



Managing Rogue Devices

- [Rogue Devices, on page 1](#)
- [Configuring Rogue Detection \(GUI\), on page 6](#)
- [Configuring Rogue Detection \(CLI\), on page 7](#)

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 containment frames are sent immediately after the authorization and associations are detected. The enhanced containment algorithm provides more effective containment of ad hoc clients.
- In a dense RF environment, where maximum rogue access points are suspected, the chances of detecting rogue access points by a local mode access point and FlexConnect mode access point in channel 157 or channel 161 are less when compared to other channels. To mitigate this problem, we recommend that you use dedicated monitor mode access points.
- The local and FlexConnect mode 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 perform high rogue detection, 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 implementations might mitigate the effectiveness of ad hoc containment.
- 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 per radio (or six per radio for access points in the monitor mode).
- 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. However, RLDP works when the managed access point is in the monitor mode on a DFS channel.
- 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.
- If the rogue is manually contained, the rogue entry is retained even after the rogue expires.
- If the rogue is contained by any other means, such as auto, rule, and AwIPS preventions, the rogue entry is deleted when it expires.
- The controller requests to 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**.
- In the 7.4 and earlier releases, if a rogue that was already classified by a rule was not reclassified. In the 7.5 release, this behavior is enhanced to allow reclassification of rogues based on the priority of the rogue rule. The priority is determined by using the rogue report that is received by the controller.
- The rogue detector AP fails to co-relate and contain the wired rogue AP on a 5Mhz channel because the MAC address of the rogue AP for WLAN, LAN, 11a radio and 11bg radio are configured with a difference of +/-1 of the rogue BSSID. In the 8.0 release, this behavior is enhanced by increasing the range of MAC address, that the rogue detector AP co-relates the wired ARP MAC and rogue BSSID, by +/-3.
- The rogue access points with open authentication can be detected on wire. The NAT wired or rogue wired detection is not supported in by WLC (both RLDP and rogue detector AP). The non-adjacent MAC address is supported by rogue detector mode of AP and not by RLDP.
- In a High Availability scenario, if the rogue detection security level is set to either High or Critical, the rogue timer on the standby controller starts only after the rogue detection pending stabilization time, which is 300 seconds. Therefore, the active configurations on the standby controller are reflected only after 300 seconds.

- After an AP is moved from rogue detection mode to any other mode or after an AP is moved from sniffer mode to local or monitor mode, the rogue detection functionality is not retained on the AP. To enable rogue detection functionality on the AP, you have to explicitly move the AP to the rogue detection mode.
- Some rogue devices exhibit RSSI value of -128 dBm although the minimum RSSI has been configured to a higher value. In some scenarios, APs show the RSSI value of 0 for some rogue devices. If the controller receives the RSSI value as 0, the controller invalidates the value and replaces it with -128 dBm so that rogue rules or policies are not applied to the rogue device.
- Even though rogue events are reported to Cisco DNA Center instantly, due to a big number of rogue events, the rogue sync occurs only on detection, on moving to contained state, and every half hour. The rogue sync does not occur for any other rogue event.



Note A rogue AP or client or adhoc containment configuration is not saved after the reload. You have to configure all the rogues again after the reload.



Note No separate command exists for controlling rogue client traps. However, you can enable or disable rogue client traps using the **config trapflags rogueap {enable | disable}** command, which is also used for rogue APs. In GUI configuration also, you should use the rogue AP flag under **Management > SNMP > TrapControl > Security > Rogue AP** to control rogue clients.

Restrictions on Rogue Detection

- Rogue containment is not supported on DFS channels.

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 rogue AP detection. It detects Open APs and NAT APs.



Note Use the **debug dot11 rldp enable** command in order to check if the Lightweight AP associates and receives a DHCP address from the rogue AP. This command also displays the UDP packet sent by the Lightweight AP to the controller .

A sample of a UDP (destination port 6352) packet sent by the Lightweight AP is shown here: 0020 0a 01 01 0d 0a 01(*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00x..... 0040 00 00 00 00 00 00 00 00 00 00

The first 5 bytes of the data contain the DHCP address given to the local mode AP by the rogue AP. The next 5 bytes are the IP address of the controller, followed by 6 bytes that represent the rogue AP MAC address. Then, there are 18 bytes of zeroes.

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.

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 not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS). If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue device.

Detecting Rogue Devices

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) and the rogue detector mode access point is connected to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authenticated and configured. 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-configuration), 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 **config rogue ap rldp retries** command.

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

1. Enter the RLDP initiation command manually from the controller CLI. The equivalent GUI option for initiating RLDP is not supported.
config rogue ap rldp initiate *mac-address*
2. Schedule RLDP from the controller CLI. The equivalent GUI option for scheduling RLDP is not supported.
config 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.

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.

This section contains the following subsections:

Configuring Rogue Detection (GUI)

- Step 1** Make sure that rogue detection is enabled on the corresponding access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, you can enable or disable rogue detection for individual access points by selecting or unselecting the **Rogue Detection** check box on the **All APs > Details for (Advanced)** page.
- Step 2** Choose **Security > Wireless Protection Policies > Rogue Policies > General**.
- The **Rogue Policies** page is displayed.
- Step 3** Choose one of the following options from the **Rogue Location Discovery Protocol** drop-down list:
- **Disable**—Disables RLDP on all the access points. This is the default value.
 - **All APs**—Enables RLDP on all the access points.
 - **Monitor Mode APs**—Enables RLDP only on the access points in the monitor mode.
- Step 4** In the **Expiration Timeout for Rogue AP and Rogue Client Entries** text box, enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds, and the default value is 1200 seconds.
- Note** If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.
- Step 5** To use the AAA server or local database to validate if rogue clients are valid clients, select the **Validate Rogue Clients Against AAA** check box. By default, the check box is unselected.
- Note** To validate a rogue client against AAA, the format of the Cisco AVP pair is mandatory. The free RADIUS format is:
- e09d3166fb2c Cleartext-Password := "e09d3166fb2c"
 - Cisco-AVPair := "rogue-ap-state=threat"
- Step 6** If necessary, select the **Detect and Report Ad-Hoc Networks** check box to enable ad hoc rogue detection and reporting. By default, the check box is selected.
- Step 7** In the **Rogue Detection Report Interval** text box, enter the time interval, in seconds, at which APs send the rogue detection report to the Cisco WLC. The valid range is 10 to 300 seconds, and the default value is 10 seconds.
- Note** The minimum value of 10 seconds is applicable only to APs in monitor mode. For the APs in Local mode, the minimum interval value that you can set is 30 seconds.
- Step 8** In the **Rogue Detection Minimum RSSI** text box, enter the minimum Received Signal Strength Indicator (RSSI) value for APs to detect the rogue and for a rogue entry to be created in the controller. The valid range is -128 dBm to -0 dBm, and the default value is 0 dBm.
- Note** This feature is applicable to all the AP modes. There can be many rogues with 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 detect rogues.

Step 9

In the **Rogue Detection Transient Interval** text box, enter the time interval at which a rogue should be scanned for by the AP after the first time the rogue is scanned. After the rogue is scanned for consistently, updates are sent periodically to the controller. Thus, the APs filter the transient rogues, which are active for a short period and are then silent. The valid range is between 120 to 1800 seconds, and the default value is 0.

The rogue detection transient interval is applicable to the monitor mode APs only.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues is avoided.

Step 10

If you want the controller to automatically contain certain rogue devices, enable the following parameters. By default, these parameters are in disabled state.

Caution When you select any of the Auto Contain parameters and click **Apply**, the following message is displayed: "Using this feature may have legal consequences. Do you want to continue?" The 2.4-GHz 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.

- **Auto Containment Level**—Set the auto containment level. By default, the auto containment level is set to 1.
- **Auto Containment only for Monitor mode APs**—Configure the monitor mode access points for auto-containment.
- **Rogue on Wire**—Configure the auto containment of rogues that are detected on the wired network.
- **Using Our SSID**—Configure the auto containment of rogues that are advertising your network's SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
- **Valid Client on Rogue AP**—Configure the auto containment of a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
- **AdHoc Rogue AP**—Configure the auto containment of ad hoc networks detected by the controller. If you leave this parameter unselected, the controller only generates an alarm when such a network is detected.

Step 11

Click **Apply**.

Step 12

Click **Save Configuration**.

Configuring Rogue Detection (CLI)

Step 1

Ensure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all the access points that are associated with the controller. You can enable or disable rogue detection for individual access points by entering this command:

config rogue detection {enable | disable} cisco-ap command.

Note To see the current rogue detection configuration for a specific access point, enter the **show ap config general Cisco_AP** command.

Note 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 a large number of rogue devices.

Step 2 Enable, disable, or initiate RLDP by entering these commands:

- **config rogue ap rldp enable alarm-only**—Enables RLDP on all the access points.
- **config rogue ap rldp enable alarm-only monitor_ap_only**—Enables RLDP only on the access points in the monitor mode.
- **config rogue ap rldp initiate *rogue_mac_address***—Initiates RLDP on a specific rogue access point.
- **config rogue ap rldp disable**—Disables RLDP on all the access points.
- **config rogue ap rldp retries**—Specifies the number of times RLDP to be tried per rogue access point. The range is from 1 to 5 and default is 1.

Step 3 Specify the number of seconds after which the rogue access point and client entries expire and are removed from the list by entering this command:

config rogue ap timeout *seconds*

The valid range for the *seconds* parameter is 240 to 3600 seconds (inclusive). The default value is 1200 seconds.

Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for a classification type.

Step 4 Enable or disable ad hoc rogue detection and reporting by entering this command:

config rogue adhoc {enable | disable}

Step 5 Enable or disable the AAA server or local database to validate if rogue clients are valid clients by entering this command:

config rogue client aaa {enable | disable}

Step 6 Specify the time interval, in seconds, at which APs should send the rogue detection report to the controller by entering this command:

config rogue detection monitor-ap report-interval *time in sec*

The valid range for the *time in sec* parameter is 10 seconds to 300 seconds. The default value is 10 seconds.

Note This feature is applicable only to the monitor mode APs.

Step 7 Specify the minimum RSSI value that rogues should have for APs to detect them and for the rogue entries to be created in the controller by entering this command:

config rogue detection min-rssi *rssi in dBm*

The valid range for the *rssi in dBm* parameter is -128 dBm to 0 dBm. The default value is 0 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 8 Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned for by entering this command:

config rogue detection monitor-ap transient-rogue-interval *time in sec*

The valid range for the *time in sec* parameter is 120 seconds to 1800 seconds. The default value is 0.

Note This feature is applicable only to the monitor mode APs.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter rogues based on their transient interval values.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

Step 9

If you want the controller to automatically contain certain rogue devices, enter these commands.

Caution When you enter any of these commands, the following message is displayed: Using this feature may have legal consequences. Do you want to continue? The 2.4-GHz 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.

- **config rogue ap rldp enable auto-contain**—Automatically contains the rogues that are detected on the wired network.
- **config rogue ap ssid auto-contain**—Automatically contains the rogues that are advertising your network's SSID.

Note If you want the controller to only generate an alarm when such a rogue is detected, enter the **config rogue ap ssid alarm** command.

- **config rogue ap valid-client auto-contain**—Automatically contains a rogue access point to which trusted clients are associated.

Note If you want the controller to only generate an alarm when such a rogue is detected, enter the **config rogue ap valid-client alarm** command.

- **config rogue adhoc auto-contain**—Automatically contains ad hoc networks detected by the controller.

Note If you want the controller to only generate an alarm when such a network is detected, enter the **config rogue adhoc alert** command.

- **config rogue auto-contain level level monitor_mode_ap_only**—Sets the auto containment level for the monitor mode access points. The default value is 1.

Step 10

Configure ad hoc rogue classification by entering these commands:

- **config rogue adhoc classify friendly state {internal | external} mac-addr**
- **config rogue adhoc classify malicious state {alert | contain} mac-addr**
- **config rogue adhoc classify unclassified state {alert | contain} mac-addr**

The following is a brief description of the parameters:

- **internal**—Trusts a foreign ad hoc rogue.
- **external**—Acknowledges the presence of an ad hoc rogue.
- **alert**—Generates a trap when an ad hoc rogue is detected.

- **contain**—Starts containing a rogue ad hoc.

Step 11 Configure RLDP scheduling by entering this command:

config rogue ap rldp schedule { add | delete | disable | enable }

- **add**—Enables you to schedule RLDP on a particular day of the week. You must enter the day of the week (for example, **mon**, **tue**, **wed**, and so on) on which you want to schedule RLDP and the start time and end time in HH:MM:SS format. For example: **config rogue ap rldp schedule add mon 22:00:00 23:00:00**.
- **delete**—Enables you to delete the RLDP schedule. You must enter the number of days.
- **disable**—Configure to disable RLDP scheduling.
- **enable**—Configure to enable RLDP scheduling.

Note When you configure RLDP scheduling, it is assumed that the scheduling will occur in the future, that is, after the configuration is saved.

Step 12 Save your changes by entering this command:

save config
