CHAPTER 16

Working with Wireless Operational Tools

The Wireless Operational Tools menu allows you to:

- Add or modify guest user templates
- Perform voice audit on controllers
- Diagnose voice calls in realtime
- Analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags
- View all config audit alarm details
- Configure and run migration analysis, and view the report
- Monitor all nearby access points and discover rogue access points
- Monitor RFID tag status
- Configure and edit chokepoints
- Monitor interference devices detected by the CleanAir enabled access points
- Configure spectrum experts and WiFi TDOA receivers

Configuring Guest User Templates

This page allows you to add a guest user template or make modifications to an existing guest user template. The purpose of a guest user account is to provide a user account for a limited amount of time. A Lobby Ambassador configures a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires.

Note When you configure a guest account with unlimited lifetime, for Catalyst 3850 Switches (Cisco IOS XE 3.2.1) and Cisco 5760 Wireless LAN Controllers, the maximum time period that the guest account will be active is one year.

Step 1 Choose **Operate > Operational Tools > Wireless > Guest User**.

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

Step 2 Do either of the following:

- To add a new template:

a. Choose **Select a command** > **Add Guest User**, and click **Go**.

b. In the New Controller Template page, complete the fields as described in the *Guest User Controller Templates Field Descriptions* section in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

- To modify an existing template, click the template name link and make your changes.

Step 3 Click **Save**.

Running a Voice Audit on a Controller

Prime Infrastructure provides a voice auditing mechanism to check controller configuration and to ensure that any deviation from the deployment guidelines is highlighted as an Audit Violation. You can run a voice audit on a maximum of 50 controllers in a single operation.

To run the voice audit:

Step 1 Choose **Operate > Operational Tools > Wireless > Voice Audit**.

Step 2 Click the **Controllers** tab, and complete the fields as described in the *Voice Audit Field Descriptions* section in the *Cisco Prime Infrastructure 2.0 Reference Guide.*

Step 3 Click the **Rules** tab.

Step 4 In the VoWLAN SSID text box, type the applicable VoWLAN SSID.

Note The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

Step 5 Do either of the following:

- To save the configuration without running a report, click **Save**.
- To save the configuration and run a report, click **Save and Run**.

Step 6 Click the **Report** tab to view the report results.

Running Voice Diagnostics

The Voice Diagnostic tool is an interactive tool that diagnoses voice calls in real time. This tool reports call control errors, clients' roaming history, and the total number of active calls accepted and rejected by an associated AP.

The Voice Diagnostic test is provisioned for multiple controllers; that is, if the AP is associated with more than one controller during roaming, the Voice Diagnostic tool tests all associated controllers. Prime Infrastructure supports testing on controllers whose APs are placed on up to three floors. For example, a Prime Infrastructure map might have floors 1 to 4, with all APs associated to controllers (WLC1, WLC2, WLC3, and WLC4) and placed on the Prime Infrastructure map. If a client on any AP is associated with WLC1 on the first floor and a Voice Diagnostic test is started for that client, a test is also provisioned on WLC2 and WLC3.

The Voice Diagnostic page lists prior test runs, if any. For information about the fields on this page, see the *Voice Diagnostic Field Descriptions* section in the *Cisco Prime Infrastructure 2.0 Reference Guide*.

From the Select a command from the drop-down list, you can start a new test, check the results of an existing test, or delete a test.

Note To support roaming, the tool figures out controllers in the same building as of client's associated AP building and adds to all controller's watchlist. The tool looks for controllers in +/-5 floors from client's current association A’s location to configure on controllers. Configuration on controller's watchlist is done for 10 minutes. After 10 minutes controller will remove the entry from the watchlist.

To run a Voice Diagnostic test:

Step 1 Choose **Operate > Operational Tools > Wireless > Voice Diagnostics**.

Step 2 From the Select a command drop-down list, choose the New test and click **Go**.

Note You can configure a maximum of two clients for voice call diagnosis. Both clients can be on the same call or can be on a different call.

Step 3 Enter a test name and the length of time to monitor the voice call.

Step 4 Enter the MAC address of the device for which you want to run the voice diagnostic test.

Step 5 Select a device type; if you select a custom phone, enter an RSSI range.

Step 6 Click **StartTest**.

Location Accuracy Tool

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy tool.

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

The Location Accuracy tool enables you to run either of the following tests:

- **Scheduled Accuracy Testing**—Employed when clients, tags, and interferers are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients, tags, and interferers are already prepositioned so that the test can be run on a regularly scheduled basis.
- **On-Demand Accuracy Testing**—Employed when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

Both are configured and executed through a single page.

Enabling the Location Accuracy Tool

Note You must enable the **Advanced Debug** option in Prime Infrastructure to use the Scheduled and On-demand location accuracy tool testing features. The Location Accuracy tool does not appear as an option on the Operate > Operational Tools > Wireless menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in Prime Infrastructure:

Step 1 In Prime Infrastructure, choose **Operate > Maps**.

Step 2 Choose **Properties** from the Select a command drop-down list, and click **Go**.

Step 3 Select the **Enabled** check box to enable the Advanced Debug Mode. Click **OK**.

Note If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

Use the Select a command drop-down list to create a new scheduled or on-demand accuracy test, to download logs for last run, to download all logs, or to delete a current accuracy test.

Note

- You can download logs for accuracy tests from the Accuracy Tests summary page. To do so, select an accuracy test and from the Select a command drop-down list, choose either **Download Logs** or **Download Logs for Last Run**. Click **Go**.
- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).

- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Scheduling a Location Accuracy Test

Use the scheduled accuracy testing to verify the accuracy of the current location of non-rogue and rogue clients, interferers, and asset tags. You can get a PDF of the test results at **Accuracy Tests** > **Results**. The Scheduled Location Accuracy report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram.
- A cumulative error distribution graph.
- An error distance over time graph.
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location), and error distance over time for each MAC.

To schedule a Location Accuracy test:

Step 1 Choose **Operate > Operational Tools > Wireless > Location Accuracy Tool**.

Step 2 Choose **New Scheduled Accuracy Test** from the Select a command drop-down list.

Step 3 Enter a test name.

Step 4 Choose an area type, a building, and a floor from the corresponding drop-down lists.

Note Campus is configured as Root Area, by default. There is no need to change this setting.

Step 5 Choose a beginning and ending time for the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.

Note When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.

Step 6 Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.)

Step 7 Click **Position Testpoints**.

Step 8 On the floor map, check the check box next to each client, tag, and interferer for which you want to check location accuracy.

When you check a MAC address check box, two icons appear on the map. One represents the actual location and the other represents the reported location. If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map. (You cannot drag the reported location.)

Step 9 (Optional) To enter a MAC address for a client, tag, or interferer that is not listed, check the **Add New MAC** check box, enter the MAC address, and click **Go**.

An icon for the newly added element appears on the map. If the element is on the location server but on a different floor, the icon appears in the left-most corner (in the 0,0 position).

Step 10 When all elements are positioned, click **Save**.

Step 11 Click **OK** to close the confirmation dialog box.

You are returned to the Accuracy Tests summary page.

Step 12 To check the test results, click the test name, click the **Results** tab in the page that appears, and click **Download** under Saved Report.

Running an On-Demand Location Accuracy Test

You can run an On-Demand Accuracy Test when elements are associated but not prepositioned. On-Demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy of a small number of clients, tags, and interferers. You can get a PDF of the test results at **Accuracy Tests** > **Results**. The On-Demand Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram
- A cumulative error distribution graph

To run an On-Demand Accuracy Test:

Step 1 Choose **Operate > Operational Tools > Wireless > Location Accuracy Tool**.

Step 2 From the Select a command drop-down list, choose **New On demand Accuracy Test**.

Step 3 Enter a test name.

Step 4 Choose an area type, a building, and a floor from the corresponding drop-down lists.

Note Campus is configured as Root Area, by default. There is no need to change this setting.

Step 5 Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.)

Step 6 Click **Position Testpoints**.

Step 7 To test the location accuracy and RSSI of a particular location, select client, tag, or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client, tag, or interferer) is displayed in a drop-down list to the right.

Step 8 Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.

Step 9 From the Zoom percentage drop-down list, choose the zoom percentage for the map.

The X and Y text boxes are populated with the coordinates based on the position of the red cross hair in the map.

Step 10 Click **Start** to begin collection of accuracy data, and click **Stop** to finish collection. You must allow the test to run for at least two minutes before stopping the test.

Step 11 Repeat Step 11 to Step 14 for each testpoint that you want to plot on the map.

Step 12 Click **Analyze Results** when you are finished mapping the testpoints, and then click the **Results** tab in the page that appears to view the report.

Configuring Audit Summary

Choose **Operate > Operational Tools > Wireless > Configuration Audit** to launch the Config Audit Summary page.

This page provides a summary of the following:

- Total Enforced Config Groups—Templates that are configured for Background Audit and are enforcement enabled.
- Total Mismatched Controllers—Configuration differences found between Prime Infrastructure and the controller during the last audit.
- Total Config Audit Alarms—Alarms generated when audit discrepancies are enforced on configuration groups. If enforcement fails, a critical alarm is generated on the configuration group. If enforcement succeeds, a minor alarm is generated on the configuration group. Alarms contain links to the audit report, where you can view a list of discrepancies for each controller.
- Most recent 5 config audit alarms—Includes object name, event type, date, and time of the audit alarm.

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

Configuring Migration Analysis

Choose **Operate > Operational Tools > Wireless > Migration Analysis** to launch the Migration Analysis Summary page.

Autonomous access points are eligible for migration only if all criteria have a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version—Conversion is supported only from Cisco IOS 12.3(7)JA releases excluding Cisco IOS 12.3(11)JA, Cisco IOS 12.3(11)JA1, Cisco IOS 12.3(11)JA2, and Cisco IOS 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point

- – root fallback repeater
- – root fallback shutdown
- – root access point only

- Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Upgrading Autonomous Access Points

You can choose to upgrade autonomous access points manually or automatically. On the Migration Analysis page, select an access point whose software version is shown as failed, and choose **Upgrade firmware (manual)** or **Upgrade firmware (automatic)** from the Select a command drop-down list. This process upgrades the autonomous firmware image of the Cisco IOS access point to a supported version.

Prime Infrastructure uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in Prime Infrastructure. The default images on each device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- ap802-k9w7-tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, an additional page with TFTP server IP, file path, and file path name appears. The final page is the Report page.

Changing Station Role to Root Mode

Because a wired connection between an access point and a controller is required to send an association request, an autonomous access point must be assigned the appropriate role. If the role shows as ineligible, choose **Change Station Role to Root Mode** from the Select a command drop-down list to change the mode.

Running Migration Analysis

On the Migration Analysis Summary page, choose **Select a command** > **Run Migration Analysis**. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Viewing the Migration Analysis Report

On the Migration Analysis Summary page, Choose **Select a command** > **View Migration Analysis Report**. The report includes the following:

- Access point address
- Status
- Time stamp
- Access point logs

Viewing a Firmware Upgrade Report

Choose **Select a command** > **View Firmware Upgrade Report** to view a current report of the upgrade status for the selected access point.

The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the firmware upgrade.
- Time stamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

Viewing a Role Change Report

Because a wired connection between an access point and a controller is required to send an association request, the autonomous access point must be assigned the appropriate role.

To view a report of these role changes, choose **View Role Change Report** from the Select a command drop-down list. The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the role change.
- Time stamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

RRM

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points to automatically discover rogue access points.

RRM, built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment.

Prime Infrastructure would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into Prime Infrastructure events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

RRM statistics help to identify trouble spots and provide possible reasons for channel or power-level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on event groupings. The event groupings may include the following:

- Worst performing access points
- Configuration mismatch between controllers in the same RF group
- Coverage holes that were detected by access points based on threshold
- Precoverage holes that were detected by controllers
- Ratios of access points operating at maximum power

Note RRM dashboard information is available only for lightweight access points.

Channel Change Notifications

Notifications are sent to the Prime Infrastructure RRM dashboard when a channel change occurs. Channel changes depend on the Dynamic Channel Assignment (DCA) configuration where the mode can be set to *auto* or *on demand*. When the mode is auto, channel assignment is periodically updated for all lightweight access points that permit this operation. When the mode is set to on demand, channel assignments are updated based on request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global defaults.

When a channel change trap is received after an earlier channel change, the event is marked as Channel Revised; otherwise, it is marked as Channel Changed. A channel change event can have multiple causes. The reason code is factored and equated to 1, irrespective of the number of reasons that are possible. For example, suppose a channel change might be caused by signal, interference, or noise. The reason code in the notification is refactored across the reasons. If the event had three causes, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events have the same reason code, all three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

Notifications are sent to the Prime Infrastructure RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one, irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done and a new group leader is chosen. Dynamic grouping has three modes: Automatic, Off, and Leader. When grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With automatic grouping, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

RRM Dashboard

The RRM dashboard is available at **Operate > Operational Tools > Wireless > Radio Resource Management**.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups. To get the latest number of RF Groups, run the configuration synchronization background task.
- The RRM Statistics portion shows network-wide statistics.
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
  - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
  - WiFi Interference
  - Load
  - Radar
  - Noise
  - Persistent Non-WiFi Interference
  - Major Air Quality Event
  - Other
- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups (derived from all of the controllers which are currently managed by Prime Infrastructure).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the preset value.

  Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

- Channel Change - APs with channel changes—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole - APs reporting coverage holes—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event (threshold based) are displayed.
- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

Note This maximum power portion shows the values from the last 24 hours and is poll driven. This occurs every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power.

Note This maximum power portion shows the value from the last 24 hours and is event driven.

Monitoring RFID Tags

The Monitor > RFID Tags page allows you to monitor tag status and location on Prime Infrastructure maps as well as review tag details.

Note This page is only available in the Location version of Prime Infrastructure.

This section provides information on the tags detected by the location appliance.

The Tag Summary page is available at **Operate > Operational Tools > Wireless > RFID Tags**.

Searching RFID Tags

Use the Prime Infrastructure Advanced Search feature to find specific tags or all tags.

To search for tags:

Step 1 Click **Advanced Search**.

Step 2 From the Search Category drop-down list, choose **Tags**.

Step 3 Enter the required information. Note that search fields sometimes change, depending on the category chosen.

Step 4 Click **Go**.

Checking RFID Tag Search Results

To check the search results, click the MAC address of a tag location on a search results page.

Note the following:

- The Tag Vendor option does not appear when Asset Name, Asset Category, Asset Group, or MAC Address is the search criterion.
- Only vendor tags that support telemetry appear.
- The Telemetry data option appears only when MSE (select for location servers), Floor Area, or Outdoor Area is selected as the “Search for tags by” option.
- Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.
- Asset Information, Statistics, Location, and Location Notification details are displayed.
- Only CCX v1 compliant tags are displayed for emergency data.

Viewing Tag List

Click the **Total Tags number** link to view the Tags List for the applicable device name. The Tag List contains the MAC address, asset details, vendor name, mobility services engine, controller, battery status, and map location.

Chokepoints

Chokepoints are low-frequency transmitting devices. When a tag passes within range of a placed chokepoint, the low-frequency field awakens the tag, which, in turn, sends a message over the Cisco Unified Wireless Network that includes the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room-level accuracy (ranging from few inches to 2 feet, depending on the vendor).

Chokepoints are installed and configured as recommended by the chokepoint vendor. After the chokepoint is installed and operational, it can be entered into the location database and plotted on a Prime Infrastructure map.

Adding a Chokepoint to the Prime Infrastructure Database

To add a chokepoint to the Prime Infrastructure database:

Step 1 Choose **Operate > Operational Tools > Wireless > Chokepoints**.

Step 2 From the Select a command drop-down list, choose **Add Chokepoint**.

Step 3 Click **Go**.

Step 4 Enter the MAC address and name for the chokepoint.

Step 5 Specify either an entry or exit chokepoint.

Step 6 Enter the coverage range for the chokepoint.

Note Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click **OK**.

After the chokepoint is added to the database, it can be placed on the appropriate Prime Infrastructure floor map.

Adding a Chokepoint to a Prime Infrastructure Map

To add a chokepoint to a map:

Step 1 Choose **Operate > Maps**.

Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.

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

Step 4 Click **Go**.

The Add Chokepoints summary page lists all recently added chokepoints that are in the database but not yet mapped.

Step 5 Check the check box next to the chokepoint that you want to place on the map.

Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top-left corner. You are now ready to place the chokepoint on the map.

Step 7 Click the chokepoint icon and drag it to the proper location.

The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8 Click **Save**.

The newly created chokepoint icon might or might not appear on the map, depending on the display settings for that floor. The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse over its map icon.

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Note Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.

Step 10 Synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from the Prime Infrastructure Database

To remove a chokepoint from the Prime Infrastructure database:

Step 1 Choose **Operate > Operational Tools > Wireless > Chokepoints**.

Step 2 Select the check box of the chokepoint that you want to delete.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

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

Removing a Chokepoint from a Prime Infrastructure Map

To remove a chokepoint from a Prime Infrastructure map:

Step 1 Choose **Operate > Maps**.

Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

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

Editing a Chokepoint

To edit a chokepoint in the Prime Infrastructure database and the appropriate map:

Step 1 Choose **Operate > Operational Tools > Wireless > Chokepoints**.

Step 2 In the MAC Address column, click the chokepoint you want to edit.

Step 3 Edit the parameters that you want to change.

Note The chokepoint range is product-specific and is supplied by the chokepoint vendor.

Step 4 Click **Save**.

Monitoring Interferers

In the **Monitor** > **Interferers** page, you can monitor interference devices detected by CleanAir-enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

Table 16-1 lists the menu paths to follow to monitor interferers.

Table 16-1 Menu Paths to Monitor Interferers

To See...	Go To...
AP-detected interferers	**Operate** > **Operational Tools** > **Wireless** > **Interferers**
AP-detected interferer details	**Operate** > **Operational Tools** > **Wireless** > **Interferers** > *Interferer ID*
AP-detected interferer details location history	**Operate** > **Operational Tools** > **Wireless** > **Interferers** > *Interferer ID*, then choose **Select a command** > **Location History** and click **Go**

Spectrum Experts

A spectrum expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, monitor, and archive detailed interferer data from spectrum experts in the network.

To configure spectrum experts, choose **Operate > Operational Tools > Wireless > 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 Prime Infrastructure. The status appears as reachable or unreachable.

Adding a Spectrum Expert

To add a spectrum expert:

Step 1 Choose **Operate > Operational Tools > Wireless > Spectrum Experts**.

Step 2 Choose **Select a command** > **Add Spectrum Expert**. (This link appears only if no spectrum experts already exist.)

Step 3 Enter the hostname or IP address of the spectrum expert. If you use the hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

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

Spectrum Experts Details

The Spectrum Expert Details page provides interference details for a single spectrum expert. This page is updated every 20 seconds, providing a real-time look at what is happening on the remote spectrum expert. This page displays the following:

- Total Interferer Count—As seen by 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 that are on channels that have active interferers detected by the spectrum expert on those channels.
- Affected Clients List—Provides a list of clients that are authenticated and associated with the radio of one of the access points listed in the access point list.

Wi-Fi TDOA Receivers

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset.

Enhancing Tag Location Reporting with Wi-Fi TDOA Receivers

TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

Note

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network. See the Adding a Mobility Services Engine section in the Cisco Prime Infrastructure 2.0 Configuration Guide.
2. Add the TDOA receiver to Prime Infrastructure database and map. See the "Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps" section on page 16-18.
3. Activate or start the partner engine service on the MSE using Prime Infrastructure.
4. Synchronize Prime Infrastructure and mobility services engines. See the Synchronizing Services section in the Cisco Prime Infrastructure 2.0 Configuration Guide.
5. Set up the TDOA receiver using the AeroScout System Manager. See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* for configuration details at the following URL:
   http://support.aeroscout.com.

Adding Wi-Fi TDOA Receivers to Prime Infrastructure and Maps

After the Wi-Fi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on a Prime Infrastructure map.

After adding TDOA receivers to Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than Prime Infrastructure.

Note For more details on configuration options, see the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide* at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the Prime Infrastructure database and the appropriate map:

Step 1 Choose **Operate > Operational Tools > Wireless > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Note To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3 Click **Go**.

Step 4 Enter the MAC address, name, and static IP address of the TDOA receiver.

Step 5 Click **OK** to save the TDOA receiver entry to the database.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6 Choose **Operate > Maps**.

Step 7 In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 8 From the Select a command drop-down list, choose **Add WiFi TDOA receivers**.

Step 9 Click **Go**.

The All WiFi TDOA Receivers summary page lists all recently-added TDOA receivers that are in the database but not yet mapped.

Step 10 Select the check box next to each TDOA receiver to add it to the map.

Step 11 Click **OK**.

A map appears with a TDOA receiver icon located in the top-left corner. You are now ready to place the TDOA receiver on the map.

Step 12 Click the TDOA receiver icon and drag it to the proper location on the floor map.

Step 13 Click **Save**.

The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 14.

Step 14 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 15 Check the **WiFi TDOA Receivers** check box.

When you hover your mouse cursor over a TDOA receiver on a map, configuration details appear for that receiver.

Step 16 Click **X** to close the Layers page.

Note Do not choose **Save Settings** from the Layers menu unless you want to save this display criteria for all maps.

Step 17 Download the partner engine software to the mobility services engine.