Resolve Rogue Detection and Mitigation in an Unified Wireless Network

Contents

Introduction

This document describes Rogue Detection and Mitigation on Cisco Wireless Networks.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless Lan Controllers.
- Cisco Prime Infrastructure.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Wireless Lan Controllers (5520, 8540 and 3504 Series) that run version 8.8.120.0.

- Wave 2 APs 1832, 1852, 2802 and 3802 series.

- Wave 1 APs 3700, 2700 and 1700 series.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Rogue Overview

Wireless networks extend wired networks and increase worker productivity and access to information. However, an unauthorized wireless network presents an additional layer of security concern. Less thought is put into port security on wired networks, and wireless networks are an easy extension to wired networks. Therefore, an employee who brings his or her own Access Point (Cisco or Non Cisco) into a well-secured wireless or wired infrastructure and allows unauthorized users access to this otherwise secured network, can easily compromise a secure network.

Rogue detection allows the network administrator to monitor and eliminate this security concern. Cisco Unified Network Architecture provides methods for rogue detection that enable a complete rogue identification and containment solution without the need for expensive and hard-to-justify overlay networks and tools.

Any device that shares your spectrum and is not managed by you can be considered a rogue. A rogue becomes dangerous in these scenarios:

- When setup to use the same Service Set Identifier (SSID) as your network (honeypot)

- When it is detected on the wired network

- Ad-hoc rogues

- When set up by an outsider, most times, with malicious intent

The best practice is to use rogue detection to minimize security risks, for example, in a corporate environment.

However, there are certain scenarios in which rogue detection is not needed, for example, in Office Extend Access Point (OEAP) deployment, citywide, and outdoors.

The use of outdoor mesh APs to detect rogues would provide little value while it would use resources to analyze.

Finally, it is critical to evaluate (or avoid altogether) rogue auto-containment, as there are potential legal issues and liabilities if left to operate automatically.

There are three main phases of rogue device management in the Cisco Unified Wireless Network (UWN) solution:

- Detection - A Radio Resource Management (RRM) scan is used to detect the presence of rogue devices.

- Classification - Rogue Location Discovery Protocol (RLDP), Rogue Detectors (Wave 1 APs only) and switch port traces are used to identify if the rogue device is connected to the wired network. Rogue classification rules also assist in the filtration of rogues into specific categories based on their characteristics.

- Mitigation - Switch port shutting, rogue location, and rogue containment are used in to track down its physical location and to nullify the threat of the rogue device.

Cisco Rogue Management Diagram
Multiple Methods
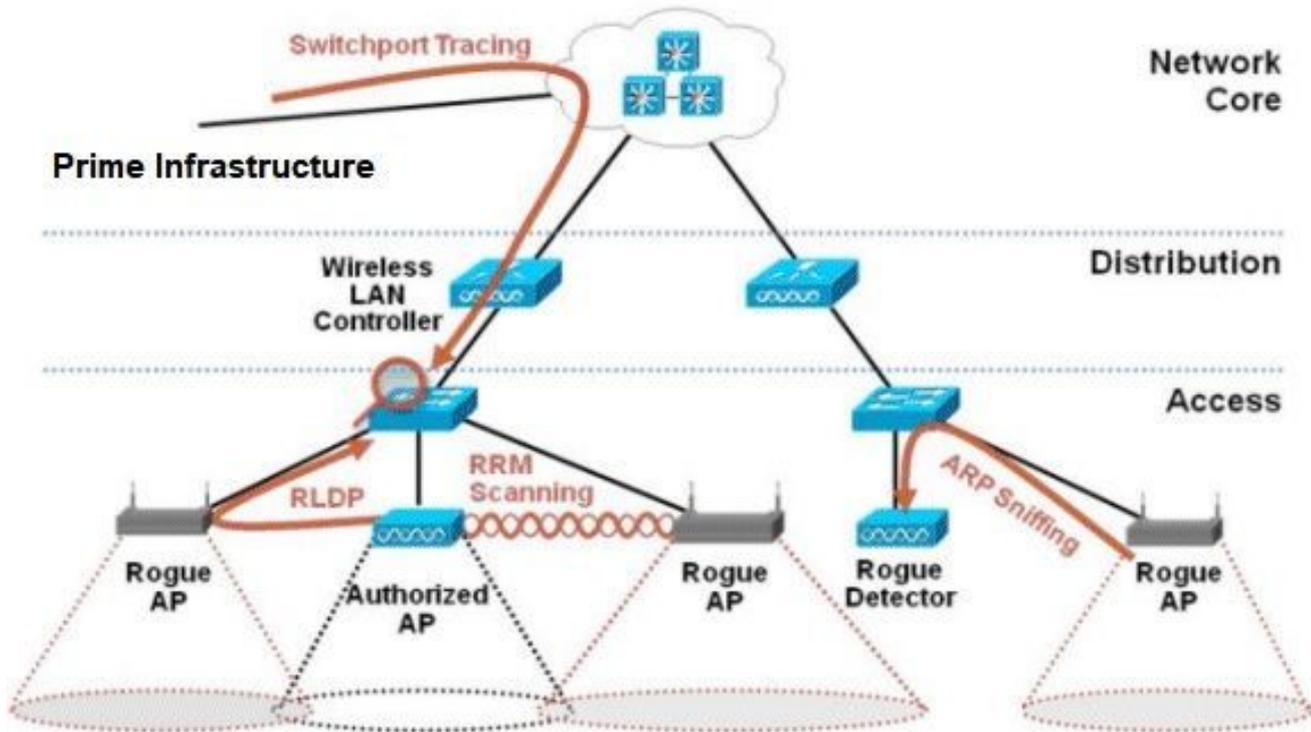
Rogue Detection

A rogue is essentially any device that shares your spectrum, but is not in your control. This includes rogue Access Points, wireless router, rogue clients, and rogue ad-hoc networks. The Cisco UWN uses a number of methods to detect Wi-Fi-based rogue devices such as an off-channel scan and dedicated monitor mode capabilities. Cisco Spectrum Expert can also be used to identify rogue devices not based on the 802.11 protocol, such as Bluetooth bridges.

Off-Channel Scan

This operation is performed by Local and Flex-Connect (in connected mode) mode APs and utilizes a time-slicing technique which allows client service and channel scan with the usage of the same radio. With the move to off-channel for a period of 50ms every 16 seconds, the AP, by default, only spends a small percentage of its time to not serve clients. Also, note there is a 10ms channel change interval that occurs. In the default scan interval of 180 seconds, each 2.4Ghz FCC channel (1–11) is scanned at least once. For other regulatory domains, such as ETSI, the AP is off channel for a slightly higher percentage of time. Both the list of channels and scan interval can be adjusted in the RRM configuration. This limits the performance impact to a maximum of 1.5% and intelligence is built into the algorithm to suspend the scan when high-priority QoS frames, such as voice, need to be delivered.

Local-Mode AP on Channel 1 - 802.11 b/g/n Off-Channel Scanning
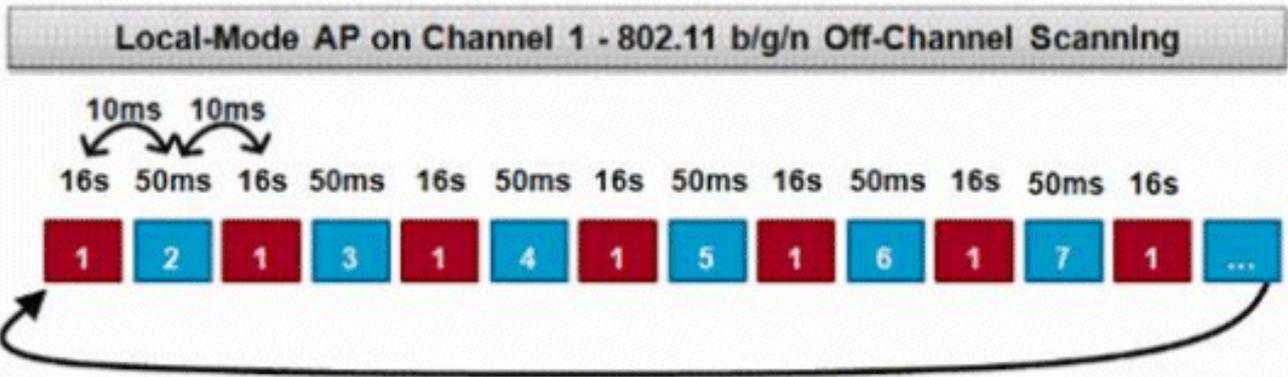
This graphic is a depiction of the off-channel scan algorithm for a local mode AP in the 2.4GHz frequency band. A similar operation is done in parallel on the 5GHz radio if the AP has one present. Each red square represents the time spent on the APs home channel, whereas each blue square represents time spent on adjacent channels for scan purposes.

Monitor Mode Scan

This operation is performed by Monitor Mode and Adaptive wIPS monitor mode APs which utilizes 100% of the radio time to scan all channels in each respective frequency band. This allows a greater speed of detection and enables more time to be spent on each individual channel. Monitor mode APs are also superior at the detection of rogue clients as they have a more comprehensive view of the activity that occurs in each channel.

Monitor-Mode AP - 802.11b/g/n Scanning All Channels
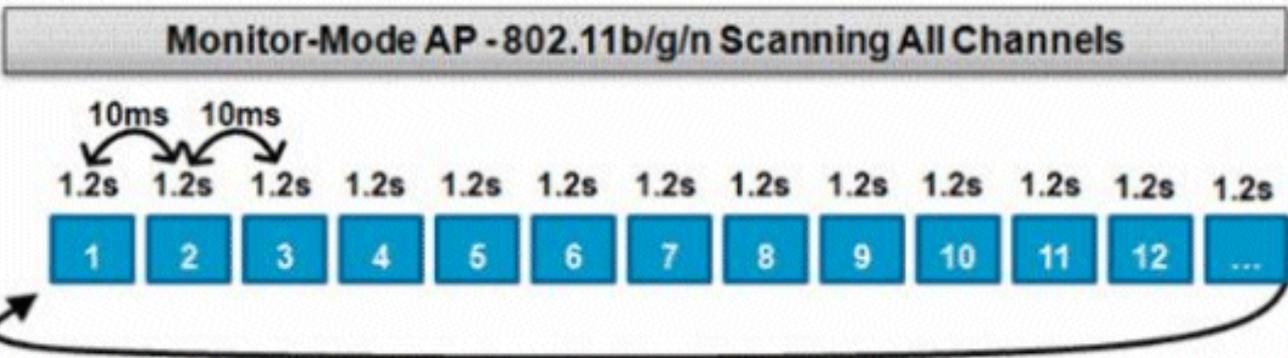
This graphic is a depiction of the off-channel scan algorithm for a monitor mode AP in the 2.4GHz frequency band. A similar operation is done in parallel on the 5GHz radio if the AP has one present.

Local Mode and Monitor Mode Comparison

A local mode AP splits its cycles between the service of WLAN clients and the scan of channels for threats. As a result, it takes a local mode AP longer to cycle through all the channels, and it spends less time in the collection data on any particular channel so that client operations are not disrupted. Consequently, rogue and attack detection times are longer (3 to 60 minutes) and a smaller range of over-the-air attacks can be detected than with a monitor mode AP.

Furthermore, detection for bursty traffic, such as rogue clients, is much less deterministic because the AP has to be on the channel of the traffic at the same time the traffic is transmitted or received. This becomes an exercise in probabilities. A monitor mode AP spends all of its cycles on the scan of channels to look for rogues and over-the-air attacks. A monitor mode AP can simultaneously be used for Adaptive wIPS, location (context-aware) services, and other monitor mode services.

When monitor mode APs are deployed, the benefits are lower time-to-detection. When monitor mode APs are additionally configured with Adaptive wIPS, a broader range of over-the-air threats and attacks can be detected.

Local Mode APs	Monitor Mode APs
Serves clients with time-slicing off-channel scan	Dedicated Scan
Listens for 50ms on each channel	Listens for 1.2s on each channel
Configurable to scan: • All channels • Country channels (default) • DCA channels	Scans all channels

Rogue Identification

If probe response or beacons from a rogue device are heard by either local, flex-connect or monitor mode APs, then this information is communicated via CAPWAP to the Wireless LAN controller (WLC) for the process. In order to prevent false positives, a number of methods are used to ensure other managed Cisco-based APs are not identified as a rogue device. These methods include mobility group updates, RF neighbor packets, and allowed list friendly APs via Prime Infrastructure (PI).

Rogue Records

While the controller's database of rogue devices contains only the current set of detected rogues, the PI also includes an event history and logs rogues that are no longer seen.

Rogue Details

A CAPWAP AP goes off-channel for 50ms in order to listen for rogue clients, monitor for noise, and channel interference. Any detected rogue clients or APs are sent to the controller, which gathers this information:

- The rogue AP MAC address

- Name of the AP detected rogue

- The rogue connected client(s) MAC address

- Security Policy

- The preamble

- The Signal-to-Noise Ratio (SNR)

- The Receiver Signal Strength Indicator (RSSI)

- Channel of Rogue detection

- Radio in which rogue is detected

- Rogue SSID (if the rogue SSID is broadcasted)

- Rogue IP address

- First and last time the rogue is reported

- Channel width

To Export Rogue Events

In order to export rogue events to a third-party Network Management System (NMS) for archival, the WLC permits additional SNMP trap receivers to be added. When a rogue is detected or cleared by the controller, a trap that contains this information is communicated to all SNMP trap receivers. One caveat with the export of events via SNMP is that if multiple controllers detect the same rogue, duplicate events are seen by the NMS as correlation is only done at PI.

Rogue Record Timeout

Once a rogue AP has been added to the WLC records, it remaina there until it is no longer seen. After a user configurable timeout (1200 seconds default), a rogue in the_**unclassified**_category is aged out.

Rogues in other states such as_**Contained**_and_**Friendly**_ persist so that the appropriate classification is applied to them if they reappear.

There is a maximum database size for rogue records that is variable across controller platforms:

- 3504 - Detection and containment of up to 600 Rogue APs and 1500 Rogue Clients

- 5520 - Detection and containment of up to 24000 Rogue APs and 32000 Rogue Clients
- 8540 - Detection and containment of up to 24000 Rogue APs and 32000 Rogue Clients

Rogue Detector AP

A rogue detector AP aims to correlate rogue information heard over the air with ARP information obtained from the wired network. If a MAC address is heard over the air as a rogue AP or client and is also heard on the wired network, then the rogue is determined to be on the wired network. If the rogue is detected to be on the wired network, then the alarm severity for that rogue AP is raised to_**critical**_. A rogue detector AP is not successful at the identification of rogue clients behind a device that uses NAT.

This approach is used when rogue AP has some form of authentication, either WEP or WPA. When a form of authentication is configured on rogue AP, the Lightweight AP cannot associate because it does not know the authentication method and credentials configured on the rogue AP.
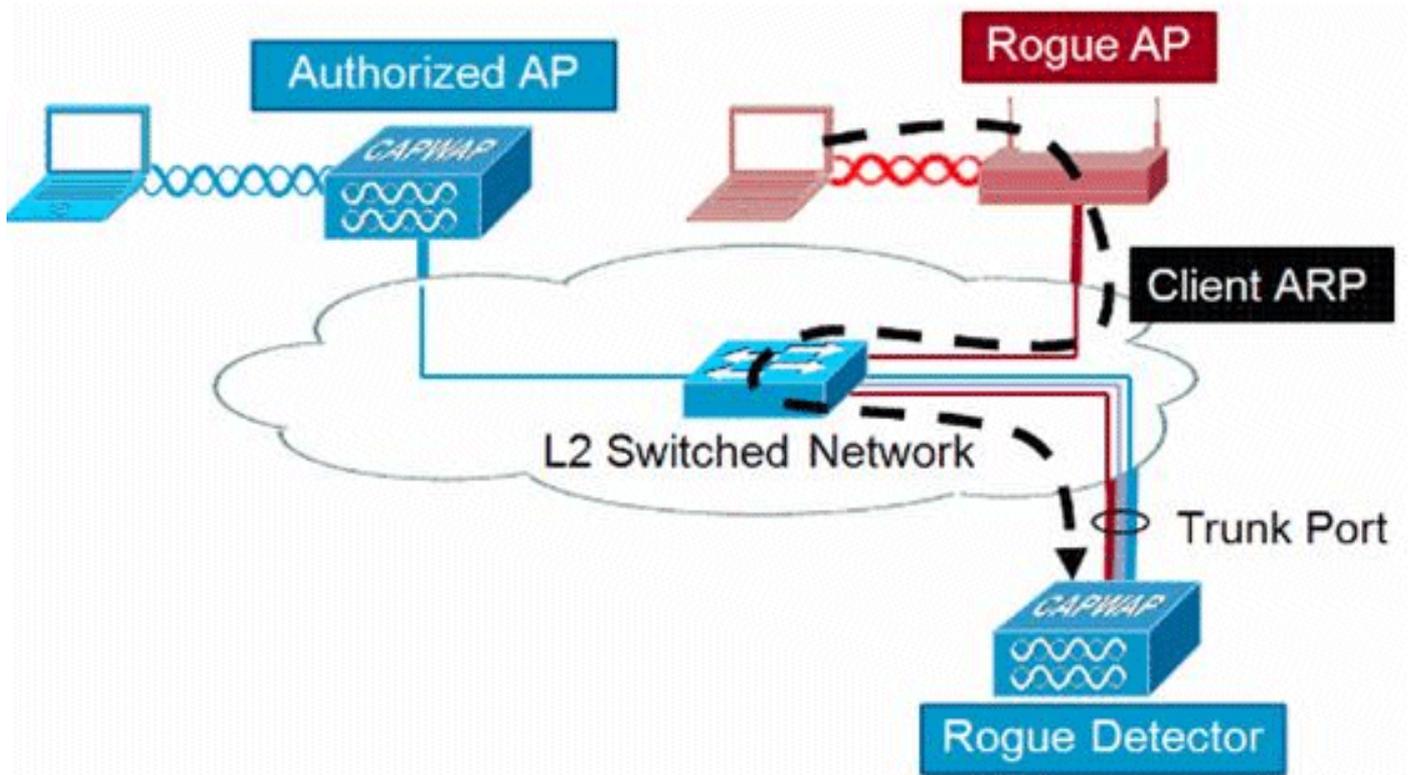
Note: Only Wave 1 APs can be configured as Rogue Detectors.

Scalability Considerations

A rogue detector AP can detect up to 500 rogues and 500 rogue clients. If the rogue detector is placed on a trunk with too many rogue devices, then these limits are exceeded, which causes issues. In order to prevent this to occurr, keep rogue detector APs at the distribution or access layer of your network.

RLDP

The aim of RLDP is to identify if a specific rogue AP is connected to the wired infrastructure. This feature essentially uses the closest AP to connect to the rogue device as a wireless client. After the connection as a client, a packet is sent with the destination address of the WLC to assess if the AP is connected to the wired network. If the rogue is detected to be on the wired network, then the alarm severity for that rogue AP is raised to critical.
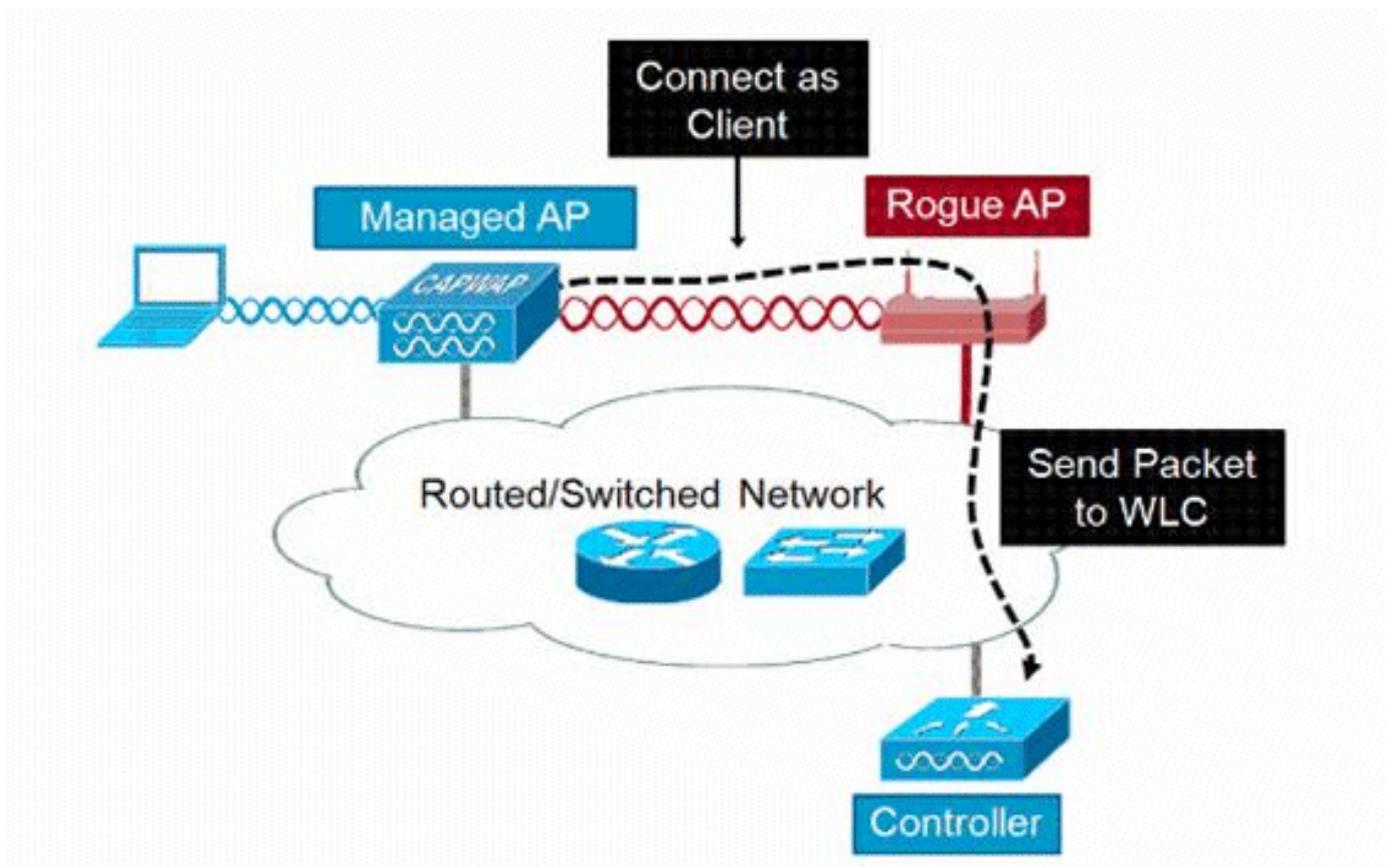
The algorithm of RLDP is listed here:

1. Identify the closest Unified AP to the rogue by the usage of signal strength values.

2. The AP then connects to the rogue as a WLAN client, attemps three associations before it times out.

3. If association is successful, the AP then uses DHCP to obtain an IP address.

4. If an IP address was obtained, the AP (that acts as a WLAN client) sends a UDP packet to each of the controller IP addresses.

5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire with a severity of critical.

Note: The RLDP packets are unable to reach the controller if the filter rules are in place between the controller network and the network where the rogue device is located.

Caveats of RLDP

- RLDP only works with open rogue APs that broadcast their SSID with authentication and encryption disabled.

- RLDP requires that the Managed AP that acts as a client is able to obtain an IP address via DHCP on the rogue network

- Manual RLDP can be used to attempt and RLDP trace on a rogue multiple times.

- On the RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs.

- RLDP does not attempt to connect to a rogue AP that operates in a 5GHz DFS channel.

Switch Port Traces

Switch port trace is a rogue AP mitigation technique. Although the switch port trace is initiated at the PI, it utilizes both CDP and SNMP information to track a rogue down to a specific port in the network.

In order for the switch port trace to run, all switches in the network must be added to the PI with SNMP credentials. Although read-only credentials work to identify the port the rogue is on, read-write credentials allow the PI to also shut the port down, thus it contains the threat.

At this time, this feature works only with Cisco switches that run Cisco IOS® with CDP enabled, and CDP must also be enabled on the Managed APs.
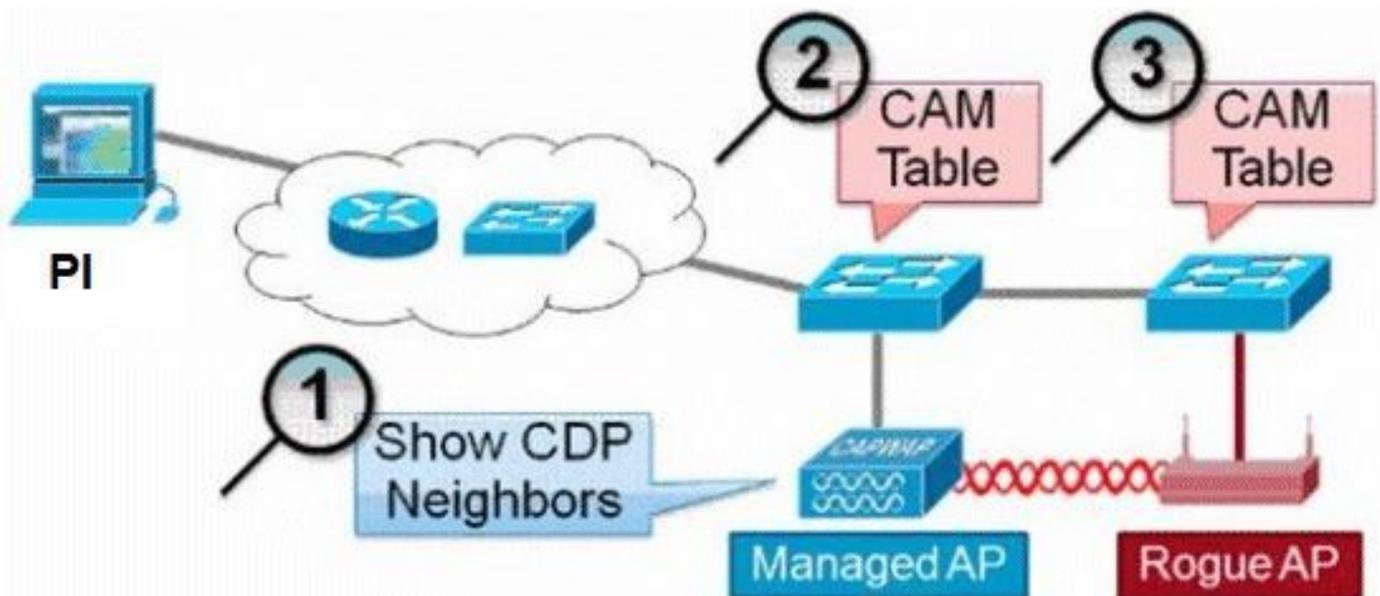
The algorithm for the switch port trace is listed here:

1. The PI finds the closest AP, which detects the rogue AP over-the-air, and retrieves its CDP neighbors.

2. The PI then uses SNMP to examine the CAM table within the neighbor switch, it looks for a positive match to identify the rogues location.

3. A positive match is based on the exact rogue MAC address, +1/−1 the rogue MAC address, any rogue client MAC addresses, or an OUI match based on the vendor information inherent in a MAC address.

4. If a positive match is not found on the closest switch, the PI continues the search in neighbor switches up to two hops away (by default).

Wired-Side Tracing Techniques
Comparison

	How it Works	What It Detects	Accuracy
Switchport Tracing	1. AP hears rogue over air 2. Detecting AP advises of nearby switches 3. Trace starts on nearby switches 4. Results reported in order of probability 5. Administrator may disable port	• Open APs • Secured APs • NAT APs	• Moderate
RLDP	1. AP hears rogue over air 2. Detecting AP connects as client to rogue AP 3. Detecting AP sends RLDP packet 4. If RLDP packet seen at WLC, then on wire	• Open APs • NAT APs	• 100%
Rogue Detector	1. Place detector AP on trunk 2. Detector receives all rogue MACs from WLC 3. Detector AP matches rogue MACs from wired-side ARPs	• Open APs • Secured APs • NAT APs	• High

Rogue Classification

By default, all rogues that are detected by the Cisco UWN are considered Unclassified. As shown in this graphic, rogues can be classified on a number of criteria that includs RSSI, SSID, Security type, on/off network, and number of clients:

Lower Severity ───────────────────────────────→ **Higher Severity**

Off-Network	On-Network
Secured	Open
Foreign SSID	Our SSID
Weak RSSI	Strong RSSI
No clients	Attracts clients
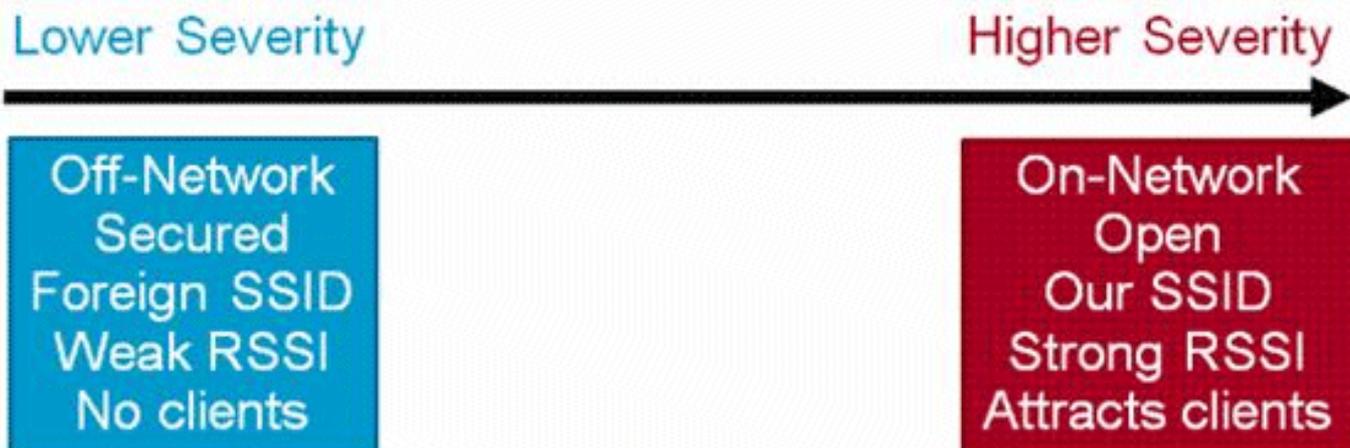
Rogue Classification Rules

Rogue classification rules, allow you to define a set of conditions that mark a rogue as either malicious or friendly. These rules are configured at the PI or the WLC, but they are always performed on the controller as new rogues are discovered.

Read the document[Rule Based Rogue Classification in Wireless LAN Controllers (WLC) and Prime Infrastructure (PI)](for more information on rogue rules in the WLCs.

HA Facts

If you manually move any rogue device to contained state (any class) or friendly state, this information is stored in the standby Cisco WLC flash memory; however, the database is not updated. When HA switchover occurs, the rogue list from the previously standby Cisco WLC flash memory is loaded.

In a High Availability scenario, if the rogue detection security level is set to either High or Critical, the rogue timer on the standby controller starts only after the rogue detection pend stabilization time, which is 300 seconds. Therefore, the active configurations on the standby controller are reflected only after 300 seconds.

Flex-Connect Facts

A FlexConnect AP (with rogue detection enabled) in the connected mode takes the containment list from the controller. If auto-contain SSID and auto contain adhoc are set in the controller, then these configurations are set to all FlexConnect APs in the connected mode and the AP stores it in its memory.

When the FlexConnect AP moves to a standalone mode, the next tasks are performed:

- The containment set by the controller continues.

- If the FlexConnect AP detects any rogue AP that has same SSID as that of infra SSID (SSID configured in the controller that the FlexConnect AP is connected to), then containment gets started if auto contain SSID was enabled from the controller before it moves to the standalone mode.

- If the FlexConnect AP detects any adhoc rogue, containment gets started if auto-contain adhoc was enabled from the controller when it was in the connected mode.

When the standalone FlexConnect AP moves back to the connected mode, then these tasks are performed:

- All containment gets cleared.

- Containment initiated from the controller takes over.

Rogue Mitigation

Rogue Containment

Containment is a method that uses over-the-air packets to temporarily interrupt service on a rogue device until it can physically be removed. Containment works with the spoof of de-authentication packets with the spoofed source address of the rogue AP so that any clients associated are kicked off.
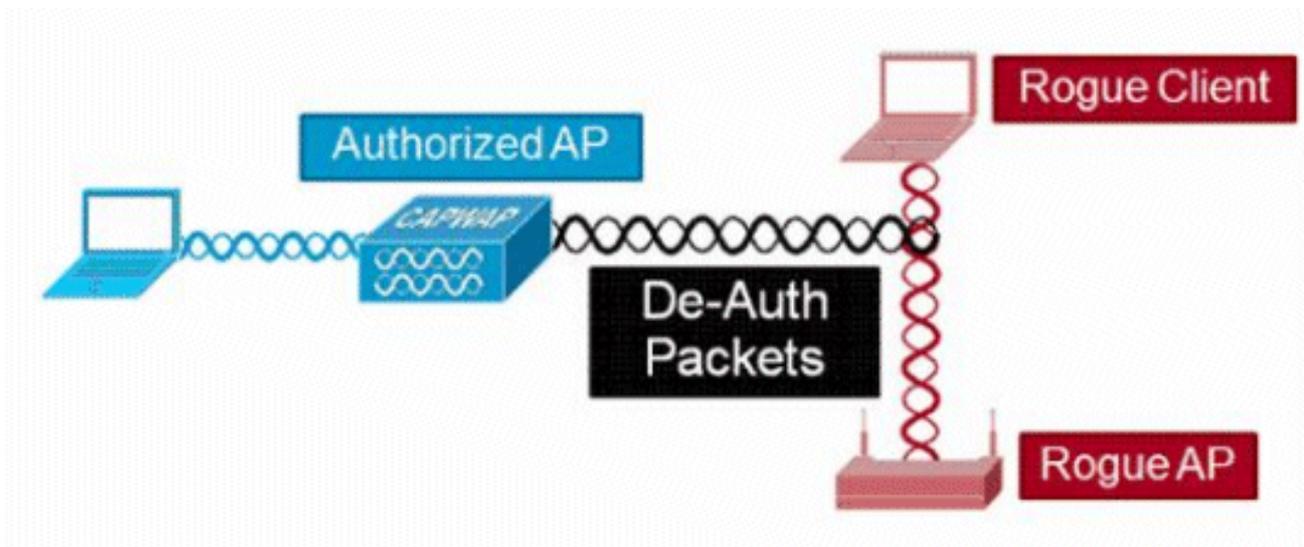
Rogue Containment Details

A containment initiated on a rogue AP with no clients only uses de-authentication frames sent to the broadcast address:

Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth

Broadcast Deauth frames only

A containment initiated on a rogue AP with client(s) use de-authentication frames sent to the broadcast address and to the client(s) address:

Source	Destination	Data Rate	Size	Protocol
Rogue AP	Ethernet Broadcast	6.0	144	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth
Rogue AP	Rogue Client	6.0	30	802.11 Deauth

Broadcast and Unicast Deauth frames

Containment packets are sent at the power level of the managed AP and at the lowest enabled data rate.

Containment sends a minimum of 2 packets every 100ms:

Source	Destination	Da...	Size	Relative Time	Protocol
Rogue AP	Ethernet Broadcast	6.0	56	0.000000	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	0.000004	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	144	0.000007	802.11 Beacon
Rogue AP	Ethernet Broadcast	6.0	56	0.102414	802.11 Deauth
Rogue AP	Ethernet Broadcast	6.0	30	0.102419	802.11 Deauth

~100ms

Note: A containment performed by non-monitor mode APs is sent at an interval of 500ms instead of the 100ms interval used by monitor mode APs..

- An individual rogue device can be contained by 1 to 4 managed APs which work in conjunction to mitigate the threat temporarily.

- Containment can be performed by the usage of local mode, monitor mode and flex-connect (Connected) mode APs. For local mode of flex-connect APs, a maximum of three rogue devices per radio can be contained. For monitor mode APs, a maximum of six rogue devices per radio can be contained.

Auto-Containment

In addition to manually initiation of containment on a rogue device via PI or the WLC GUI, there is also the ability to automatically launch containment under certain scenarios. This configuration is found under**General**in the**Rogue Policies**section of the PI or controller interface. Each of these features is disabled by default and are to be enabled only to nullify the threats that cause the most damage.

- Rogue on Wire - If a rogue device is identified to be attached to the wired network, then it is automatically placed under containment.

- Use of our SSID - If a rogue device uses an SSID which is the same as that configured on the controller, it is automatically contained. This feature aims to address a honey-pot attack before it causes damage.

- Valid client on Rogue AP - If a client listed in Radius/AAA server is found to be associated with a rogue device, containment is launched against that client only, it prevents it from the association to any non-managed AP.

- AdHoc Rogue AP - If an ad-hoc network is discovered, it is automatically contained.

Rogue Containment Caveats

- Because containment uses a portion of the managed AP radio time to send the de-authentication frames, the performance to both data and voice clients is negatively impacted by up to 20%. For data clients, the impact is reduced throughput. For voice clients, containment can cause interruptions in conversations and reduced voice quality.

- Containment can have legal implications when launched against neighbor networks. Ensure that the rogue device is within your network and poses a security risk before you launch the containment.

Switch Port Shut

Once a switch port is traced by the usage of SPT, there is an option to disable that port in PI. Administrator has to do this exercise manually. An option is available to enable the switch port through PI if rogue is

physically removed from the network.

Configure

Configure Rogue Detection

Rogue detection is enabled in the controller by default.

In order to configure various options, navigate to **Security > Wireless Protection Policies > Rogue Policies > General**. As Example:

Step 1. Change the timeout for rogue APs.

Step 2. Enable the detection of ad-hoc rogue networks.
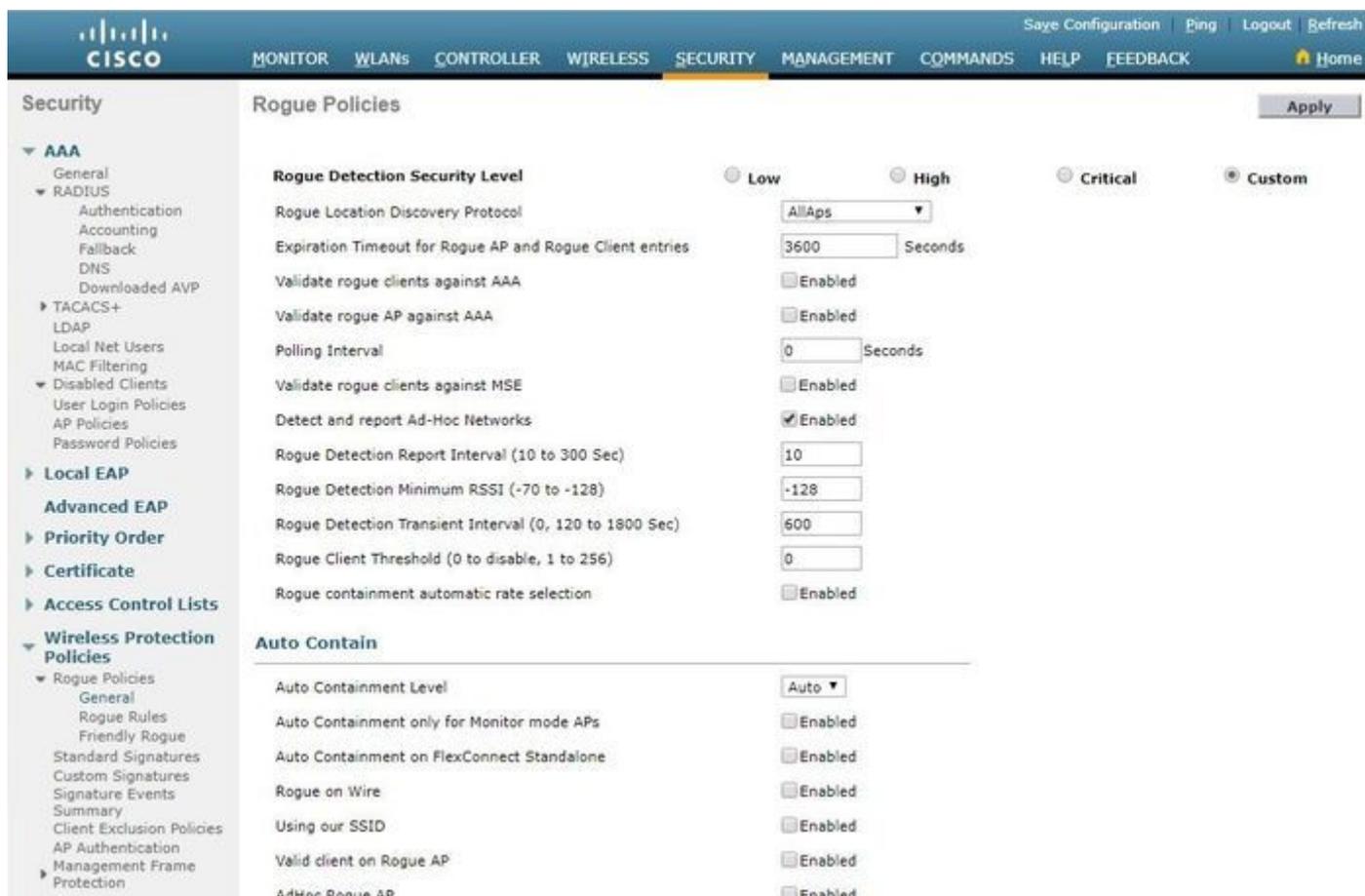
From the CLI:

```
<#root>

(Cisco Controller) >

config rogue ap timeout ?

<seconds>        The number of seconds<240 - 3600> before rogue entries are flushed

(Cisco Controller) >

config rogue adhoc enable/disable
```

Configure Channel Scan for Rogue Detection

For a local/Flex-Connect/Monitor mode AP there is an option under RRM configuration which allows the user to choose which channels are scanned for rogues. It Depends on the config, the AP scans all channel/country channel/DCA channel for rogues.

In order to configure this from the GUI, navigate to **Wireless > 802.11a/802.11b > RRM > General,** as shown in the image.
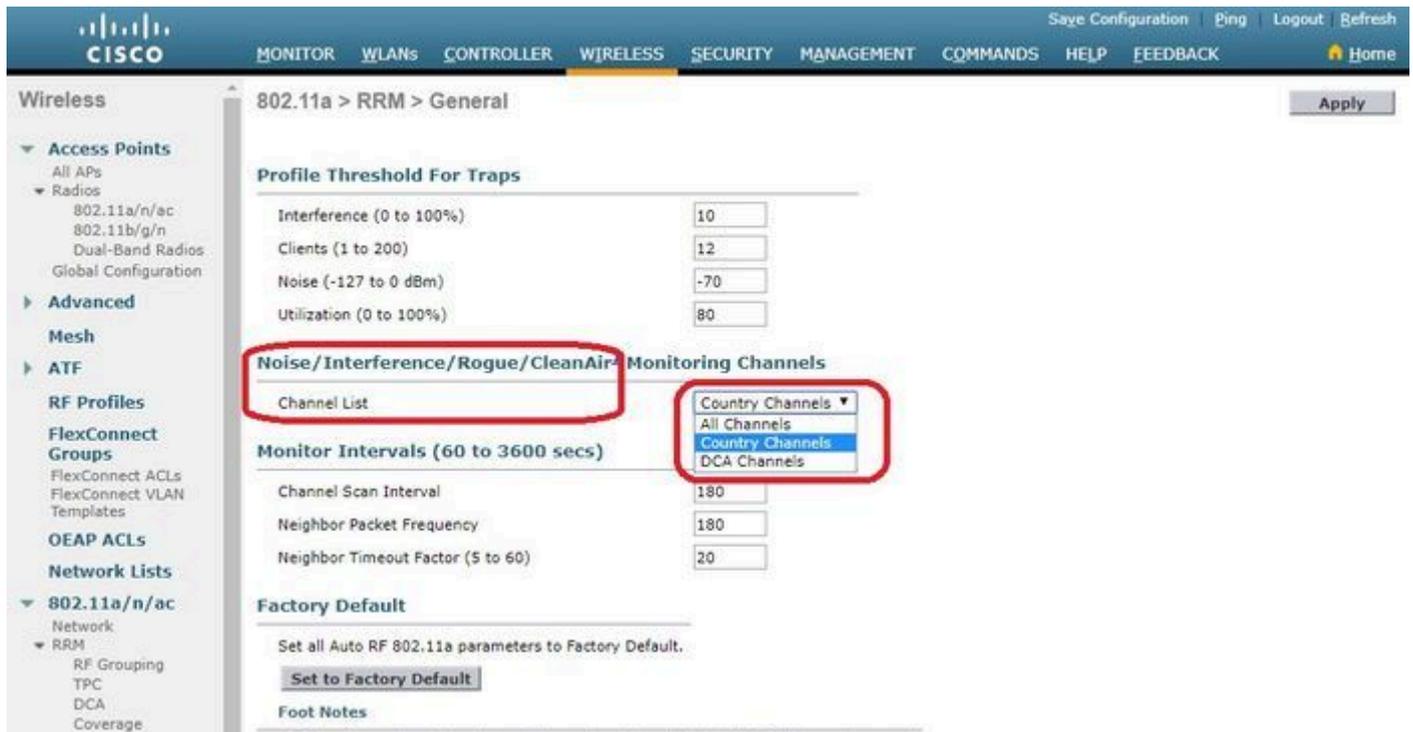
From the CLI:

```
<#root>

(Cisco Controller) >

config advanced 802.11a monitor channel-list ?


all           Monitor all channels
country       Monitor channels used in configured country code
dca           Monitor channels used by automatic channel assignment
```

Configure Rogue Classification

Manually Classify a Rogue AP

In order to classify a rogue AP as friendly, malicious, or unclassified, navigate to **Monitor > Rogue > Unclassified** APs, and click the particular rogue AP name. Choose the option from the drop-down list, as shown in the image.

From the CLI:

```
<#root>

(Cisco Controller) >

config rogue ap ?


classify      Configures rogue access points classification.
friendly      Configures friendly AP devices.
rldp          Configures Rogue Location Discovery Protocol.
ssid          Configures policy for rogue APs advertsing our SSID.
timeout       Configures the expiration time for rogue entries, in seconds.
valid-client  Configures policy for valid clients which use rogue APs.
```

In order to remove a rogue entry manually from the rogue list, navigate to**Monitor > Rogue > Unclassified** APs, and click**Remove**, as shown in the image.
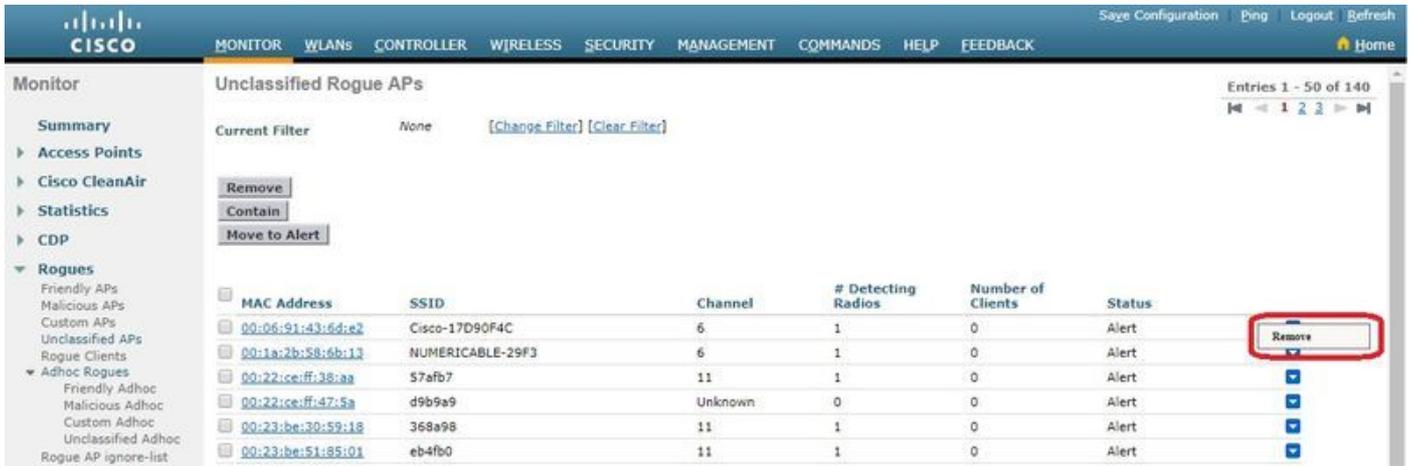
In order to configure a Rogue AP as a friendly AP, navigate to**Security > Wireless Protection Policies > Rogue Policies > Friendly Rogues**and add the rogue MAC address.

The added friendly rogue entries can be verified from**Monitor > Rogues > Friendly Rogue**page, as shown in the image.
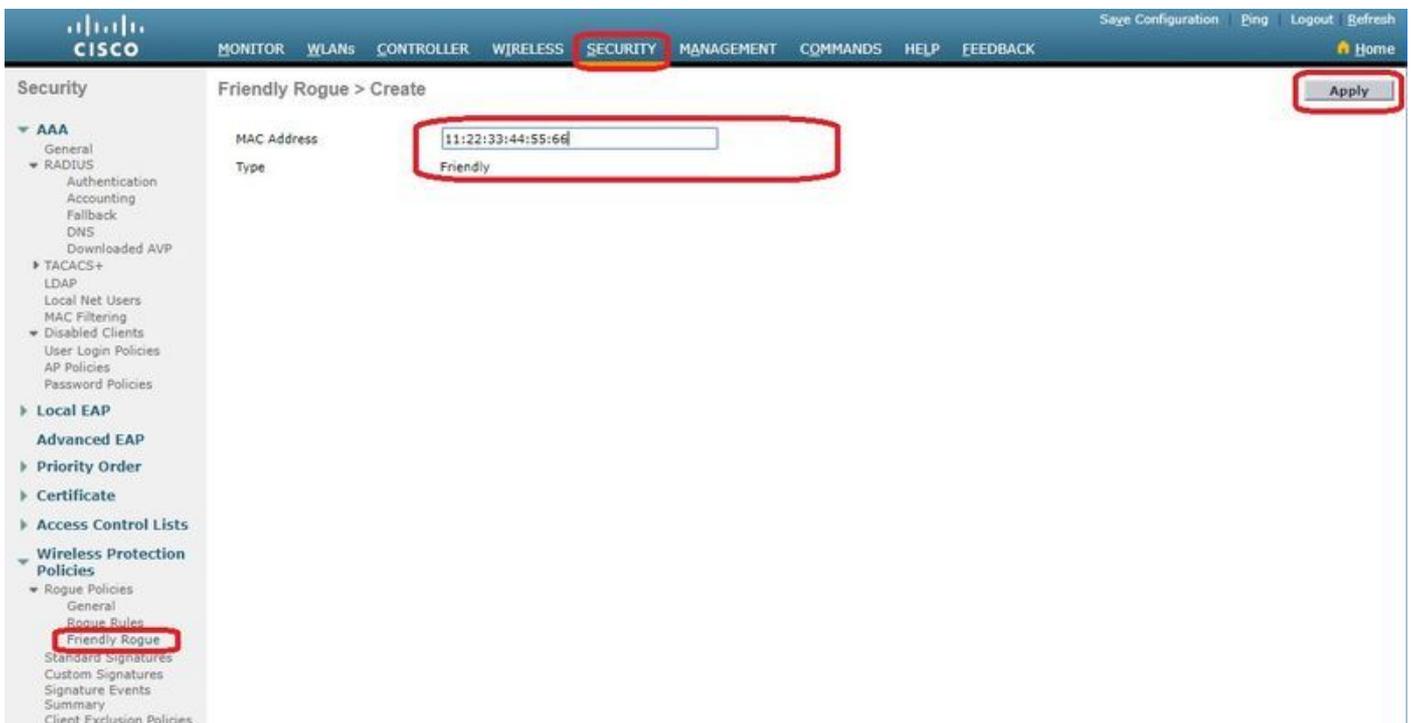
Configure a Rogue Detector AP

In order to configure the AP as a rogue detector through the GUI, navigate to Wireless > All APs. Choose the AP name and change the AP mode as shown in the image.

From the CLI:

```
<#root>

(Cisco Controller) >

config ap mode rogue AP_Managed


Changing the AP's mode cause the AP to reboot.
Are you sure you want to continue? (y/n) y
```

Configure Switchport for a Rogue Detector AP

```
interface GigabitEthernet1/0/5
description Rogue Detector
switchport trunk native vlan 100
switchport mode trunk
```

Note: The native VLAN in this configuration is one that has IP connectivity to the WLC.

Configure RLDP

In order to configure RLDP in the controller GUI, navigate to **Security > Wireless Protection Policies > Rogue Policies > General**.

Monitor Mode APs– Allows only APs in monitor mode to participate in RLDP.

All APs– Local/Flex-Connect/Monitor mode APs participate in the RLDP process.

Disabled– RLDP is not triggered automatically. However, the user can trigger RLDP manually for a particular MAC address through the CLI.

✎ **Note**: Monitor mode AP gets preference over local/Flex-Connect AP to perform RLDP if both of them detect a particular rogue in excess of -85dbm RSSI.

From the CLI:

```
<#root>

(Cisco Controller) >

config rogue ap rldp enable

 ?

alarm-only     Enables RLDP and alarm if rogue is detected
auto-contain   Enables RLDP, alarm and auto-contain if rogue is detected.

(Cisco Controller) >config rogue ap rldp enable alarm-only ?

monitor-ap-only Perform RLDP only on monitor AP
```

RLDP schedule and manually trigger is configurable only through command prompt. To Initiate RLDP manually:

```
<#root>

(Cisco Controller) >

config rogue ap rldp initiate

 ?

<MAC addr> Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).
```

For schedule of RLDP:

```
<#root>

(Cisco Controller) >

config rogue ap rldp schedule ?


add             Enter the days when RLDP scheduling to be done.
delete          Enter the days when RLDP scheduling needs to be deleted.
enable          Configure to enable RLDP scheduling.
disable         Configure to disable RLDP scheduling.


(Cisco Controller) >

config rogue ap rldp schedule add ?


fri             Configure Friday for RLDP scheduling.
sat             Configure Saturday for RLDP scheduling.
sun             Configure Sunday for RLDP scheduling.
mon             Configure Monday for RLDP scheduling.
tue             Configure Tuesday for RLDP scheduling.
wed             Configure Wednesday for RLDP scheduling.
thu             Configure Thursday for RLDP scheduling.
```

RLDP retries can be configured with the command:

```
<#root>

(Cisco Controller) >

config rogue ap rldp retries ?


<count>         Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.
```

Configure Rogue Mitigation

Configure Manual Containment

In order to contain a rogue AP manually, navigate to**Monitor > Rogues > Unclassified**, as shown in the image.

From the CLI:

<#root>

(Cisco Controller) >

config rogue client

?

```
aaa              Configures to validate if a rogue client is a valid client which uses AAA/local database
alert            Configure the rogue client to the alarm state.
contain          Start to contain a rogue client.
delete           Delete rogue Client
mse              Configures to validate if a rogue client is a valid client which uses MSE.
```

(Cisco Controller) >

config rogue client contain 11:22:33:44:55:66

?

```
<num of APs>     Enter the maximum number of Cisco APs to actively contain the rogue client [1-4].
```

✎ **Note**: A particular rogue can be contained with 1-4 APs. By default, the controller uses one AP to contain a client. If two APs are able to detect a particular rogue, the AP with the highest RSSI contains the client regardless of the AP mode.

Auto Containment

To configure auto containment, go to **Security**>**Wireless Protection Policies**>**Rogue Policies**>**General**, and enable all applicable options for your network.

If you want the Cisco WLC to automatically contain certain rogue devices, check those boxes. Otherwise, leave the check boxes unselected, which is the default value.

⚠️ **Warning**: When you enable any of these parameters, the message appears:"Use of this feature has legal consequences. Do you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, the containment of devices on another party's network could have legal consequences.

These are the Auto Contain Parameters:

Parameter	Description
Auto Containment Level	Drop-down list from which you can choose the rogue auto containment level from 1 to 4. You can choose up to four APs for auto containment when a rogue is moved to a contained state through any of the auto containment policies. You can also choose Auto for automatic selection of the number of APs used for auto containment. The Cisco WLC chooses the required number of APs based on the RSSI for effective containment. The RSSI value that is associated with each containment level is as follows: • 1 — 0 to –55 dBm • 2 — –75 to –55 dBm • 3 — –85 to –75 dBm • 4 — Less than –85 dBm
Auto Containment only for Monitor mode APs	Check box that you can select to enable the monitor mode APs for auto containment. The default is disabled state.
Auto Containment on FlexConnect Standalone	Check box that you can select to enable auto containment on FlexConnect APs in the standalone mode. The default is disabled state. When the FlexConnect APs are in the standalone mode, you can enable only the Use our SSID or AdHoc Rogue AP auto containment policies. The containment stops after the standalone AP connects back to the Cisco WLC.
Rogue on Wire	Check box that you enable to automatically contain the rogues that are detected on the wired network. The default is disabled state.
Use our SSID	Check box that you enable to automatically contain those rogues that advertises your network's SSID. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a rogue is detected. The default is disabled state.

Parameter	Description
Valid client on Rogue AP	Check box that you enable to automatically contain a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a rogue is detected. The default is disabled state.
AdHoc Rogue AP	Check box that you enable to automatically contain ad-hoc networks that are detected by the Cisco WLC. If you leave this parameter unselected, the Cisco WLC only generates an alarm when such a network is detected. The default is disabled state.
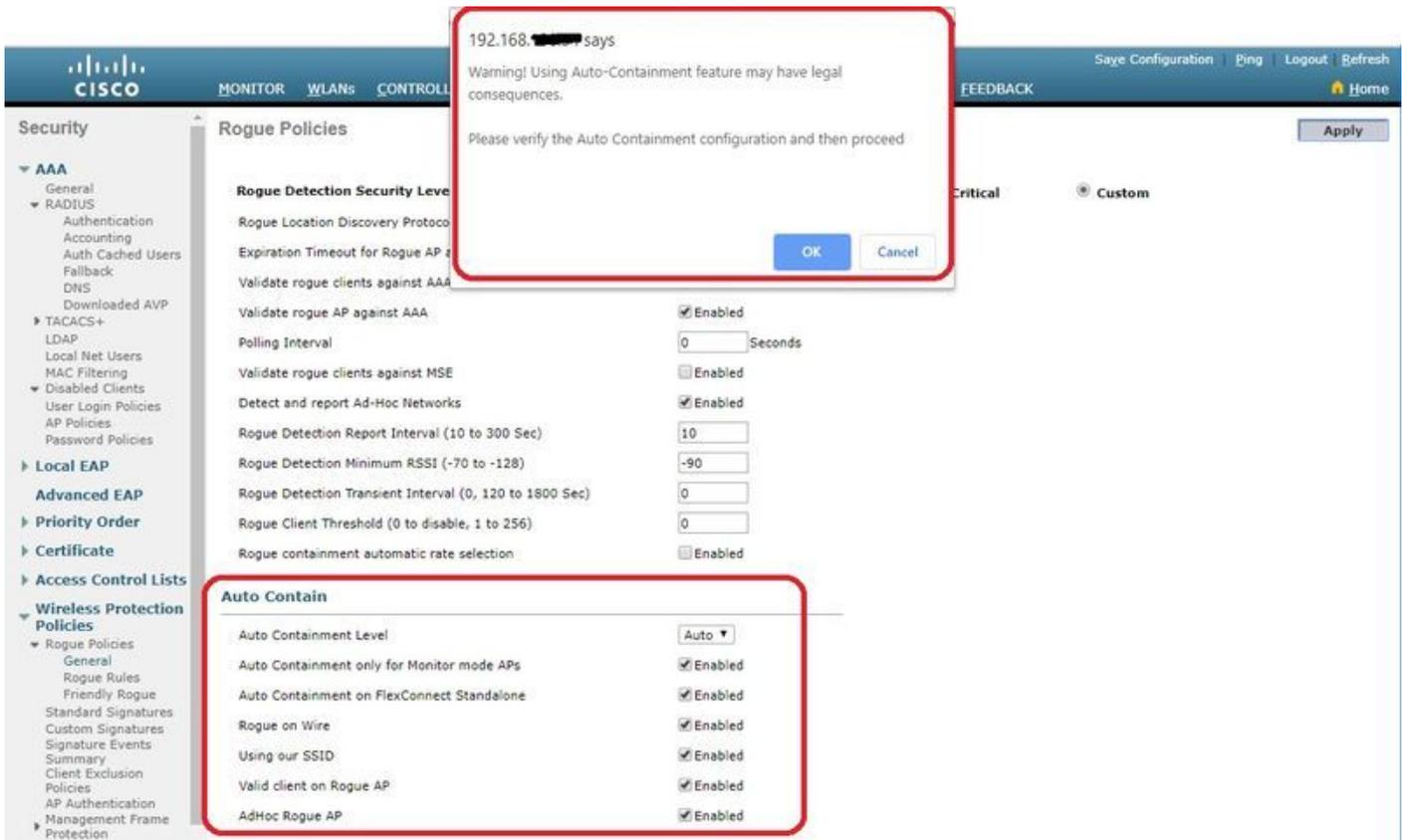
Click Apply to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

From the CLI:

<#root>

(Cisco Controller) >

config rogue adhoc ?

```
alert          Stop Auto-Containment, generate a trap upon detection of the
                 adhoc rogue.
auto-contain   Automatically contain adhoc rogue.
contain        Start to contain adhoc rogue.
disable        Disable detection and reporting of Ad-Hoc rogues.
enable         Enable detection and reporting of Ad-Hoc rogues.
external       Acknowledge presence of a adhoc rogue.
```

```
(Cisco Controller) >

config rogue adhoc auto-contain ?

(Cisco Controller) >

config rogue adhoc auto-contain

 Warning! Use of this feature has legal consequences
          Do you want to continue(y/n) :y
```

With Prime Infrastructure

Cisco Prime Infrastructure can be used to configure and monitor one or more controllers and associated APs. Cisco PI has tools to facilitate large-system monitor and control. When you use Cisco PI in your Cisco wireless solution, controllers periodically determine the client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco PI database.

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

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if theroguestate is **Internal** or **External.**

- If arogueentry is removed after the timeout expires, the controller sends a trap toCisco Prime Infrastructureforrogueaccess points that are categorized as **Malicious** (Alert, Threat) or **Unclassified** (Alert). The controller does not removerogueentries with theseroguestates: **Contained, Contained Pending**, **Internal,** and **External.**

Verify

In order to find rogue details in a controller in the graphical interface, navigate to**Monitor > Rogues**, as shown in the image.

In this page, different classification for rogues are available:

- Friendly APs – APs which are marked as friendly by administrator.

- Malicious APs – APs which are identified as malicious via RLDP or Rogue detector AP.

- Custom APs – APs that are classified as Custom by Rogue Rules.

- Unclassified APs – By default rogue APs are shown as unclassified list in controller.

- Rogue Clients – Clients connected to Rogue APs.

- Adhoc Rogues – Adhoc rogue clients.

- Rogue AP ignore list – As listed through PI.

Note: If WLC and autonomous AP is managed by the same PI, WLC lists automatically this autonomous AP in Rogue AP ignore list. There is no additional configuration required in WLC to enable this feature.

Click a particular rogue entry in order to get the details of that rogue. Here is an example of a Rogue detected on wired network:

From the CLI:

```
<#root>

(Cisco Controller) >

show rogue ap summary




Rogue Detection Security Level................... custom
```

```
Rogue Pending Time............................... 180 secs
Rogue on wire Auto-Contain....................... Disabled
Rogue uses our SSID Auto-Contain................. Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................. 1200
Rogue Detection Report Interval.................. 10
Rogue Detection Min Rssi......................... -90
Rogue Detection Transient Interval............... 0
Rogue Detection Client Num Threshold............. 0
Validate rogue AP against AAA.................... Enabled
Rogue AP AAA validation interval................. 0 secs
Total Rogues(AP+Ad-hoc) supported................ 600
Total Rogues classified.......................... 12
```

MAC Address	Class	State	#Det Aps	#Rogue Clients	#Highest RSSI det-Ap	#RSSI	#Channel
00:a3:8e:db:01:a0	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:a1	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:a2	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-16	13
00:a3:8e:db:01:b0	Malicious	Threat	2	1	00:27:e3:36:4d:a0	-27	40
00:a3:8e:db:01:b1	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40
00:a3:8e:db:01:b2	Unclassified	Alert	2	0	00:27:e3:36:4d:a0	-28	40
50:2f:a8:a2:0a:60	Malicious	Threat	1	2	00:27:e3:36:4d:a0	-66	1
50:2f:a8:a2:0d:40	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-65	11
9c:97:26:61:d2:79	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-89	6
ac:22:05:ea:21:26	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-89	(1,5)
c4:e9:84:c1:c8:90	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-89	(6,2)
d4:28:d5:da:e0:d4	Unclassified	Alert	1	0	00:27:e3:36:4d:a0	-85	13

```
(Cisco Controller) >
```

show rogue ap detailed 50:2f:a8:a2:0a:60

```
Rogue BSSID...................................... 50:2f:a8:a2:0a:60
Is Rogue on Wired Network........................ Yes
Classification................................... Malicious
Classification change by......................... Auto
Manual Contained................................. No
State............................................ Threat
State change by.................................. Auto
First Time Rogue was Reported.................... Tue Jun  4 13:06:55 2019
Last Time Rogue was Reported..................... Wed Jun  5 08:25:57 2019
Reported By
    AP 1
        MAC Address.............................. 00:27:e3:36:4d:a0
        Name..................................... tiagoAPcb.98E1.3DEC
        Radio Type............................... 802.11n2.4G
        SSID..................................... buterfly
        Channel.................................. 1
        RSSI..................................... -64 dBm
        SNR...................................... 29 dB
        Security Policy.......................... WPA2/FT
        ShortPreamble............................ Disabled
        Last reported by this AP................. Wed Jun  5 08:25:57 2019
```

Troubleshoot

If The Rogue Is Not Detected

Verify that rogue detection is enabled on the AP. On the GUI:
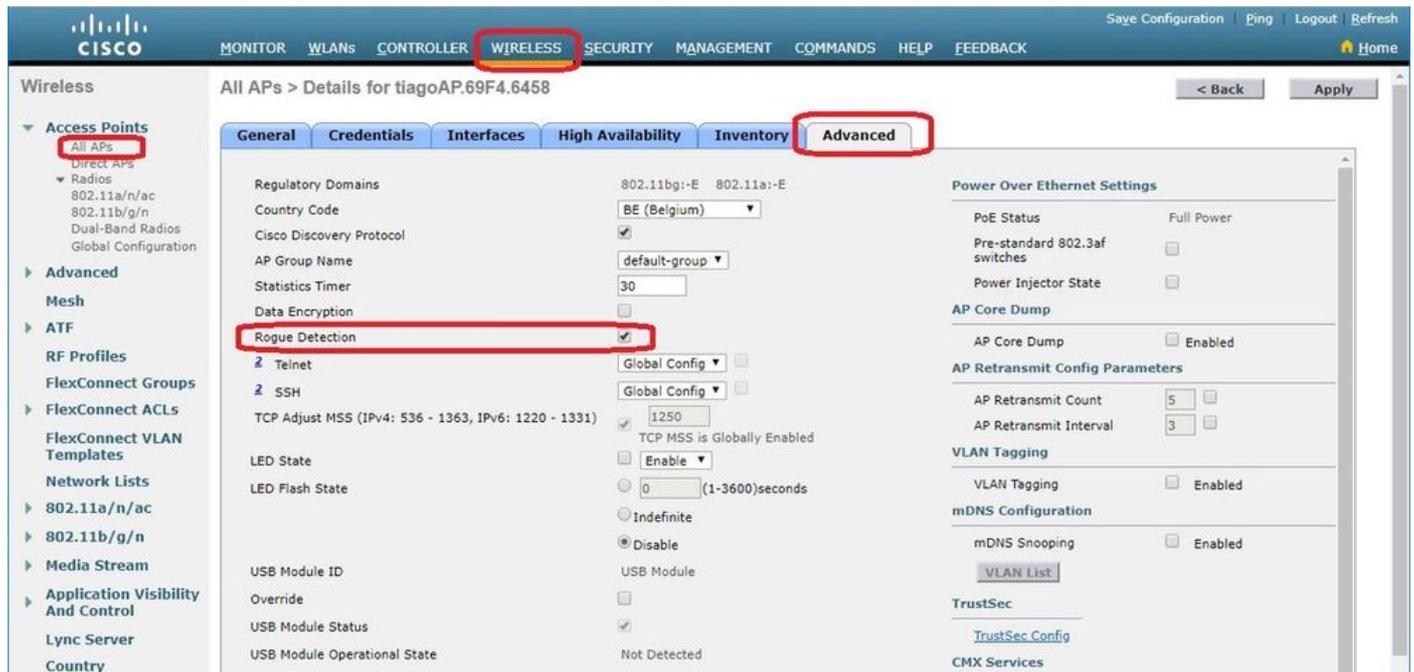
In the CLI:

```
<#root>

(Cisco Controller) >show ap config general tiagoAPcb.98E1.3DEC

Cisco AP Identifier.............................. 13
Cisco AP Name.................................... tiagoAPcb.98E1.3DEC
[...]
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Disabled
AP SubMode ...................................... Not Configured

Rogue Detection ................................. Enabled

Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
KPI not configured ..............................
Logging syslog facility ......................... kern
S/W  Version .................................... 8.8.120.0
Boot  Version ................................... 1.1.2.4
[...]
Power Type/Mode.................................. PoE/Full Power
Number Of Slots.................................. 3
AP Model......................................... AIR-AP3802I-I-K9
AP Image......................................... AP3G3-K9W8-M
Cisco IOS Version................................ 8.8.120.0
Reset Button..................................... Enabled
AP Serial Number................................. FGL2114A4SU
[...]
```

Rogue detection can be enabled on an AP with this command:

```
<#root>

(Cisco Controller) >

config rogue detection enable ?

all          Applies the configuration to all connected APs.
<Cisco AP>   Enter the name of the Cisco AP.
```

A local mode AP scans only country channels/DCA channels and depends on the configuration. If the rogue is in any other channel, the controller is not able to identify the rogue if you do not have monitor mode APs in the network. Issue this command in order to verify:

```
<#root>

(Cisco Controller) >

show advanced 802.11a monitor


Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Mode for Mesh AP Backhaul...... disable


802.11a Monitor Channels...................... Country channels

  802.11a RRM Neighbor Discover Type............ Transparent
  802.11a RRM Neighbor RSSI Normalization....... Enabled
  802.11a AP Coverage Interval.................. 90 seconds
  802.11a AP Load Interval...................... 60 seconds
  802.11a AP Monitor Measurement Interval....... 180 seconds
  802.11a AP Neighbor Timeout Factor............ 20
  802.11a AP Report Measurement Interval........ 180 seconds
```

- Rogue AP does not be broadcast the SSID.

- Ensure the rogue AP MAC address is not added in the friendly rogue list or allowed listed through PI.

- Beacons from the rogue AP are not reachable to the AP that detected rogues. This can be verified by the capture of the packets with a sniffer close to the AP-detector rogue.

- A local mode AP can take up to 9 minutes to detect a rogue (3 cycles 180x3).

- Cisco APs are not able to detect rogues on frequencies like the public safety channel (4.9 Ghz).

- Cisco APs are not able to detect rogues that work on FHSS (Frequency Hopping Spread Spectrum).

Useful Debugs

```
<#root>
```

```
(Cisco Controller) >

debug client <rogue_mac_address>

 (If rogue mac is known)
(Cisco Controller) >

debug client 50:2f:a8:a2:0a:60


(Cisco Controller) >*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Found Rogue AP: 50:2f:a8:a2

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417. Detecti
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or channel wi
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 rg changed rssi prev -64, new -55
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0  rssi -55,
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malici

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule classification :

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=but

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Im

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly


<#root>

(Cisco Controller) >

debug dot11 rogue enable


(Cisco Controller) >*emWeb: Jun 05 08:39:46.828:
Debugging session started on Jun 05 08:39:46.828  for WLC AIR-CT3504-K9   Version :8.8.120.0  SN :FCW22
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for proces

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid b0:72:bf:93:e0:d7 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 50:2f:a8:a2:0a:60 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:a1 src
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b0 src
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b2 src
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Found Rogue AP: 00:a3:8e:db:01:a1 on slot 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue SSID timestmap expired. last update at 0
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  knownApCount=0, totalNumOfRogueE
```

```
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  avgNumOfRogues[0]/10=4, rogueAla
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2  SYNC for Channel (new/old : 40/0) or channel w
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0 l
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 rg changed rssi prev -28, new -28
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1  SYNC for Channel (new/old : 13/0) or channel w
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Updated AP report 00:27:e3:36:4d:a0  rssi -28,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Updated AP report 00:27:e3:36:4d:a0  rssi -16,
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 Receive

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclas

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xff

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for  : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Added Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclass

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Scheduled pending Time 184 and expiry time 1200
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 ssidLen = 0 min = 0 00:a3:8e:db:01:b2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 0 to 1 for rogue AP b0:72:bf:9
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2  Rogue AP: 00:a3:8e:db:01:b2 autocontain = 2 Mo

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Checking Impersonation source 00:a3:8e:db:01:b2
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 Receive

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for  : Class Change by

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7  Send Rogue Info Notificaiton for AP report 00:
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg send new rssi -59
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue After Rule Classification : Class unclass

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0  rssi -59,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 ssidLen = 0 min = 0 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 RadioType: 3 lradInfo->containSlotId = 2 Receive

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 This rogue does not use my ssid. Rogue ssid=
```

```
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue before Rule Classification : Class unconf

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1  Rogue AP: 00:a3:8e:db:01:a1 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrad, cannot apply ro

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule classification : (

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source 00:a3:8e:db:01:a1
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Manual Contained Flag = 0, trustlevel = 1

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Known AP 0 mfp global 0 AP Auth Global 0 mfp Imp

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source b0:72:bf:93:e0:d7
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Known AP 0 mfp global 0 AP Auth Global 0 mfp Imp

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Found Rogue AP: 00:a3:8e:db:01:b0 on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg new Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 New RSSI report from AP 00:27:e3:36:4d:a0  rssi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0  SYNC for Channel (new/old : 40/0) or channel w
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997. Detecti
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 rg changed rssi prev -28, new -26
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or channel wi
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Updated AP report 00:27:e3:36:4d:a0  rssi -26,
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 rg changed rssi prev -65, new -63
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0  rssi -63,
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2 Receiv

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class malici

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 ssidLen = 8 min = 8 00:a3:8e:db:01:b0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel = 7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 This rogue does not use my ssid. Rogue ssid=bli

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0  Rogue AP: 00:a3:8e:db:01:b0 autocontain = 2 Mo

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=but

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60  Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mo

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Imp

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Imp

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Rogue Client IPv6 addr: Not known
```

```
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue Client ssid: blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 New AP report 00:27:e3:36:4d:a0  rssi -37, snr
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 rgc change from -38 RSSI -37
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 rgc change from -39 RSSI -39
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Updated AP report 00:27:e3:36:4d:a0 rssi -37, sn
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Updated AP report 00:27:e3:36:4d:a0 rssi -39, sn
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 APF processing Rogue Client: on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New AP report 00:27:e3:36:4d:a0  rssi -62, snr
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rgc change from -61 RSSI -62
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -62, sn
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 1 to 2 for rogue AP b0:72:bf:9
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Deleting Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Freed rogue client table for Rogue AP at 0xfff0

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg delete for Rogue AP: b0:72:bf:93:e0:d7
```

Expected Trap Logs

Once a rogue is detected/removed from the rogue list:

0	Wed Jun 5 09:01:57 2019	Rogue client: b4:c0:f5:2b:4f:90 is **detected** by 1 APs Rogue Client Bssid: a6:b1:e9:f0:e8:41, State: Alert, Last detecting AP :00:27:e3:36:4d:a0 Rogue Client gateway mac 00:00:00:02:02:02.
1	Wed Jun 5 09:00:39 2019	Rogue AP : 9c:97:26:61:d2:79 **removed** from Base Radio MAC : 00:27:e3:36:4d:a0 Interface no:0(802.11n(2.4 GHz))
2	Wed Jun 5 08:53:39 2019	Rogue AP : 7c:b7:33:c0:51:14 **removed** from Base Radio MAC : 00:27:e3:36:4d:a0 Interface no:0(802.11n(2.4 GHz))
3	Wed Jun 5 08:52:27 2019	Rogue client: fc:3f:7c:5f:b1:1b is **detected** by 1 APs Rogue Client Bssid: 50:2f:a8:a2:0a:60, State: Alert, Last detecting AP :00:27:e3:36:4d:a0 Rogue Client gateway mac 00:26:44:73:c5:1d.
4	Wed Jun 5 08:52:17 2019	Rogue AP : d4:28:d5:da:e0:d4 **removed** from Base Radio MAC : 00:27:e3:36:4d:a0 Interface no:0(802.11n(2.4 GHz))

Recommendations

1. Configure the channel scan to all channels if you suspect potential rogues in your network.

2. The number and location of rogue detector APs can vary from one per floor to one per building and depends on the layout of the wired network. It is advisable to have at least one rogue detector AP in each floor of a building. Because a rogue detector AP requires a trunk to all layer 2 network broadcast domains that are to be monitored, placement is dependent on the logical layout of the network.

If the Rogue Is Not Classified

Verify the rogue rules are configured properly.

Useful Debugs

```
<#root>

(Cisco Controller) >

debug dot11 rogue rule enable



(Cisco Controller) >*emWeb: Jun 05 09:12:27.095:
Debugging session started on Jun 05 09:12:27.095 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN :FCW2245M0

(Cisco Controller) >
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr

*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr

*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40

Rogue Classification:malicious, RuleName:TestRule, Rogue State:Containment Pending



*apfRogueTask_3: Jun 05 09:13:27.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr

*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16, maxRssiLr
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious, RuleName:TestRu

*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15, maxRssiLr
```

Recommendations

If you have known rogue entries, add them in the friendly list or enable validation with AAA and ensure known client entries are there in the Authentication, Authorization and Accounting (AAA) database.

RLDP Does Not Locate Rogues

- If the rogue is in the DFS channel, RLDP does not work.
- RLDP works only if the rogue WLAN is open and DHCP is available.
- If the local mode AP serves the client in the DFS channel, it does not participate in RLDP process.

- RLDP is not supported on AP model 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs.

Useful Debugs

```
<#root>

(Cisco Controller) >

debug dot11 rldp enable



!--- RLDP not available when AP used to contain only has invalid channel for the AP country code

*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Rogue detected slot :0 Rogue contains SlotId :2
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61

Invalid channel 1 for the country IL for AP 00:27:e3:36:4d:a0


*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Waiting for ARLDP request

!--- ROGUE detected on DFS channel

*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Received request to detect Rogue
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Rogue detected slot :1 Rogue contains SlotId :1
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e

Our AP 00:27:e3:36:4d:a0 detected this rogue on a DFS Channel 100


*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Waiting for ARLDP request

!--- RLDP is not supported on AP model 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series

*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Received request to detect Rogue
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a

Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP1852I-E-K9


*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: Waiting for ARLDP request

!--- Association TO ROGUE AP

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP
*apfRLDP: Jun 05 15:02:49.602: Rogue detected slot :0 Rogue contains SlotId :0
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61
```

Monitor Mode AP found b4:de:31:a4:e0:30 with RSSI -61

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 found closest monitor AP b4:de:31:a4:e0:30 slot = 0, c

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Found RAD: 0xffd682b5b8, slotId = 0, Type=1

*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 AP b4:de:31:a4:e0:30 Client b4:de:31:a4:e0:31 Slot = 0
*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 WARNING!!!!! mscb already exists!

*apfRLDP: Jun 05 15:02:50.102: b4:de:31:a4:e0:31 In rldpSendAddMobile:724 setting Central switched to Th
*apfRLDP: Jun 05 15:02:50.302: 50:2f:a8:a2:0a:61

rldp started association, attempt 1

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP Sta

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 rldp started association, attempt 2
*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP Sta

*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 rldp started association, attempt 3
*apfOpenDtlSocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.
*apfOpenDtlSocket: Jun 05 15:03:00.808:

50:2f:a8:a2:0a:61 RLDP state RLDP_ASSOC_DONE

 (3).

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Successfully associated with rogue: 50:2F:A8:A2:0A:61

!--- Attempt to get ip from ROGUE

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Starting dhcp

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61

Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   htype: Ethernet

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   hlen: 6

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   hops: 1

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   secs: 0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   flags: 0x0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   my IP: 0.0.0.0

```
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31      gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31    options:

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31          DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:00.870: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:00.870:        [0000] 02 40

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31           host name: RLDP

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         htype: Ethernet

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          hlen: 6

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          hops: 1

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31           xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          secs: 0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         flags: 0x0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31       hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31     client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31     server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31    gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31          DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:10.878: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:10.878:        [0000] 02 40

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31           host name: RLDP

*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         htype: Ethernet

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          hlen: 6
```

```
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          hops: 1

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31           xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          secs: 0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         flags: 0x0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31     gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:20.885: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:20.885:      [0000] 02 40

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          host name: RLDP

*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP 50:2f:a8:a2:0a:61

!--- RLDP DHCP fails as there is no DHCP server providing IP address

*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCP FAILED state for rogue  50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 DHCP failed
*apfRLDP: Jun 05 15:03:20.885: Waiting for ARLDP request
```

Recommendations

1. Initiate RLDP manually on suspicious rogue entries.

2. Schedule RLDP periodically.

3. RLDP can be deployed on local or monitor mode APs. For most scalable deployments, and to eliminate any impact on client service, RLDP is to be deployed on monitor mode APs when possible. However, this recommendation requires that a monitor mode AP overlay be deployed with a typical ratio as 1 monitor mode AP for every 5 local mode APs. APs in Adaptive wIPS monitor mode can also be leveraged for this task.

Rogue Detector AP

Rogue entry in a rogue detector can be seen with this command in the AP console. For wired rogues, the flag moves to set status.

```
<#root>

tiagoAP.6d09.eff0#
```

```
show capwap rm rogue detecto
```

```
r
 LWAPP Rogue Detector Mode
  Current Rogue Table:
  Rogue hindex = 0: MAC 502f.a8a2.0a61,
```

```
flag = 0
```

```
, unusedCount = 1
  Rogue hindex = 0: MAC 502f.a8a2.0a60,
```

```
flag = 0
```

```
, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d41,
```

```
flag = 0
```

```
, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d40,
```

```
flag = 0
```

```
, unusedCount = 1
```

```
!--- once rogue is detected on wire, the flag is set to 1
```

Useful Debug Commands in an AP Console

<#root>

Rogue_Detector#

```
debug capwap rm rogue detector
```

```
*Jun 05 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
```

```
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 05 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 05 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

Rogue Containment

Expected Debugs

<#root>

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Updated AP report b4:de:31:a4:e0:30 rssi -33, s
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Looking for Rogue 00:a3:8e:db:01:b0 in known AP
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue AP 00:a3:8e:db:01:b0 is not found either
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6 ContainmentLe

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected by AP: b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RadioType: 2 lradInfo->containSlotId = 1 Receiv

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue before Rule Classification :
```

Class malicious, Change by Auto State Contained Change by Auto

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue doesnt qualify for rule classification : 

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel = 6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0
```

Rogue AP: 00:a3:8e:db:01:b0 autocontain = 1 Mode = 6

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 apfRogueMode : 6 apfRogueContainmentLevel : 4 l

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 1 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Skipping xor radio for 1 band and cont slotid 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 0 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 2 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected on detected slot 0 contains slot
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 1 channels to try containment for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -28
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0 RSSI = -31
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC b4:de:31:a4:e0:30 RSSI = -33
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -28 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI = -31 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC b4:de:31:a4:e0:30 RSSI = -33 t
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0
```

Contains rogue with 3 container AP(s).Requested containment level : 4

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Checking Impersonation source 00:a3:8e:db:01:b0
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Imp
```

Recomendations

1. The local/Flex-Connect mode AP can contain 3 devices at a time per radio, and the monitor mode AP can contain 6 devices per radio. As a result, ensure the AP does not already contain the maximum number of devices permitted. In this scenario, the client is in a containment pending state.

2. Verify auto containment rules.

Conclusion

Rogue detection and containment within the Cisco centralized controller solution is the most effective and least intrusive method in the industry. The flexibility provided to the network administrator allows for a more customized fit that can accommodate any network requirements.

Related Information

- **Cisco Wireless Controller Configuration Guide, Release 8.8 - Rogue Management**
- **Cisco Wireless LAN Controller (WLC) Configuration Best Practices**
- **WLC 3504 Release 8.5 Deployment Guide**
- **Cisco 5520 Wireless LAN Controller Deployment Guide**
- **Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.8.120.0**