Managing Rogue Devices

- Rogue devices and detection, on page 1
- Rogue Location Discovery Protocol (RLDP), on page 16
- Wireless Service Assurance (WSA) rogue events, on page 23
- Rogue PMF containment, on page 25

Rogue devices and detection

A rogue device is any unauthorized network device.

A rogue device can:

- disrupt wireless LAN operations by hijacking legitimate clients,
- facilitate attacks such as plaintext, denial-of-service, and man-in-the-middle attacks on wireless networks, and
- pose serious security risks by allowing unauthorized access, interception, and breaches inside the corporate firewall.

Risks and impact on network security

Rogue access points are a common form of rogue devices. Hackers can use rogue access points to capture sensitive information such as usernames and passwords. By transmitting a series of Clear to Send (CTS) frames, a rogue access point can mimic a legitimate access point. This action instructs a specific client to transmit while forcing other clients to wait, which prevents legitimate clients from accessing network resources.

Ban rogue access points from the air space to protect users and maintain network integrity.

Because rogue access points are inexpensive and available, staff may connect unauthorized access points to existing LANs. This can create ad hoc wireless networks without approval from IT departments.

These rogue access points can create serious security risks because they may connect inside the corporate firewall. If security settings are disabled on these devices, unauthorized users can intercept network traffic and hijack client sessions. When wireless users connect to rogue access points within the enterprise network, the risk of a security breach increases.

Rogue client status change

The controller marks the rogue client as a threat if a wireless client in the RUN state has the same MAC address.

Restrictions on rogue detection

- Rogue containment is not supported on DFS channels.

Rogue AP containment and attack signatures

A rogue AP containment and attack signature is a set of wireless network security mechanisms that

- detect and contain unauthorized rogue wireless APs,
- use automated or manual methods to select the best access point for containment actions, and
- define specific attack signatures, including behaviors of rogue AP impersonators and new threats based on beacon frames.

Containment operation

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point (AP) for containment and pushes the containment information to it. Each AP stores its list of containments per radio.

For auto-containment, you can configure the controller to use only APs in monitor mode. Containment operations occur through two primary methods:

- The container AP periodically reviews its containment list and sends unicast containment frames. For rogue AP containment, these are sent only if a rogue client is associated.
- When the system detects contained rogue activity, the AP immediately transmits containment frames.

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

Attack signature examples

These signatures help identify sophisticated attack methods targeting wireless networks and support more effective containment and remediation strategies.

-
-

Cisco Prime Infrastructure interaction and rogue detection

A rogue access point classification rule is a network security mechanism that

- applies predefined criteria to evaluate and categorize access points detected on the network,
- determines the current state of each detected access point (such as Friendly, Malicious, Internal, or External), and

- defines when and how the controller communicates rogue events to Cisco Prime Infrastructure.

How Cisco Prime Infrastructure interacts with the controller for rogue detection

Cisco Prime Infrastructure interacts with controllers to detect and manage rogue access points according to the classification rules set on the controllers. The rule-based classification enables Cisco Prime Infrastructure to receive detailed trap notifications when rogue access point events occur. Key interactions and behaviors include:

- The controller uses its configured classification rules to determine the state of each rogue access point.
- When certain rogue access point events occur (such as state changes or rogue entry removal), the controller sends traps (notifications) to Cisco Prime Infrastructure.
- Trap notifications depend on both the rogue state and the event type, including these cases:
  - If an unknown access point moves to the Friendly state for the first time and the rogue state is Alert, a trap is sent.
  - No trap is sent if the rogue state is Internal or External.
  - If a rogue entry is removed after timeout, the controller sends a trap for entries classified as Malicious (Alert, Threat) or Unclassified (Alert).
  - The controller does not remove rogue entries with the following states: Contained, Contained Pending, Internal, and External.
- When a new, unknown access point is detected and moves to the Friendly state under Alert, Cisco Prime Infrastructure receives a notification.
- If a rogue entry with a Malicious or Unclassified (Alert) state is removed after a timeout, a trap is generated and sent to Cisco Prime Infrastructure.
- Rogue entries in Contained, Contained Pending, Internal, and External states are retained by the controller and not removed automatically, so no removal trap is sent for them.

AP impersonation detection

An AP impersonation is a wireless security attack that

- allows a rogue device to masquerade as a legitimate AP
- enables attackers to intercept and manipulate wireless communication between client devices and the network, and
- threatens the confidentiality, integrity, and security of wireless network traffic.

Detection methods

The various methods to detect AP impersonation are:

- You can detect AP impersonation if a managed AP reports itself as Rogue. This method is always enabled and does not require configuration.

- AP impersonation detection uses Management Frame Protection (MFP).

Management Frame Protection (MFP)-based detection

Infrastructure MFP protects 802.11 session management by adding Message Integrity Check (MIC) elements to management frames sent by APs (not clients). Other APs in the network then validate these management frames.

- If infrastructure MFP is enabled, managed APs check whether the MIC elements are present and valid.
- If either condition is not met, the managed AP sends rogue AP reports with an updated AP authentication failure counter field.

AP authentication-based detection

When you enable AP authentication, the controller creates an AP domain secret and shares it with all APs in the same network. This process enables 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, an off timestamp, or the information element is missing, the AP that detects the condition increments the **AP authentication failure count** field.
- An impersonation alarm is raised after the **AP authentication failure count** field exceeds its threshold.
- The rogue AP is classified as **Malicious** with the state **Threat**.

Run the **show wireless wps rogue ap detail** command to see when AP impersonation is detected as a result of authentication errors.

Configuration notes

- Run the **CCX Aironet-IESupport** command in all WLAN procedures to prevent the BSSID from being detected as a rogue.
- For AP impersonation detection, Network Time Protocol (NTP) must be enabled under the AP profile. CAPWAP-based time is not sufficient.

Rogue detection security level

A rogue detection security level is a configuration preset that

- determines the sensitivity and scope of rogue wireless device detection
- restricts or allows configuration of specific detection parameters, and
- provides predefined or customizable options for different deployment needs.

- Rogue detection: identifies unauthorized or unknown wireless devices in a network environment.
- Security level: specifies a preset combination of parameters for rogue detection.

The system provides four rogue detection security levels.

- Critical: Provides basic rogue detection for highly sensitive deployments. Fixed configuration parameters ensure maximum security and consistency.
- High: Provides basic rogue detection suitable for medium-scale environments. Several parameters are fixed to balance protection and operational simplicity.
- Low: Provides basic rogue detection suitable for small-scale deployments. Fixed parameters provide easy management.
- Custom: The default security level. You can fully configure all rogue detection parameters to suit any environment.

Note To modify all parameters, select the Custom security level. The critical, high, and low levels have fixed settings.

Table 1: Rogue Detection: Predefined Levels

Parameter	Critical	High	Low
Cleanup Timer	3600 seconds (1 hour)	1200 seconds (20 minutes)	240 seconds (4 minutes)
AAA Validate Clients	Disabled	Disabled	Disabled
Adhoc Reporting	Enabled	Enabled	Enabled
Monitor Mode Report Interval	10 seconds (0:10)	30 seconds (0:30)	60 seconds (1:00)
Minimum RSSI	-128 dBm	-80 dBm	-80 dBm
Transient Interval	600 seconds (10 minutes)	300 seconds (5 minutes)	120 seconds (2 minutes)
Auto Contain **This feature 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

Parameter	Critical	High	Low
Validate Clients with Cisco Connected Mobile Experiences (CMX)	Enabled	Enabled	Enabled
Containment FlexConnect	Enabled	Enabled	Enabled
Rogue Location Discovery Protocol (RLDP)	The device functions as a monitor mode AP if RLDP scheduling is disabled.	The device functions as a monitor mode AP if RLDP scheduling is disabled.	Disabled
Auto Contain RLDP	Disabled	Disabled	Disabled

You can configure all these parameters in the Custom security level.

- A hospital implements the Critical security level to maintain rigorous control over rogue detection with fixed settings.
- A small business chooses the Low security level for straightforward rogue detection with minimal configuration.
- An enterprise IT team uses the Custom security level to tailor all rogue detection parameters to their unique requirements.

Set rogue detection security level (CLI)

Set the wireless rogue detection security level for your network deployment.

Before you begin

Use these steps to set the rogue detection security level.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the rogue detection security level to custom.

Example:

```
Device(config)# wireless wps rogue security-level custom
```

Step 3 Configure the rogue detection security level for small-scale deployments.

Example:

```
Device(config)# wireless wps rogue security-level low
```

Step 4 Configure the rogue detection security level for medium-scale deployments.

Example:

```
Device(config)# wireless wps rogue security-level high
```

Step 5 Configure the rogue detection security level for highly sensitive deployments.

Example:

```
Device(config)# wireless wps rogue security-level critical
```

The device applies the selected rogue detection security level to enhance wireless intrusion protection for your deployment.

Configuring rogue detection (GUI)

Enable rogue access point detection and set parameters in the GUI.

Use rogue detection to identify and manage unauthorized or suspicious APs in your network. Complete this task when you establish or update your wireless security policies.

Before you begin

Use these steps to configure rogue detection using the GUI:

Procedure

Step 1 Choose Configuration, then Tags and Profiles, then AP Join.
Step 2 Click the **AP Join Profile Name** to edit the access point (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 (minutes).
Step 7 In the **Rogue Detection Report Interval** field, enter the report interval value in seconds (minutes).
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 and Apply to Device**.

The rogue-detection feature is activated with your configured parameters. This helps you identify and contain unauthorized access points (APs) in the network.

Configure rogue detection (CLI)

You enable and customize rogue detection on Cisco wireless access points using specific CLI commands.

Use these commands to detect and contain unauthorized access points (APs) and improve wireless network security.

Before you begin

Use these steps to configure rogue detection.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Set how often APs consistently scan for rogues after the initial detection.

Example:

```
Device(config)# ap profile profile-name
Device(config)# rogue detection min-transient-time time in seconds
```

You can enter a time between two minutes (120 seconds) and thirty minutes (1,800 seconds). The default is zero.

Note
You can use this feature with any AP mode.

Use the transient interval to control how often APs scan for rogues. APs can also filter rogues based on this value.

This feature provides these advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.

The system avoids unnecessary memory allocation for transient rogues.

Step 3 Choose a rogue containment option.

Example:

```
Device(config)# ap profile profile-name
Device(config)# rogue detection containment flex-rate
```

The **auto-rate** option contains rogues automatically. The **flex-rate** option contains standalone FlexConnect APs.

Step 4 Turn on rogue detection for all APs.

Example:

```
Device(config)# ap profile profile-name
```

Step 5 Set the interval for rogue reports on monitor mode APs.

Example:

```
Device(config)# ap profile profile-name
Device(config)# rogue detection report-interval time in seconds
```

The valid range for the reporting interval is 10 to 300 seconds.

If the controller detects thousands of rogue APs, the PUBD (Public Utility Bulletin Daemon) process may cause sustained high CPU usage. Increase the Rogue Detection Report Interval to a value higher than the default of 10 to resolve this issue.

Rogue detection is active using your specified parameters on the AP profile. This improves security by monitoring and containing unauthorized devices.

Configure RSSI deviation notification threshold for rogue APs (CLI)

Set the signal strength deviation threshold to trigger notifications for rogue access points on your network.

Before you begin

Use these steps to configure the RSSI deviation notification threshold for rogue APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the RSSI deviation notification threshold for rogue APs.

Example:

```
Device(config)# wireless wps rogue ap notify-rssi-deviation
```

Step 3 Return the system to privileged EXEC mode.

Example:

```
Device(config)# end
```

You can press Ctrl and Z to exit global configuration mode.

The system notifies you when a rogue APs RSSI deviation exceeds the set threshold.

Configure management frame protection (GUI)

Enable and configure management frame protection (MFP) to secure wireless network communications against attacks such as rogue AP impersonation.

Before you begin

Use these steps to configure management frame protection.

Procedure

Step 1 Choose **Configuration**, then **Security**, then **Wireless Protection Policies**.

Step 2 In the **Rogue Policy** tab, under the **MFP Configuration** section, check the **Global MFP State** check box to enable the global MFP state.

Step 3 Check the **AP Impersonation Detection** check box to enable AP impersonation detection.

Step 4 In the **MFP Key Refresh Interval** field, specify the refresh interval in hours.

Step 5 Click **Apply**.

Management frame protection is enabled and configured, providing enhanced security for wireless management frames.

Configure Management Frame Protection (CLI)

Configure Management Frame Protection (MFP) on a device using the command-line interface (CLI).

Before you begin

Use these steps to configure management frame protection.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure management frame protection.

Example:

```
Device(config)# wireless wps mfp
```

Step 3 Configure AP impersonation detection or set the MFP key refresh interval in hours.

Example:

```
Device(config)# wireless wps mfp ap-impersonation
Device(config)# wireless wps mfp key-refresh-interval
```

key-refresh-interval: Set sthe MFP key refresh interval in hours.

The valid range is one to 24 hours. The default value is 24 hours.

Step 4 Save the configuration, exit configuration mode, and return to privileged **EXEC** mode.

Example:

```
Device(config)# end
```

The device protects wireless management traffic according to the configured settings.

Verify management frame protection

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

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

Verify 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 this 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
```

Verify rogue detection

This section describes the new command for rogue detection.

These commands can be used to verify rogue detection on the device.

Table 2: 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 3: 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 4: Verifying Rogue Auto-Containment Information

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

Table 5: 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 6: Verifying Rogue Statistics

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

Table 7: 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 8: Verifying Rogue Ignore List

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

Examples: rogue detection onfiguration

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# wireless wps rogue ap notify-min-rssi 100
```

This example shows how to configure the classification interval:

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

Configure rogue policies (GUI)

Use this task to define and customize rogue wireless protection policies. These policies help the system detect and respond to unauthorized wireless activity.

Before you begin

Perform the steps in this section to configure rogue policies.

Procedure

Step 1 Choose **Configuration**, then **Security**, then **Wireless Protection Policies**.

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

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

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

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

Step 6 In the **Rogue Polling Interval** field, enter the interval in seconds at which the system polls the AAA server for rogue information.

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

Step 8 In the **Rogue Detection Client Number Threshold** field, enter the number of clients at which the system generates an SNMP trap.

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

Step 10 Select the containment level from the **Auto Containment Level** drop-down.

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

Step 12 Select the **Using our SSID** check box to limit automatic containment to rogue APs that use an SSID that is configured on the controller.

Step 13 Select the **Adhoc Rogue AP** check box to enable automatic containment for ad hoc rogue APs.

Step 14 Click **Apply**.

The system updates rogue policies to enhance detection and containment of unauthorized wireless threats according to your configuration.

Configure rogue policies (CLI)

Establish rogue policies to enhance network security by managing rogue access points and clients.

This configuration is essential in environments where rogue devices may pose a security threat to the network.

Before you begin

Ensure you have access to the device's global configuration mode.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 2 Configure the expiration time for rogue entries.

Example:

```
Device(config)# wireless wps rogue ap timeout timout-in-seconds
```

Valid range for the time in seconds is 240 seconds to 3600 seconds.

Step 3 Configure the minimum RSSI notification threshold for rogue clients.

Example:

```
Device(config)# wireless wps rogue client notify-min-rssi RSSI-threshold
```

Valid range for the RSSI threshold in dB is -128 dB to -70 dB.

Step 4 Configure the RSSI deviation notification threshold for rogue clients.

Example:

```
Device(config)# wireless wps rogue client notify-min-deviation RSSI-threshold-value
```

Valid range for the RSSI threshold in dB is 0 dB to 10 dB.

Step 5 Configure rogue AP AAA validation interval.

Example:

```
Device(config)# wireless wps rogue ap aaa polling-interval AP-AAA-interval-value
```

The valid range for the AP AAA interval in seconds is 60 seconds to 86400 seconds.

Step 6 Enable detecting and reporting adhoc rogue (IBSS).

Example:

```
Device(config)# wireless wps rogue adhoc
```

Enables detecting and reporting adhoc rogue (IBSS).

Step 7 Configure the rogue client per a rogue AP SNMP trap threshold.

Example:

```
Device(config)# wireless wps rogue client client-threshold threshold-value
```

The valid range for the threshold is 0 to 256.

The rogue policies are now configured, enhancing the network's security against rogue devices.

Rogue Location Discovery Protocol (RLDP)

A rogue location discovery protocol is a network security protocol that

- detects rogue access points by actively investigating their presence
- enables authorized access points to associate with rogue devices and communicate findings to network controllers, and
- enhances wireless network protection by identifying open and NATed rogue APs.

How RLDP Works

Rogue Location Discovery Protocol (RLDP) operates when a rogue access point uses open authentication (lacks password protection). RLDP instructs an authorized AP to temporarily disconnect its clients, switch to the rogue channel, and attempt to join the rogue AP as a client.

Once associated, the AP requests an IP address from the rogue AP and sends a UDP packet (port 6352) containing connection details to the controller. If the controller receives this packet, it triggers an alarm to alert administrators about the presence of a rogue AP on the wired network.

RLDP offers high accuracy in rogue AP detection, especially for open and NAT-enabled rogue devices. However, RLDP packets may be blocked if filtering rules exist between the controller network and the rogue network.

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

Guidelines to manage RLDP

- Use Rogue Location Discovery Protocol (RLDP) to detect rogue access points configured for open-authentication.
- Use RLDP to detect rogue access points that broadcast a Basic Service Set Identifier (BSSID). In this case, the access point broadcasts its Service Set Identifier in beacons.
- You can use RLDP to detect only rogue access points on the same network. RLDP does not function if an access list in the network blocks RLDP traffic from the rogue access point to the embedded wireless controller.
- You cannot use RLDP on 5-GHz (5-gigahertz) Dynamic Frequency Selection (DFS) channels.
- If you enable RLDP on mesh APs and they perform RLDP tasks, the mesh APs will be dissociated from the embedded wireless controller. To prevent this, disable RLDP on mesh APs.

- If you enable RLDP on non-monitor APs, clients may experience connectivity outages while RLDP runs.

Best practices for RLDP initiation commands and configuration

Your embedded wireless controller collects information about rogue access points and clients from nearby APs.

When your embedded wireless controller discovers a rogue AP, it uses Rogue Location Discovery Protocol (RLDP) (if enabled and the rogue detector mode AP is connected) to determine whether the rogue is attached to your network.

The Embedded Wireless Controller initiates RLDP on rogue devices that use open .

If RLDP uses FlexConnect or local mode access points, clients disconnect briefly and reconnect after RLDP completes.

When a rogue access point appears , RLDP starts automatically.

You can configure the embedded wireless controller to use RLDP on all access points or only on those set to monitor (listen-only) mode.

Monitoring-mode access points let you detect rogue access points automatically in crowded RF spaces without creating interference or affecting data access point functionality.

If both monitor and local (data) access points are nearby, the embedded wireless controller selects the monitor access point for RLDP.

If RLDP determines that the rogue is on your network, choose to contain the rogue manually or automatically.

RLDP checks whether rogue access points that use open authentication are present on the wire only once by default.

You can configure the number of retries using the .

Use these best practices to initiate and configure RLDP on the embedded wireless controller.

1. Initiate RLDP manually from the controller CLI.
2. Schedule RLDP from the controller CLI.
3. Configure auto RLDP on your controller from the CLI or GUI after setting the correct security level.

Additional guidance

- You can configure auto RLDP only when the rogue detection security level is set to custom.
- Enable either auto RLDP or scheduled RLDP, but not both at the same time.

Restrictions for RLDP

- You can use Rogue Location Discovery Protocol (RLDP) only with open rogue APs that broadcast their SSID with authentication and encryption disabled.
- Ensure the managed AP acting as a client can obtain an IP address using DHCP on the rogue network.
- You can use manual RLDP to run an RLDP trace on a rogue device multiple times.

- During the RLDP process, the AP cannot serve clients, which reduces performance and connectivity for local mode APs. To prevent this issue, enable RLDP only on Monitor Mode APs.
- RLDP does not connect to rogue APs operating in 5GHz DFS channels.
- You can use RLDP only on Cisco IOS APs.

Rogue Location Discovery Protocol (RLDP) process

Summary

Use Rogue Location Discovery Protocol (RLDP) to help Unified APs identify and verify whether a rogue device is connected to the network.

RLDP associates with the rogue device, obtains network parameters, and reports the results to controllers.

Workflow

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 is obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the embedded wireless controller's IP addresses.
5. If the embedded wireless controller receives even one RLDP packet from the client, the system marks the rogue as on-wire.

Result

You can use RLDP to automatically detect and confirm rogue devices connected to your enterprise wired network.

RLDP supports rapid security response.

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**.

Configure RLDP to generate alarms (CLI)

Enable the Rogue Location Discovery Protocol (RLDP) to generate alarms using CLI commands.

Before you begin

Follow these steps to configure RLDP to create alarms.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable RLDP to generate alarms.

Example:

```
Device(config)# wireless wps rogue ap rldp alarm-only
```

```
Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only
```

In this method, RLDP is always enabled.

The **monitor-ap-only** keyword is optional.

The command with only the **alarm-only** keyword enables RLDP without restrictions on AP mode.

The command with the "alarm-only monitor-ap-only" keyword enables RLDP only in monitor-mode access points.

Step 3 Go to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can press **Ctrl-Z** to exit global configuration mode.

RLDP generates alarms when the system detects rogue access points, according to your configuration.

Configure a schedule for RLDP (GUI)

Define and apply a scheduled operation for the Rogue Location Discovery Protocol (RLDP) to automate rogue device detection on your wireless network.

Before you begin

Use these steps to configure a schedule for RLDP.

Procedure

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

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

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

Step 3 In the **Retry Count** field, enter a value between 1 and 5 for the number of retries.

Step 4 Select the **Schedule RLDP** check box, and then specify the days, start time (for example, 8:00 a.m. [0800]), and end time (for example, 5:00 p.m. [1700]) for the process.

Step 5 Click **Apply**.

The system schedules RLDP based on your configuration and automatically detects rogue APs during the specified periods.

Configure a schedule for RLDP (CLI)

Set up a scheduled Rogue Location Discovery Protocol (RLDP) scan to run at specific days and times using CLI.

Before you begin

Use these steps to configure an RLDP schedule using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable Rogue Location Discovery Protocol (RLDP) based on a scheduled day, start time, and end time.

Example:

```
Device(config)# wireless wps rogue ap rldp schedule day Monday start start-time end end-time
```

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 Enable the schedule.

Example:

```
Device(config)# wireless wps rogue ap rldp schedule
```

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

The RLDP schedule runs automatically on the specified days and times, enabling periodic rogue AP detection.

Configure an RLDP for auto-contain (GUI)

Enable RLDP-based automatic containment of rogue devices detected on the wired network.

Before you begin

Use these steps to configure RLDP for auto-contain.

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** .

The system will automatically contain rogue devices detected through RLDP on the wired network.

Configure an RLDP for auto-contain (CLI)

Enable Rogue Location Discovery Protocol (RLDP) auto-contain mode on a wireless LAN controller using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable RLDP to perform auto-contain. This method always keeps RLDP enabled.

Example:

```
Device config)# wireless wps rogue ap rldp auto-contain
```

```
Device (config)# wireless wps rogue ap rldp auto-contain monitor-ap-only
```

The **monitor-ap-only** keyword is optional.

Using the command with only **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 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

RLDP is enabled for auto-contain. Rogue APs matching the configured behavior are automatically contained by the controller.

Configure RLDP retry times on rogue APs (GUI)

Set the number of RLDP retry attempts on rogue wireless APs.

Before you begin

Use these steps to configure RLDP retry times for rogue APs.

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 to 5.

Step 4 Save the configuration.

The RLDP retry count value for rogue APs are updated and applied on the network controller.

Configure RLDP retry times on rogue APs (CLI)

Set the number of RLDP (Rogue Location Discovery Protocol) retry attempts for rogue APs.

Before you begin

Use these steps to configure RLDP retry times on rogue APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable RLDP retry times on rogue APs.

Example:

```
Device(config)# wireless wps rogue ap rldp retries num-entries
```

Here, *num-entries* is the number of RLDP retry times for each of the rogue APs.

The valid range is 1 to 5.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

The device updates the RLDP retry times for rogue AP as specified, affecting future rogue AP RLDP attempts.

Verify rogue AP RLDP

These commands can be used to verify rogue AP RLDP.

Table 9: Verify 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.

Wireless Service Assurance (WSA) rogue events

Wireless Service Assurance (WSA) rogue events are telemetry notifications that replicate the information of corresponding SNMP traps. Support is available in Release 16.12.x, where x denotes a release version.

- You receive details such as the MAC address of the rogue AP.
- You receive information about the managed AP and the radio that detected the rogue AP with the strongest RSSI.
- You receive event-specific data, such as SSID; channel for potential honeypot events; and MAC address of the impersonating AP for impersonation events.

WSA Rogue Events: Details and Support

For all exported events, these 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 the strongest RSSI

- Event-specific data such as SSID; channel for potential honeypot events; and MAC address of the impersonating AP for impersonation events.

You can scale the WSA rogue events feature up to four times the maximum number of supported access points (APs). You can also scale it to one-half of the maximum number of supported clients.

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

Wireless service assurance rogue events

Configure your wireless device to send service assurance rogue event data to the event queue.

Before you begin

To configure wireless service assurance for rogue events, complete these steps.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable wireless service assurance.

Example:

```
Device# network-assurance enable
```

Step 3 Enable wireless service assurance for rogue devices.

Example:

```
Device# wireless wps rogue network-assurance enable
```

This ensures that the wireless service assurance (WSA) rogue events are sent to the event queue.

Your device sends wireless service assurance rogue events to the event queue for enhanced monitoring.

Monitor wireless service assurance rogue events

View wireless service assurance (WSA) rogue event statistics and details.

Before you begin

Use these steps to monitor wireless service assurance rogue events.

Procedure

Step 1 **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 occurred, but only six events were enqueued. Three events occurred before you enabled the WSA rogue feature.

Step 2 **show wireless wps rogue stats internal**

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

These commands display information about WSA events in the event history.

You can track WSA rogue event activity, investigate event history, and verify system responsiveness to rogue threats.

Rogue PMF containment

Rogue PMF containment is a wireless security feature that

- uses 802.11w Protected Management Frames (PMF) to contain rogue APs and clients
- operates on centrally switched WLANs when the radio channel of the detecting AP matches the rogue AP's channel, and
- activates only when certain mode and channel conditions are met to secure the network against unauthorized devices.

Feature history

Table 10: Feature history table for rogue PMF containment

Feature name	Release information	Feature description
Rogue PMF containment	Cisco IOS XE 17.12.1	Starting with Cisco IOS XE Dublin 17.12.1, the controller contains a rogue AP with 802.11w Protected Management Frame (PMF) on centrally switched wireless LANs. Containment occurs if the client-serving radio channel of a rogue-detecting AP matches the channel of the corresponding rogue AP.

Operational scenarios

PMF containment occurs in these scenarios:

- You can use PMF containment only in the local mode.
- You can perform PMF containment only for rogue clients that have not joined a rogue AP.
- You can use PMF containment only if a rogue-detecting AP shares the same primary channel with a rogue client.
- You cannot use PMF containment on DFS channels, even if a DFS channel serves as the client-serving channel.
- PMF containment works only if at least one WLAN operates on the serving radio.

For information about APs that support the Rogue PMF Containment feature, see Cisco AP Feature Matrix.

Enable rogue PMF containment

Enable PMF containment to protect your wireless network from rogue APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile and enter AP profile configuration mode.

Example:

```
Device(config)# ap profile ap-profile
```

Step 3 Enable PMF-denial rogue AP containment.

Example:

```
Device(config-ap-profile)# rogue detection containment pmf-denial
```

Step 4 Enable PMF-denial type deauthentication rogue AP containment.

Example:

```
Device(config-pmf-denial)# pmf-deauth
```

Step 5 Return to privileged EXEC mode.

Example:

```
Device(config-ap-profile)# end
```

Rogue AP PMF containment is enabled for the specified AP profile.

```
Device# configure terminal
Device(config)# ap profile pmf-ap-profile
```

```
Device(config-ap-profile)# rogue detection containment pmf-denial
Device(config-pmf-denial)# pmf-deauth
Device(config-ap-profile)# end
```

Verify PMF containment

To verify PMF containment and the relevant statistics, use these commands.

To view the summary of containment details for all AP radios, use this command

```
Device# show wireless wps rogue containment summary

Rogue Containment activities for each managed AP

AP: 687d.b45f.2ae0  Slot: 1
  Active Containments   : 3
   Containment Mode     : DEAUTH_PMF
   Rogue AP MAC         : 687d.b45f.2a2d
   Containment Channels : 40
```

To verify the rogue statistics, use this command:

```
Device# show wireless wps rogue stats
.
.
.
 States
  Alert                          : 256
  Internal                       : 0
  External                       : 0
  Contained                      : 1
  Containment-pending            : 0
  Threat                         : 0
  Pending                        : 0
Rogue Clients
  Total/Max Scale                : 20/16000
  Contained                      : 0
  Containment-pending            : 0
.
.
.
```