解决统一无线网络中的欺诈检测和缓解

目录

简介

本文档介绍Cisco无线网络上的欺诈检测和缓解。

无线网络是对有线网络的延伸，它提高了工作人员的工作效率，便于工作人员访问信息。但是，未授权的无线网络带来额外的安全隐患。对有线网络上的端口安全问题关注较少，并且无线网络相对于有线网络来说，更易于推广。因此，如果员工将自己的接入点（思科或非思科）带入安全可靠的无线或有线基础设施，并允许未经授权的用户访问此安全网络，则很容易危及安全网络。

恶意程序检测允许网络管理员监控和排除此类安全问题。思科统一网络架构提供欺诈检测的方法，可实现完整的欺诈识别和遏制解决方案，而无需昂贵且难以证明的重叠网络和工具。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco无线局域网控制器.
- Cisco Prime基础设施。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本8.8.120.0的思科统一无线局域网控制器（5520、8540和3504系列）。
- Wave 2 APs 1832、1852、2802和3802系列。
- Wave 1 AP 3700、2700和1700系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

欺诈概述

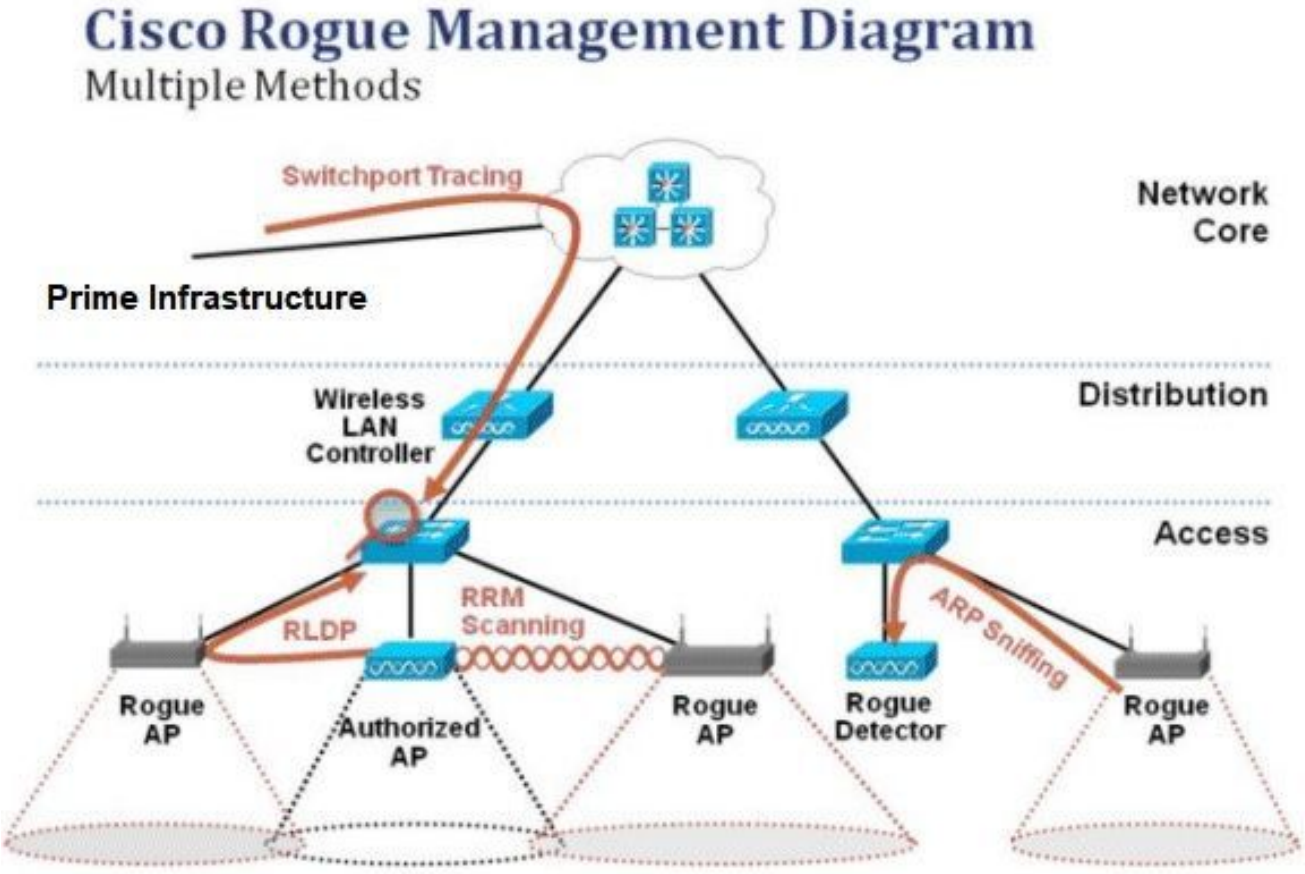
共享您的频谱且不受您管理的任何设备均可被视为欺诈设备。流氓会在以下情况下变得危险：

- 设置使用与您的网络（蜜罐）相同的服务集标识符(SSID)时。
- 在有线网络上检测到时。
- 临时的流氓。
- 通常由外部人员以恶意目的设置。

最佳实践是使用欺诈检测将安全风险降至最低，例如在企业环境中。但是，在某些情况下不需要进行恶意软件检测，例如，在全市范围内的Office Extend Access Point(OEAP)部署以及户外。使用室外网状AP检测恶意程序几乎不会产生任何价值，同时会使用资源进行分析。最后，评估（或完全避免）流氓自动遏制至关重要，因为如果任其自动运行，存在潜在的法律问题和责任。

思科统一无线网络(UWN)解决方案中的欺诈设备管理有三个主要阶段：

- 检测 — 无线电资源管理(RRM)扫描用于检测欺诈设备的存在。
- 分类 — 欺诈位置发现协议(RLDP)、欺诈检测器（仅限第1波AP）和交换机端口跟踪用于识别欺诈设备是否连接到有线网络。欺诈分类规则还有助于根据欺诈特征将其过滤为特定类别。
- 缓解 — 交换机端口关闭、欺诈位置和欺诈遏制用于跟踪其物理位置并消除欺诈设备的威胁。

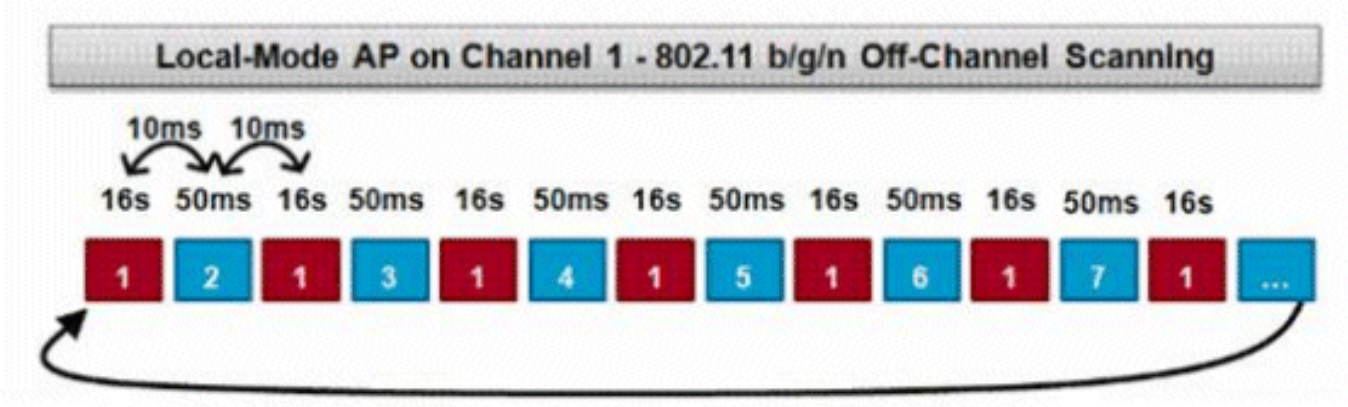


入侵检测

非法设备基本上是共享您的频谱但不受您控制的任何设备。这包括欺诈接入点、无线路由器、欺诈客户端和欺诈对等网络。Cisco UWN使用多种方法来检测基于Wi-Fi的恶意设备，例如信道外扫描和专用监控模式功能。Cisco Spectrum Expert还可用于识别不基于802.11协议的欺诈设备，例如蓝牙网桥。

信道外扫描

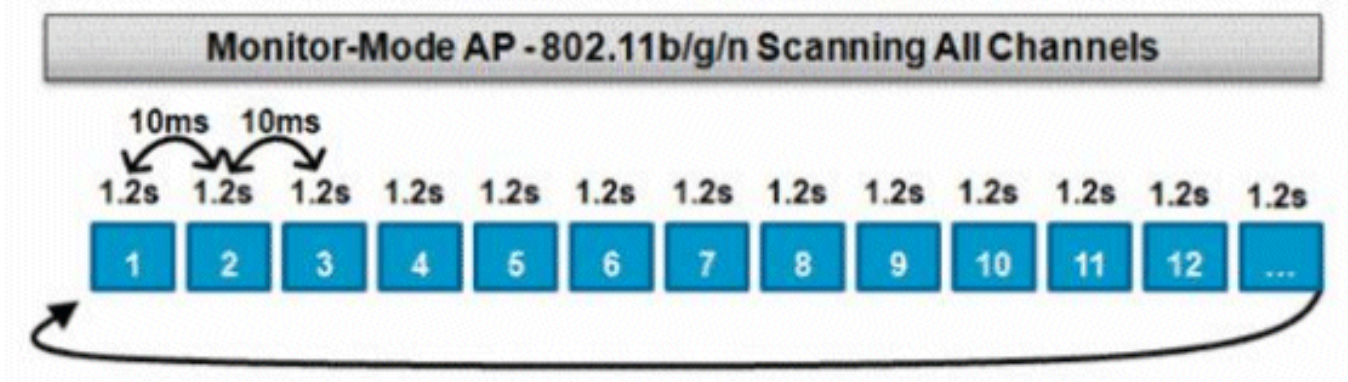
此操作由本地和Flex-Connect（在连接模式下）模式AP执行，并采用时间分割技术，允许使用同一无线电进行客户端服务和信道扫描。由于每16秒切换到信道外50ms的时间段，默认情况下，AP仅花费少量的时间不为客户端提供服务。另请注意，会出现10ms的信道更改间隔。在默认扫描间隔180秒内，每个2.4Ghz FCC信道(1−11)至少扫描一次。对于其他管制域（例如ETSI），AP处于信道外状态的时间百分比略高。信道列表和扫描间隔都可以在RRM配置中调整。这将性能影响限制为最大1.5%，并且算法中内置了智能功能，可在需要传送高优先级QoS帧（例如语音）时暂停扫描。



此图描述了2.4GHz频段中本地模式AP的信道外扫描算法。如果AP有一个类似操作，则在5GHz无线电上并行执行操作。每个红色方块代表在AP主信道上花费的时间，而每个蓝色方块代表为扫描目的在相邻信道上花费的时间。

监控模式扫描

此操作由监控模式和自适应wIPS监控模式AP执行，它们利用100%的无线电时间扫描各个频段中的所有信道。这样可以加快检测速度，并且每个信道可以花费更多时间。监控模式AP在检测欺诈客户端方面也远远优于其他模式，因为它们可以更全面地了解每个通道中发生的活动。



此图描述了2.4GHz频段中监控模式AP的信道外扫描算法。如果AP有一个类似操作，则在5GHz无线电上并行执行操作。

本地模式和监控模式比较

本地模式AP在WLAN客户端服务与扫描通道之间拆分其周期以查找威胁。因此，本地模式AP在遍历所有信道时花费的时间更长，而且它花在收集任何特定信道上的数据上的时间更少，因此客户端操作不会中断。因此，欺诈和攻击检测时间较长（3至60分钟），与监控模式AP相比，可检测到的空中攻击范围更小。

此外，对突发流量（如恶意客户端）的检测确定性要低得多，因为AP必须在传输或接收流量的同时处于流量的信道上。这变成了一种可能性的练习。监控模式AP将所有周期用于扫描信道，以查找恶意程序和空中攻击。监控模式AP可同时用于自适应wIPS、位置（情景感知）服务和其他监控模式服务。

部署监控模式AP时，检测时间更短。当监控模式AP额外配置了自适应wIPS时，可以检测到更广泛的空中威胁和攻击。

本地模式AP	监控模式AP
为客户端提供分时离通道扫描 在每个信道上侦听50毫秒 可配置为扫描： • 所有信道 • 国家/地区渠道（默认） • DCA通道	专用扫描 侦听每个信道上的1.2秒 扫描所有通道

欺诈识别

如果本地、灵活连接或监控模式AP侦听来自欺诈设备的探测响应或信标，则此信息通过CAPWAP传送到无线LAN控制器(WLC)进行处理。为了防止误报，使用了多种方法来确保其他基于Cisco的受管AP不被识别为欺诈设备。这些方法包括移动组更新、RF邻居数据包和允许通过Prime基础设施(PI)列出的友好AP。

恶意记录

虽然控制器的恶意设备数据库仅包含当前检测到的恶意程序集，但PI还包括一个事件历史记录，并记录不再发现的恶意程序。

恶意程序详细信息

CAPWAP AP在信道外传输50ms，以侦听恶意客户端、监控噪声和信道干扰。所有检测到的恶意客户端或 AP 被发送到用于收集此信息的控制器：

- 恶意 AP MAC 地址
- 检测到欺诈的AP的名称
- 恶意程序连接的客户端 MAC 地址
- 安全策略
- 报头
- 信噪比 (SNR)
- 接收信号强度指示符 (RSSI)
- 欺诈检测通道
- 检测到欺诈的无线电
- 欺诈SSID（如果广播欺诈SSID）
- 非法IP地址
- 第一次和最后一次报告欺诈设备
- 通道宽度

导出欺诈事件

为了将恶意事件导出到第三方网络管理系统(NMS)进行存档，WLC允许添加额外的SNMP陷阱接收器。当控制器检测到欺诈或清除欺诈时，包含此信息的陷阱会传送到所有SNMP陷阱接收器。通过SNMP导出事件时需要注意的一点是，如果多个控制器检测到相同的欺诈设备，NMS会看到重复的事件，因为关联仅在PI完成。

欺诈记录超时

欺诈AP添加到WLC记录后，它将一直保留在该记录中，直到不再显示。在用户可配置超时（默认值为1200秒）之后，_unclassified_category中的欺诈已过期。

其他状态(如_Contained_and_Friendly_)中的恶意程序会持续存在，以便重新出现时对其应用适当的分类。

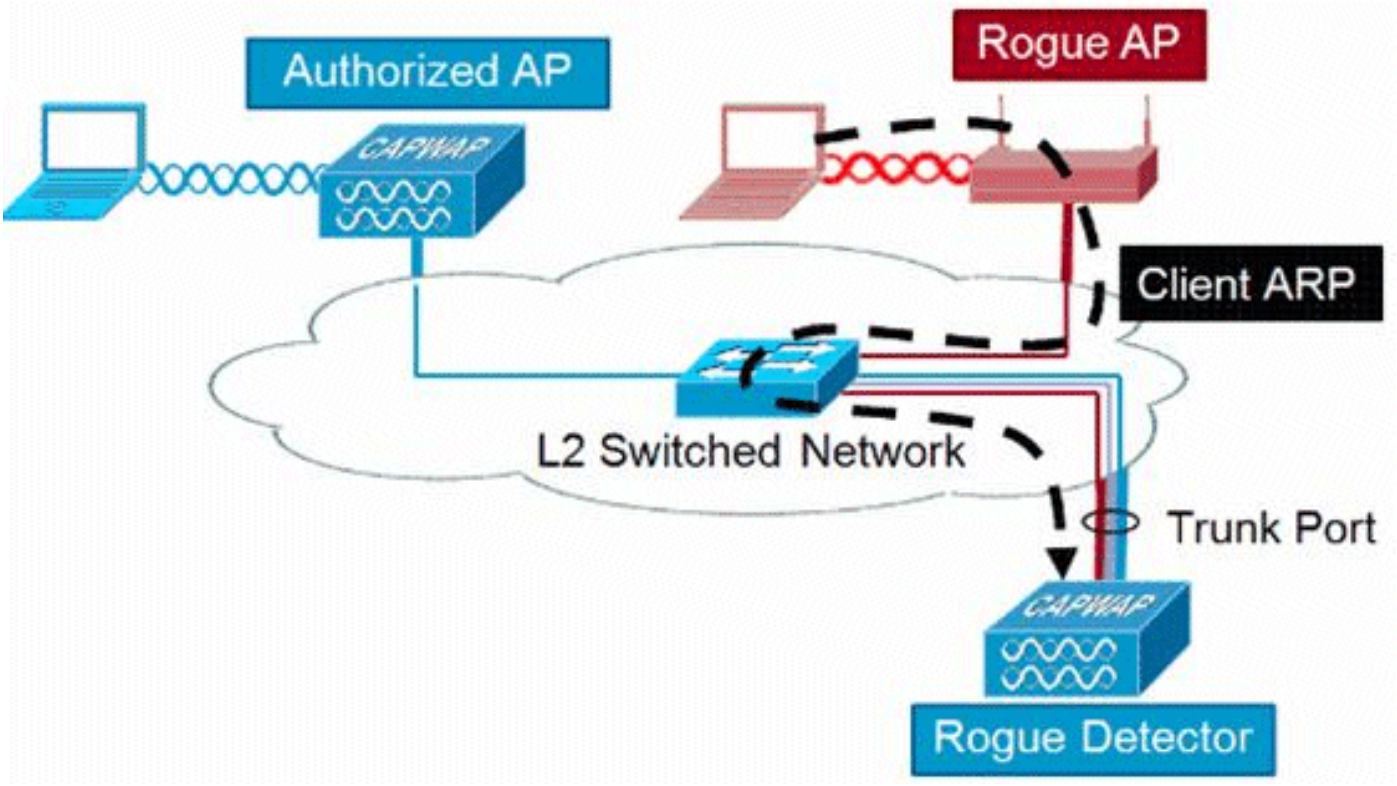
对于可在控制器平台之间变化的恶意记录，有一个最大数据库大小：

- 3504 — 检测和遏制多达600个欺诈AP和1500个欺诈客户端
- 5520 — 检测和遏制最多24000欺诈AP和32000欺诈客户端
- 8540 — 检测和遏制最多24000欺诈AP和32000欺诈客户端

欺诈检测器AP

恶意检测器AP旨在将空中侦听的恶意信息与从有线网络获取的ARP信息相关联。如果通过空中侦听到作为欺诈AP或客户端的MAC地址，并且也在有线网络上侦听到该地址，则确定该欺诈位于有线网络中。如果检测到欺诈无线接入点位于有线网络上，则该欺诈AP的警报严重性将提高到_critical_。欺诈检测器AP在识别使用NAT的设备背后的欺诈客户端时失败。

当恶意 AP 有某种形式的认证（WEP 或 WPA）时使用此方法。当欺诈AP上配置了身份验证形式时，轻量AP无法关联，因为它不知道欺诈AP上配置的身份验证方法和凭证。



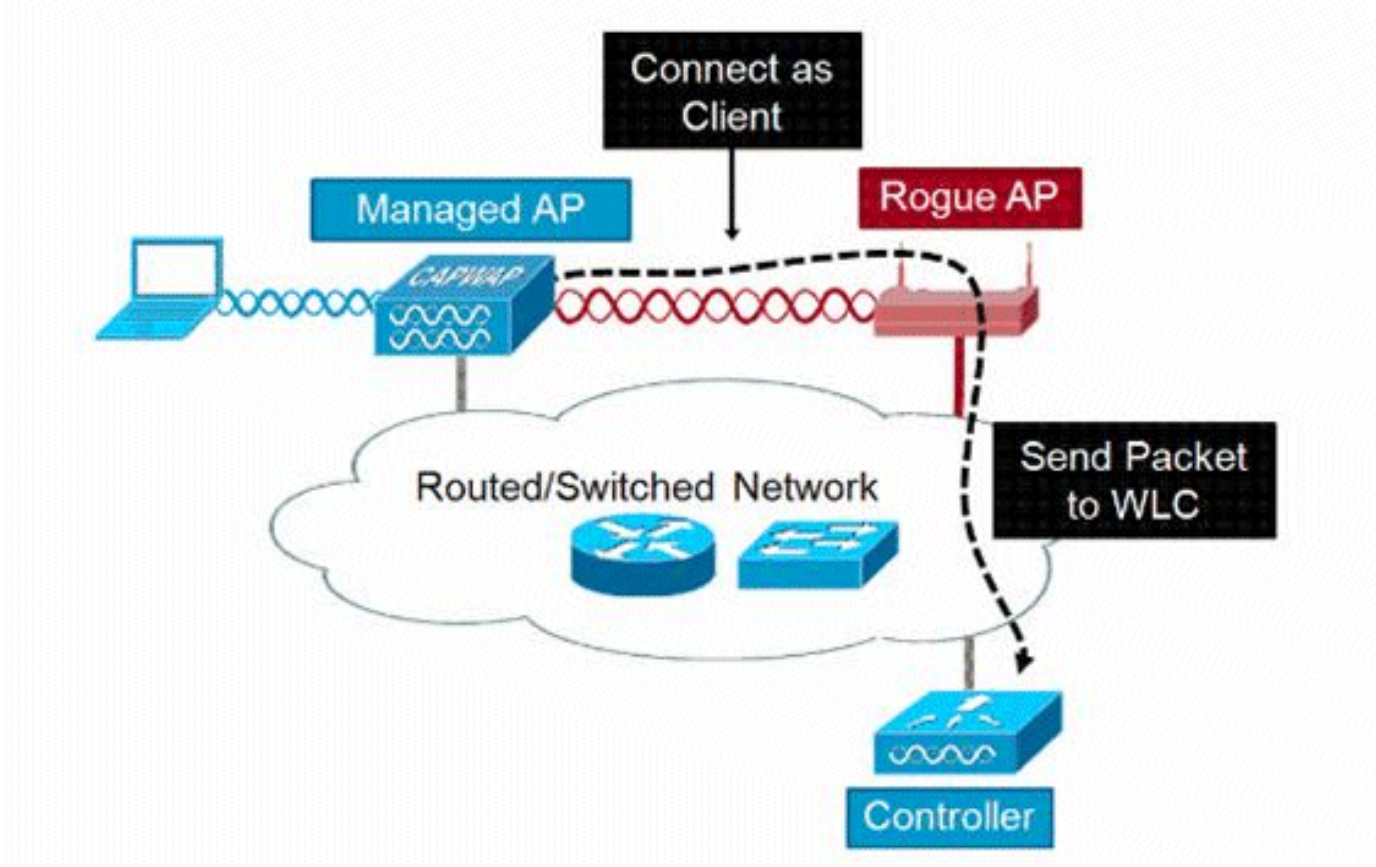
注意：只有第1波AP可配置为欺诈检测器。

可扩展性注意事项

欺诈检测器AP可检测多达500个恶意客户端和500个恶意客户端。如果欺诈检测器放置在中继上非法设备过多，则会超出这些限制，从而导致问题。为防止发生这种情况，请将恶意检测器AP保留在网络的分布层或接入层。

RLDP

RLDP的目的是确定特定欺诈AP是否连接到有线基础设施。此功能基本上使用最近的AP作为无线客户端连接到非法设备。在作为客户端的连接之后，将发送一个包含WLC目标地址的数据包，以评估AP是否连接到有线网络。如果检测到欺诈无线接入点位于有线网络上，则该欺诈AP的警报严重性将提升为严重。



RLDP算法如下所示：

1. 使用信号强度值确定离欺诈设备最近的统一AP。
2. 然后，AP将作为WLAN客户端连接到欺诈，在其超时之前尝试三次关联。
3. 如果关联成功，则AP使用DHCP获取IP地址。
4. 如果获取了IP地址，则AP（充当WLAN客户端）会向每个控制器IP地址发送UDP数据包。
5. 如果控制器收到来自客户端的甚至一个RLDP数据包，该恶意软件会标记为在线且严重性为critical。

注意：如果在控制器网络和恶意设备所在的网络之间设置了过滤规则，则RLDP数据包无法到

达控制器。

RLDP注意事项

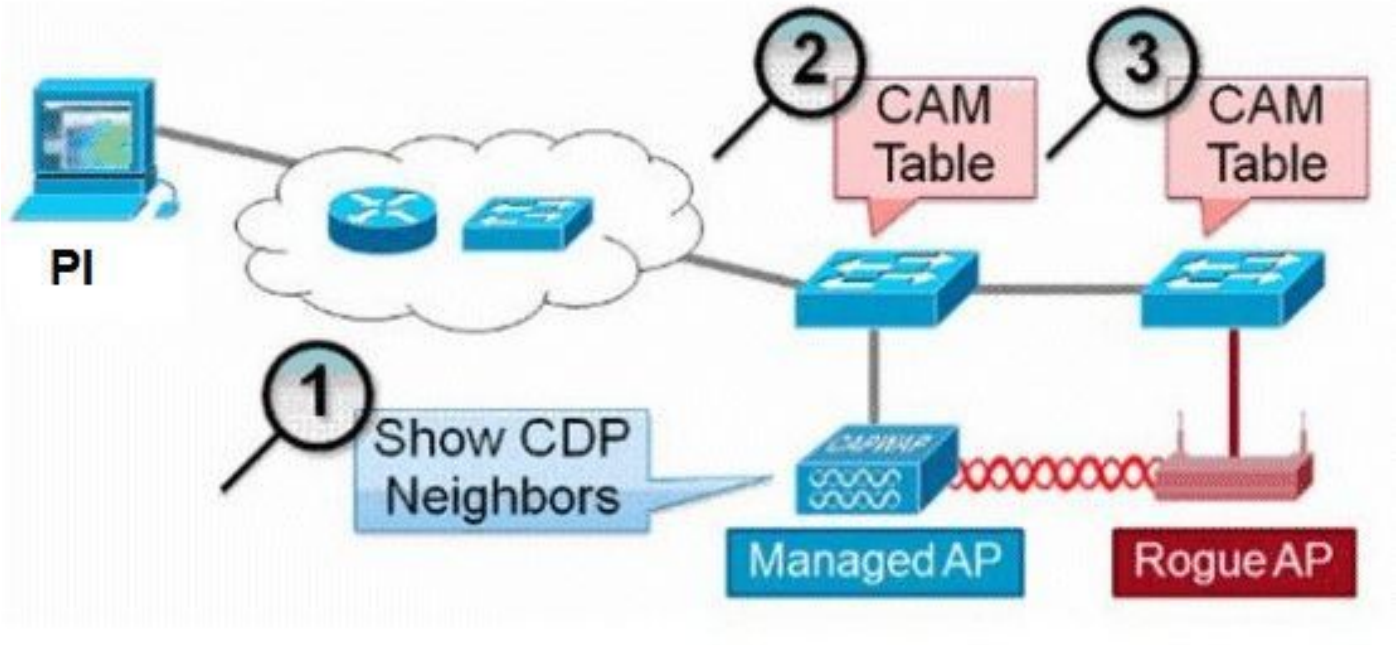
- RLDP仅适用于在禁用身份验证和加密的情况下广播其SSID的开放欺诈AP。
- RLDP要求充当客户端的受管AP能够通过DHCP在欺诈网络上获取IP地址
- 手动RLDP可用于多次尝试和对欺诈进行RLDP跟踪。
- 在RLDP进程中，AP无法为客户端提供服务。这会对本地模式AP的性能和连接产生负面影响。
- RLDP不会尝试连接到在5GHz DFS信道中运行的欺诈AP。

交换机端口跟踪

交换机端口跟踪是一种恶意AP缓解技术。虽然交换机端口跟踪是在PI上启动的，但它同时利用CDP和SNMP信息来跟踪流氓到网络中的特定端口。

为了运行交换机端口跟踪，必须将网络中的所有交换机使用SNMP凭证添加到PI。虽然只读凭证能够识别非法设备所在的端口，但读写凭证允许PI也关闭端口，因此它包含威胁。

目前，此功能仅适用于运行启用CDP的Cisco IOS®的Cisco交换机，并且还必须在托管AP上启用CDP。



交换机端口跟踪的算法如下所示：

1. PI查找最近的AP，它通过空中检测非法AP，并检索其CDP邻居。
2. 然后，PI使用SNMP检查邻居交换机中的CAM表，查找正匹配以识别恶意程序位置。
3. 正匹配基于完全欺诈MAC地址、+1/−1欺诈MAC地址、任何欺诈客户端MAC地址或基于MAC地址中固有的供应商信息的OUI匹配。
4. 如果在最近的交换机上找不到正匹配项，则PI会在最远两跳的相邻交换机中继续搜索（默认情况下）。

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

欺诈分类

默认情况下，Cisco UWN检测到的所有恶意程序均被视为未分类。如图所示，恶意程序可以按照包括RSSI、SSID、安全类型、打开/关闭网络以及客户端数量的多个标准进行分类：

欺诈分类规则

通过恶意分类规则，您可以定义一组条件，将恶意程序标记为恶意或友好。这些规则在PI或WLC上

配置，但在发现新的恶意程序时，它们始终在控制器上执行。

有关无线局域网控制器(WLC)和Prime基础设施(PI)中欺诈规则的详细信息，请阅读文档基于规则的欺诈分类。

HA事实

如果手动将任何非法设备移至包含状态（任何类）或友好状态，则此信息存储在备用Cisco WLC闪存中；但是，数据库不会更新。当发生HA切换时，加载来自先前备用Cisco WLC闪存的恶意列表。

在“高可用性”场景中，如果欺诈检测安全级别设置为“高”或“严重”，则备用控制器上的欺诈计时器仅在欺诈检测挂起稳定时间（300秒）后启动。因此，备用控制器上的活动配置仅在300秒后才会反映。

Flex-Connect事实

处于连接模式的FlexConnect AP（已启用欺诈检测）从控制器获取包含列表。如果在控制器中设置了自动包含SSID和自动包含对等，则这些配置将设置为处于连接模式的所有FlexConnect AP，并且AP将其存储在其内存中。

当FlexConnect AP移至独立模式时，将执行以下任务：

- 由控制器设置的遏制会继续。
- 如果FlexConnect AP检测到任何欺诈AP的SSID与基础设施SSID（在FlexConnect AP所连接的控制器中配置的SSID）的SSID相同，则在进入独立模式之前，如果从控制器启用了“自动包含SSID”(auto contain SSID)，则限制会启动。
- 如果FlexConnect AP检测到任何对等欺诈，当控制器处于连接模式时，如果从控制器启用自动包含对等模式，则遏制开始。

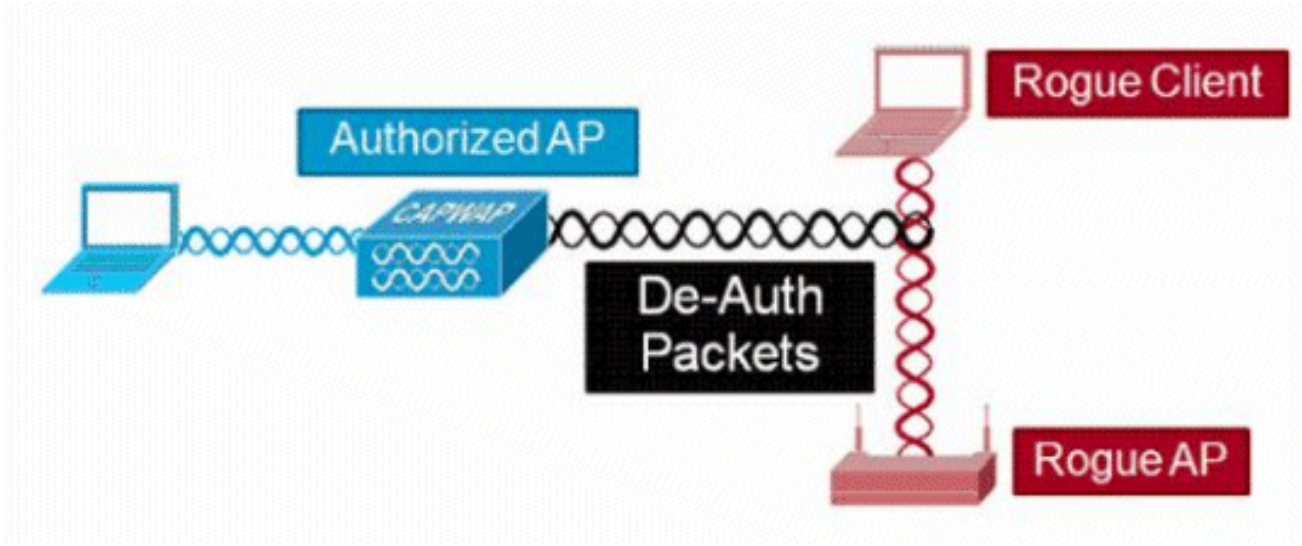
当独立FlexConnect AP返回连接模式时，将执行以下任务：

- 所有遏制都会清除。
- 由控制器发起的遏制会接管控制权。

欺诈缓解

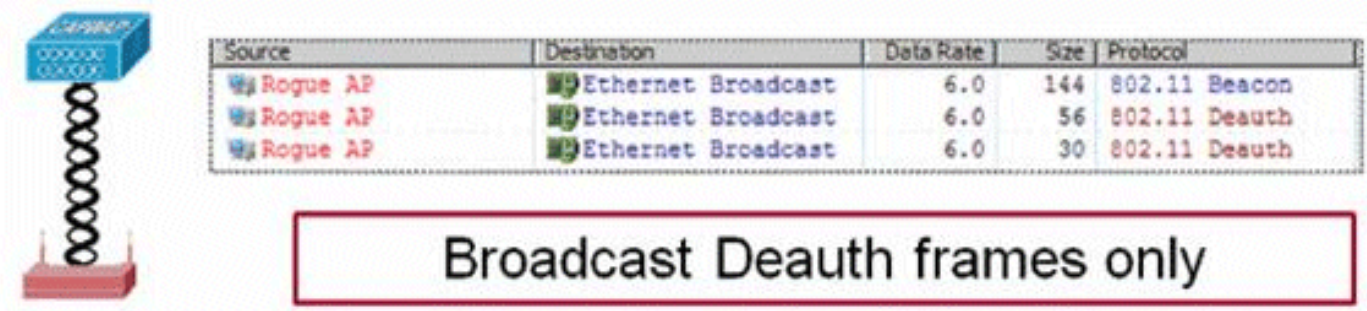
非法控制

遏制是一种使用空中数据包来临时中断欺诈设备上的服务直到可以实际移除的方法。遏制使用欺诈AP的欺骗源地址来欺骗解除身份验证数据包，以便启动关联的任何客户端。

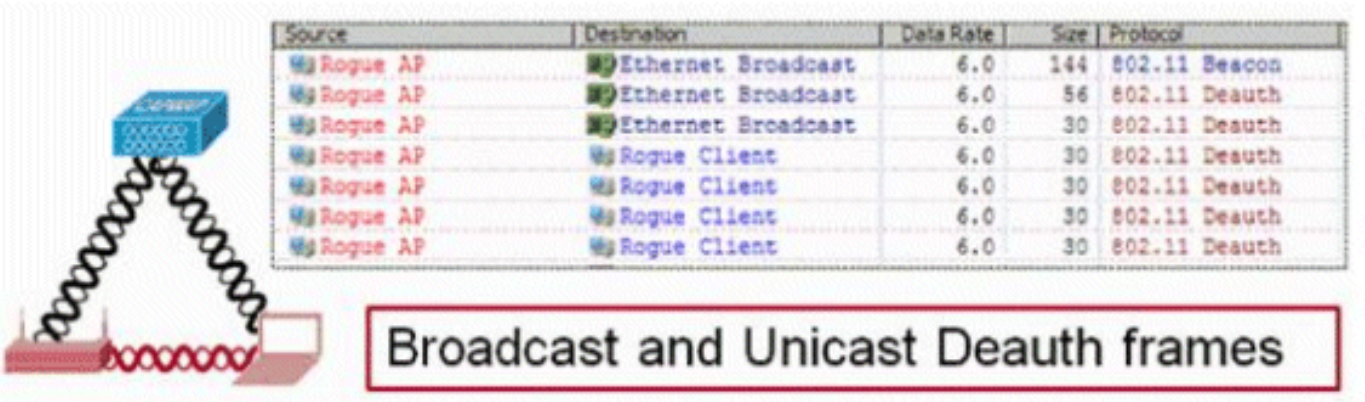


欺诈遏制详细信息

在无客户端的欺诈AP上发起的遏制仅使用发送到广播地址的反身份验证帧：

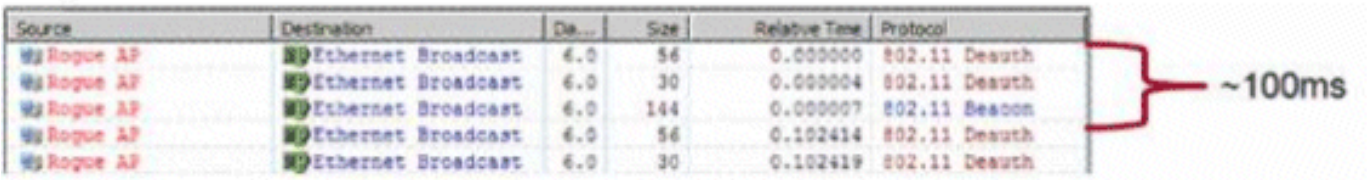


在带有客户端的欺诈AP上启动的遏制使用发送到广播地址和客户端地址的反身份验证帧：



控制数据包以受管AP的电源级别和最低的启用数据速率发送。

遏制每100毫秒至少发送2个数据包：



注意：非监控模式AP执行的包含以500ms的间隔而不是监控模式AP使用的100ms间隔发送。

- 单个非法设备可以由1到4个受管AP控制，这些AP可协同工作，以暂时缓解威胁。
- 可以使用本地模式、监控模式和Flex-connect（连接）模式AP来执行限制。对于flex-connect AP的本地模式，每个无线电最多可以包含三个非法设备。对于监控模式AP，每个无线电最多可以包含六个非法设备。

自动遏制

除了通过PI或WLC GUI在欺诈设备上手动启动遏制功能外，还可以在某些情况下自动启动遏制。此配置位于PI或控制器接口的Rogue Policies部分的Generalin下。默认情况下，这些功能均处于禁用状态，启用这些功能只是为了消除造成最大损害的威胁。

- Rogue on Wire — 如果识别出非法设备要连接到有线网络，则会自动将其置于控制之下。
- 使用我们的SSID — 如果欺诈设备使用的SSID与控制器上配置的SSID相同，则会自动包含该SSID。此功能旨在解决蜜罐攻击造成损害的问题。
- 欺诈AP上的有效客户端 — 如果发现Radius/AAA服务器中列出的客户端与欺诈设备关联，则仅针对该客户端启动遏制，阻止其关联到任何非托管AP。
- AdHoc欺诈AP — 如果发现ad-hoc网络，则会自动将其包含在内。

恶意遏制警告

- 由于遏制使用受管AP的一部分无线电时间发送取消身份验证帧，因此数据和语音客户端的性能受到多达20%的负面影响。对于数据客户端，影响是吞吐量降低。对于语音客户端，遏制可能导致对话中断和语音质量下降。
- 对邻居网络发起遏制可能会产生法律影响。在启动遏制之前，请确保流氓设备位于您的网络中并带来安全风险。

交换机端口关闭

使用SPT跟踪交换机端口后，PI中有一个禁用该端口的选项。管理员必须手动完成此练习。如果从网络物理上删除了欺诈设备，则可以选择通过PI启用交换机端口。

配置

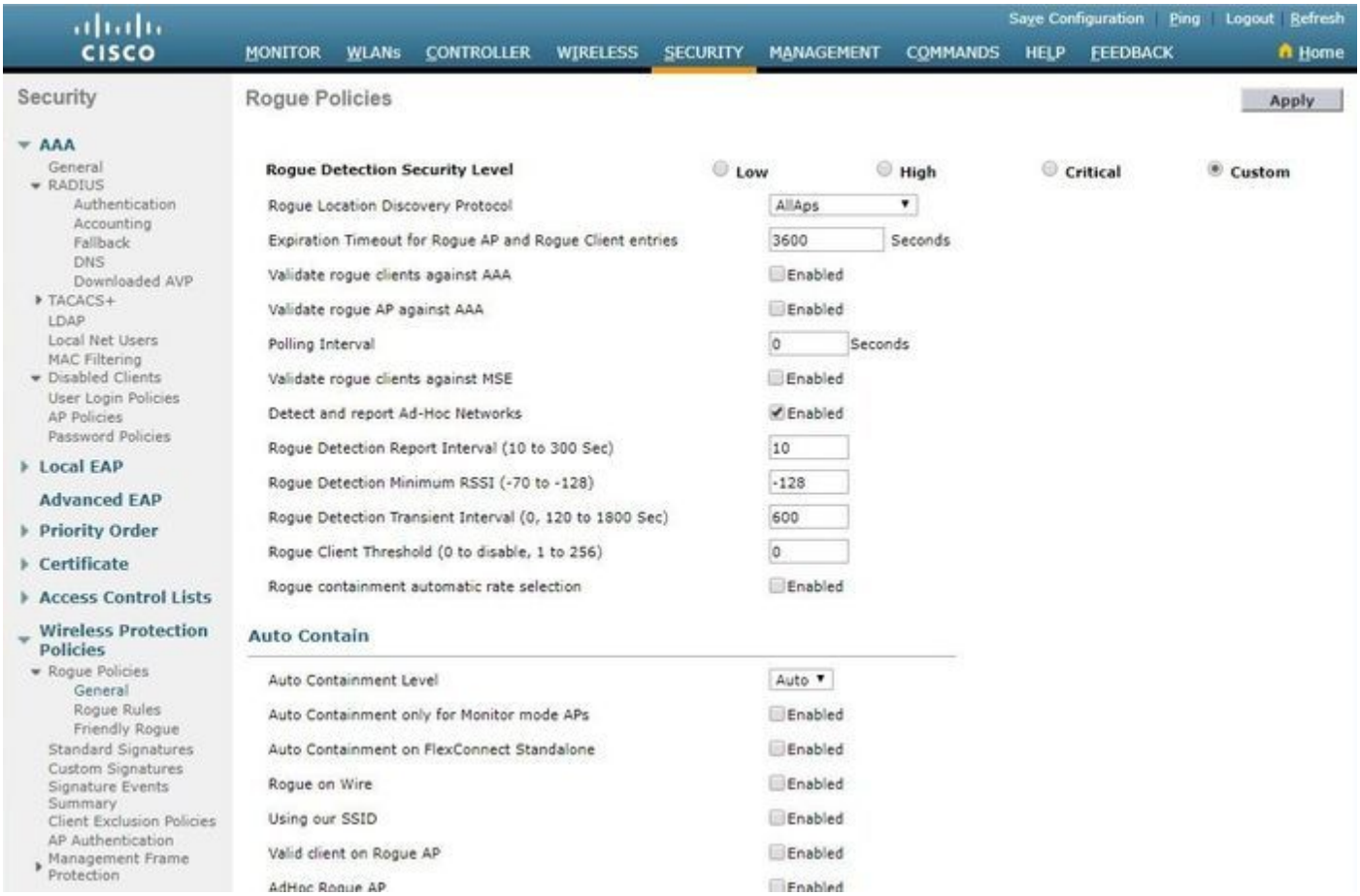
配置欺诈检测

默认情况下，在控制器中启用欺诈检测。

要配置各种选项，请导航到**安全>无线保护策略>欺诈策略>常规**。例如：

步骤1.更改非法AP的超时。

步骤2.启用ad-hoc欺诈网络检测。



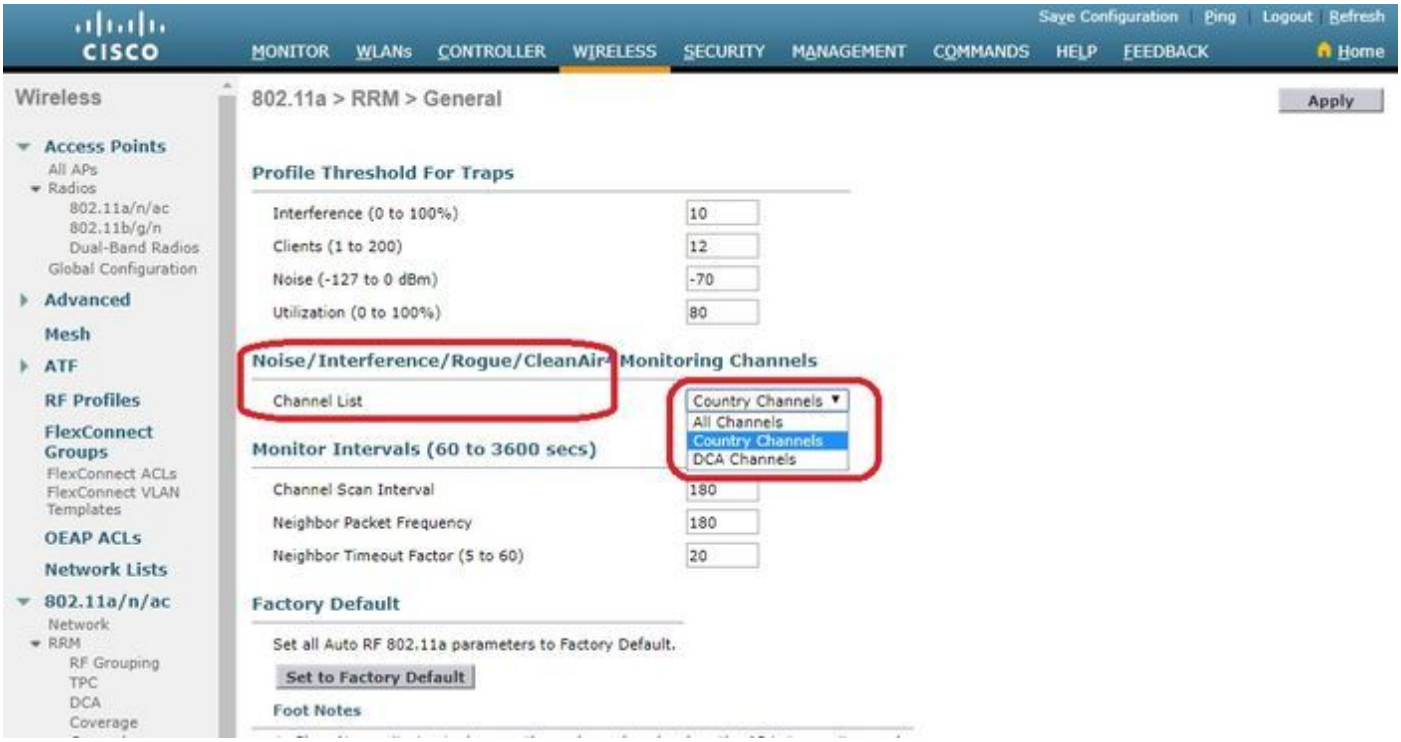
从CLI:

```
(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
```

为欺诈检测配置信道扫描

对于本地/Flex-Connect/Monitor模式AP，在RRM配置下有一个选项，允许用户选择扫描哪些信道以查找欺诈。取决于配置，AP扫描所有信道/国家/地区信道/DCA信道以查找欺诈。

要从GUI中配置此设置，请导航到**Wireless > 802.11a/802.11b > RRM > General**，如图所示。



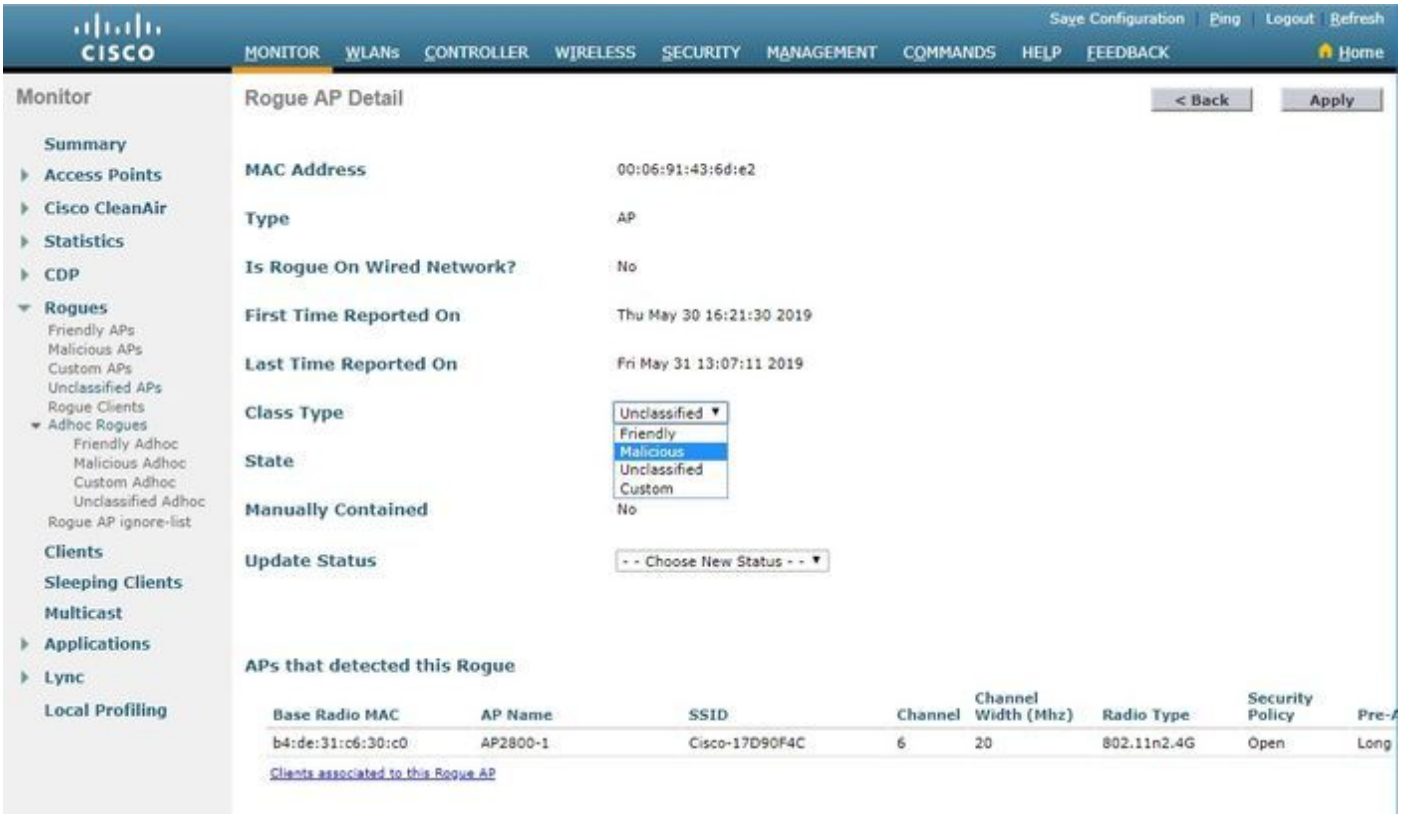
从CLI:

```
(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
```

配置欺诈分类

手动对欺诈AP分类

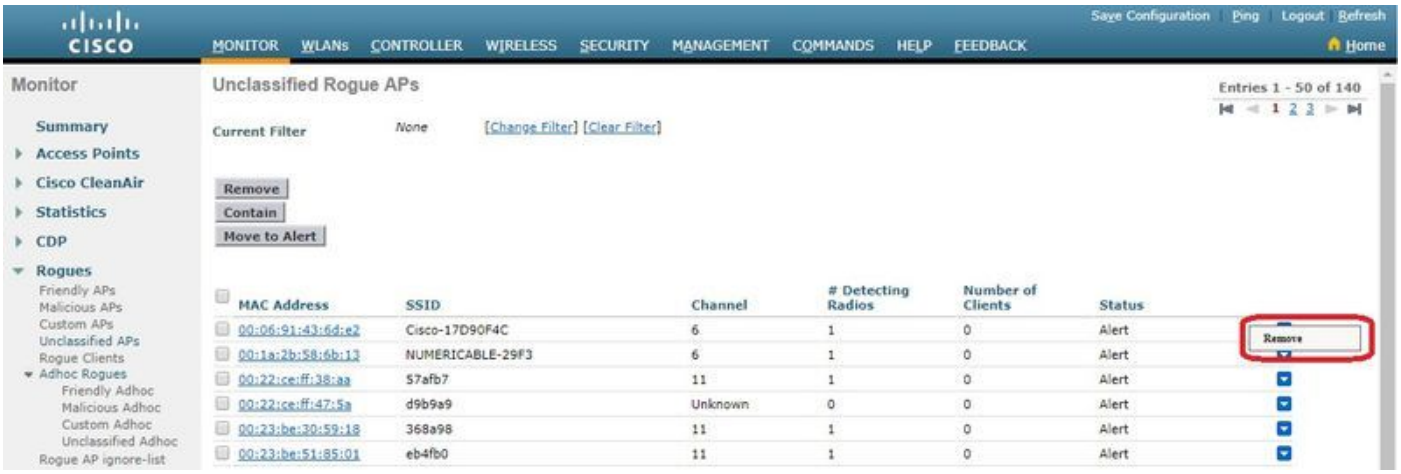
要将欺诈AP分类为友好、恶意或未分类，请导航到**Monitor > Rogue > Unclassified** AP，然后点击特定的欺诈AP名称。从下拉列表中选择选项，如图所示。



从CLI:

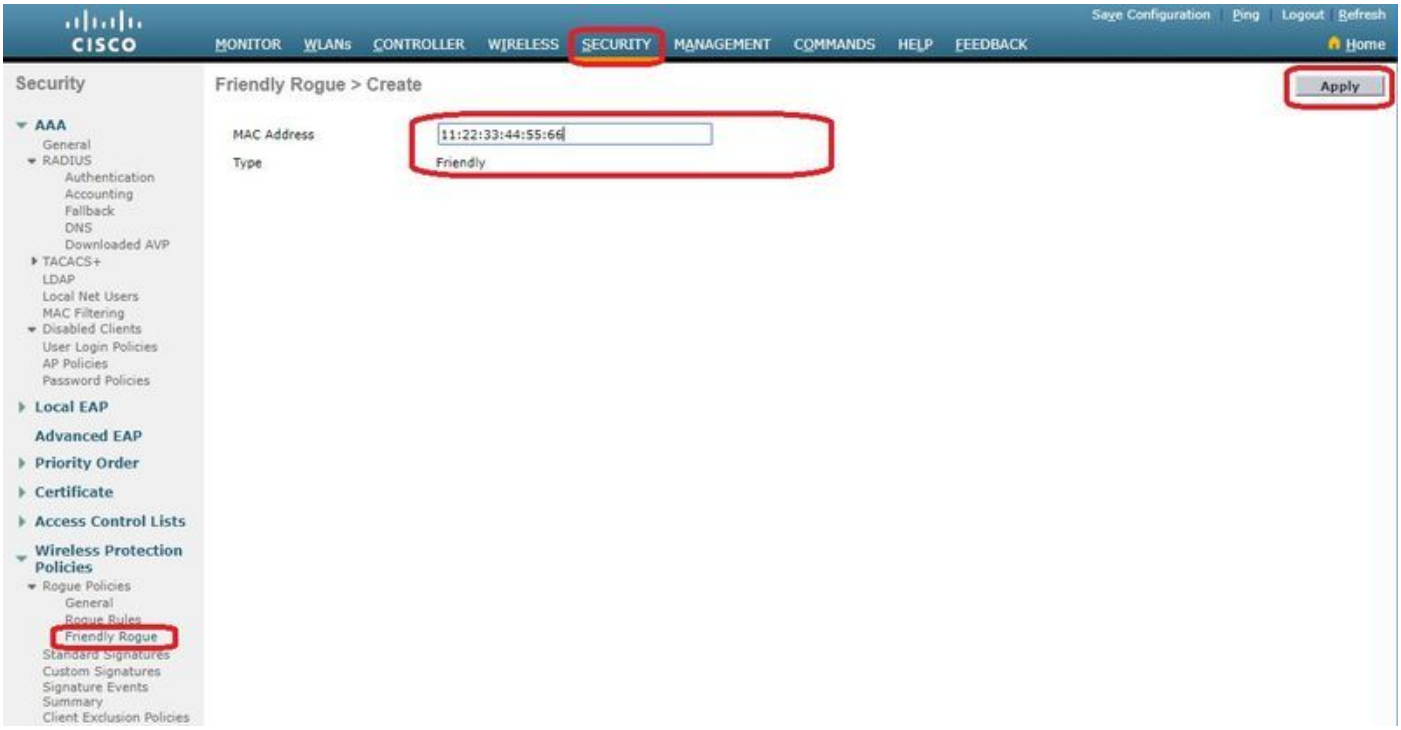
```
(Cisco Controller) >config rogue ap ?

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.
```

要从欺诈列表中手动删除欺诈条目，请导航到**Monitor > Rogue > Unclassified** AP，然后单击**Remove**，如图所示。



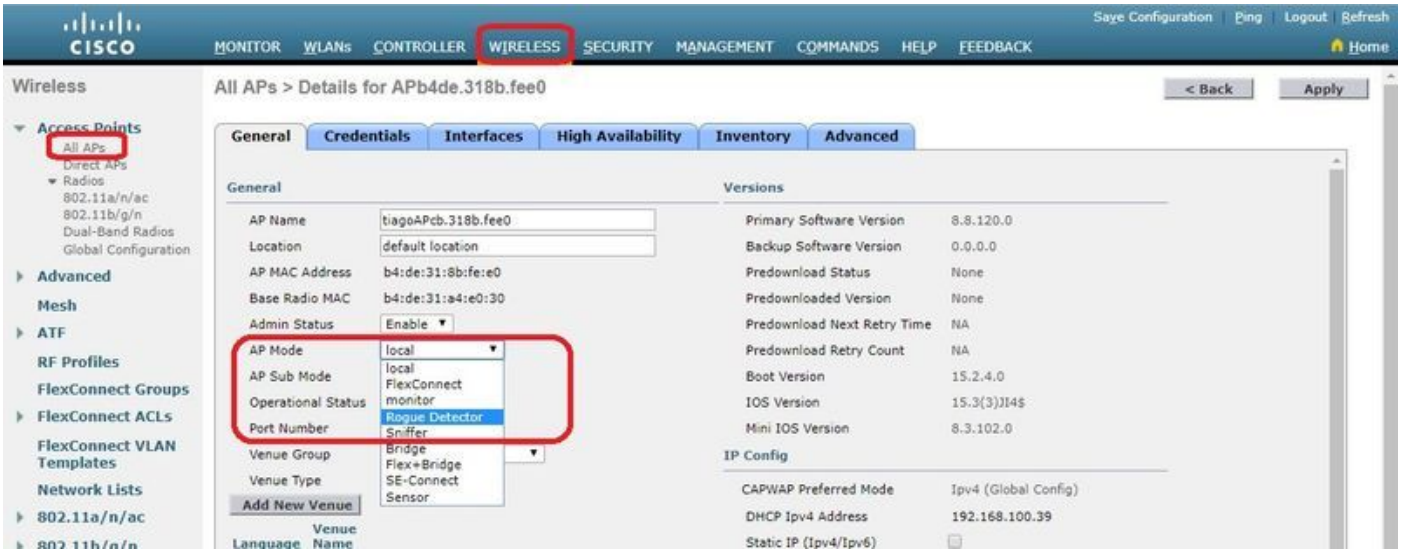
要将欺诈AP配置为友好AP，请导航到**安全>无线保护策略>欺诈策略>友好**，然后添加欺诈MAC地址。

如图所示，添加的友好欺诈条目可以通过**Monitor > Rogues > Friendly** Roguepage进行验证。



配置欺诈检测器AP

要通过GUI将AP配置为欺诈检测器，请导航到Wireless > All APs。选择AP名称并更改AP模式，如图所示。



从CLI:

```
(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
```

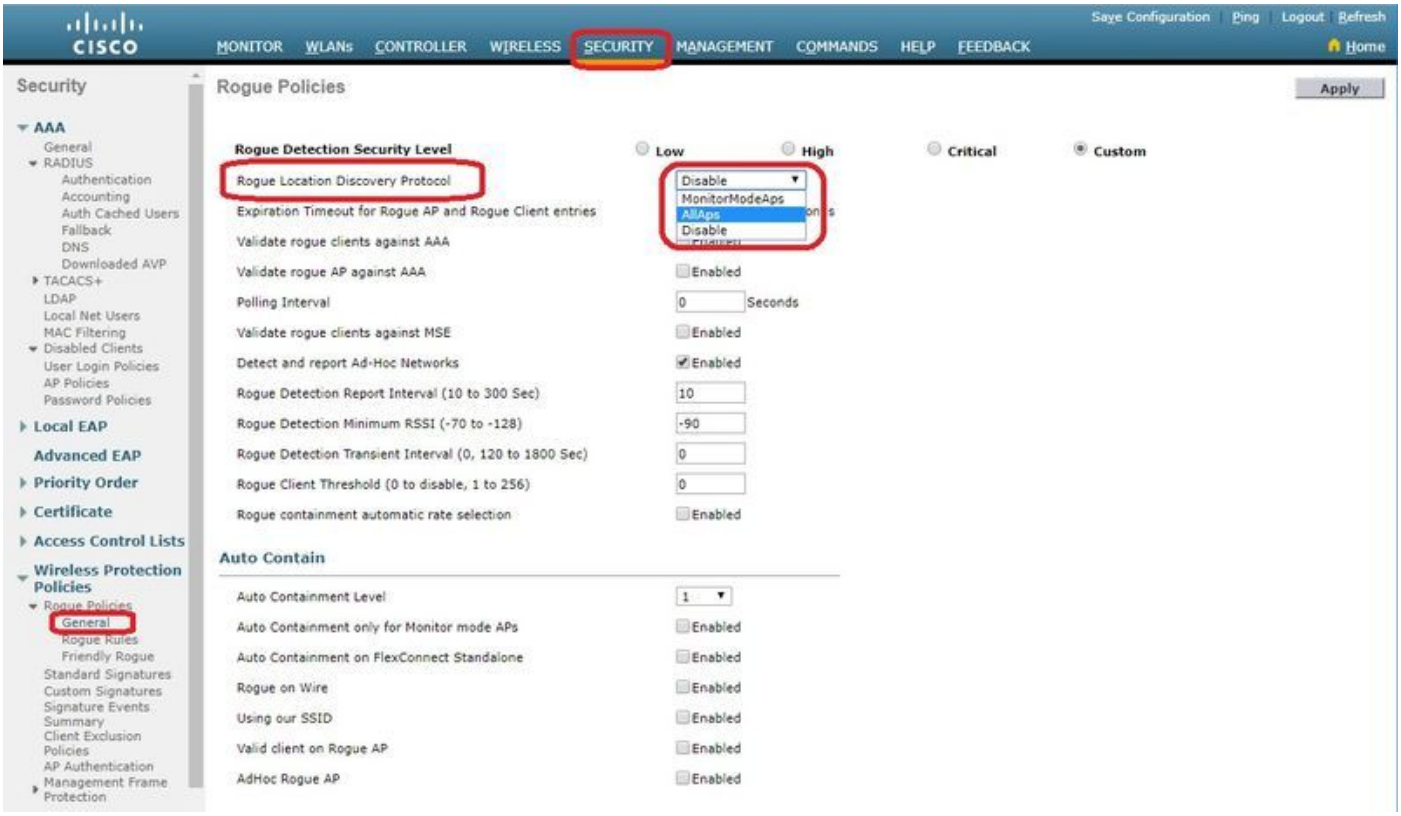
为欺诈检测器AP配置交换机端口

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

注意：此配置中的本地VLAN是与WLC具有IP连接的本地VLAN。

配置RLDP

要在控制器GUI中配置RLDP，请导航到**安全>无线保护策略>欺诈策略>常规**。



监控模式AP — 仅允许处于监控模式的AP参与RLDP。

所有AP — 本地/Flex-Connect/监控模式AP均参与RLDP进程。

已禁用 — 不会自动触发RLDP。但是，用户可以通过CLI为特定MAC地址手动触发RLDP。

注意：如果监控模式AP和本地/Flex-Connect AP都检测到特定欺诈超过–85dbm RSSI，则监控模式AP会优先于本地/Flex-Connect AP执行RLDP。

从CLI:

```
(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计划和手动触发器只能通过命令提示符进行配置。要手动启动RLDP，请执行以下操作：

```
(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).
```

对于RLDP计划：

```
(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.
```

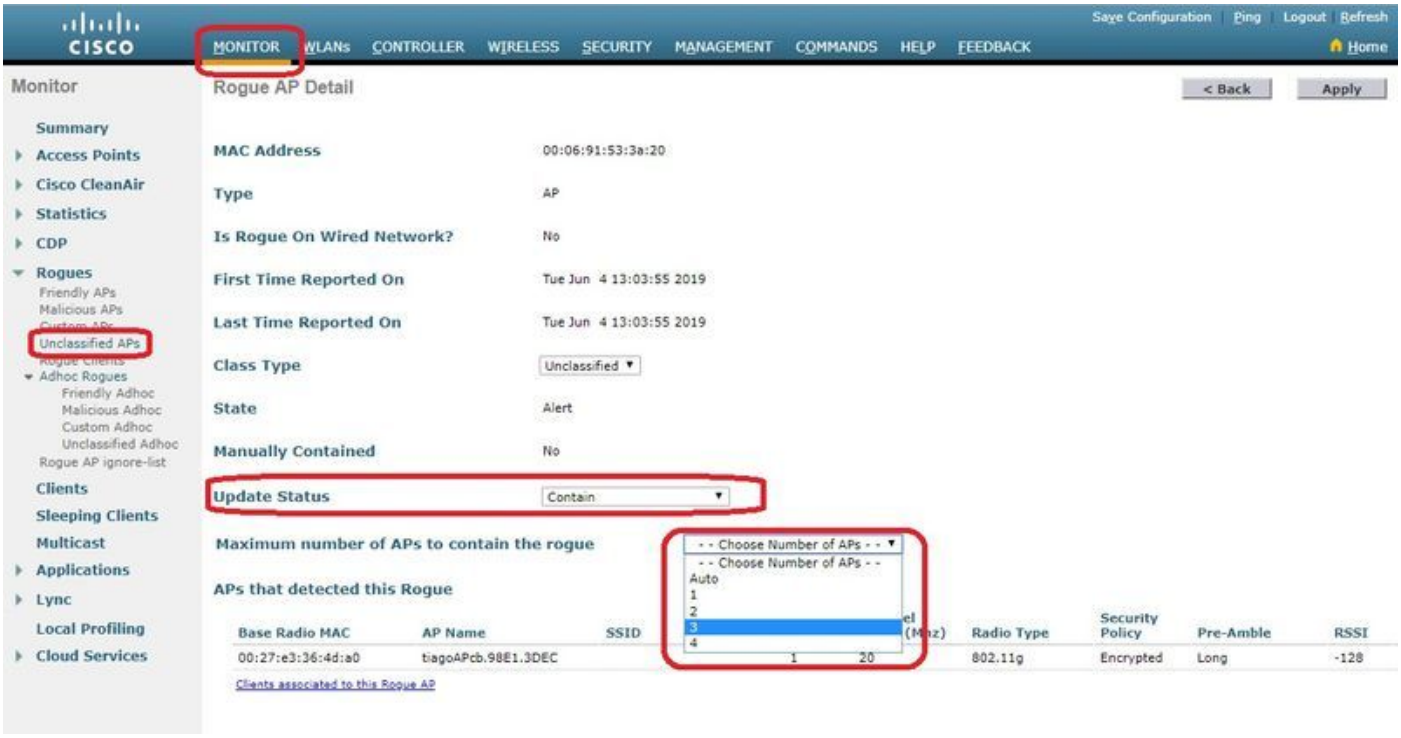
可以使用以下命令配置RLDP重试：

```
(Cisco Controller) >config rogue ap rldp retries ?

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

配置欺诈缓解

配置手动遏制

要手动控制非法AP，请导航到**Monitor > Rogues > Unclassified**，如图所示。



从CLI：

```
(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].
```

注意：1-4个AP可以控制特定的欺诈。默认情况下，控制器使用一个AP来包含客户端。如果两个AP能够检测特定的欺诈，则无论该AP模式如何，具有最高RSSI的AP都包含客户端。

自动遏制

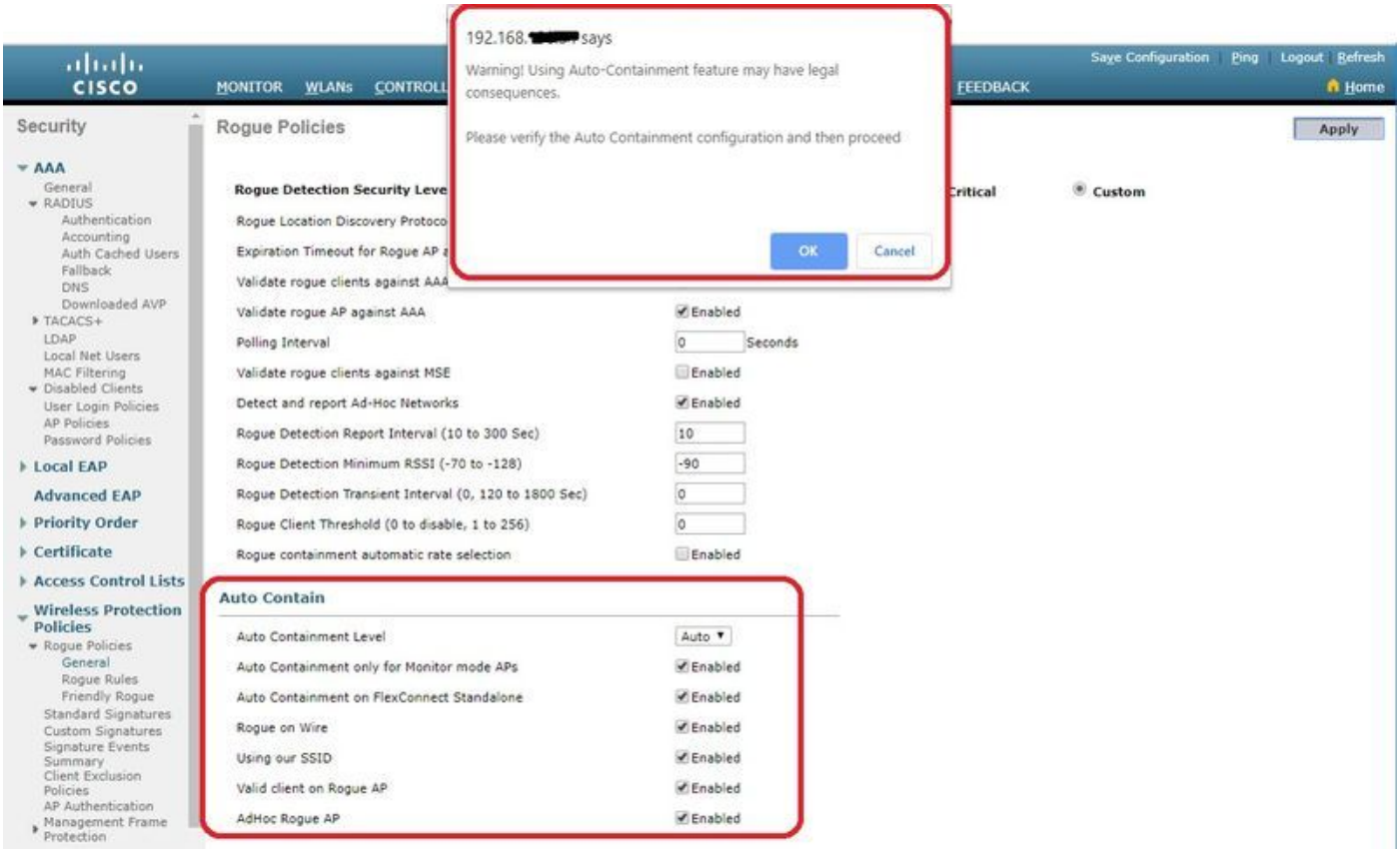
要配置自动遏制，请转到**Security>Wireless Protection Policies>Rogue Policies>General**，然后为网络启用所有适用的选项。

如果您希望Cisco WLC自动包含某些非法设备，请选中这些复选框。否则，请取消选中复选框，这是默认值。

警告：当您启用这些参数中的任何一个时，系统会显示以下消息："使用此功能会产生法律后果。要继续码？"工业、科学和医疗(ISM)频段中的2.4 — 和5-GHz频率对公众开放，无需许可证即可使用。因此，控制另一方网络上的设备可能会产生法律后果。

以下是自动包含参数：

参数	描述
自动包含级别	下拉列表，您可以从中选择欺诈自动遏制级别从1到4。 通过任何自动遏制策略，当欺诈设备移至被包含状态时，您最多可以选择 您也可以选择Auto自动选择用于自动包容的AP数量。Cisco WLC根据RS 现有效遏制。 与每个遏制级别关联的RSSI值如下： • 1 - 0至–55 dBm • 2 —75至–55 dBm • 3 —85至–75 dBm • 4 — 小于–85 dBm
仅对监控模式AP自动包含	选中此复选框可启用监控模式AP以进行自动遏制。默认设置为禁用状态。
FlexConnect独立版上的自动遏制	选中此复选框可在独立模式下启用FlexConnect AP上的自动遏制。默认设 FlexConnect AP处于独立模式时，您只能启用使用我们的SSID或即席欺 AP连接回Cisco WLC后，遏制将停止。
有线欺诈	选中此复选框可自动包含有线网络上检测到的恶意程序。默认设置为禁用
使用我们的SSID	选中此复选框可自动包含通告网络SSID的恶意程序。如果未选择此参数 类欺诈时生成警报。默认设置为禁用状态。
欺诈AP上的有效客户端	选中此复选框可自动包含与受信任客户端关联的欺诈接入点。如果未选择 检测到此类欺诈时生成警报。默认设置为禁用状态。
临时欺诈AP	复选框可启用自动包含由Cisco WLC检测到的对等网络。如果未选择此参 到此类网络时生成警报。默认设置为禁用状态。



单击Apply将数据发送到Cisco WLC，但不会在整个电源周期中保留数据；这些参数临时存储在易失性RAM中。

从CLI:

```
(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
```

使用Prime基础设施

Cisco Prime基础设施可用于配置和监控一个或多个控制器和关联的AP。思科PI拥有促进大型系统监控和控制的工具。当您在思科无线解决方案中使用思科PI时，控制器会定期确定客户端、非法接入点、非法接入点客户端、射频ID(RFID)标签位置，并将位置存储在思科PI数据库中。

Cisco Prime基础设施支持基于规则的分类并使用在控制器上配置的分类规则。发生以下事件后，控制器将陷阱发送到Cisco Prime基础设施：

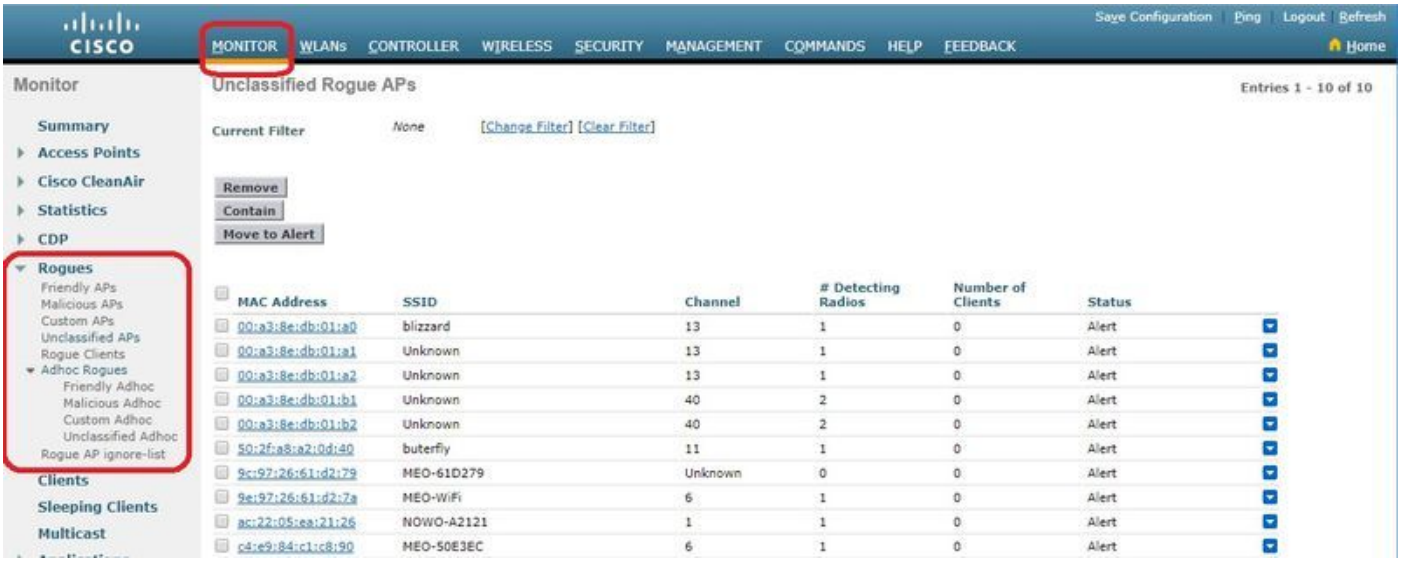
- 如果未知接入点首次进入友好状态，则仅当欺诈状态为警报时，控制器才会向Cisco Prime基础

设施发送陷阱。如果oguestate为**Internal**或**External**，则不会发送陷阱。

- 如果arogueentry在超时过期后被删除，控制器会向Cisco Prime Infrastructurefor rogueaccess points发送陷阱，该接入点被归类为**Malicious**（警报、威胁）或**Unclassified**（警报）。 控制器不删除具有erogeuestates的条目：**Contained、Contained Pending、Internal**和External**。**

验证

要在图形界面中的控制器中查找欺诈详细信息，请导航到**Monitor > Rogues**，如图所示。

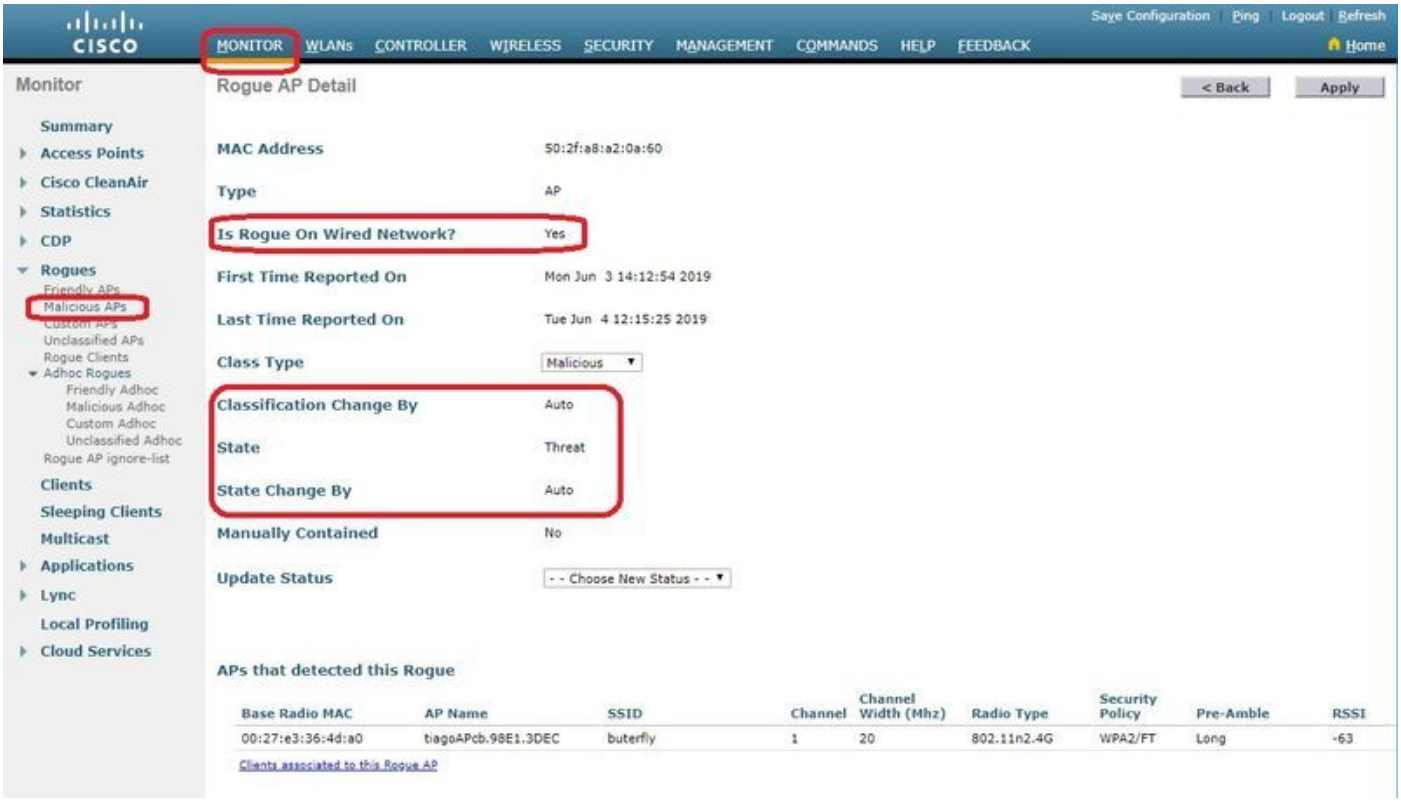


在此页中，欺诈的不同分类可用：

- 友好AP — 管理员标记为友好AP。
- 恶意AP — 通过RLDP或欺诈检测器AP识别为恶意的AP。
- 自定义AP — 被欺诈规则归类为自定义的AP。
- 未分类的AP — 默认情况下，欺诈AP在控制器中显示为未分类列表。
- 欺诈客户端 — 连接到欺诈AP的客户端。
- 临时恶意客户端 — 临时恶意客户端。
- 非法AP忽略列表 — 通过PI列出。

> **注意**：如果WLC和自治AP由同一PI管理，则WLC会在欺诈AP忽略列表中自动列出此自治AP。在WLC中无需其他配置即可启用此功能。

单击特定欺诈条目以获取该欺诈的详细信息。以下是在有线网络上检测到欺诈的示例：



从CLI:

```
(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 #Rogue  #Highest RSSI     #RSSI
#Channel        #Second Highest   #RSSI  #Channel
                                                     Aps  Clients  det-Ap
RSSI Det-Ap
----------------- ------------ -------------------- ---- ------- ----------------- ------ ------
--------- ----------------- ------ ---------------
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
00:27:e3:36:4d:a0 -37    40
00:a3:8e:db:01:b1 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
00:27:e3:36:4d:a0 -36    40
00:a3:8e:db:01:b2 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
00:27:e3:36:4d:a0 -37    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
```

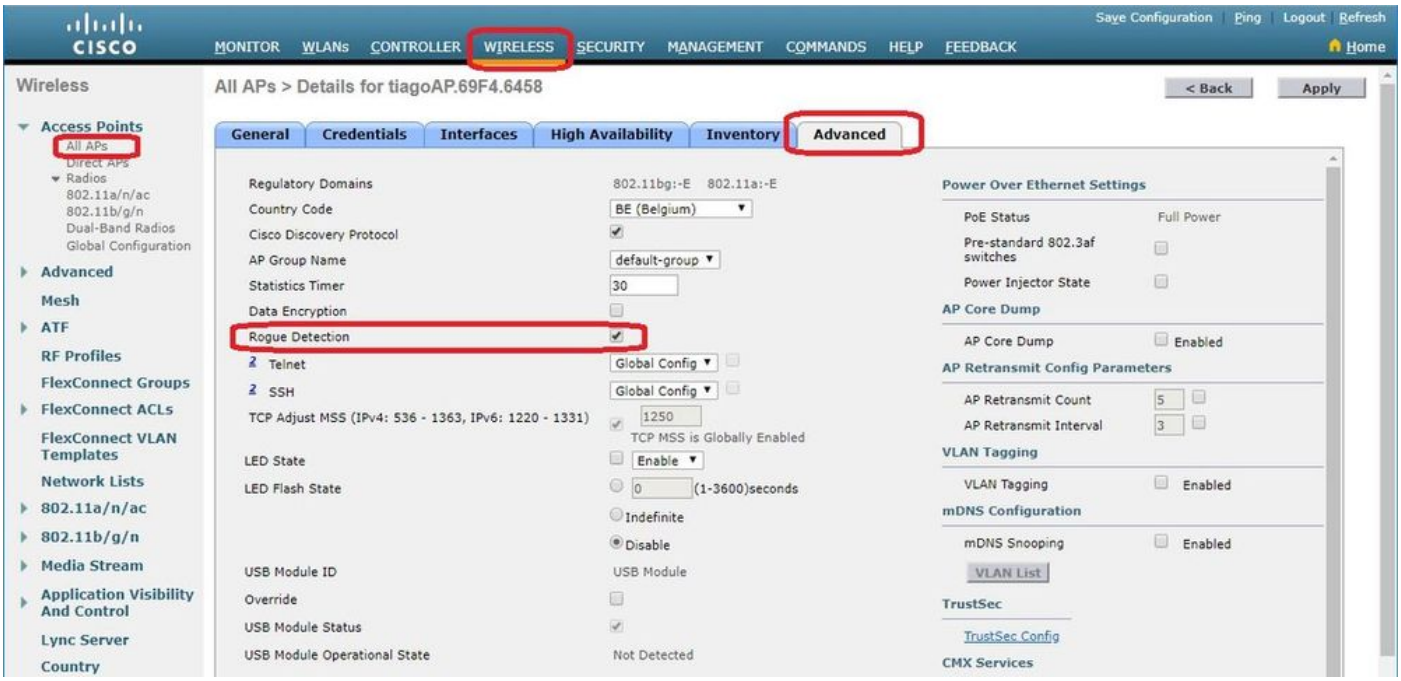
```
9c:97:26:61:d2:79 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    6
ac:22:05:ea:21:26 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (1,5)
c4:e9:84:c1:c8:90 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (6,2)
d4:28:d5:da:e0:d4 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
```

故障排除

如果未检测到欺诈设备

验证AP上已启用欺诈检测。在GUI上：



在CLI中：

```
(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
[...]
```

可通过以下命令在AP上启用欺诈检测：

```
(Cisco Controller) >config rogue detection enable ?
all            Applies the configuration to all connected APs.
<Cisco AP>     Enter the name of the Cisco AP.
```

本地模式AP仅扫描国家/地区信道/DCA信道并取决于配置。如果欺诈处于任何其他信道中，如果网络中没有监控模式AP，则控制器无法识别欺诈设备。发出此命令以进行验证：

```
(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
```

- 欺诈AP不广播SSID。
- 确保欺诈AP的MAC地址未添加到友好欺诈列表中或通过PI列出。
- 来自欺诈AP的信标无法到达检测到欺诈的AP。这可以通过使用靠近AP检测器欺诈的嗅探器捕获数据包来验证。
- 本地模式AP可能需要9分钟来检测欺诈设备（3个循环180x3）。
- 思科AP无法在公共安全信道(4.9 Ghz)等频率上检测欺诈。

- 思科AP无法检测在FHSS（跳频扩展频谱）上工作的欺诈。

有用的调试

```
(Cisco Controller) >debug client
```

```
        (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:a2:0a:60 on slot 0

*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 -55, snr 39 wepMode 81 wpaMode 86, detectinglradtypes :20
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417.
Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or
channel width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*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, snr 39
*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
ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class
malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule
classification : Class malicious, Change by Auto State Threat Change by Auto

*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=buterfly

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  Rogue AP: 50:2f:a8:a2:0a:60 autocontain
= 2 Mode = 7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source
50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*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 Impersonation 0 ids flags 2

*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
```

```
(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
```

```
:FCW2245M09Y  Hostname tiagoWLCcb
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for
processing Payload version:c1, slot:0 , Total Entries:5, num entries this packet:5 Entry index
:0, pakLen:285

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0,
(Radio_upTime-now)=152838
*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 b0:72:bf:93:e0:d7 channel 1 rssi -59 ssid SMA1930072865
*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 50:2f:a8:a2:0a:60 channel 1 rssi -63 ssid buterfly
*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 00:a3:8e:db:01:a1 channel 13 rssi -16 ssid
*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 a4:c3:f0:cf:db:18 channel 40 rssi -26 ssid blizzard
*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 -28, snr 61 wepMode 81 wpaMode 82, detectinglradtypes :30
*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 00:a3:8e:db:01:b2 channel 40 rssi -28 ssid
*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 Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  knownApCount=0,
totalNumOfRogueEntries=5, #entriesThisPkt=5, #totalEntries=5
*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 -16, snr 76 wepMode 81 wpaMode 82, detectinglradtypes :28
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check:  avgNumOfRogues[0]/10=4,
rogueAlarmInitiated[0]=0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2  SYNC for Channel (new/old : 40/0) or
channel width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last
update at 0 Detecting lrad: 00:27:e3:36:4d:a0
*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 width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*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, snr 61
*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, snr 76
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1
ReceiveSlotId = 0 ReceiveBandId = 1

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class
unclassified, Change by Default State Alert Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP
at 0xfff0617238

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

*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 table
*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 in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class
unclassified, Change by Default State Alert Change by Default
```

```
*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 for rogue AP b0:72:bf:93:e0:d7
*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:93:e0:d7
*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 Mode = 2

*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 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0,
ptype -155740480 mfp_supported 1
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2
ReceiveSlotId = 0 ReceiveBandId = 0

*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 -59, snr 36 wepMode 81 wpaMode 83, detectinglradtypes :20
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for  : Class
Change by Default State Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7  Send Rogue Info Notificaiton for AP
report 00:27:e3:36:4d:a0  Rogue ssid change from   to SMA1930072865
*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.
Detecting lrad: 00:27:e3:36:4d:a0
*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
unclassified, Change by Default State Alert Change by Default

*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, snr 36
*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
ReceiveSlotId = 0 ReceiveBandId = 0

*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
unconfigured, Change by Default State Pending Change by Default

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

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

```
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule
classification : Class unconfigured, Change by Default State Pending Change by Default

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source
00:a3:8e:db:01:a1 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0,
ptype -155740480 mfp_supported 1
*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 Impersonation 0 ids flags 6

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source
b0:72:bf:93:e0:d7 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 1, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*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 Impersonation 0 ids flags 2

*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 -26, snr 61 wepMode 81 wpaMode 82, detectinglradtypes :32
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997.
Detecting lrad: 00:27:e3:36:4d:a0
*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 -63, snr 5 wepMode 81 wpaMode 86, detectinglradtypes :20
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0  SYNC for Channel (new/old : 40/0) or
channel width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997.
Detecting lrad: 00:27:e3:36:4d:a0
*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 width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*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, snr 61
*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, snr 5
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1
ReceiveSlotId = 0 ReceiveBandId = 1

*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
ReceiveSlotId = 0 ReceiveBandId = 0

*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
malicious, Change by Auto State Threat Change by Auto

*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=blizzard

*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 Mode = 7

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

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60  Rogue AP: 50:2f:a8:a2:0a:60 autocontain
= 2 Mode = 7

*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 Impersonation 0 ids flags 2

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source
50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*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 Impersonation 0 ids flags 2

*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 50
*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, snr 50
*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, snr 43
*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 32
*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, snr 32
*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 table
*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 in AP list or neighbor, known or Mobility group AP lists
*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:93:e0:d7
*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
0xfff0617238

*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
```

预期的陷阱日志

一旦检测到欺诈设备，即会将其从欺诈列表中删除：

0	2019年6月5日09:01:57星期三	恶意客户端：b4:c0:f5:2b:4f:90由1个AP**检测**到欺诈客户端Bssid:a6:b1:e9: 时间：00:27:e3:36:4d:a0恶意客户端网关mac 00:00:00:02:02:02。
1	2019年6月5日09:00:39星期三	欺诈AP:9c:97:26:61:d2:79已从基**射**频MAC中删除：00:27:e3:36:4d:a0接
2	2019年6月5日08:53:39星期三	欺诈AP:7c:b7:33:c0:51:14已从基**射**频MAC中删除：00:27:e3:36:4d:a0接
3	2019年6月5日08:52:27星期三	恶意客户端：fc:3f:7c:5f:b1:1b由1个AP**检测**到欺诈客户端Bssid:50:2f:a8:a 时间：00:27:e3:36:4d:a0非法客户端网关mac 00:26:44:73:c5:1d。
4	2019年6月5日08:52:17星期三	欺诈AP:d4:28:d5:da:e0:d4 **从基**射频MAC中删除：00:27:e3:36:4d:a0接口

建议

1. 如果您怀疑网络中可能存在欺诈，请为所有信道配置信道扫描。
2. 非法检测器AP的数量和位置可能因每层一楼而有所不同，取决于有线网络的布局。建议建筑物每层至少有一个非法检测器AP。由于欺诈检测器AP需要中继到要监控的所有第2层网络广播域，因此放置取决于网络的逻辑布局。

如果流氓未分类

验证非法规则是否配置正确。

有用的调试

```
(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
:FCW2245M09Y Hostname tiagoWLCcb

(Cisco Controller) >
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154623, wep=1, ssid=blizzard slotId = 0
channel = 13 snr = 76 dot11physupport =
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5790, wep=1, ssid=NOWO-A2121 slotId = 0
channel = 1 snr = 4 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5820, wep=1, ssid=NOWO-A2121 slotId = 0
channel = 1 snr = 4 dot11physupport = 3
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62,
```

```
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154353, wep=1, ssid=buterfly slotId = 0
channel = 11 snr = 30 dot11physupport =
*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,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154713, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid=blizzard slotId = 0
channel = 13 snr = 76 dot11physupport =
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious,
RuleName:TestRule, Rogue State:Containment Pending

*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154743, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3
```

建议

如果您有已知的恶意条目，请将它们添加到友好列表中或使用AAA启用验证，并确保已知的客户端条目存在于身份验证、授权和记帐(AAA)数据库中。

RLDP找不到恶意程序

- 如果欺诈在DFS信道中，则RLDP不起作用。
- 仅当非法WLAN打开且DHCP可用时，RLDP才起作用。
- 如果本地模式AP为DFS信道中的客户端提供服务，则不会参与RLDP进程。
- AP型号1800i、1810 OEAP、1810W、1815、1830、1850、2800和3800系列AP不支持RLDP。

有用的调试

```
(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 APs

*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-AP1852I-E-K9 *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, channel = 1

*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 TRUE
*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 State(2)

*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 State(2)

*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
```

建议

1. 对可疑欺诈条目手动启动RLDP。
2. 定期安排RLDP。
3. RLDP可以部署在本地或监控模式AP上。对于大多数可扩展的部署，为了消除对客户端服务的任何影响，应尽可能在监控模式AP上部署RLDP。但是，此建议要求以典型比率部署监控模式AP，即每5个本地模式AP部署1个监控模式AP。自适应wIPS监控模式下的AP也可以用于此任务。

欺诈检测器AP

在AP控制台中使用此命令可看到欺诈检测器中的欺诈条目。对于有线欺诈，标志将移动以设置状态。

```
tiagoAP.6d09.eff0#show capwap rm rogue detector
 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
```

AP控制台中的有用调试命令

```
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
```

非法控制

预期调试

```
*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, snr 59
*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 table
*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 in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6
ContainmentLevel : 4 level 4

*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
```

```
ReceiveSlotId = 1 ReceiveBandId = 1

*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 : Class malicious, Change by Auto State Contained Change by Auto

*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 lineNumber : 8225 apfRogueManualContained : 0 function :
apfUpdateRogueContainmentState

*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 1 for detecting lrad 00:27:e3:36:4d:a0.
*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 totClientsDetected = 2
*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 totClientsDetected = 2
*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 totClientsDetected = 1
*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. Containment mode 1
*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. Containment mode 1
*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. Containment mode 1
*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 detected by b4:de:31:a4:e0:30, FailCnt 0, mode 6, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*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 Impersonation 0 ids flags 3
```

建议

1. 本地/Flex-Connect模式AP每次可包含3台设备，每个无线电可包含6台设备。因此，请确保AP不包含允许的最大设备数量。在这种情况下，客户端处于包含挂起状态。
2. 检验自动包含规则。

结论

Cisco 集中式控制器解决方案中的恶意检测和遏制是业内最有效和干扰度最低的方法。网络管理员可以灵活调整方案，以适应任何网络要求。

相关信息

- 思科无线控制器配置指南，版本8.8 — 欺诈管理
- 思科无线局域网控制器(WLC)配置最佳实践
- WLC 3504版本8.5部署指南
- Cisco 5520无线LAN控制器部署指南
- 思科无线控制器和轻量接入点版本说明，思科无线版本8.8.120.0

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。