Managing Rogue Devices

Rogue Detection

Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to detect a large number of rogue APs and clients with high sensitivity, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect many rogue devices.
- Client card implementation might mitigate the effectiveness of containment. This normally happens when a client might quickly reconnect to the network after receiving a "de-association/de-authentication" frame, so it might still be able to pass some traffic. However, the browsing experience of the rogue client would be badly affected when it is contained.
- It is possible to classify and report rogue access points by using rogue states and user-defined classification rules that enable rogues to automatically move between states.
- Each controller limits the number of rogue containments to three and six per radio for access points in the monitor mode.
- When manual containment is performed using configuration, the rogue entry is retained even after the rogue entry expires.
- When a rogue entry expires, the managed access points are instructed to stop any active containment on it.
- To validate a Rogue Client against AAA, add the rogue client MAC to the AAA user-database with relevant delimiter, username, and password being the MAC address with relevant delimiter. The Access-Accept contains the Cisco-AV-pair with one of the following keywords:

  rogue-ap-state=*state*

Note Here, **state** can be of three types, namely: alert, threat, and contain.

For instance, **rogue-ap-state**=*threat*.

If Access-Accept has no AV-Pair rogue-ap-class or an invalid value of rogue-ap-class, such a rogue client state is set to either of the following:

- Contained, if the config is set to autocontain clients or untrusted AP.
- Threat

The Radius Access-Reject for rogue client AAA validation is ignored.

- When Validate Rogue Clients Against AAA is enabled, the controller requests the AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling Validate Rogue Clients Against AAA.

Restrictions on Rogue Detection

- Rogue containment is not supported on DFS channels.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
- If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points that are categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

Information About Rogue Containment (Protected Management Frames (PMF) Enabled)

From Cisco IOS XE Amsterdam, 17.3.1 onwards, rogue devices that are enabled with 802.11w Protected Management Frames (PMF) are not contained. Instead, the rogue device is marked as *Contained Pending*, and a WSA alarm is raised to inform about the Contained Pending event. Because the device containment is not performed, access point (AP) resources are not consumed unnecessarily.

Note This feature is supported only on the Wave 2 APs.

Run the **show wireless wps rogue ap detailed** command to verify the device containment, when PMF is enabled on a rogue device.

AP Impersonation Detection

The various methods to detect AP impersonation are:

- AP impersonation can be detected if a managed AP reports itself as Rogue. This method is always enabled and no configuration is required.
- AP impersonation detection is based on MFP.
- AP impersonation detection based on AP authentication.

Infrastructure MFP protects 802.11 session management functions by adding message integrity check (MIC) information elements, to the management frames sent by APs (and not those sent by clients), which are then validated by other APs in the network. If infrastructure MFP is enabled, the managed APs check if the MIC information elements are present and if MIC information elements are as expected. If either of these conditions is not fulfilled, the managed AP sends rogue AP reports with updated AP authentication failure counter.

The AP Authentication functionality allows you to detect AP impersonation. When you enable this functionality, the controller creates an AP domain secret and shares it with other APs in the same network. This allows the APs to authenticate each other.

An AP Authentication information element is attached to beacon and probe response frames. If the AP Authentication information element has an incorrect Signature field, or the timestamp is off, or if the AP Authentication information element is missing, then the AP that has detected such a condition increments the **AP authentication failure count** field. An impersonation alarm is raised after the **AP authentication failure count** field breaches its threshold. The rogue AP is classified as **Malicious** with state **Threat**.

Run the **show wireless wps rogue ap detail** command to see when the impersonation is detected due to authentication errors.

Note Ensure that the **ccx aironet-iesupport** command is run in all the WLAN procedures, else the BSSID will be detected as a rogue.

For AP impersonation detection, Network Time Protocol (NTP) must be enabled instead of CAPWAP based time, under the AP profile.

Configuring Rogue Detection (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click the **AP Join Profile Name** to edit the AP join profile properties.

Step 3 In the **Edit AP Join Profile** window, click the **Rogue AP** tab.

Step 4 Check the **Rogue Detection** check box to enable rogue detection.

Step 5 In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

Step 6 In the **Rogue Detection Transient Interval** field, enter the interval in seconds.

Step 7 In the **Rogue Detection Report Interval** field, enter the report interval value in seconds.

Step 8 In the **Rogue Detection Client Number Threshold** field, enter the threshold for rogue client detection.

Step 9 Check the **Auto Containment on FlexConnect Standalone** check box to enable auto containment.

Step 10 Click **Update & Apply to Device**.

Configuring Rogue Detection (CLI)

Procedure

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

	Command or Action	Purpose

Step 2	**ap profile** *profile-name* **rogue detection min-rssi** *rssi in dBm*
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection min-rssi -100`
		Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the device.
		Valid range for the rssi in dBm parameter is –128 dBm to -70 dBm, and the default value is -128 dBm.
		Note This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

Step 3	**ap profile** *profile-name* **rogue detection containment** {**auto-rate** | **flex-rate**}
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection containment flex-rate`
		Specifies the rogue containment options. The **auto-rate** option enables auto-rate for containment of rogues. The **flex-rate** option enables rogue containment of standalone FlexConnect APs.

Step 4	**ap profile** *profile-name* **rogue detection enable**
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection enable`
		Enables rogue detection on all APs.

Step 5	**ap profile** *profile-name* **rogue detection report-interval** *time in seconds*
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection report-interval 120`
		Configures rogue report interval for monitor mode Cisco APs.
		The valid range for reporting the interval in seconds is 10 seconds to 300 seconds.

Configuring RSSI Deviation Notification Threshold for Rogue APs (CLI)

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless wps rogue ap notify-rssi-deviation** **Example:** `Device(config)# wireless wps rogue ap notify-rssi-deviation`	Configures RSSI deviation notification threshold for Rogue APs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Management Frame Protection (GUI)

Procedure

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

Step 2 In the **Rogue Policy** tab, under the **MFP Configuration** section, check the **Global MFP State** check box and the **AP Impersonation Detection** check box to enable the global MFP state and the AP impersonation detection, respectively.

Step 3 In the **MFP Key Refresh Interval** field, specify the refresh interval in hours.

Step 4 Click **Apply**.

Configuring Management Frame Protection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps mfp** **Example:** `Device(config)# wireless wps mfp`	Configures a management frame protection.
Step 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**} **Example:** `Device(config)# wireless wps mfp ap-impersonation`	Configures ap impersonation detection (or) MFP key refresh interval in hours. key-refresh-interval—Refers to the MFP key refresh interval in hours. The valid range is from 1 to 24. Default value is 24.

	Command or Action	Purpose
	`Device(config)# wireless wps mfp key-refresh-interval`	
Step 4	**end** **Example:** `Device(config)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Enabling Access Point Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps ap-authentication** **Example:** `Device(config)# wireless wps ap-authentication`	Configures the wireless WPS AP authentication.
Step 3	**wireless wps ap-authentication threshold** *threshold* **Example:** `Device(config)# wireless wps ap-authentication threshold 100`	Configures AP neighbor authentication and sets the threshold for AP authentication failures.
Step 4	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Configures a WLAN.
Step 5	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet Information Elements on this WLAN.
Step 6	**end** **Example:** `Device# end`	Returns to privileged EXEC mode.

Verifying Management Frame Protection

To verify if the Management Frame Protection (MFP) feature is enabled or not, use the following command:

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

To view the MFP details, use the following command:

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

Verifying Rogue Events

To verify the rogue event history, run the **show wireless wps rogue ap detailed** command:

```
Device# show wireless wps rogue ap detailed d8b1.901c.3cfd

Rogue Event history

Timestamp                  #Times Class/State Event               Ctx
 RC
--------------------------- ------ ----------- ------------------- ------------------------
 ---
05/01/2020 08:37:03.55645  41616  Mal/CPend   FSM_GOTO            ContPending(NotContYet)
 0x0
05/01/2020 08:37:03.55427  28163  Mal/CPend   EXPIRE_TIMER_START  1200s
 0x0
05/01/2020 08:37:03.55380  28163  Mal/CPend   RECV_REPORT         38ed.18cf.83e0/1
 0x0
05/01/2020 08:36:54.659136 7356   Mal/CPend   NO_OP_UPDATE
 0x0
05/01/2020 08:36:33.347132 3185   Mal/CPend   CHANNEL_CHANGE      e4aa.5d44.fec0/2,36->40
 0x0
05/01/2020 08:25:19.573720 247    Mal/CPend   LRAD_EXPIRE         7c21.0e41.0700/0
 0x0
04/30/2020 07:55:37.977450 2      Mal/CPend   PMF_CONTAINMENT  ContPending(PMFDetected) 0x0
04/30/2020 07:55:37.977242 1      Unc/Alert    INIT_TIMER_DONE     0xab9800439e00024f
 0x0
04/30/2020 07:52:33.600332 1      Unk/Init     INIT_TIMER_START    180s
 0x0
04/30/2020 07:52:33.600326 1      Unk/Init     CREATE
 0x0
```

To verify the impersonations detected due to authentication errors, use the following command:

```
Device# show wireless wps rogue ap detailed

Rogue BSSID                          : 0062.ecf3.8d30
Last heard Rogue SSID                : rogueA
802.11w PMF required                 : No
```

```
Is Rogue an impersonator                : Yes
Is Rogue on Wired Network               : No
Classification                          : Malicious
Manually Contained                      : No
State                                   : Threat
First Time Rogue was Reported           : 01/07/2020 15:51:01
Last Time Rogue was Reported            : 01/08/2020 08:08:35

Number of clients                       : 0

Reported By
  AP Name : AP38ED.18CE.45E0
    MAC Address                         : 38ed.18cf.83e0
    Detecting slot ID                   : 0
    Radio Type                          : dot11g, dot11n - 2.4 GHz
    SSID                                : rogueA
    Channel                             : 6 (From DS)
    Channel Width                       : 20 MHz
    RSSI                                : -33 dBm
    SNR                                 : 52 dB
    ShortPreamble                       : Disabled
    Security Policy                     : WPA2/WPA/FT
    Last reported by this AP            : 01/08/2020 08:02:53
    Authentication Failure Count        : 237
```

Verifying Rogue Detection

This section describes the new command for rogue detection.

The following command can be used to verify rogue detection on the device.

Table 1: Verifying Adhoc Rogues Information

Command	Purpose
show wireless wps rogue adhoc detailed *mac_address*	Displays the detailed information for an Adhoc rogue.
show wireless wps rogue adhoc summary	Displays a list of all Adhoc rogues.

Table 2: Verifying Rogue AP Information

Command	Purpose
show wireless wps rogue ap clients *mac_address*	Displays the list of all rogue clients associated with a rogue.
show wireless wps rogue ap custom summary	Displays the custom rogue AP information.
show wireless wps rogue ap detailed *mac_address*	Displays the detailed information for a rogue AP.
show wireless wps rogue ap friendly summary	Displays the friendly rogue AP information.
show wireless wps rogue ap list *mac_address*	Displays the list of rogue APs detected by a given AP.
show wireless wps rogue ap malicious summary	Displays the malicious rogue AP information.

show wireless wps rogue ap summary	Displays a list of all Rogue APs.
show wireless wps rogue ap unclassified summary	Displays the unclassified rogue AP information.

Table 3: Verifying Rogue Auto-Containment Information

Command	Purpose
show wireless wps rogue auto-contain	Displays the rogue auto-containment information.

Table 4: Verifying Classification Rule Information

Command	Purpose
show wireless wps rogue rule detailed *rule_name*	Displays the detailed information for a classification rule.
show wireless wps rogue rule summary	Displays the list of all rogue rules.

Table 5: Verifying Rogue Statistics

Command	Purpose
show wireless wps rogue stats	Displays the rogue statistics.

Table 6: Verifying Rogue Client Information

Command	Purpose
show wireless wps rogue client detailed *mac_address*	Displays detailed information for a Rogue client.
show wireless wps rogue client summary	Displays a list of all the Rogue clients.

Table 7: Verifying Rogue Ignore List

Command	Purpose
show wireless wps rogue ignore-list	Displays the rogue ignore list.

Examples: Rogue Detection Configuration

This example shows how to configure the minimum RSSI that a detected rogue AP needs to be at, to have an entry created in the device:

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-rssi -100
```

```
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

This example shows how to configure the classification interval:

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

Configuring Rogue Policies (GUI)

Procedure

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

Step 2 In the **Rogue Policies** tab, use the **Rogue Detection Security Level** drop-down to select the security level.

Step 3 In the **Expiration timeout for Rogue APs (seconds)** field, enter the timeout value.

Step 4 Select the **Validate Rogue Clients against AAA** check box to validate rogue clients against AAA server.

Step 5 Select the **Validate Rogue APs against AAA** check box to validate rogue access points against AAA server.

Step 6 In the **Rogue Polling Interval (seconds)** field, enter the interval to poll the AAA server for rogue information.

Step 7 Select the **Detect and Report Adhoc Networks** check box to enable detection of rogue adhoc networks.

Step 8 In the **Rogue Detection Client Number Threshold** field, enter the threshold to generate SNMP trap.

Step 9 In the **Auto Contain** section, enter the following details.

Step 10 Use the **Auto Containment Level** drop-down to select the level.

Step 11 Select the **Auto Containment only for Monitor Mode APs** check box to limit the auto-containment only to monitor mode APs.

Step 12 Select the **Rogue on Wire** check box to limit the auto-containment only to rogue APs on wire.

Step 13 Select the **Using our SSID** check box to limit the auto-containment only to rogue APs using one of the SSID configured on the controller.

Step 14 Select the **Adhoc Rogue AP** check box to limit the auto-containment only to adhoc rogue APs.

Step 15 Click **Apply**.

Configuring Rogue Policies (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**Example:**	Configures the rogue detection security level.

	Command or Action	Purpose
	`Device(config)# wireless wps rogue security-level custom`	You can select **critical** for highly sensitive deployments, **custom** for customizable security level, **high** for medium-scale deployments, and **low** for small-scale deployments.
Step 3	**wireless wps rogue ap timeout** *number of seconds* **Example:** `Device(config)# wireless wps rogue ap timeout 250`	Configures the expiration time for rogue entries, in seconds. Valid range for the time in seconds 240 seconds to 3600 seconds.
Step 4	**Example:** `Device(config)# wireless wps rogue client aaa`	Configures the use of AAA or local database to detect valid MAC addresses.
Step 5	**Example:** `Device(config)# wireless wps rogue client mse`	Configures the use of MSE to detect valid MAC addresses.
Step 6	**wireless wps rogue client notify-min-rssi** *RSSI threshold* **Example:** `Device(config)# wireless wps rogue client notify-min-rssi -128`	Configures the minimum RSSI notification threshold for rogue clients. Valid range for the RSSI threshold in dB is -128 - dB to -70 dB.
Step 7	**wireless wps rogue client notify-min-deviation** *RSSI threshold* **Example:** `Device(config)# wireless wps rogue client notify-min-deviation 4`	Configures the RSSI deviation notification threshold for rogue clients. Valid range for the RSSI threshold in dB is 0 dB to 10 dB.
Step 8	**wireless wps rogue ap aaa polling-interval** *AP AAA Interval* **Example:** `Device(config)# wireless wps rogue ap aaa polling-interval 120`	Configures rogue AP AAA validation interval. The valid range for the AP AAA interval in seconds is 60 seconds to 86400 seconds.
Step 9	**wireless wps rogue adhoc** **Example:** `Device(config)# wireless wps rogue adhoc`	Enables detecting and reporting adhoc rogue (IBSS).
Step 10	**wireless wps rogue client client-threshold** *threshold* **Example:** `Device(config)# wireless wps rogue client client-threshold 100`	Configures the rogue client per a rogue AP SNMP trap threshold. The valid range for the threshold is 0 to 256.

	Command or Action	Purpose
Step 11	**wireless wps rogue ap init-timer** **Example:** `Device(config)# wireless wps rogue ap init-timer 180`	Configures the init timer for rogue APs. The default timer value is set to 180 seconds. **Note** When a rogue AP is detected, an init timer is started and the rules are applied when this timer expires. This allows for rogue AP information to stabilize before applying any rules. However, you can change the value of this timer using this command. For instance, the init timer can be set to 0, if the rules need to be applied as soon as a new rogue AP is detected.

Rogue Location Discovery Protocol (RLDP)

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature. RLDP has 100 % accuracy in rouge AP detection. It detects Open APs and NAT APs.

Following are some guidelines to manage RLDP:

- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.
- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller , RLDP does not work.
- RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels.
- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the controller . The workaround is to disable RLDP on mesh APs.
- If RLDP is enabled on non-monitor APs, client connectivity outages occur when RLDP is in process.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller 's IP addresses.
5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.

Note The RLDP packets are unable to reach the controller if filtering rules are placed between the controller 's network and the network where the rogue device is located.

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP), if RLDP is enabled, to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authentication. If RLDP uses FlexConnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configured), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the **wireless wps rogue ap rldp retries** configuration CLI.

You can initiate or trigger RLDP from controller in three ways:

1. Enter the RLDP initiation command manually from the controller CLI.

   wireless wps rogue ap mac-address *mac-address* **rldp initiate**

2. Schedule RLDP from the controller configuration CLI.

   wireless wps rogue ap rldp schedule

3. Auto RLDP. You can configure auto RLDP on controller either from controller CLI or GUI but keep in mind the following guidelines:

   - The auto RLDP option can be configured only when the rogue detection security level is set to custom.
   - Either auto RLDP or schedule of RLDP can be enabled at a time.

Restrictions for RLDP

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.
- During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.
- RLDP is supported only on Cisco IOS APs.

Configuring RLDP for Generating Alarms (GUI)

Procedure

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

Step 2 In the **RLDP** tab, use the **Rogue Location Discovery Protocol** drop-down to select one of the following options:

a) **Disable**: Disables RLDP on all the access points. **Disable** is the default option.
b) **All APs**: Enables RLDP on all APs.
c) **Monitor Mode APs**: Enables RLDP only on APs in the monitor mode.

Note The **Schedule RLDP** check box is enabled only if the **Disable** option is selected. The Schedule RLDP check box remains disabled when you select the **All APs** option or the **Monitor Mode APs** option.

Step 3 In the **Retry Count** field, specify the number of retries that should be attempted. The range allowed is between 1 and 5.

Step 4 Click **Apply**.

Configuring an RLDP for Generating Alarms (CLI)

Procedure

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

	Command or Action	Purpose

Step 2	**wireless wps rogue ap rldp alarm-only <monitor-ap-only>**
	Example:
	`Device(config)# wireless wps rogue ap rldp alarm-only`
	`Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only`
		Enables RLDP to generate alarms. In this method, the RLDP is always enabled.
		The **monitor-ap-only** keyword is optional.
		The command with just the **alarm-only** keyword enables RLDP without any restriction on the AP mode.
		The command with **alarm-only <monitor-ap-only>** keyword enables RLDP in monitor mode access points only.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Schedule for RLDP (GUI)

Procedure

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

Step 2 In the **RLDP** tab, choose the following options from the **Rogue Location Discovery Protocol** drop-down list:

- **Disable (default)**: Disables RLDP on all the access points.

Step 3 In the Retry Count field, specify the number of retries that should be attempted. Provide a valid range between 1 to 5.

Step 4 Check the **Schedule RLDP** check box and then specify the days, start time, and end time for the process to take place.

Step 5 Click **Apply**.

Configuring a Schedule for RLDP (CLI)

Procedure

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

	Command or Action	Purpose
Step 2	**wireless wps rogue ap rldp schedule day** *day* **start** *start-time* **end** *end-time* **Example:** `Device(config)# wireless wps rogue ap rldp schedule day Monday start 10:10:01 end 12:00:00`	Enables RLDP based on a scheduled day, start time, and end time. Here, *day* is the day when the RLDP scheduling can be done. The values are Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. *start-time* is the start time for scheduling RLDP for the day. You need to enter start time in **HH:MM:SS** format. *end-time* is the end time for scheduling RLDP for the day. You need to enter end time in **HH:MM:SS** format.
Step 3	**wireless wps rogue ap rldp schedule** **Example:** `Device(config)# wireless wps rogue ap rldp schedule`	Enables the schedule.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RLDP for Auto-Contain (GUI)

Procedure

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

Step 2 In the **Rogue Policies** tab, under the **Auto Contain** section, check the **Rogue on Wire** checkbox.

Step 3 Click **Apply**.

Configuring an RLDP for Auto-Contain (CLI)

Procedure

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

	Command or Action	Purpose

Step 2	**wireless wps rogue ap rldp auto-contain** [**monitor-ap-only**]
	Example:
	`Device(config)# wireless wps rogue ap rldp auto-contain`
	`Device(config)# wireless wps rogue ap rldp auto-contain monitor-ap-only`
		Enables RLDP to perform auto-contain. In this method, the RLDP is always enabled.
		The **monitor-ap-only** keyword is optional.
		The command with just the **auto-contain** keyword enables RLDP without any restriction on the AP mode.
		The command with **auto-contain <monitor-ap-only>** keyword enables RLDP in monitor mode access points only.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RLDP Retry Times on Rogue Access Points (GUI)

Procedure

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

Step 2 On the **Wireless Protection Policies** page, click the **RLDP** tab.

Step 3 Enter the RLDP retry attempt value for rogue access points in the **Retry Count** field.

The valid range is between 1 and 5.

Step 4 Save the configuration.

Configuring RLDP Retry Times on Rogue Access Points (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue ap rldp retries** *num-entries* **Example:** `Device(config)# wireless wps rogue ap rldp retries 2`	Enables RLDP retry times on rogue access points. Here, *num-entries* is the number of RLDP retry times for each of the rogue access points. The valid range is 1 to 5.

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Rogue AP RLDP

The following commands can be used to verify rogue AP RLDP:

Table 8: Verifying Rogue AP Information

Command	Purpose
show wireless wps rogue ap rldp detailed *mac_address*	Displays the RLDP details for a rogue AP.
show wireless wps rogue ap rldp in progress	Displays the list of in-progress RLDP.
show wireless wps rogue ap rldp summary	Displays the summary of RLDP scheduling information.

Rogue Detection Security Level

The rogue detection security level configuration allows you to set rogue detection parameters.

The available security levels are:

- Critical: Basic rogue detection for highly sensitive deployments.
- High: Basic rogue detection for medium-scale deployments.
- Low: Basic rogue detection for small-scale deployments.
- Custom: Default security-level, where all detection parameters are configurable.

Note When in Critical, High or Low, some rogue parameters are fixed and cannot be configured.

The following table shows parameter details for the three predefined levels:

Table 9: Rogue Detection: Predefined Levels

Parameter	Critical	High	Low
Cleanup Timer	3600	1200	240
AAA Validate Clients	Disabled	Disabled	Disabled
Adhoc Reporting	Enabled	Enabled	Enabled

Parameter	Critical	High	Low
Monitor-Mode Report Interval	10 seconds	30 seconds	60 seconds
Minimum RSSI	-128 dBm	-80 dBm	-80 dBm
Transient Interval	600 seconds	300 seconds	120 seconds
Auto Contain Works only on Monitor Mode APs.	Disabled	Disabled	Disabled
Auto Contain Level	1	1	1
Auto Contain Same-SSID	Disabled	Disabled	Disabled
Auto Contain Valid Clients on Rogue AP	Disabled	Disabled	Disabled
Auto Contain Adhoc	Disabled	Disabled	Disabled
Containment Auto-Rate	Enabled	Enabled	Enabled
Validate Clients with CMX	Enabled	Enabled	Enabled
Containment FlexConnect	Enabled	Enabled	Enabled
RLDP	Monitor-AP if RLDP scheduling is disabled.	Monitor-AP if RLDP scheduling is disabled	Disabled
Auto Contain RLDP	Disabled	Disabled	Disabled

Setting Rogue Detection Security-level

Follow the procedure given below to set the rogue detection security-level:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless wps rogue security-level custom** **Example:** `Device(config)# wireless wps rogue security-level custom`	Configures rogue detection security level as custom.

	Command or Action	Purpose
Step 3	**wireless wps rogue security-level low** **Example:** `Device(config)# wireless wps rogue security-level low`	Configures rogue detection security level for basic rogue detection setup for small-scale deployments.
Step 4	**wireless wps rogue security-level high** **Example:** `Device(config)# wireless wps rogue security-level high`	Configures rogue detection security level for rogue detection setup for medium-scale deployments.
Step 5	**wireless wps rogue security-level critical** **Example:** `Device(config)# wireless wps rogue security-level critical`	Configures rogue detection security level for rogue detection setup for highly sensitive deployments.

Wireless Service Assurance Rogue Events

Wireless Service Assurance (WSA) rogue events, supported in Release 16.12.x and later releases, consist of telemetry notifications for a subset of SNMP traps. WSA rogue events replicate the same information that is part of the corresponding SNMP trap.

For all the exported events, the following details are provided to the wireless service assurance (WSA) infrastructure:

- MAC address of the rogue AP
- Details of the managed AP and the radio that detected the rogue AP with strongest RSSI
- Event-specific data such as SSID, channel for potential honeypot event, and MAC address of the impersonating AP for impersonation event

The WSA rogue events feature can scale up to four times the maximum number of supported APs and half of the maximum number of supported clients.

The WSA rogue events feature is supported on Cisco Catalyst Center and other third-party infrastructure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**network-assurance enable** **Example:** `Device# network-assurance enable`	Enables wireless service assurance.

	Command or Action	Purpose
Step 3	**wireless wps rogue network-assurance enable** **Example:** `Device# wireless wps rogue network-assurance enable`	Enables wireless service assurance for rogue devices. This ensures that the WSA rogue events are sent to the event queue.

Monitoring Wireless Service Assurance Rogue Events

Procedure

- **show wireless wps rogue stats**

  Example:

```
Device# show wireless wps rogue stats

WSA Events
  Total WSA Events Triggered            : 9
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 2
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 3
    ROGUE_AP_IMPERSONATION_DETECTED     : 4
  Total WSA Events Enqueued             : 6
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 1
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 2
    ROGUE_AP_IMPERSONATION_DETECTED     : 3
```

  In this example, nine events have been triggered, but only six of them have been enqueued. This is because three events were triggered before the WSA rogue feature was enabled.

- **show wireless wps rogue stats internal**

  show wireless wps rogue ap detailed *rogue-ap-mac-addr*

  These commands show information related to WSA events into the event history.