels 1, 6, and 11) in your network. To enable LOMM, you must also make additional edits on the 802.11b/g radio of the access point. Refer to the "Configuring Access Point Radios for Location Optimized Monitor Mode" section on page 9-14 for configuration details.

- Rogue Detector — In this mode, the access point radio is turned off, and the access point listens to wired traffic only. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
- Sniffer Mode — Operating in sniffer mode, the access point captures and forwards all the packets on a particular channel to a remote machine that runs Airopeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run Airopeek, which is a third-party network analyzer software that supports the decoding of data packets. For more information on Airopeek, see http://www.wildpackets.com/products.
- HREAP —Choose **HREAP** from the AP Mode drop-down menu to enable hybrid REAP for up to six access points. The HREAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Step 7 In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

Step 8 The AP Group Name drop-down shows all access point group names that have been defined using WLANs > AP Group VLANs, and you can specify whether this access point is tied to any group.

Step 9 Enter a description of the physical location where the access point was placed.

Step 10 In the Stats Collection Period parameter, enter the time in which the access point sends .11 statistics to the controller. The valid range is 0 to 65535 seconds. A value of 0 means statistics should not be sent.

Step 11 Choose Enabled for **Mirror Mode** if you want to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point. Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port since any connections to this port become unresponsive.

Step 12 You can globally configure MFP on a controller. When you do, management frame protection and validation are enabled by default for each joined access point, and access point authentication is automatically disabled. After MFP is globally enabled on a controller, you can disable and re-enable it for individual WLANs and access points.

If you click to enable MFP Frame Validation, three main functions are performed:

- Management frame protection — When management frame protection is 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, and the receiving access points which were configured to detect MFP frames report the discrepancy.
- Management frame validation — When management frame validation is enabled, the access point validates every management frame it receives from other access points in the network. When the originator is configured to transmit MFP frames, the access point ensures that the MIC IE is present and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE, it reports the discrepancy to the network management system. In order to report this discrepancy, the access point must have been configured to transmit MFP frames. Likewise, for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.
- Event reporting — The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to alert the network manager.

Step 13 Click the **Cisco Discovery Protocol** check box if you want to enable it. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment, such as routers, bridges, and communication servers. Each device sends periodic messages to a multicast address and listens to the messages that others send in order to learn about neighboring devices. When the device boots, it sends a CDP packet specifying whether the device is inline power enabled so that the requested power can be supplied.

Note Changing access point parameters temporarily disables an access point and might result in loss of connectivity to some clients.

Step 14 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 15 Select the role of the mesh access point from the AP Role drop-down menu. The default setting is MAP.

Note An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

Step 16 Enter the name of the bridge group to which the access point belongs. The name can have up to 10 characters.

Note Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.

Note For mesh access points to communicate, they must have the same bridge group name.

Note For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.

Note For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

The Type parameter appears whether the mesh access point is an indoor or outdoor access point, and the Backhaul Interface parameter displays the access point radio that is being used as the backhaul for the access point.

Step 17 Select the data rate for the backhaul interface from the drop-down menu. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

Note This data rate is shared between the mesh access points and is fixed for the whole mesh network.

Note Do NOT change the data rate for a deployed mesh networking solution.

Step 18 Choose the Enable option from the Ethernet Bridging drop-down menu to enable Ethernet bridging for the mesh access point.

Step 19 Click **Save** to save the configuration.

Step 20 If you need to perform a hardware reset on this access point, click **Reset AP Now**.

Step 21 If you need to clear the access point configuration and reset all values to the factory default, click **Clear Config**.

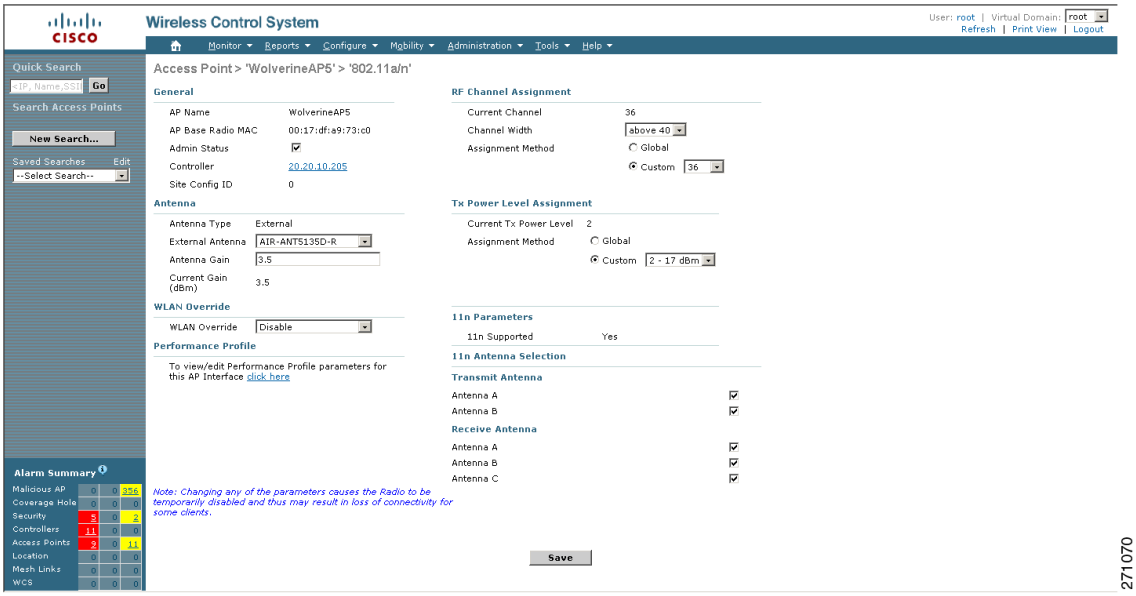
11n Antenna Selection

WCS provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

If you choose **Configure > Access Points** and select an **802.11n** item from the Radio column, the following page appears (see Figure 9-3).

Figure 9-3 Access Point > 802.11a/n



The following 11n Parameters display and can be modified:

Note Changing any of the parameters causes the radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the access point's base radio.
- Admin Status—Check the box to enable the administration state of the access point.
- Controller—IP address of the controller. Click the controller's IP address for more details.
- Site Config ID—Site identification number.

Antenna

- Antenna Type—Indicates an external or internal antenna.
- External Antenna—Use the drop-down menu to choose the appropriate external antenna.
- Antenna Gain—The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.
- Current Gain—The current antenna gain.

WLAN Override

- WLAN Override—Enable or disable WLAN override for this access point. .

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

RF Channel Assignment

- Current Channel—The current channel being utilized.
- Channel Width—Select the channel bandwidth from the drop-down menu.
- Assignment Method—Select one of the following:
  - Global—Use this setting if your access point's channel is set globally by the controller.
  - Custom—Use this setting if your access point's channel is set locally. Choose a channel from the drop-down list.

Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following:
  - Global—Use this setting if your access point's power level is set globally by the controller.
  - Custom—Use this setting if your access point's power level is set locally. Choose a power level from the drop-down list.

11n Parameters

- 11n Supported—Indicates whether or not 802.11n radios are supported.

11n Antenna Selection

- Transmit Antenna—Click the check box beside Antenna A or Antenna B to enable them.
- Receive Antenna—Click the check box beside Antenna A, B, or C to enable them.

Configuring Access Point Radios for Location Optimized Monitor Mode

To optimize monitoring and location calculation of tags, you can enable LOMM on up to four channels within the 2.4 GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor Mode at the access point level, you must then enable LOMM and assign monitoring channels on the 802.11b/g radio of the access point.

Note For details on enabling Monitor Mode on an access point, refer to Step 6 in the "Configuring Access Points" section on page 9-7.

Follow the steps below to set enable LOMM and assign monitoring channels on the access point radio.

Step 1 After enabling Monitor Mode at the access point level, choose **Configure > Access Points**.

Step 2 At the All Access Points Summary window, choose the **802.11 b/g Radio** link for the appropriate access point.

Step 3 At the Radio parameters window, disable **Admin Status** by unchecking the check box. This disables the radio.

Step 4 Check the **Location Optimized Channel Assignment** checkbox. Drop-down menus for each of the four configurable channels display.

Step 5 Select the four channels on which you want the access point to monitor tags.

Note You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, select **None** from the channel drop-down menu.

Step 6 Click **Save**. Channel selection is saved.

Step 7 At the Radio parameters window, re-enable the radio by checking the **Admin Status** check box.

Step 8 Click **Save**. The access point is now configured as a LOMM access point.

The AP Mode displays as Monitor/LOMM on the **Monitor > Access Points** window.

Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Choose the check box for the applicable access point(s).

Step 3 From the Select a command drop-down menu, choose **Schedule Radio status**.

Step 4 Click **GO**.

Step 5 Choose **Enable** or **Disable** from the Admin Status drop-down menu.

Step 6 Use the **Hours** and **Minutes** drop-down menus to determine the scheduled time.

Step 7 Click the calendar icon to select the scheduled date for the status change.

Step 8 If the scheduled task is recurring, choose **Daily** or **Weekly**, as applicable. If the scheduled task is a one-time event, choose **No Recurrence**.

Step 9 Choose **Submit** to confirm the scheduled task.

Viewing Scheduled Tasks

To view currently scheduled radio status tasks, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Choose the check box for the applicable access point(s).

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

Step 4 Click **GO**.

The Scheduled Task(s) information includes:

- Scheduled Task(s)—Choose the task to view its access points and access point radios.
- Scheduled Radio adminStatus—Indicates the status change (Enable or Disable).
- Schedule Time—Indicates the time the schedule task occurs.
- Execution status—Indicates whether or not the task is scheduled.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.
- Next Execution—Indicates the time and date of the next task occurrence.
- Last Execution—Indicates the time and date of the last task occurrence.
- Unschedule—Click **Unschedule** to cancel the scheduled task. Click **OK** to confirm the cancellation.

Viewing Audit Status (for Access Points)

An Audit Status column on the Configure > Access Points window shows an audit status for each of the access points. You can also view the audit report for the selected access points. The report shows the time of the audit, the IP address of the selected access point, and the synchronization status.

Step 1 Choose **Configure > Access Points**.

Step 2 Click the Audit Status column value to go to the latest audit details page for the selected access point. This report is interactive and per access point.

Note If you hover over the Audit Status column value, the time of the last audit is displayed.

To run an access point on-demand audit report, select the desired access point for which you want to run the report and choose **Audit Now** from the Select a command drop-down menu. In versions prior to 4.1, the audit only spanned the parameters present on the AP Details and AP Interface Details page. In release 4.1, this audit report covers complete access point level auditing. The audit results are stored in the database so that you can view the latest audit reports without having to run another audit.

Note The audit can only be run on an access point that is associated to a controller.

Searching Access Points

Use the controls in the left sidebar to create and save custom searches:

- **New Search** drop-down menu: Opens the Search Access Points window. Use the Search Access Points window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit Link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

You can configure the following parameters in the Search Access Points window:

- Search By
- Radio Type
- Search in
- Save Search
- Items per page

After you click GO, the access point search results appear:

Table 9-1 Access Point Search Results

Parameter	Options
AP Name	Name assigned to the access point. Click the access point name item to display details.
WCS	WCS name where access point was detected.
Ethernet MAC	MAC address of the access point.
IP Address	IP address of the access point.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.
Controller	IP address of the controller.
Admin Status	Administration site of the access point (Enabled or Disabled).
AP Type	Access point radio frequency type.
Operational Status	Displays the operational status of the Cisco radios (Up or Down).
Alarm Status	Alarms are color coded as follows: • Clear = No Alarm • Red = Critical Alarm • Orange = Major Alarm • Yellow = Minor Alarm

Viewing or Editing Rogue Access Point Rules

You can view or edit current rogue access point rules on a single WLC. Follow these steps to access the rogue access point rules. Refer to the "Configuring a Rogue AP Rules Template" section on page 11-44 for more information.

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address under the IP Address column.

Step 3 From the left sidebar menu, choose **Security > Rogue AP Rules**. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.

Step 4 Choose a **Rogue AP Rule** to view or edit its details.

Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to WCS. This feature allows the WCS to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose Configure > Spectrum Experts. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address— The MAC address of the spectrum sensor card in the laptop.
- Reachability Status— Specifies whether the Spectrum Expert is successfully running and sending information to WCS. The status appears as reachable or unreachable.

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

Step 1 Choose **Configure > Spectrum Experts**.

Step 2 Click **Add a Spectrum Expert**.

Note This link only appears when no spectrum experts are added. You can also access the Add a Spectrum Expert page by choosing Add a Spectrum Expert from the Select a command drop-down menu.

Step 3 Enter the Spectrum Expert's Hostname or IP address. If you use hostname, your spectrum expert must be registered with DNS in order to be added to WCS.

Note To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to WCS.

Monitoring Spectrum Experts

You also have the option to monitor spectrum experts. Follow these steps to monitor spectrum experts:

Step 1 Choose **Monitor > Spectrum Experts**.

Step 2 From the left sidebar menu, you can access the **Spectrum Experts > Summary** page and the **Interferers > Summary** page.

Spectrum Experts > Summary

The Spectrum Experts Summary page provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

Hostname—Displays the host name or IP address.

Active Interferers—Indicates the current number of interferes being detected by the Spectrum Experts.

Alarms APs—The number of access points seen by the Spectrum Experts that are potentially affected by detected interferers.

Alarms—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.

Reachability Status—Indicates "Reachable" in green if the Spectrum Expert is running and sending data to WCS. Otherwise, indicates "unreachable" in red.

Location—When the Spectrum Expert is a wireless client, a link for location is available. It shows the location of the Spectrum Expert with a red box that shows the effective range.

Interferers > Summary

The Interferers Summary page displays a list of all the interferers detected over a 30-day interval. The table provides the following interferers' information:

- Interferer ID—An identifier that is unique across different spectrum experts.
- Category—Indicates the category of the interferer. Categories include: Bluetooth, cordless phones, microwave ovens, 802.11 FH, generic: fixed-frequency, jammers, generic: frequency-hopped, generic:continuous, and analog video.
- Type—Active indicates that the interferer is currently being detected by a spectrum expert. Inactive indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert saw that the interferer is no longer reachable by WCS.
- Discover Time—Indicates when the interferer was discovered.
- Affected Channels—Identifies affected channels.
- Number of APs Affected—The number of access points managed by WCS that the spectrum expert detects or the interferers that the spectrum expert detected on the channels of the access point. Only active interferers are shown. If all of the following conditions are met, the access point is labelled as ***affected***:
  - If the access point is managed by WCS.
  - If the spectrum expects detects the access point.
  - If the spectrum expert detects an interferer on the serving channel of the access point.
- Power—Indicated in dBm.
- Duty Cycle—Indicated in percentage. 100% is the worst value.
- Severity—Indicates the severity ranking of the interferer. 100 is the worst case whereas 0 is no interference.

Spectrum Experts Details

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds and gives a real-time look at the remote spectrum expert. This page includes the following items:

- Total Interferer Count—Given from the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers grouped by category on different channels.
- AP List—Provides a list of access points detected by the spectrum expert. These access points are on channels that have active interferers detected.
- Affected Clients List—Provides a list of clients that are currently authenticated to an access point. You can select specific RADIUS or LDAP servers to provide external authentication on the **Security > AAA** panel.