Classifying Rogue Access Points

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

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, or Unclassified.

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, and unclassified) in the Alert state only.

Note Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.

Note 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:

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.

Rule-Based Classification Type	Rogue States
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. • 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. • Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.
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

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

Table 2: Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

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.

Restrictions for Classifying Rogue Access Points

The following rules apply to this feature:

- 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 using rogue rules.
- There are traps that are sent for containment by rule and for 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.
- Once a rogue satisfies a higher priority rule and 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.
- When service set identifiers (SSIDs) are defined as part of a rogue rule, and details of the rogue rule are displayed using the **show wireless wps rogue rule detailed** command, the output differs in Cisco IOS XE Release 3.6E and prior releases and Cisco IOS XE Denali 16.1.1 and later releases.

  The following is sample output from the **show wireless wps rogue rule detailed** command in Cisco IOS XE Release 3.6E and prior releases:

```
Switch# show wireless wps rogue rule detailed test

Priority                                : 1
Rule Name                               : wpstest
State                                   : Disabled
Type                                    : Pending
Match Operation                         : Any
Hit Count                               : 0
Total Conditions                        : 1
Condition :
  type                                  : Ssid
  SSID Count                            : 2 ! SSID count differs.
```

```
  SSID 1                                  : ssid1
  SSID 2                                  : ssid2
```

The following is sample output from the **show wireless wps rogue rule detailed** command in Cisco IOS XE Denali 16.1.1 and later releases:

```
Switch# show wireless wps rogue rule detailed test

Priority                                  : 1
Rule Name                                 : wpstest
State                                     : Disabled
Type                                      : Pending
Match Operation                           : Any
Hit Count                                 : 0
Total Conditions                          : 1
Condition :
  type                                    : Ssid
  SSID Count                              : 2 ! SSID count differs.
  SSID                                    : ssid1
  SSID                                    : ssid2
```

How to Classify Rogue Access Points

Configuring Rogue Classification Rules (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wireless wps rogue rule** *rule-name* **priority** *priority*
3. **classify** {**friendly** | **malicious**}
4. **condition** {**client-count** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}
5. **match** {**all** | **any**}
6. **default**
7. **exit**
8. **shutdown**
9. **end**
10. **configure terminal**
11. **wireless wps rogue rule shutdown**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 2	**wireless wps rogue rule** *rule-name* **priority** *priority*
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)#`
		Creates or enables a rule. While creating a rule, you must enter priority for the rule.
		Note After creating the rule, if you are editing the rule, you can change the priority only for the rogue rules that are disabled. You cannot change priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.

Step 3	**classify** {**friendly** | **malicious**}
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# classify friendly`
		Classifies a rule.

Step 4	**condition** {**client-count** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# condition client-count 5`
		Specifies to add the following conditions to a rule that 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, 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.
		• **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.
		• **encryption**—Requires that the advertised WLAN does not have encryption enabled.
		• **infrastructure**—Requires the SSID to be known to the controller.
		• **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*. The valid range is –95 to –50 dBm (inclusive), and the default value is 0 dBm.

	Command or Action	Purpose
		• **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.

Step 5	**match** {**all** | **any**}
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# match all`
		Specifies 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.

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

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

Step 8	**shutdown**
	Example:
	`Switch(config)# wireless wps rogue rule rule_3 priority 3`
	`Switch(config-rule)# shutdown`
		Specifies to disable a particular rogue rule. For example, the rule **rule_3** is disabled.

Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 10	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 11	**wireless wps rogue rule shutdown** **Example:** `Switch(config)# wireless wps rogue rule shutdown`	Specifies to disable all the rogue rules.
Step 12	**end** **Example:**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
	`Switch(config)# end`	

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 If you ever want to delete a rule, hover your mouse 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**

d) 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**

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

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.

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.

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

e) To disable this particular rule, unselect the **Enable Rule** check box.

Note You cannot disable all the rogue rule in one shot from GUI but you can disable all the rogue rules from CLI using the **wireless wps rogue rule shutdown** command.

f) 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**. The user-configured SSIDs are added and listed.

Note To delete an SSID, highlight the SSID and click **Remove**. The SSID applied on a WLAN cannot be applied for the rogue rule.

- **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 –95 to –50 dBm (inclusive), and the default value is 0 dBm.
- **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 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 If you ever want to delete a condition from this rule, click **Remove** near the condition.

- **User configured SSID**—Requires that the rogue access point have a substring of the specific user-configured SSID. The controller searches the substring in the same occurrence pattern and returns a match if the substring is found in the whole string of an SSID.

g) Click **Apply**.

Step 4 If you want to change the priority in which rogue classification rules are applied, follow these steps:

a. 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.

b. Click on a specific 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.

Note You can change priority only for the disabled rule. You cannot change priority only for the enabled rule.

c. Click **Apply**.

Viewing and Classifying Rogue Devices (GUI)

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**

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

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.

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 See any adhoc 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 adhoc rogue, the number of radios that detected the adhoc rogue, and the current status of the adhoc rogue.

Step 9 Obtain more details about an adhoc 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 adhoc rogue, the dates and times when the rogue was first and last reported, and the current status of the rogue.

Step 10 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this adhoc 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 11 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 adhoc rogue: **1**, **2**, **3**, or **4**.

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

Step 12 Click **Apply**.

Step 13 Click **Save Configuration**.

Step 14 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.

Examples: Classifying Rogue Access Points

This example shows how to create rule that can organize and display rogue access points as Friendly:

```
Switch# configure terminal
Switch(config)# wireless wps rogue rule ap1 priority 1
Switch(config-rule)# classify friendly
Switch(config-rule)# end
```

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

```
Switch# configure terminal
Switch(config)# wireless wps rogue rule ap1 priority 1
Switch(config-rule)# condition client-count 5
Switch(config-rule)# condition duration 1000
Switch(config-rule)# end
```

Additional References for Classifying Rogue Access Points

Related Documents

Related Topic	Document Title
Security commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Classifying Rogue Access Points

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.