Classifying Rogue Access Points

Information About Classifying Rogue Access Points

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, Custom, or Unclassified.

By default, none of the classification rules are used. You need to enable them. Therefore, all unknown access points are categorized as Unclassified. When you create or change a rule, configure conditions, and enable it, all rogue access points are then reclassified. Whenever you change a rule, it is applied to all the access points (friendly, malicious, and unclassified).

Note

- Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.
- You can configure up to 64 rogue classification rules per controller .

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

- If the unknown access point is in the friendly MAC address list, the controller classifies the access point as Friendly.
- If the unknown access point is not in the friendly MAC address list, the controller starts applying the rogue classification rules to the access point.
- If the rogue access point is manually classified, rogue rules are not applied to it.
- If the rogue access point matches the configured rules criteria, the controller classifies the rogue based on the classification type configured for that rule.
- If the rogue access point does not match any of the configured rules, the rogue remains unclassified.

  The controller repeats the previous steps for all the rogue access points.

- If the rogue access point is detected on the same wired network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if there are no configured rules. You can then manually contain the rogue to change the rogue state to Contained. If the rogue access point is not available on the network, the controller marks the rogue state as Alert. You can then manually contain the rogue.
- If desired, you can manually move the access point to a different classification type and rogue state.
- Before performing any classification, the rogue access points are temporarily marked as Pending.

Table 1: Classification Mapping

Rule-Based Classification Type	Rogue State
Custom	• Alert—No action is taken other than notifying the management station. The management station in the controller manages the controller and wired networks. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in Contained Pending state.
Delete	Deletes the rogue access point.
Friendly	• Internal—If the unknown access point poses no threat to WLAN security, you can manually configure it as Friendly, Internal. An example of this would be 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 can manually configure it as Friendly, External. An example of this would be the access point in your neighboring coffee shop. • Alert—No action is taken other than notifying the management station. The management station manages the controller and wired networks.
Malicious	• Alert—No action is taken other than notifying the management station. The management station manages the controller and wired networks. • Threat—The unknown access point is found to be on the network and poses a threat to WLAN security. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in Contained Pending state.
Unclassified	• Alert— No action is taken other than notifying the management station. The management station manages the controller and wired networks. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in contained pending state.

As mentioned earlier, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules. Alternatively, you can manually move the unknown access point to a different classification type and rogue state.

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 SNMP traps are sent for containment by rule and every 30 minutes for rogue classification change.
- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.
- After a rogue satisfies a rule and is classified, it does not move down the priority list for the same report.
- The rogue classification rules are re-evaluated at every report received by the managed access points. Hence, a rogue access point can move from one state to another, if a different rule matches the last report.
- If a rogue AP is classified as friendly or ignored, all rogue clients associated with it are not tracked.
- 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.
- The rouge AP manual classification limit has been enhanced from 625 to 10,000 configurations at a time. The rouge client manual classification limit has been enhanced from 625 to 10,000 configurations at a time.

How to Classify Rogue Access Points

Classifying Rogue Access Points and Clients Manually (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **Rogues**.

Step 2 In the **Unclassified** tab, select an AP to view the detail in the lower pane.

Step 3 Use the **Class Type** drop-down to set the status.

Step 4 Click **Apply**.

Classifying Rogue Access Points and Clients Manually (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue adhoc** {**alert** *mac-addr* | **auto-contain** | **contain** *mac-addr containment-level* | **internal** *mac-addr* | **external** *mac-addr*} **Example:** `Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520`	Detects and reports the ad hoc rogue. Enter one of these options after you enter the **adhoc** keyword: • **alert**—Sets the ad hoc rogue access point to alert mode. If you choose this option, enter the MAC address for the *mac-addr* parameter. • **auto-contain**—Sets the automatically containing ad hoc rogue to auto-contain mode. • **contain**—Sets the containing ad hoc rogue access point to contain mode. If you choose this option, enter the MAC address for the *mac-addr* parameter and containment level for the *containment-level* parameter. The valid range for *containment-level* is from 1 to 4. • **external**—Sets the ad hoc rogue access point as **external**. If you choose this option, enter the MAC address for the *mac-addr* parameter. • **internal**—Sets the ad hoc rogue access point as **internal**. If you choose this option, enter the MAC address for the *mac-addr* parameter.
Step 3	**wireless wps rogue ap** {**friendly** *mac-addr* **state** [**external** | **internal**] | **malicious** *mac-addr* **state** [**alert** | **contain** *containment-level*]} **Example:**	Configures the rogue access points. Enter one of the following options after the **ap** keyword:

	Command or Action	Purpose
	`Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3`	• **friendly**—Configures the friendly rogue access points. If you choose this option, enter the MAC address for the *mac-addr* parameter. After that enter the **state** keyword followed by either of these options: **internal** or **external**. If you select an **internal** option, it indicates that you trust a foreign access point. If you select an **external** option, it indicates that you acknowledge the presence of a rogue access point. • **malicious**—Configures the malicious rogue access points. If you choose this option, enter the MAC address for the *mac-addr* parameter. After that enter the **state** keyword followed by either of these options: **alert** or **contain**. • **alert**—Sets the malicious rogue access point to **alert** mode. • **contain**—Sets the malicious rogue access point to **contain** mode. If you choose this option, enter the containment level for the *containment-level* parameter. The valid range is from 1 to 4.
Step 4	**wireless wps rogue client** {**contain** *mac-addr containment-level*} **Example:** `Device(config)# wireless wps rogue client contain 74a0.2f45.c520 2`	Configures the rogue clients. Enter the following option after you enter the **client** keyword: **contain**—Contains the rogue client. After you choose this option, enter the MAC address for the *mac-addr* parameter and the containment level for *containment-level* parameter. The valid range for *containment-level* is from 1 to 4.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Classification Rules (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 In the **Wireless Protection Policies** page, choose **Rogue AP Rules** tab.

Step 3 On the **Rogue AP Rules** page, click the name of the **Rule** or click **Add** to create a new one.

Step 4 In the **Add/Edit Rogue AP Rule** window that is displayed, enter the name of the rule in the **Rule Name** field.

Step 5 Choose the rule type from the following **Rule Type** drop-down list options:

- Friendly
- Malicious
- Unclassified
- Custom

Configuring Rogue Classification Rules (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue rule** *rule-name* **priority** *priority* **Example:** `Device(config)# wireless wps rogue rule rule_3 priority 3`	Creates or enables a rule. While creating a rule, you must enter the priority for the rule. **Note** After creating a rule, you can edit the rule and change the priority only for the rogue rules that are disabled. You cannot change the priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.

Step 3	**classify** {**friendly state** {**alert** | **external** | **internal**} | **malicious state** {**alert** | **contained** }}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# classify friendly`
		Specifies the classification that needs to be applied to the rogue access points matching this rule.
		• **friendly**—Configures the friendly rogue access points. After that enter the **state** keyword followed by either of these options: **alert**, **internal**, or **external**. If you select an **internal** option, it indicates that you trust a foreign access point. If you select an **external** option, it indicates that you acknowledge the presence of a rogue access point.

	Command or Action	Purpose
		• **malicious**—Configures the malicious rogue access points. After that enter the state keyword followed by either of these options: alert or contained. • **alert**—Sets the malicious rogue access point to alert mode. • **contained**—Sets the malicious rogue access point to contained mode.

Step 4	**condition** {**client-count** *value* | **duration** *duration_value* | **encryption** | **infrastructure** | **rssi** | **ssid** *ssid_name* | **wildcard-ssid**}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# condition client-count 5`
		Adds the following conditions to a rule, which the rogue access point must meet:
		• **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, 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 *value* parameter. The valid range is from 1 to 10 (inclusive), and the default value is 0.
		• **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 *duration_value* parameter. The valid range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
		• **encryption**—Requires that the advertised WLAN does not have encryption enabled. You can choose **any** for any type of encryption, **off** for no encryption, **wpa1** for WPA encryption, **wpa2** for WPA2 encryption, **wpa3-owe** for WPA3 OWE encryption, or **wpa3-sae** for WPA3 SAE encryption.
		• **infrastructure**—Requires the SSID to be known to the controller.
		• **rssi**—Requires the rogue access point to be detected with a minimum RSSI value. If the classification is Friendly, the condition requires the rogue access point

	Command or Action	Purpose
		to be detected with a maximum RSSI value. The valid range is from –95 to –50 dBm (inclusive). • **ssid**—Requires the rogue access point to have a specific SSID. You could specify up to 25 different SSIDs. You should specify an SSID that is not managed by the controller. If you choose this option, enter the SSID for the *ssid_name* parameter. The SSID is added to the configured SSID list you just created. • **wildcard-ssid**—Allows you to specify an expression that could match an SSID string. You can specify up to 25 of these SSIDs.

Step 5	**match** {**all** | **any**}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# match all`
		Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule for the rule to be matched and the rogue access point to adopt the classification type of the rule.

Step 6	**default**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# default`
		Sets a command to its default.

Step 7	**exit**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# exit`
	`Device(config)#`
		Exits the sub-mode.

Step 8	**shutdown**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# shutdown`
		Disables a particular rogue rule. In this example, the rule **rule_3** is disabled.

Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 10	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 11	**wireless wps rogue rule shutdown** **Example:** `Device(config)# wireless wps rogue rule shutdown`	Disables all the rogue rules.
Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Rogue Classification Rules

You can monitor the rogue classification rules using the following commands:

Table 2: Commands for Monitoring Rogue Classification Rules

Command	Purpose
show wireless wps rogue rule detailed	Displays detailed information of a classification rule.
show wireless wps rogue rule summary	Displays a summary of the classification rules.

Examples: Classifying Rogue Access Points

This example shows how to classify a rogue AP with MAC address 00:11:22:33:44:55 as malicious and mark it for being contained by 2 managed APs:

```
Device# configure terminal
Device(config)# wireless wps rogue ap malicious 0011.2233.4455 state contain 2
```

This example shows how to create a rule that can categorize a rogue AP that is using SSID **my-friendly-ssid**, and it is seen for at least for 1000 seconds as friendly internal:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition ssid my-friendly-ssid
Device(config-rule)# condition duration 1000
Device(config-rule)# match all
Device(config-rule)# classify friendly state internal
Device(config-rule)# no shutdown
```

This example shows how to apply a condition that a rogue access point must meet:

```
Device# configure terminal
```

```
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# no shutdown
Device(config-rule)# end
```

This example shows a condition to classify rogue devices with the controller SSIDs as malicious:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)#  classify malicious state alert
Device(config-rule)#  condition duration 30
Device(config-rule)#  condition infrastructure ssid
Device(config-rule)#  match all
Device(config-rule)#  no shutdown
Device(config-rule)# end
```