Configuring and Deploying wIPS Solution

This section describes how to configure and deploy the wIPS solution using the Lifecycle theme in the Prime Infrastructure UI.

Choose **Design** > **Wireless Security** from the Lifecycle theme in the Prime Infrastructure UI. The Wireless Security wizard page appears and allows you to perform the following wIPS related configurations:

- Allows rogue policy to detect and report ad hoc networks.
- Allows rogue rules to define rules to automatically classify rogue access points.
- Allows you to add new wIPS profiles.

This section contains the following topics:

Viewing the Before You Begin Wizard Page

The Before You Begin wizard page displays information about how to use the Wireless Security wizard and includes the following information:

- Rogue Policy—The Rogue Policy page enables you to configure the rogue policy. It has three pre-configured rogue policy settings for rogue detection and containment.
- Rogue Rules—The Rogue Rules page allows you to automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Rogue rules can be created to classify rogues as Malicious and Friendly.
- wIPS Profile—The wIPS Profile page provides several pre-defined profiles from which to choose. These profiles allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. The profile can be further customized by selecting the awIPS signatures to be detected and contained.

- Devices—The Devices page allows you to apply rogue policy, rogue rules, and wIPS profiles to controllers.

Click **Next** to configure the Rogue Policy to detect and report ad hoc networks.

Configuring Rogue Policies

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

To configure the rogue policies, follow these steps:

Step 1 Choose **Design** > **Wireless Security** > **Rogue Policy**.

Step 2 You can either set the policy settings to **Low**, **High**, or **Critical** by moving the Configure the rogue policy settings sliding bar with the mouse or select the **Custom** check box to configure the policy settings.

Step 3 In the General group box, configure the following fields:

- Rogue Location Discovery Protocol—Determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - **Disable—**Disables RLDP on all access points.
  - **All APs—**Enables RLDP on all access points.
  - **Monitor Mode APs—**Enables RLDP only on access points in monitor mode.

  Note With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points, that do not have encryption enabled.
- Expiration Timeout for Rogue AP and Rogue Client Entries—Set the expiration timeout (in seconds) for rogue access point entries. The valid range is 240 to 3600 seconds.
- Validate rogue clients against AAA—Select the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.
- Detect and report Adhoc networks—Select the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.
- Rogue Detection Report Interval—In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
- Rogue Detection Minimum RSSI—In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBM to -128 dBm. This feature is applicable to all the AP modes.
- Rogue Detection Transient Interval—In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

Step 4 In the Auto Contain group box, configure the following fields:

- Rogue on Wire—Select the **Rogue on Wire** check box to auto contain those APs that are detected on the wired network.
- Using our SSID—Select the **Using our SSID** check box.
- Valid client on Rogue AP—Select the **Valid client on Rogue AP** check box to auto contain the valid clients from connecting to the rogue APs.
- AdHoc Rogue—Select the **AdHoc Rogue** checkbox to auto contain adhoc rogue APs.

Step 5 Click **Apply** to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click **Apply to Controllers**

Step 6 Click **Next** to configure the rogue rules.

Configuring Rogue Rules

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

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

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

Step 1 Choose **Design** > **Wireless Security** > **Rogue Rules**.

Step 2 Click **Create New** to create new rogue rules.
The Add/Edit Rogue Rule window appears.

Step 3 In the General group box, configure the following fields:

- Rule Name—Enter a name for the rule in the text box.
- Rule Type—Choose **Malicious** or **Friendly** from the drop-down list.

  Note 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.

- Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.

Step 4 In the Rogue Classification Rule group box, configure the following fields:

- Open Authentication—Select the **Open Authentication** check box to enable Open Authentication.
- Match Managed AP SSID—Select the **Match Managed AP SSID** check box to enable the matching of managed AP SSID rule condition.

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

- Match User Configured SSID (Enter one per line)—Select the **Match User Configured SSID** check box to enable the matching of user configured SSID rule condition.

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

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

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

- Time Duration—Select the **Time Duration** check box to enable the Time Duration limit.

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

- Minimum Number Rogue Clients—Select the **Minimum Number Rogue Clients** check box to enable the Minimum Number Rogue Clients limit.

  Note 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 5 Click **Ok** to save the rule or **Cancel** to cancel the creation or changes made to the current rule.
You are returned to the Rogue Rules page and the newly added rogue rule is listed.

Step 6 Click **Apply** to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click **Apply to Controllers**.
Note

Step 7 Click **Next** to configure the wIPS profiles.

Viewing Currently Added Rogue Rules

To view currently added rogues rules, follow these steps:

Choose **Design** > **Wireless Security** > **Rogue Rules** from the Lifecycle theme in the Prime Infrastructure UI.
The following parameters are displayed in the Rogue Rules page.

- Add Existing Rules
- Rule Name

- Rule Type
- Last Saved At
- Actions

Configuring the wIPS Profiles

Prime Infrastructure provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

For more information on configuring the wIPS profile, see the Configuring wIPS and Profiles section.

After configuring wIPS profile, click **Next** to open the Devices page where you can select the controllers to apply the settings.