# Wireless Security: Threats, Origins, & Modern Solutions

By Ambuj Mahendra (CCIE, CWNE)

August 31, 2021

Wireless security is key to any successful wireless network operation. There are many vulnerabilities that can exploit wireless networks for reconnaissance, compromise, degrade, or disable wireless access all together. Examples include Airsnarf attacks, rogue Access Points, honeypot & honeypotter tools, and Denial-of-Service (DoS) attacks like beacon flood, deauth flood, and some of the recent ones such as KRACK and FRAG attacks. See the Resources section for a detailed list of common attacks & signatures.

At the very least, what we typically want in our wireless network is to:

1. Detect threats immediately!

2. Have the ability to contain devices that are performing attacks.

3. Find the attack device location.

4. Keep the system signature up to date to detect new threats and improve security over time.

Our goals for this article are for you to understand the above items and help you deploy them in a Cisco wireless network environment.

So, if this is something that interests you, then please continue on!

(Estimated read time: 15 minutes)

## Looking Back

Wireless based attacks are nothing new. They date back to 1903 when Guglielmo Marconi set up a large wireless demonstration – a Morse code transmission 300 miles across England - when a signal intrusion occurred from rival inventor Nevil Maskelyne. In other words, early evidence of a wireless hacker!

ONE HALFPENNY.

GHOST'S TAPPING.

THE WIRELESS MYSTERY SOLVED.

But coming back to recent history on the LAN side, every Cisco wireless controller has always had some form of wireless intrusion prevention built into it. However, it's more of a question of how many signatures it can support… because the more signatures supported, the more threats it can detect.

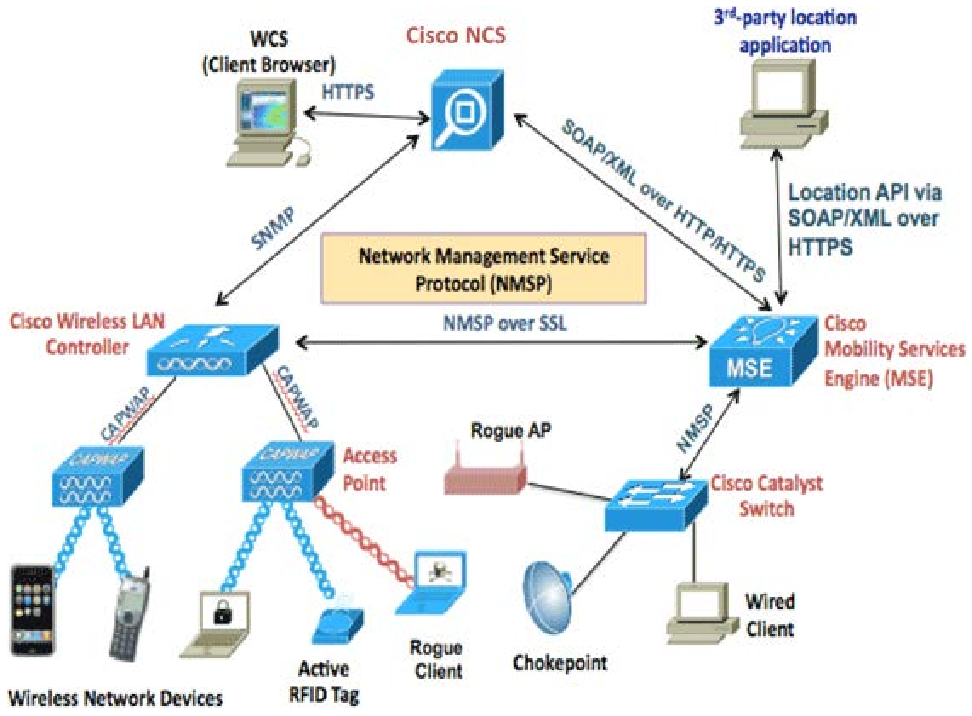
For example, an AirOS controller is supported by about 17 signatures, including:

- Bcast deauth
- NULL Probe Response - Zero length SSID element
- NULL Probe Response - No SSID element
- Association request flood
- Authentication request flood
- Broadcast Probe request flood
- Disassociation flood
- Deauthentication flood
- Reserved mgmt 7
- Reserved mgmt F
- EAPOL flood
- Wellenreiter
- NetStumbler

Cisco Meraki markets WIPS with the name Air Marshall and has 24+ signatures.

In the recent past we used something called Mobility Services Engine with WIPS services running on it, increasing the signature count from 17 on WLC to 60+ signatures. If you ran another MSE or CMX for location services, you were able to pinpoint the location of these malicious/rogue devices as well.

You are probably familiar with this architecture below, and maybe even deployed it at some point:



But things have evolved since then. Since MSE version 8.0.150.0, we have been waiting for a new platform for the replacement of the MSE WIPS platform.

## Modern Solutions

This brings us to present day with the release of the DNA Center 2.1.2 WIPS application package. With IOSXE based controller, tri radio access points, and a cloud-based location engine like DNA Spaces, it's a new world! However, so are the threats on wireless. We have to learn how to use these new tools to protect our network.

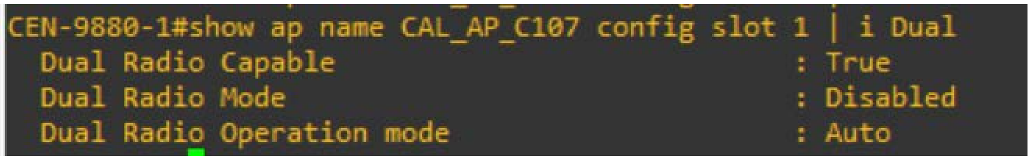
## Rogue Management & Wireless Intrusion Prevention System (WIPS)

We are dealing with two different terms here: Rogue Management for rogue APs and WIPS for intrusion attacks. Let's clarify the difference before we move forward:

> **Rogue AP:** Every time a Cisco AP joins the controller, the controller adds a little authentication Information Element (IE) into its beacon/probe frame. It's like a dress code: if you don't have the dress code (IE in your beacon frame in this case), then the AP is a rogue. APs listen to all APs around them, and if they see a beacon frame without IE code, they consider it to be advertised by a rogue AP
>
> **Intrusion Attack:** Intrusion attack is an AP or client performing a malicious behavior. This AP can very well be a rogue AP, a client connected to a rogue AP, or a client connected to your own infrastructure. Examples include 1) an AP configured to advertise the same SSID as your corporate SSID to redirect traffic to itself  and steal passwords and 2) an endpoint sending a deauthenticaton frame flood on the same channel as the production AP to kick out users and cause service disruption.

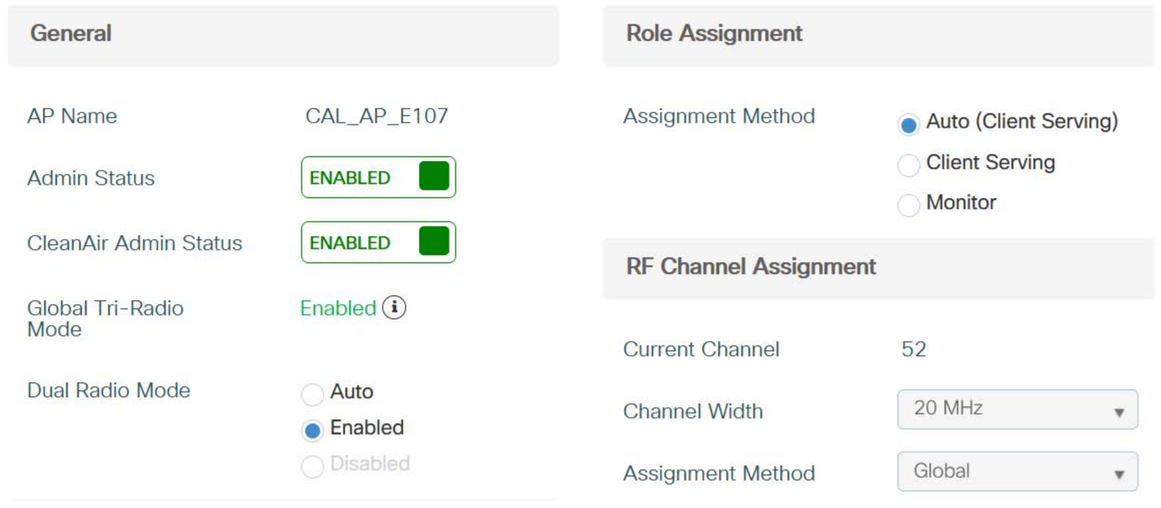
Given the nature of WiFi, you are either listening or transmitting at a time, so if you are listening to beacon frame for rogue then you are not serving your clients. Not so long ago the solution was to add an extra AP for every 5-6 APs at the highest power and lowest data rate, which worked in dedicated monitor mode and this AP's job was just to listen and report without worrying about serving clients. More recently, most APs comes with a third radio element that can be used for multiple functions. One of the functions Is to constantly monitor/listen to the air while the other two radios are dedicated to serve the clients.

Most vendors who support the third radio have a unique way of deploying it. As far as Cisco 9100s are concerned, slot 1 (5Ghz) can be divided into dual radio that uses 5Ghz as 4X4 and frees up the third radio for additional functions like monitoring. If you do not plan to do this, then you can use slot 1 as 8X8 radio. By default, slot 1 is dual radio capable but is disabled.



```
CEN-9880-1#show ap name CAL_AP_C107 config slot 1 | i Dual
  Dual Radio Capable                                 : True
  Dual Radio Mode                                    : Disabled
  Dual Radio Operation mode                          : Auto
```

To enable it, we have to first enable triband globally. Then enable dual radio on an individual AP and assign respective role to both radios. In this example case I will use the 1st radio slot 1 for client serving and 2nd radio slot 1 (slot2) for monitoring.



General

AP Name: CAL_AP_E107

Admin Status: ENABLED 🟩

CleanAir Admin Status: ENABLED 🟩

Global Tri-Radio Mode: Enabled ⓘ

Dual Radio Mode: ○ Auto ● Enabled ○ Disabled

Role Assignment

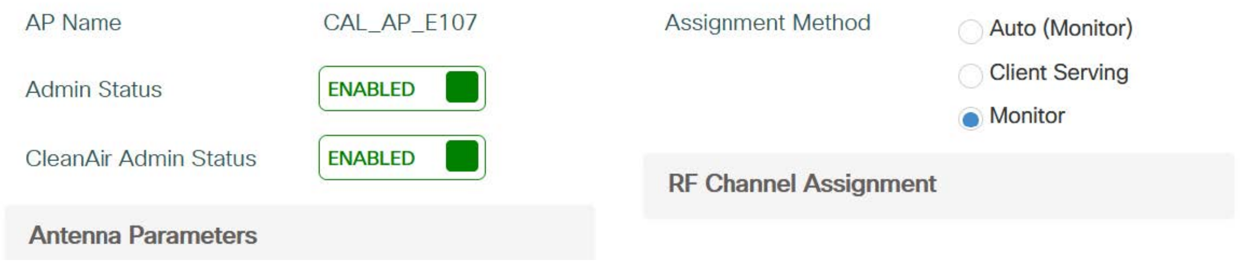
Assignment Method: ● Auto (Client Serving) ○ Client Serving ○ Monitor

RF Channel Assignment

Current Channel: 52

Channel Width: 20 MHz ▾

Assignment Method: Global ▾



AP Name: CAL_AP_E107

Admin Status: ENABLED 🟩

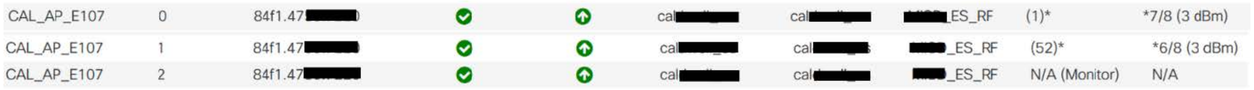
CleanAir Admin Status: ENABLED 🟩

Antenna Parameters

Assignment Method: ○ Auto (Monitor) ○ Client Serving ● Monitor

RF Channel Assignment

Here is tri radio in action, with slot 0 (2.4GHz) serving clients on channel 1, slot 1 (5GHz) serving clients on channel 52, and slot2 used for dedicated monitor mode.



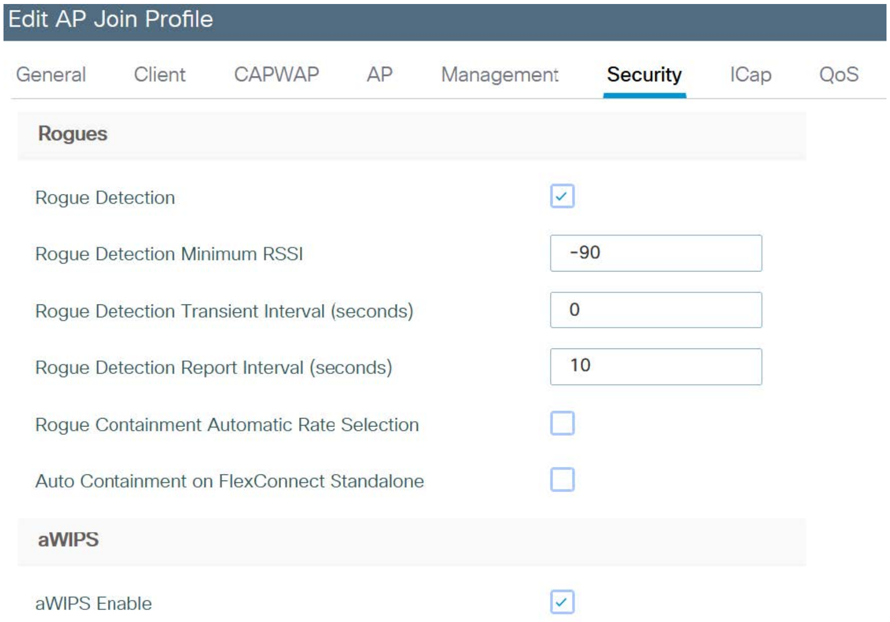
| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CAL_AP_E107 | 0 | 84f1.47[redacted] | ✓ | ⬆ | cal[redacted] | cal[redacted] | [redacted]_ES_RF | (1)* | *7/8 (3 dBm) |
| CAL_AP_E107 | 1 | 84f1.47[redacted] | ✓ | ⬆ | cal[redacted] | cal[redacted] | [redacted]_ES_RF | (52)* | *6/8 (3 dBm) |
| CAL_AP_E107 | 2 | 84f1.47[redacted] | ✓ | ⬆ | cal[redacted] | cal[redacted] | [redacted]_ES_RF | N/A (Monitor) | N/A |

If you plan on trying this out, I suggest you read this document first: Cisco Access Points with Tri-Radio

Now that I've prepped our infrastructure to better listen to rogues, let's get our controllers configured for WIPS and rogues to achieve our first task…

## Detect Threats Immediately

We start by enabling rogue detection and a WIPS under the AP join profile, which pushes the configuration to all APs. We can visit Monitor>WIPS to start seeing threats immediately.



Edit AP Join Profile

Rogues

| | |
|---|---|
| Rogue Detection | ☑ |
| Rogue Detection Minimum RSSI | -90 |
| Rogue Detection Transient Interval (seconds) | 0 |
| Rogue Detection Report Interval (seconds) | 10 |
| Rogue Containment Automatic Rate Selection | □ |
| Auto Containment on FlexConnect Standalone | □ |

aWIPS

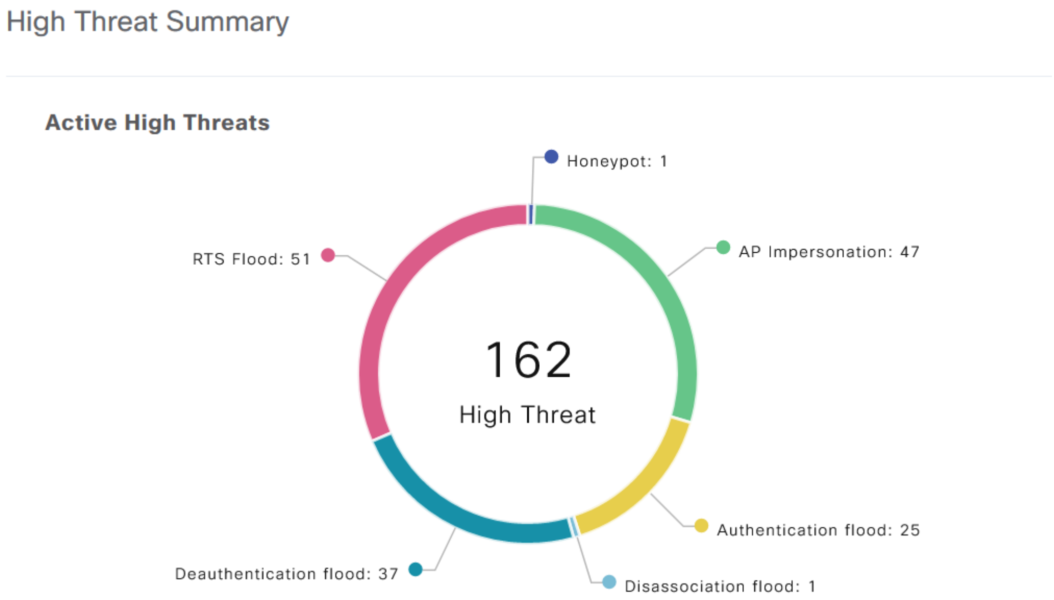
| | |
|---|---|
| aWIPS Enable | ☑ |

Since I have DNA Center (DNAC), I also want to take advantage of that to enable rogue and WIPS. As soon as I do this, DNAC will push a configuration to the controller. This will ask the controller to add to DNAC the WIPS and rogue configuration to the telemetry data its streaming. Not that you have to worry about the configuration, but the config pushed by DNAC to the controller looks something like this:

```
telemetry ietf subscription 9991
encoding encode-tdl
filter tdl-uri /services;serviceName=rogue_oper/rogue_client_data
source-address 10.1.251.11
stream native
update-policy on-change
receiver ip address 10.1.253.100 25103 protocol tls-native profile sdn-network-infra-iwan
telemetry ietf subscription 9992
encoding encode-tdl
filter tdl-uri /services;serviceName=rogue_oper/rogue_data
source-address 10.1.251.11
stream native
update-policy on-change
receiver ip address 10.1.253.100 25103 protocol tls-native profile sdn-network-infra-iwan
telemetry ietf subscription 9993
encoding encode-tdl
filter tdl-uri /services;serviceName=ewlc_oper/awips_alarm
source-address 10.1.251.11
stream native
update-policy on-change
receiver ip address 10.1.253.100 25103 protocol tls-native profile sdn-network-infra-iwan
```

With this, the controller will immediately start streaming WIPS and rogue data to DNAC. Now we have a single point of visibility and management for rogue and WIPS.

Here is an example of some of the threats detected by controller and pushed to DNAC. You should also be mindful of a bug that causes an AP to detect itself as rogue (click for details).

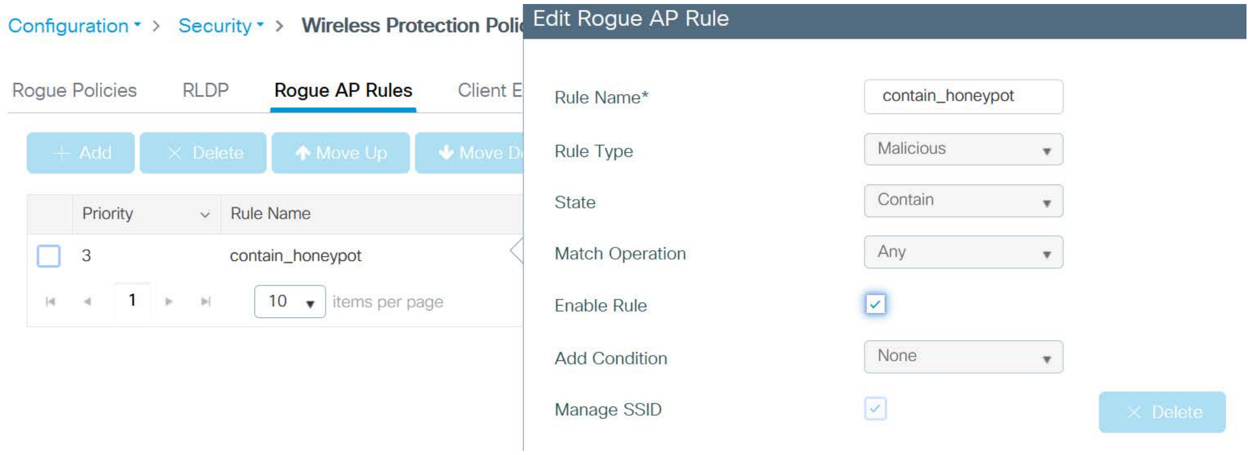


Now that we have our detection working, we can start to look at our second task…

## Ability to Contain Devices that are Performing Attacks

Containment can be done automatically based on certain rules or it can be done manually. You need to be aware of a legal aspect to containment before containing a device.

Let's say I want to automatically mark a rogue as malicious and contain it if it is advertising the same SSID as my corporate infrastructure (honeypot).



Configuration > Security > Wireless Protection Poli

Rogue Policies | RLDP | Rogue AP Rules | Client E

+ Add | × Delete | Move Up | Move D

| Priority | Rule Name |
|---|---|
| 3 | contain_honeypot |

1 | 10 items per page

Edit Rogue AP Rule

Rule Name* contain_honeypot

Rule Type Malicious

State Contain

Match Operation Any

Enable Rule ☑

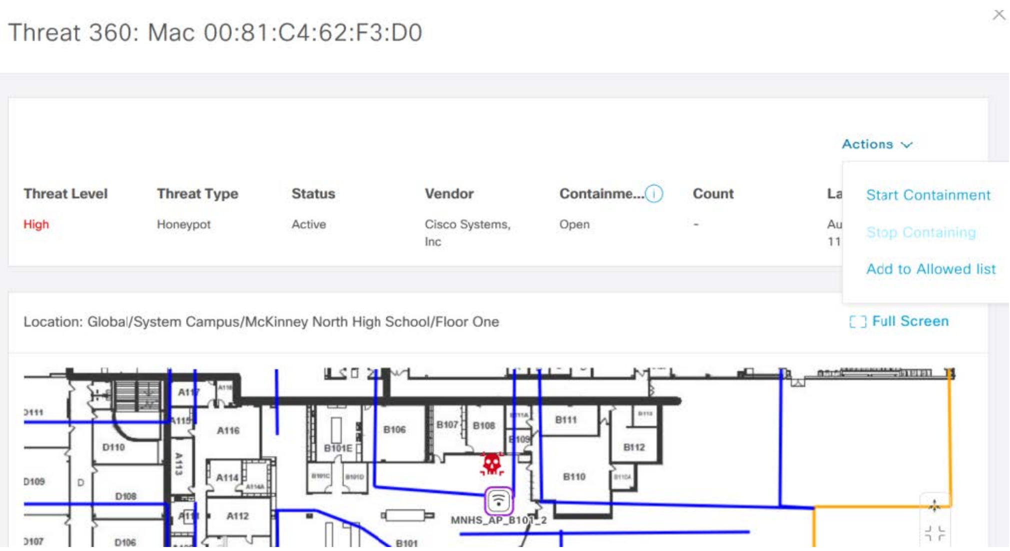
Add Condition None

Manage SSID ☑

× Delete

You can get as creative as you want here! Even if the AP is contained, one might be interested to know the details of this AP and location of this rogue.

Another option is to contain the threat manually through DNA Center:



Threat 360: Mac 00:81:C4:62:F3:D0

Actions

| Threat Level | Threat Type | Status | Vendor | Containme... | Count | La |
|---|---|---|---|---|---|---|
| High | Honeypot | Active | Cisco Systems, Inc | Open | - | Au 11 |

Start Containment
Stop Containing
Add to Allowed list

Location: Global/System Campus/McKinney North High School/Floor One

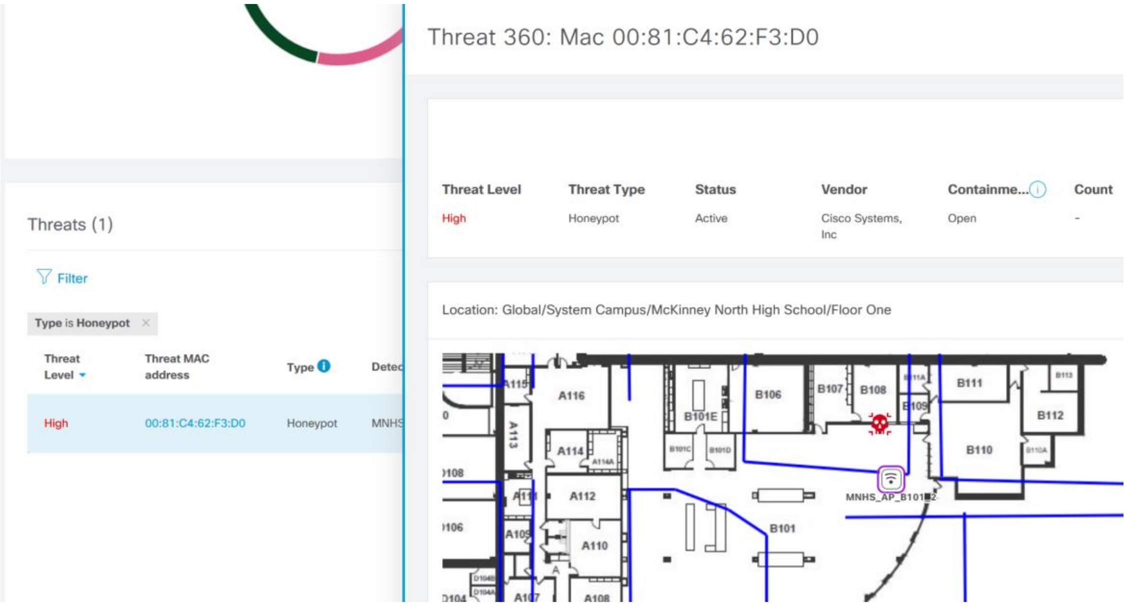
Full Screen

Which brings us to the third objective…

## Find the Attack Device Location

We need some kind of location-based engine in order to add location attribute to the devices, APs, interferers, rogues, attackers, etc. DNA Spaces does a great job at this and provides a comprehensive view of the floor with all elements.

Your point of location management is still DNA Center; DNA Spaces syncs its map with DNA Center and, in this case, acts more like an engine to push location data to DNA Center. By simply clicking the alert details, DNA Center takes me to the exact location of the honeypot device, thanks to DNA Spaces.



Threats (1)

Filter

Type is Honeypot ×

| Threat Level | Threat MAC address | Type | Detec |
|---|---|---|---|
| High | 00:81:C4:62:F3:D0 | Honeypot | MNHS |

Threat 360: Mac 00:81:C4:62:F3:D0

| Threat Level | Threat Type | Status | Vendor | Containme... | Count |
|---|---|---|---|---|---|
| High | Honeypot | Active | Cisco Systems, Inc | Open | - |

Location: Global/System Campus/McKinney North High School/Floor One

With every new release of software version, we are seeing more and more signatures being added, which brings us to the final goal…

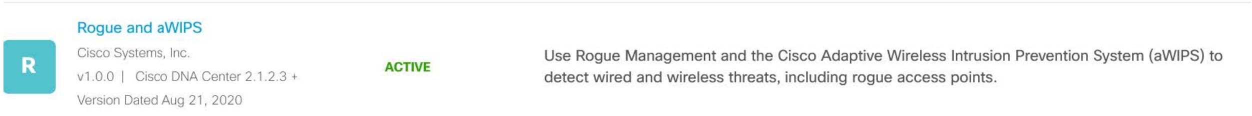
## Keep the System Signature Up to Date

Manually updating the intrusion prevention signature on the system to detect new threats is something handled by Cisco. For instance, prior to IOS-XE 7.5 only limited signatures were supported but that list grew much longer with 17.5. Cisco also gives you the ability to download static signature packages. If you are interested in this, I recommend that you work with Cisco Technical Assistance Center (TAC).

| Prior to IOS-XE 17.5 | With 17.5 |
|---|---|
| Authentication Flood Alarm | Deauthentication Flood by Pair |
| Association Flood Alarm | Fuzzed Beacon |
| Broadcast Probe Flood Alarm | Fuzzed Probe Request |
| Disassociation Flood Alarm | Fuzzed Probe Response |
| Broadcast Dis-Association Flood Alarm | PS Poll Flood by Signature |
| De-Authentication Flood Alarm | Eapol Start V1 Flood by Signature |
| Broadcast De-Authentication Flood Alarm | Reassociation Request Flood by Destination |
| EAPOL-Logoff Flood Alarm | Beacon Flood by Signature |
| CTS Flood Alarm | Probe Response Flood by Destination |
| RTS Flood Alarm | Block Ack Flood by Signature |

| | |
|---|---|
| | Airdrop Session |
| | Malformed Association Request |
| | Authentication Failure Flood by Signature |
| | Invalid MAC OUI by Signature |
| | Malformed Authentication |

Last, but certainly not least, you can also consume WIPS data with other applications. DNA Center has APIs for WIPS. To use it, make sure to activate the WIPS API bundle.

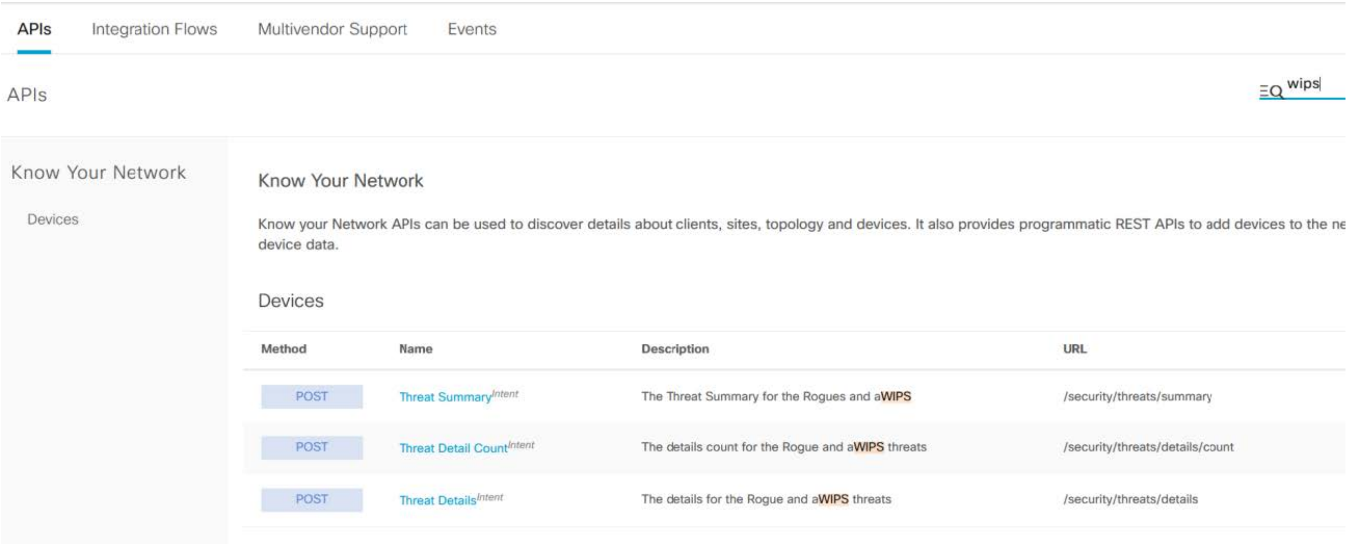


Rogue and aWIPS
Cisco Systems, Inc.
v1.0.0 | Cisco DNA Center 2.1.2.3 +
Version Dated Aug 21, 2020

ACTIVE

Use Rogue Management and the Cisco Adaptive Wireless Intrusion Prevention System (aWIPS) to detect wired and wireless threats, including rogue access points.

Under "Develop Tools" search for "WIPS" and it will show all supported API calls that you can make.

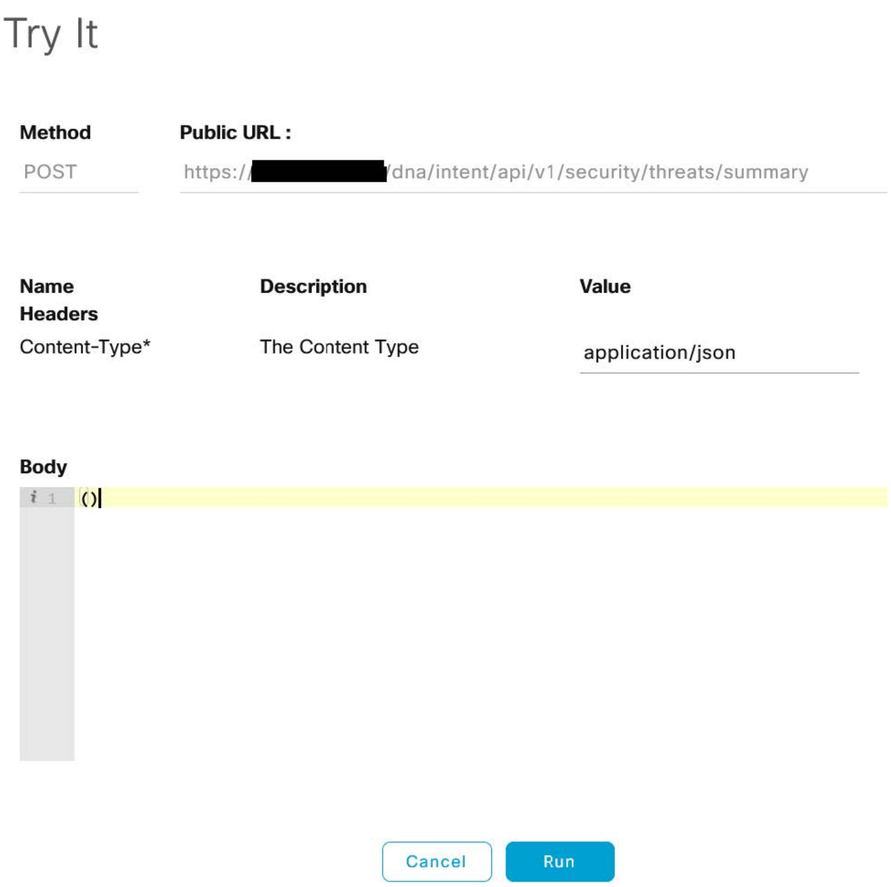


Know Your Network

Know your Network APIs can be used to discover details about clients, sites, topology and devices. It also provides programmatic REST APIs to add devices to the ne
device data.

Devices

| Method | Name | Description | URL |
|---|---|---|---|
| POST | Threat Summary Intent | The Threat Summary for the Rogues and aWIPS | /security/threats/summary |
| POST | Threat Detail Count Intent | The details count for the Rogue and aWIPS threats | /security/threats/details/count |
| POST | Threat Details Intent | The details for the Rogue and aWIPS threats | /security/threats/details |



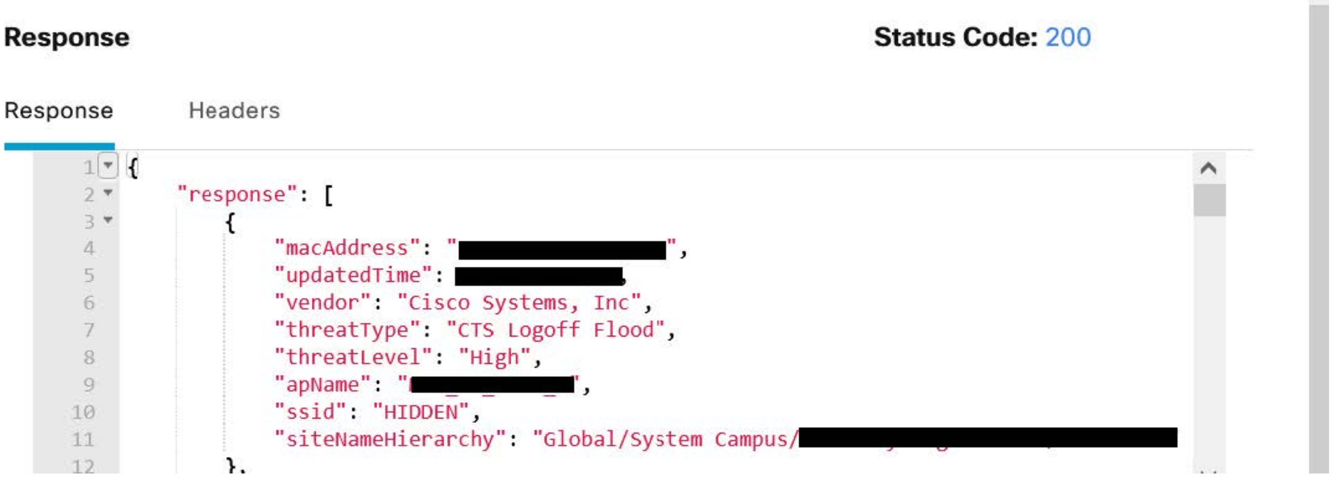
## Try It

| Method | Public URL : |
|---|---|
| POST | https://[redacted]/dna/intent/api/v1/security/threats/summary |

| Name | Description | Value |
|---|---|---|
| **Headers** | | |
| Content-Type* | The Content Type | application/json |

**Body**

```
{}
```



**Response** **Status Code:** 200

```
{
    "response": [
        {
            "macAddress": "[redacted]",
            "updatedTime": [redacted],
            "vendor": "Cisco Systems, Inc",
            "threatType": "CTS Logoff Flood",
            "threatLevel": "High",
            "apName": "[redacted]",
            "ssid": "HIDDEN",
            "siteNameHierarchy": "Global/System Campus/[redacted]
        },
```

## Conclusion

One of the goals of Cisco DNA Center, Wireless Infrastructure, and DNA Spaces is to provide visibility into your network for Rogue and WIPS. If you already have DNA Center, then you can start taking advantage of it and using this feature simply by installing the WIPS package and activating it.

I hope you gained some valuable information and insight for your network. If you plan to try it out, I highly encourage you do so in a test environment first.

If you have any questions, please reach out to your DSI account manager or email sales@dsitech.com. They can get put you in touch with me directly and we can talk about it further.

See you next month with a new topic!

## Resources

Bug Search Tool Example – AP Reporting its own MAC as Rogue

Cisco Access Points with Tri-Radio

Cisco Adaptive WIPS Deployment Guide

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.4.x

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.5.x

Cisco Technical Assistance Center (TAC)

### Common Attacks & Signatures

| | |
|---|---|
| Airdrop Session | Airdrop session refers to the Apple feature named AirDrop. AirDrop is used to setup a peer-to-peer link for file sharing. This might create a security risk due to unauthorized peer-to-peer networks dynamically created in your WLAN environment. |
| Authentication Failure Flood by Signature | Authentication Failure Flood is when a specific device tries to flood the AP with invalid authentication requests spoofed from a valid client. This results in disconnection. |

| | |
|---|---|
| Beacon Flood by Signature | Beacon Flood is when stations actively search for a network bombarded with beacons from networks generated using different MAC addresses and SSIDs. This flood prevents a valid client to detect beacons sent by corporate APs. This initiates a Denial-of-Service attack. |
| Block Ack Flood by Signature | Block Ack Flood is when an attacker transmits an invalid Add Block Acknowledgement (ADDBA) frame to AP while spoofing the MAC address of the valid client. This process causes AP to ignore any valid traffic transmitted from the client until it reaches the invalid frame range. |
| Deauthentication Flood by Pair | In the enhanced context of threat, both source (attacker) and destination (victim) of attacks (Track by Pair) have visibility. |
| EAPOL Start V1 Flood by Signature | EAPOL Start Flood is when an attacker attempts to bring down an AP by flooding it with EAPOL-Start frames to exhaust the AP internal resources. |
| Fuzzed Beacon | Fuzzed Beacon is when invalid, unexpected, or random data is introduced in the beacon and replays those modified frames into the air. This causes unexpected behavior on the destination device that includes driver crashes, operating system crashes, and stack-based overflows. This in turn allows execution of arbitrary code of the affected system. |
| Fuzzed Probe Request | Fuzzed Probe Request is when invalid, unexpected, or random data is introduced in the probe request and replays those modified frames into the air. |
| Fuzzed Probe Response | Fuzzed Probe Response is when invalid, unexpected, or random data is introduced in the probe response and replays those modified frames into the air. |
| Invalid MAC OUI by Signature | Invalid MAC OUI is when a spoofed MAC address is used that does not have a valid OUI. |

| | |
|---|---|
| Malformed Association Request | Malformed Association Request is when an attacker sends a malformed association request to trigger bugs in AP. This results in Denial-of-Service. |
| Malformed Authentication | Malformed Authentication is when an attacker sends malformed authentication frames that can expose vulnerabilities in some drivers. |
| Probe Response Flood by Destination | Probe Response Flood is when a device tries to flood the clients with a large number of spoofed probe responses from AP. This prevents clients from detecting the valid probe response sent by the corporate APs. |
| PS Poll Flood by Signature | PS Poll Flood is when a potential hacker spoofs the MAC address of the wireless client and sends out a flood of PS poll frames. The AP sends out the buffered data frames to the wireless client. This results in client missing the data frames as it could be in the power safe mode. |
| Reassociation Request Flood by Destination | Reassociation Request Flood is when a specific device tries to flood the AP with a large number of emulated and spoofed client re-associations, to exhaust the APs resources, particularly the client association table. Once the client association table overflows, the legitimate clients are not able to associate, causing a DoS attack. |

## About the Author

Ambuj Mahendra is a Cisco Certified Internetwork Expert (CCIE) and Certified Wireless Network Expert (CWNE) with 15 years of industry experience. He currently works as a Network Solutions Architect for DISYS Solutions Inc. (DSI).