
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Understanding Wireless Security

And the Implications for Secure Wireless Network Design

Mark Krischer, Principal Wireless Architect, Asia Pacific, Japan & Greater China
@mkrisch

BRKEWN-3004

Abstract

This session will explore secure wireless network design, with a key focus on the latest WPA3 and Wi-Fi 6 standards. Mobility brings unique challenges to network security, such as the need for secure fast roaming. Participants will learn how 802.11 addresses theses requirements, and explore the changes WPA3 brings and the implications for wireless deployments. We will also address specific scenarios such as BYOD, Cloud Identity Providers and Zero Trust.

This session will also explore how Cisco DNA Center expands upon the wireless security standards with Rogue AP detection and location, and Advanced Wireless Intrusion Detection and Prevention, including upcoming capabilities. The intent is to provide a deeper understanding, not just about the security capabilities themselves, but to do so from the perspective of the attacks that they defend against.

Cisco Webex App

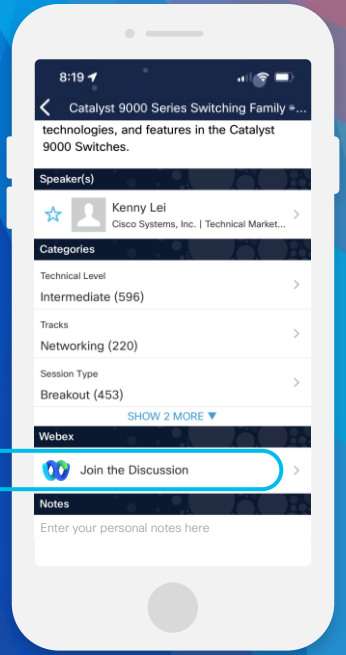
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-3004

Agenda

- Wireless Security Fundamentals
  - WPA3
  - Authentication and Authorization
  - Wi-Fi 6E Security
- Rogue Detection and Advanced WIPS
  - Threat 360˚
  - Rogue Detection and Containment
  - Advanced Wireless Intrusion Prevention

Wireless Security Fundamentals

cisco Live!

Wireless Attack Surface

- Wireless networks propagate beyond the physical constraints of the wired network
- Attacks may originate from anywhere within the wireless coverage
  - Passive scanning attacks
  - Layer 2 active spoofing attacks
  - Layer 1 active jamming or DoS attacks
  - Rogue APs
    - Honeypot and Evil Twin APs
    - Unsecured backdoor access

Securing the Wireless Network

Wireless Protected Access

WPA	• A snapshot of the 802.11i Wireless Security Standard • Commonly used with TKIP encryption
WPA2	• Final version of 802.11i Wireless Security Standard • Commonly used with AES encryption
Authentication Mechanisms	• Personal (PSK – Pre-Shared Key) • Enterprise (802.1X/EAP)
WPA3	• Wi-Fi Alliance security update • Includes new capabilities and new certification requirements

WPA3

- Mandatory for Wi-Fi 6 Certification
- Remove insecure legacy protocols
  - WEP
  - TKIP
  - SHA1
- Negative Testing
  - KRACK

- Protected Management Frames (802.11w)
- Simultaneous Authentication of Equals (SAE)

- Wi-Fi Certified Enhanced Open
  - Opportunistic Wireless Encryption (OWE)

802.11 Fundamentals

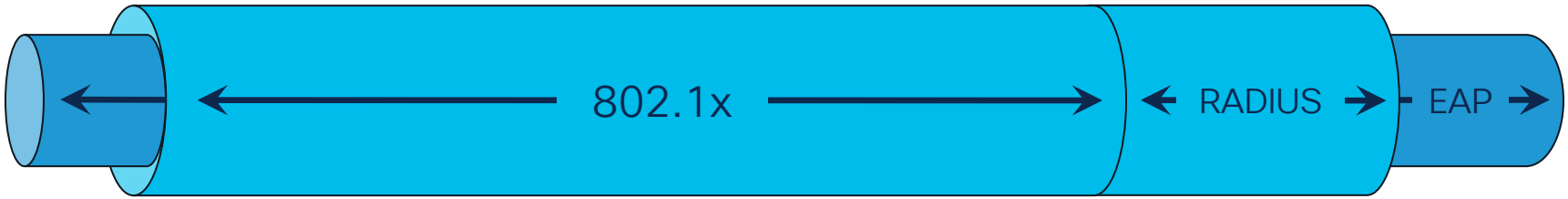
Authentication

802.11 Fundamentals

Authentication

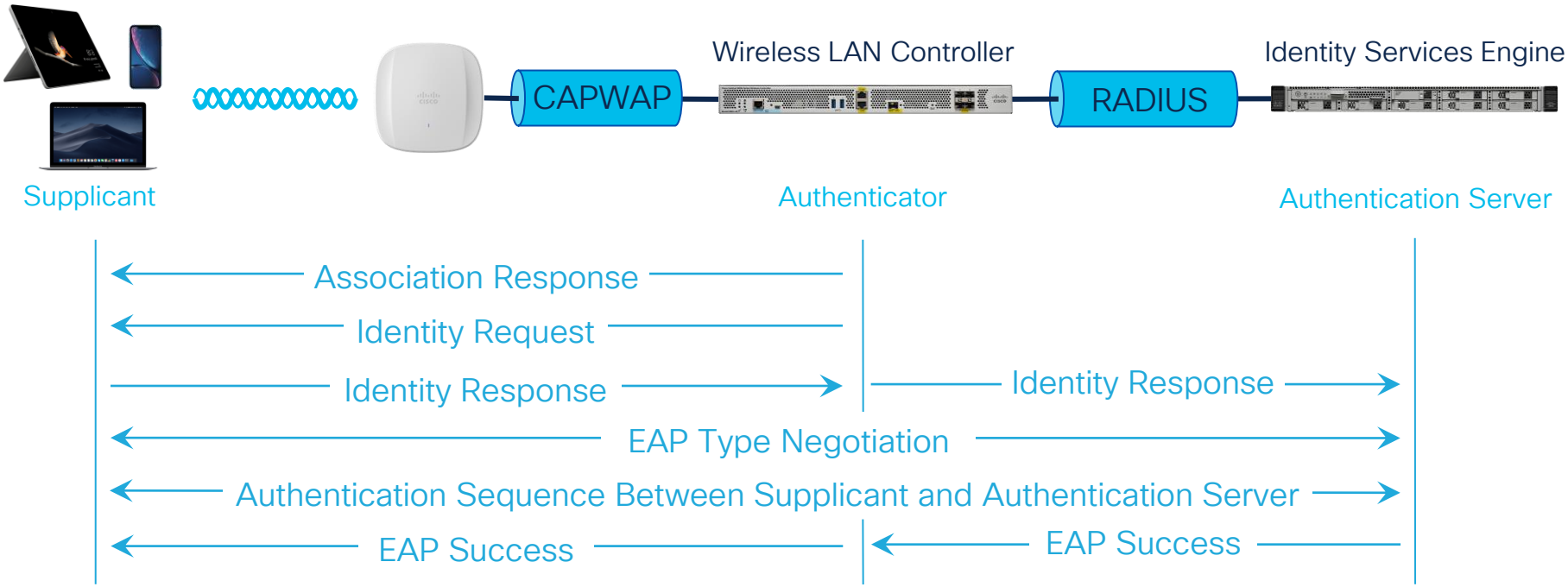
802.11 Fundamentals

Authentication



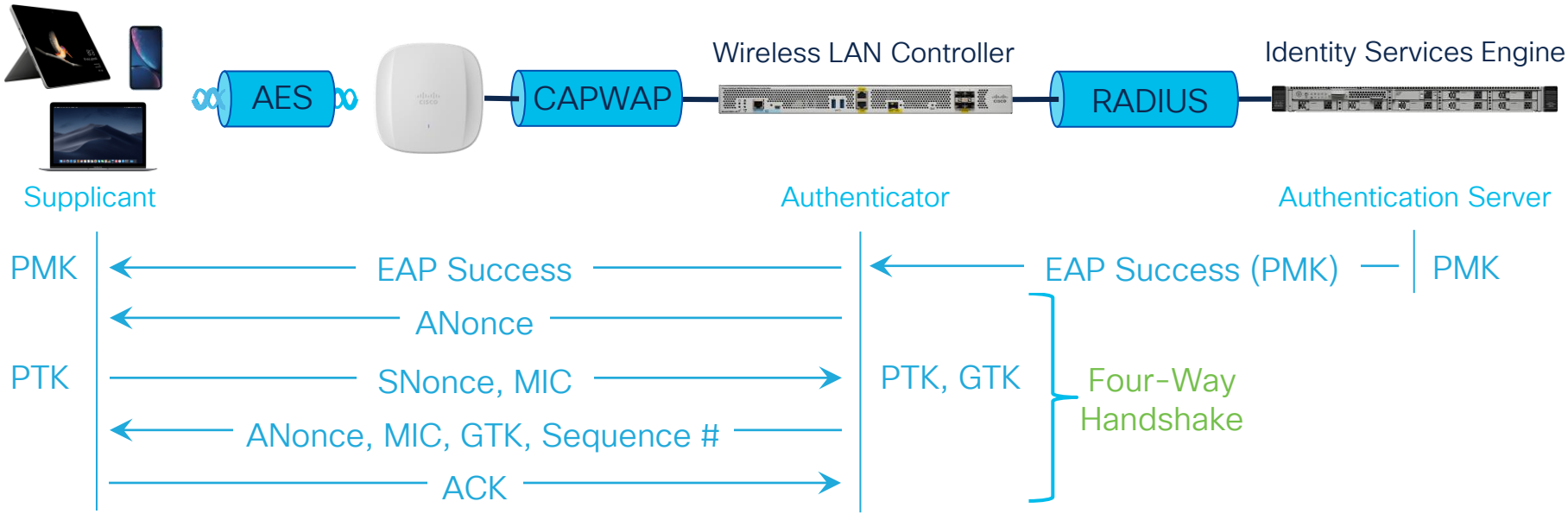
802.11 Fundamentals

Authentication



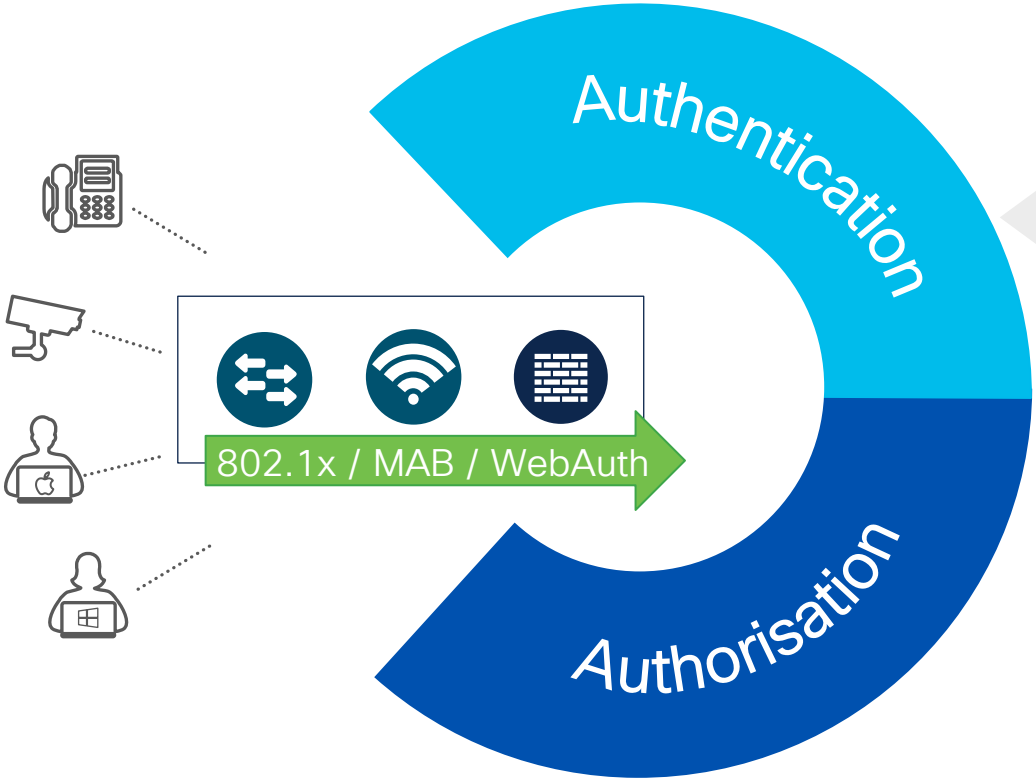
802.11 Fundamentals

Encryption



PTK = SHA(PMK + ANonce + SNonce + AP MAC + STA MAC)

Authentication and Authorisation



- Device Posture
- Device Type
- User Credentials
- MAC Address
- Identity Elements

- Location
- Day and Time
- Access Type
- Context

- Policy Elements
- VLAN/VN
- SGT / Group Policy
- QoS / BDRL
- URL Redirect / Filter
- Bonjour Service Policy
- Application Control

Authorization Options

URL-Redirect

Provide conditional web redirect when traffic is blocked

URL-Filter

Controls which FQDNs the endpoint can reach or not

Bandwidth

Control maximum bandwidth and burst rate per endpoint/user

Calendar Profile

Controls active hours for endpoint access.

Timer

Control session, idle-timeout, active hours

QoS

QoS Profile is assigned per endpoint

AVC Profile

Application Visibility Profile is assigned per endpoint

mDNS Profile

Assigns mDNS profile to broker mDNS advertisement

Open DNS

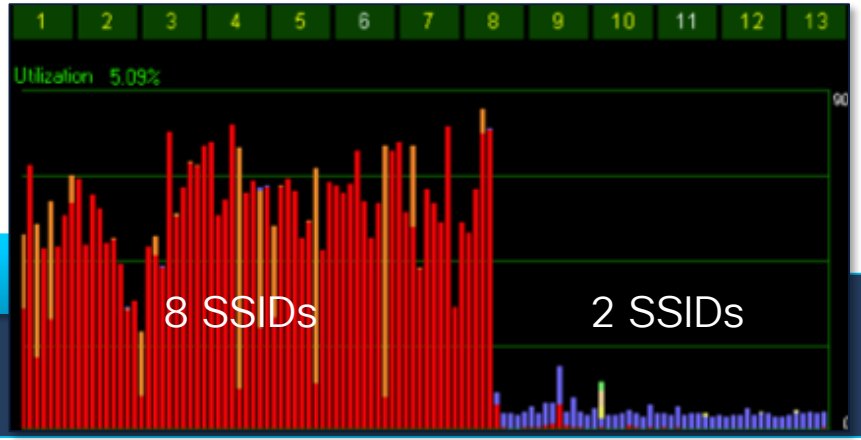
Assigns Open DNS profile to intercept DNS packets for custom response

Service Template & Roles

Assigns multiple access characteristics: VLAN, ACL, QoS, Timer, etc.

Authorisation

Network Segmentation



Static VLAN Assignment

- VLAN based on SSID
- VLAN segregation based on security policy

Dynamic VLAN Assignment

- VLAN based on authentication credentials
- VLAN segregation based on role

TrustSec / Group Based Policy / Software Defined Access

- Security based on TrustSec Scalable Group Tags instead of source and destination addresses
- ACLs applied at the packet level with enforcement across the network (or network fabric)

Secure Fast Roaming Challenges

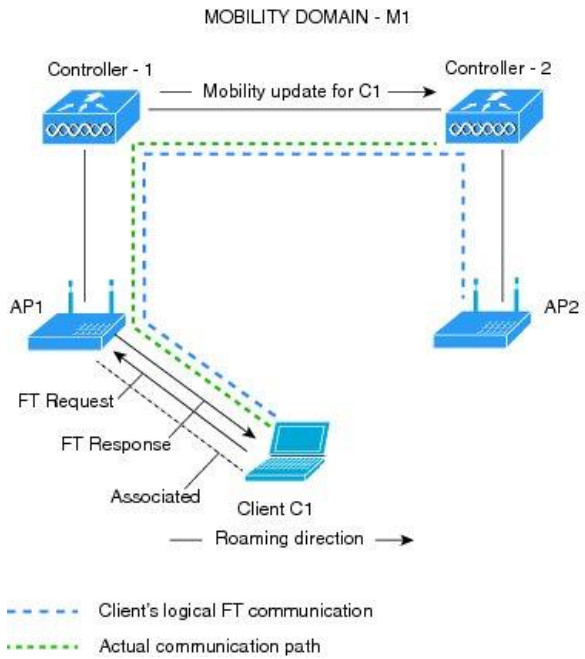
- Client channel scanning and AP selection
- Re-authentication of client device and re-keying

Secure Fast Roaming

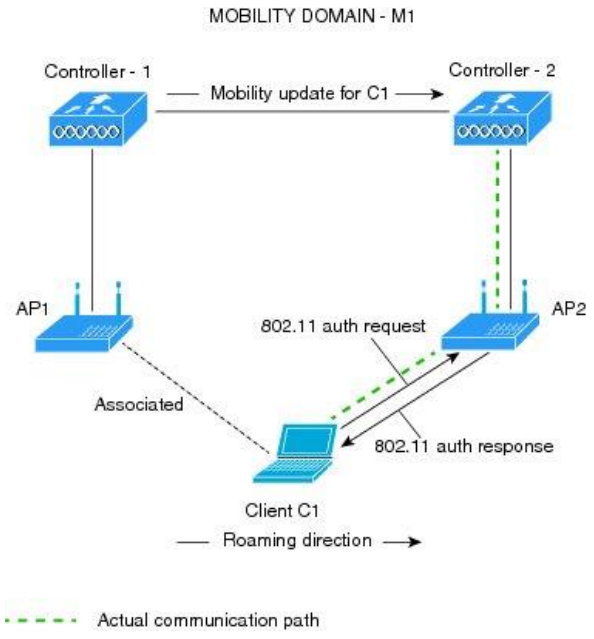
802.11k/v/r and Wi-Fi Agile Multiband

- Client channel scanning and AP selection
  - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
  - 802.11v BSS Transition
- Re-authentication of client device and re-keying
  - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

802.11r Fast Transition



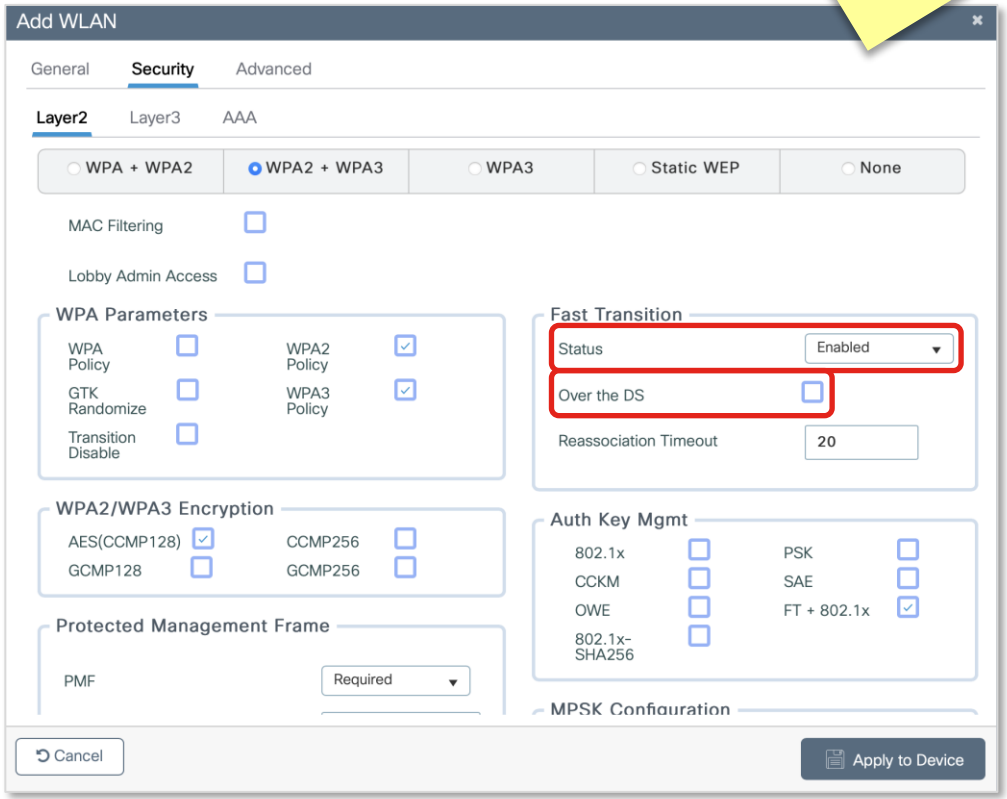
Over the DS



Over the Air

802.11r Fast Transition

- Over the Air is recommended for best client interoperability



Key Reinstallation AttaCK

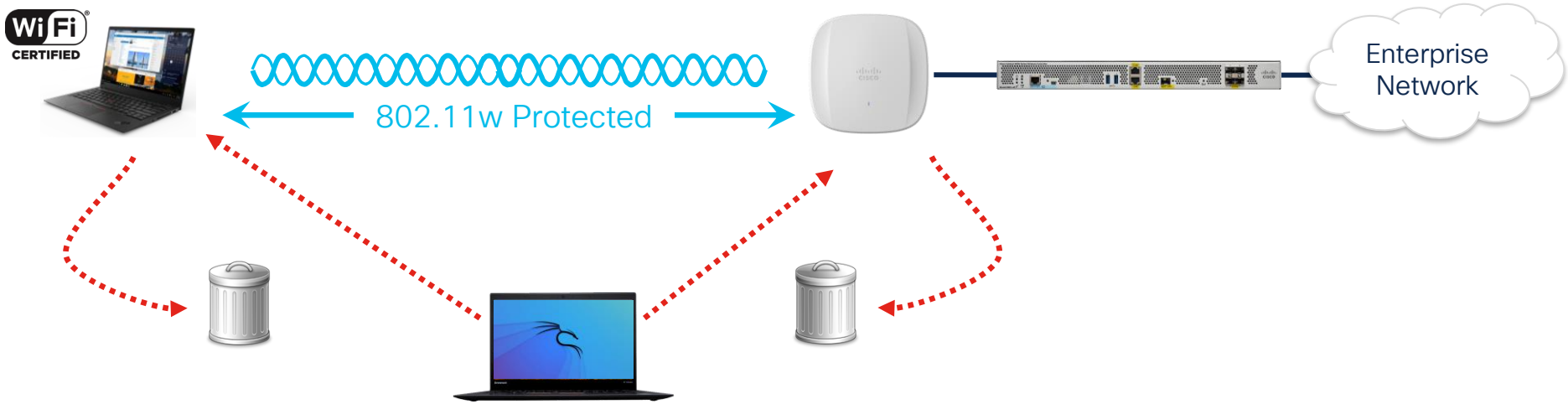
- 10 Vulnerabilities were discovered
  - May allow the reinstallation of keys already in use
- Only 1 impacts Access Points
  - Specific to 802.11r (Fast BSS Transition)
  - CVE-2017-13082

- This was an industry wide issue
  - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
  - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection and WIDS/WIPS can detect potential attack vectors

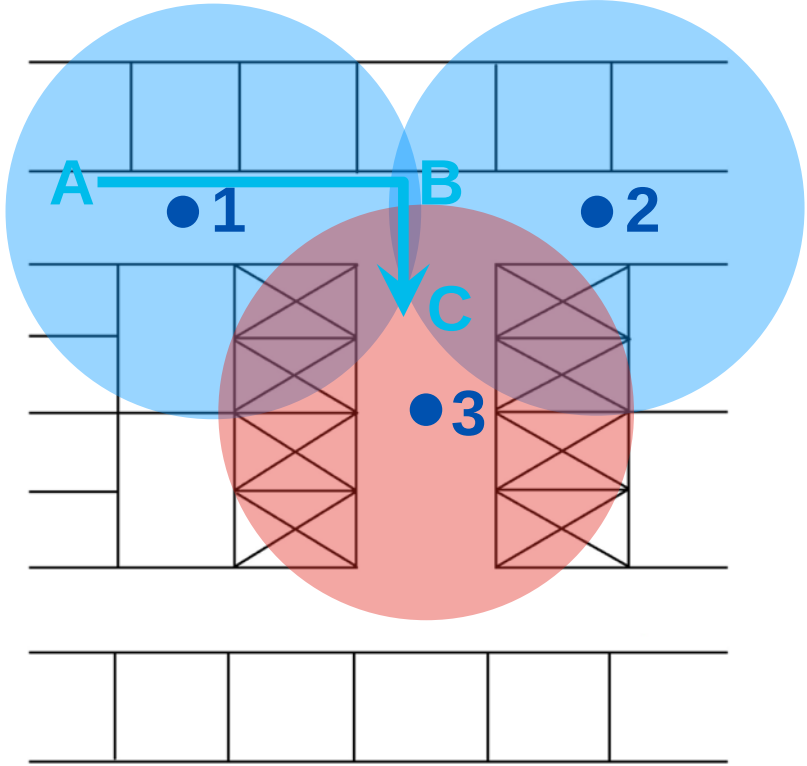
KrØØk Vulnerability

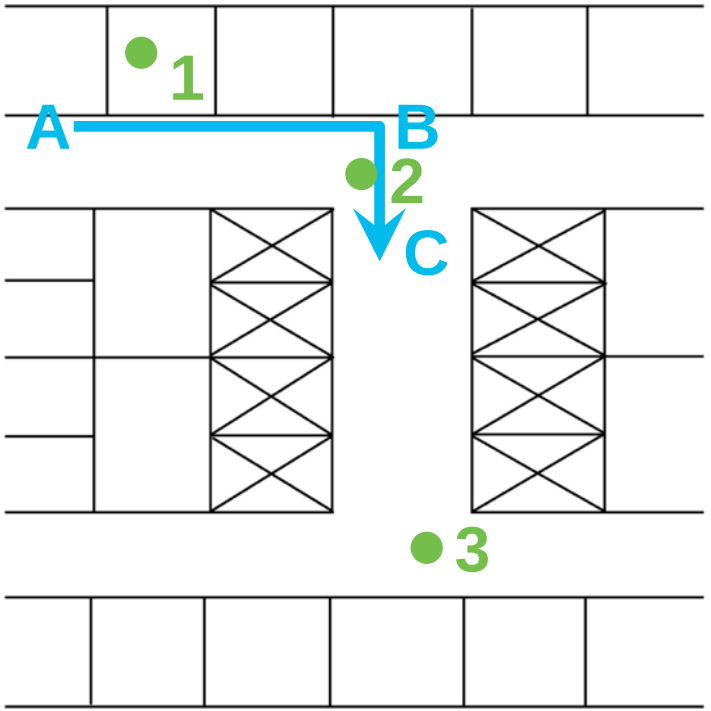
- On February 26th, 2020, researchers Štefan Svorencík and Robert Lipovsky disclosed a vulnerability in the packet processing of certain Wi-Fi chipsets
- This vulnerability could allow an unauthenticated, adjacent attacker to decrypt Wi-Fi frames without the knowledge of the PTK
- After an affected device handles a disassociation event, it could send a limited number of Wi-Fi frames encrypted with a static, weak PTK
- An attacker could exploit this vulnerability by triggering a disassociation and then acquiring these frames and decrypting them with the static PTK
- WIDS/WIPS can detect potential attack vectors

802.11w Protected Management Frames



AP Placement and Roaming Optimization

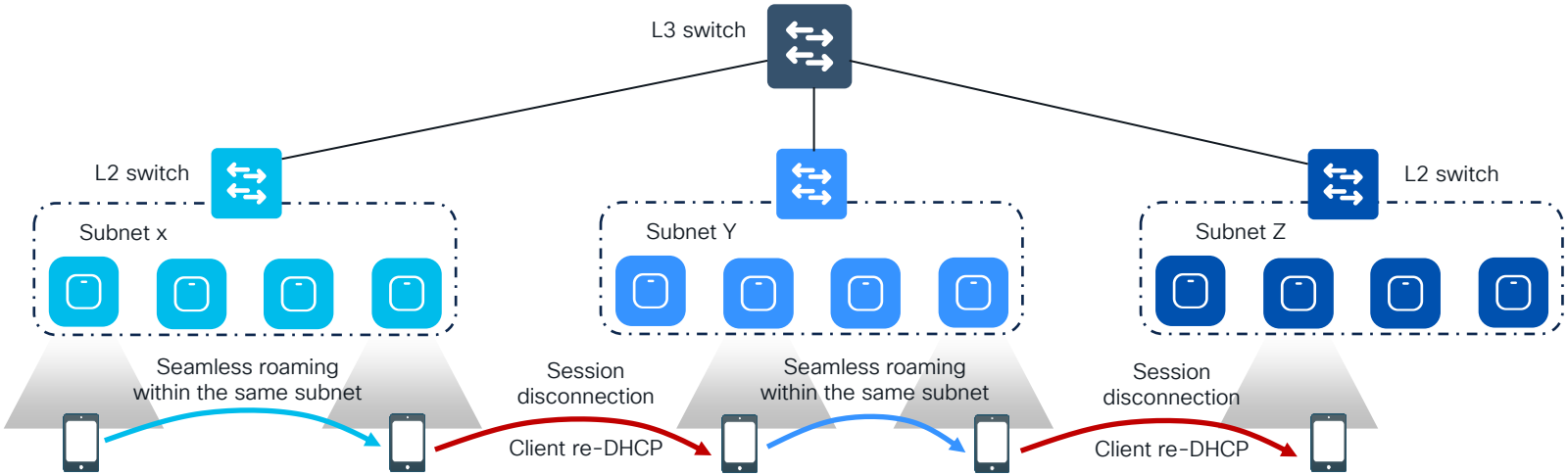




Seamless Roaming at Scale

For L2 seamless roaming everywhere need to span the same VLAN across all roaming domain

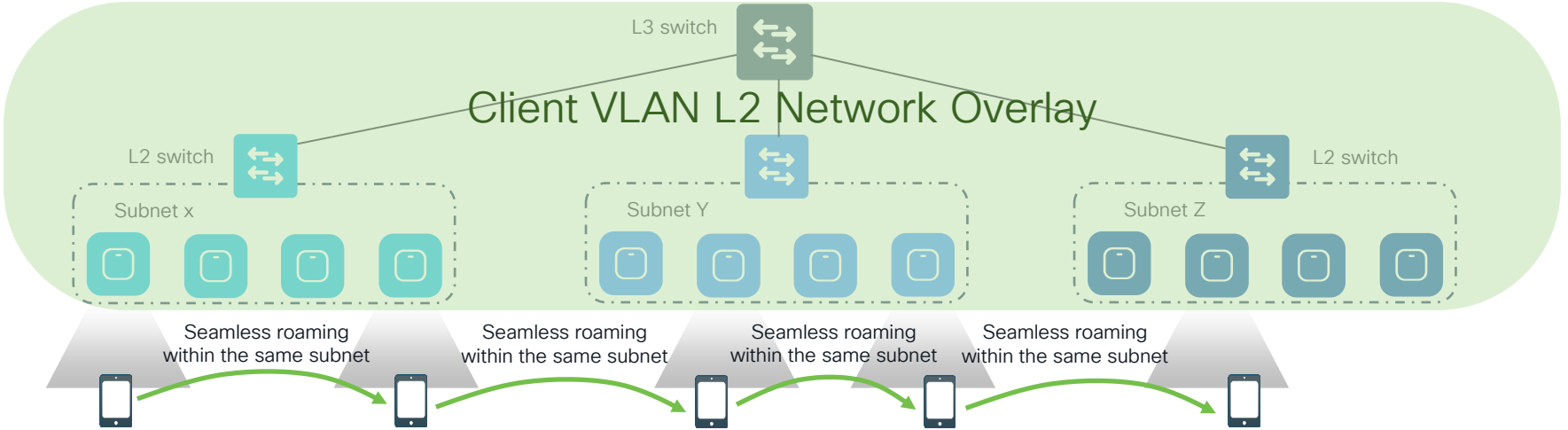
Large broadcast domains do not scale and is counter to networking best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

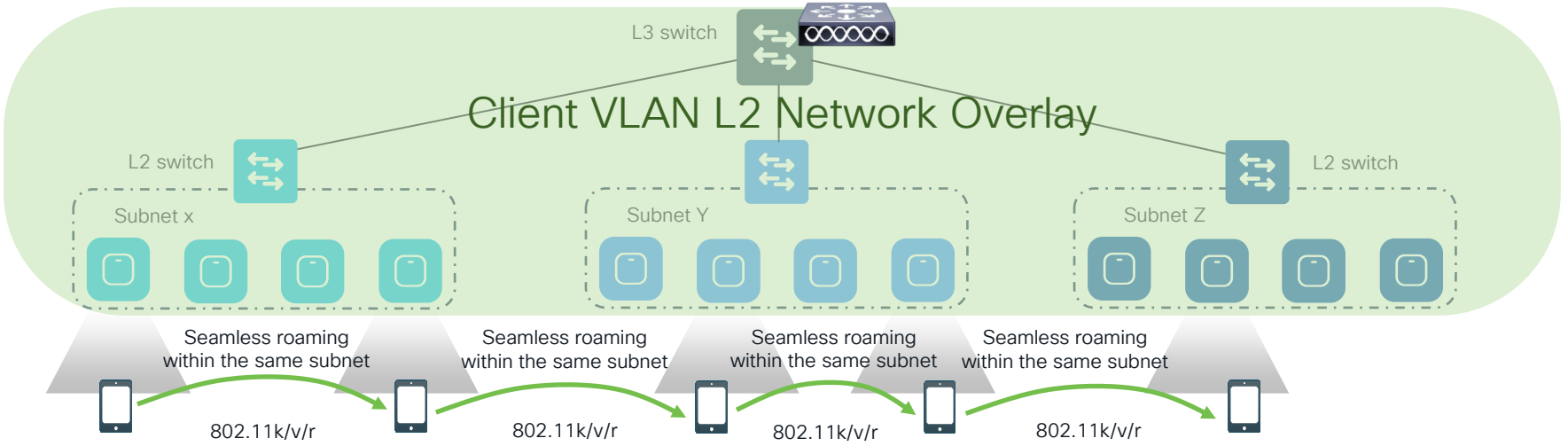
A data termination point is required to roam across L3 boundaries



Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

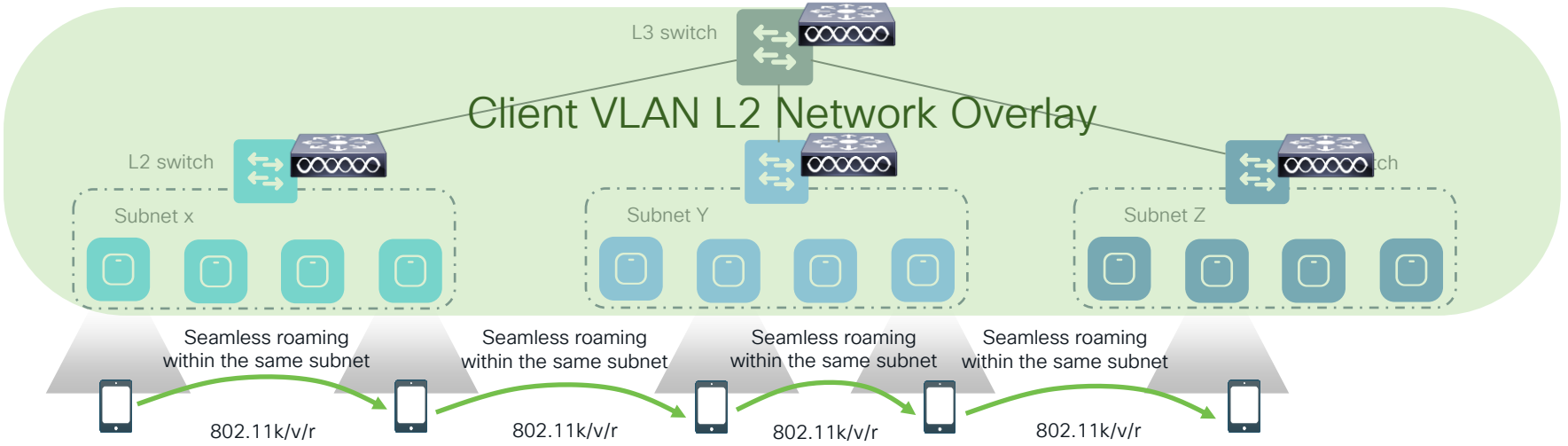
Can be deployed as centralized (CAPWAP / EoGRE) or distributed (fabric) architectures



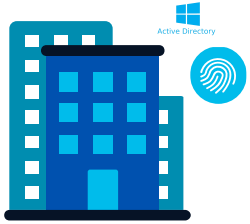
Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

Can be deployed as centralized (CAPWAP / EoGRE) or distributed (fabric) architectures



On-Prem and Cloud Identity



On-Prem Identity

802.1x, Network Access

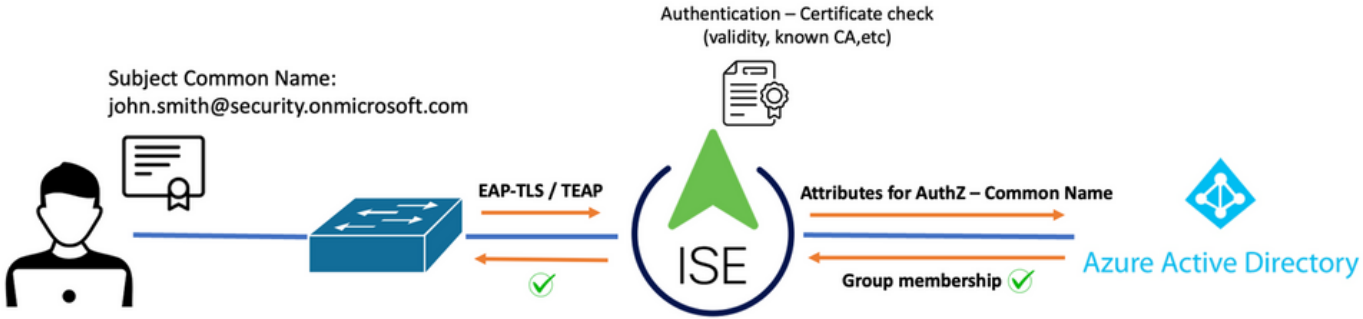
PEAP-MSCHAPv2,
EAP-FAST, EAP-TLS
PAP, MAC Auth Bypass

Cloud Identity

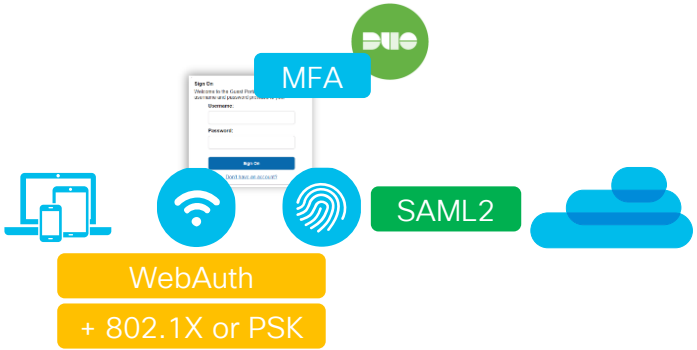
VPN, Application Access

SAMLv2, OpenID Connect

Cloud Identity with EAP-TLS



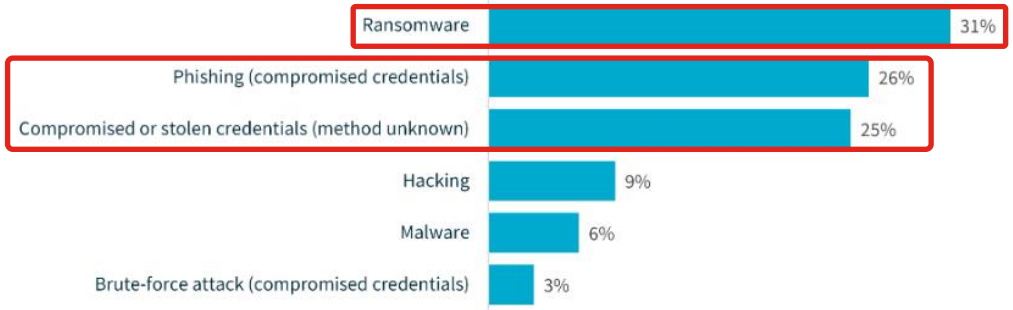
Multi-Factor Authentication



Zero Trust

41% of all data breaches resulted from cyber security incidents (162 notifications)

Cyber incident breakdown



- Ransomware
  - East/West Traversal
  - Authorisation
    - Micro-segmentation
  - Rapid Threat Containment

- Phishing and compromised or stolen credentials
  - Username/Password
  - Digital Certificates

Central Web Authentication

URL Redirect

Any Packet

RADIUS Access Request

RADIUS Access Accept

Network Access Granted
Redirect ACL

HTTP Packet

Redirect to ISE Web Page

Web Authentication Sequence

RADIUS CoA Request

RADIUS CoA ACK

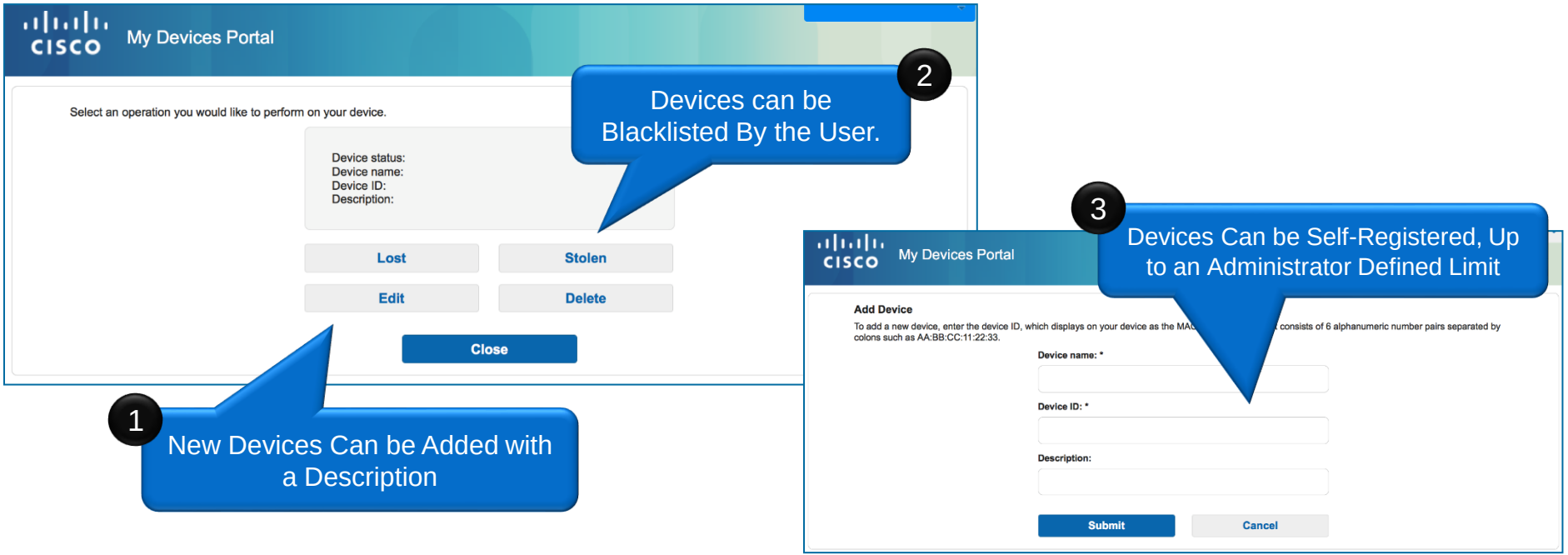
CoA Request
- Re-authenticate session
- Terminate session
- Terminate session with port bounce
- Disable host port

Central Web Authentication

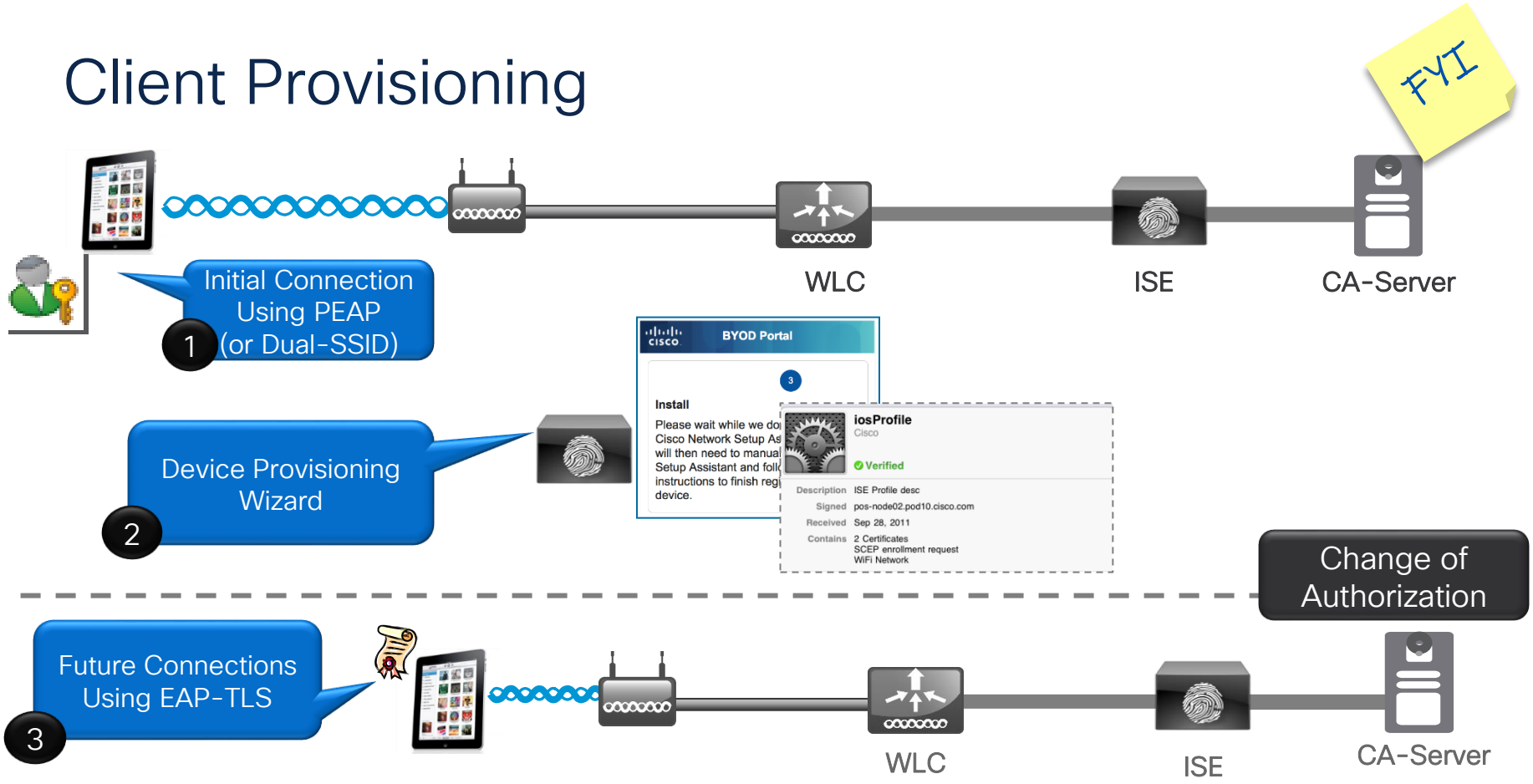
CENTRAL because the redirection URL, the pre-webauth ACL are **centrally** configured on ISE and dynamically communicated to the WLC (NAD*) via RADIUS. CWA is partially L2 (MAC Authentication) and partially L3 (redirect on IP resolution).

*Network Access Device

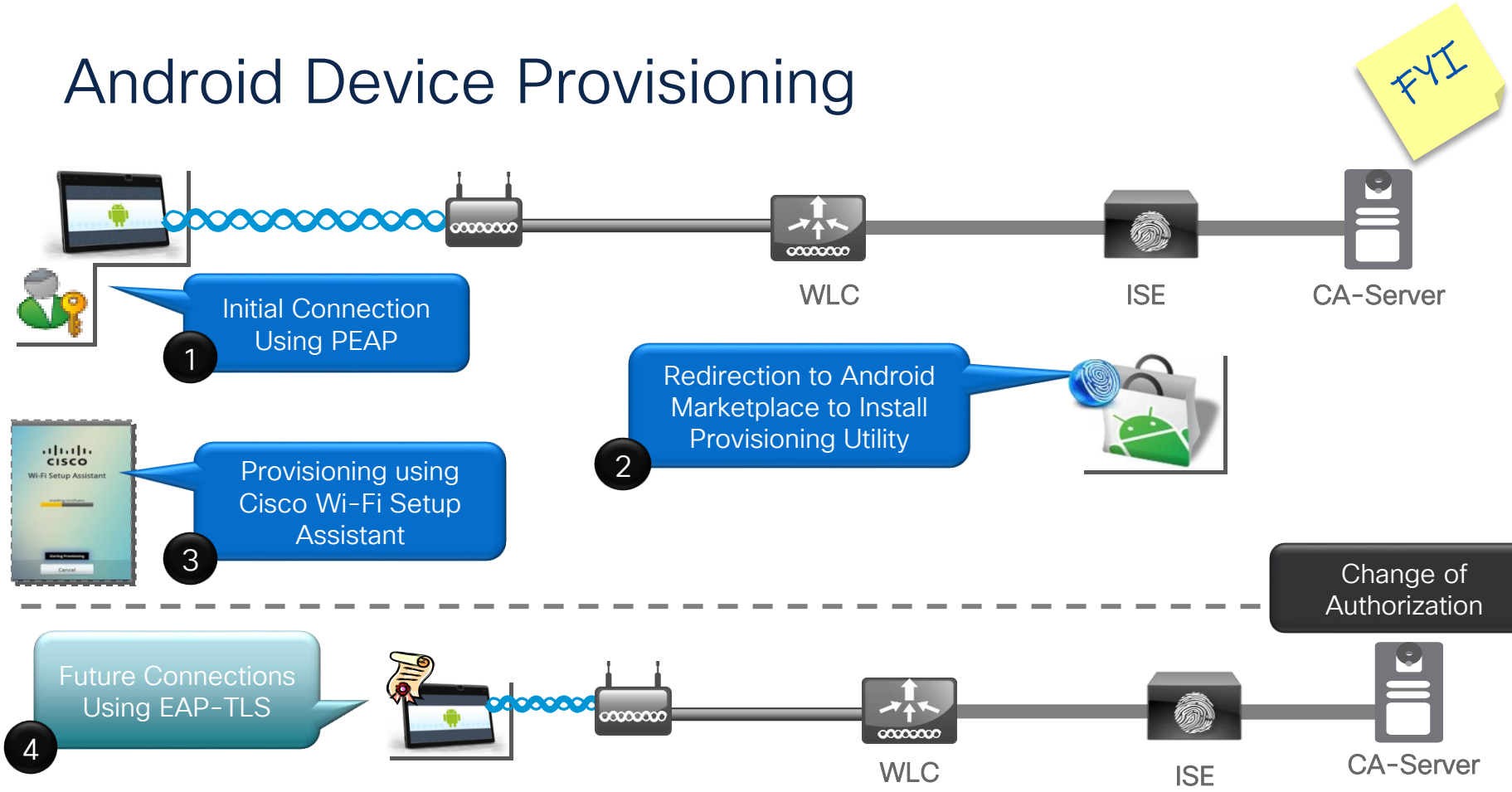
Self-Registration of BYOD Devices



Client Provisioning



Android Device Provisioning



Client Provisioning Policy

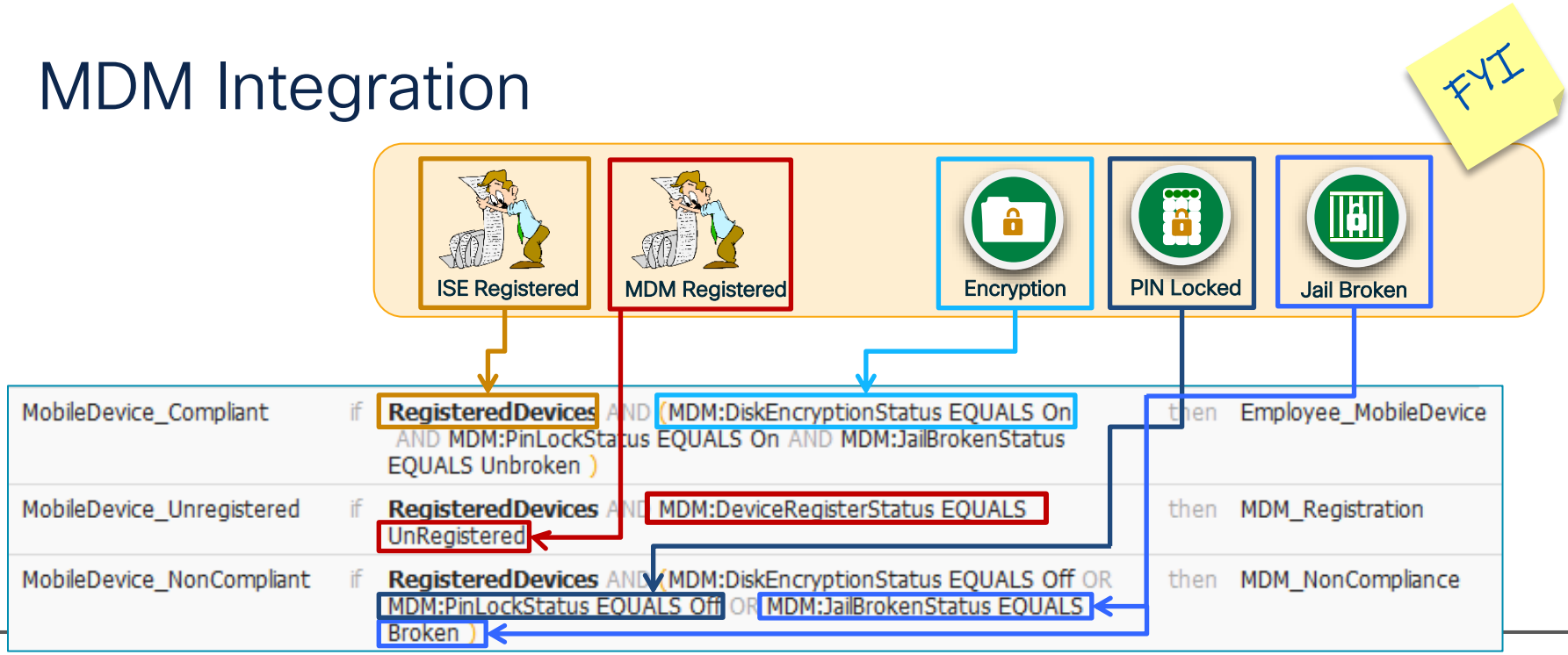
FYI

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Mac iOS All	and AD1:ExternalGroups EQUALS cts.l...	then WiFi_Profile
Android	If Any	and Android	and AD1:ExternalGroups EQUALS cts.l...	then WiFi_Profile
WinThings	If Any	and Windows...	and AD1:ExternalGroups EQUALS cts.l...	then WinSPWizard 1.0.0.14 And WiFi_Profile
MAC-OSX	If Any	and Mac OSX	and AD1:ExternalGroups EQUALS cts.l...	then MacOsXSPWizard 1.0.0.6 And WiFi_Profile

MDM Integration



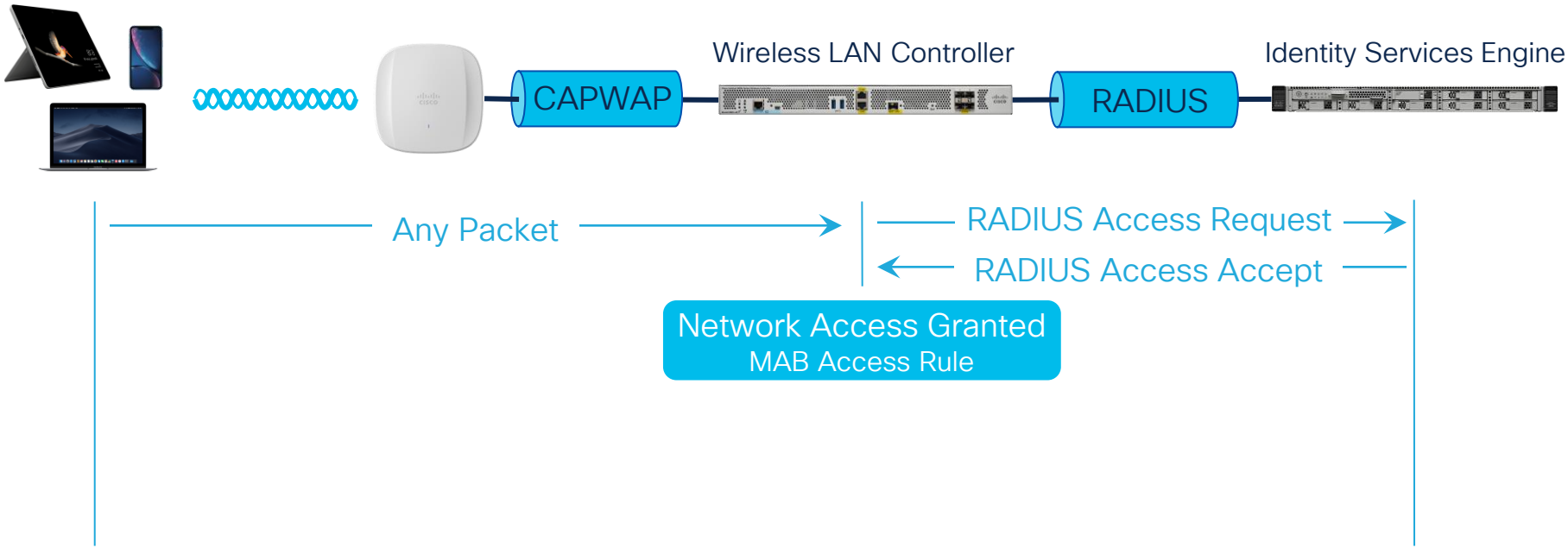
vmware airwatch · IBM MaaS360 by Fiberlink · Good · Tangoe · MobileIron · Symantec · SAP · Citrix XenMobile · Cisco Meraki

Captive Portal Detection

- Native operating system support to detect captive portals
- User is aware of captive portal even when not using browser
- Simplifies guest access adoption
- Avoids the need to redirect HTTPS traffic

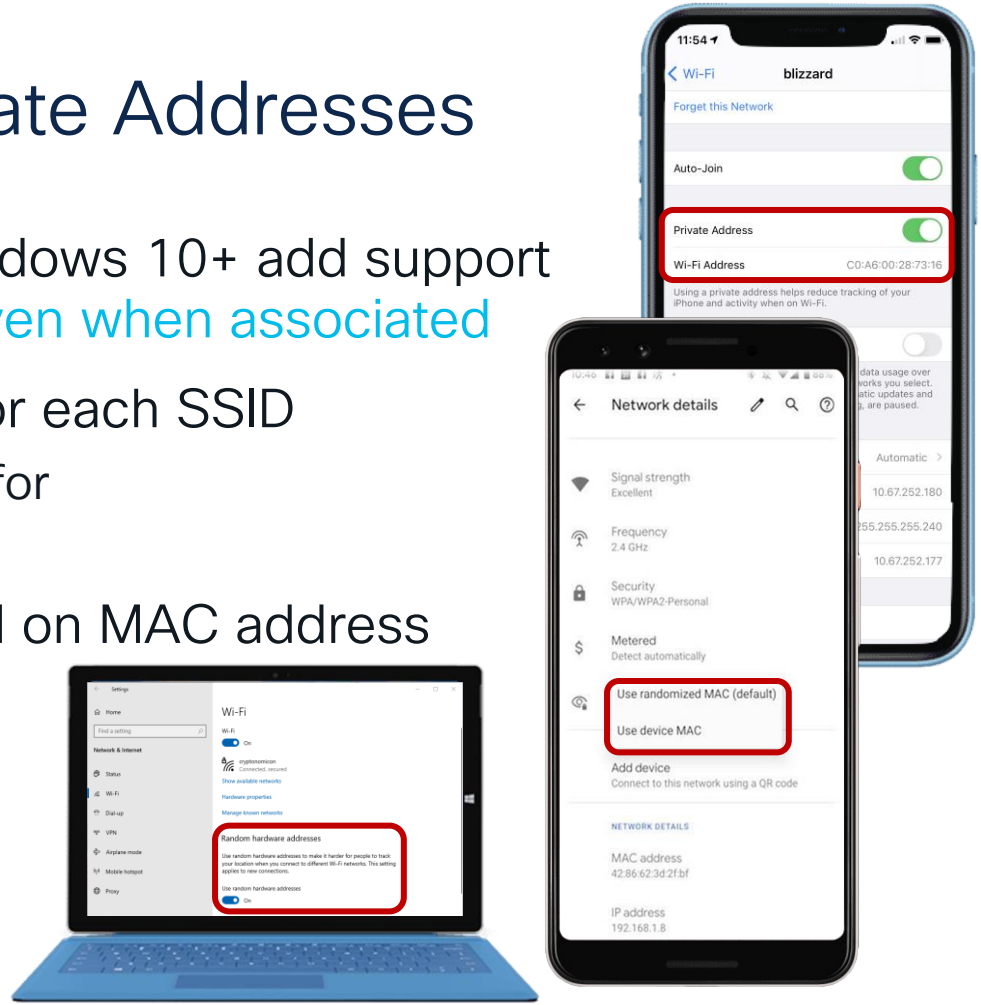
Central Web Authentication

MAC Authentication Bypass



Random MAC and Private Addresses

- iOS 14+, Android 10+ and Windows 10+ add support for random MAC Addresses even when associated
- A random MAC is generated for each SSID
  - That MAC may remain constant for the saved profile
- This will impact services based on MAC address
  - MAC authentication bypass
  - Web authentication
  - Location analytics



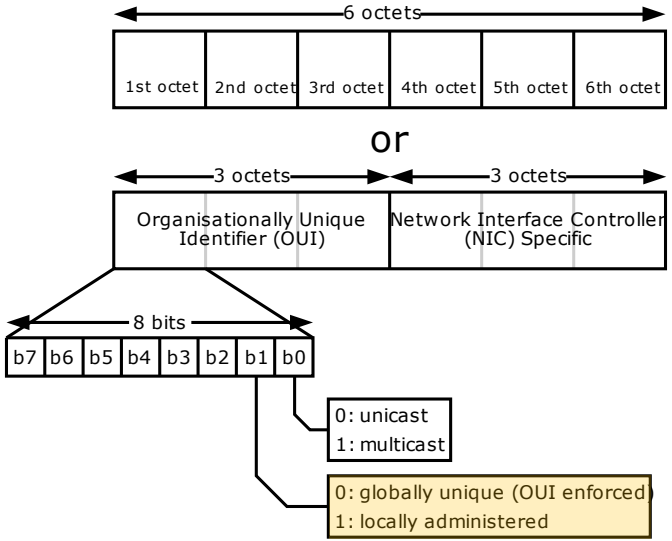
Detailed implementation

	Windows 10+	Android 10+	iOS 14+, iPadOS 14+, watch
Randomization enabled by default	No	Yes	Yes
Same random MAC used for subsequent connection	Yes	Yes	Yes
Randomization saved between device reboot	Yes	Yes	Yes
Random MAC saved when Wi-Fi profile recreated	No	Yes	Yes
Randomization per day and/or per association	Optional	Optional (Android 11 Developer Mode)	No
Randomization enabled upon upgrade for existing Wi-Fi profile	No	No	Yes
Can be enabled/disabled globally	Yes	No	No
API to control randomization exists	Unknown	Yes (Android 11+)	Yes
Randomization saved between factory reset	No	No	Unknown

Random MAC Implications

 Profiling	 BYOD	 Whitelisting	 MDM Flow	 Guest
 Location lookup	 User Defined Network	 Endpoint Analytics	 Forensics	 Quarantine

Detecting Random MAC Addresses



By Inductiveload, modified/corrected by Kju - SVG drawing based on PNG uploaded by User:Vtraveller. This can be found on Wikipedia here., CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=1852032

FYI

32-28-6D-51-13-AF

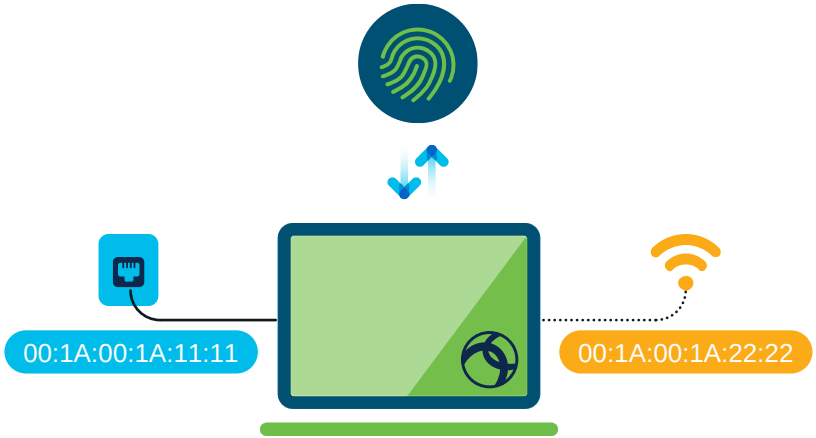
56-EF-68-F6-0D-30

0A-13-A8-8E-B5-EF

AE-83-37-55-A7-22

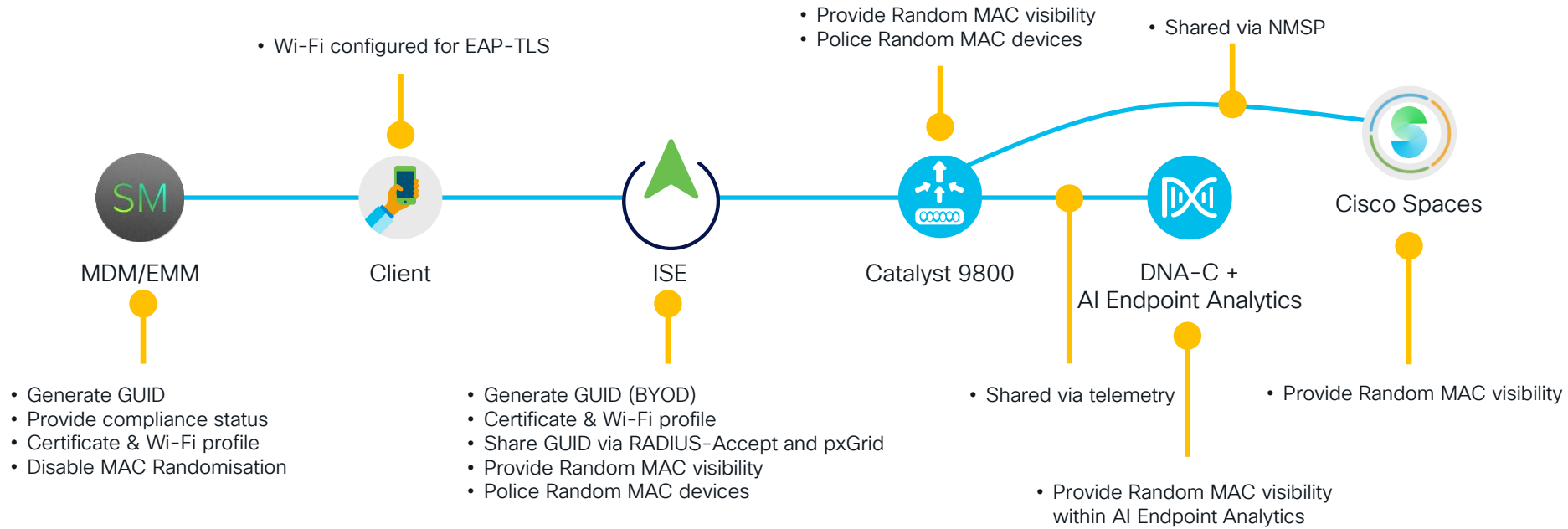
Unique Device Identifier

UDID	MAC Address(s)	Compliance
01669b65...05ee93	00:1a:00:1a:11:11 00:1a:00:1a:22:22	✓

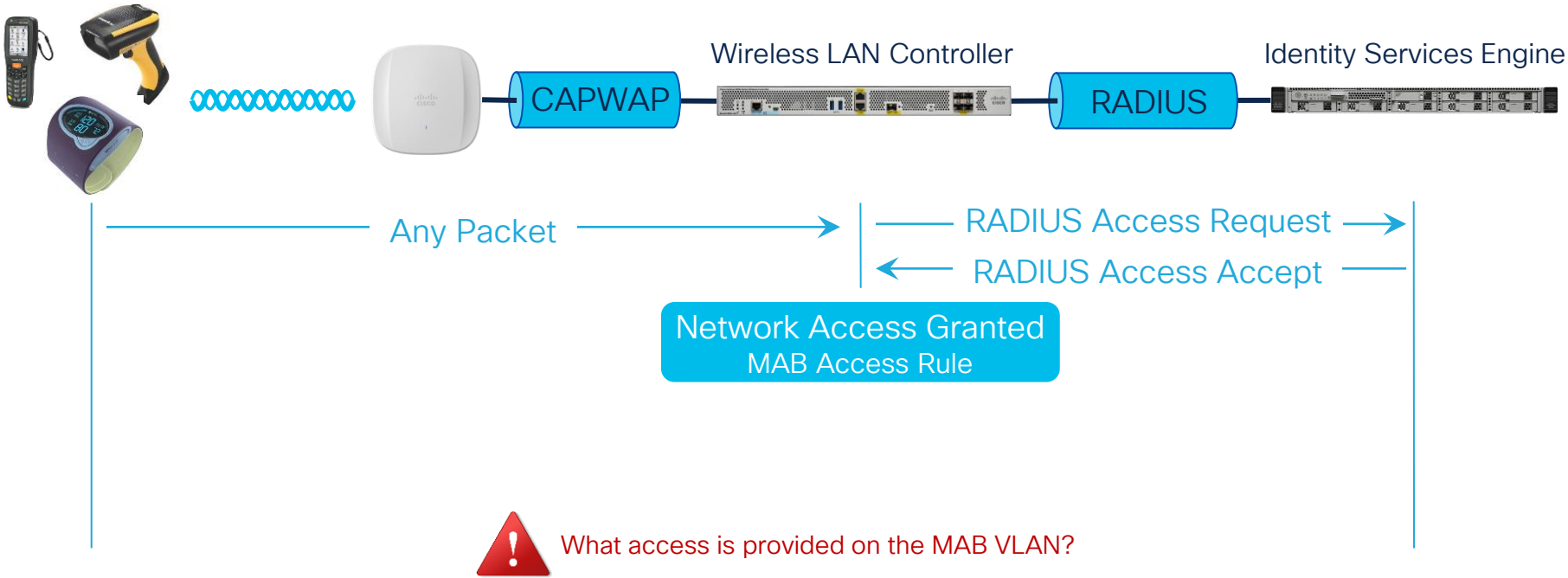


- In open seating environments with docking stations for PCs and Ethernet dongles for Apple MacBooks, lead to a different challenge:
- The same MAC address will be used by different users.
- ISE can perform authorization for managed end-points leveraging the laptop UDID (Unique Device Identifier) instead of the MAC address.
- Requirements
  ISE 2.6, AnyConnect 4.7

Globally Unique Identifier



MAC Authentication Bypass



Wi-Fi Certified Easy Connect

WPA3

Device Provisioning Protocol (DPP)

- 3 Phases
  - Bootstrapping
    - Obtains the public key of new device
  - Authentication and Provisioning
    - Public key is used to create a secure tunnel for credential exchange
  - Network Access
    - PMK derived
    - Four-Way Handshake used as normal
    - Supports Protected Management Frames

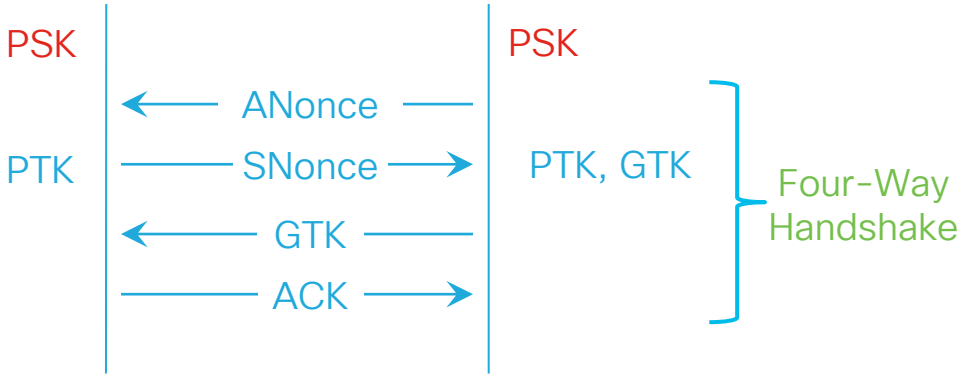
WPA Personal

Pre-Shared Key

WPA Personal

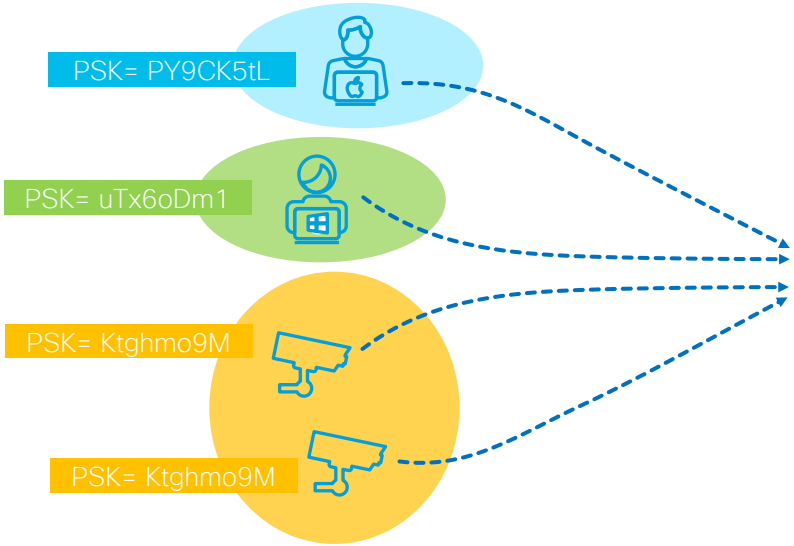
Pre-Shared Key

- Offline Attacks
  - Dictionary
  - Rainbow Table
- Strong Passwords Matter



PTK = SHA(PSK + ANonce + SNonce + AP MAC + STA MAC)

Identity PSK

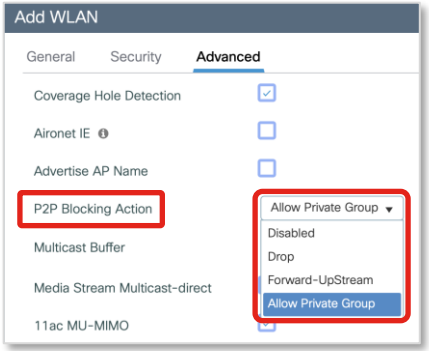


PSK WLAN

WLC

MAC-Filtering

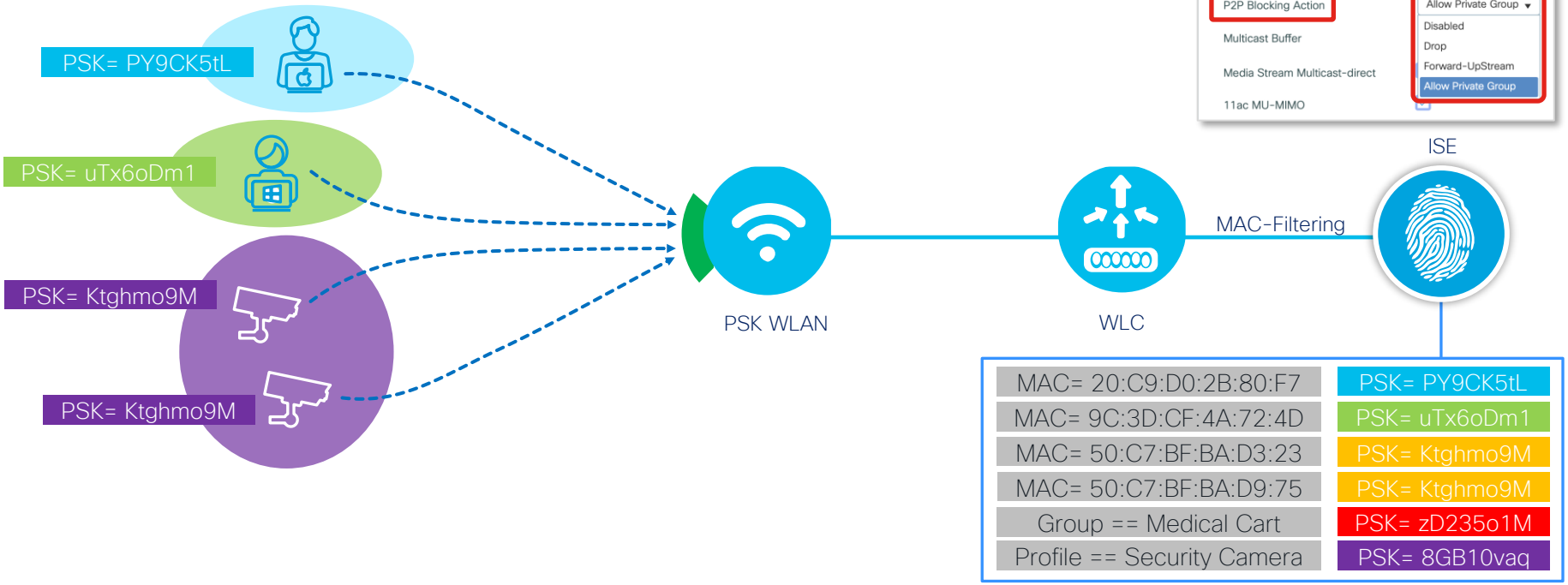
ISE

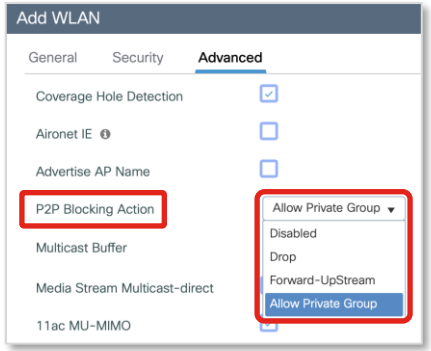


MAC= 20:C9:D0:2B:80:F7	PSK= PY9CK5tL
MAC= 9C:3D:CF:4A:72:4D	PSK= uTx6oDm1
MAC= 50:C7:BF:BA:D3:23	PSK= Ktghmo9M
MAC= 50:C7:BF:BA:D9:75	PSK= Ktghmo9M

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

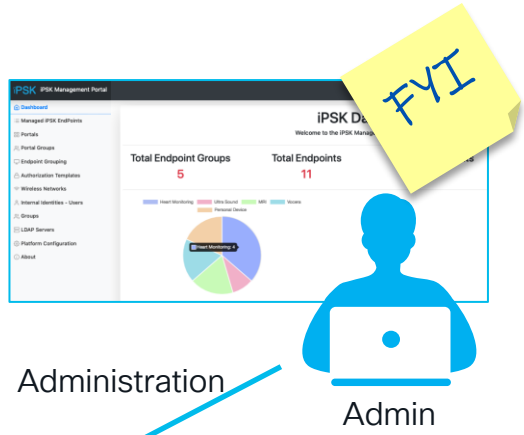
Identity PSK

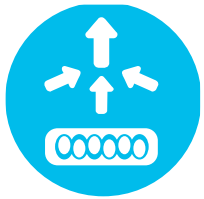




https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

iPSK Manager





WLC / AP

RADIUS

CoA

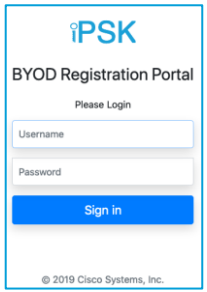
ISE

SQL

API

iPSK Manager
- Linux
- Apache
- MySQL
- PHP

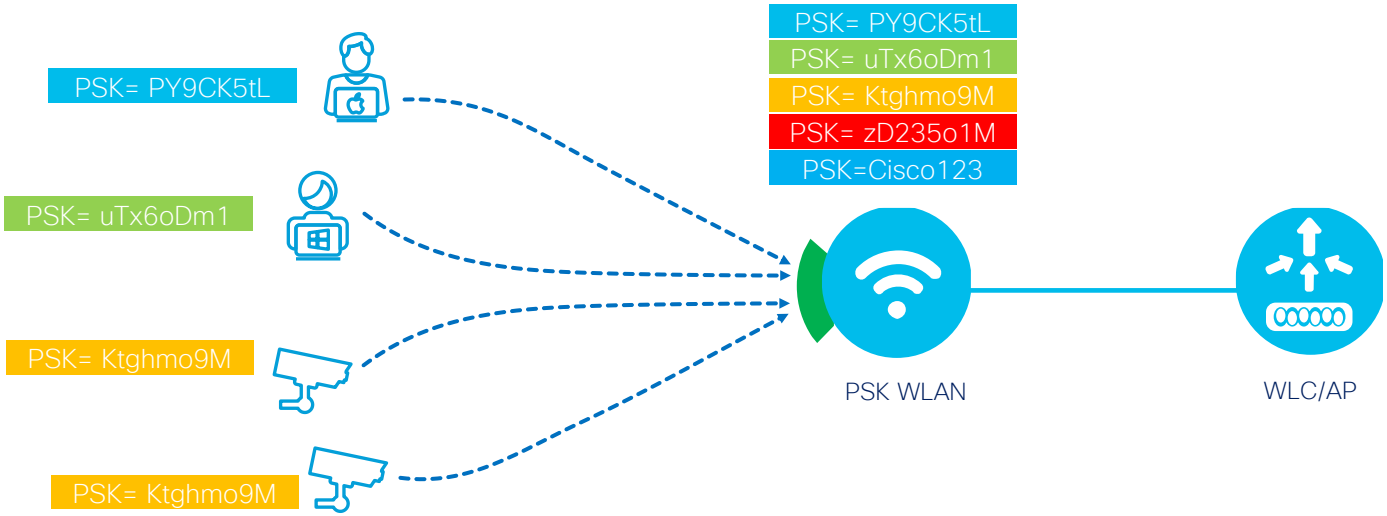
iPSK Lifecycle Management



End Users

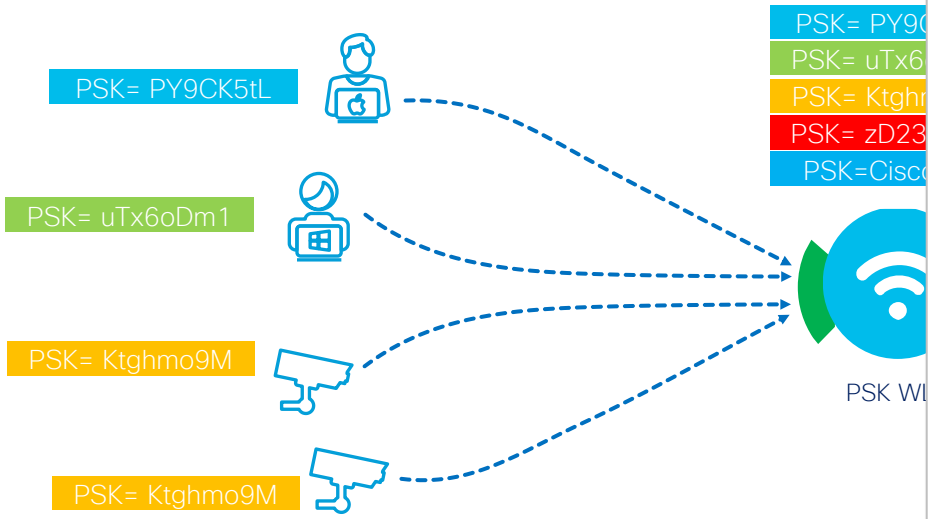
http://cs.co/iPSK-Manager

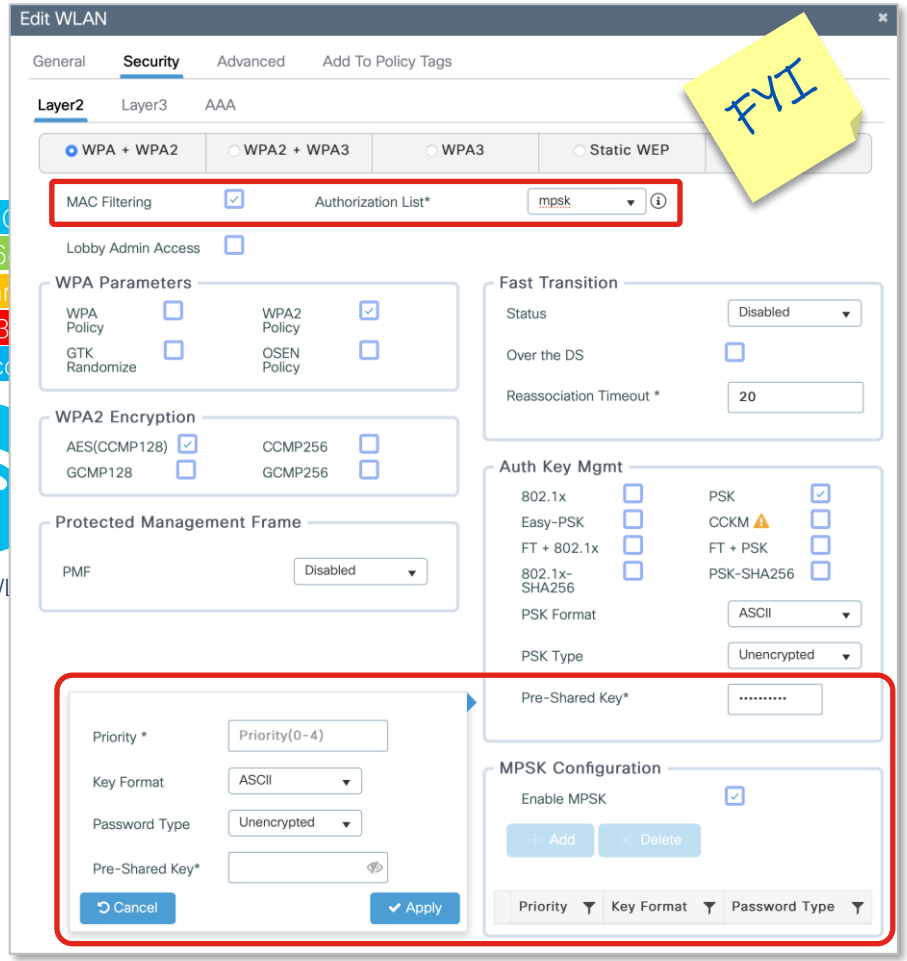
Multi Pre-Shared Key



https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/17-2/config-guide/ewc_cg_17_2/multi_preshared_key.pdf

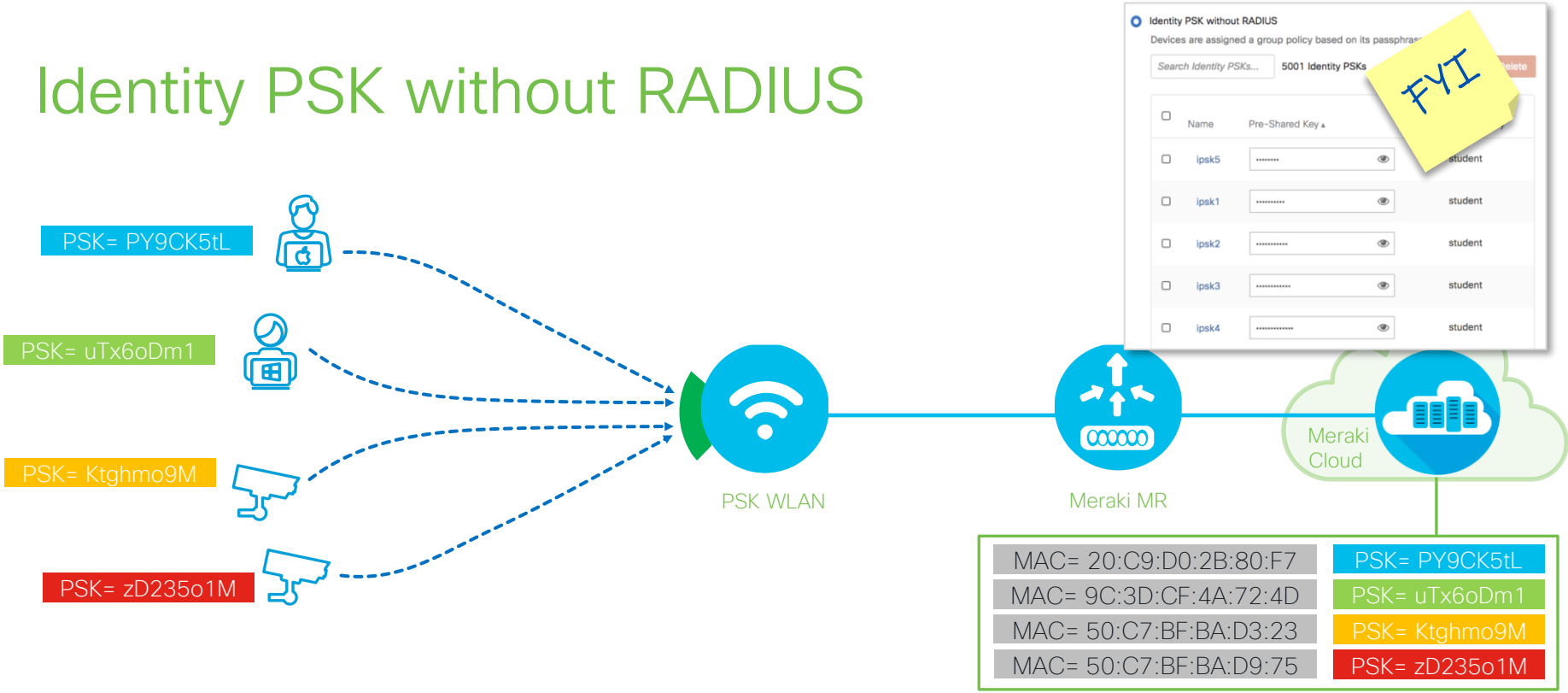
Multi Pre-Shared Key





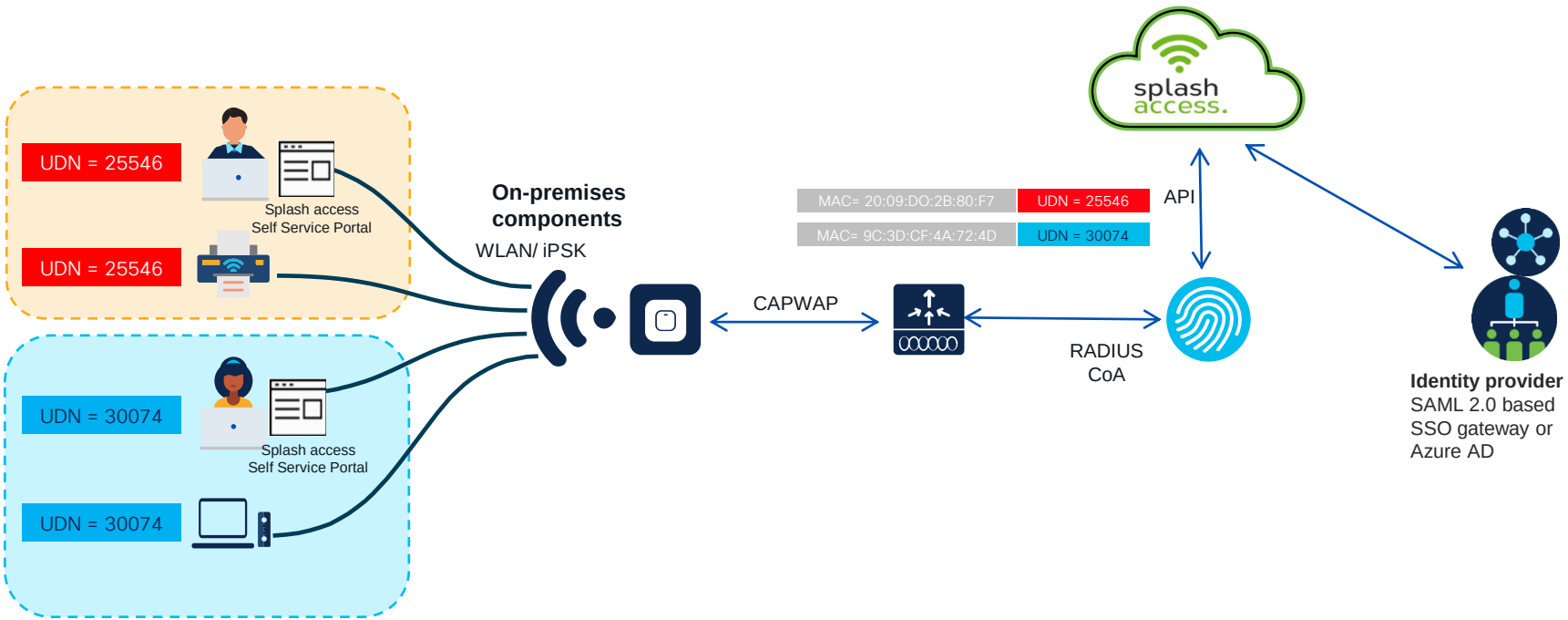
https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/17-2/config-guide/ewc_cg_17_2/multi_preshared_key.pdf

Identity PSK without RADIUS

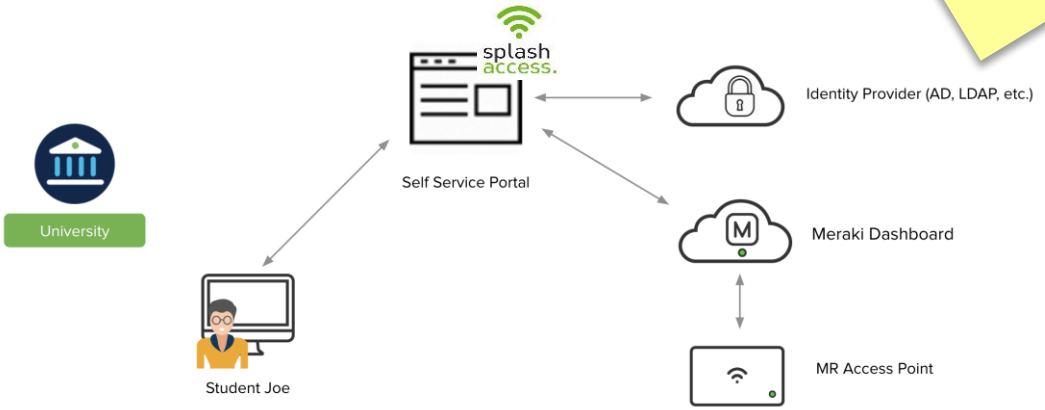


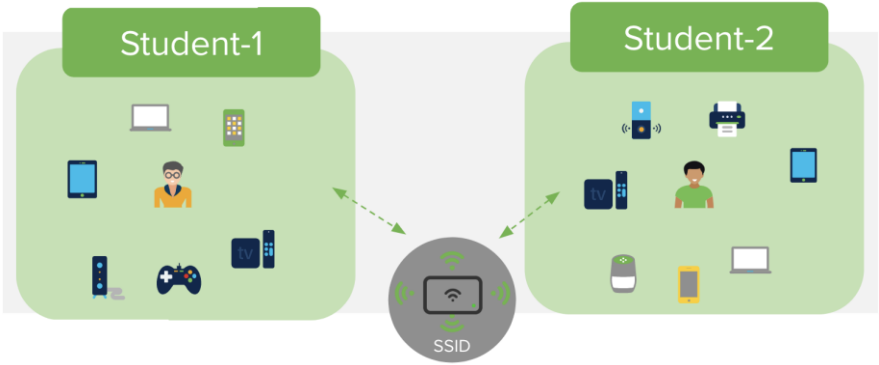
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_Authentication_without_RADIUS

User Defined Network



Wi-Fi Personal Network





https://documentation.meraki.com/MR/Encryption_and_Authentication/Wi-Fi_Personal_Network_(WPN)

Simultaneous Authentication of Equals

WPA3

- Based on the Dragonfly Key Exchange
  - Balanced Password Authenticated Key Exchange
    - Security of SAE not tied to the complexity of the shared secret
  - SAE exchanges results in a 32-byte PMK
    - Protects against offline dictionary attacks
    - Forward secrecy protects traffic if the password is compromised in future
    - Supports Protected Management Frames
  - WPA3-SAE Transition Mode supports both WPA2-PSK and WPA3-SAE on the same SSID

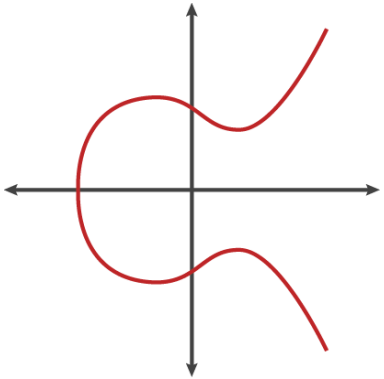
Dragonblood

- Backwards Compatibility Attack
  - Clients can be tricked into connecting to a Rogue WPA2 Personal only network
  - The attacker uses the partial WPA2 handshake for offline attacks
  - Certain devices, even when connected to WPA3 Personal only networks, could be tricked into using WPA2
- Denial of Services Attacks
  - APs should implement anti-exhaustion mechanisms
  - APs should implement detection mechanism and blacklist misbehaving clients

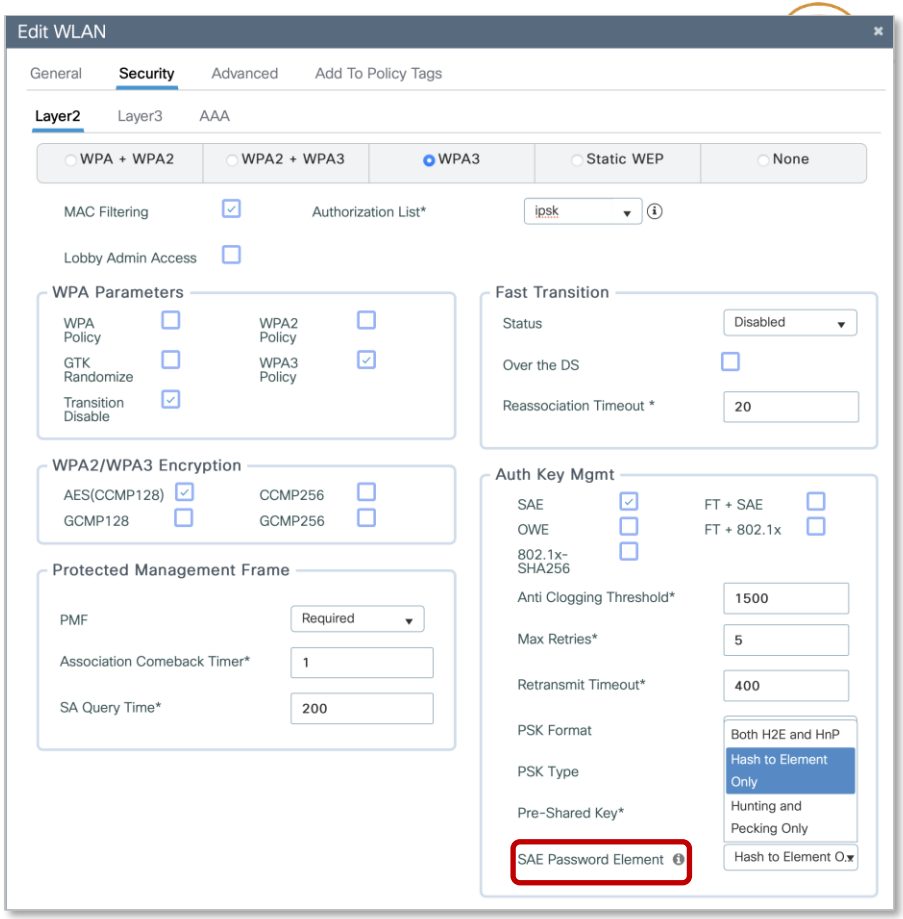
Dragonblood: Analysing WPA3's Dragonfly Handshake

Dragonblood

- Timing-Based Side-Channel Attacks
  - The time it takes an AP to respond to commit frames may leak information about the password



$$y^2 = x^3 + ax + b$$



Wi-Fi Certified Enhanced Open

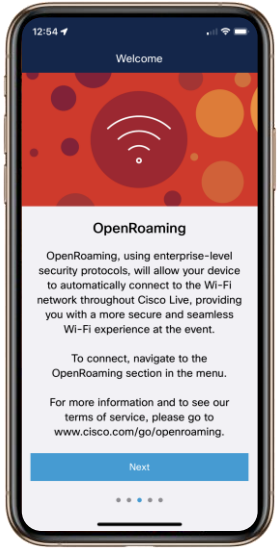
WPA3

- Opportunistic Wireless Encryption (OWE)
  - Replaces 802.11 “open” authentication support
  - Client and AP perform an unauthenticated Diffie-Hellman Key Exchange to establish a PMK
  - Four-Way Handshake used as normal
  - Supports Protected Management Frames
- Diffie-Hellman is susceptible to MitM attacks
  - Would allow the attacker same visibility as on an Open network

Decoupling Access and Identity

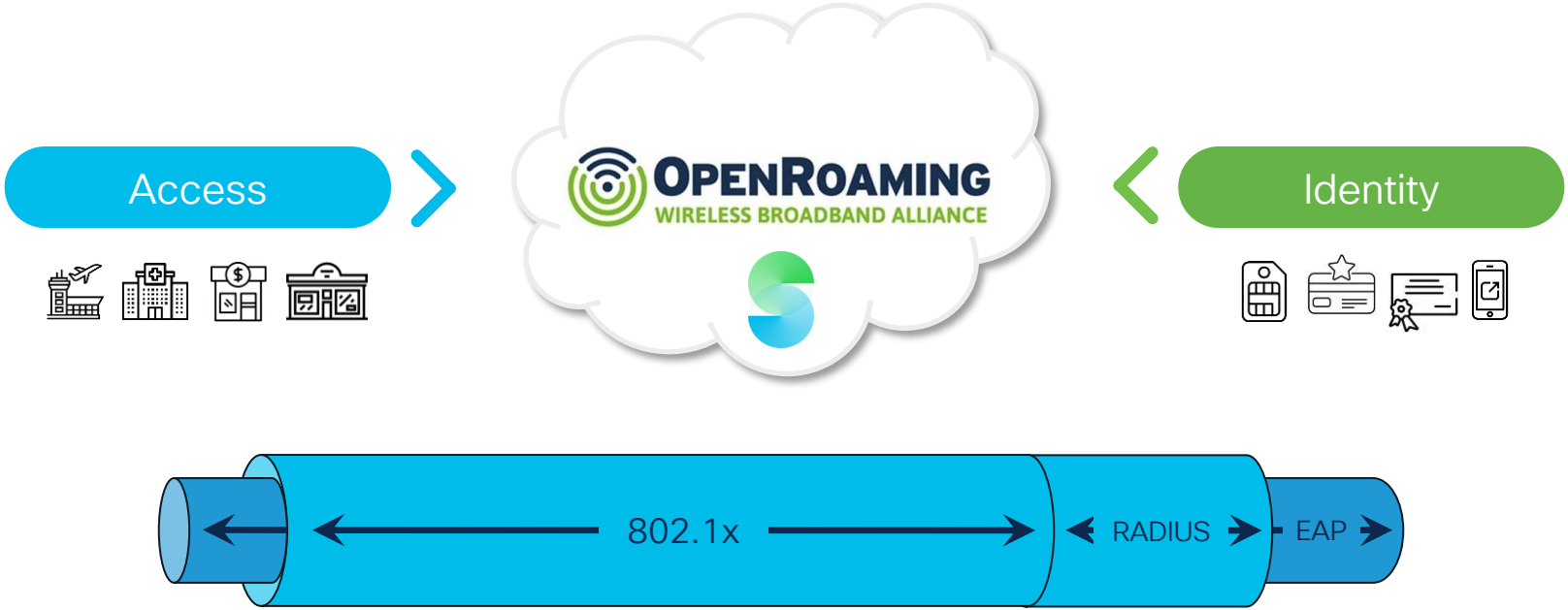
Decoupling Access and Identity

Access



Identity

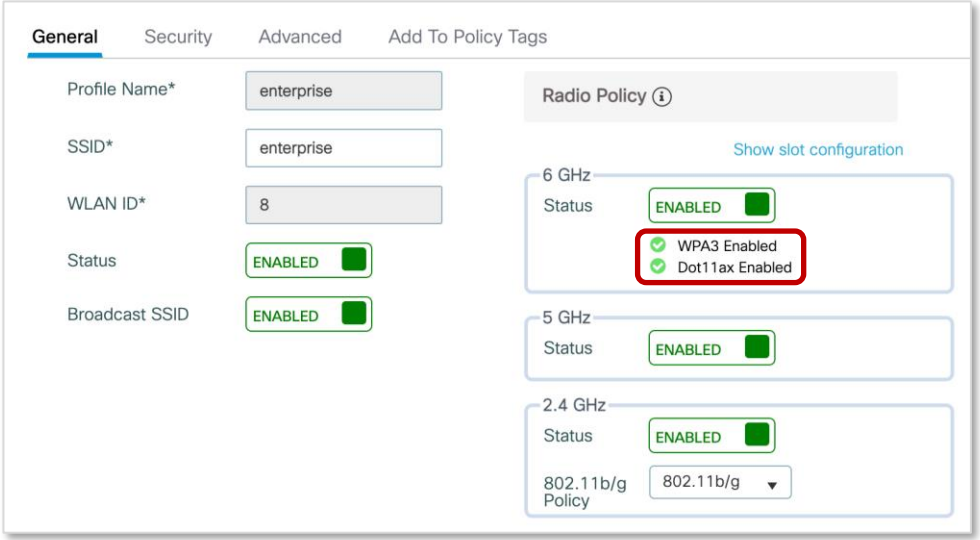
OpenRoaming



Wi-Fi 6E Security

WPA3 and OWE are mandatory for Wi-Fi 6E

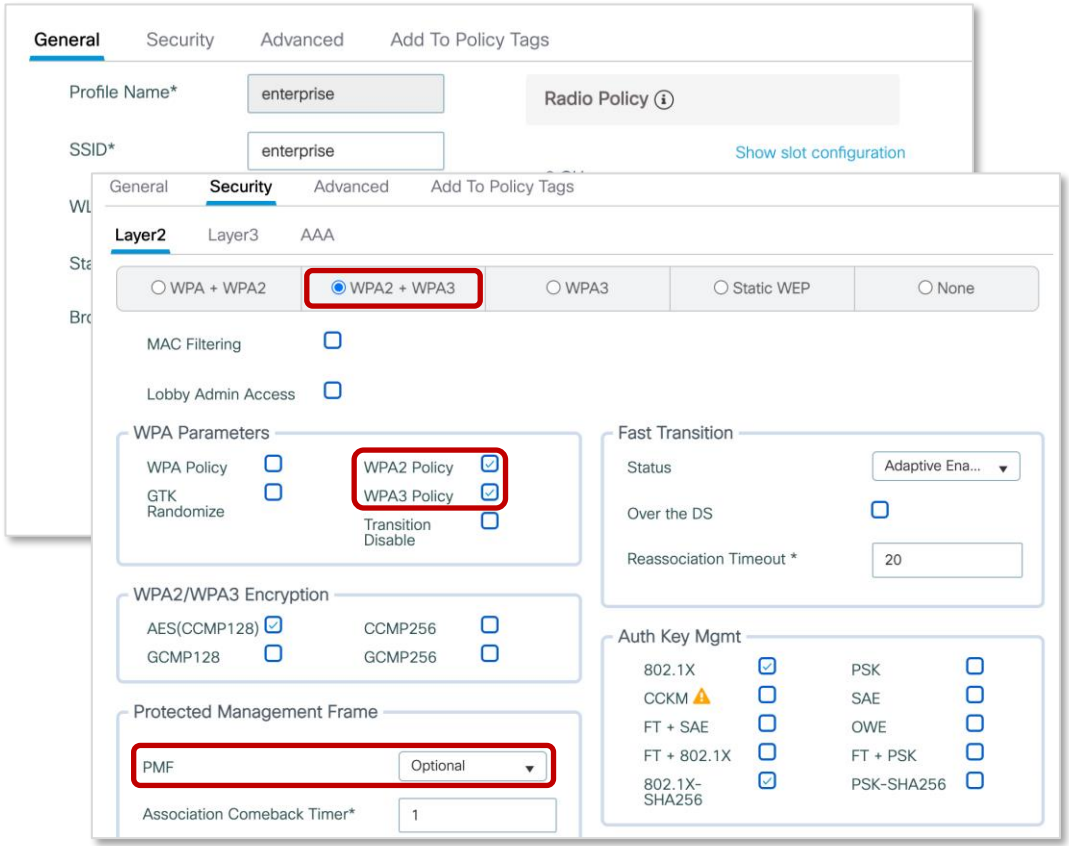
WPA2 and Open are not supported on 6GHz



Wi-Fi 6E Security

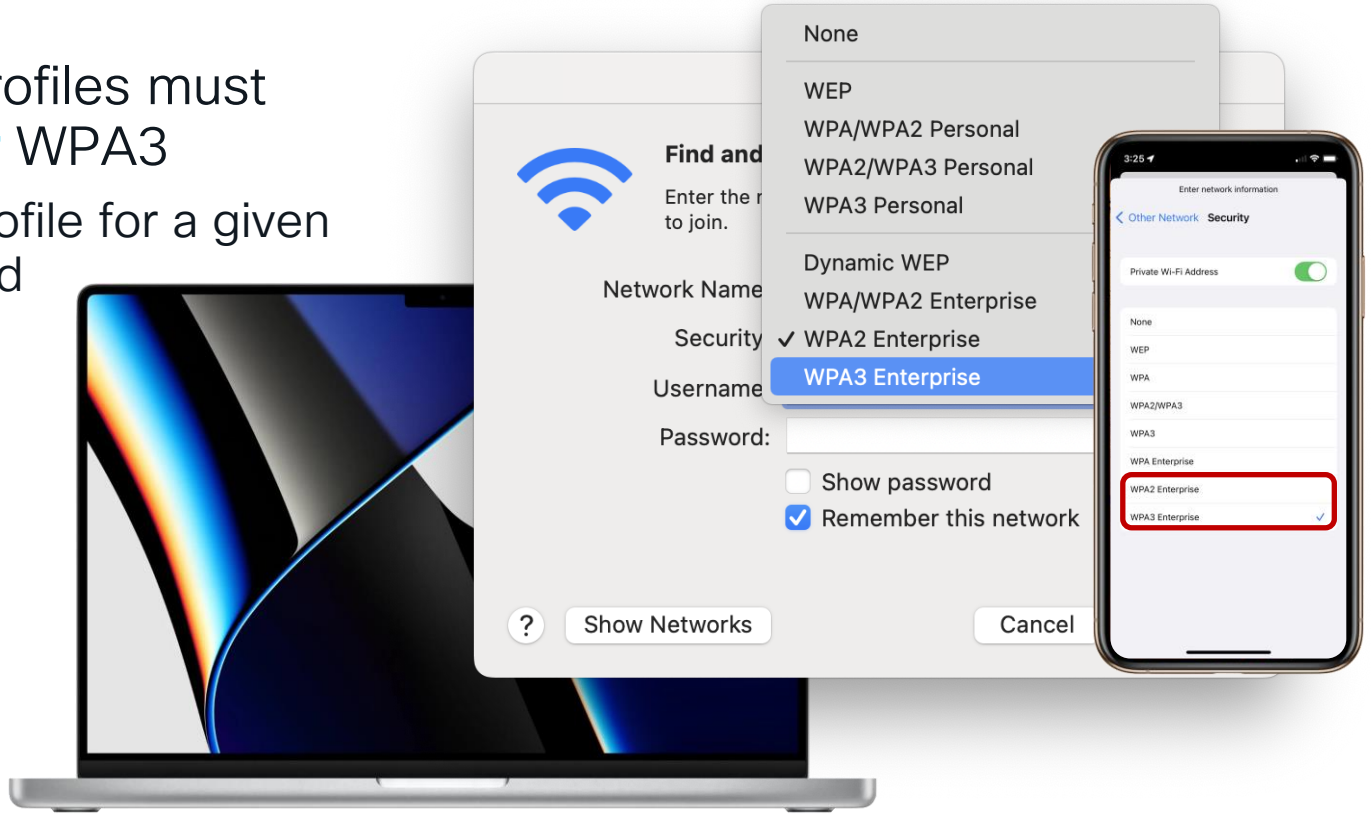
WPA3 and OWE are mandatory for Wi-Fi 6E

WPA2 and Open are not supported on 6GHz

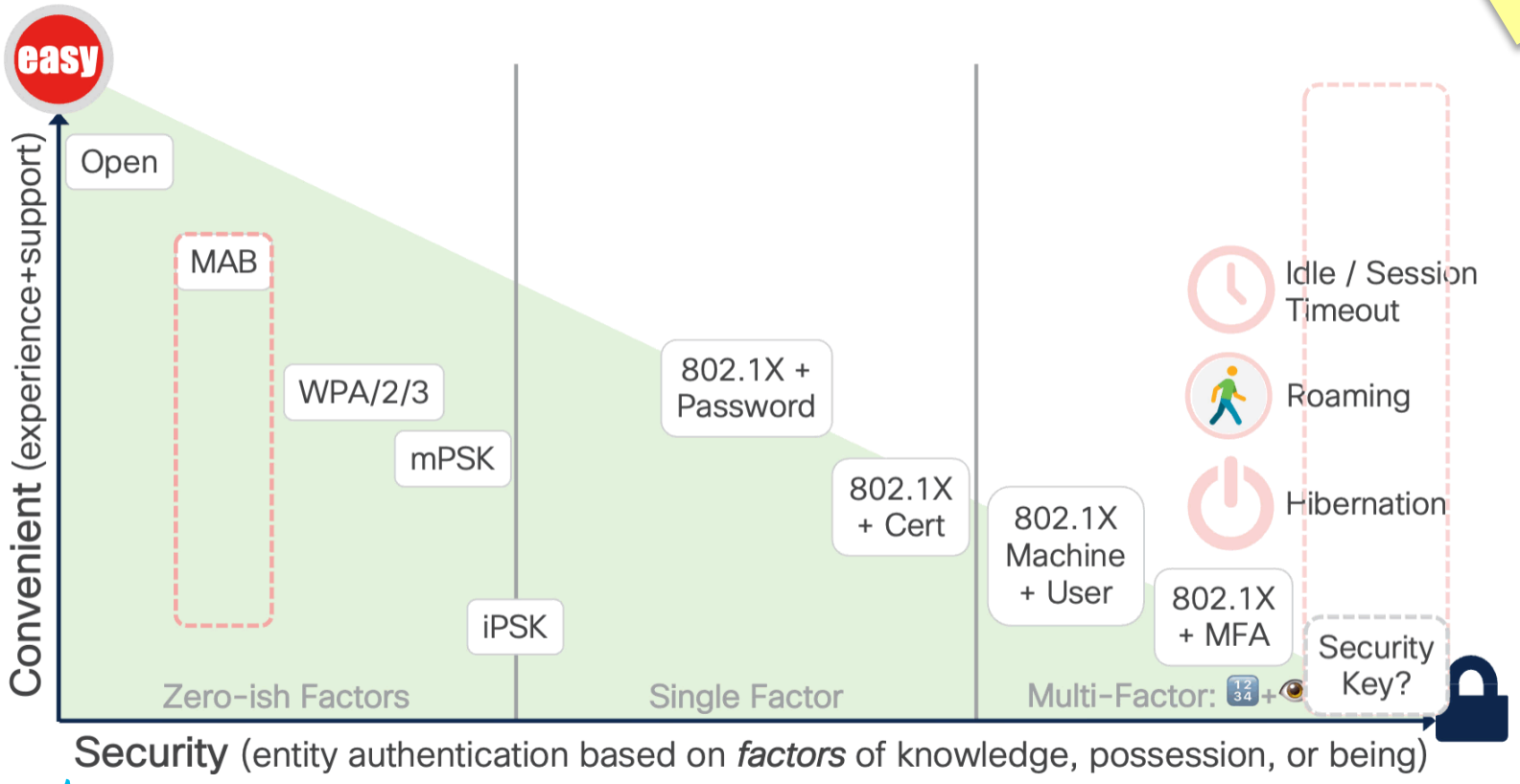


Wi-Fi 6E Security

- Client device profiles must select WPA2 or WPA3
  - And only one profile for a given SSID is permitted



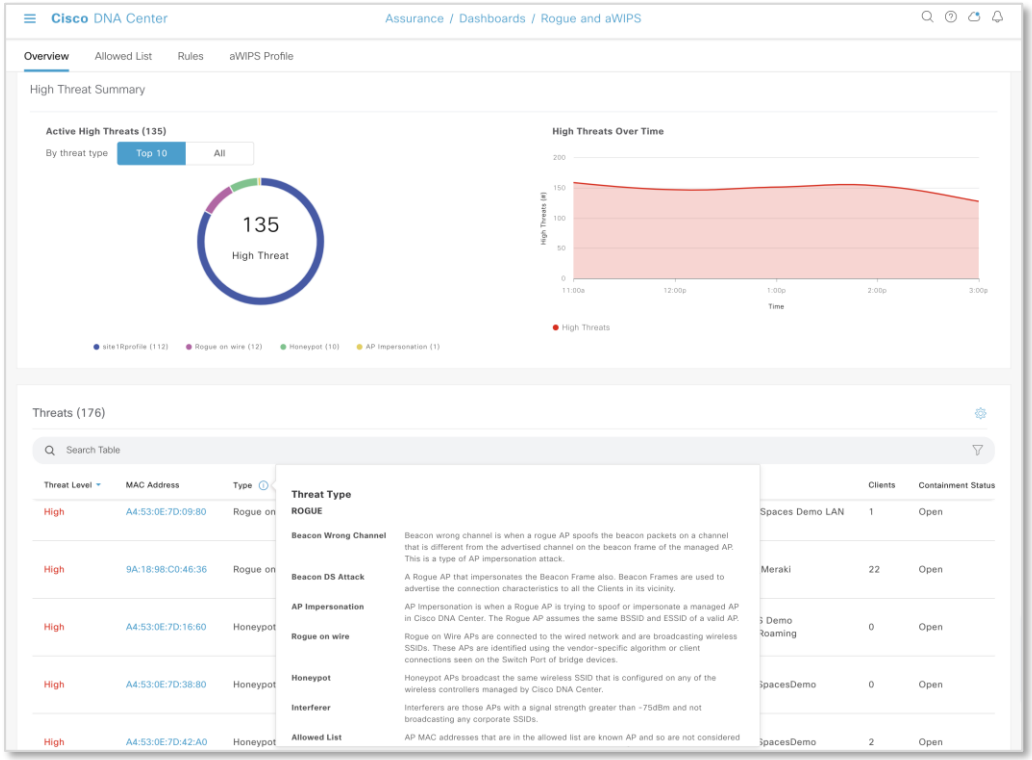
Network Access Security Spectrum



Rogue Detection and Advanced WIPS

Rogue Detection and Advanced WIPS

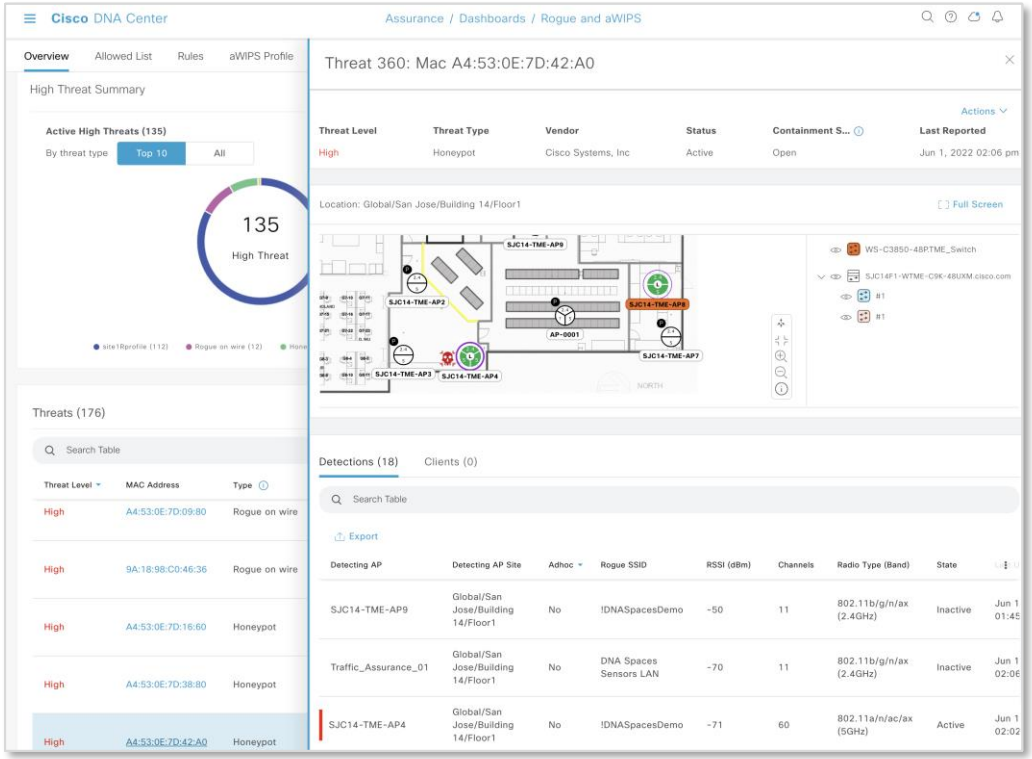
- Centralized wireless threat management
- Rogue detection
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3.html

Rogue Detection and Advanced WIPS

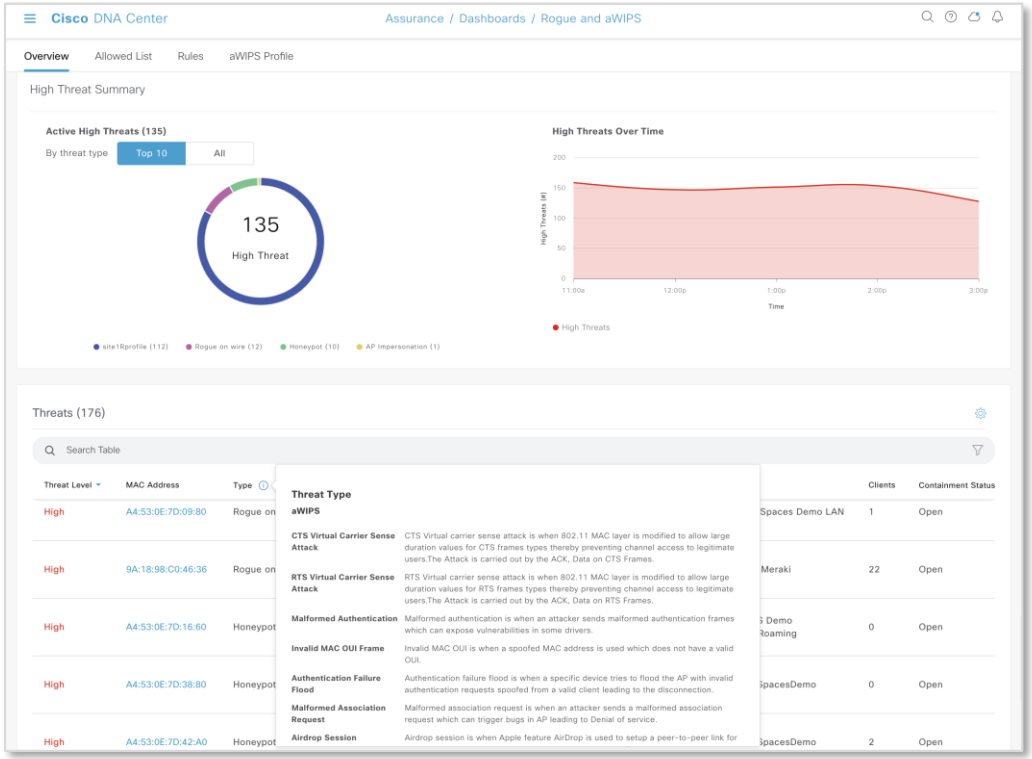
- Centralized wireless threat management
- Rogue detection
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3.html

Rogue Detection and Advanced WIPS

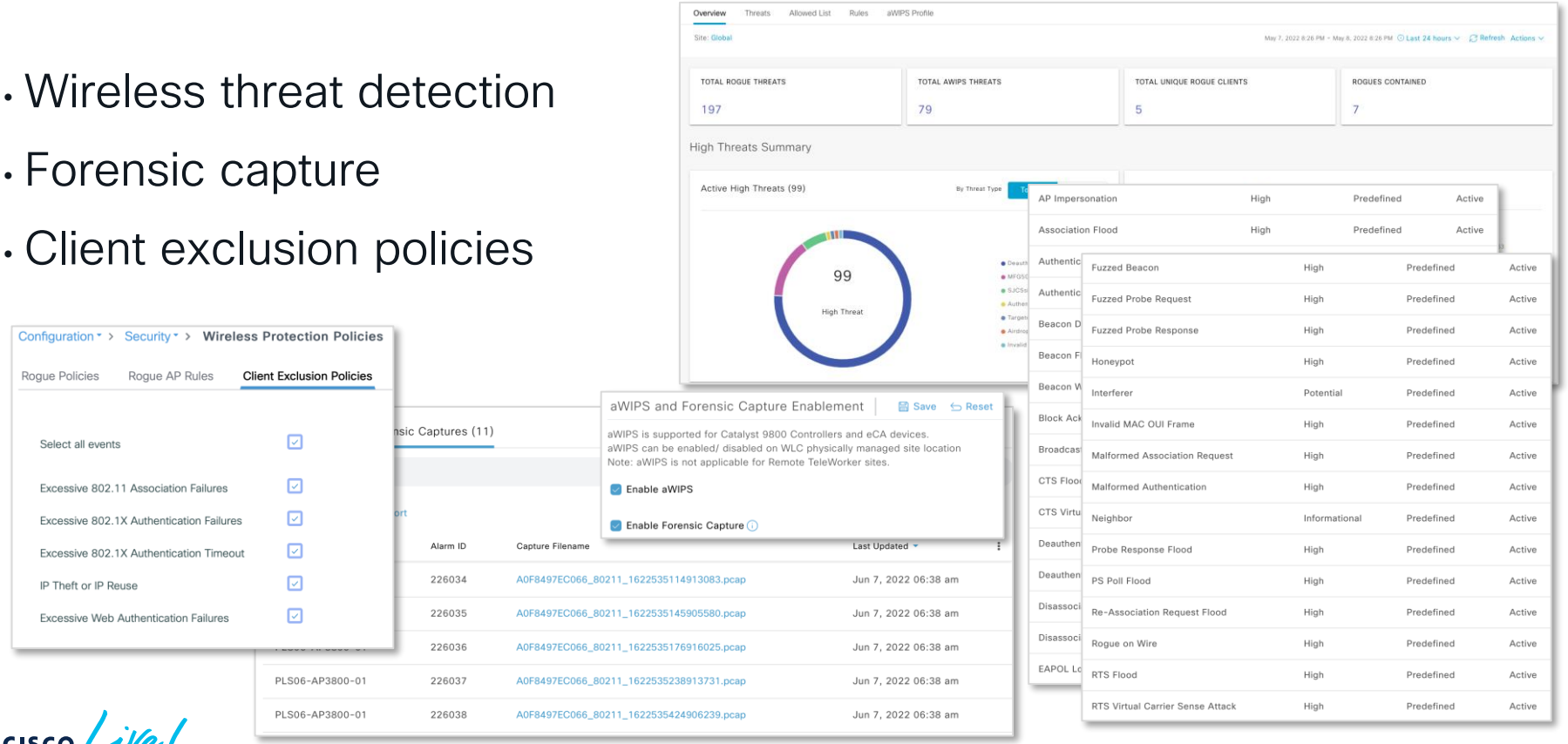
- Centralized wireless threat management
- Rogue detection
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



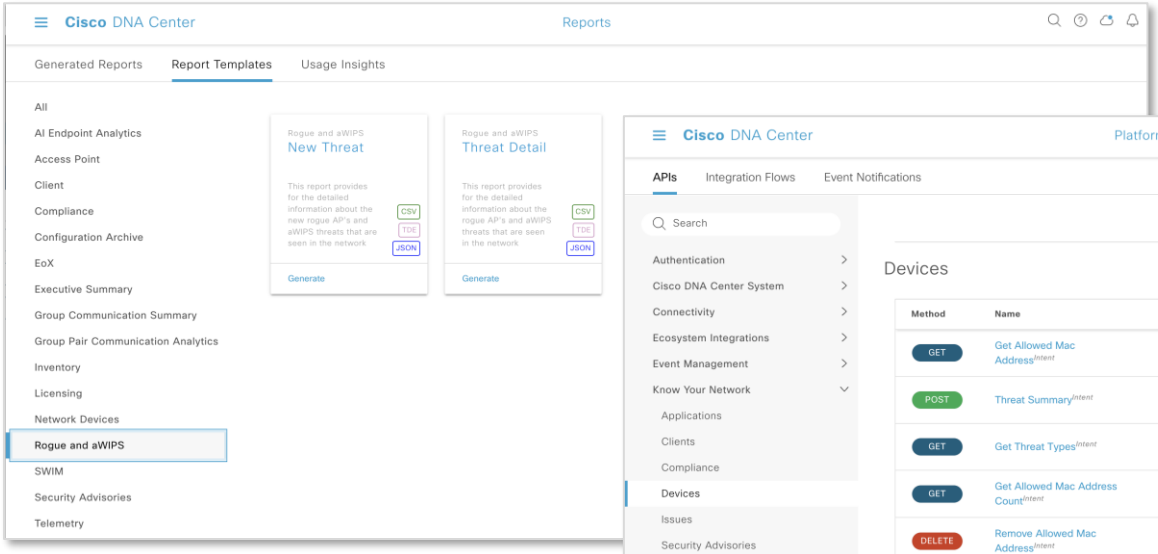
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3.html

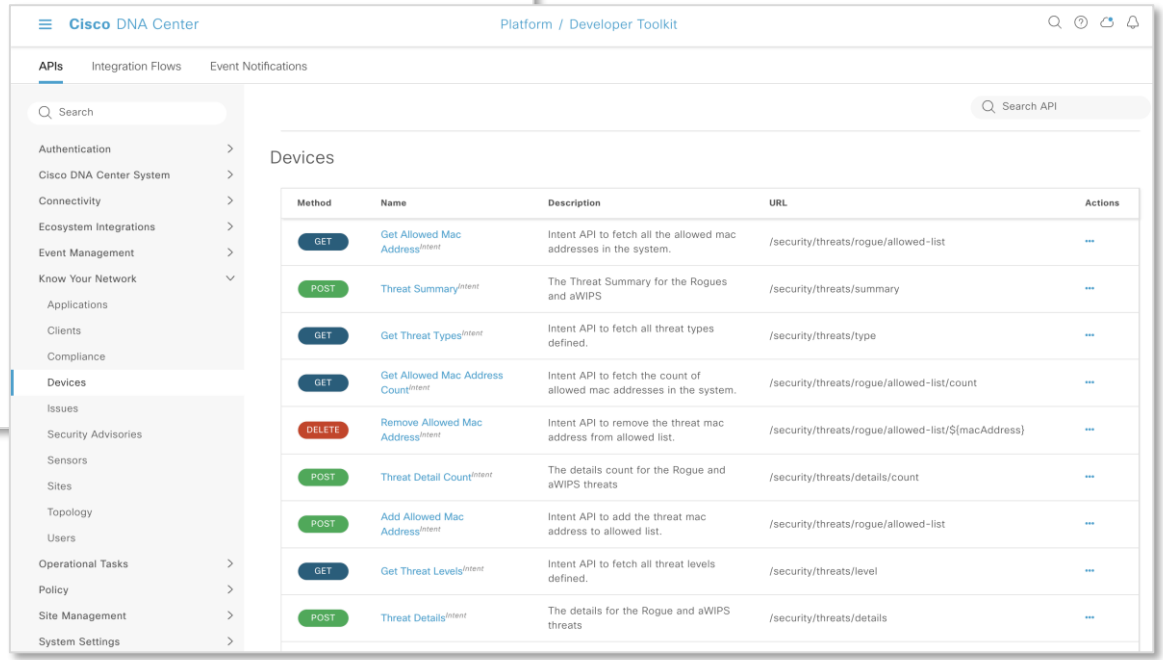
Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies



Rogue and WIPS Reporting and APIs





Access Point Scanning Options

FYI

Off-Channel Scanning

- All channels scanned every 180s within a 3m period
- Dwell time is 50ms
- Channel change is 10 ms
- AP is off-channel for 60ms

Monitor Mode Access Point

- Continuous cycle 1200ms dwell across all channels
- Supports Rogue Detection & WIPS, RRM & CleanAir, and Fast Locate

Dedicated Scanning Radio

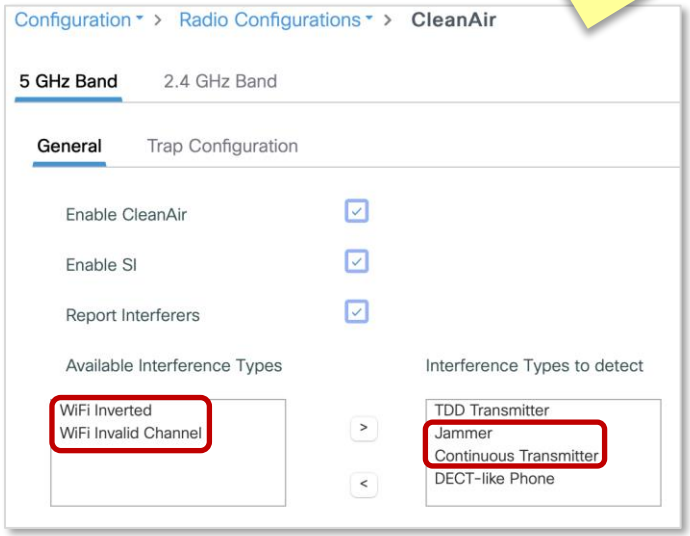
- Catalyst 9136
- Catalyst 9130
- Catalyst 9120

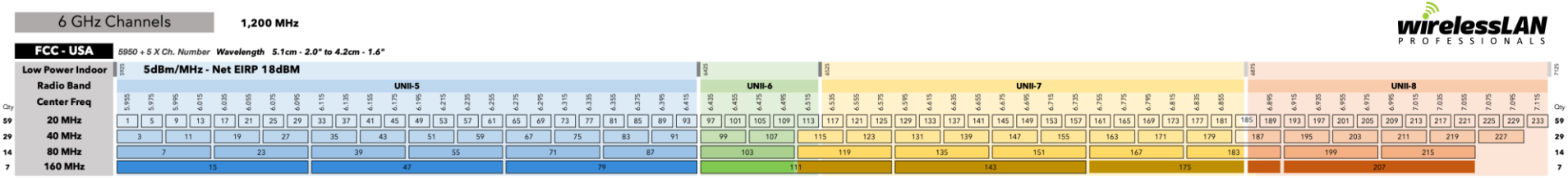
- Catalyst 9166
- Catalyst 9164
- Catalyst 9162

CleanAir Spectrum Intelligence

FYI

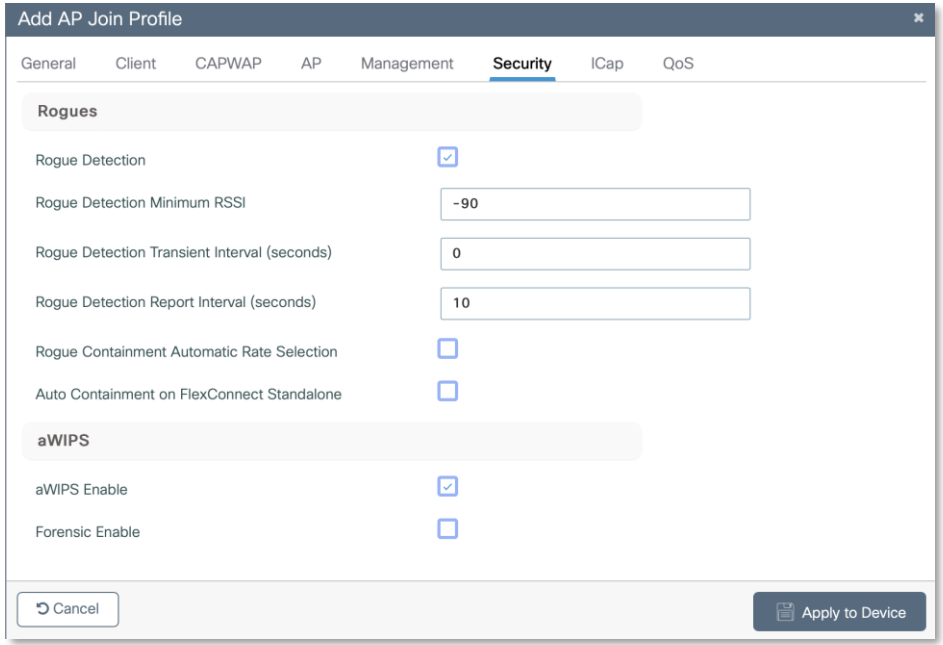
- Interferers
  - Layer 1 Denial of Service Attack
- Rogue AP Detection
  - Inverted
  - Invalid Channel
- 6GHz Support
  - Rogue Detection and WIPS





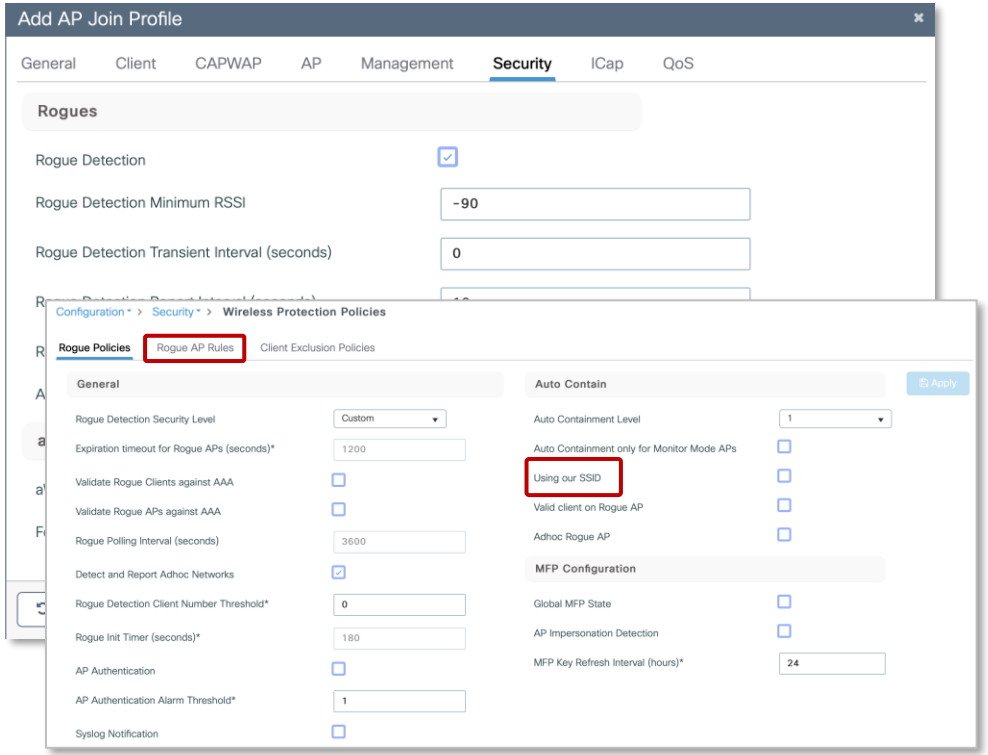
Rogue Access Points

- A Rogue AP is any AP which is not part of our infrastructure
  - Most of them will be legitimate
  - Some of them may be malicious



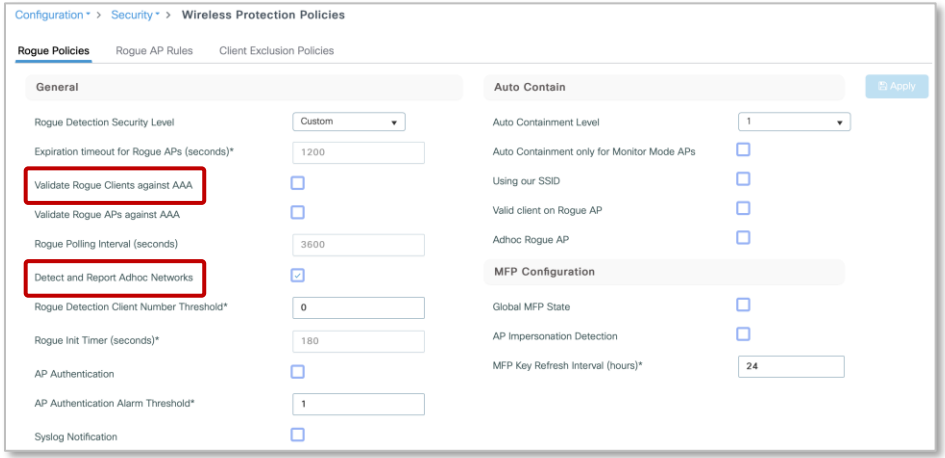
Rogue Access Points

- A Rogue AP is any AP which is not part of our infrastructure
  - Most of them will be legitimate
  - Some of them may be malicious
  - Correctly differentiating between the two is critical
  - Detecting APs on the wired network is hard
    - Wired 802.1x matters



Rogue Clients

- A Rogue Client is any client which is connected to a Rogue AP
  - What we care about are our clients which have connected to the Rogue AP
  - But this is not necessarily a risk
- Clients may create ad-hoc wireless networks
  - This can be a risk if they have bridged to the wired network



Cisco DNA Center Threat Levels

Informational

- RSSI <= -75 dBm and not on wire
- Rogue Type: Neighbor

Potential

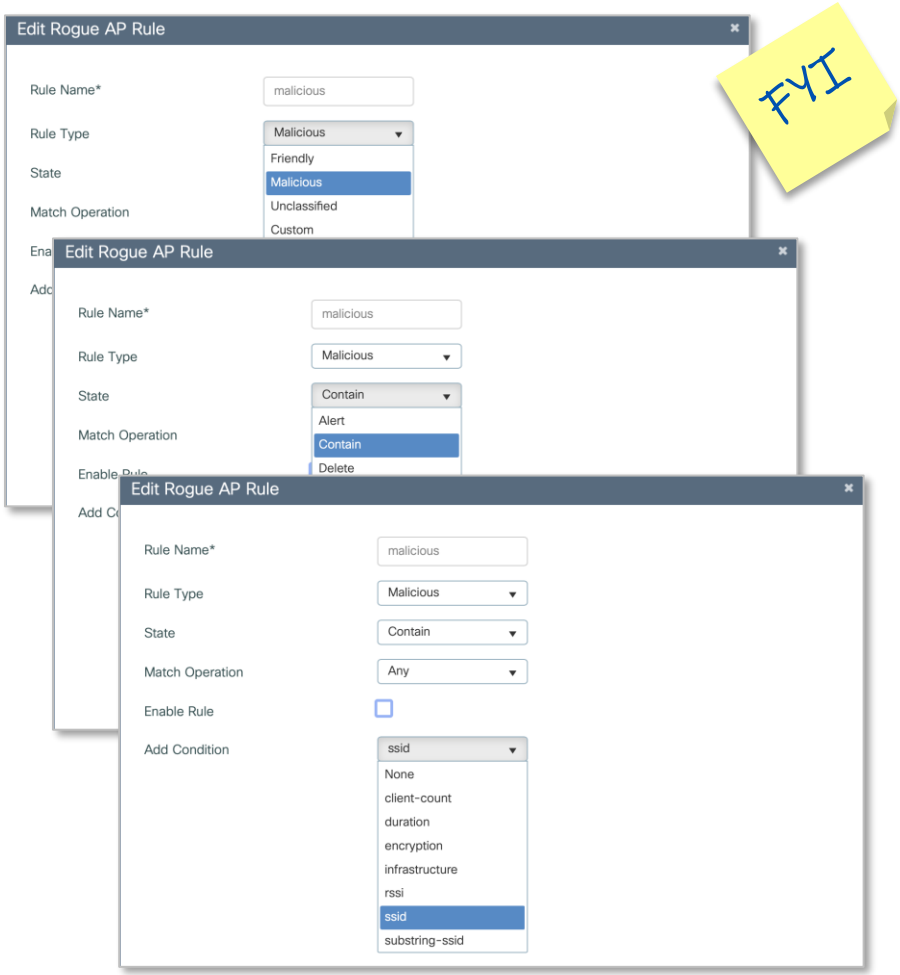
- RSSI >-75 dBm and not on wire
- Rogue Type: Interferer

High

- Rogue Types
  - Honeypot
  - Impersonation AP
  - Rogue on wire
  - Beacon DS attack
- All WIPS threats

Rogue AP Rules

- Create Rogue Rules to classify rogues as Malicious or Friendly based on specific criteria
  - SSID name
  - RSSI value
  - Encryption condition
  - Minimum rogue client count
- Rules can also define actions
  - Alert
  - Contain



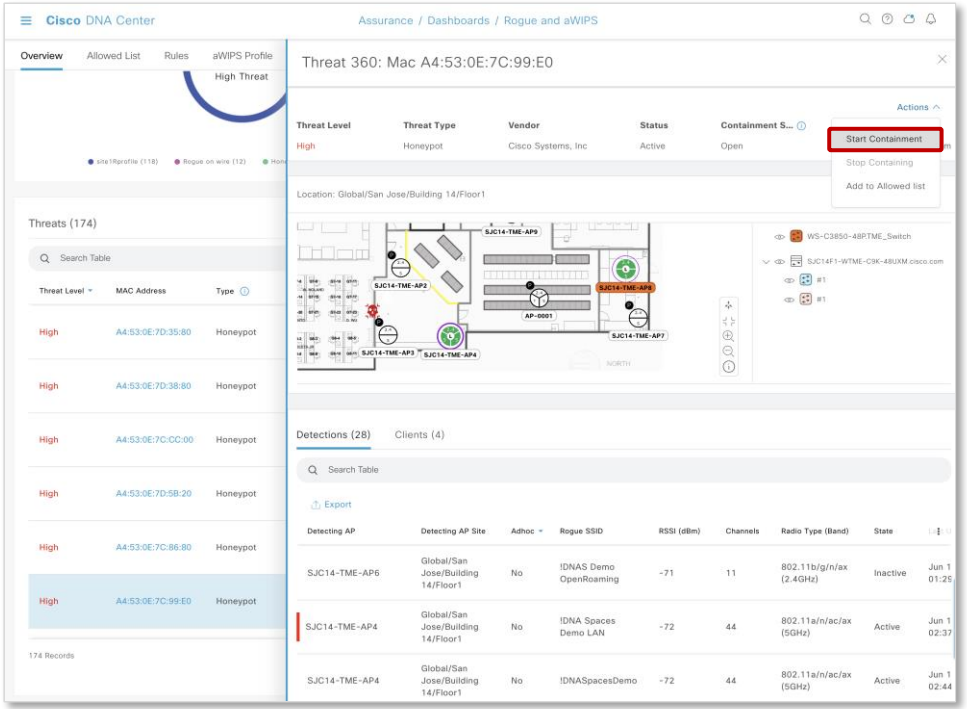
Rogue Notification Triggers

- The Catalyst 9800 has aggressive rogue notification thresholds by default
- In environments with a large number of Rogues, this may result in excessive notifications sent to the receiver
- In these scenarios, increase the Rogue AP and Client RSSI notification threshold
  - The default value is 0
  - Recommendation to increase to 5 or higher

```
C9800(config)#wireless wps rogue ap notify-rssi-deviation 5
C9800(config)#wireless wps rogue clients notify-rssi-deviation 5
```

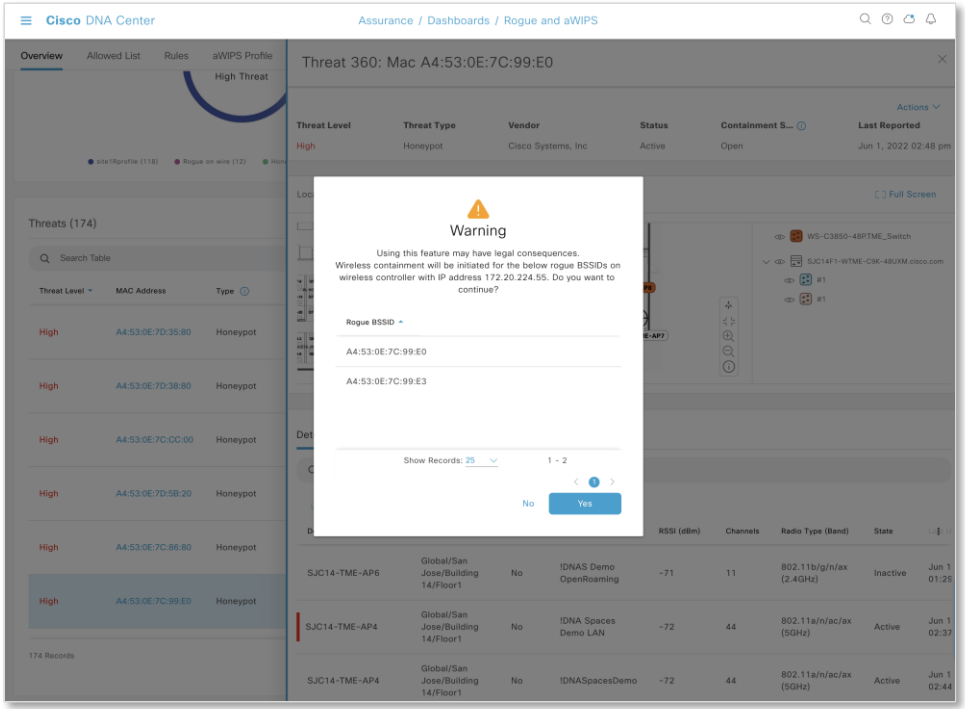
Rogue AP Containment

- How do we contain Rogue APs?
  - Containment is a spoofed 802.11 disassociation/deauthentication request attack



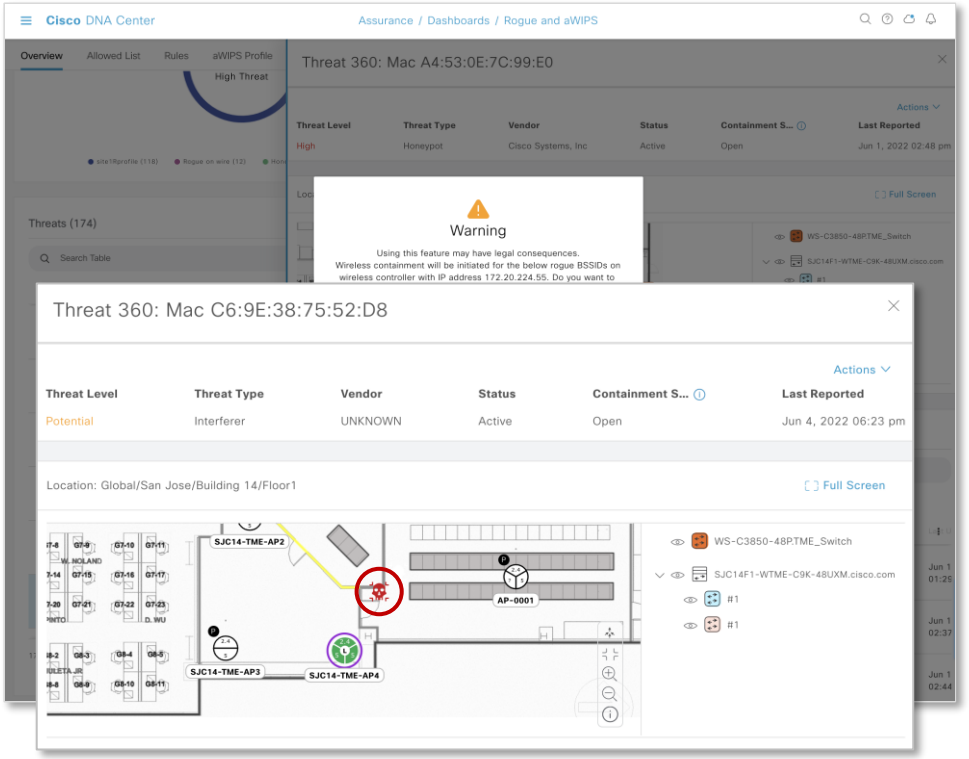
Rogue AP Containment

- How do we contain Rogue APs?
  - Containment is a spoofed 802.11 disassociation/deauthentication request attack

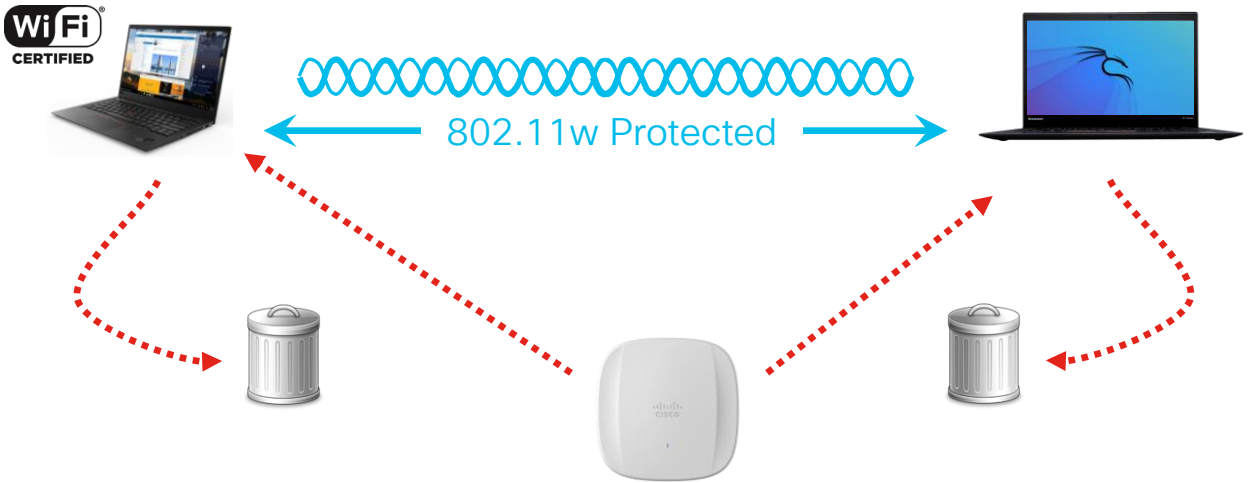


Rogue AP Containment

- How do we contain Rogue APs?
  - Containment is a spoofed 802.11 disassociation/deauthentication request attack
- How does WPA3 affect Rogue AP containment?
  - 802.11w will change how we can mitigate Rogue AP related threats
  - The ability to physically locate rogues will be key

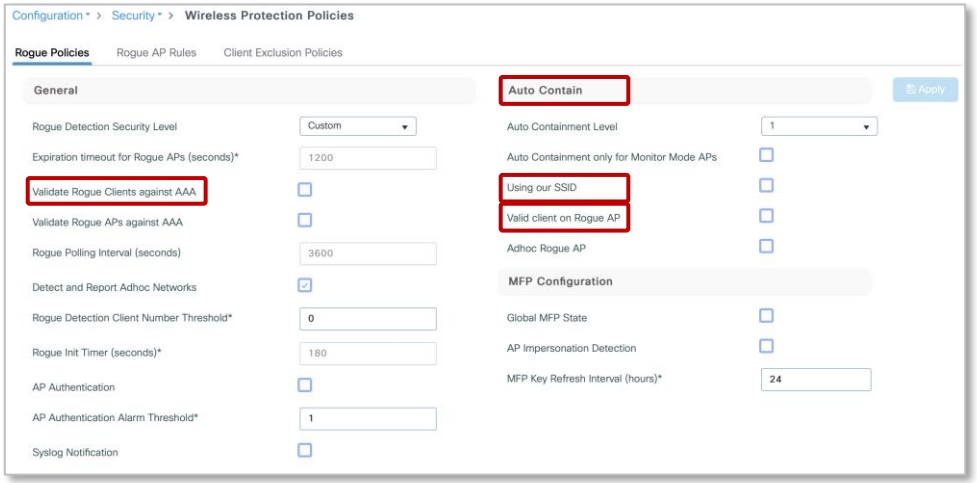


Rogue Containment with WPA3

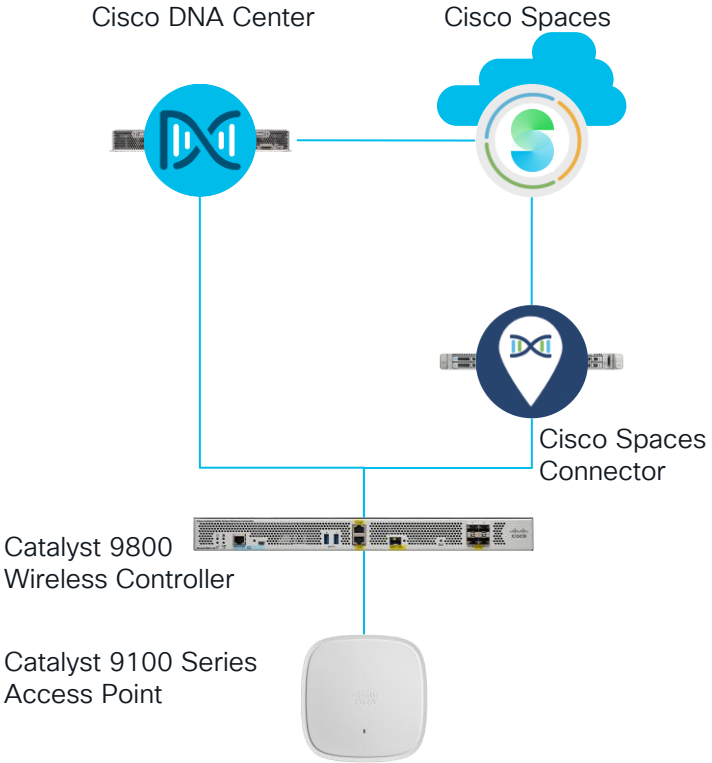


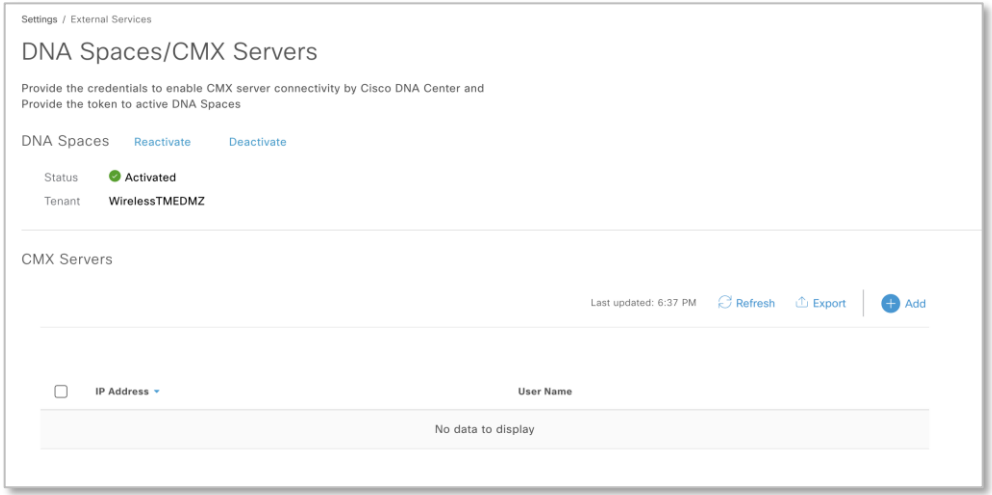
Rogue AP Auto Containment

- While we can configure the network to automatically contain detect Rogue APs, consider your environment and how to ensure that only malicious Rogues are being contained

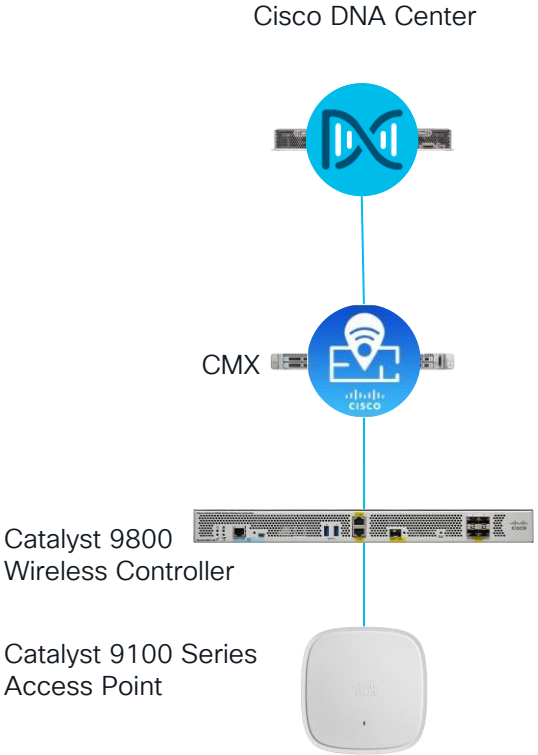


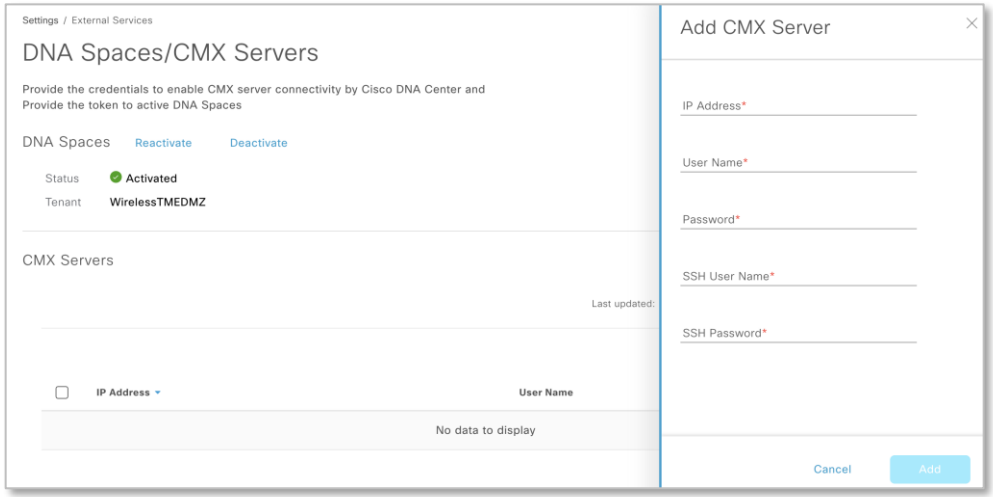
Enabling Location Services





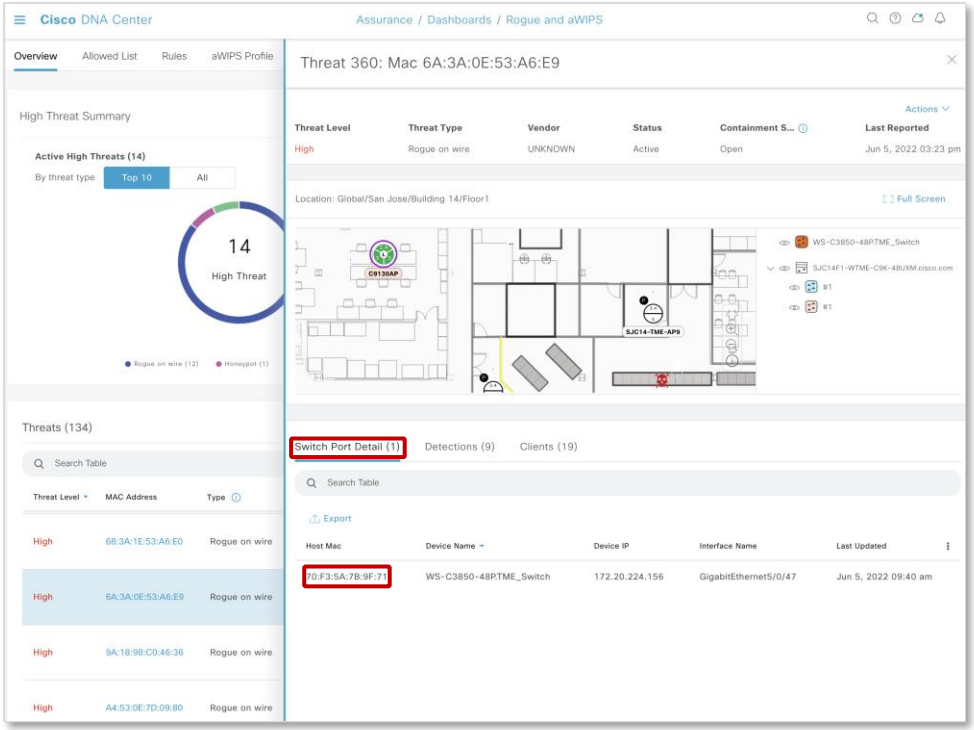
Enabling Location Services





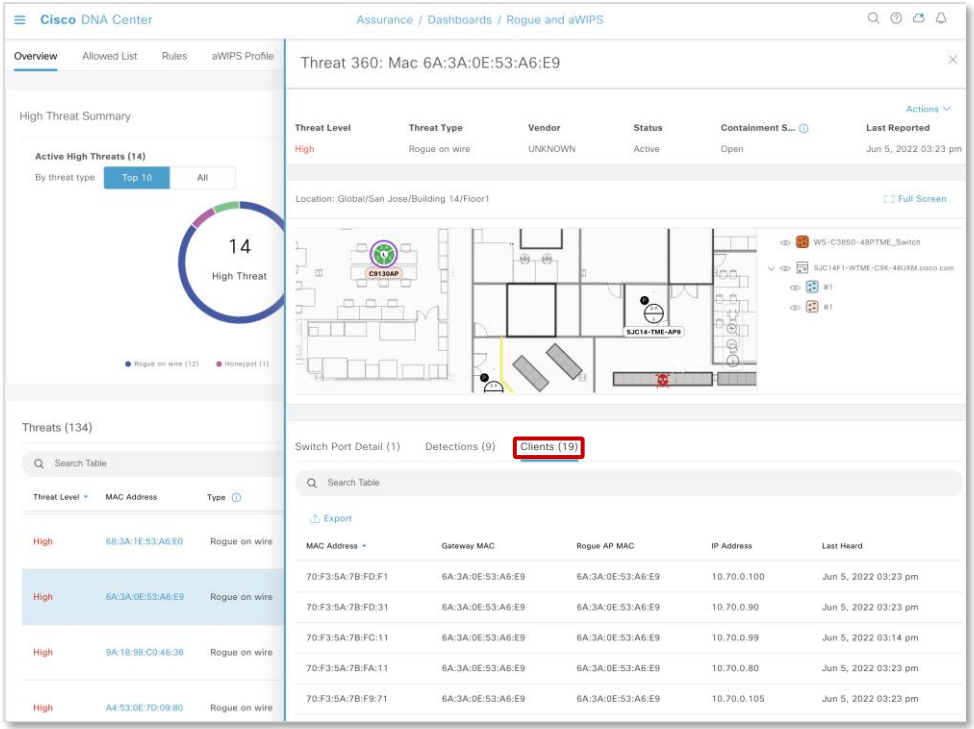
Rogue on Wire

- Matching Algorithms
  - MAC Address ±3/±2/±1
  - Vendor matching algorithms



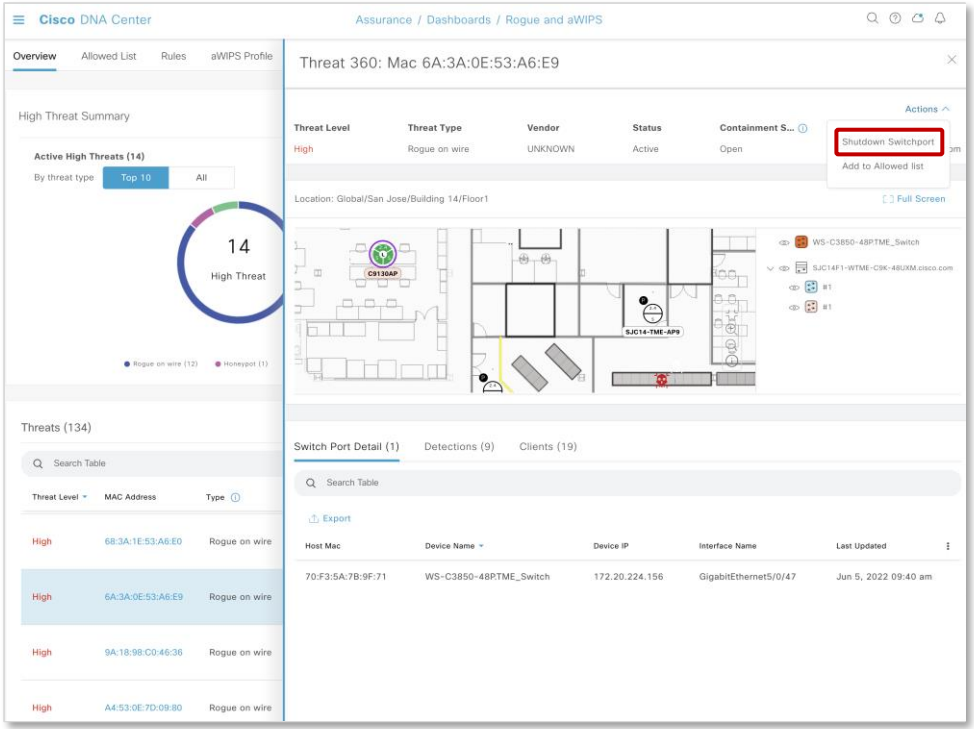
Rogue on Wire

- Matching Algorithms
  - MAC Address ±3/±2/±1
  - Vendor matching algorithms
- Rogue AP in Bridge Mode
  - Locate the Rogue AP via the Rogue Client MAC address and Gateway MAC Address

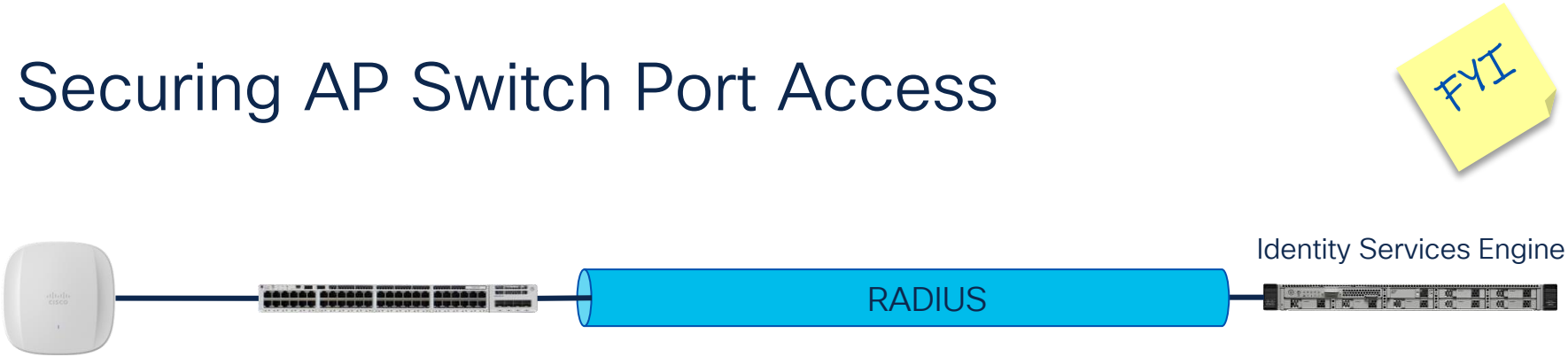


Rogue on Wire

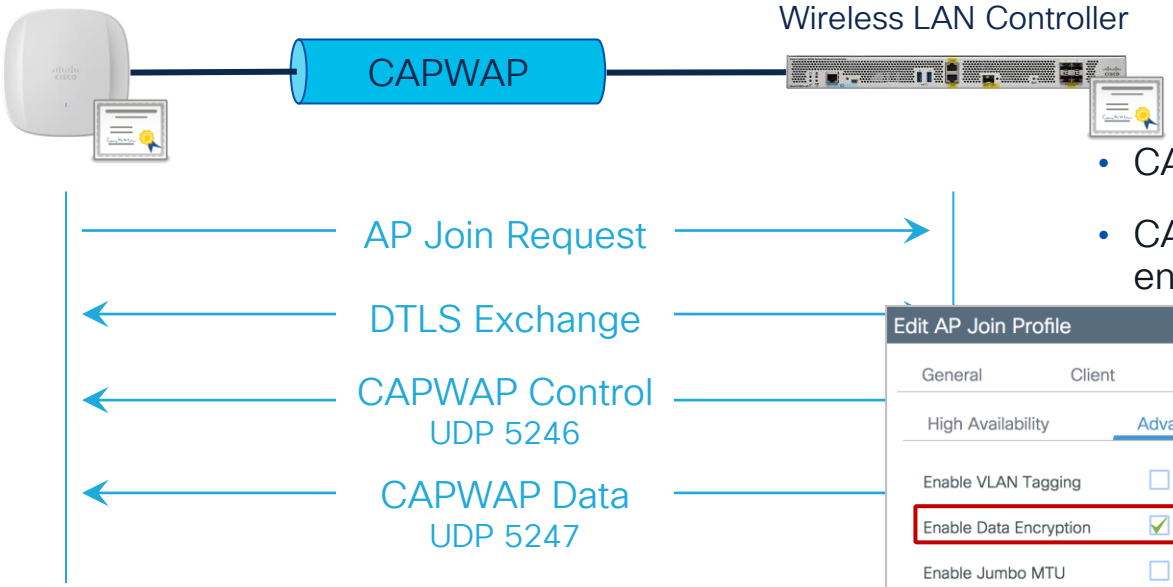
- Matching Algorithms
  - MAC Address ±3/±2/±1
  - Vendor matching algorithms
- Rogue AP in Bridge Mode
  - Locate the Rogue AP via the Rogue Client MAC address and Gateway MAC Address



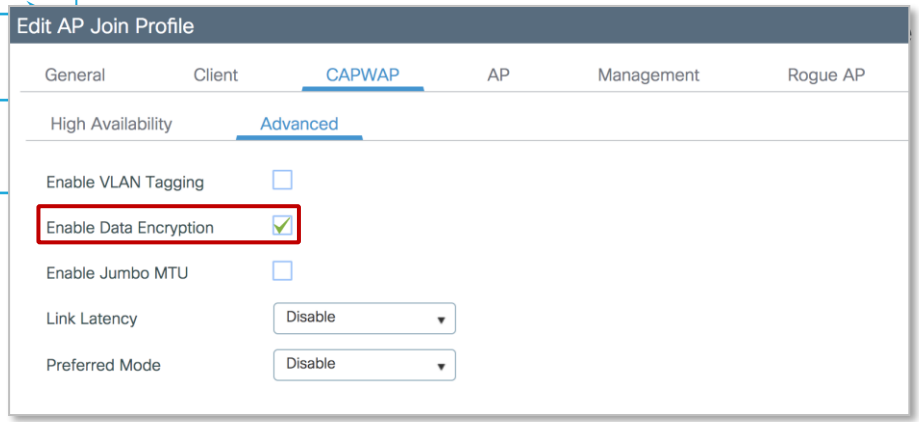
Securing AP Switch Port Access



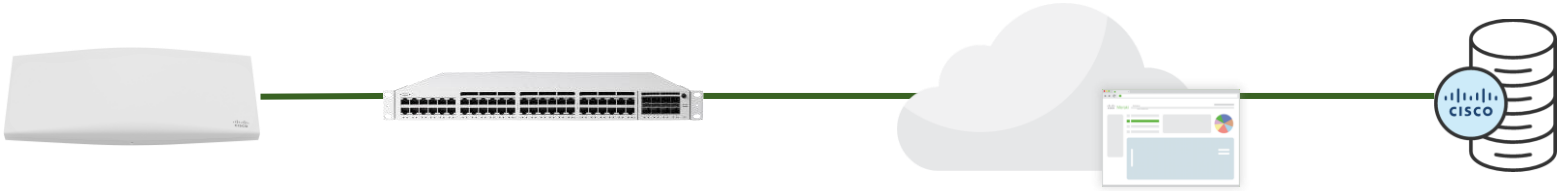
Securing AP to Controller Communication



- CAPWAP Control encrypted by default
- CAPWAP Data encapsulated but not encrypted by default



SecurePort



MR connected to MS

1

2

MS permits Meraki dashboard connection for MR

MR requests certificate from Cisco PKI

3

4

MR authenticates with acquired certificate

MS authorizes port based on configured profile

5

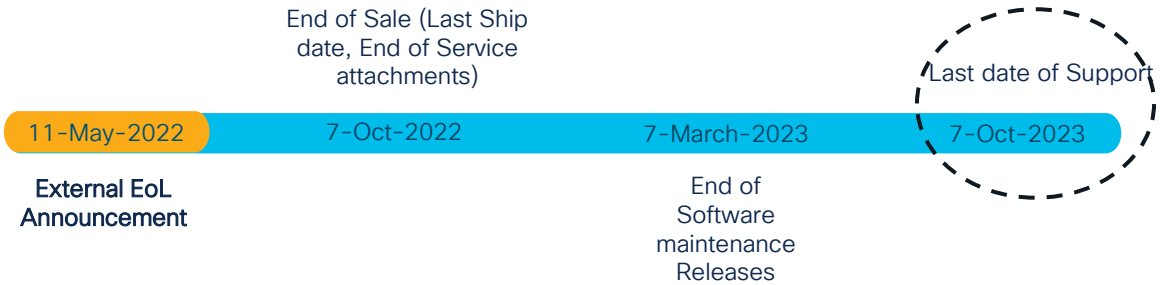
Air Marshal

- Rogue AP Detection
  - Wired Rogue
- WIDS/WIPS
  - Spoofed Management Frames
  - Malicious Broadcasts / DoS
  - Packet Floods

MSE WIPS End of Life

WIPS service on MSE is declared as EoL from 11th May 2022 onwards.

- MSE platform had already been declared EoL in Nov 2018.
- MSE 8.x had already been declared EoL Aug 2018.
- All the PIDs corresponding to WIPS license would be EoL.
- The EoL is applicable to all the MSE 7.x and 8.x releases

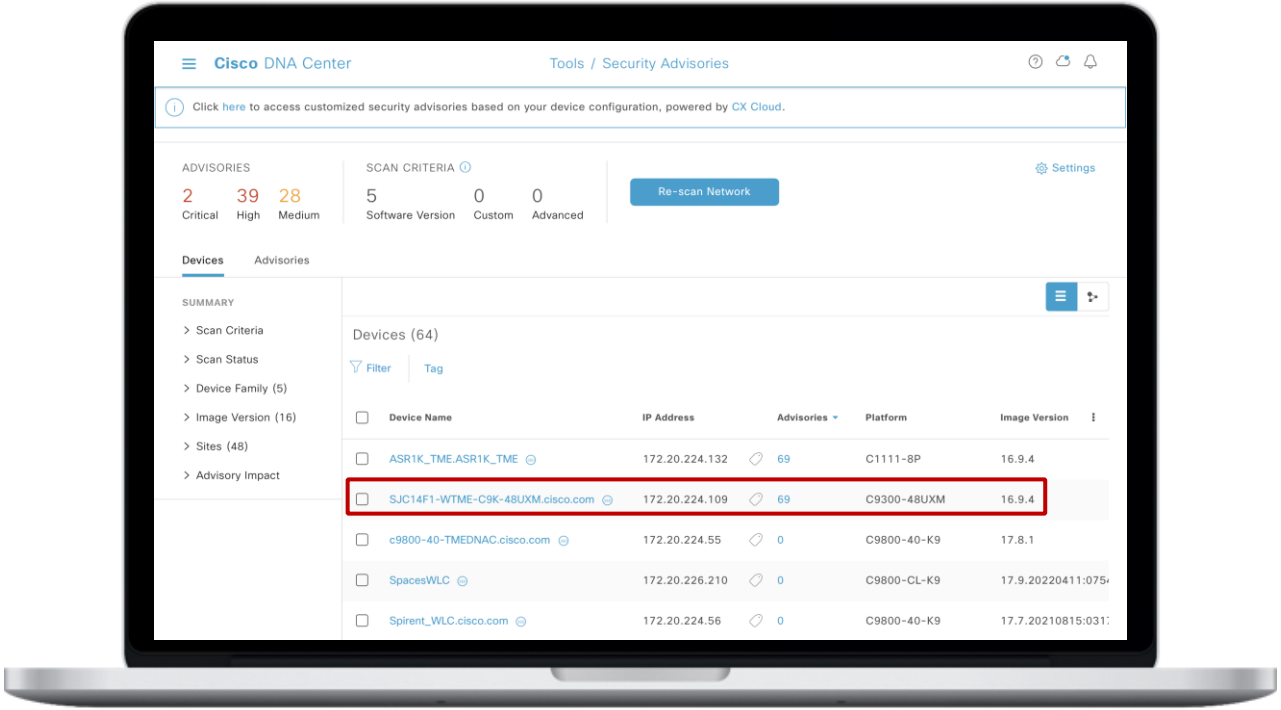


Product ID	Product Description
AIR-LM-WIPS-*	Cisco Enhanced Local Mode wIPS License
AIR-WIPS-*	Cisco wIPS License
C1-MSE-WIPS-*	Cisco ONE Mobility Svcs
L-LM-WIPS-*	Wireless IPS Lic For Enhanced Local Mode AP- E Delivery
L-MM-WIPS-*	Wireless IPS Lic For Monitor Mode AP- E Delivery
L-WIPS-*	WIPS Monitor Mode and Enhanced Local Mode licenses
MSE-WIPS-*	MSE WIPS Tracker Term

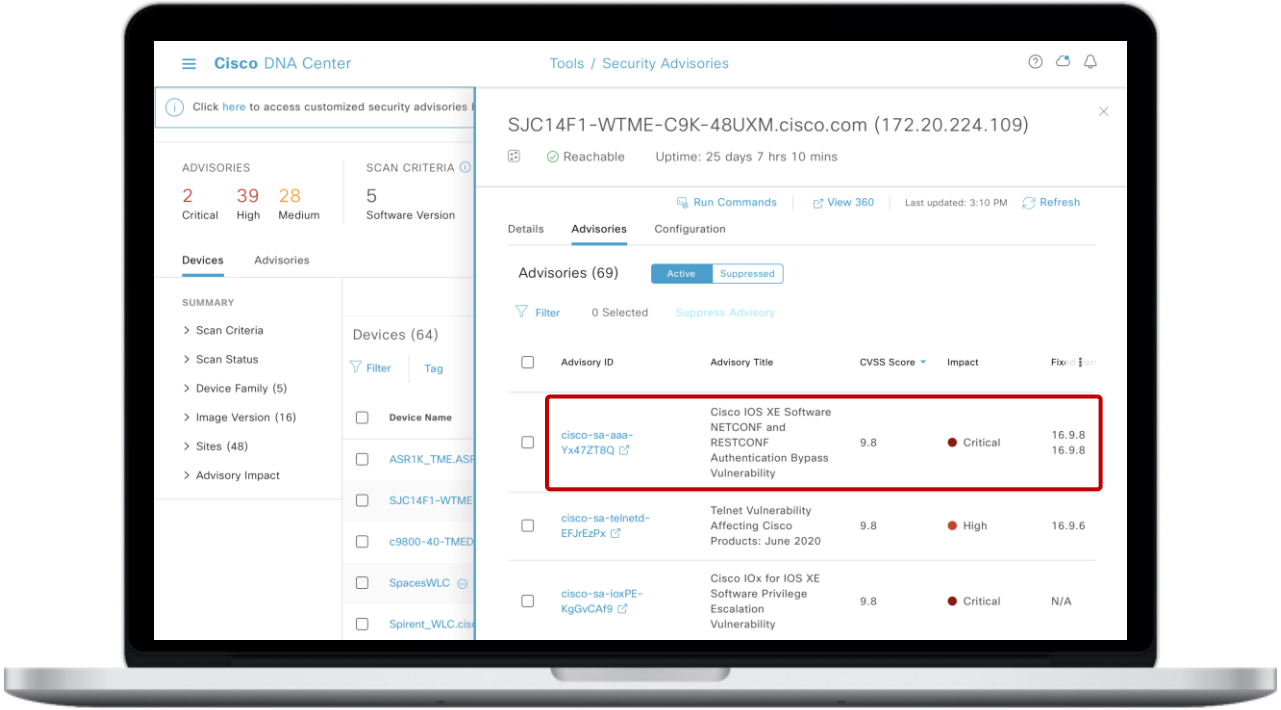
Next Steps

- NextGen aWIPS solution is available with DNA Center and WLC 9800 with DNA-A license.
- No separate local mode or monitor mode licenses are required for APs.
- High touch escalation support based on customer needs is available.

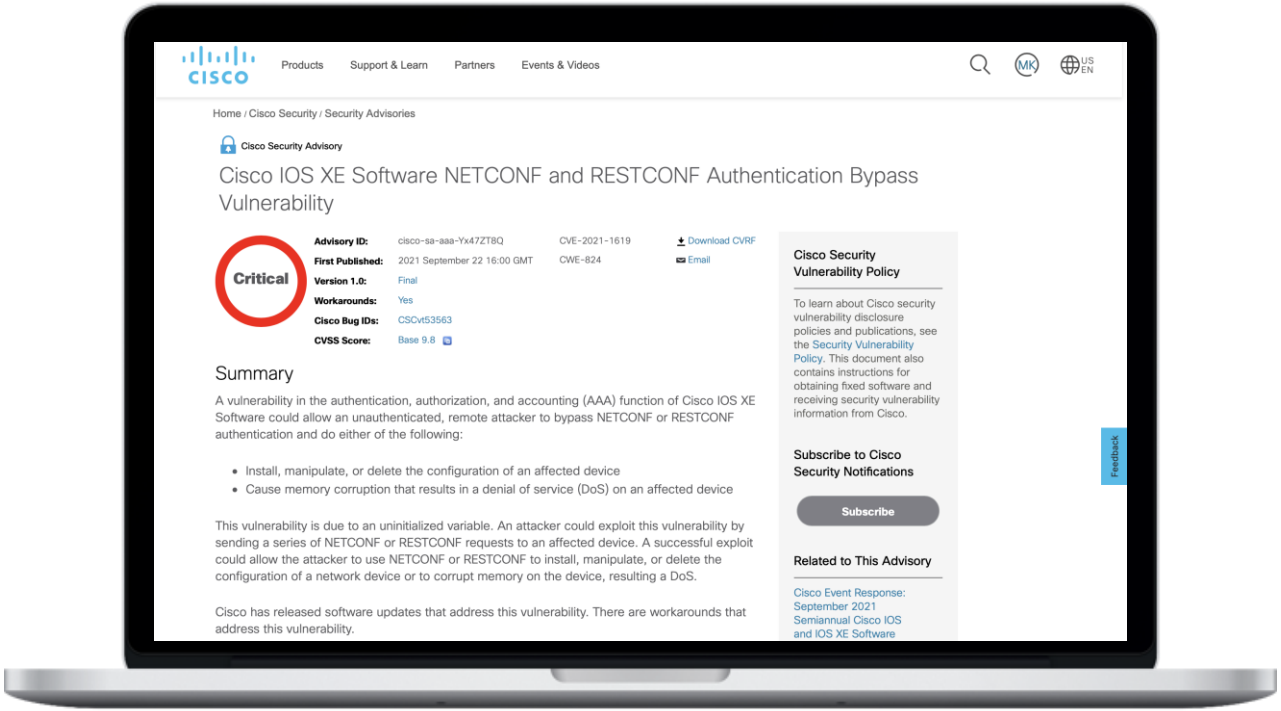
Cisco DNA Center Security Advisories



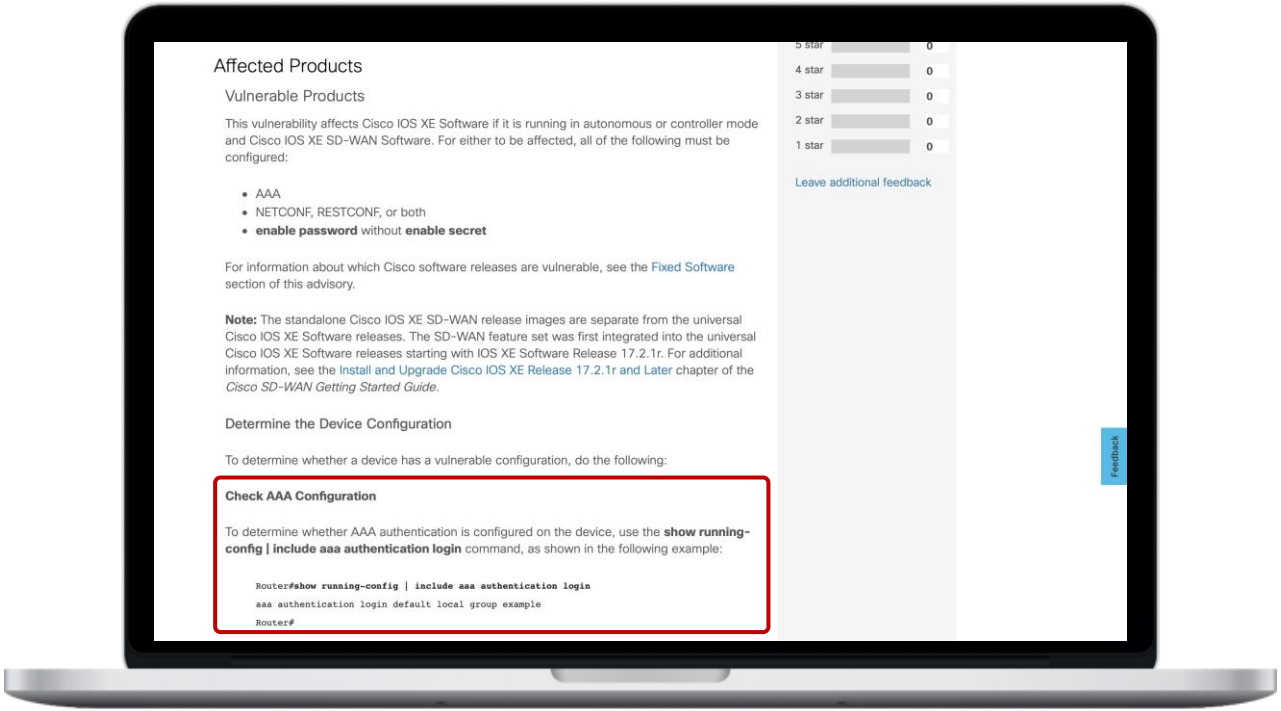
Cisco DNA Center Security Advisories



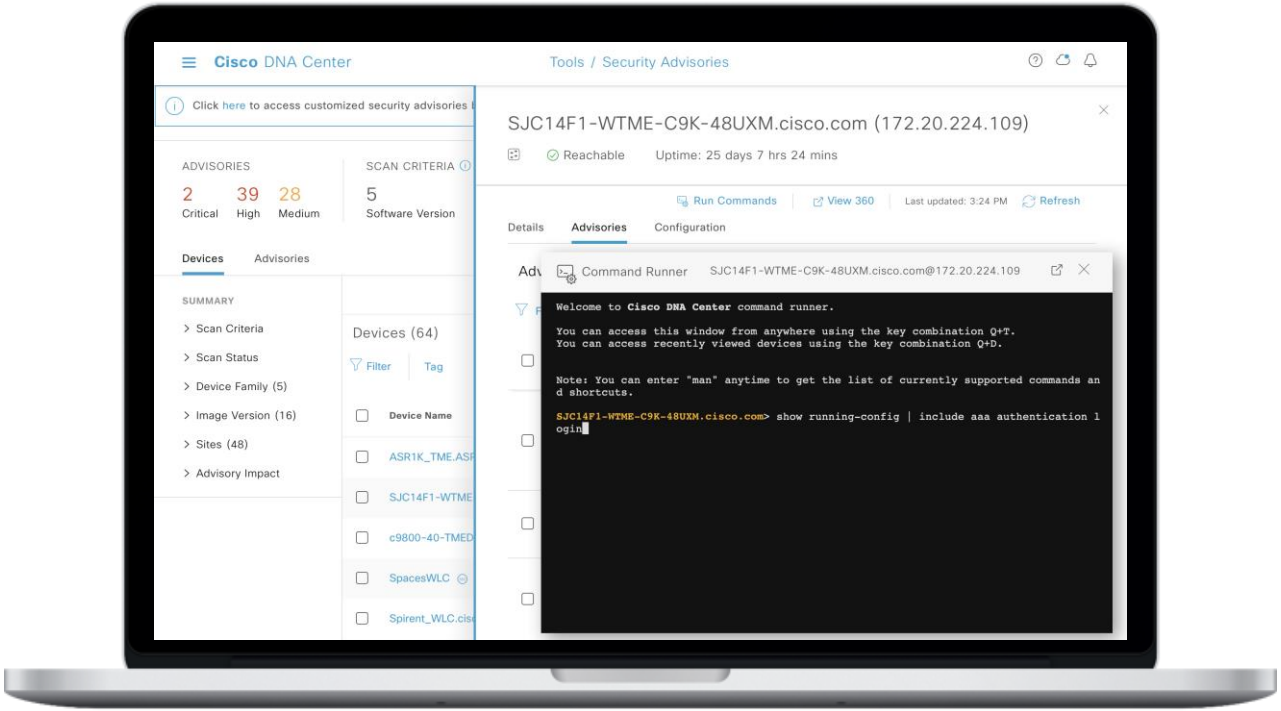
Cisco DNA Center Security Advisories



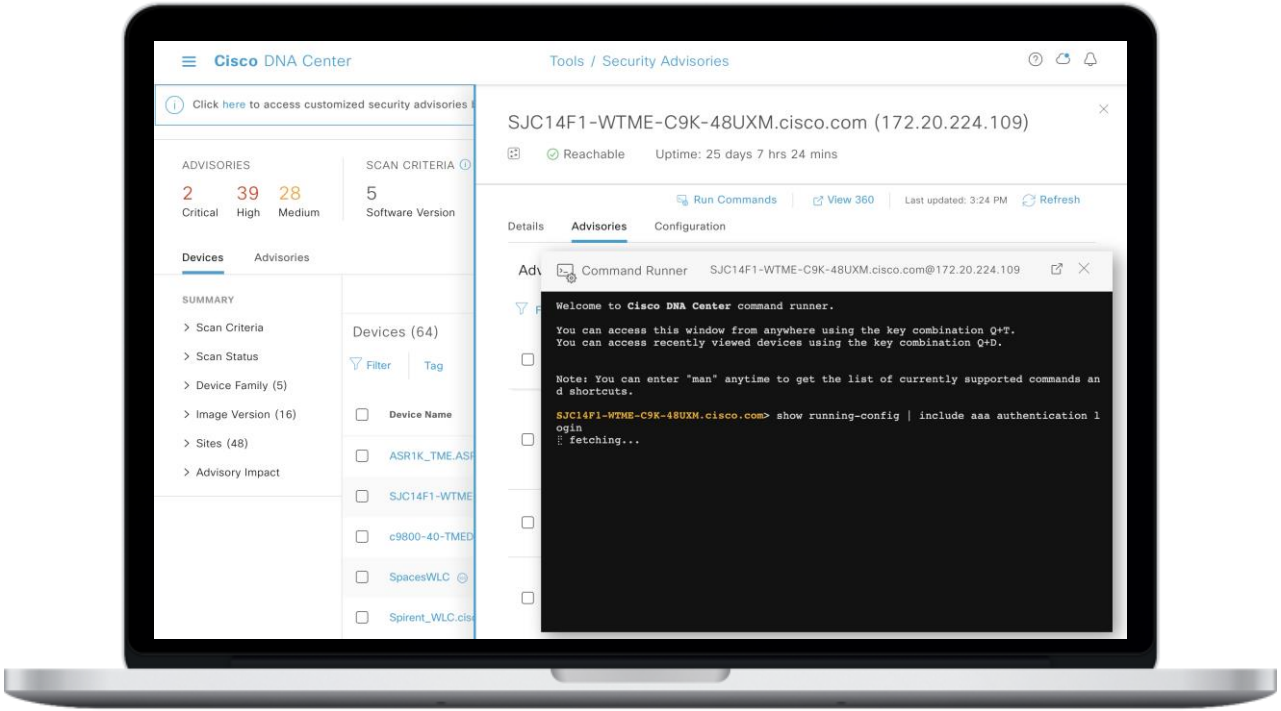
Cisco DNA Center Security Advisories



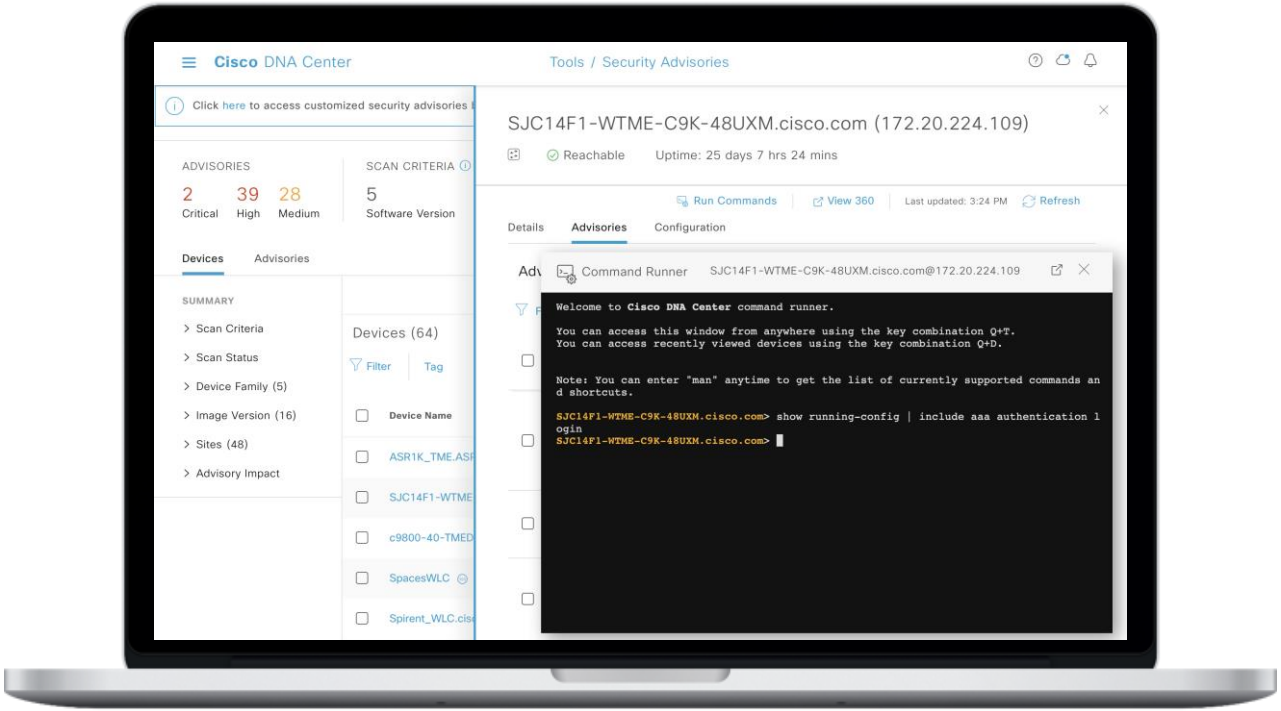
Cisco DNA Center Security Advisories



Cisco DNA Center Security Advisories

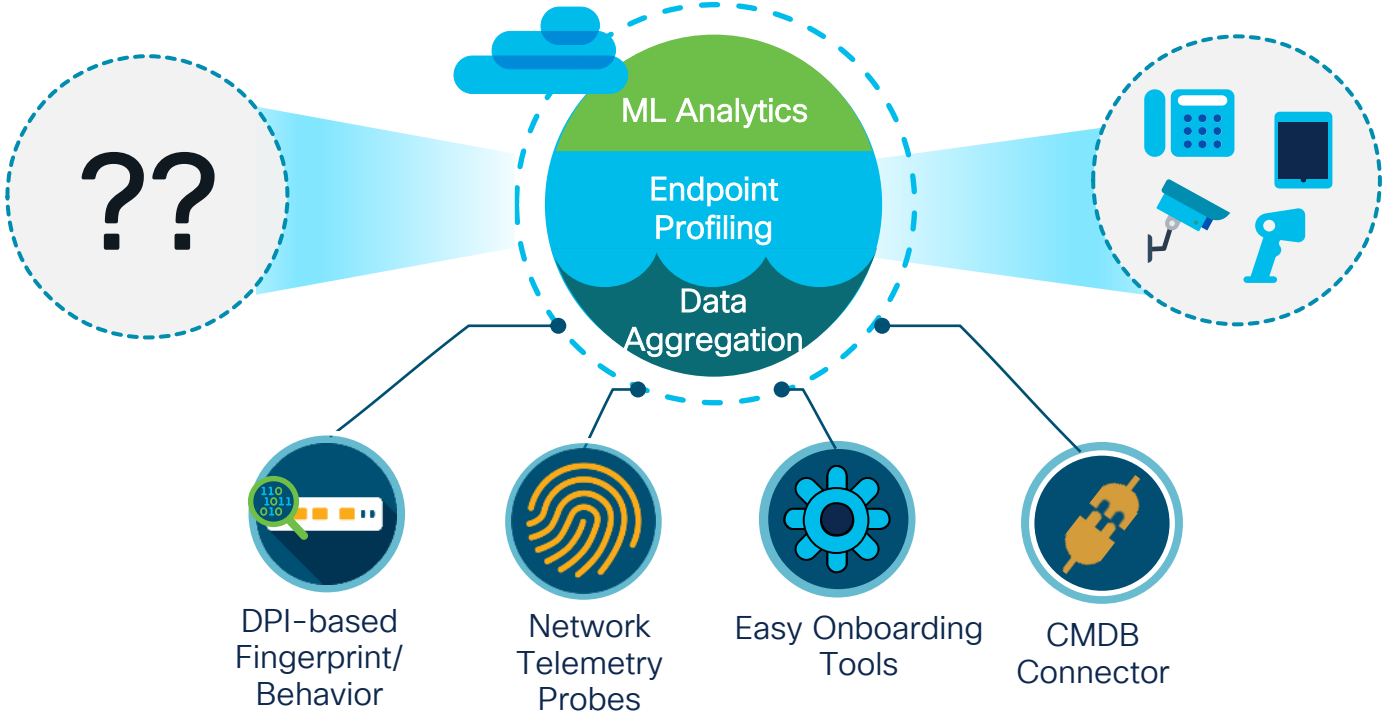


Cisco DNA Center Security Advisories



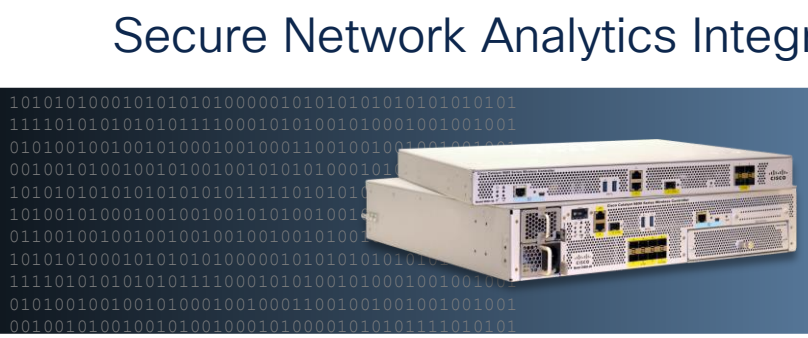
Cisco DNA Center AI Endpoint Analytics

FYI



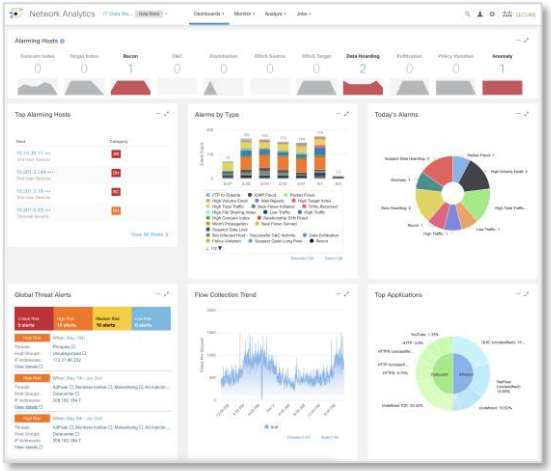
Network as a Sensor

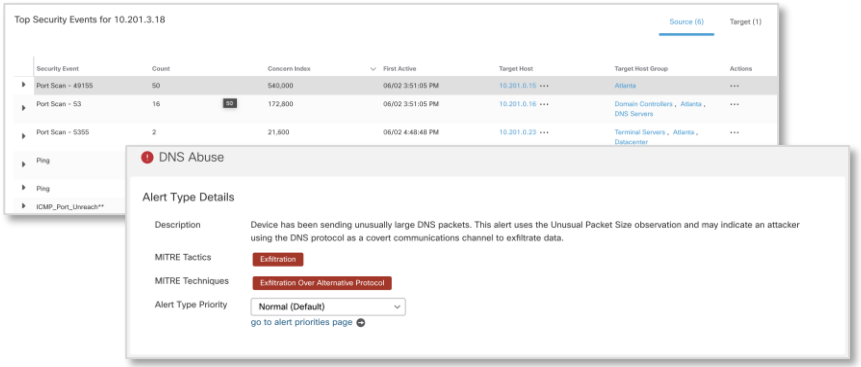
Secure Network Analytics Integration



Netflow

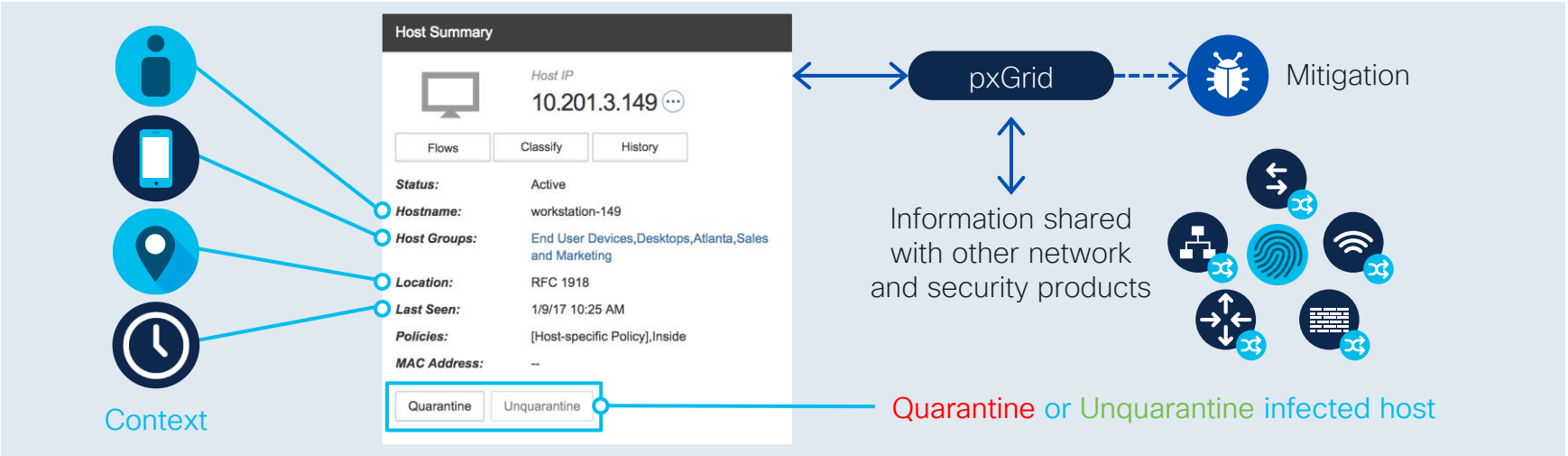
Malware detection and cryptographic compliance on Cisco Stealthwatch





Network as an Enforcer

Rapid Threat Containment



Identity Services Engine

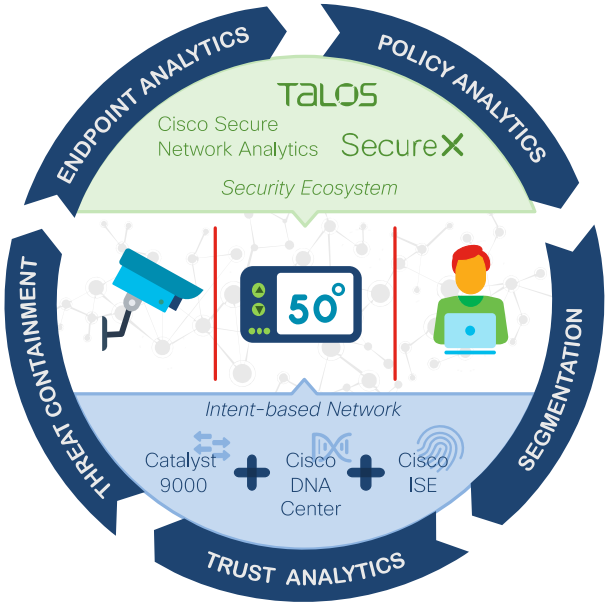
Secure Network Analytics Management Console

Securing the Wireless Network

Secure the Air

Secure the Devices

Secure the Network



Trustworthy Systems

Secure the Network

Secure the Air

DHCP Snooping | Port Security | WIPS

802.11i,r,w | IP Source Guard | ACLs

Secure the Device

ISE | Secure Network Analytics | Umbrella | SDA

Secure the Platform

Secure Boot | Image Signing | Counterfeit Protections | Hardware Trust Anchor | Runtime Defenses | OS Validation | Modern Crypto | Secure Device Onboarding

Secure the Development

Value Chain Security | Open Source Registration | Security Training | Threat Modeling | Product Security Baseline | PSIRT Advisories

Cisco Secure Development Lifecycle

https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html

The bridge to possible

Thank you

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

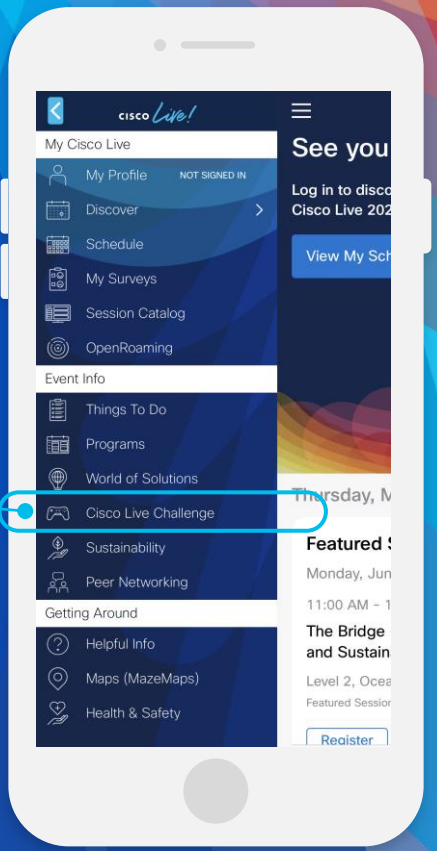
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive