Managing Rogue Devices

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.

- **Beacon DS Attack** —When managed and rogue APs use the same BSSID, the rogue APs are termed as impersonators. An attacker can add the Direct-Sequence parameter set information element with any channel number. If the added channel number is different from the channel number used by the managed AP, the attack is termed as Beacon DS Attack.
- **Beacon Wrong Channel** —When managed and rogue APs use the same BSSID, the rogue APs are termed as AP impersonators. If an AP impersonator uses a channel number that is different from the one used by the managed AP with the same BSSID, the attack is termed as Beacon Wrong Channel. In such a case, the Direct-Sequence Information Element might not even be present in the Beacon frame.

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.

Rogue containment (Protected Management Frames (PMF) enabled)

Starting with Cisco IOS XE 17.3.1, the system does not contain rogue devices enabled with 802.11w Protected Management Frames (PMF). Instead, the system marks the rogue device as *Contained Pending*, and raises a Web Security Appliance (WSA) alarm for the *Contained Pending* event. Skipping device containment prevents unnecessary use of AP resources.

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

Note This feature is supported only on Wave 2 APs.

Off-channel PMF rogue containment

A off-channel PMF rogue containment is a wireless security technique that

- detects rogue access points using off-channel or non-serving radios
- enables access points to report rogue APs to a central controller, and
- allows continuous monitoring and containment of rogue APs without disrupting client service on the primary radio.

The containment process involves three steps:

1. An AP detects a rogue AP and reports its details to the controller.
2. The controller sends a containment request specifying the off-channel PMF containment type.
3. The AP validates the request and contains the rogue AP using designated off-channel radios.

The **pmf-offchannel** command is introduced in the AP profile of the controller to enable off-channel PMF rogue containment.

If a rogue AP is detected operating on a frequency not currently used by client devices, the Cisco AP can use its off-channel radio to monitor and contain that rogue AP, minimizing interruption to legitimate wireless clients.

Standard rogue containment only uses the serving radio, which can interfere with client service. Off-channel PMF rogue containment specifically avoids disruption by using non-serving or dedicated radios.

Limitations for off-channel PMF rogue containment

The limitations for off-channel PMF rogue containment are:

- You can only contain rogue clients that are not in power-saving mode.
- You cannot contain rogue clients on Dynamic Frequency Selection (DFS), or 5 gigahertz (GHz).
- You cannot contain rogue clients on the 6 gigahertz (GHz) band.
- After you contain rogue clients, they might re-associate with the rogue Service Set Identifier (SSID).
- Containment depends on client behavior and may not work if future changes are made to client wireless drivers.

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).
- AP impersonation detection uses AP authentication.

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
AAA Validate AP	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

Parameter	Critical	High	Low
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 Cisco Connected Mobile Experiences (CMX)	Enabled	Enabled	Enabled
Containment FlexConnect	Enabled	Enabled	Enabled

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 the minimum RSSI value for APs to detect rogues and create entries in the system.

Example:

```
Device(config)# ap profile profile-name
Device(config)# rogue detection rssi in dBm
```

You can enter an RSSI value from –128 to –70 dBm. The default is –128 dBm.

Note
You can use this feature with any AP mode.

Many rogues have weak RSSI values and do not provide useful information for rogue analysis. Specify a minimum RSSI value to filter these 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
Device(config)# rogue detection enable
```

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.

Enable AP authentication

Set up AP authentication on a wireless controller. This enhances network security by authenticating APs and by configuring threshold values for authentication failures.

Before you begin

Use these steps to enable AP authentication.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the wireless Wi-Fi Protected Setup (WPS) AP authentication.

Example:

```
Device(config)# wireless wps ap-authentication
```

Step 3 Configure AP neighbor authentication and set the threshold for AP authentication failures.

Example:

```
Device(config)# wireless wps ap-authentication threshold threshold
```

Step 4 Configure a WLAN.

Example:

```
Device(config)# wlan wlan-namewlan-idSSID-name
```

Step 5 Enable support for Aironet information elements on this Wireless Local Area Network (WLAN).

Example:

```
Device(config-wlan)# ccx aironet-iesupport
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device# end
```

AP authentication is enabled on the wireless controller. Authentication thresholds and Aironet IE support are configured for the specified WLAN.

Configure off-channel PMF rogue containment (GUI)

This task enables off-channel Protected Management Frame (PMF) rogue containment on an AP policy profile.

Before you begin

Perform the steps in this section to configure off-channel PMF rogue containment.

Procedure

Step 1 Choose **Configuration**, then **Tags & Profiles**, then **AP Join**.

Step 2 Click **Add**.

The window labeled **Add AP Join Profile** appears.

Step 3 In the **Add AP Join Profile** window, click the **General** tab and enter the profile name.

Step 4 Click the **Security** tab.

Step 5 Under the **Rogues** section, check the **Rogue Containment PMF-Offchannel** check box.

Step 6 Click **Apply to Device**.

Off-channel PMF rogue containment is enabled on the AP policy profile.

Configure off-channel PMF rogue containment (CLI)

Set up off-channel Protected Management Frame (PMF) rogue AP containment on APs using CLI commands.

Before you begin

Use these steps to configure off-channel PMF rogue containment on APs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter a profile name to create an AP profile.

Example:

```
Device(config)# ap profile ap-pmf-off-channel
```

Step 3 Enable PMF-denial for rogue AP containment.

Example:

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

Note
The **pmf-deauth** feature is enabled by default when **pmf-denial** is enabled. If you do not want **pmf-deauth**, then you must disable it explicitly.

Step 4 Enable PMF-denial type off-channel PMF rogue AP containment.

Example:

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

Off-channel PMF containment for rogue APs is enabled on the configured AP profile.

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
Rogue Event history

Timestamp                  #Times   Class/State Event                Ctx
     RC
-------------------------- -------- ----------- -------------------- -------------------------
 ----
05/10/2021 13:56:46.657434 2        Mal/Threat  FSM_GOTO
Threat  0x0
05/10/2021 13:56:46.654905 1        Unk/Init    EXPIRE_TIMER_START
240s  0x0
05/10/2021 13:56:46.654879 1       Unk/Init   AP_IMPERSONATION         DS:1,ch:1,band_id:0
  0x0
05/10/2021 13:56:46.654673 1       Unk/Init    RECV_REPORT                70db.98fc.2680/0
  0x0
05/10/2021 13:56:46.654663 1        Unk/Init    INIT_TIMER_START
180s  0x0
05/10/2021 13:56:46.654608 1        Unk/Init    CREATE
      0x0


Rogue BSSID                          : 002c.c8c1.096d
Last heard Rogue SSID                : MarvellAP0d
802.11w PMF required                 : No
Is Rogue an impersonator             : Yes
Beacon Wrong Channel                 : Yes
Beacon DS Attack                     : Yes
Is Rogue on Wired Network            : No
Classification                       : Malicious
Manually Contained                   : No
State                                : Threat
First Time Rogue was Reported        : 05/10/2021 13:56:46
Last Time Rogue was Reported         : 05/10/2021 13:56:46

Number of clients                    : 0
```

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.

Verify off-channel PMF rogue containment

Verify rogue containment summary

To verify rogue containment summary, use this command:

```
Device# show wireless wps rogue containment summary
Rogue Containment activities for each managed AP

AP: 6XXX.b4XX.2aXX  Slot: 1
  Active Containments   : 3
   Containment Mode     : OFFCHAN_PMF
   Rogue AP MAC         : 68XX.b4XX.2aXX
   Containment Channels : 40
                                  0.0.0.0                          372           64
         AGL          Enabled
```

Verify rogue statistics

To display rogue statistics, use this command:

```
Device# show wireless wps rogue stats
 Stats
  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
```

```
.
.
.
        0.0.0.0                         372             64                  AGL             Enabled
```

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# 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
```

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 rogue detection security level.

Example:

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

You can set the *security-level* to be **critical** for highly sensitive deployments, **custom** for customizable security level, **high** for medium-scale deployments, and **low** for small-scale deployments.

Step 3 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 4 Configure the use of AAA or local database to detect valid MAC addresses.

Example:

```
Device(config)# wireless wps rogue client aaa
```

Configures the use of AAA or local database to detect valid MAC addresses.

Step 5 Configure the use of MSE to detect valid MAC addresses.

Example:

```
Device(config)# wireless wps rogue client mse
```

Configures the use of MSE to detect valid MAC addresses.

Step 6 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 7 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 8 Configure the use of AAA or local database to classify rogue AP based on rogue AP MAC addresses.

Example:

```
Device(config)# wireless wps rogue ap aaa
```

Configures the use of AAA or local database to classify rogue AP based on rogue AP MAC addresses.

Step 9 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 10 Enable detecting and reporting adhoc rogue (IBSS).

Example:

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

Enables detecting and reporting adhoc rogue (IBSS).

Step 11 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.

Step 12 Configure the init timer for rogue APs.

Example:

```
Device(config)# wireless wps rogue ap init-timer timer-value
```

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.

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

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 AP scale modes per class

A rogue AP scale mode is a database management mechanism that

- decides if the system adds or discards a newly detected rogue AP when the database reaches its capacity
- lets you set quotas or priorities by rogue AP classification to use available space efficiently, and
- allows you to customize storage management based on classification needs and resources.

Types of rogue AP scale modes

These modes determine whether the system adds a rogue AP to the database when it reaches maximum scale:

- **Quota**: Quotas apply to each classification as a percentage of the maximum scale. If a classification has a quota of X percent, that portion of the rogue AP database is reserved for the classification. If all memory for that classification is used, the system drops any new rogue APs in that classification.
- **Priority**: Priorities apply to different classifications. If you do not set quotas, the system uses priority mode by default. The system uses these priorities:
  - malicious: highest
  - custom: high
  - unclassified: medium
  - friendly: low

  The system enforces priorities only when the maximum database scale is reached. If you classify a new rogue AP and the database is full, the system adds it only if there are lower-priority rogue APs that are present. If this happens, the system deletes the newest rogue AP entry of the lowest priority. If there are no lower-priority rogue APs, the system drops the new AP.
- **Hybrid**: Hybrid mode combines quotas and priorities. When space is available, rogue APs of lower priority use any unused quota reserved for higher-priority rogue APs.

Rogue AP scale mode logic after reaching maximum scale

After the rogue AP database reaches maximum scale, the system applies this logic when it classifies a new rogue AP:

- If the number of stored rogue APs in the new rogue AP's class is below its quota, store the new rogue AP and delete the newest rogue AP of the lowest-priority classification that exceeds its quota.
- If a lower-priority classification exceeds its quota, the system deletes the newest rogue AP in that classification and stores the new rogue AP.
- If neither condition applies, the system drops the new rogue AP.

Note

- Configure quotas and priorities carefully to balance security requirements with database limitations.
- If you do not configure quotas, the system uses priority mode.

Suppose the database has reached maximum scale and a new rogue AP classified as malicious is detected. If the malicious quota allows storage, the system stores the new rogue AP and removes the newest rogue AP from the lowest-priority classification that exceeds its quota. If no such rogue AP exists, the system drops the new rogue AP.

Feature history for rogue full scale quotas and priorities

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 9: Feature History for Rogue Full Scale Quotas and Priorities

Release	Feature	Feature information
Cisco IOS XE 17.9.1	Rogue full scale quotas and priorities	The rogue full scale quotas and priorities feature helps you to improve the scalability, performance, manageability, and serviceability of rogue Access Points (APs).

Advantages and disadvantages of role-scale modes

Mode	Advantages	Disadvantages
Quota	Simple to use and understand.	• Memory is not used efficiently. • New rogue APs for a class that is already in its maximum quota are dropped. While the memory reserved for another class that does not have any rogue APs, stays empty. For example, this could lead to dropping malicious rogue APs, while there is still memory available.
Priority	• Simple to use and understand. • Utilizes the available memory. • Stores the important rogue APs.	Some of the lower-priority rogue AP classes might not be represented in the rogue database, if higher-priority rogue APs utilize all the available memory.
Hybrid	Utilizes the available memory, while providing quotas so that all the classes are represented in the database.	Difficult for users to understand the exact behavior.

Configure rogue AP scale (CLI)

Set scale quotas, priorities, and hybrid modes for rogue AP types (malicious, custom, unclassified, friendly) using CLI commands.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure rogue scale quota for malicious, custom, unclassified, and friendly rogue APs.

Example:

```
Device(config)# wireless wps rogue scale quota maliciouspercentage-malicious-rogue-AP custom
 percentage-custom-rogue-AP unclassified percentage-unclassified-rogue-AP friendly
percentage-friendly-rogue-AP
```

The default value for quota is 0. The sum of all the quotas must be less than or equal to 100 percent.

If the sum of all the configured quotas is equal to 0, then priority mode is used. If the sum of all the quotas is not equal to 0, then quota mode is used. If hybrid mode is configured, hybrid mode is used no matter what the quota configuration is. Hybrid mode with all the quotas equal to 0, is identical to the priority mode.

Note
Hybrid mode is enabled after the maximum scale is reached. All the rogue APs are stored before the maximum scale is reached.

Step 3 Configure rogue scale priority for malicious, custom, unclassified, and friendly rogue APs.

Example:

```
Device(config)# wireless wps rogue scale priority malicious highest custom high unclassified
 medium friendly low
```

Example:

```
[no] wireless wps rogue scale priority malicious { high| highest| low|
medium } custom{ high | highest | low | medium } unclassified { high | highest
 | low | medium } friendly { high | highest | low | medium }
```

The default value for malicious is **highest** , the default value for custom is **high** , the default value for unclassified is **medium** , and the default value for friendly is **low** .

Step 4 Configure rogue scale hybrid mode.

Example:

```
Device(config)# wireless wps rogue scale mode hybrid
```

Unused quota reserved for higher-priority rogue APs are used by rogue APs of lower priority when space is available.

Rogue AP classification uses configured quotas, priorities, or hybrid mode to efficiently manage detected rogue APs according to defined organizational policies.

Verify rogue scale details

To verify the rogue scale details, run this command:

```
Device# show wireless wps rogue stats
  Total Post Init/Max            : 0/4000
  Total/Max                      : 0/4200
  Init                           : 0
Classification
  Friendly                       : 0/0/0 (Total/Init/Quota[%])
  Malicious                      : 0/0/0 (Total/Init/Quota[%])
  Custom                         : 0/0/0 (Total/Init/Quota[%])
  Unclassified                   : 0/0/0 (Total/Init/Quota[%])
  Unknown                        : 0/0 (Total/Init)
Configured Quotas by Classification
  Custom         : <% of max scale>
  Friendly       : <% of max scale>
  Malicious      : <% of max scale>
  Unclassified   : <% of max scale>
Configured Priorities by Classification
  Custom          :  2 (High)
  Friendly        :  4 (Low)
  Malicious       :  1 (Highest)
  Unclassified    :  3 (Medium)

Configured Rogue Scale Mode: [Priority|Quota|Hybrid]
```

To view the rogue ad hoc summary, run this command:

```
Device# show wireless wps rogue adhoc summary
Detect and report Ad-Hoc Networks : Enabled
Auto-Contain Ad-Hoc Networks      : Disabled
Total Number of Rogue Ad-Hoc      : 0
Friendly Ad-Hoc Rogues            : 0
Malicious Ad-Hoc Rogues           : 0
Custom Ad-Hoc Rogues              : 0
Unclassified Ad-Hoc Rogues        : 0
Unknown Ad-Hoc Rogues             : 0
Client MAC Address   Adhoc BSSID        Classification  State        # APs  Last Heard

---------------------------------------------------------------------------------------------
```