Classifying Rogue Access Points

Rogue Access Point Classification

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, Custom, or Unclassified. For the Custom type, you must specify a severity score and a classification name.

Note Manual classification and classification that is the result of auto-containment or rogue-on-wire overrides the rogue rule. If you have manually changed the class and/or the state of a rogue AP, then to apply rogue rules to the AP, you must change it to unclassified and alert condition.

Note If you manually move any rogue device to contained state (any class) or friendly state, this information is stored in the standby Cisco WLC flash memory; however, the database is not updated. When HA switchover occurs, the rogue list from the previously standby Cisco WLC flash memory is loaded.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, custom, and unclassified) in the Alert state only.

You can configure up to 64 rogue classification rules per controller.

You can also apply rogue rules to ad hoc rogues except for client count condition.

The number of rogue clients that can be stored in the database table of a rogue access point is 256.

If a rogue AP or an ad hoc rogue is classified because of an RSSI rogue rule condition, the RSSI value that caused the trigger is displayed on the controller GUI/CLI. The controller includes the classified RSSI, the classified AP MAC address, and rule name in the trap. A new trap is generated for every new classification or change of state due to rogue rule but[3] is rate limited to every half hour for every rogue AP or ad hoc rogue. However, if there is a change of state in containment by rogue rule, the trap is sent immediately. The 'classified by,' 'classified at,' and 'classified by rule name' are valid for the non-default classification types, which are Friendly, Malicious, and Custom classifications. For the unclassified types, these fields are not displayed.

Note For the RSSI condition of rogue rule, reclassification occurs only if the RSSI change is more than 2 dBm of the configured RSSI value.

The rogue rule may not work properly if friendly rogue rule is configured with RSSI as a condition. Then, you need to modify the rules with the expectation that friendly rule is using maximum RSSI and modify rules accordingly.

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

Table 1: Classification Mapping

Rule-Based Classification Type	Rogue States
Friendly	• Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. An example is the access points in your lab network. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. An example is an access point that belongs to a neighboring coffee shop. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.
Malicious	• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained.
Custom	• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained.
Unclassified	• Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained. • Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

The classification and state of the rogue access points are configured as follows:

- From Known to Friendly, Internal
- From Acknowledged to Friendly, External
- From Contained to Malicious, Contained

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

This section contains the following subsections:

Guidelines and Restrictions for Classifying Rogue Access Points

- Classifying Custom type rogues is tied to rogue rules. Therefore, it is not possible to manually classify a rogue as Custom. Custom class change can occur only when rogue rules are used.
- Some are sent for containment by rule and every 30 minutes for rogue classification change. For custom classification, the first trap does not contain the severity score because the trap has existed before the custom classification. The severity score is obtained from the subsequent trap that is generated after 30 minutes if the rogue is classified.
- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.
- After a rogue satisfies a higher priority rule and is classified, it does not move down the priority list for the same report.
- Previously classified rogue gets re-classified on every new rogue report with the following restrictions:
  - Rogues which are classified as friendly by rule and whose state is set to ALERT, go through re-classification on receiving the new rogue report.
  - If a rogue is classified as friendly by the administrator manually, then the state is INTERNAL and it does not get re-classified on successive rogue reports.
  - If rogue is classified as malicious, irrespective of the state it does not get re-classified on subsequent rogue reports.
- Transition of the rogue's state from friendly to malicious is possible by multiple rogue rules if some attribute is missing in new rogue report.
- Transition of the rogue's state from malicious to any other classification is not possible by any rogue rule.
- If a rogue AP is classified as friendly, it means that the rogue AP exists in the vicinity, is a known AP, and need not be tracked. Therefore, all the rogue clients are either deleted or not tracked if they are associated with the friendly rogue AP.
- Until the controller discovers all the APs through neighbor reports from APs, the rogue APs are kept in unconfigured state for three minutes after they are detected. After 3 minutes, the rogue policy is applied on the rogue APs and the APs are moved to unclassified, friendly, malicious, or custom class. Rogue APs kept in unconfigured state means that no rogue policy has yet been applied on them.
- When a rogue BSSID is submitted for a containment on Cisco Catalyst 9800 Series Wireless Controller, if the controller has enough resources, it will contain. The APs that detect the particular contained rogue AP starts broadcasting the DEAUTH packets.

  Wireless client connected to the contained rogue BSSID will disconnect once DEAUTH packets are received. However, when the client assumes being in a connected state, repeatedly tries to reconnect and the wireless client's user browsing experience would be badly affected.

  Also, in a high RF environment like that of a stadium, though DEAUTH packets are broadcasted, client does not receive all of them because of RF disturbance. In this scenario, the client may not be fully disconnected but will be affected badly.

Configuring Rogue Classification Rules (GUI)

Step 1 Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Rogue Rules** to open the Rogue Rules page.

Any rules that have already been created are listed in priority order. The name, type, and status of each rule is provided.

Note To delete a rule, hover your cursor over the blue drop-down arrow for that rule and click **Remove**.

Step 2 Create a new rule as follows:

a) Click **Add Rule**. An Add Rule section appears at the top of the page.

b) In the **Rule Name** text box, enter a name for the new rule. Ensure that the name does not contain any spaces.

c) From the **Rule Type** drop-down list, choose from the following options to classify rogue access points matching this rule as friendly or malicious:

- **Friendly**
- **Malicious**
- **Custom**

d) Configure the notification when the rule is matched from the **Notify** drop-down list to **All**, **Global**, **Local**, or **None**.

Rule description:

- **All**—Notifies the Cisco WLC and a trap receiver such as Cisco Prime Infrastructure.
- **Global**—Notifies only a trap receiver such as Cisco Prime Infrastructure.
- **Local**—Notifies only Cisco WLC.
- **None**—No notifications are sent.

Note Rogue Rule Notification options **All**, **Global**, **Local**, and **None** can control only the following rogue traps mentioned:

- Rogue AP Detected (Rogue AP: XX:XX:XX:XX:XX:XX detected on Base Radio MAC: XX:XX:XX:XX:XX:XX Interface no: 0(1) Channel: 6 RSSI: 45 SNR: 10 Classification: unclassified, State: alert, RuleClassified : unclassified, Severity Score: 100, RuleName: rule1, Classified AP MAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue Adhoc Detected (Adhoc Rogue : XX:XX:XX:XX:XX:XX detected on Base Radio MAC : XX:XX:XX:XX:XX:XX Interface no: 0(1) on Channel 6 with RSSI: 45 and SNR: 10 Classification: unclassified, State: alert, RuleClassified: unclassified, Severity Score: 100, RuleName: rule1,Classified APMAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue AP contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX has been contained due to rule with containment Level : 1)
- Rogue AP clear contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX is no longer contained due to rule

e) Configure the state of the rogue AP when the rule is matched from the **State** drop-down list.

f) If you choose the Rule Type as Custom, enter the Severity Score and the Classification Name.

g) Click **Add** to add this rule to the list of existing rules, or click **Cancel** to discard this new rule.

Step 3 Edit a rule as follows:

a) Click the name of the rule that you want to edit. The **Rogue Rule > Edit** page appears.

b) From the Type drop-down list, choose from the following options to classify rogue access points matching this rule:

- **Friendly**
- **Malicious**
- **Custom**

c) Configure the notification when the rule is matched from the **Notify** drop-down list to **All**, **Global**, **Local**, or **None**.

d) Configure the state of the rogue AP when the rule is matched from the **State** drop-down list.

e) From the Match Operation text box, choose one of the following:

Match All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.

Match Any—If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. This is the default value.

f) To enable this rule, select the **Enable Rule** check box. The default value is unselected.

g) If you choose the Rule Type as Custom, enter the Severity Score and the Classification Name.

h) From the Add Condition drop-down list, choose one or more of the following conditions that the rogue access point must meet and click **Add Condition**.

- **SSID**—Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the **User Configured SSID** text box, and click **Add SSID**.

  Note To delete an SSID, highlight the SSID and click **Remove**.

- **RSSI**—Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the **Minimum RSSI** text box. The valid range is 0 to –128 dBm (inclusive).
- **Duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the **Time Duration** text box. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.

- **Client Count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the **Minimum Number of Rogue Clients** text box. The valid range is 1 to 10 (inclusive), and the default value is 0.

- **No Encryption**—Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option.

  Note Cisco Prime Infrastructure refers to this option as "Open Authentication."

- **Managed SSID**—Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.

Note The SSID and Managed SSID conditions cannot be used with the Match All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

You can add up to six conditions per rule. When you add a condition, it appears under the Conditions section.

Note To delete a condition from this rule, hover your cursor over the blue drop-down arrow for that condition and click **Remove**.

i) Click **Apply**.

Step 4 Click **Save Configuration**.

Step 5 If you want to change the order in which rogue classification rules are applied, follow these steps:

a. Click **Back** to return to the Rogue Rules page.

b. Click **Change Priority** to access the Rogue Rules > Priority page.

The rogue rules are listed in priority order in the Change Rules Priority text box.

c. Highlight the rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.

d. Continue to move the rules up or down until the rules are in the desired order.

e. Click **Apply**.

Step 6 Classify any rogue access points as friendly and add them to the friendly MAC address list as follows:

- Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Friendly Rogue** to open the Friendly Rogue > Create page.
- In the MAC Address text box, enter the MAC address of the friendly rogue access point.
- Click **Apply**.
- Click **Save Configuration**. This access point is added to the controller's list of friendly access points and should now appear on the Friendly Rogue APs page.

Viewing and Classifying Rogue Devices (GUI)

Before you begin

Caution When you choose to **contain a rogue device**, the following warning appears: "There may be legal issues following this containment. Are you sure you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Step 1 Choose **Monitor** > **Rogues**.

Step 2 Choose the following options to view the different types of rogue access points detected by the controller:

- **Friendly APs**
- **Malicious APs**
- **Unclassified APs**
- **Custom APs**

The respective rogue APs pages provide the following information: the MAC address and SSID of the rogue access point, channel number, the number of radios that detected the rogue access point, the number of clients connected to the rogue access point, and the current status of the rogue access point.

Note To remove acknowledged rogues from the database, change the rogue state to Alert. If the rogue is no longer present, the rogue data is deleted from the database in 20 minutes.

Note To delete a rogue access point from one of these pages, hover your cursor over the blue drop-down arrow and click **Remove**. To delete multiple rogue access points, select the check box corresponding to the row you want to delete and click **Remove**.

Note You can move the Malicious or Unclassified rogue APs that are being contained or were contained back to Alert state by clicking the **Move to Alert** button on the respective pages.

Step 3 Get more details about a rogue access point by clicking the MAC address of the access point. The Rogue AP Detail page appears.

This page provides the following information: the MAC address of the rogue device, the type of rogue device (such as an access point), whether the rogue device is on the wired network, the dates and times when the rogue device was first and last reported, and the current status of the device.

The Class Type text box shows the current classification for this rogue access point:

- **Friendly**—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained.
- **Malicious**—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the Friendly or Unclassified classification type.

  Note Once an access point is classified as Malicious, you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the Unclassified classification type, you must delete the access point and allow the controller to reclassify it.

- **Unclassified**—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the Friendly or Malicious classification type automatically in accordance with user-defined rules or manually by the user.
- **Custom**—A user-defined classification type that is tied to rogue rules. It is not possible to manually classify a rogue as Custom. Custom class change can occur only using rogue rules.

Step 4 If you want to change the classification of this device, choose a different classification from the Class Type drop-down list.

Note A rogue access point cannot be moved to another class if its current state is Contain.

Step 5 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue access point:

- **Internal**—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly.
- **External**—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly.
- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

The bottom of the page provides information on both the access points that detected this rogue access point and any clients that are associated to it. To see more details for any of the clients, click **Edit** to open the Rogue Client Detail page.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Step 8 View any rogue clients that are connected to the controller by choosing **Rogue Clients**. The Rogue Clients page appears. This page shows the following information: the MAC address of the rogue client, the MAC address of the access point to which the rogue client is associated, the SSID of the rogue client, the number of radios that detected the rogue client, the date and time when the rogue client was last reported, and the current status of the rogue client.

Step 9 Obtain more details about a rogue client by clicking the MAC address of the client. The Rogue Client Detail page appears.

This page provides the following information: the MAC address of the rogue client, the MAC address of the rogue access point to which this client is associated, the SSID and IP address of the rogue client, the dates and times when the rogue client was first and last reported, and the current status of the rogue client.

Step 10 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue client:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.

The bottom of the page provides information on the access points that detected this rogue client.

Step 11 Click **Apply**.

Step 12 If desired, you can test the controller's connection to this client by clicking **Ping**.

Step 13 Click **Save Configuration**.

Step 14 See any ad-hoc rogues detected by the controller by choosing **Adhoc Rogues**. The Adhoc Rogues page appears.

This page shows the following information: the MAC address, BSSID, and SSID of the ad-hoc rogue, the number of radios that detected the ad-hoc rogue, and the current status of the ad-hoc rogue.

Step 15 Obtain more details about an ad-hoc rogue by clicking the MAC address of the rogue. The Adhoc Rogue Detail page appears.

This page provides the following information: the MAC address and BSSID of the ad-hoc rogue, the dates and times when the rogue was first and last reported, and the current status of the rogue.

Step 16 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this ad-hoc rogue:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.
- **Internal**—The controller trusts this rogue access point.
- **External**—The controller acknowledges the presence of this rogue access point.

Step 17 From the Maximum number of APs to contain the rogue drop-down list, choose one of the following options to specify the maximum number of access points used to contain this ad-hoc rogue: **1**, **2**, **3**, or **4**.

The bottom of the page provides information on the access points that detected this ad-hoc rogue.

- **1**—Specifies targeted rogue access point is contained by one access point. This is the lowest containment level.
- **2**—Specifies targeted rogue access point is contained by two access points.
- **3**—Specifies targeted rogue access point is contained by three access points.
- **4**—Specifies targeted rogue access point is contained by four access points. This is the highest containment level.

Step 18 Click **Apply**.

Step 19 Click **Save Configuration**.

Step 20 View any access points that have been configured to be ignored by choosing **Rogue AP Ignore-List**. The Rogue AP Ignore-List page appears.

This page shows the MAC addresses of any access points that are configured to be ignored. The rogue-ignore list contains a list of any autonomous access points that have been manually added to Cisco Prime Infrastructure maps by the users. The controller regards these autonomous access points as rogues even though the Prime Infrastructure is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

- When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
- If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
- If the unknown access point is not in the rogue-ignore list, the controller sends a trap to the Prime Infrastructure. If the Prime Infrastructure finds this access point in its autonomous access point list, the Prime Infrastructure sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
- If a user removes an autonomous access point from the Prime Infrastructure, the Prime Infrastructure sends a command to the controller to remove this access point from the rogue-ignore list.

Configuring Rogue Classification Rules (CLI)

Step 1 Create a rule by entering this command:

config rogue rule add ap priority *priority* **classify** {**friendly** | **malicious**} *rule-name*

If you later want to change the priority of this rule and shift others in the list accordingly, enter the **config rogue rule priority** *priority rule-name* command.

If you later want to change the classification of this rule, enter the **config rogue rule classify** {**friendly** | **malicious**} *rule-name* command.

If you ever want to delete all of the rogue classification rules or a specific rule, enter the {**config rogue rule delete** {**all** | *rule-name*} command.

Step 2 Create a rule by entering these commands:

- Configure a rule for friendly rogues by entering this command:

  config rogue rule add ap priority *priority* **classify friendly notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **internal** | **external**} *rule-name*

- Configure a rule for malicious rogues by entering this command:

  config rogue rule add ap priority *priority* **classify malicious notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain**} *rule-name*

- Configure a rule for custom rogues by entering this command:

  config rogue rule add ap priority *priority* **classify custom** *severity-score classification-name* **notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain**} *rule-name*

If you later want to change the priority of this rule and shift others in the list accordingly, enter the **config rogue rule priority** *priority rule-name* command.

If you later want to change the classification of this rule, enter the **config rogue rule classify** {**friendly** | **malicious** | **custom** *severity-score classification-name*} *rule-name* command.

If you ever want to delete all of the rogue classification rules or a specific rule, enter the {**config rogue rule delete** {**all** | *rule-name*} command.

Step 3 Configure the state on the rogue AP upon rule match by entering this command:

config rogue rule state {**alert** | **contain** | **internal** | **external**} *rule-name*

Step 4 Configure the notification upon rule match by entering this command:

config rogue rule notify {**all** | **global** | **local** | **none**} *rule-name*

Step 5 Disable all rules or a specific rule by entering this command:

config rogue rule disable {*all* | *rule_name*}

Note A rule must be disabled before you can modify its attributes.

Step 6 Add conditions to a rule that the rogue access point must meet by entering this command:

config rogue rule condition ap set *condition_type condition_value rule_name*

The following condition types are available:

- **ssid**—Requires that the rogue access point have a specific SSID. You should add SSIDs that are not managed by the controller. If you choose this option, enter the SSID for the *condition_value parameter*. The SSID is added to the user-configured SSID list.

  Note If you ever want to delete all of the SSIDs or a specific SSID from the user-configured SSID list, enter the **config rogue rule condition ap delete ssid** {**all** | **ssid**} *rule_name* command.

  Note The sub-string should be specified in full or part of SSID (without any asterisks). This sub-string is matched in the same sequence to its occurrence in the rogue AP SSID. Once the condition is met, the rogue AP is classified (depending on OR or AND match condition).

- **rssi**—Requires that the rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value for the *condition_value parameter*.

  In Release 8.0 and later releases, for friendly rogue rules, you are required to set a maximum RSSI value. The RSSI value of the rogue AP must be less than the RSSI value set, for the rogue AP to be classified as a friendly rogue. For malicious and custom rogue rules, there is no change in functionality.

  For example, for a friendly rogue rule, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is less than –80 dBm are classified as friendly rogues. For malicious and custom rogue rules, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is more than –80 dBm are classified as malicious or custom rogue APs.

- **duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the *condition_value parameter*. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.

- **client-count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the *condition_value parameter*. The valid range is 1 to 10 (inclusive), and the default value is 0.

- **managed-ssid**—Requires that the rogue access point's SSID be known to the controller. A *condition_value parameter* is not required for this option.

  Note You can add up to six conditions per rule. If you ever want to delete all of the conditions or a specific condition from a rule, enter the **config rogue rule condition ap delete all** *condition_type condition_value rule_name* command.

Step 7 Specify whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule by entering this command:

config rogue rule match {**all** | **any**} *rule_name*

Step 8 Enable all rules or a specific rule by entering this command:

config rogue rule enable {**all** | **rule_name**}

Note For your changes to become effective, you must enable the rule.

Step 9 Add a new friendly access point entry to the friendly MAC address list or delete an existing friendly access point entry from the list by entering this command:

config rogue ap friendly {**add** | **delete**} *ap_mac_address*

Step 10 Save your changes by entering this command:

save config

Step 11 View the rogue classification rules that are configured on the controller by entering this command:

show rogue rule summary

Step 12 View detailed information for a specific rogue classification rule by entering this command:

show rogue rule detailed *rule_name*

Viewing and Classifying Rogue Devices (CLI)

Procedure

- View a list of all rogue access points detected by the controller by entering this command:

  show rogue ap summary
- See a list of the friendly rogue access points detected by the controller by entering this command:

  show rogue ap friendly summary
- See a list of the malicious rogue access points detected by the controller by entering this command:

  show rogue ap malicious summary
- See a list of the unclassified rogue access points detected by the controller by entering this command:

  show rogue ap unclassified summary
- See detailed information for a specific rogue access point by entering this command:

  show rogue ap detailed *ap_mac_address*
- See the rogue report (which shows the number of rogue devices detected on different channel widths) for a specific 802.11a/n radio by entering this command:

  show ap auto-rf 802.11a *Cisco_AP*
- See a list of all rogue clients that are associated to a rogue access point by entering this command:

  show rogue ap clients *ap_mac_address*
- See a list of all rogue clients detected by the controller by entering this command:

  show rogue client summary
- See detailed information for a specific rogue client by entering this command:

  show rogue client detailed *Rogue_AP client_mac_address*

- See a list of all ad-hoc rogues detected by the controller by entering this command:

  show rogue adhoc summary

- See detailed information for a specific ad-hoc rogue by entering this command:

  show rogue adhoc detailed *rogue_mac_address*

- See a summary of ad hoc rogues based on their classification by entering this command:

  show rogue adhoc {**friendly** | **malicious** | **unclassified**} **summary**

- See a list of rogue access points that are configured to be ignore by entering this command:

  show rogue ignore-list

- Classify a rogue access point as friendly by entering this command:

  config rogue ap classify friendly state {**internal** | **external**} *ap_mac_address*

  where

  internal means that the controller trusts this rogue access point.

  external means that the controller acknowledges the presence of this rogue access point.

Note A rogue access point cannot be moved to the Friendly class if its current state is Contain.

- Mark a rogue access point as malicious by entering this command:

  config rogue ap classify malicious state {**alert** | **contain**} *ap_mac_address*

  where

  alert means that the controller forwards an immediate alert to the system administrator for further action.

  contain means that the controller contains the offending device so that its signals no longer interfere with authorized clients.

Note A rogue access point cannot be moved to the Malicious class if its current state is Contain.

Caution Performing rogue containment might be illegal if the target of the attack is a device that you do not own. Enable rogue containment only if none of your APs can transmit radio signals outside of your property.

- Mark a rogue access point as unclassified by entering this command:

  config rogue ap classify unclassified state {**alert** | **contain**} *ap_mac_address*

Note A rogue access point cannot be moved to the Unclassified class if its current state is Contain.

alert means that the controller forwards an immediate alert to the system administrator for further action.

contain means that the controller contains the offending device so that its signals no longer interfere with authorized clients.

- Choose the maximum number of access points used to contain the ad-hoc rogue by entering this command:

  config rogue ap classify unclassified state contain *rogue_ap_mac_address 1, 2, 3, or 4*

  - **1**—Specifies targeted rogue access point will be contained by one access point. This is the lowest containment level.
  - **2**—Specifies targeted rogue access point will be contained by two access points.
  - **3**—Specifies targeted rogue access point will be contained by three access points.
  - **4**—Specifies targeted rogue access point will be contained by four access points. This is the highest containment level.

- Specify how the controller should respond to a rogue client by entering one of these commands:

  config rogue client alert *client_mac_address*—The controller forwards an immediate alert to the system administrator for further action.

  config rogue client contain *client_mac_address*—The controller contains the offending device so that its signals no longer interfere with authorized clients.

- Specify how the controller should respond to an ad-hoc rogue by entering one these commands:

  config rogue adhoc alert *rogue_mac_address*—The controller forwards an immediate alert to the system administrator for further action.

  config rogue adhoc contain *rogue_mac_address*—The controller contains the offending device so that its signals no longer interfere with authorized clients.

  config rogue adhoc external *rogue_mac_address*—The controller acknowledges the presence of this ad-hoc rogue.

- Configure the classification of ad hoc rogues by entering any one of these commands:
  - Friendly state—**config rogue adhoc classify friendly state** {**internal** | **external**} *mac-addr*
  - Malicious state—**config rogue adhoc classify malicious state** {**alert** | **contain**} *mac-addr*
  - Unclassified state—**config rogue adhoc classify unclassified state** {**alert** | **contain**} *mac-addr*

- View a summary of custom rogue AP information by entering this command:

  show rogue ap custom summary

- See custom ad hoc rogue information by entering this command:

  show rogue adhoc custom summary

- Delete the rogue APs by entering this command:

  config rogue ap delete {**class** | **all** | *mac-addr*}

- Delete the rogue clients by entering this command:

  config rogue client delete {**state** | **all** | *mac-addr*}
- Delete the ad hoc rogues by entering this command:

  config rogue adhoc delete {**class** | **all** | *mac-addr*}
- Save your changes by entering this command:
  save config