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

BRKEWN-3004

cisco Live!

#CiscoLive

Agenda

- Wireless Security Fundamentals
  - WPA3
  - Authentication and Authorisation
  - Implications of 6GHz
- Wireless Intrusion Detection and Prevention
  - Rogue Detection and Containment
  - Advanced WIPS
  - Air Marshal
- Network as a Sensor and Enforcer

Cisco Webex App

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

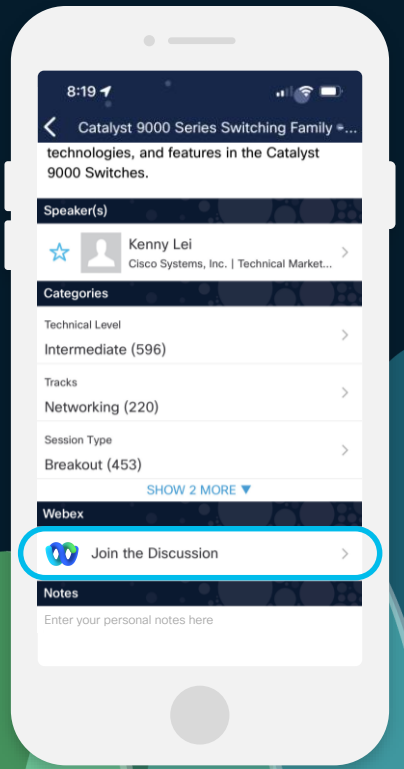
Questions?

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

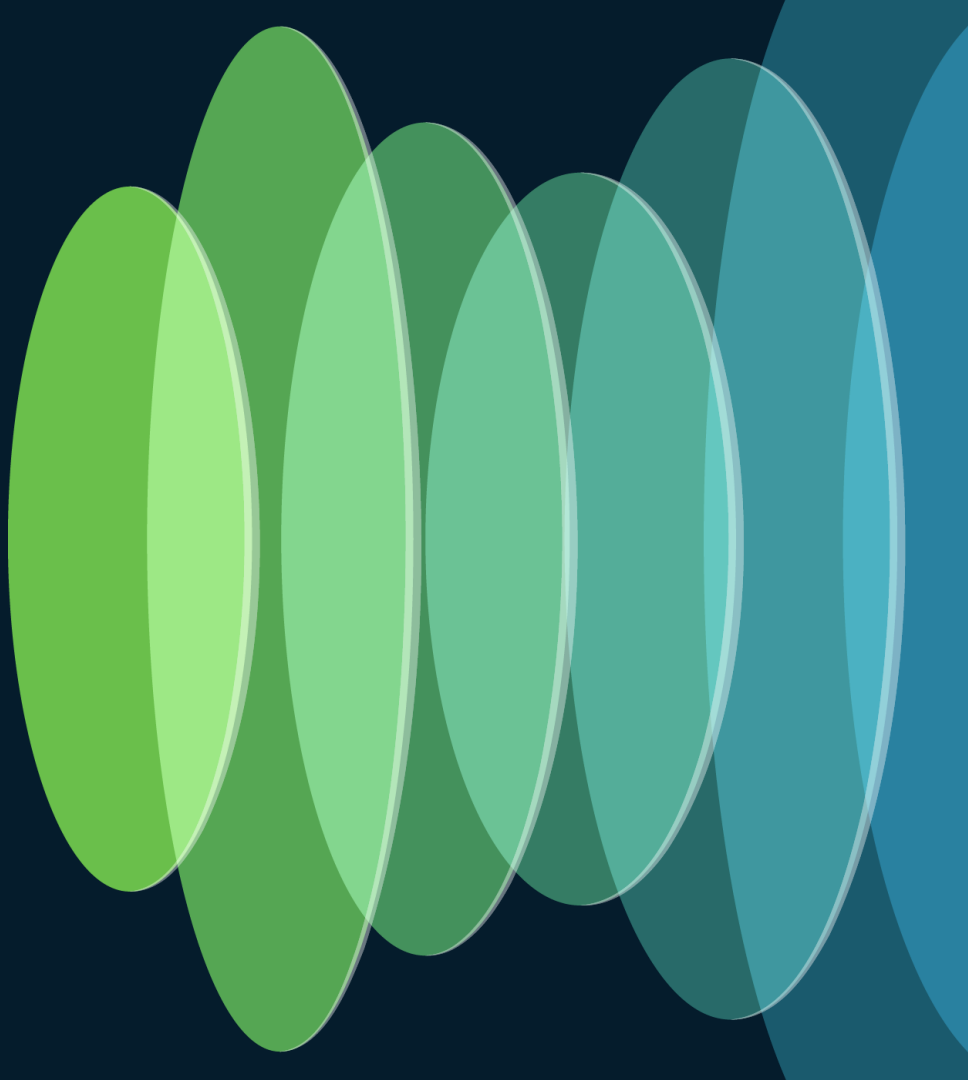
How

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 7, 2024.



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

WPA3-Personal

- Replace WPA2-PSK with WPA3-SAE
- Resistant to offline dictionary attacks
- WPA3-Personal Transition Mode

WPA3-Enterprise

- WPA3-Enterprise 192-bit
- Addition of GCM & ECC for crypto
- Quantum computer resistant encryption

Enhanced Open

- OWE for enhanced open networks
- OWE mandatory for WPA3 certification
- OWE Transition Mode

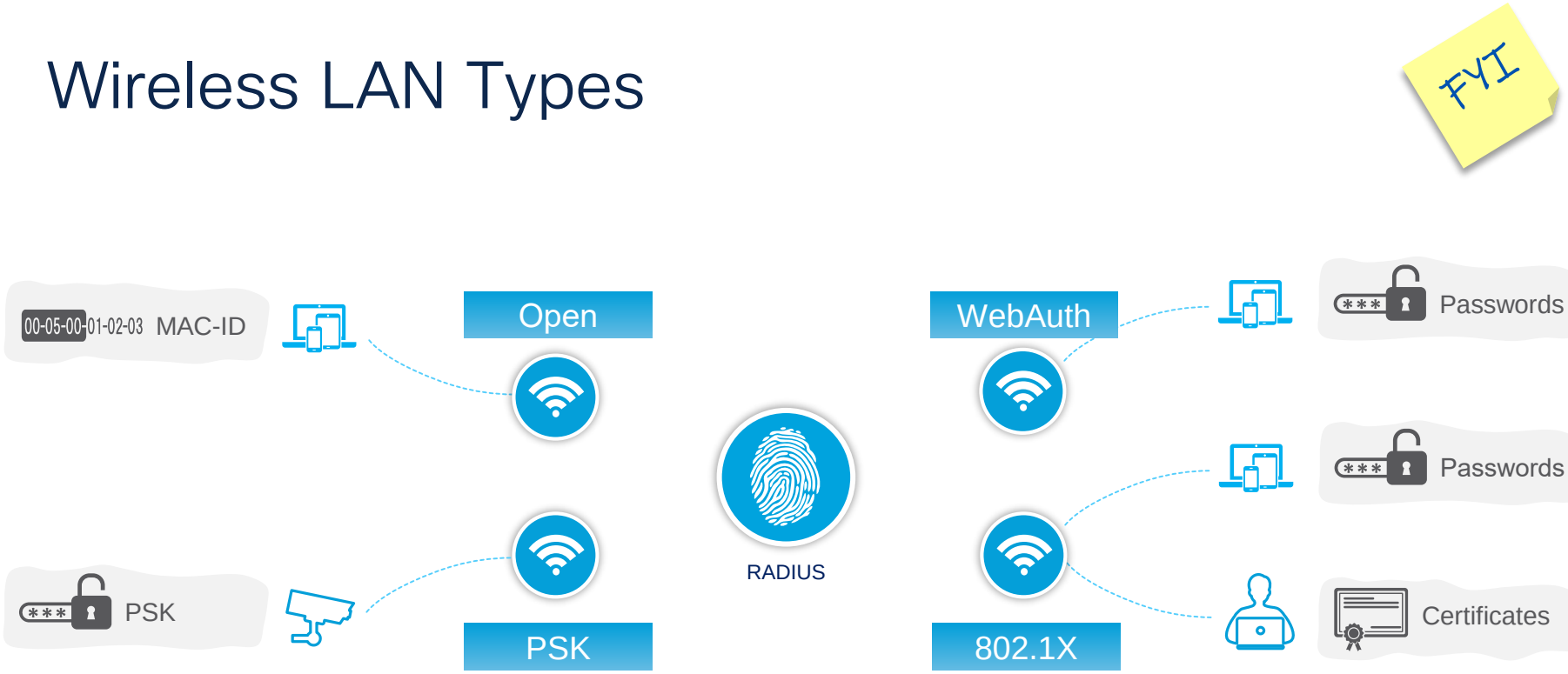
802.11w Protected Management Frames Mandatory

Supported across Catalyst and Meraki

WPA3 OWE/SAE/FT-SAE/802.1X-SHA256/FT-802.1X-SHA256 + AES-CCMP128
WPA3 SAE-EXT/FT-SAE-EXT + AES-CCMP128/GCMP256(Wi-Fi 7 Compliant)*
WPA3 Transition Mode
AP Beacon Protection*

*Planned (IOS-XE 17.15.1, Meraki R31-1)

Wireless LAN Types



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)

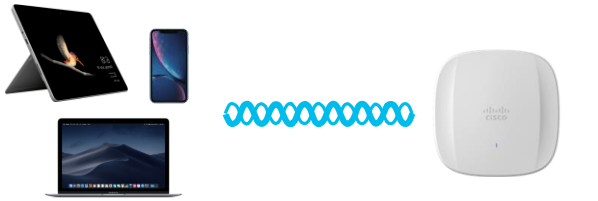
- Wi-Fi Certified Enhanced Open
  - Opportunistic Wireless Encryption (OWE)

802.11 Fundamentals

Authentication

802.11 Fundamentals

Authentication



Supplicant

Authenticator

802.11 Fundamentals

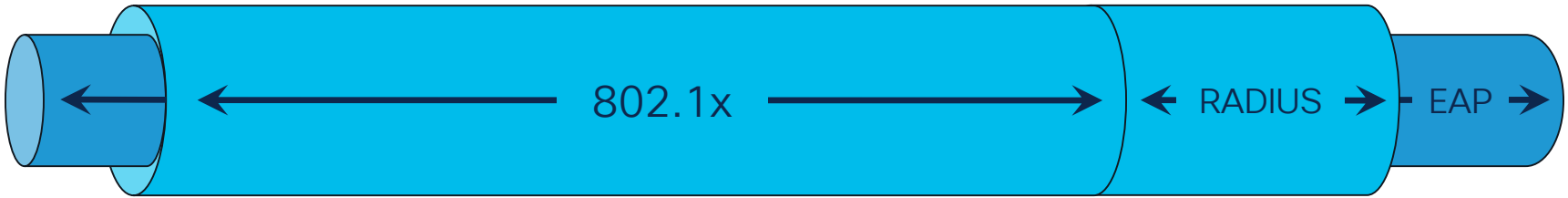
Authentication

802.11 Fundamentals

- Authentication

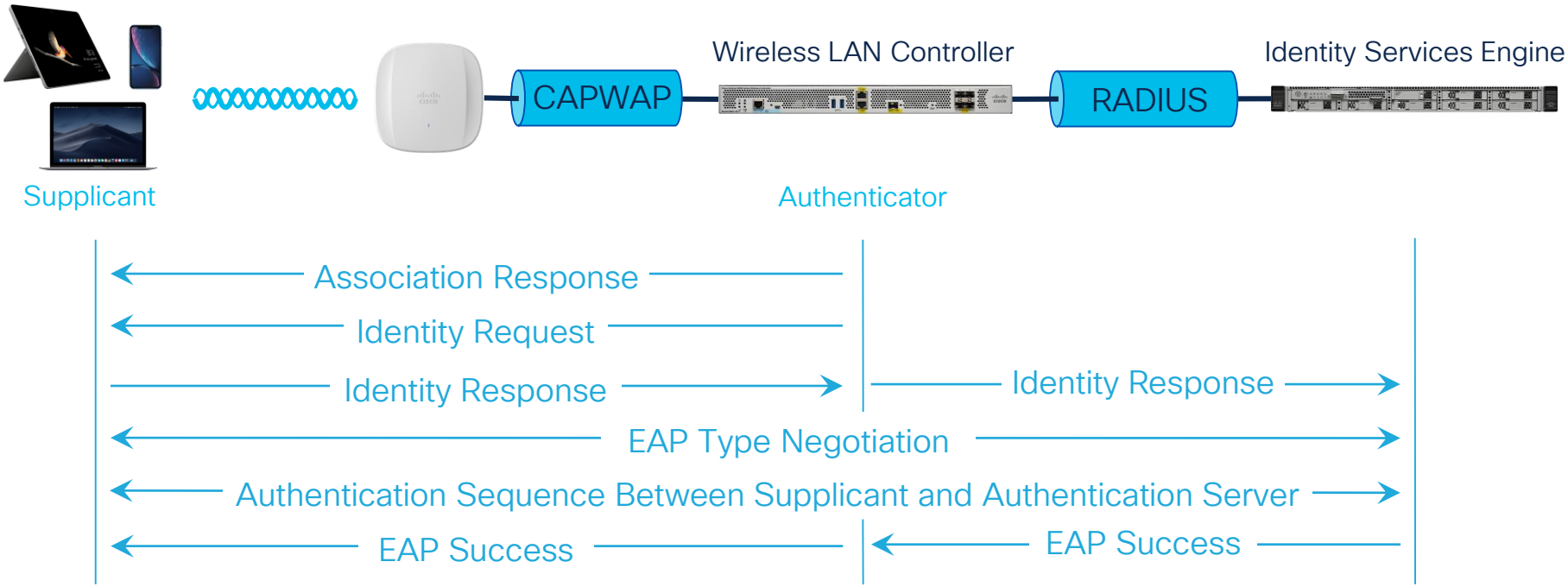
802.11 Fundamentals

Authentication

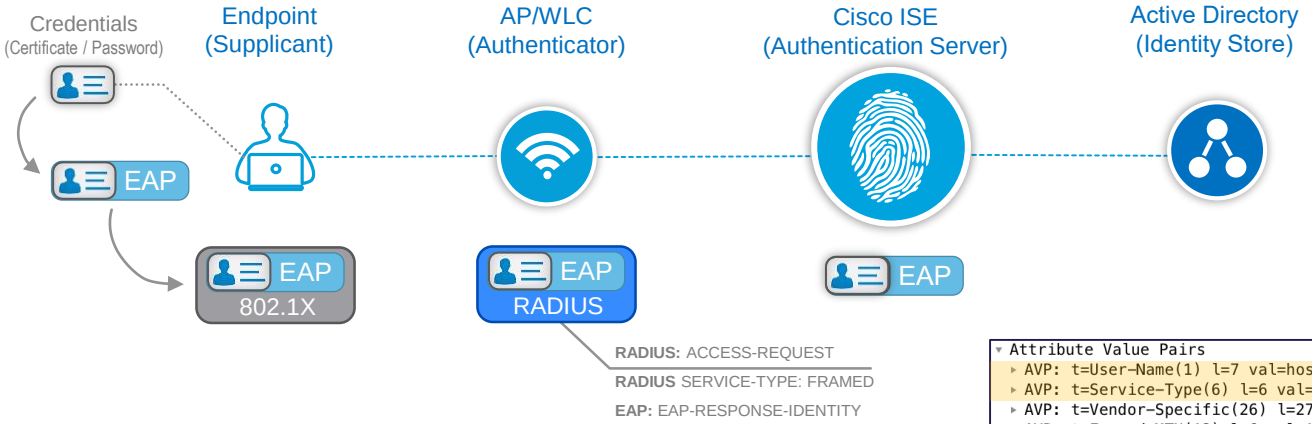


802.11 Fundamentals

Authentication



802.1X



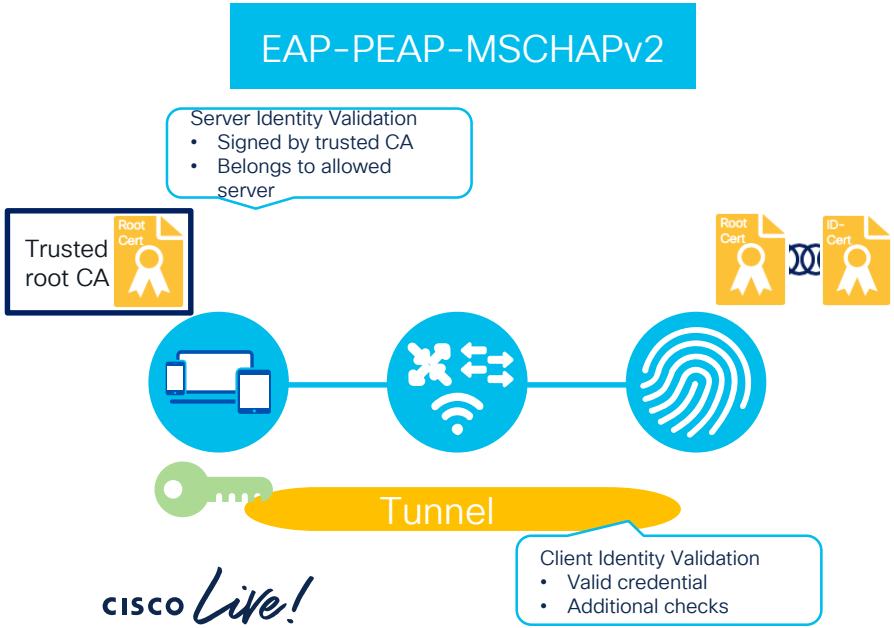
EAP: Extensible Authentication Protocol

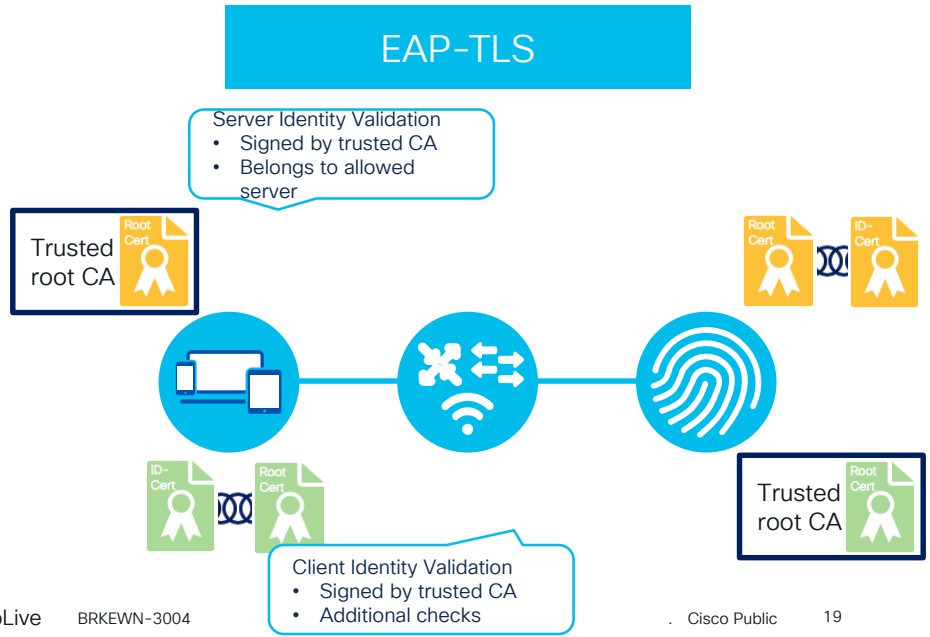
Supplicant: Software running on the client that provides credentials to the authenticator (Network Device).

```
▾ Attribute Value Pairs
  ▸ AVP: t=User-Name(1) l=7 val=hosuk
  ▸ AVP: t=Service-Type(6) l=6 val=Framed(2)
  ▸ AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
  ▸ AVP: t=Framed-MTU(12) l=6 val=1485
  ▸ AVP: t=EAP-Message(79) l=12 Last Segment[1]
  ▸ AVP: t=Message-Authenticator(80) l=18 val=10c87be3950f1cec07ae61f4dfad789a
  ▸ AVP: t=EAP-Key-Name(102) l=2 val=
  ▸ AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  ▸ AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
  ▸ AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
  ▸ AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
  ▸ AVP: t=NAS-IP-Address(4) l=6 val=192.168.201.61
  ▸ AVP: t=NAS-Port-Id(87) l=17 val=capwap_90000004
  ▸ AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
  ▸ AVP: t=NAS-Port(5) l=6 val=8013
  ▸ AVP: t=Called-Station-Id(30) l=31 val=38:0e:4d:4a:3b:20:C9800-DOT1X
  ▸ AVP: t=Calling-Station-Id(31) l=19 val=08:e6:89:2d:26:4d
  ▸ AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
  ▸ AVP: t=Vendor-Specific(26) l=35 vnd=ciscoSystems(9)
  ▸ AVP: t=NAS-Identifier(32) l=10 val=C9800-CL
```

EAP-PEAP-MSCHAPv2 and EAP-TLS

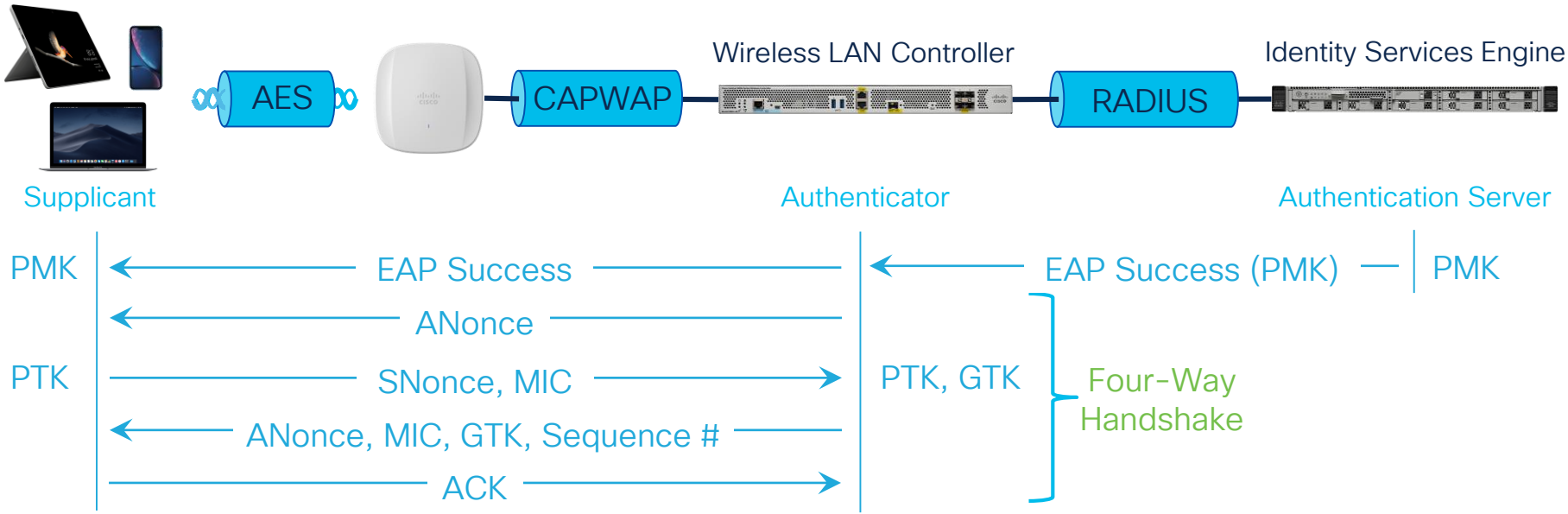
- Both: Use of server certificate
- EAP-TLS: Mutual certificate authentication
- EAP-PEAP: Use of tunnel to encrypt transport





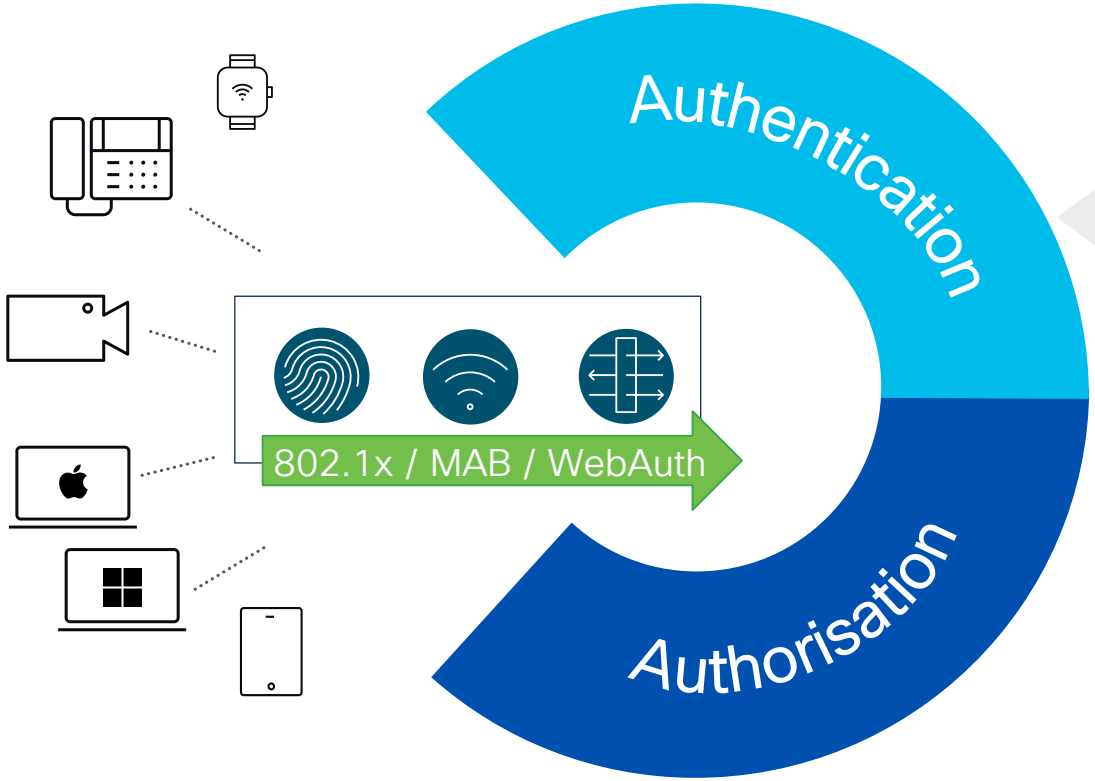
802.11 Fundamentals

Encryption



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

Authentication and Authorisation



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

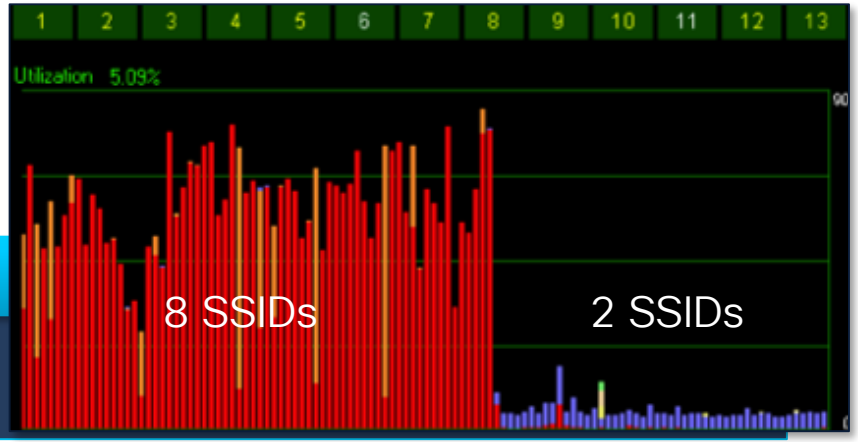
- Location
- Day and Time
- Access Type
- Context

Policy Elements

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

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

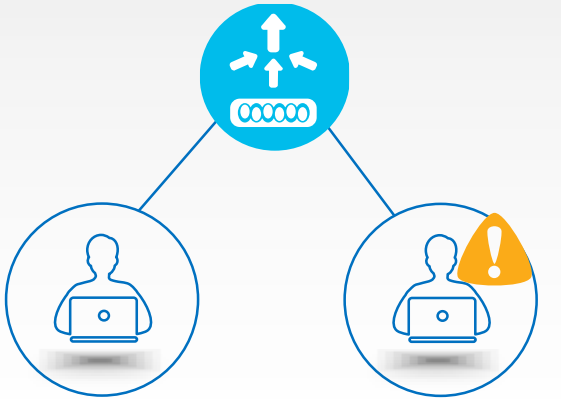
TrustSec / Adaptive Policy / Software Defined Access

- 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)

Authorization Options

Named ACL

Named ACL

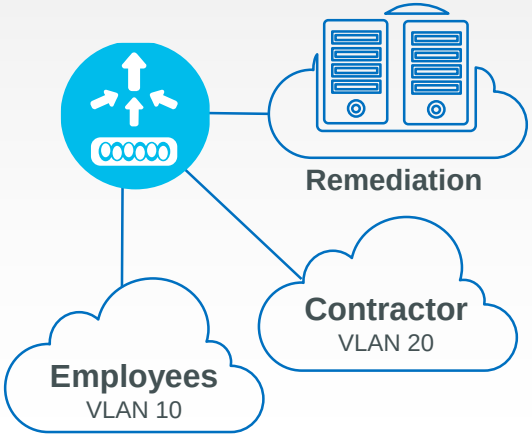


Healthy
permit ip any any

Non-compliant
permit ip host <remediation>
deny ip any any

VLANs

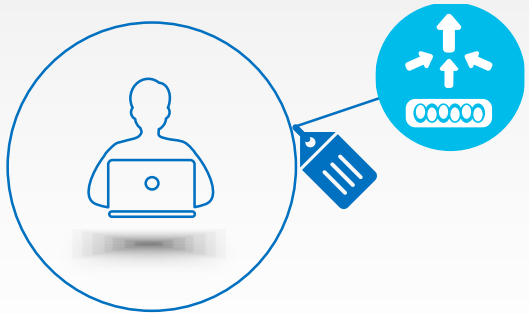
Dynamic VLAN Assignments



Per user / Per group / Per MAC

SGTs or UDN/WPN ID

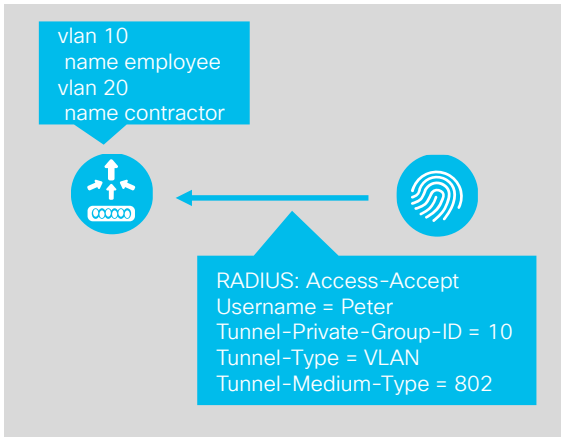
User Defined Network
or Scalable Group Tags



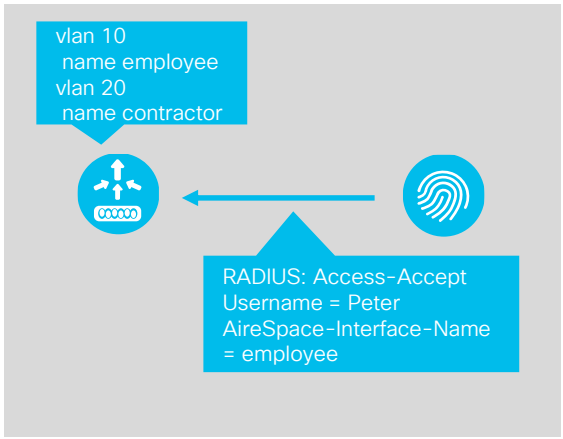
Scalable Group Tags for group based policies and SDA
UDN/WPN ID Access Control for personal networks

Dynamic VLAN

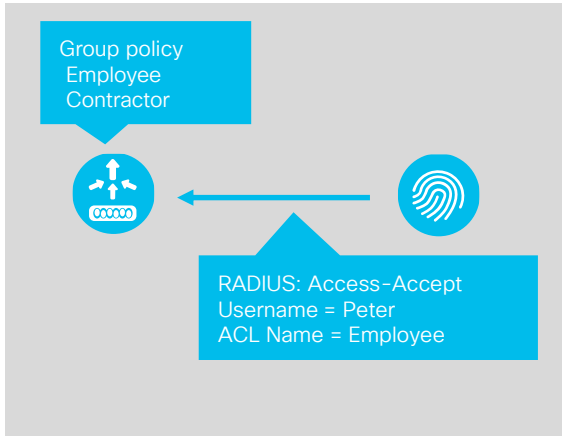
Standard RADIUS



VSA: AireSpace Interface Name



Group policy



Dynamic VLAN Assignment via RADIUS

- Dynamic VLAN assignment via RADIUS Standard 64/65/81 & Airespace-interface-name VSA

RADIUS attribute specifying group policy name

Filter-Id

- **Filter-Id**
- Reply-Message
- Airespace-ACL-Name
- Aruba-User-Role

Named VLANs (1)

Single, multiple, or range of IDs allowed per name (comma separated).

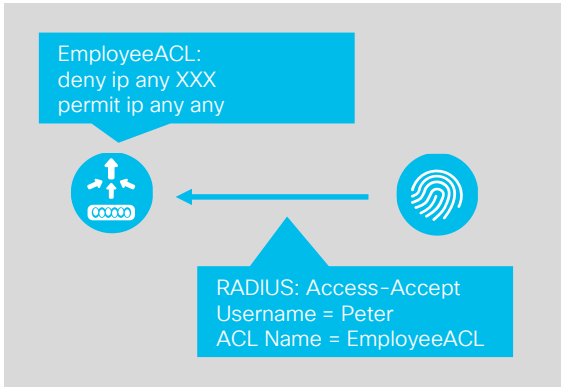
#	VLAN name	VLAN ID
1	employee	200,220,300-310

Add a Named VLAN

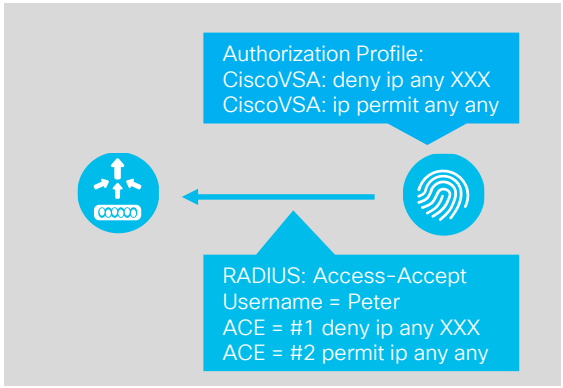
Note: For ISE integration each AP is a NAS client unlike WLC that acts as NAS for all APs

RADIUS Enforced ACLs

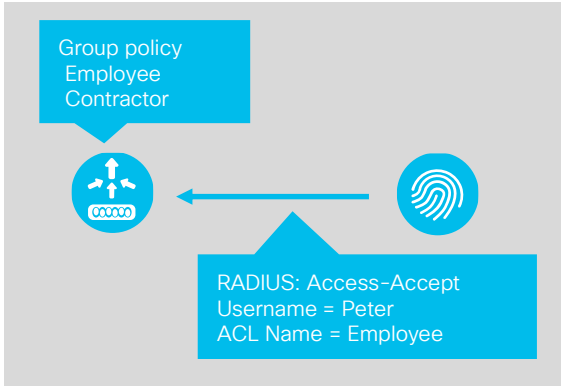
Named ACL



Per-User ACL



Group policy



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.

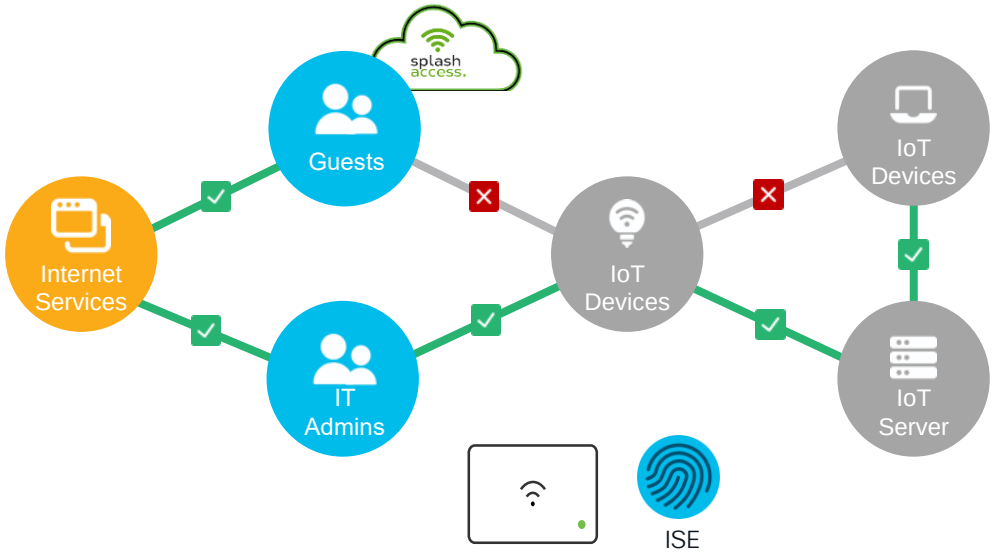
Security with Network Access Control

Secure Enterprise Access
Trusted users and their devices access resources across network

BYOD & Guest Wi-Fi
Manage policies on personal devices and secure Guest Wi-Fi with walled garden

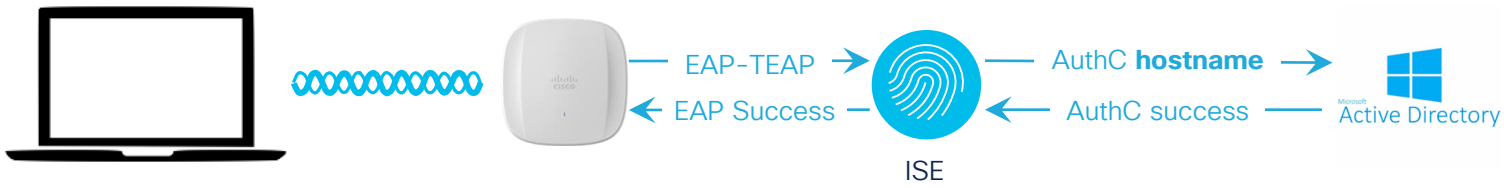
Profiling & Posturing
Classification of unknown endpoints and posture check for compliance

TrustSec
Granular policies using SGTs for micro segmentation



Machine Authentication

EAP Chaining with TEAP



EAP-Chaining Result:
User failed and Machine succeeded

Machine Authentication

EAP Chaining with TEAP

Time	Status	Details	Identity	Endpoint ID	Auth Met...	Authentication Protocol
	Auth Passed			00:50:56:91:41:6A		
Jan 24, 2023 02:08:38.5...	✓		tuiuser3@trappedunderise.com,host/WIN10-VM3...	00:50:56:91:41:6A	dot1x	TEAP (EAP-TLS)
Jan 24, 2023 02:08:13.9...	✓		host/WIN10-VM3.trappedunderise.com	00:50:56:91:41:6A	dot1x	TEAP (EAP-TLS)

EAP-Chaining Result:
User and Machine both succeeded

EndPointMACAddress	00-50-56-91-41-6A
EapChainingResult	User and machine both succeeded

On-Prem and Cloud Identity

On-Prem Identity

802.1x, Network Access

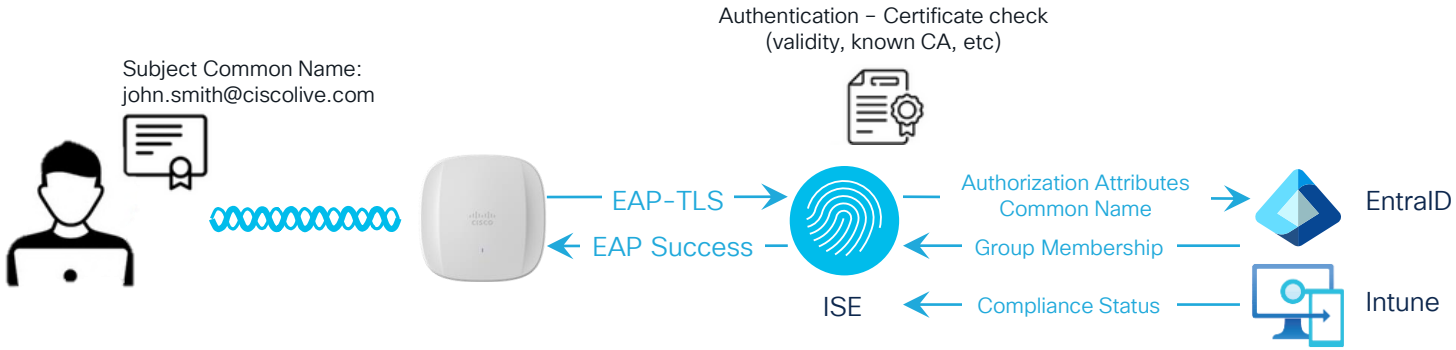
PEAP-MSCHAPv2,
EAP-FAST, EAP-TLS
PAP, MAC Auth Bypass

Cloud Identity

VPN, Application Access

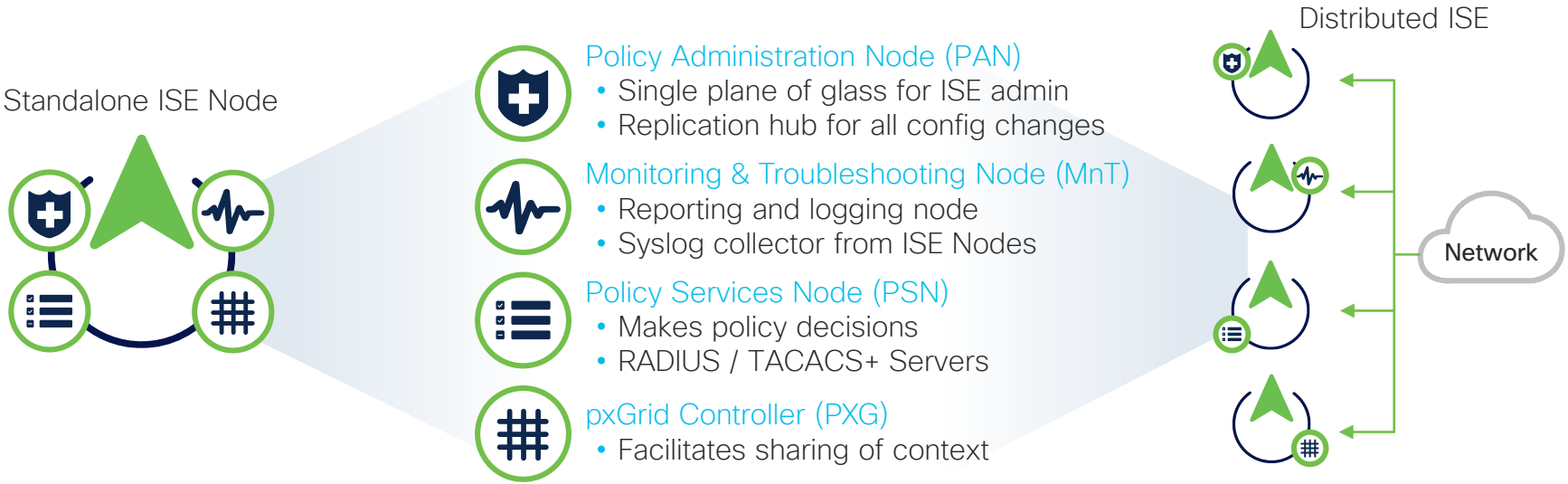
SAMLv2, OpenID Connect

Cloud Identity with EAP-TLS



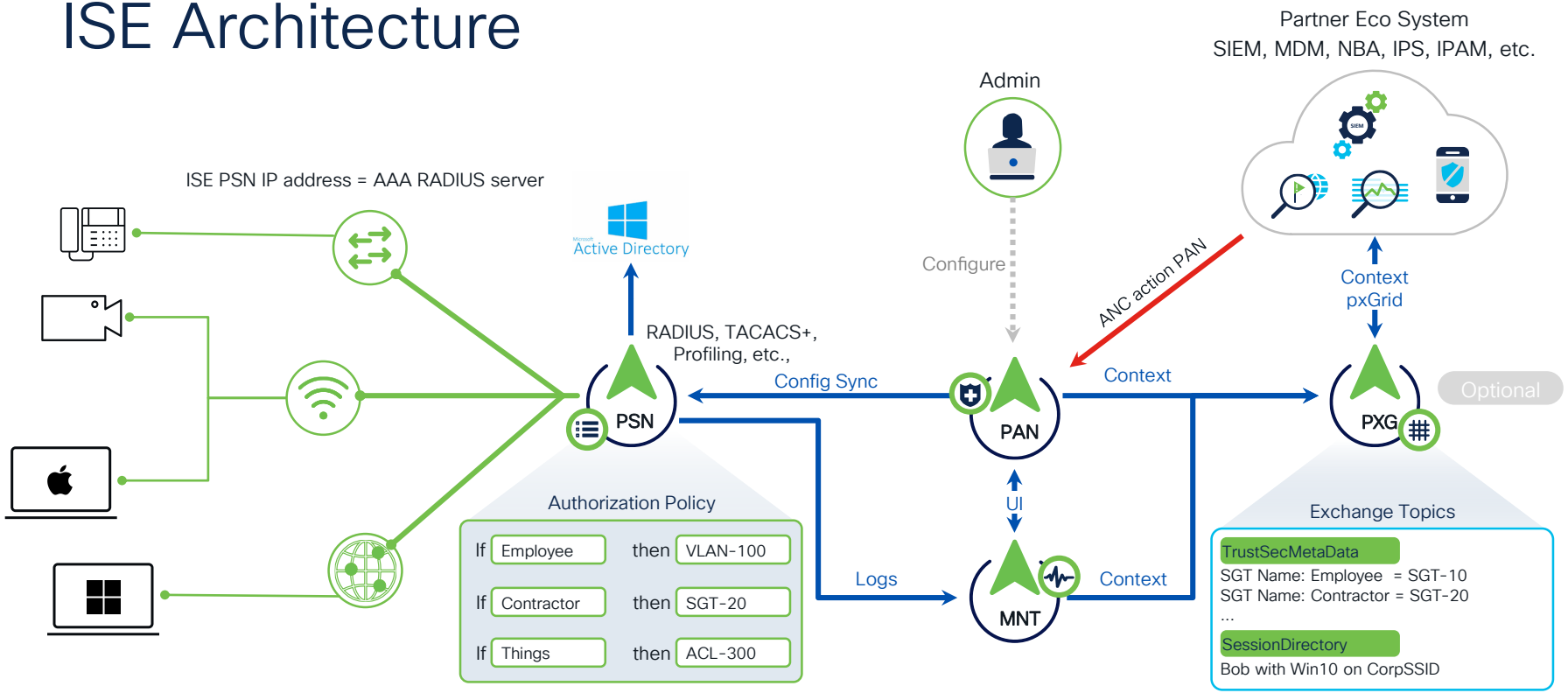
https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hld-76840754

ISE Personas



- Standalone provides no redundancy
  - Use for demo, testing, lab

ISE Architecture



https://cs.co/ise-scale

Secure Fast Roaming Challenges

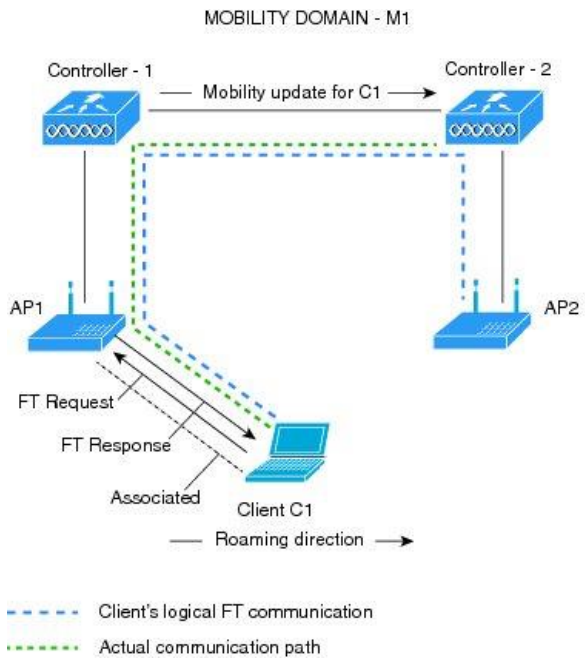
- Client channel scanning and AP selection
- Re-authentication of client device and re-keying

Secure Fast Roaming

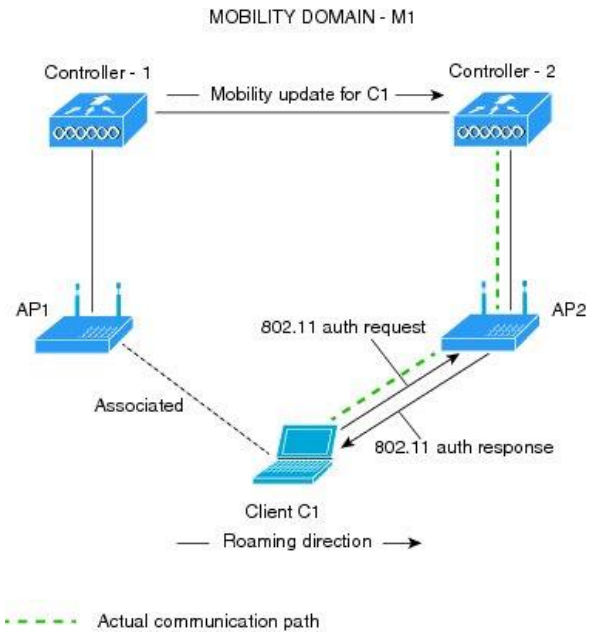
802.11k/v/r and Wi-Fi Agile Multiband

- 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



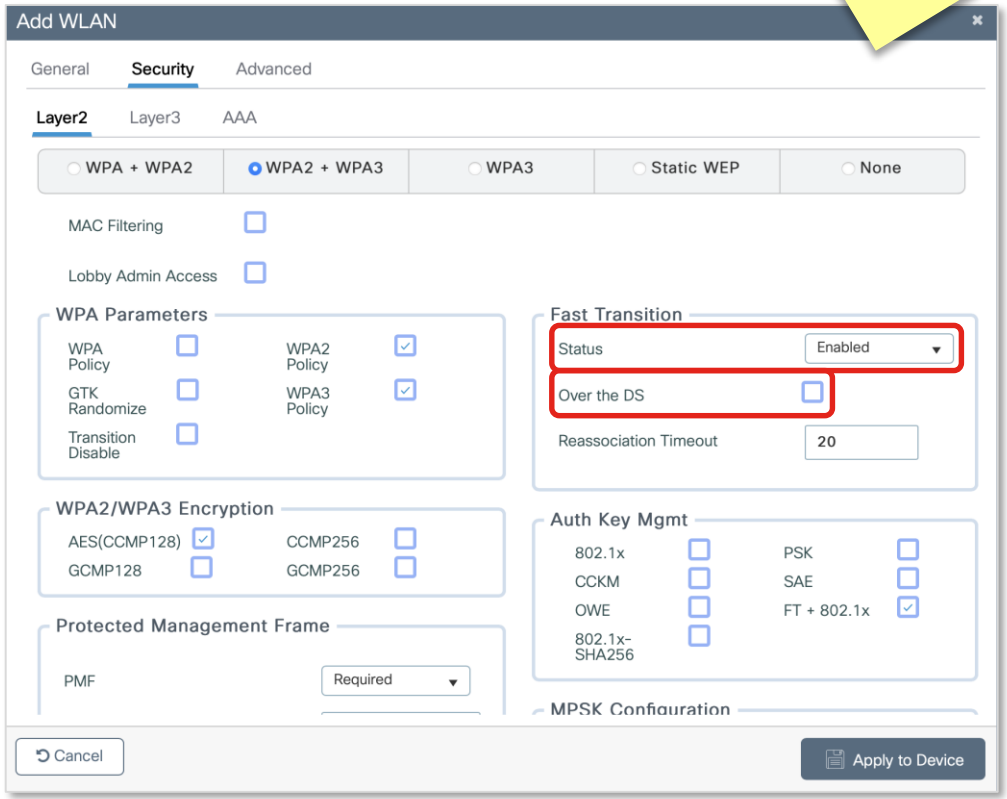
Over the DS



Over the Air

802.11r Fast Transition

- Over the Air is recommended for best client interoperability



Secure Fast Roaming

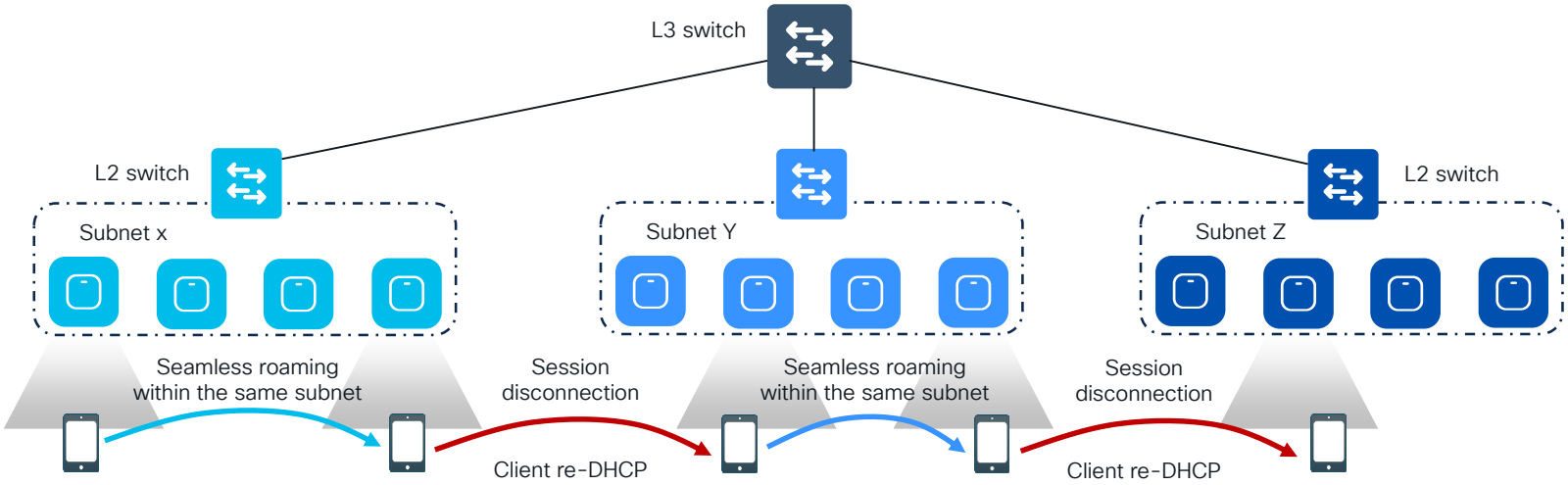
802.11k/v/r and Wi-Fi Agile Multiband

From MR 30

Seamless Roaming at Scale

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

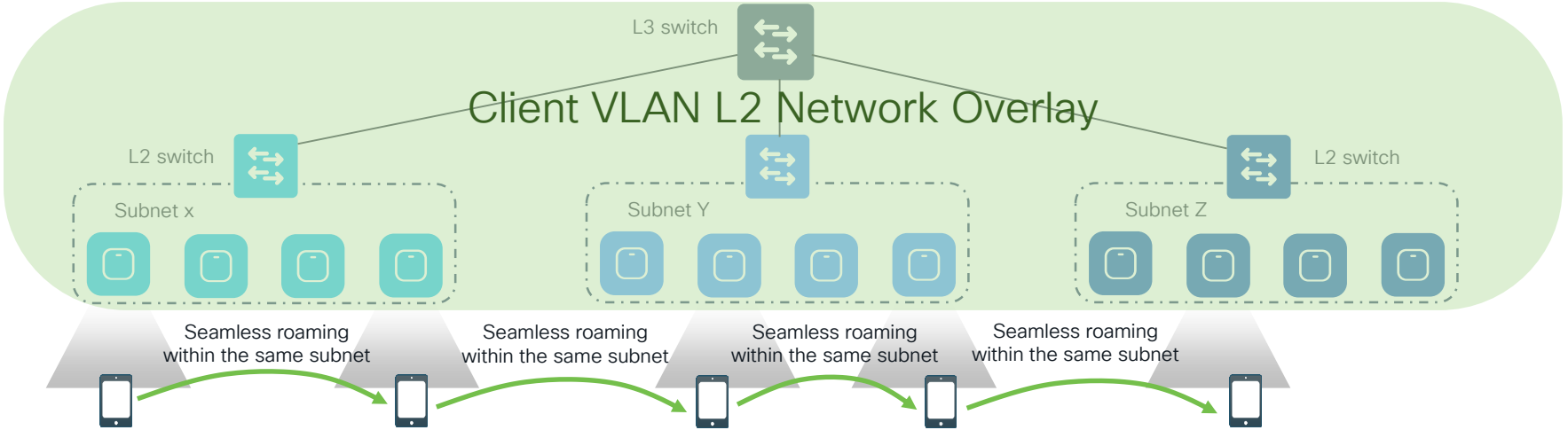
Large broadcast domains do not scale and is counter to networking best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

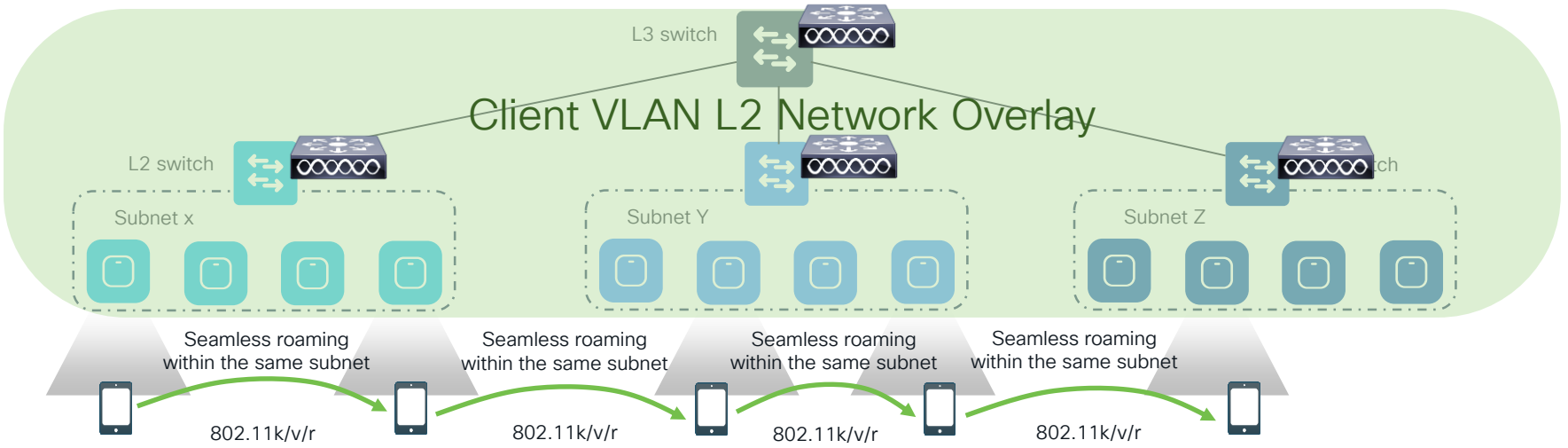
A data termination point is required to roam across L3 boundaries



Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

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



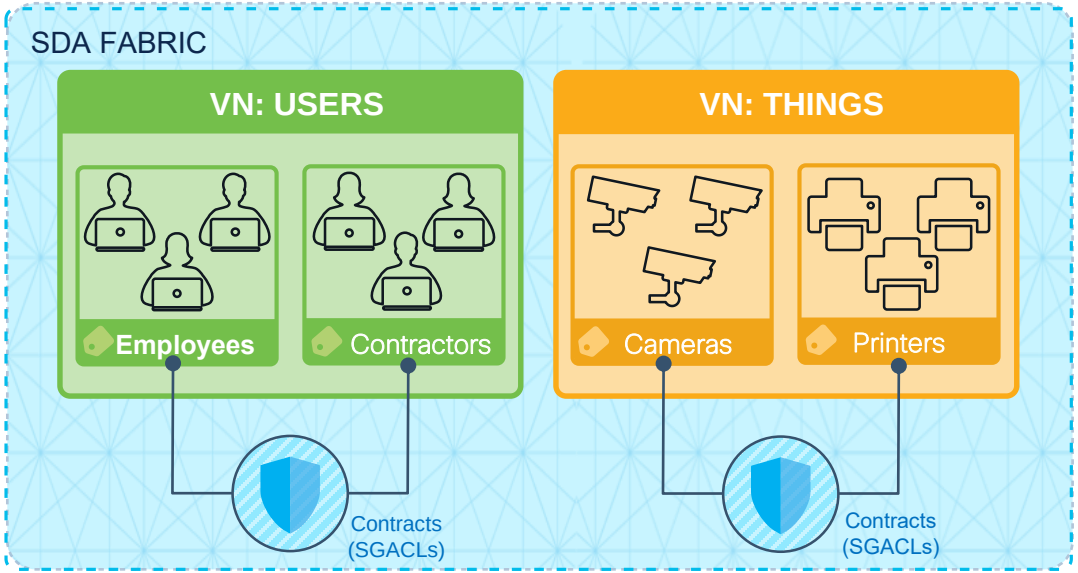
SD-Access at Scale with Fabric

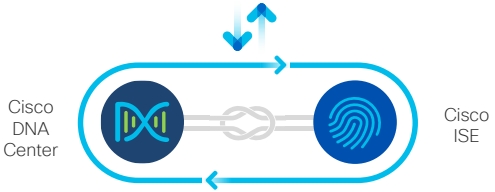
Consistent Segmentation and Network Automation

FYI

Use cases

- Network segmentation with ‘Virtual Networks’
- Group segmentation with ‘Scalable Groups’
- Fabric-Native Wireless



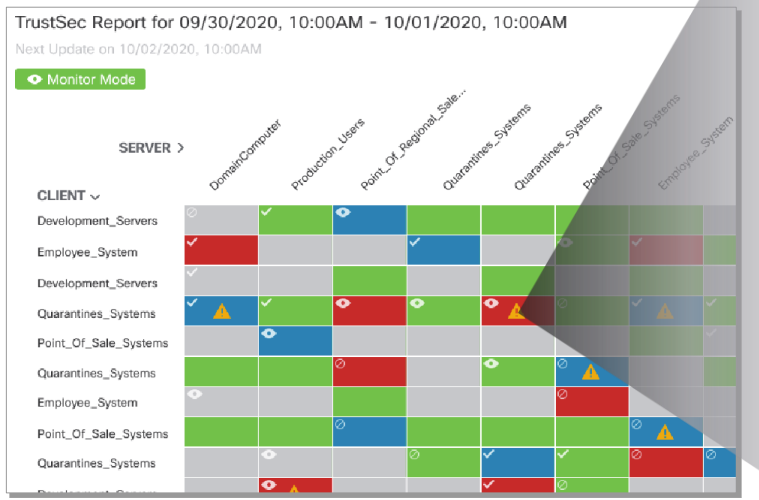


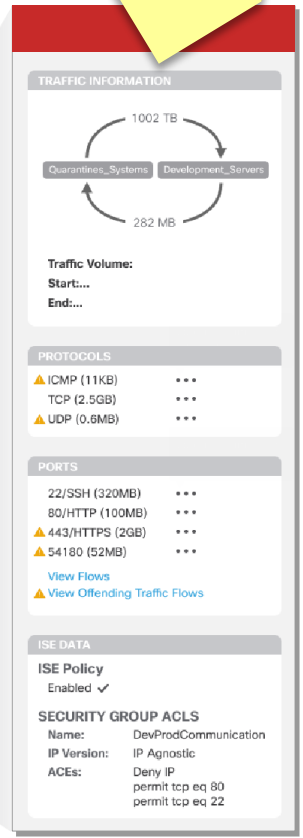
Adaptive Policy & Secure Analytics

Informed Policy Creation and Validation

Global flow **visibility** and **context**

Group based policy and traffic **flow tracking**





Key Reinstallation Attack

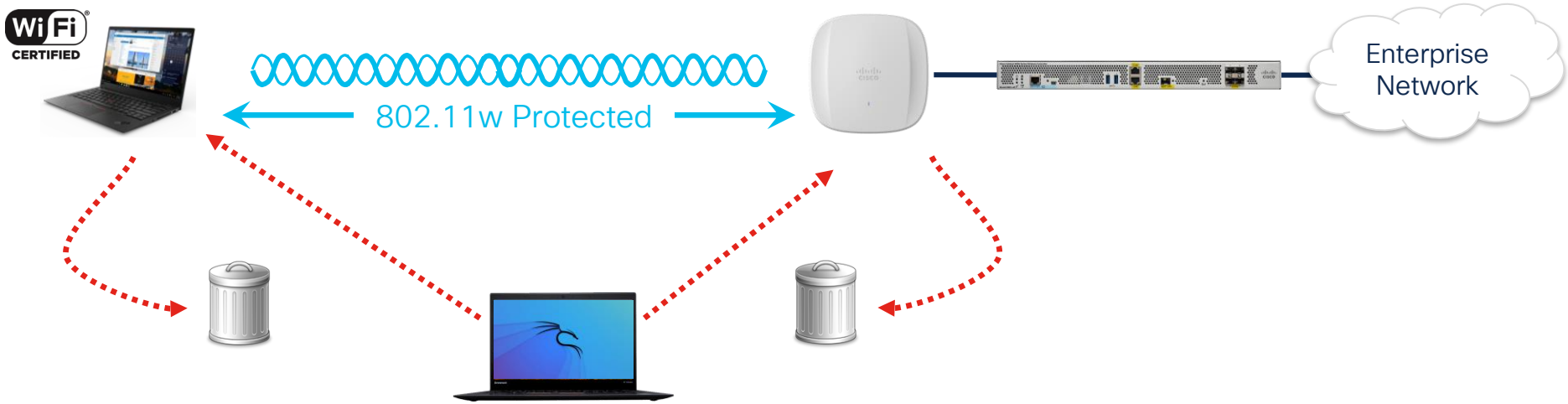
- 10 Vulnerabilities were discovered
  - May allow the reinstallation of keys already in use
- Only 1 impacts Access Points
  - Specific to 802.11r (Fast BSS Transition)
  - CVE-2017-13082

- 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



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

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

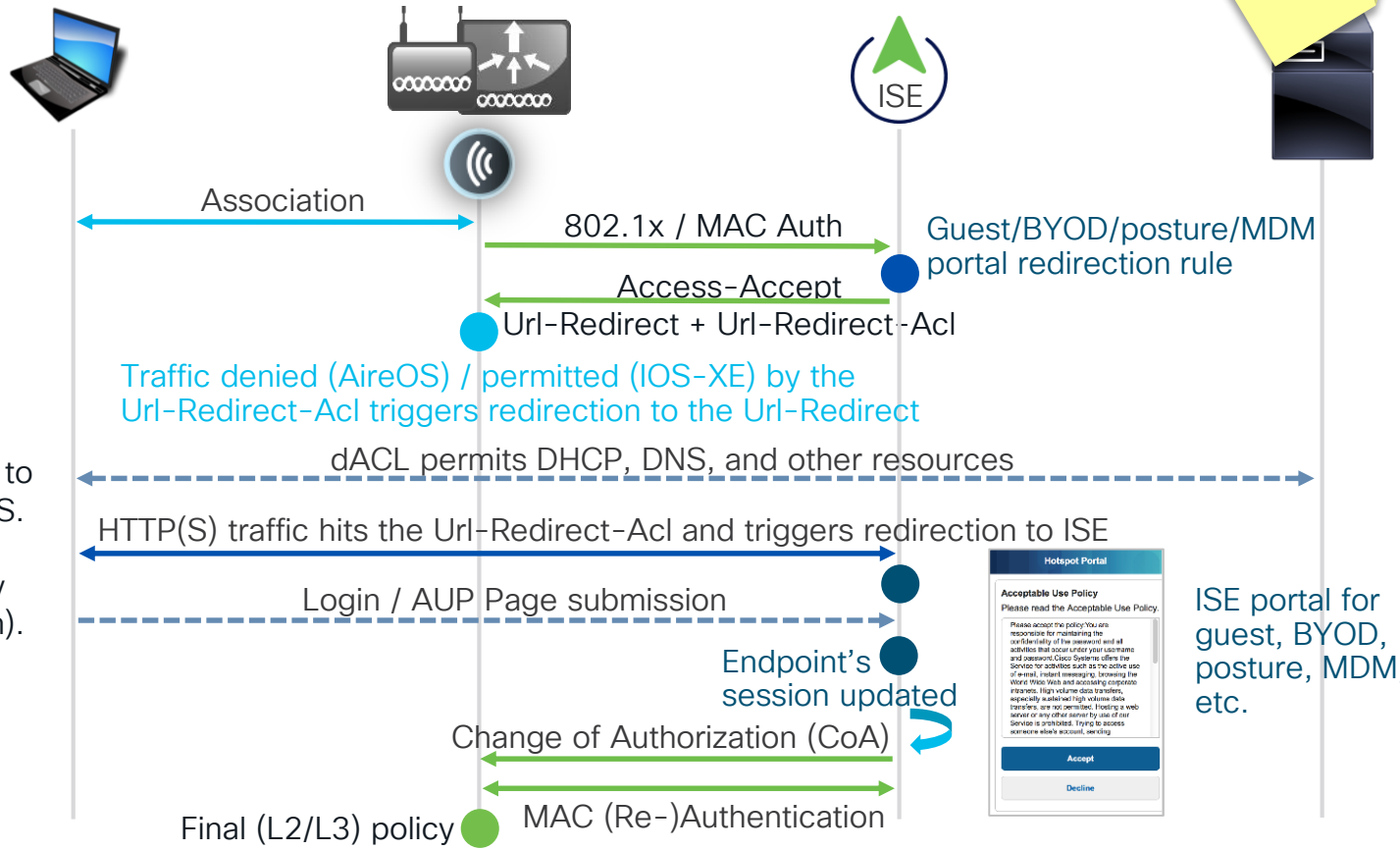
RADIUS CoA Request

RADIUS CoA ACK

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

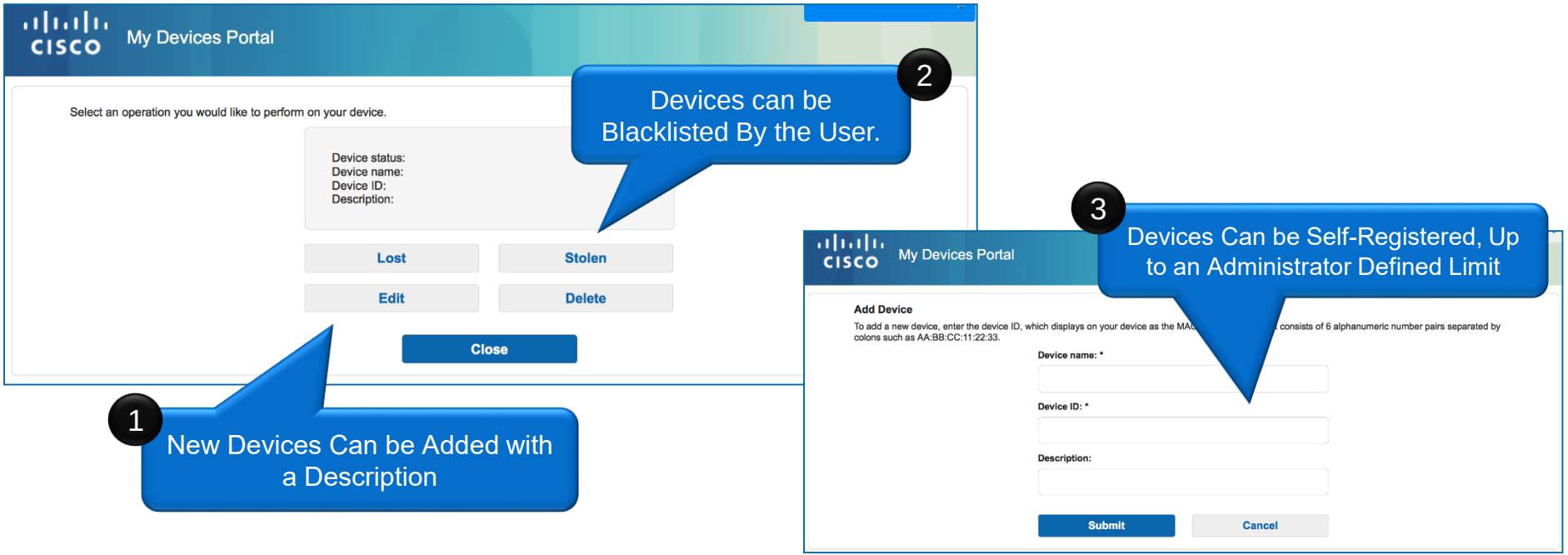
Central Web Authentication



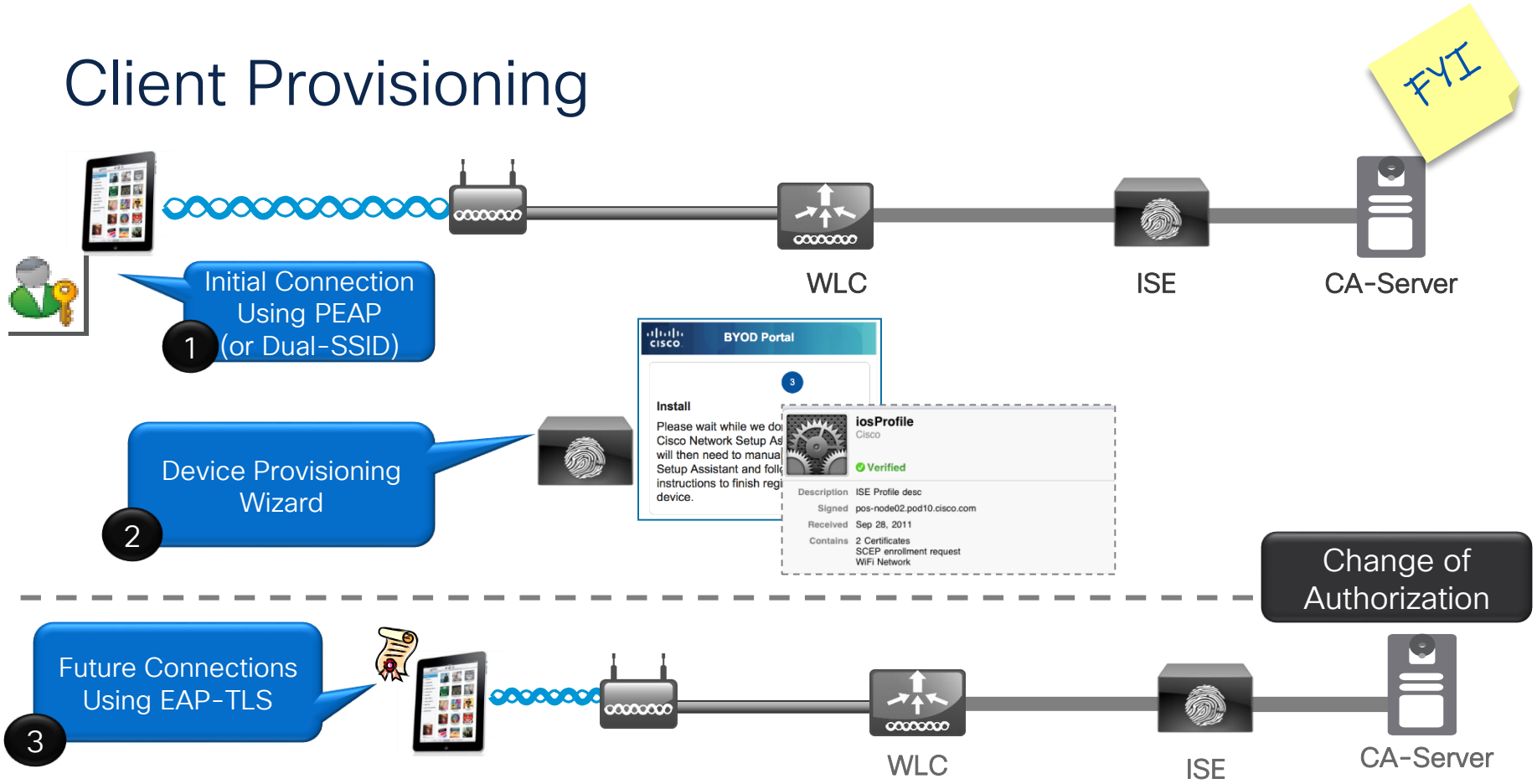
CENTRAL because the redirection URL, the pre-webauth ACL are **centrally** configured on ISE and dynamically communicated to the WLC (NAD*) via RADIUS. CWA is partially L2 (MAC Authentication) and partially L3 (redirect on IP resolution).

*Network Access Device

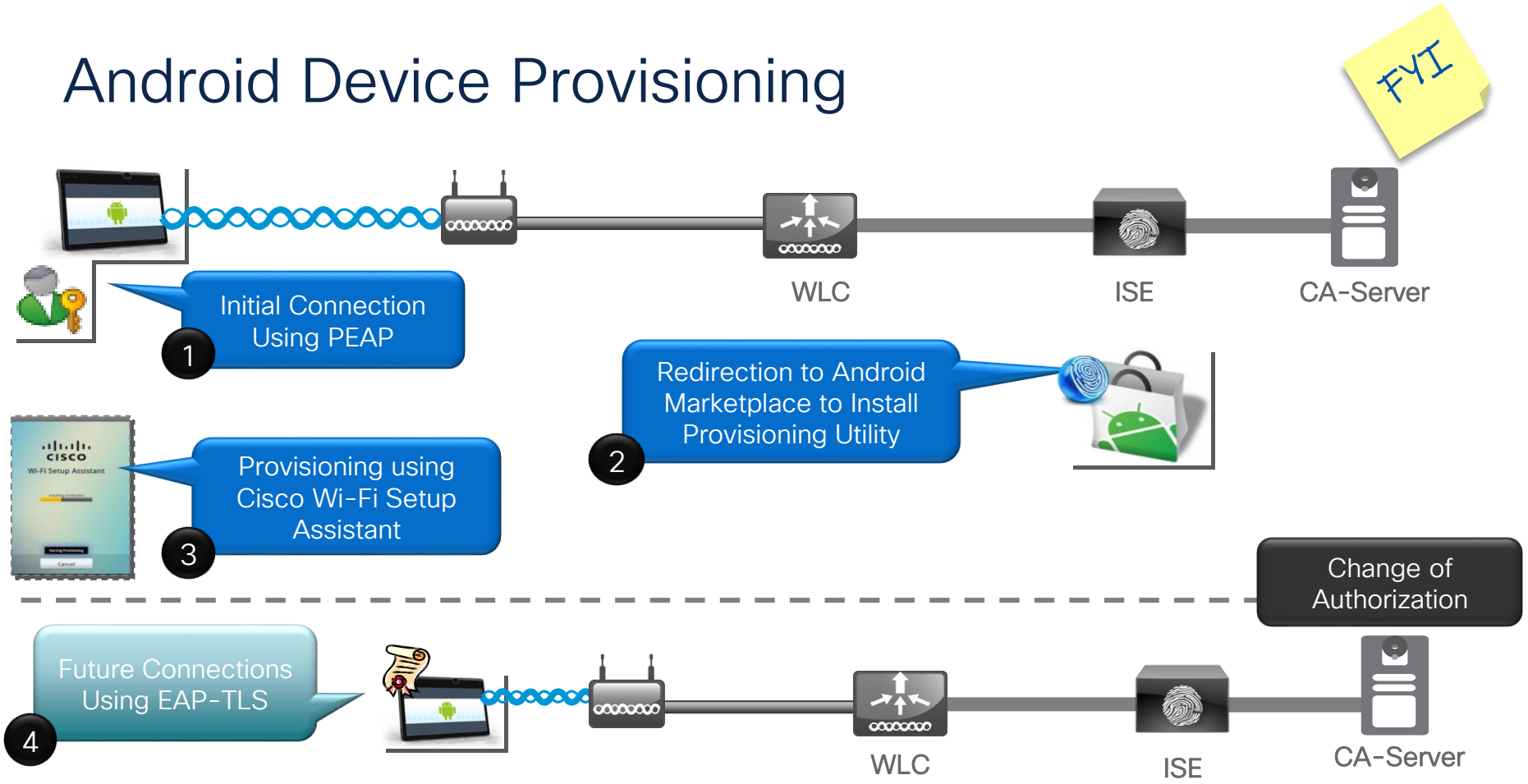
Self-Registration of BYOD Devices



Client Provisioning



Android Device Provisioning



Client Provisioning Policy

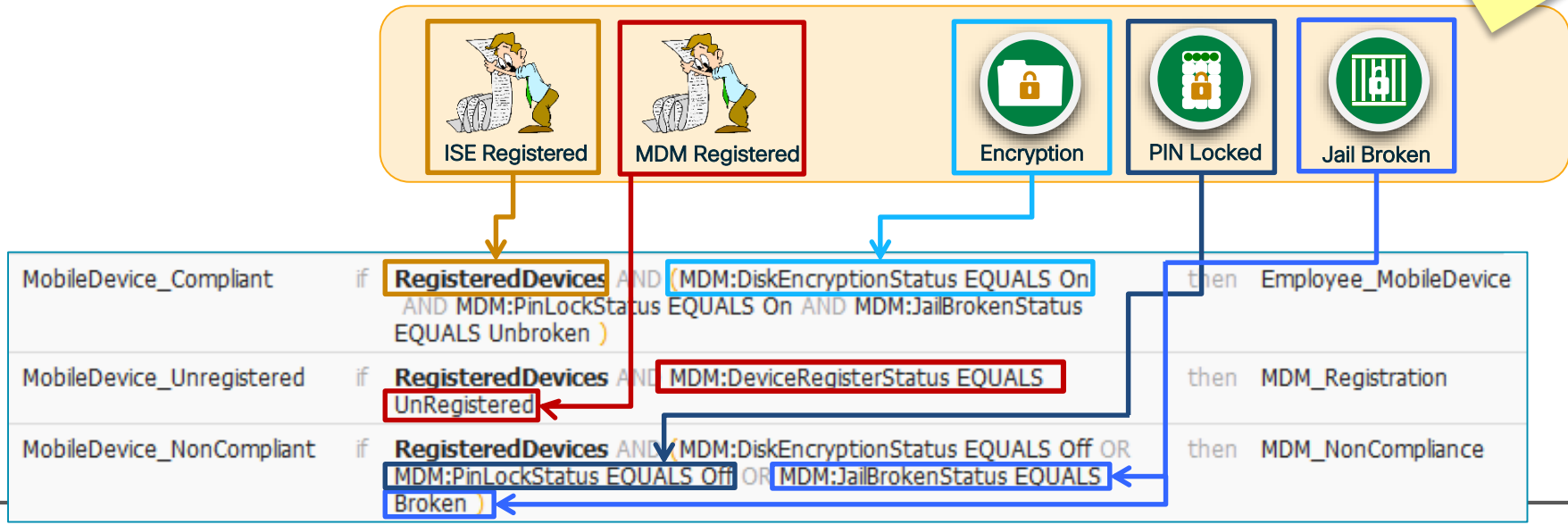
FYI

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

Central Web Authentication

MAC Authentication Bypass

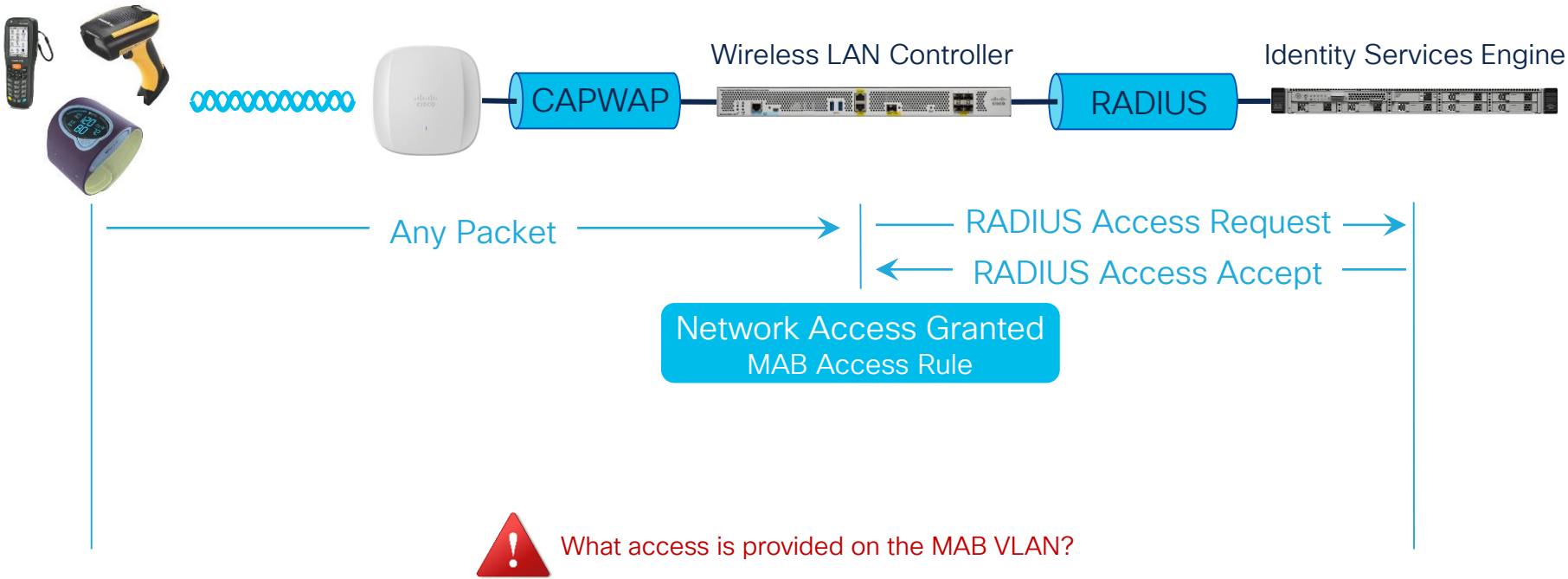
Any Packet

RADIUS Access Request

RADIUS Access Accept

Network Access Granted
MAB Access Rule

MAC Authentication Bypass



Wi-Fi Certified Easy Connect

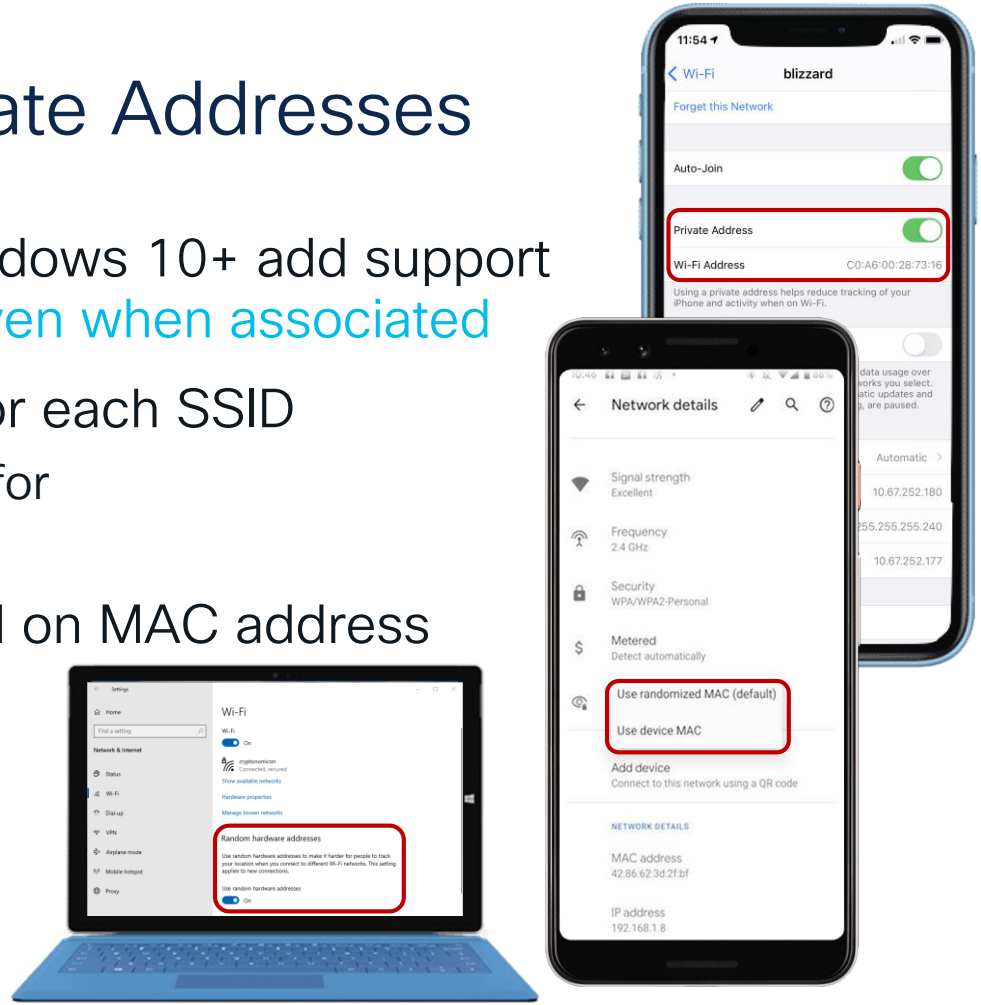
WPA3

Device Provisioning Protocol (DPP)

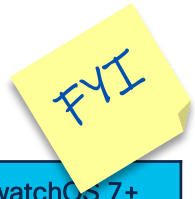
- 3 Phases
  - Bootstrapping
    - Obtains the public key of new device
  - Authentication and Provisioning
    - Public key is used to create a secure tunnel for credential exchange
  - Network Access
    - PMK derived
    - Four-Way Handshake used as normal
    - Supports Protected Management Frames

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
  - Network troubleshooting
  - Location analytics



Detailed implementation

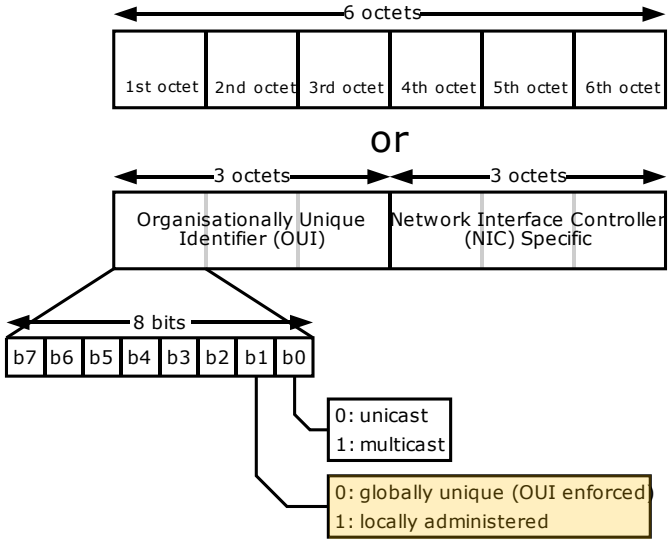


	Windows 10+	Android 10+	iOS 14+, iPadOS 14+, watchOS 7+
Randomization enabled by default	No	Yes	Yes
Same random MAC used for subsequent connection	Yes	Yes	Yes
Randomization saved between device reboot	Yes	Yes	Yes
Random MAC saved when Wi-Fi profile recreated	No	Yes	Yes
Randomization per day and/or per 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



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

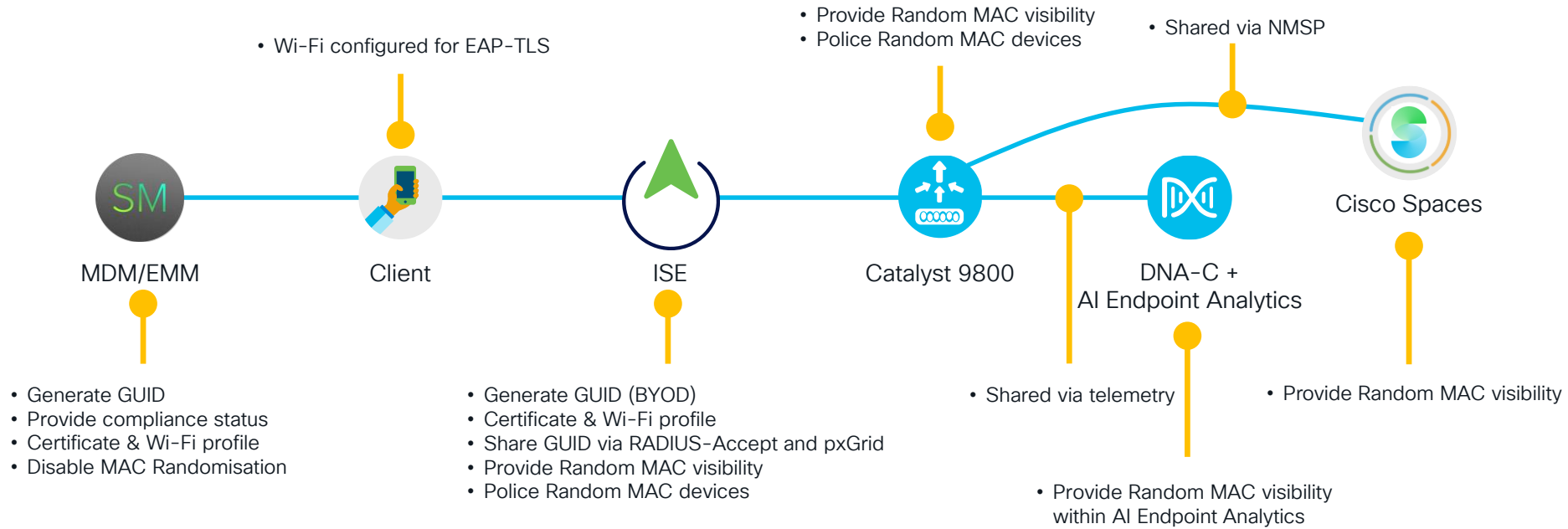
56-EF-68-F6-0D-30

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

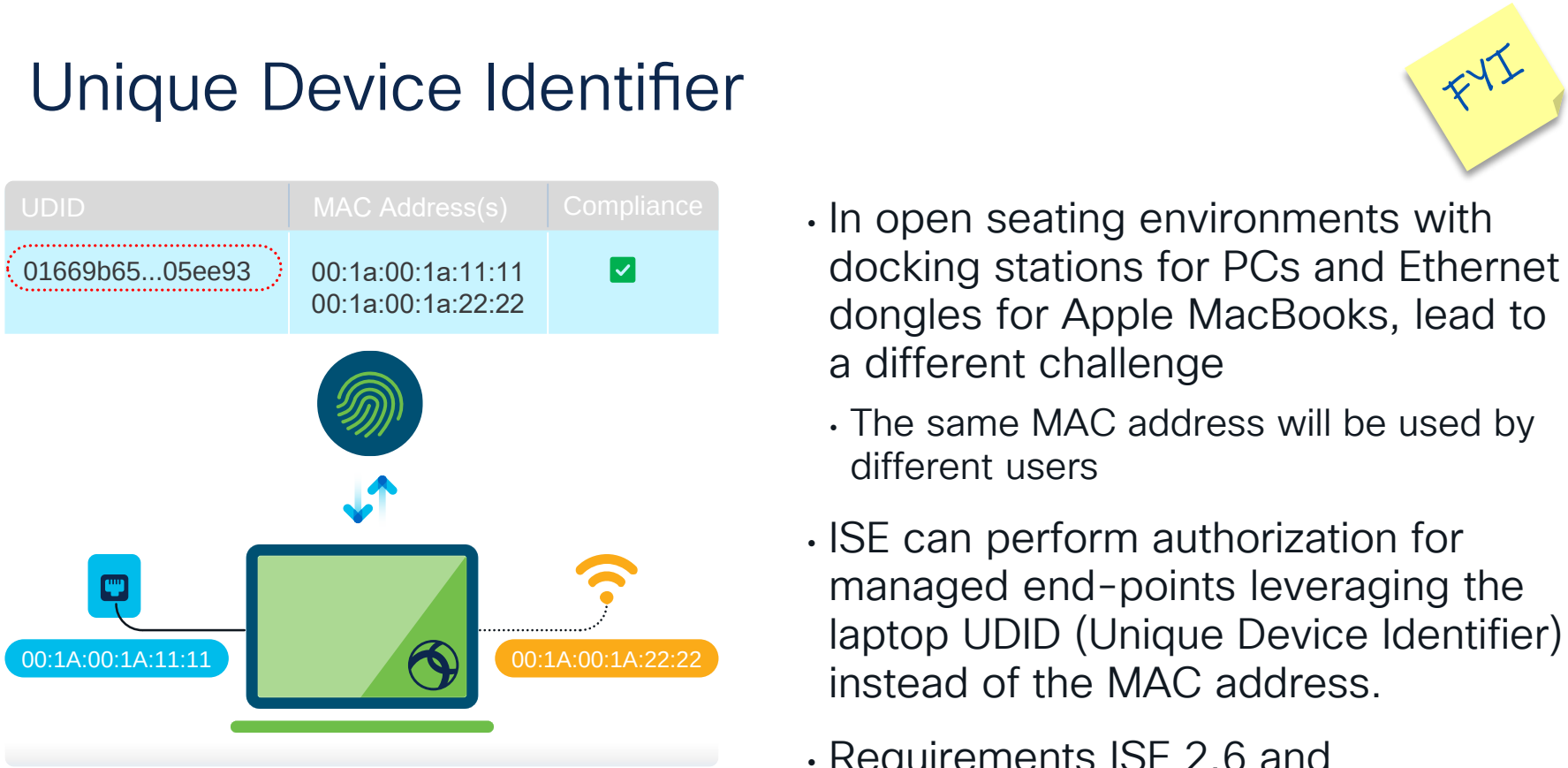
AE-83-37-55-A7-22

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

Addressing Random MAC Issues

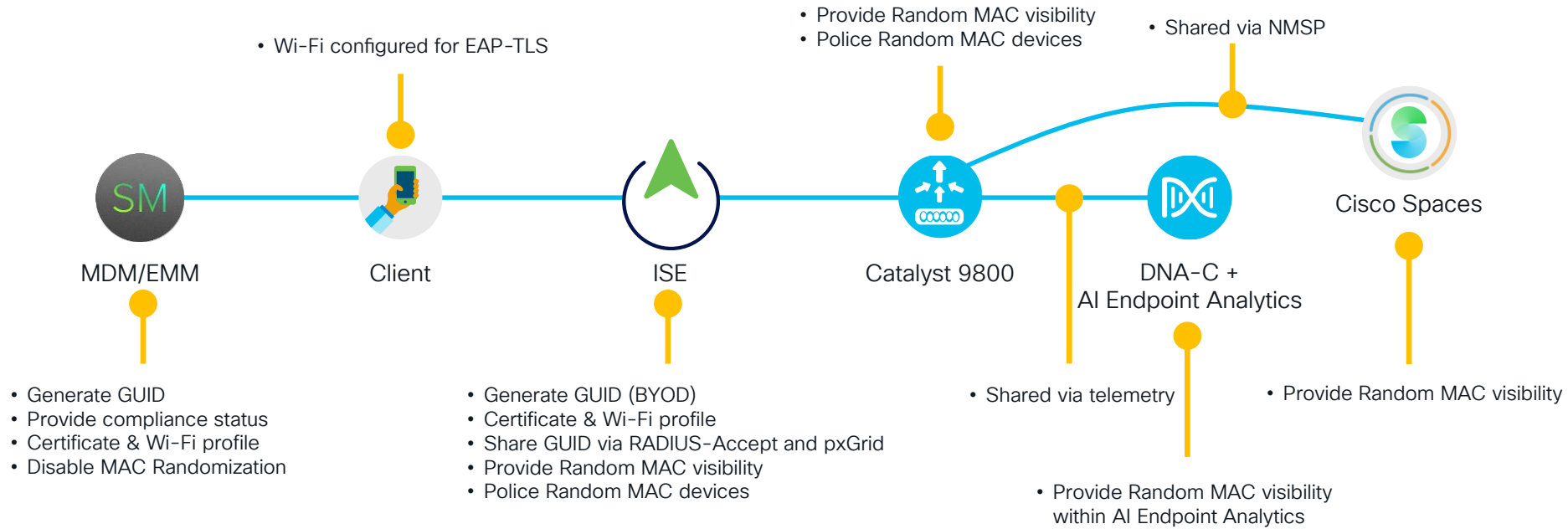


Unique Device Identifier



- 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 and AnyConnect 4.7

Globally Unique Identifier



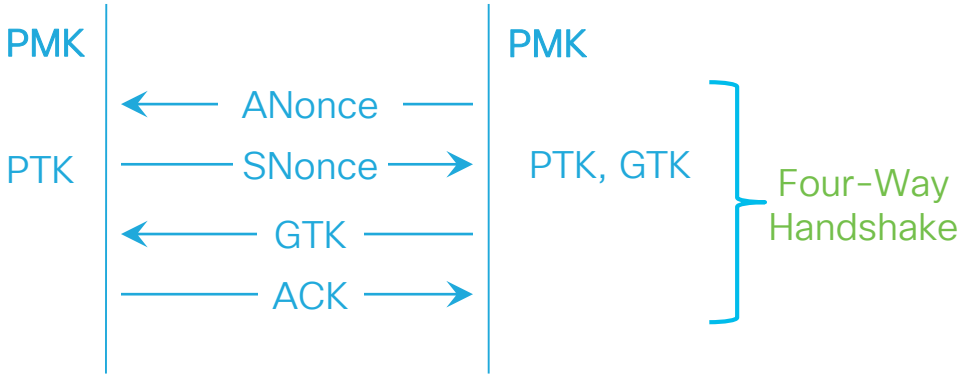
WPA Personal

Pre-Shared Key

WPA Personal

Pre-Shared Key

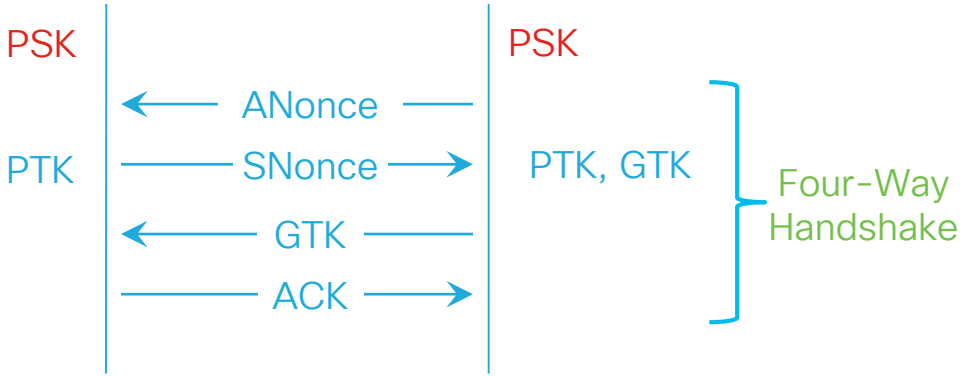
- Offline Attacks
  - Dictionary
  - Rainbow Table
- Strong Passwords Matter



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

WPA Personal

Pre-Shared Key



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

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

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
    - Transition Disable will prevent WPA3-Personal clients from downgrading to WPA2-Personal on roams mitigating downgrade attacks

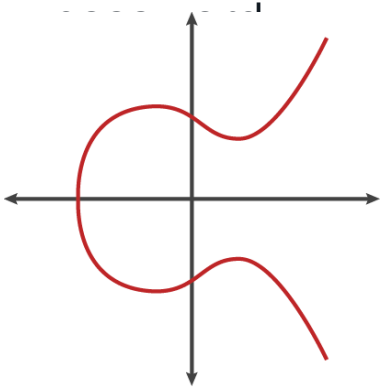
Dragonblood

- 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

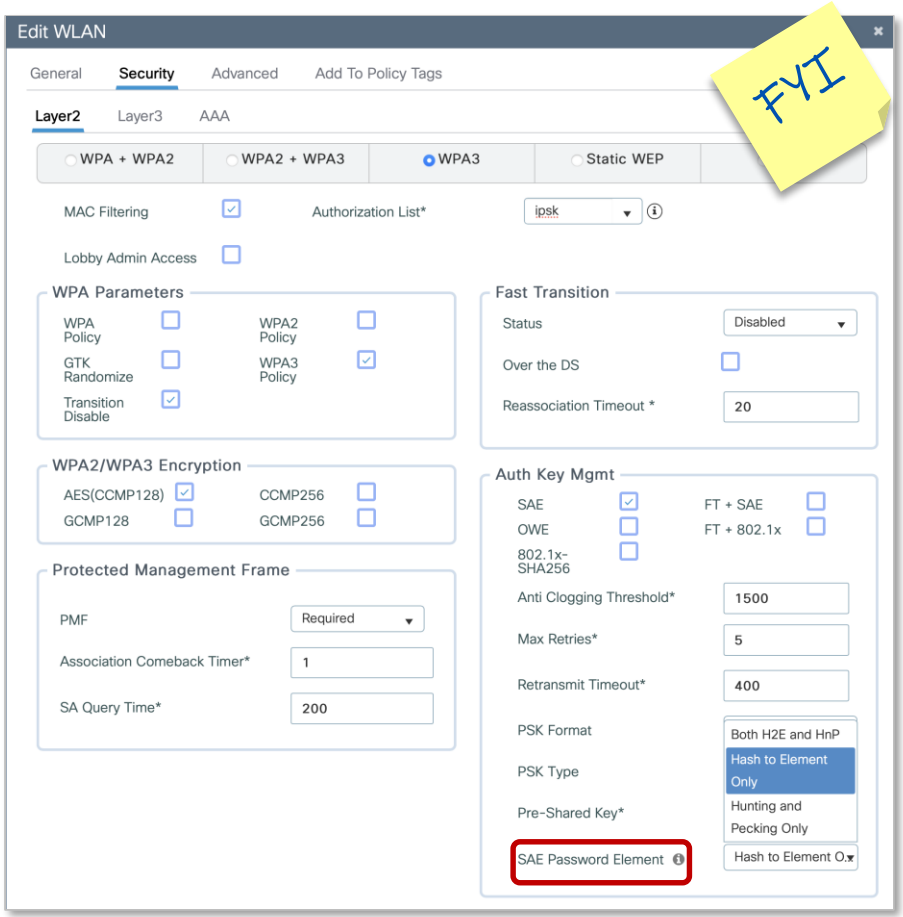
Dragonblood: Analysing WPA3's Dragonfly Handshake

Dragonblood

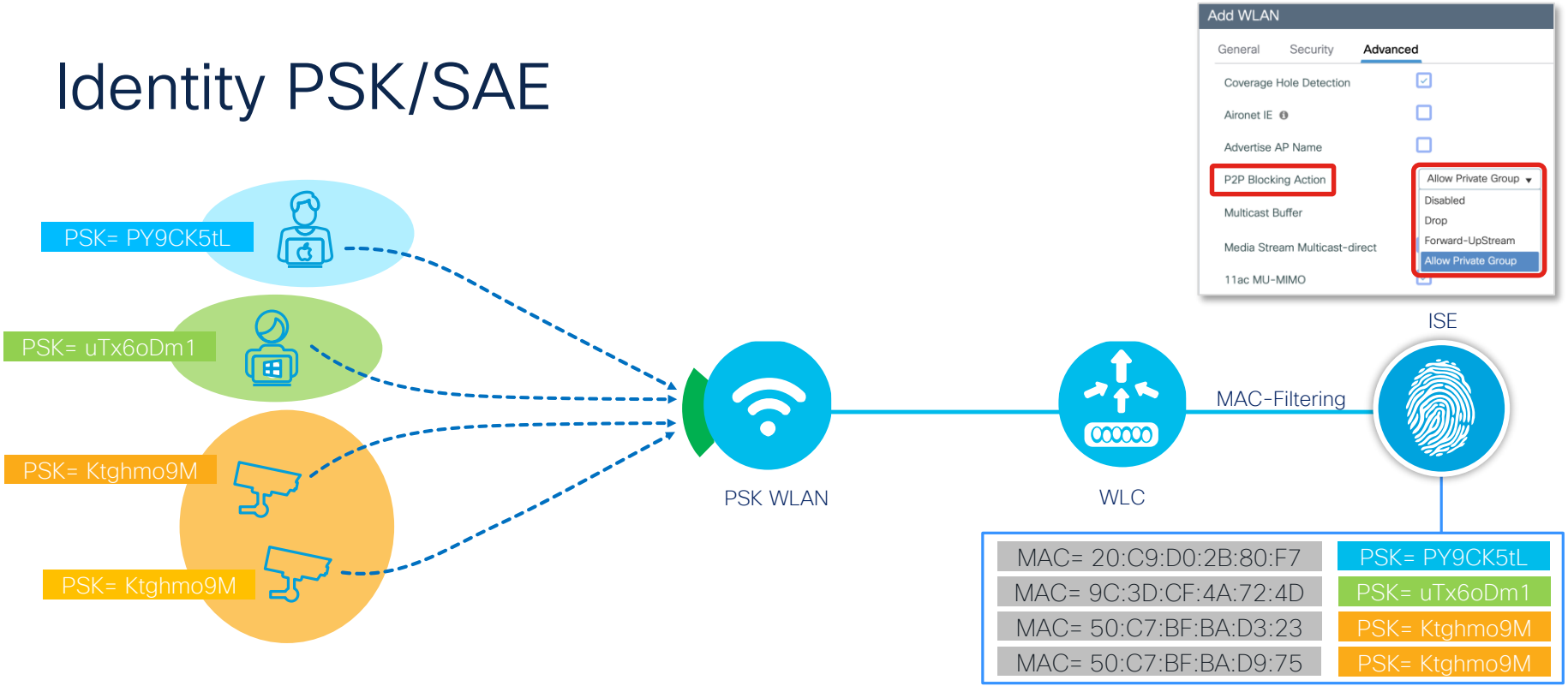
- Timing-Based Side-Channel Attacks
  - The time it takes an AP to respond to commit frames may leak information about the



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

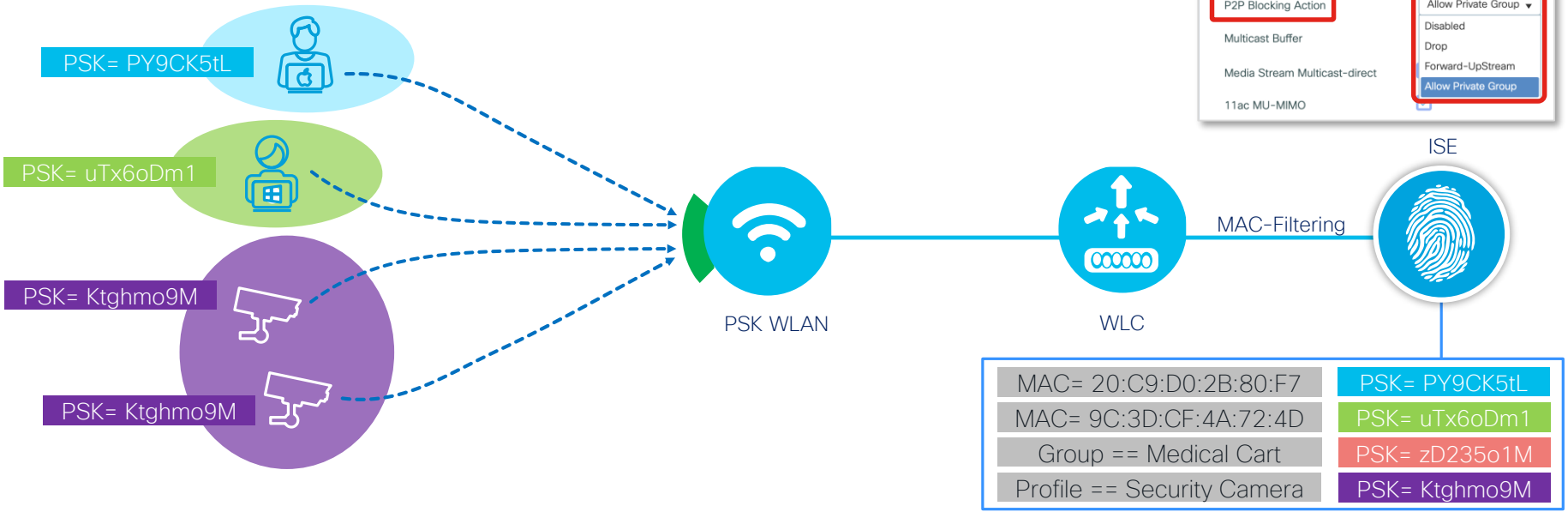


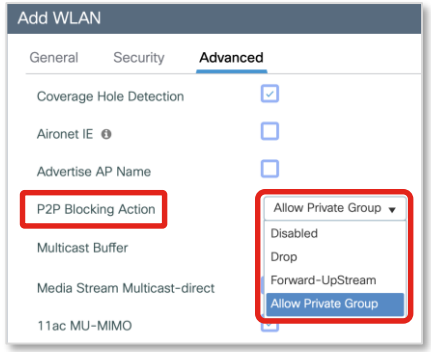
Identity PSK/SAE



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

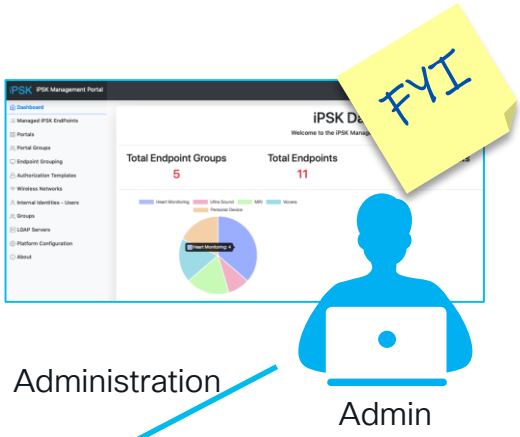
Identity PSK/SAE

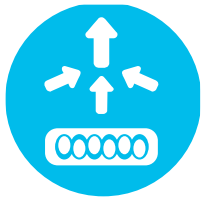




https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

iPSK Manager





WLC / AP

RADIUS

CoA

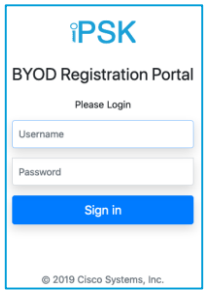
ISE

SQL

API

iPSK Manager
- Linux
- Apache
- MySQL
- PHP

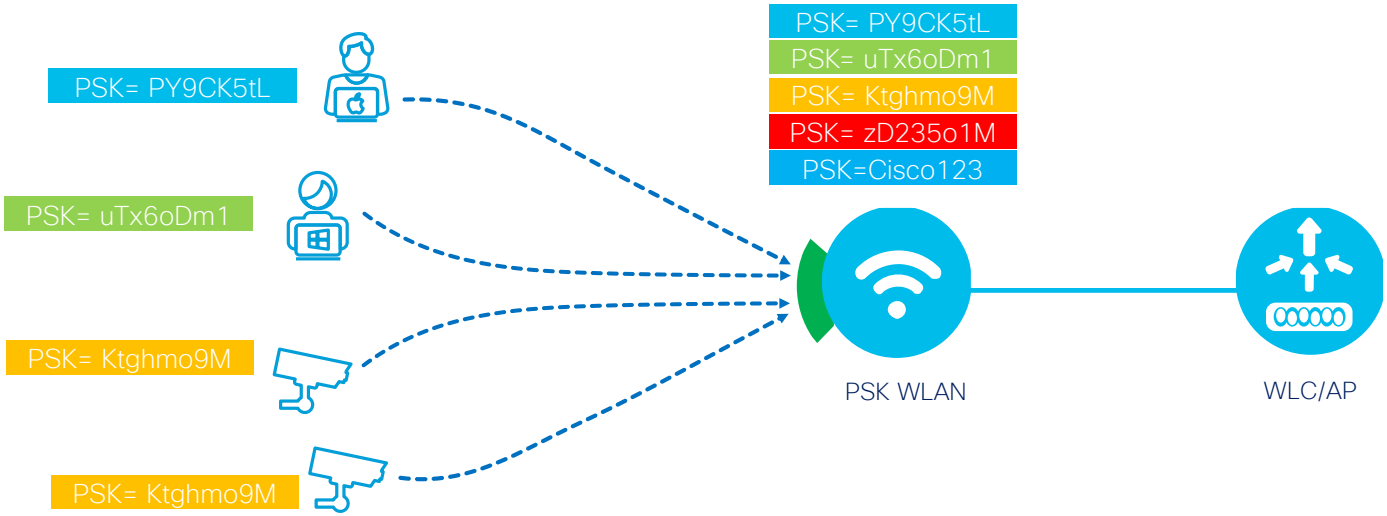
iPSK Lifecycle Management



End Users

http://cs.co/iPSK-Manager

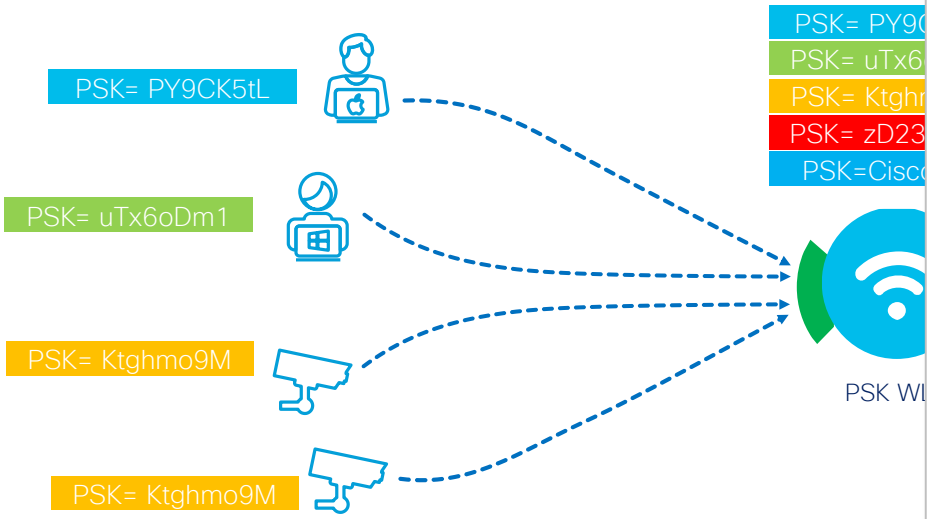
Multi Pre-Shared Key

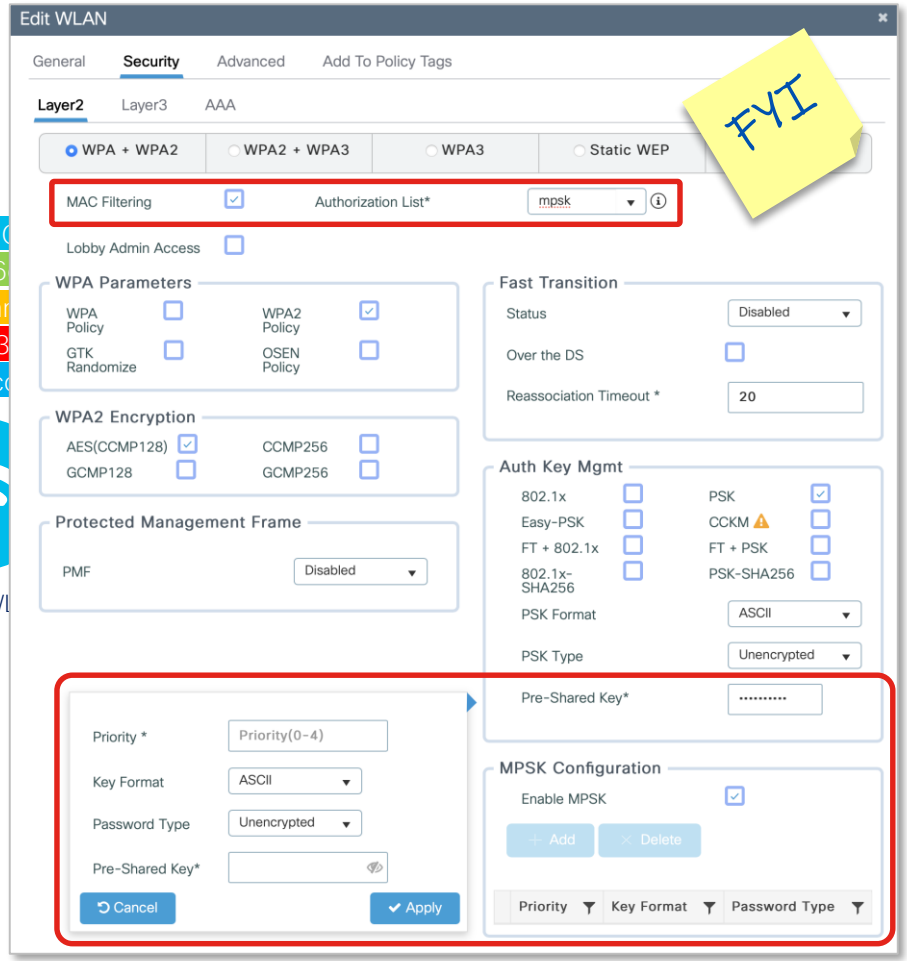


FYI

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

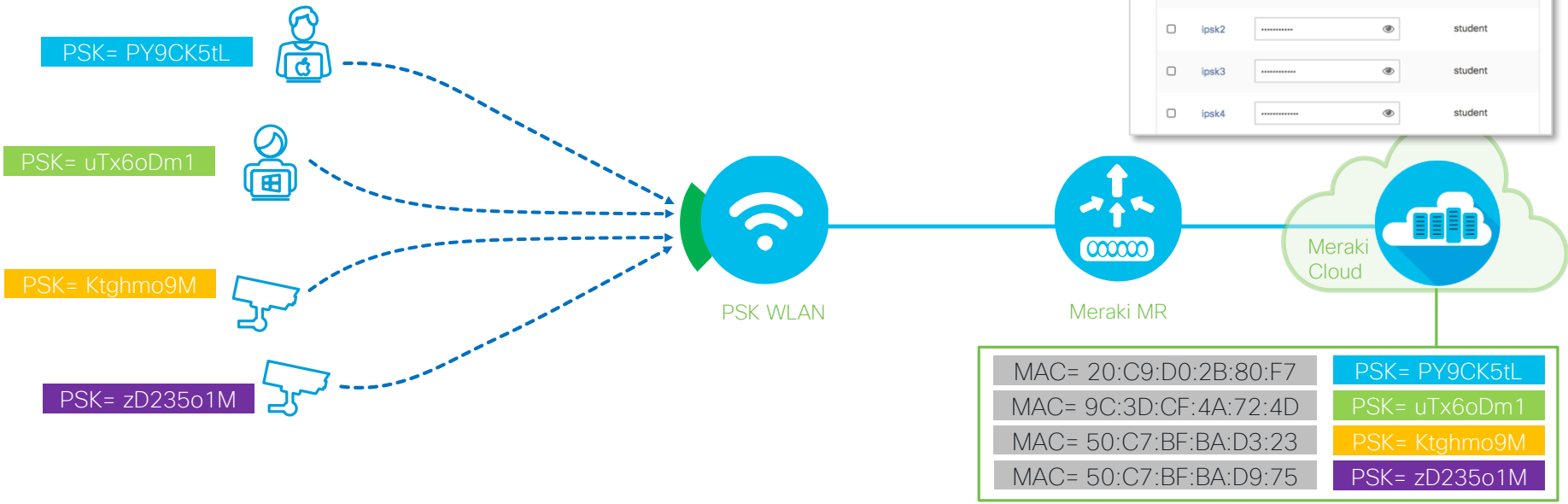
Multi Pre-Shared Key

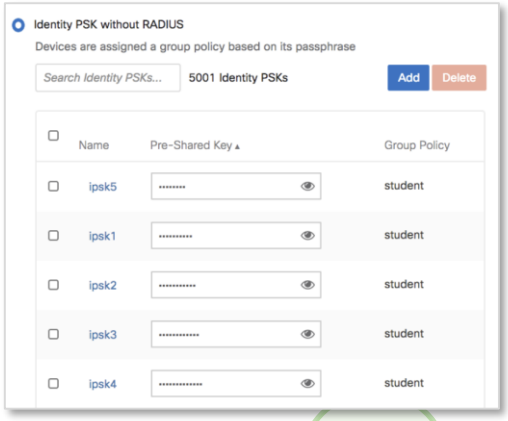




https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/17-2/config-guide/ewc_cg_17_2/multi_preshared_key.pdf

Identity PSK without RADIUS



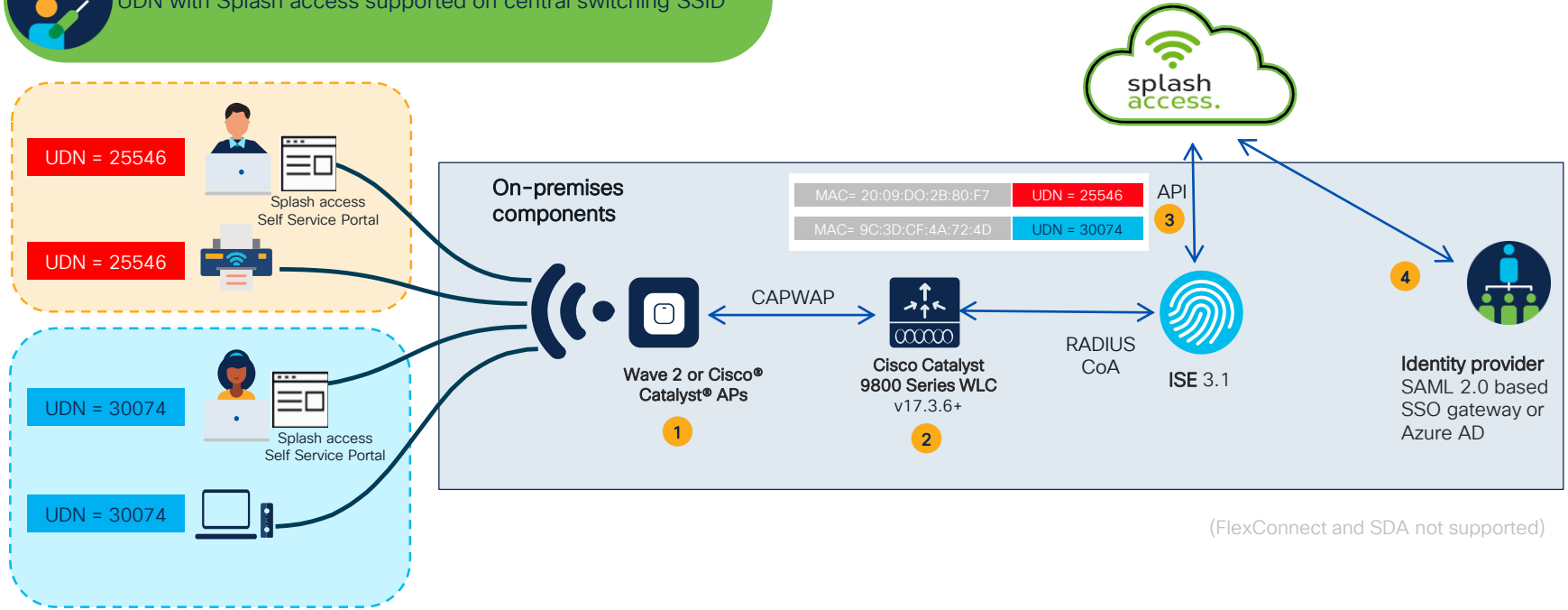


https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_Authentication_without_RADIUS

User Defined Network+

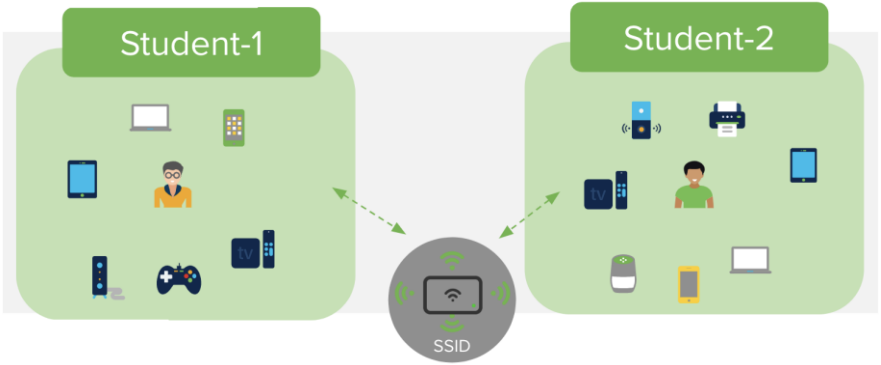
FYI

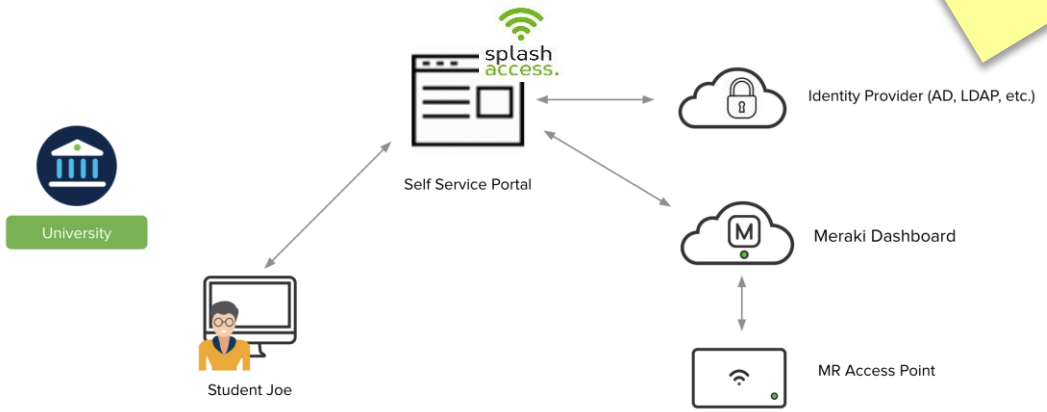
UDN with Splash access supported on central switching SSID



(FlexConnect and SDA not supported)

Wi-Fi Personal Network





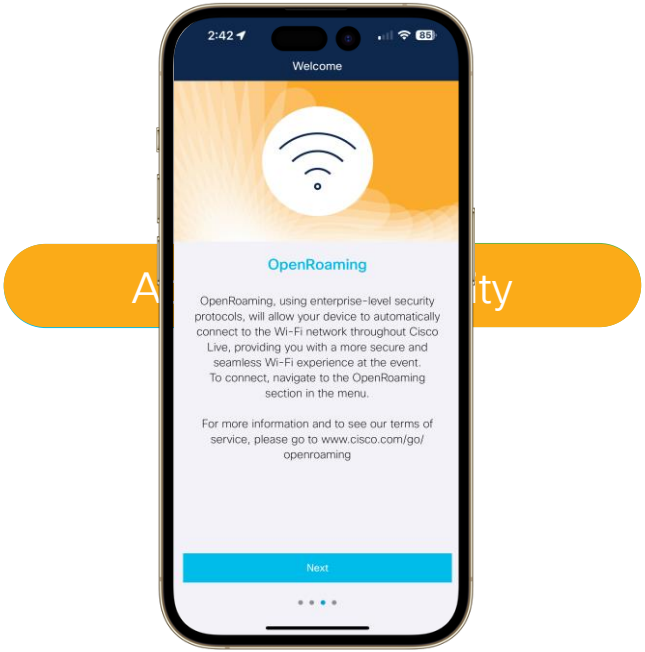
https://documentation.meraki.com/MR/Encryption_and_Authentication/Wi-Fi_Personal_Network_(WPN)

Wi-Fi Certified Enhanced Open

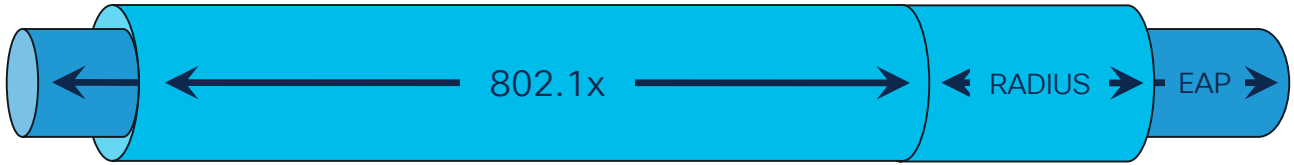
WPA3

- 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



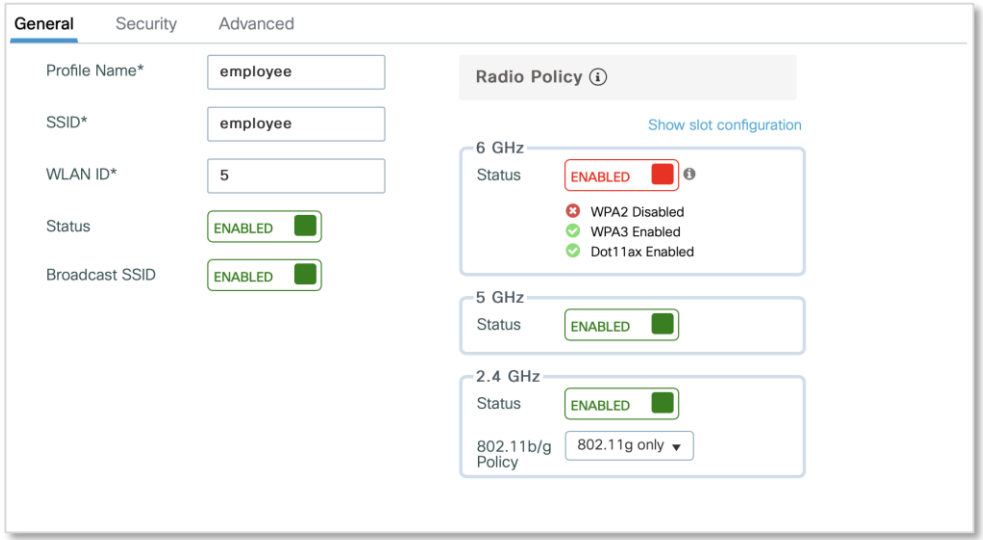
OpenRoaming



Security Implications of 6GHz

WPA3 and OWE are mandatory for 6GHz

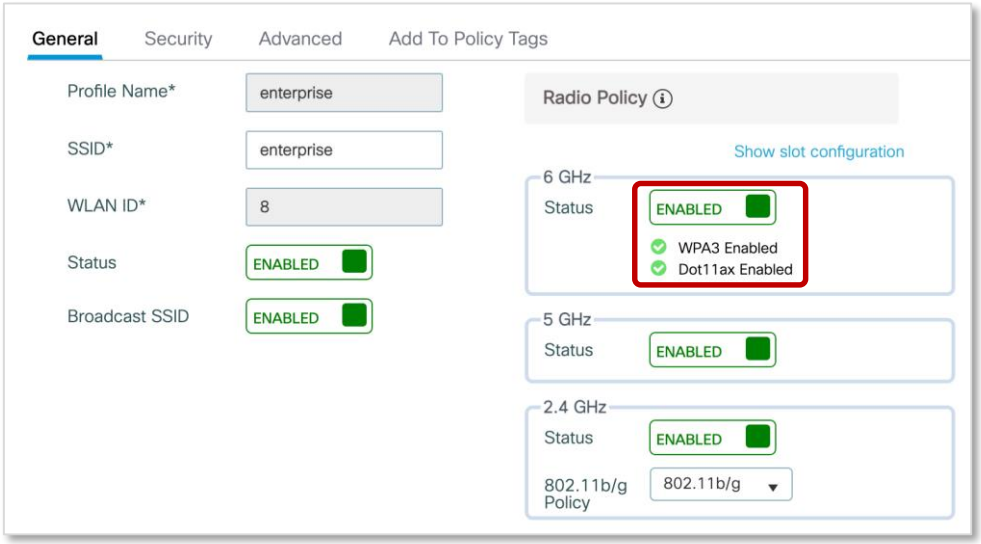
WPA2 and Open are not supported on 6GHz



Security Implications of 6GHz

WPA3 and OWE are mandatory for 6GHz

WPA2 and Open are not supported on 6GHz

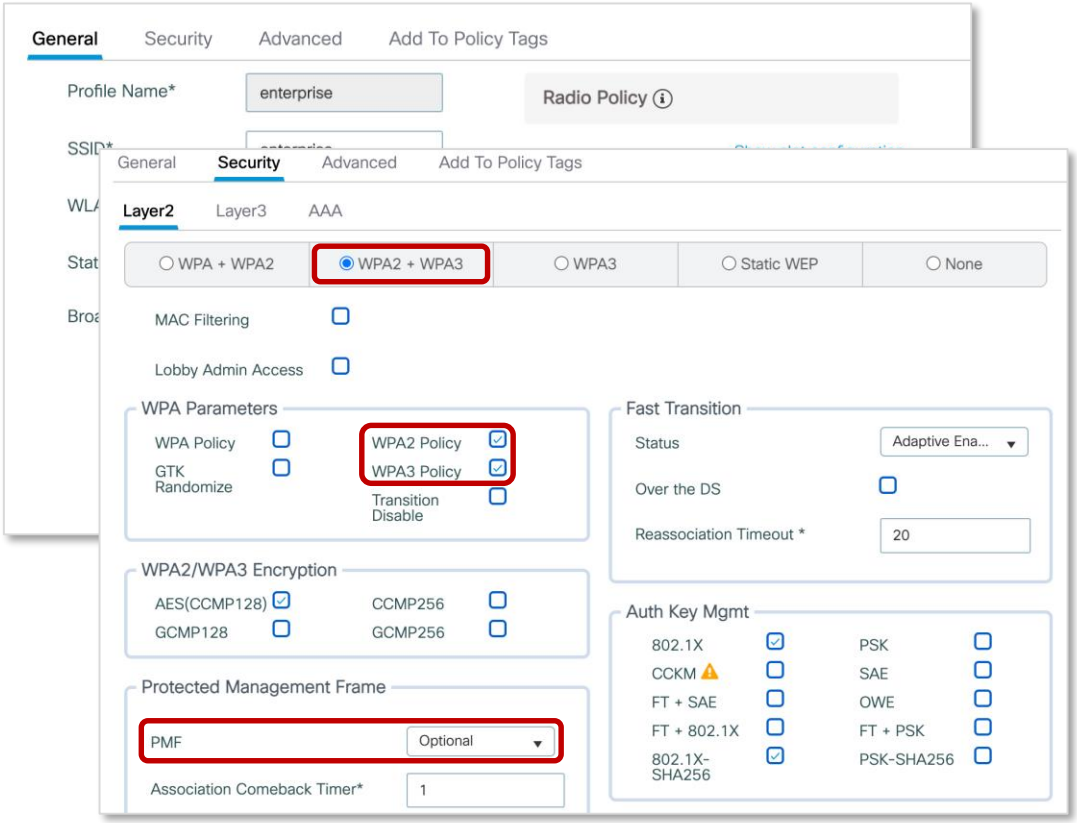


From IOS-XE 17.12.1

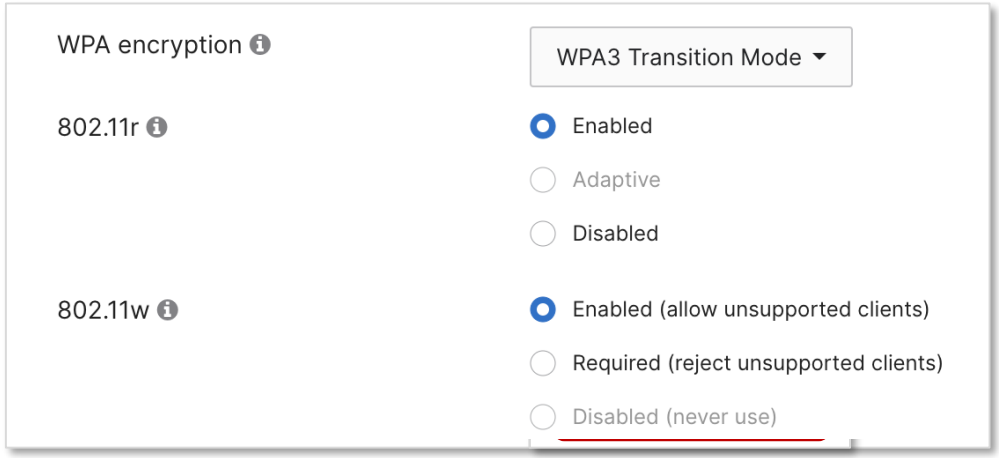
Security Implications of 6GHz

WPA3 and OWE are mandatory for 6GHz

WPA2 and Open are not supported on 6GHz



Security Implications of 6GHz



WPA3 and OWE are mandatory for 6GHz

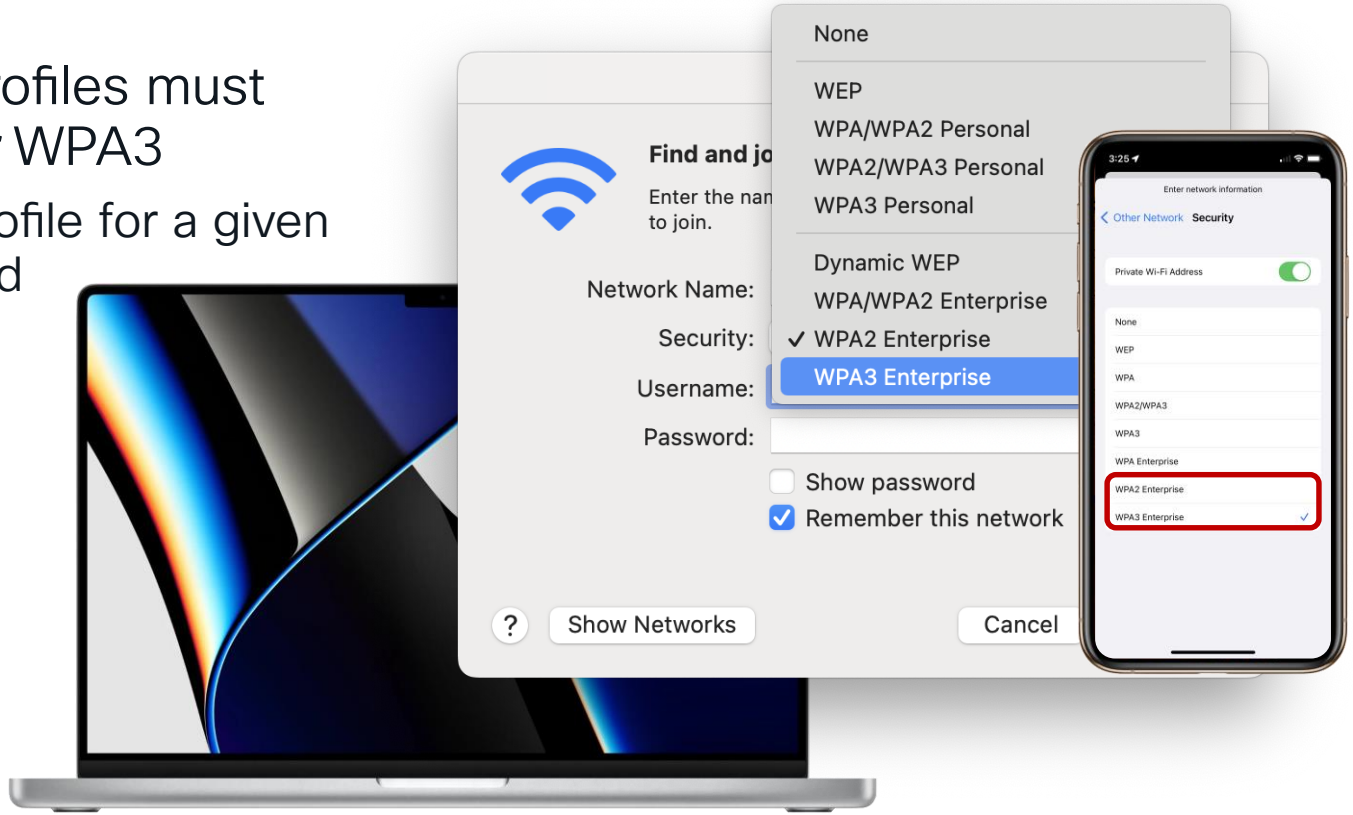
WPA2 and Open are not supported on 6GHz

From MR 31.X

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

Wi-Fi 6E and Wi-Fi 7 Client Security

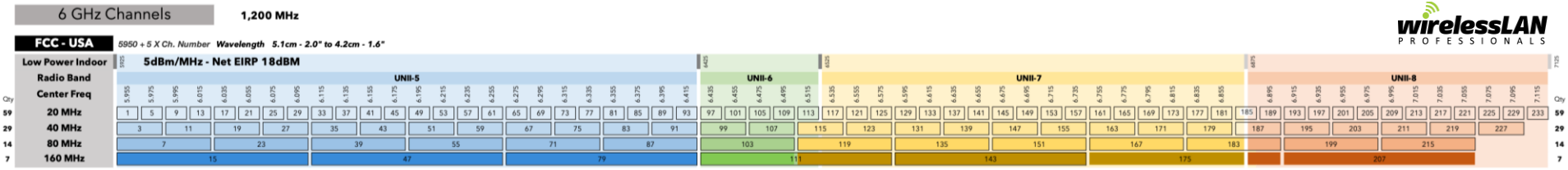
- Client device profiles must select WPA2 ***or*** WPA3
  - And only one profile for a given SSID is permitted



AP Discovery Challenges

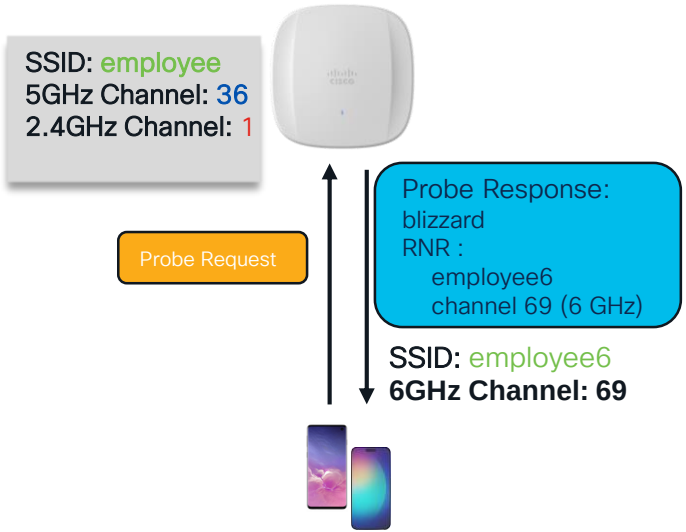
Wi-Fi 6E

- There are a total of 59x 20MHz channels in the 6GHz band
- Wi-Fi clients can only send Probe Requests on 20MHz channels
- It would take 6 seconds to passively scan all 59 channels



Reduced Neighbour Report (RNR)

Wi-Fi 6E



- Co-Located 6GHz radio information in beacon and probe response from the 2.4GHz and 5GHz radios
- Target Beacon Transmission Time (TBTT) points client to watch for beacon with additional information
- Most clients will only use RNR and will not start scanning 6GHz unless discovered through legacy bands

Fast Initial Link Setup (FILS)

Wi-Fi 6E

- AP broadcast beacon transmitted every 100ms with detailed WLAN metadata
- Smaller beacons transmitted every 20ms
  - Contains information the client can use to decide which AP to join
    - Short SSID name
    - Channel
    - TBTT
- Reduces probe request overhead

- Target Beacon Transmission Time (TBTT) points client to watch for beacon with additional information
- Unclear if clients use FILS to supplement decision making or simply default to using RNR only

Unsolicited Broadcast Probe Response (UBPR)

Wi-Fi 6E

- Broadcast probe response transmitted every 20ms
- Contains detailed information as in the beacon
- Carries multiple BSSIDs
- Reduces rrobe request overhead

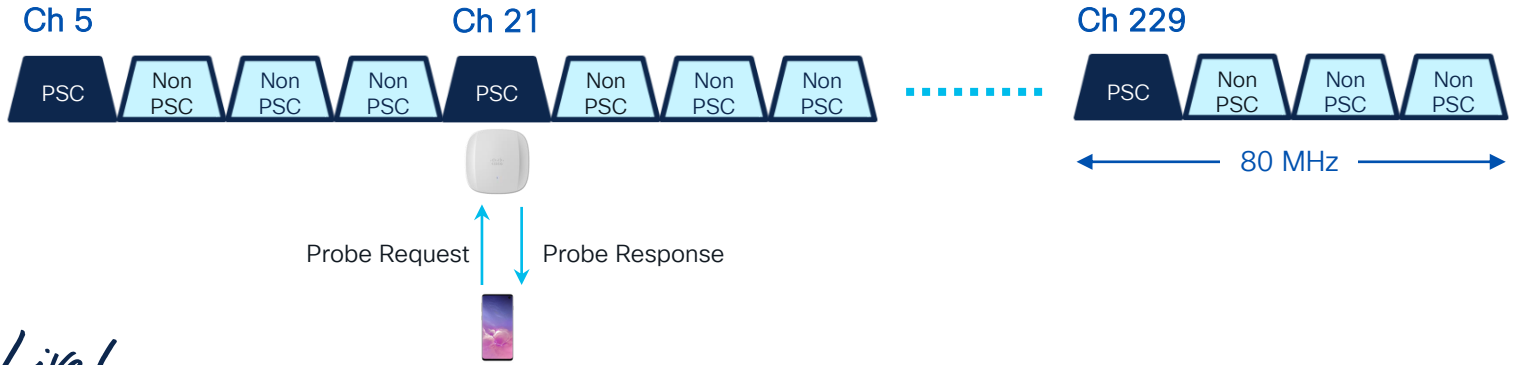
- UBPR is not as widely adopted as FILS
- FILS and UBPR are mutually exclusive

Probe Restrictions in 6GHz

Wi-Fi 6E

- Clients cannot send blind probe with wildcard SSID/BSSID
- Clients must wait at least the duration of minimum probe delay interval (20ms)
- Probe response is always broadcast

- Preferred Scanning Channels (PSC)
  - Every fourth 20MHz channel designated for active probing
  - PSC channels serve as the primary channel for channel bonding
  - Reduces the number of channels to be scanned from 59 to 15



Wi-Fi 6E AP Discovery Considerations

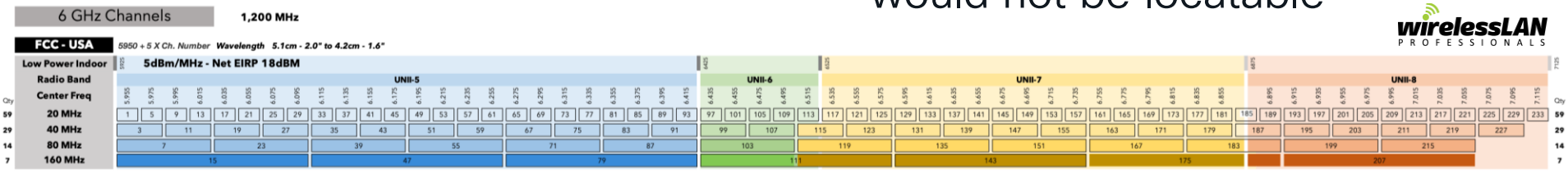
Wi-Fi 6E

- RNR will be the primary means for AP discovery of 6GHz SSIDs
  - Assumes 2.4GHz and/or 5GHz is enabled for the AP
- Recommendation to only use RNR and disable FILS and UBPR
  - Alternatively enable FILS to supplement RNR particularly if 2.4GHz and 5GHz are for some reason disabled
- Hidden SSIDs in 6GHz would force probes as the means to find the AP
  - If a non-PSC is used, then the SSID cannot be located
- Some clients (e.g. Intel) will look for 6GHz beacon to determine if they can enable 6GHz operation to meet regulatory requirements
  - If all 6GHz SSIDs are hidden, this would be a “no initial radiation” state and 6GHz on the client would not be enabled

Hidden SSIDs and 6GHz

- Probe and Association Requests are sent in the clear with the SSID
- This implies that “Hidden SSIDs” are not truly “hidden” and therefore of no security value

- In 6GHz Probe Requests are only permitted on Preferred Scanning Channels (PFCs)
- Hidden SSIDs would require Probes to be used for discovery
- WLANs on non-PFC channels would not be locatable



WPA2/WPA3 Transition Mode

- 3 Band SSID
- All WPA3
- Control of devices

BOH/Office

- Separate 2.4+5 and 6GHz
- WPA 2 legacy
- WPA 3 6GHz
- Same SSID

General Use

- Separate 2.4+5 and 6GHz
- WPA 2 legacy
- WPA 3 6GHz
- Different 6GHz SSID

Special Case

- Separate 2.4+5 and 6GHz
- WPA 2 transition legacy
- WPA 3 6GHz
- Same 6GHz SSID

Not recommended

- BOH/Office
  - If you can control the devices.
  - Fast roaming works across bands
- General use
  - Accommodates legacy clients
  - No fast roaming between bands
  - Some clients may “bounce” causing disruption to client and network loading.
  - Typically recommended for Eduroam
- Special Case
  - Like General Use
  - Can help reduce the bounce in general use
  - RNR is still effective
  - Clients will often stay at 5GHz
- Not recommended
  - It works
  - Client may think they are on WPA3 when on WPA2

17.12 adds support for Transition Mode

WPA2/WPA3

Interoperability and Compliance

Features	Catalyst (Local)	Catalyst (Flexconnect)	Meraki
WPA2 PSK/FT-PSK/802.1X + AES-CCMP128	✅	✅	✅
WPA2 802.1X SuiteB + AES-GCMP128, 802.1X SuiteB-192bit + AES-CCMP256/GCMP256	✅	☑	✕
WPA3 OWE/SAE/FT-SAE/802.1X-SHA256/FT-802.1X-SHA256 + AES-CCMP128	✅	✅	✅
WPA3 802.1X Suite B + AES-GCMP128, 802.1X SuiteB-192bit + AES-CCMP256/GCMP256	✅	☑	✅ (only SuiteB-192 + GCMP256)
*WPA3 SAE-EXT/FT-SAE-EXT + AES-CCMP128/GCMP256 (AKM 24 and 25, DH Group 19 and Wi-Fi 7 Compliant)	☑	☑	☑
WPA3 FT-802.1X-SuiteB-192bit + AES-CCMP256/GCMP256	✕	✕	☑ (only GCMP256)
*AP Beacon protection	☑	☑	☑
*WFA R2 Compliance for FT-SAE	☑	✕	✅
WPA3 Transition Mode	✅	✅	✅ (Only WPA3-Personal)

✅ Supported ☑ Planned (IOS-XE 17.15.1, Meraki R31-1) ✕ Not supported and no release planning * Mandatory for WPA3-Personal compliance

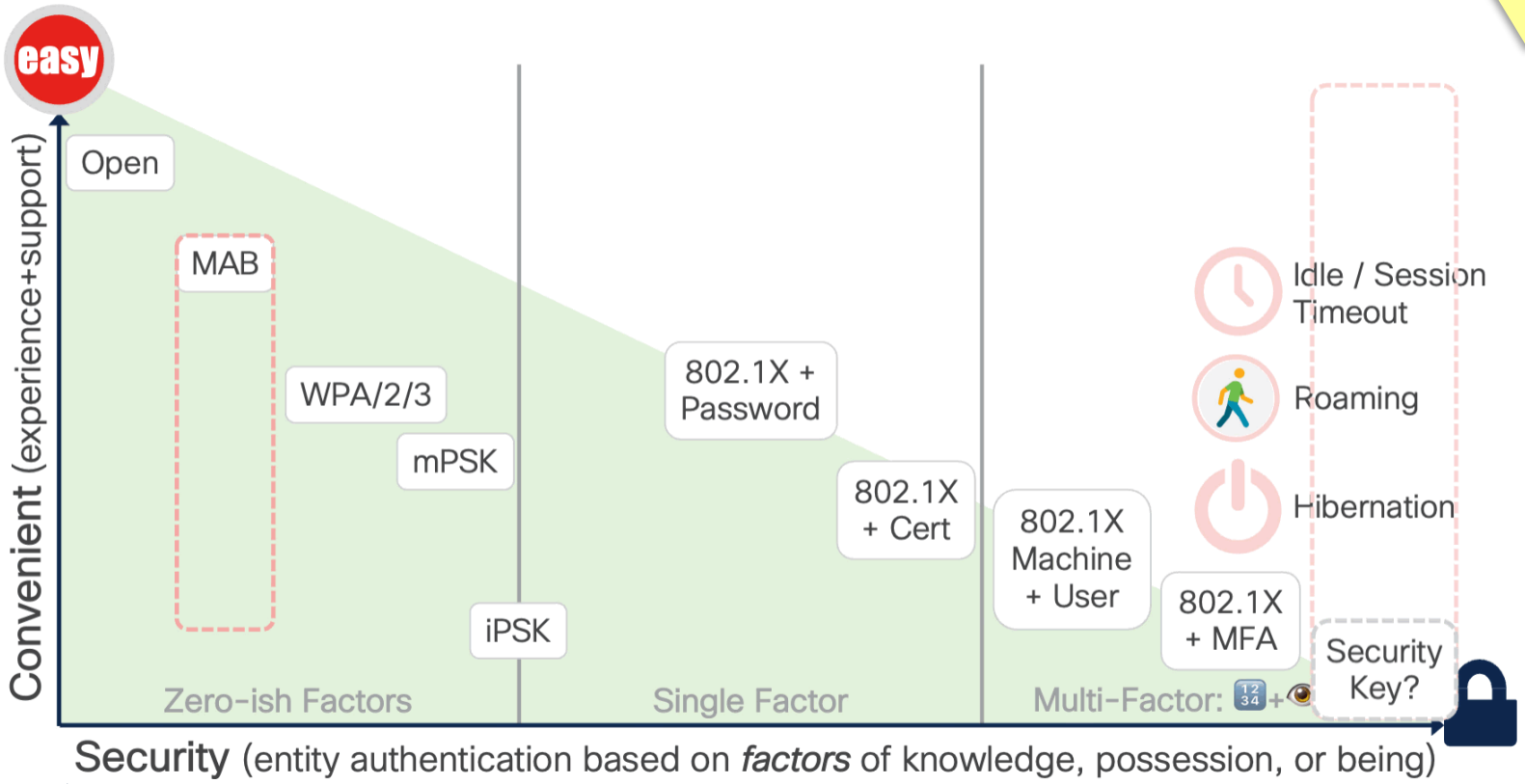
WPA3

New Requirements

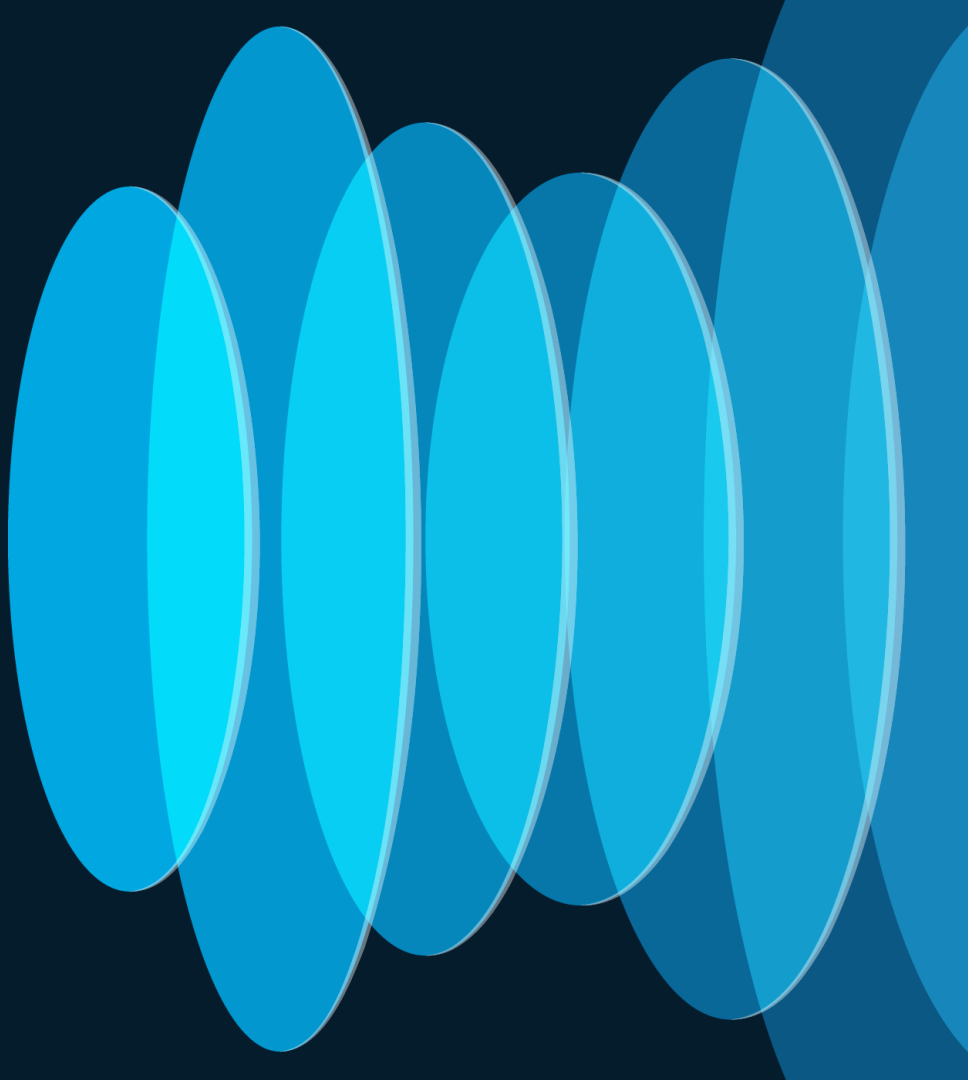
Features	Catalyst (Local)	Catalyst (Flexconnect)	Meraki
WPA3 FT-802.1X-SuiteB-192bit + AES-GCMP256 (Microsoft and Zebra ASK)	✕	✕	☑
AKM FT-802.1X-SHA384(22) and 802.1X-SHA384(23) Support	✕	✕	✕
SAE iPSK Central Auth support	☑	✕	✕
WGB WPA3 Support for COS AP	✕	✕	N/A
SAE-PK Support	✕	✕	TBD
WPA3 Enterprise Level Compliance (WFA underworking)	✕	✕	✕
WPA3 FT-802.1X-SuiteB-192bit + AES-GCMP256 (Microsoft and Zebra ASK)	✕	✕	☑
AKM FT-802.1X-SHA384(22) and 802.1X-SHA384(23) Support	✕	✕	✕
SAE iPSK Central Auth support	☑	✕	✕

☐ ☑ Supported planning ☑ Planned (IOS-XE 17.15.1, Meraki R31-1) ✕ Not supported and no release

Network Access Security Spectrum



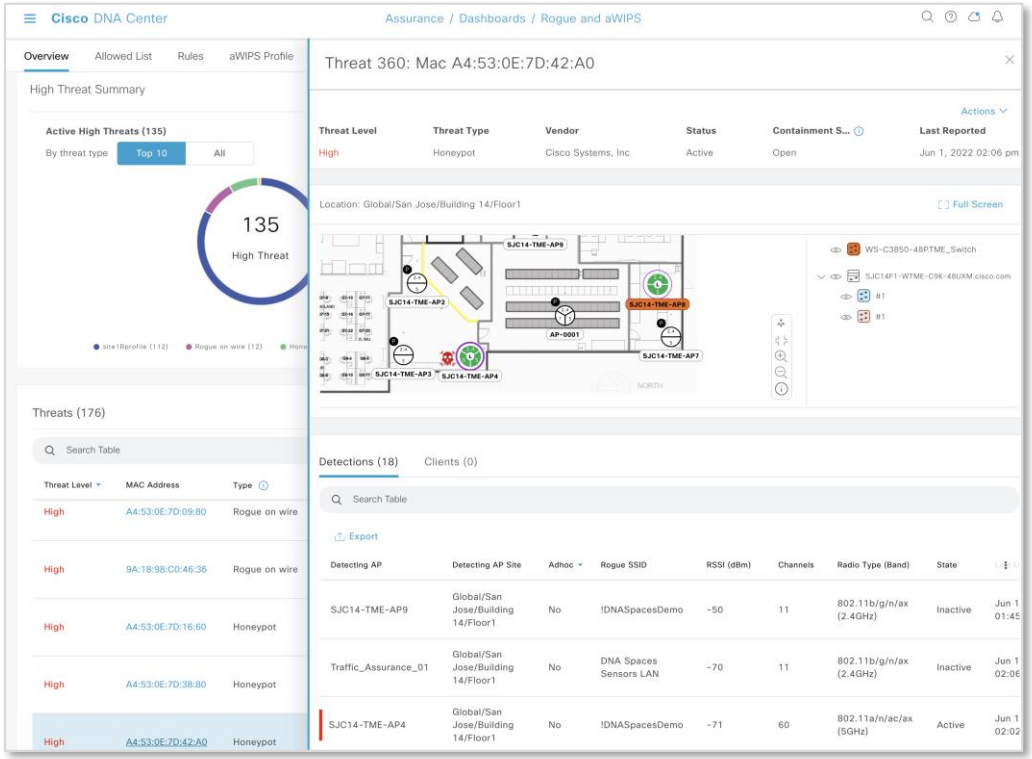
Wireless Intrusion Detection and Prevention



cisco Live!

Rogue Detection and Advanced WIPS

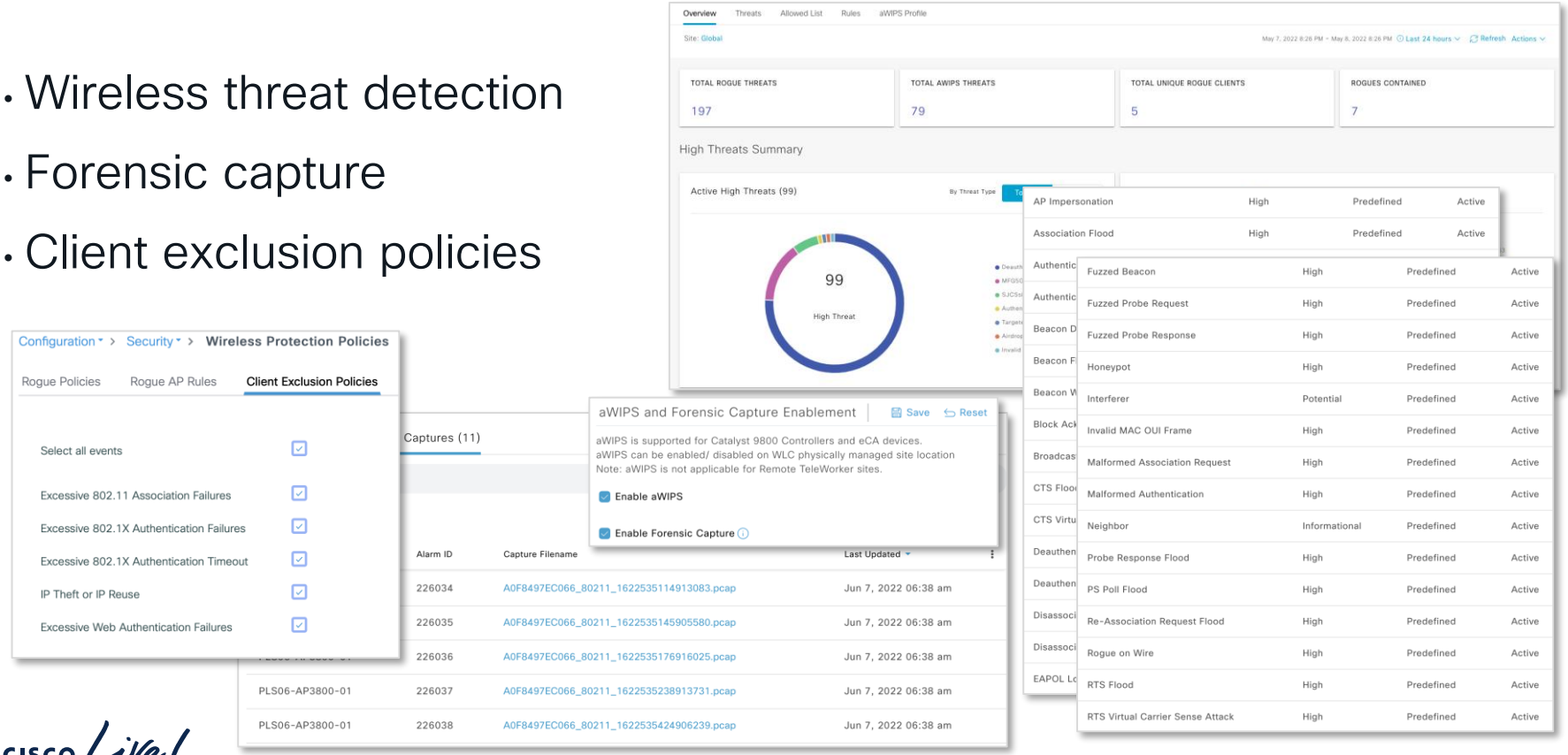
- Centralized wireless threat management
- Rogue detection and classification
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



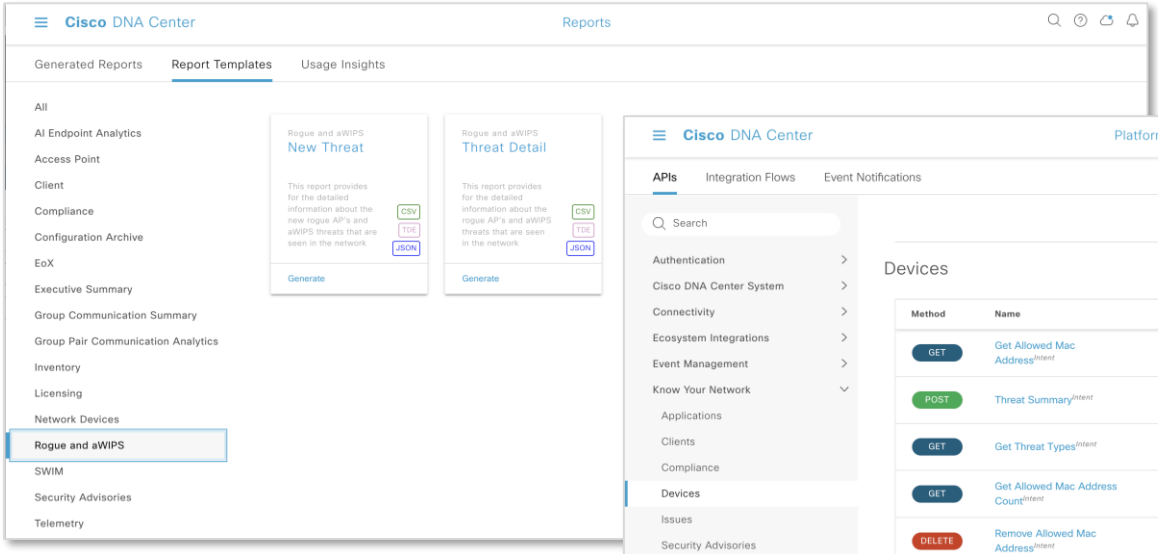
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3.html

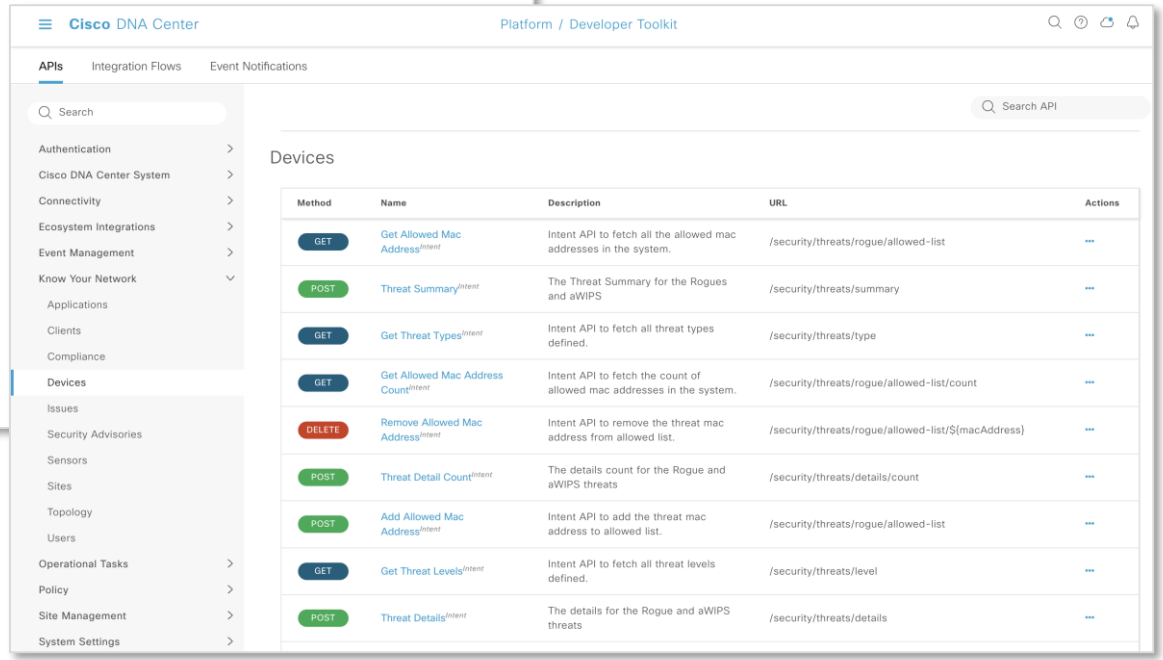
Rogue Detection and Advanced WIPS

- 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

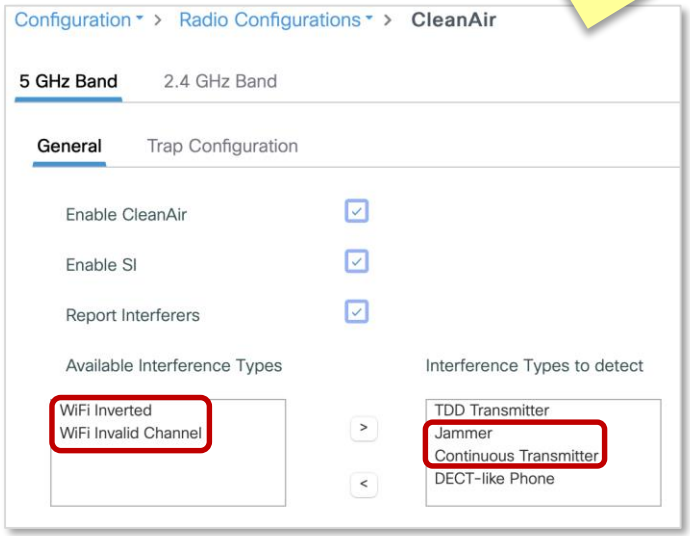
- Catalyst 9136
- Catalyst 9130
- Catalyst 9120

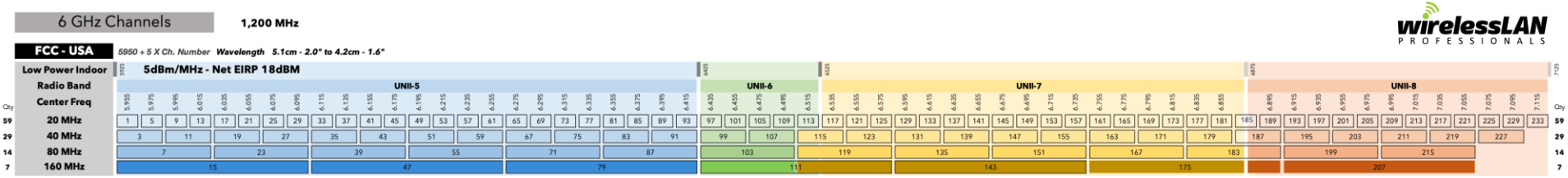
- Catalyst 9166
- Catalyst 9164
- Catalyst 9162

CleanAir Pro Spectrum Intelligence

FYI

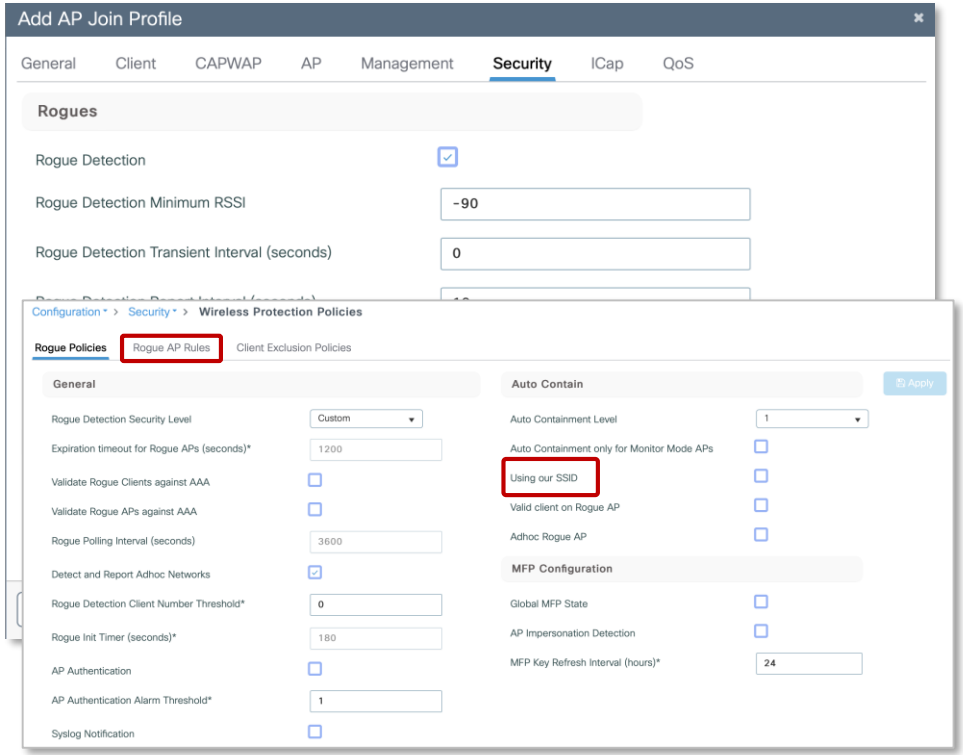
- Interferers
  - Layer 1 Denial of Service Attack
- Rogue AP Detection
  - Inverted
  - Invalid Channel
- 6GHz Support
  - Rogue Detection and WIPS





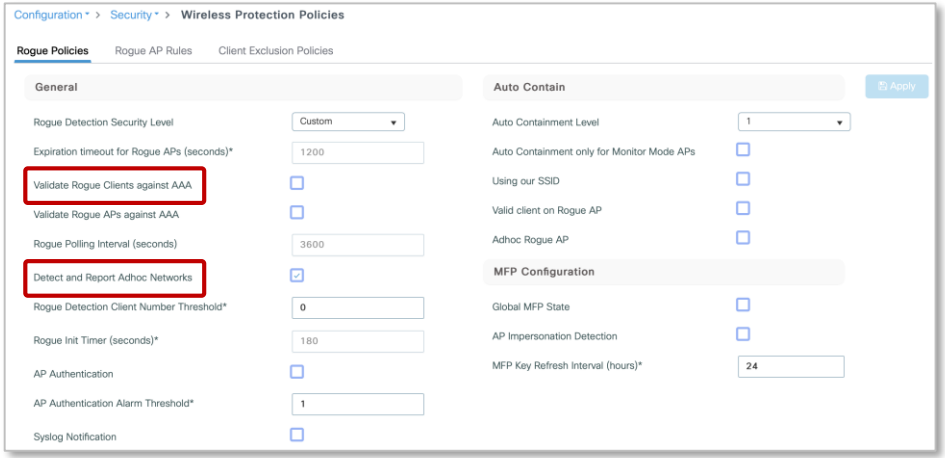
Rogue Access Points

- 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
  - Correctly differentiating between the two is critical

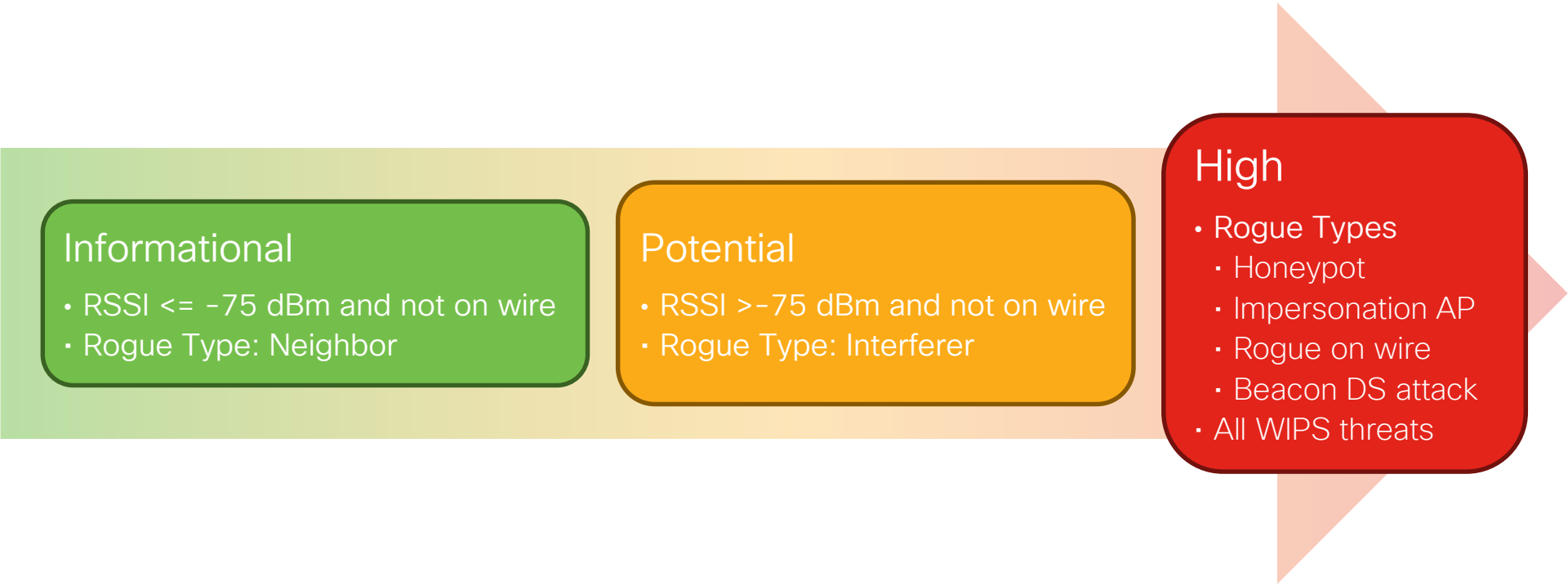


Rogue Clients

- 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

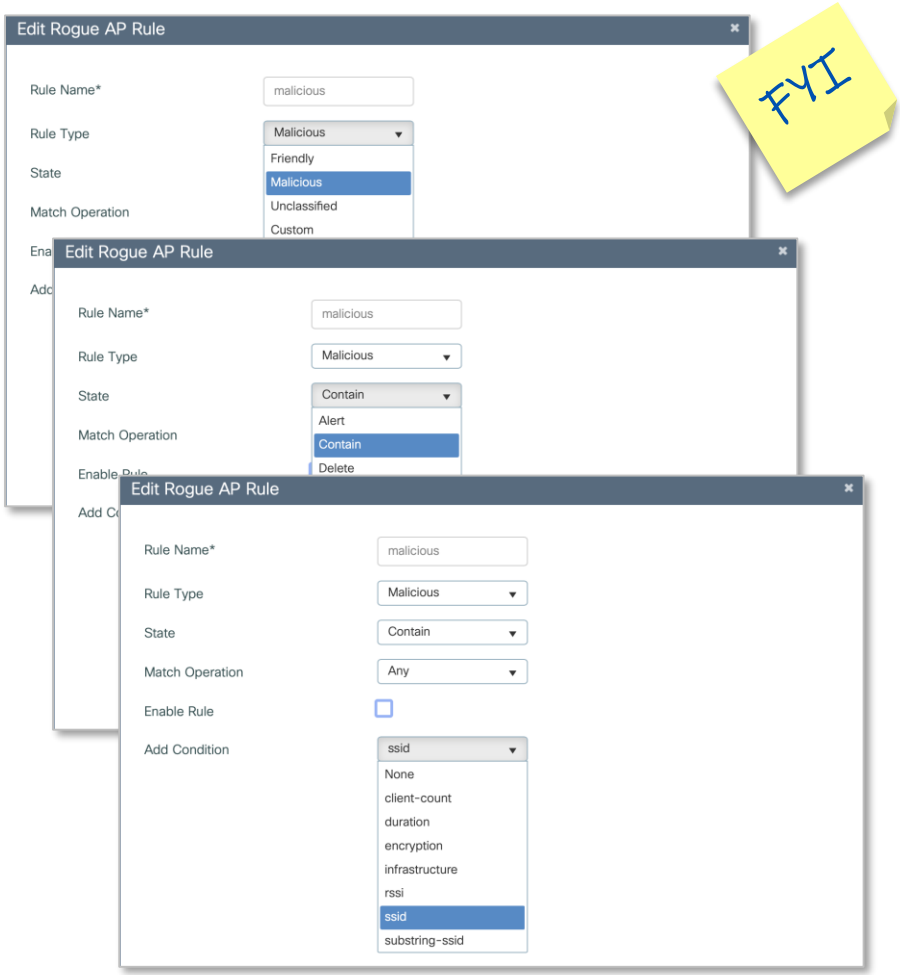


Cisco Catalyst Centre Threat Levels



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



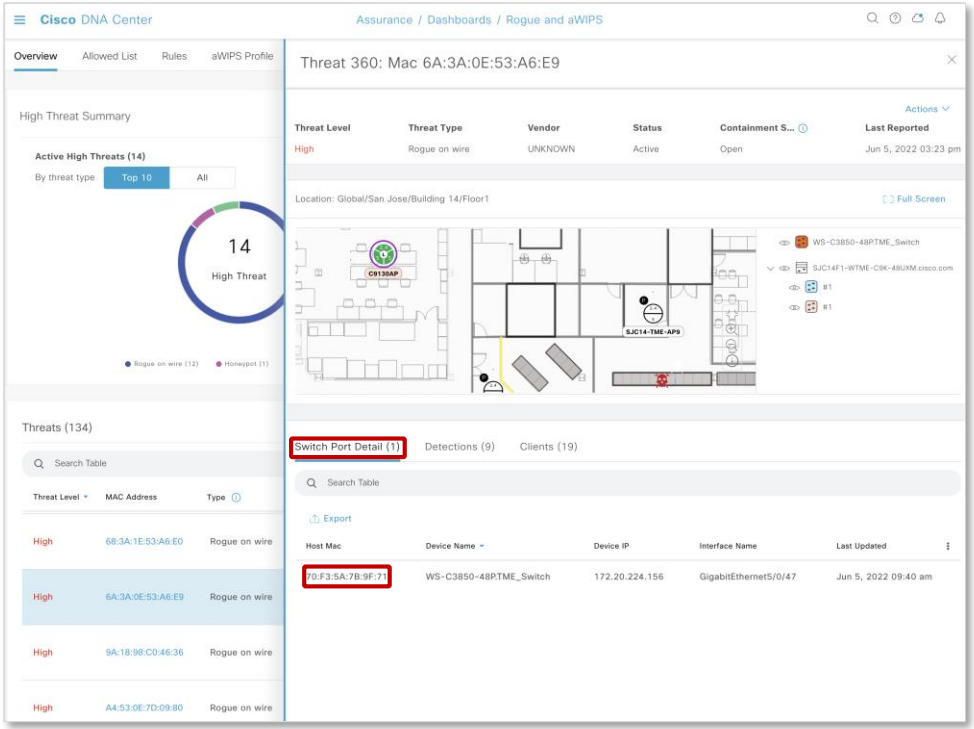
Rogue Notification Triggers

- 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
```

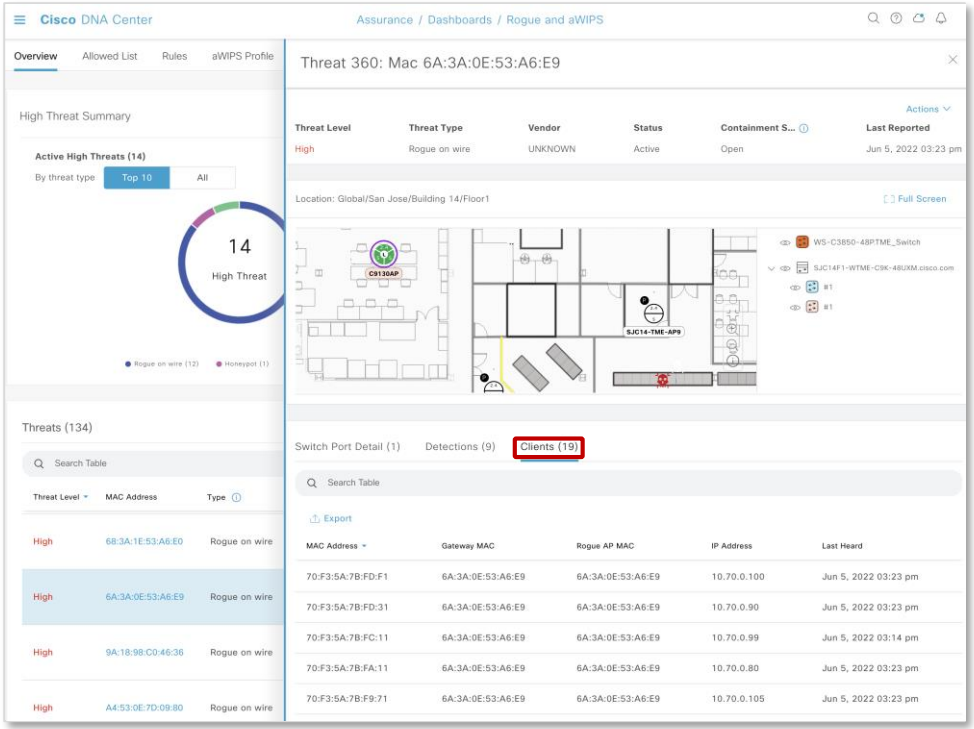
Rogue on Wire

- 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
- Wired 802.1x matters



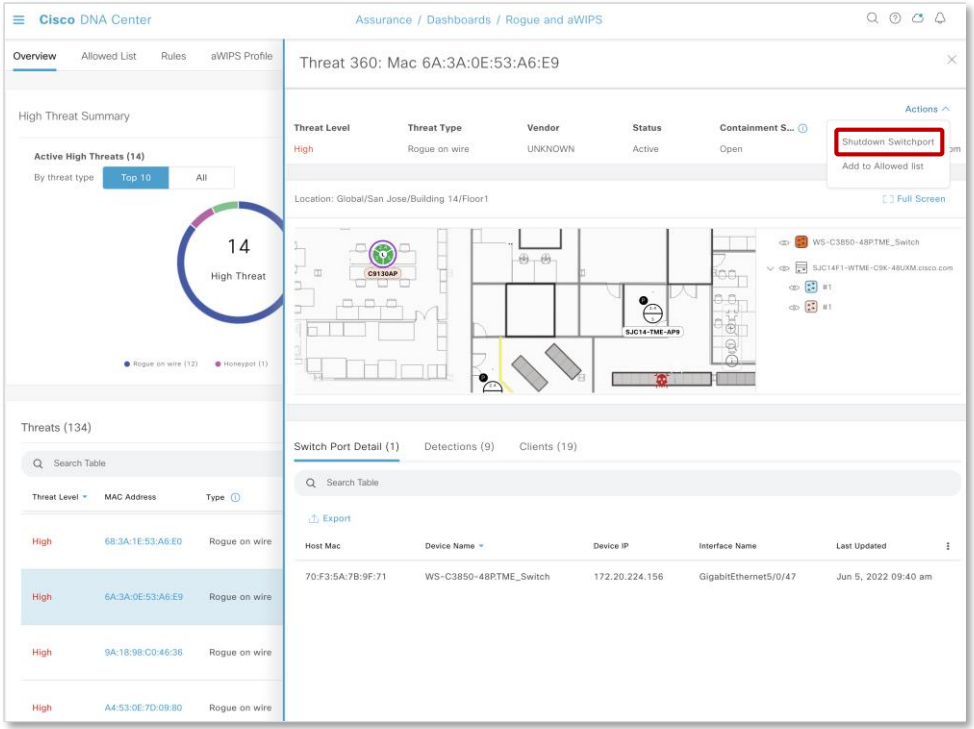
Rogue on Wire

- 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
- Wired 802.1x matters

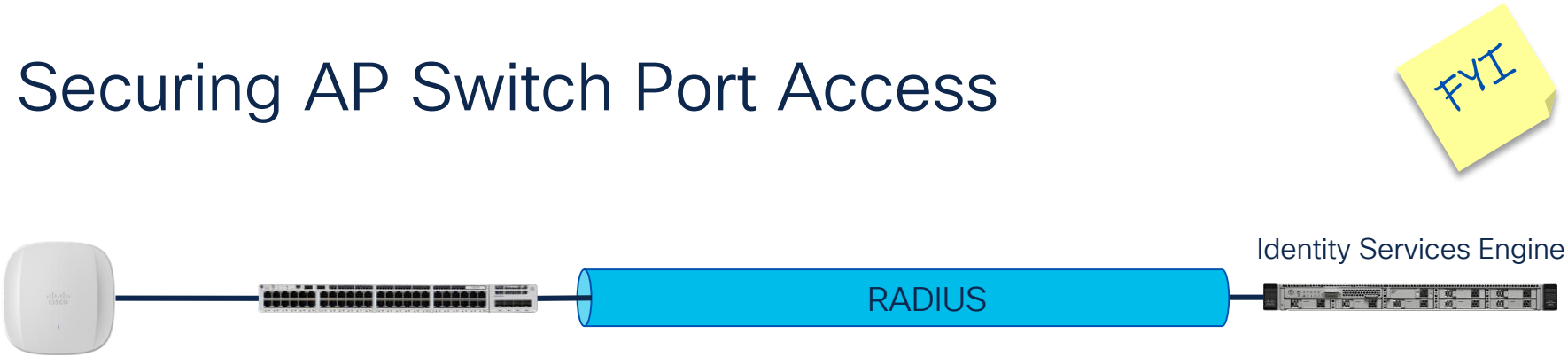


Rogue on Wire

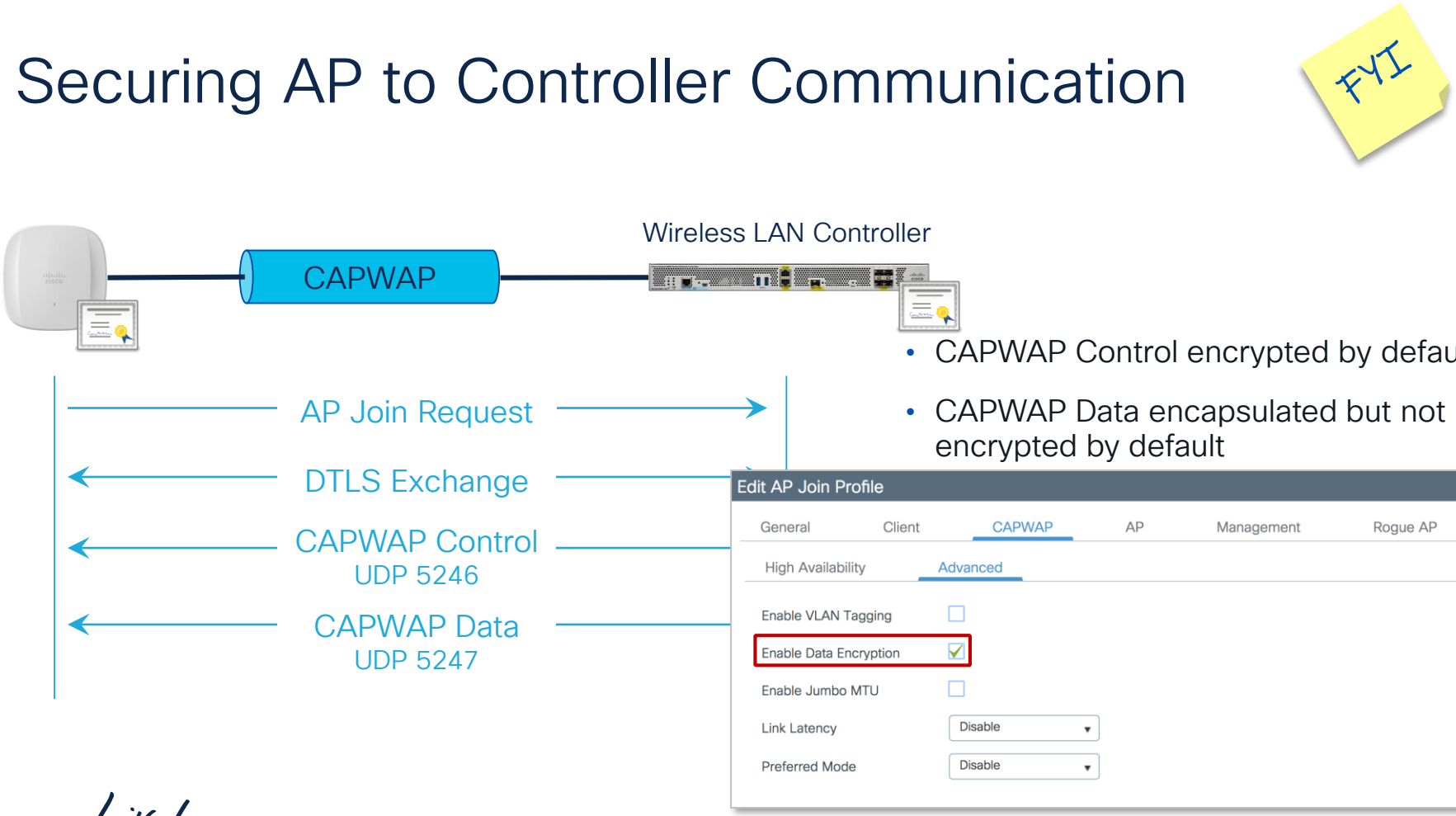
- Matching Algorithms
  - MAC Address ±3/±2/±1
  - Vendor matching algorithms
- Rogue AP in Bridge Mode
  - Locate the Rogue AP via the Rogue Client MAC address and Gateway MAC Address
- Wired 802.1x matters



Securing AP Switch Port Access

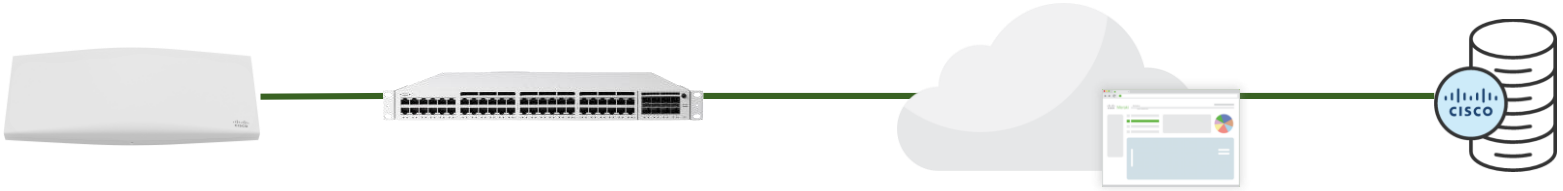


Securing AP to Controller Communication



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

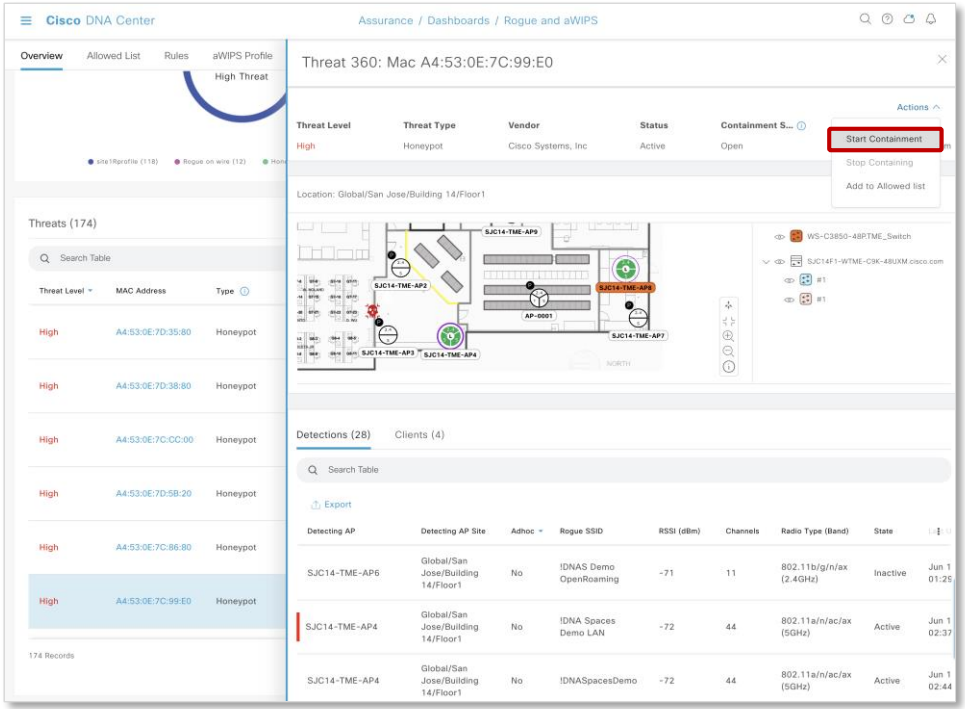
SecurePort



1. MR connected to MS
2. MS permits Meraki dashboard connection for MR
3. MR requests certificate from Cisco PKI
4. MR authenticates with acquired certificate
5. MS authorizes port based on configured profile

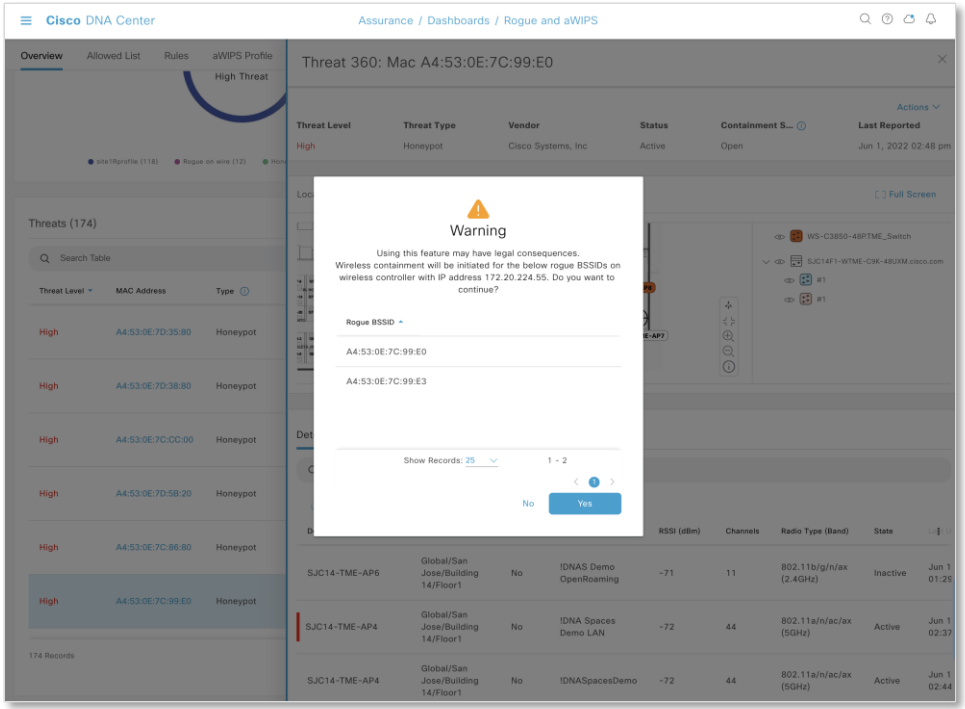
Rogue AP Containment

- How do we contain Rogue APs?



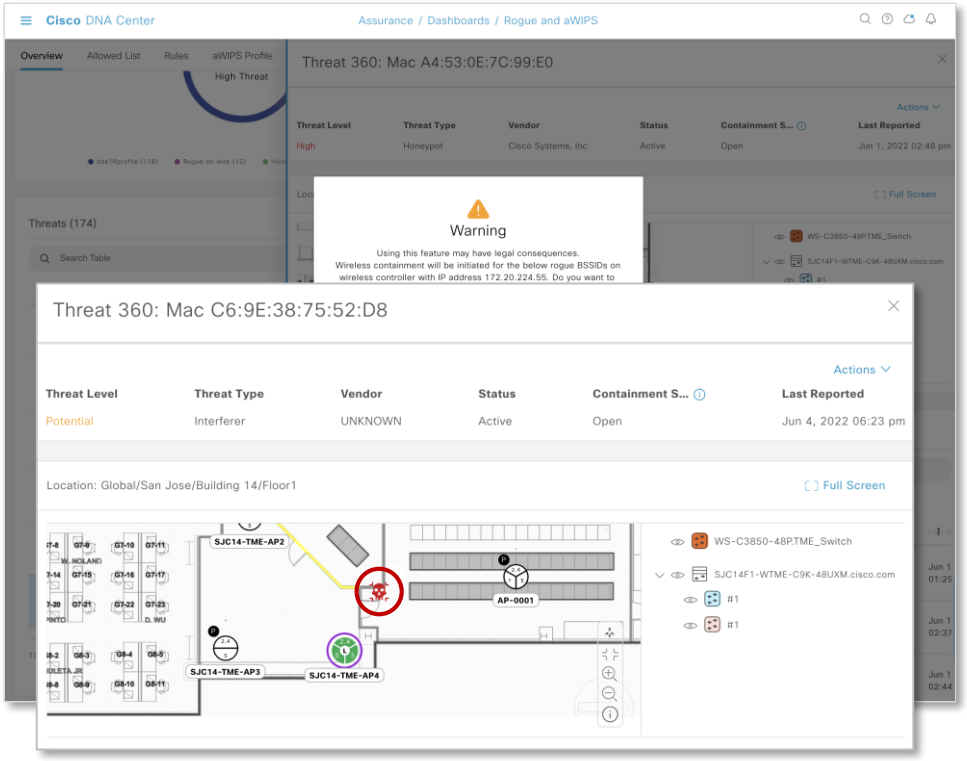
Rogue AP Containment

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

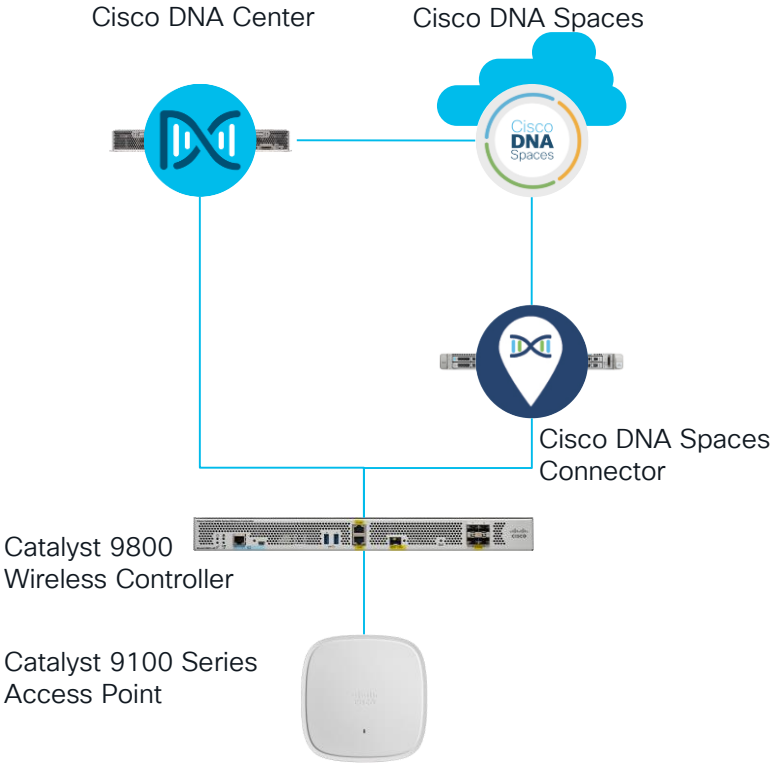


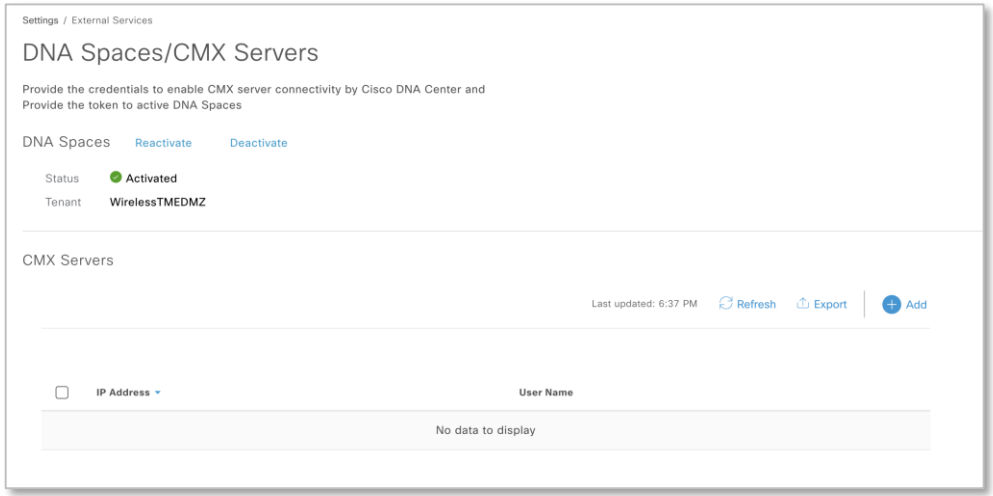
Rogue AP Containment

- 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

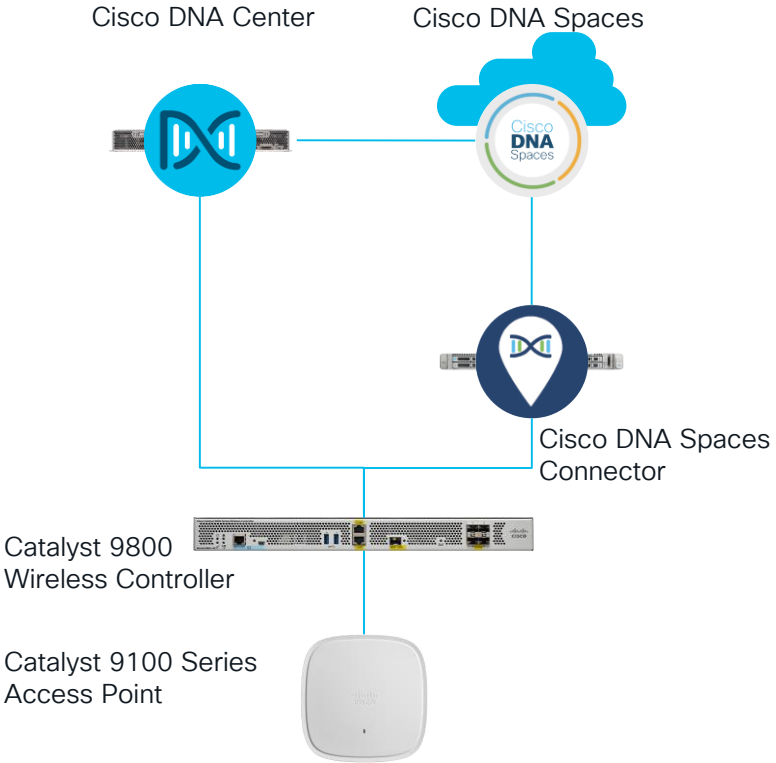


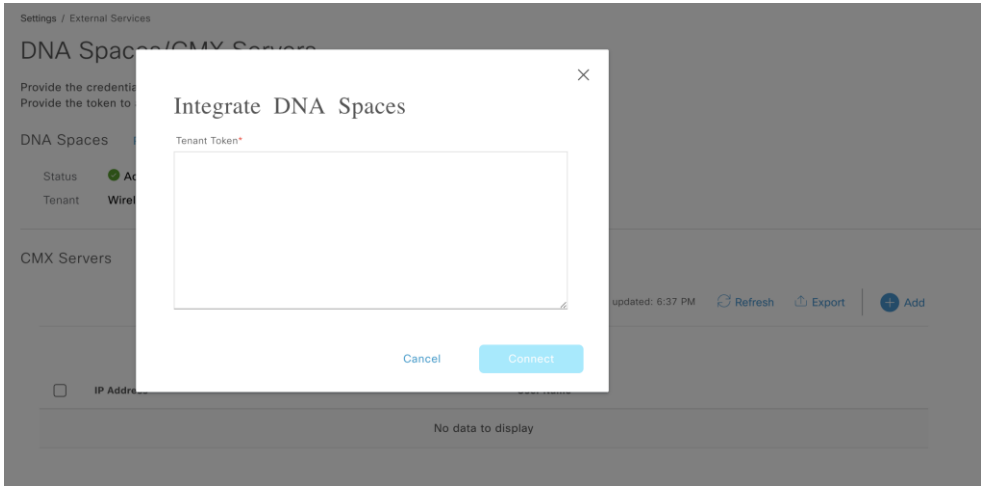
Enabling Location Services



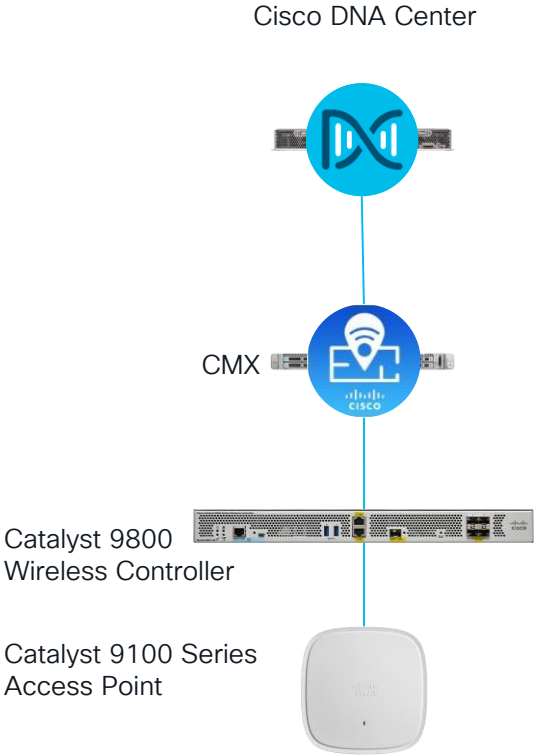


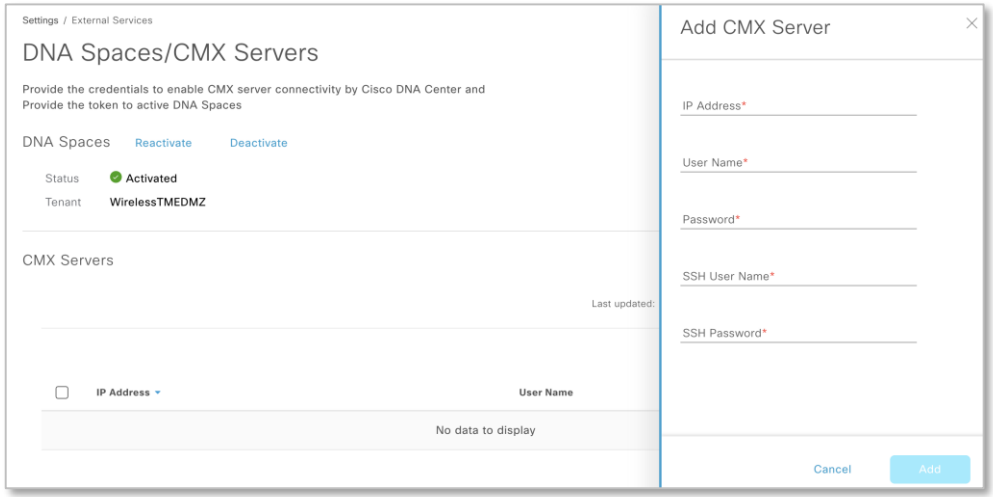
Enabling Location Services



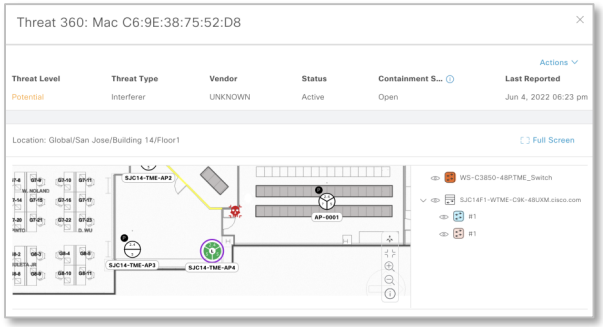


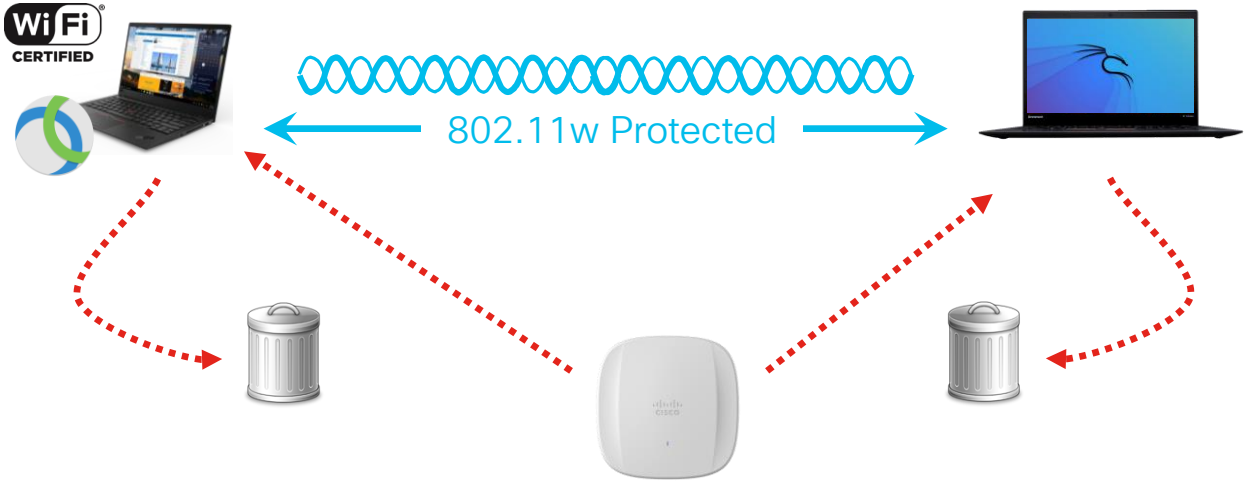
Enabling Location Services





Rogue Containment with WPA3

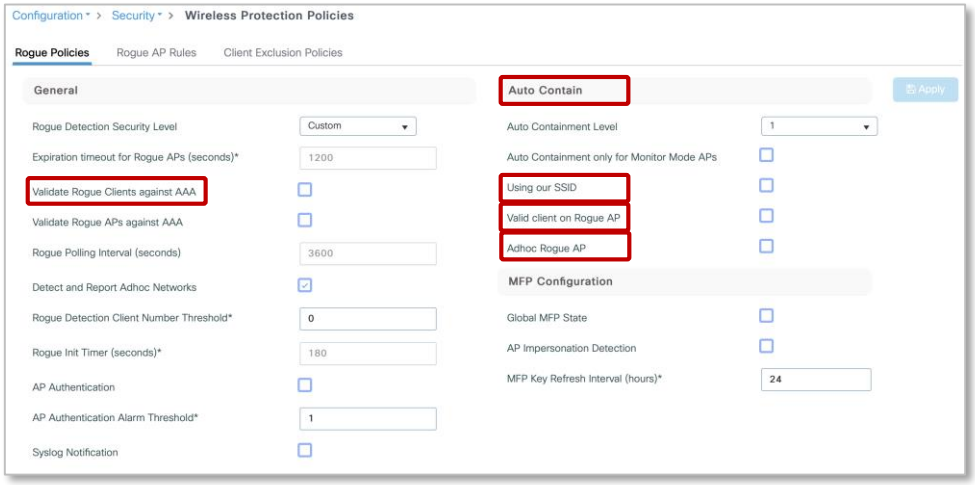




From IOS-XE 17.12.1

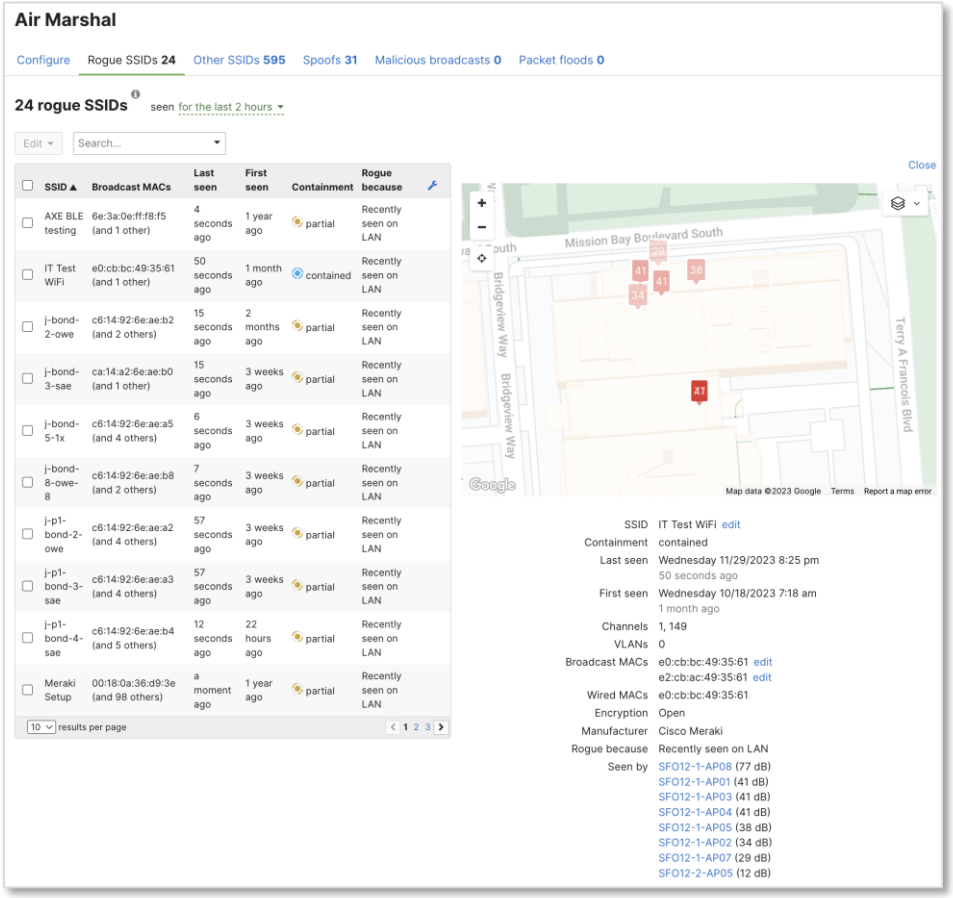
Rogue AP Auto Containment

- 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



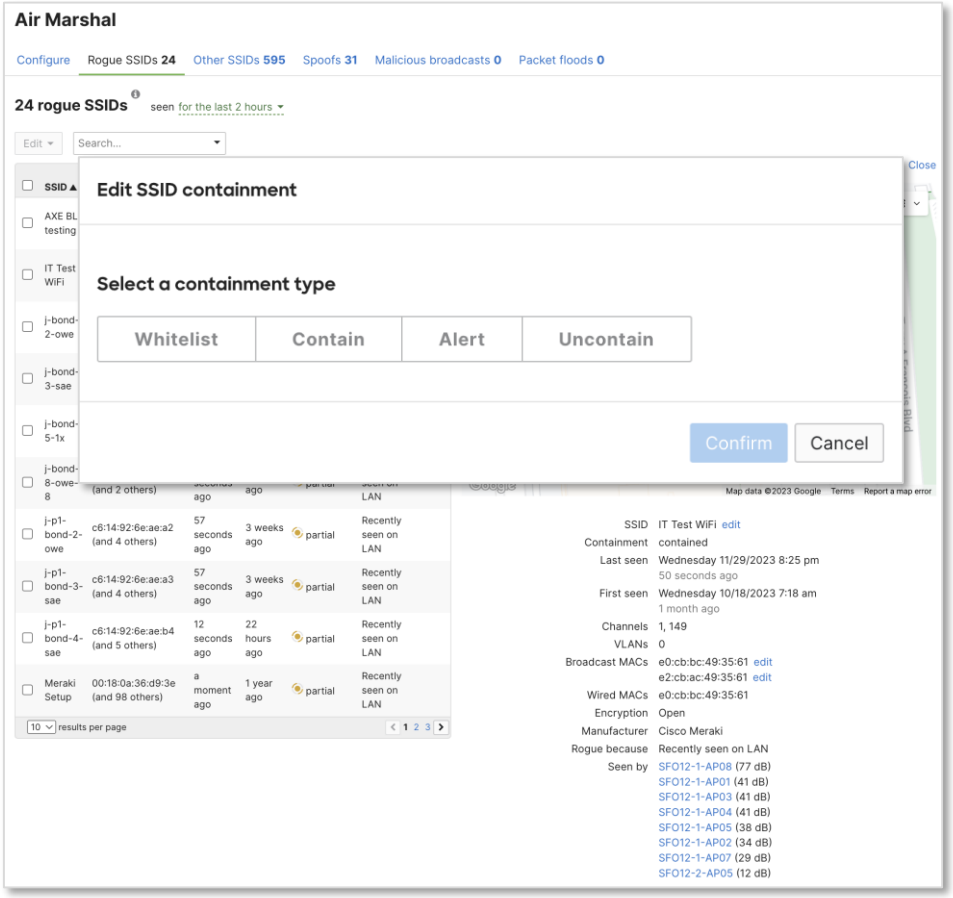
Air Marshal

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



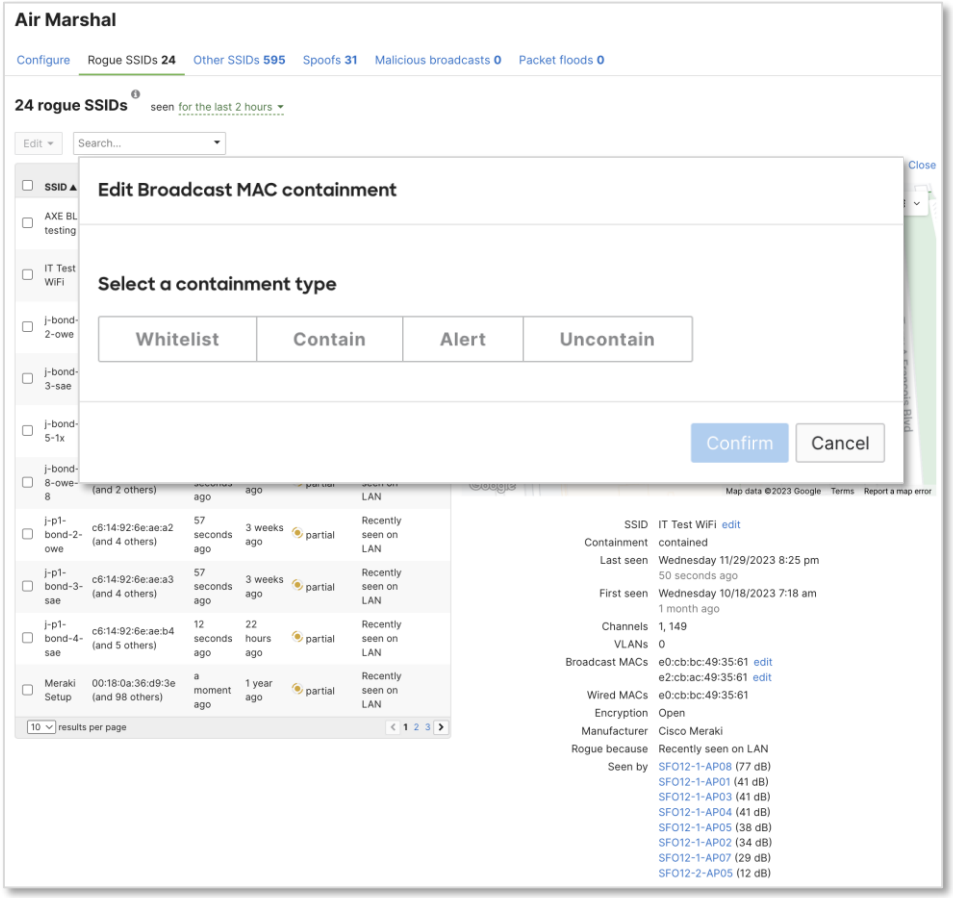
Air Marshal

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



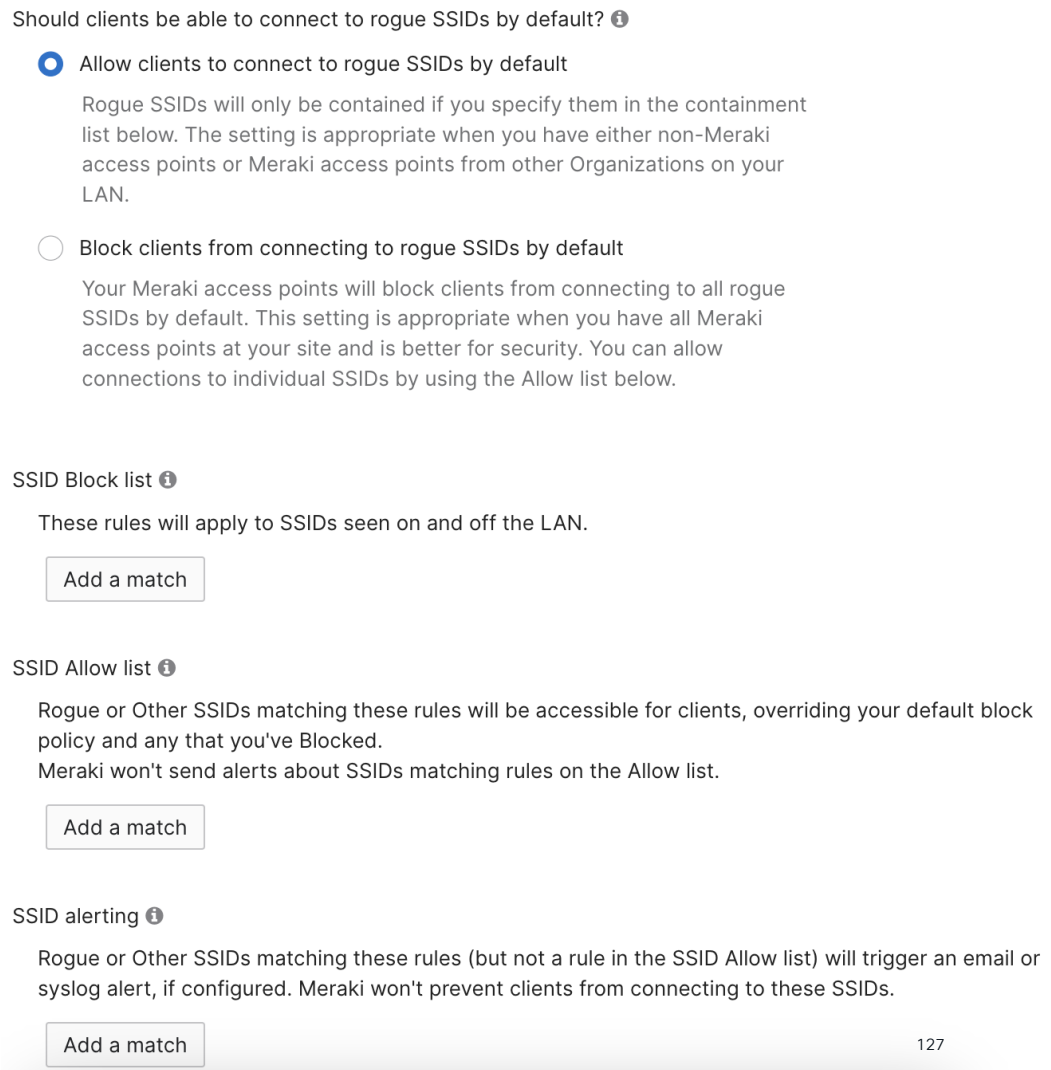
Air Marshal

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



Air Marshal

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



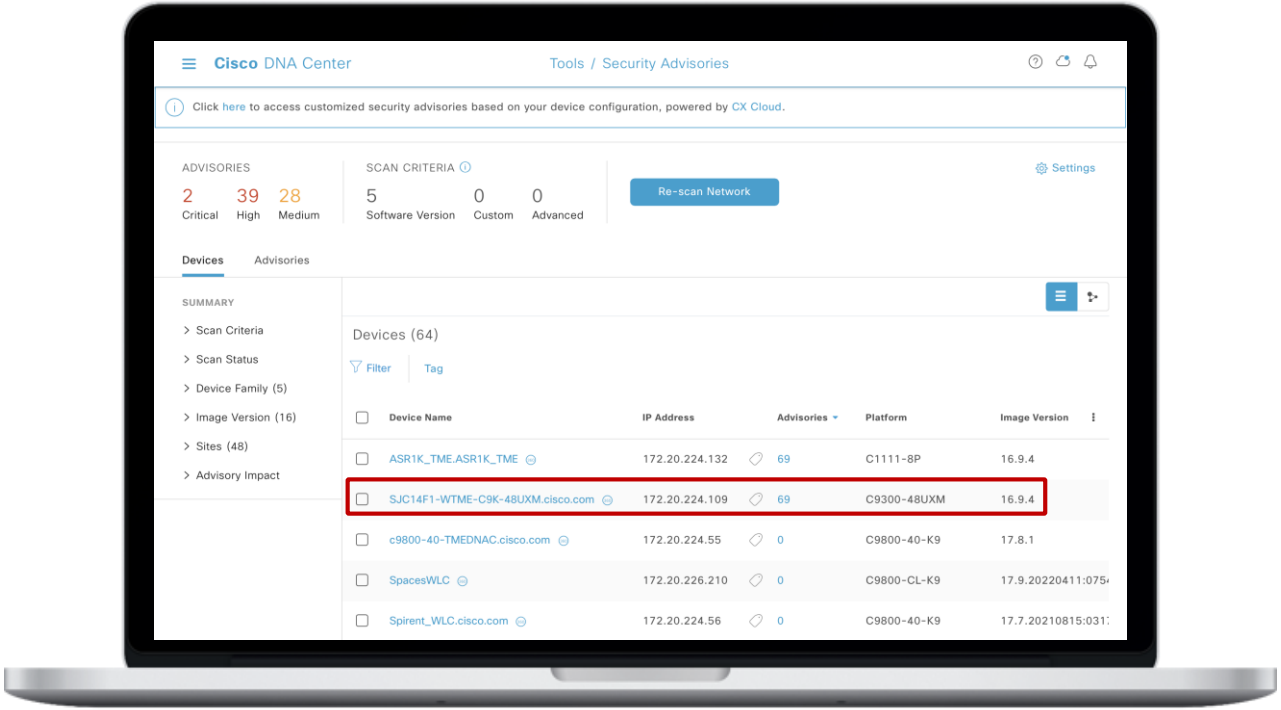
Air Marshal

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

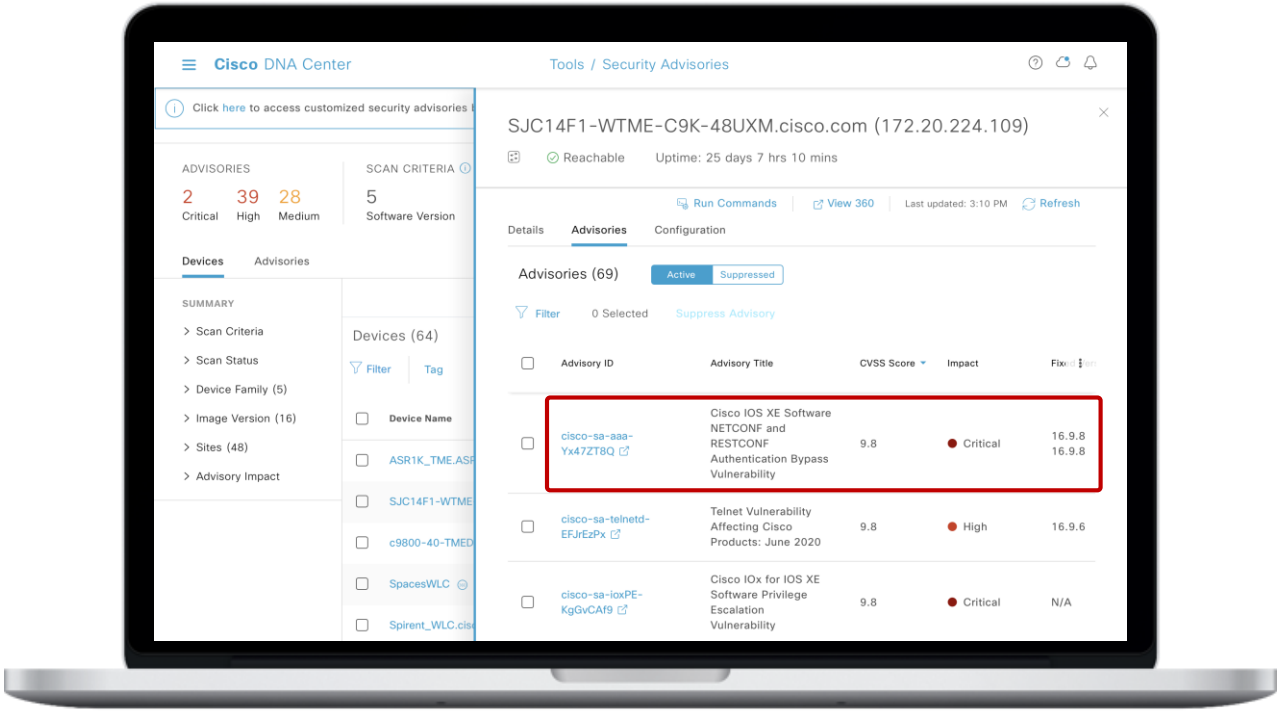
- Rogue detection support has been extended beyond the regulatory domain of the network
- Alerts are generated for rogue APs broadcasting on unauthorized 2.4 and 5 GHz radio channels

From MR 31.X

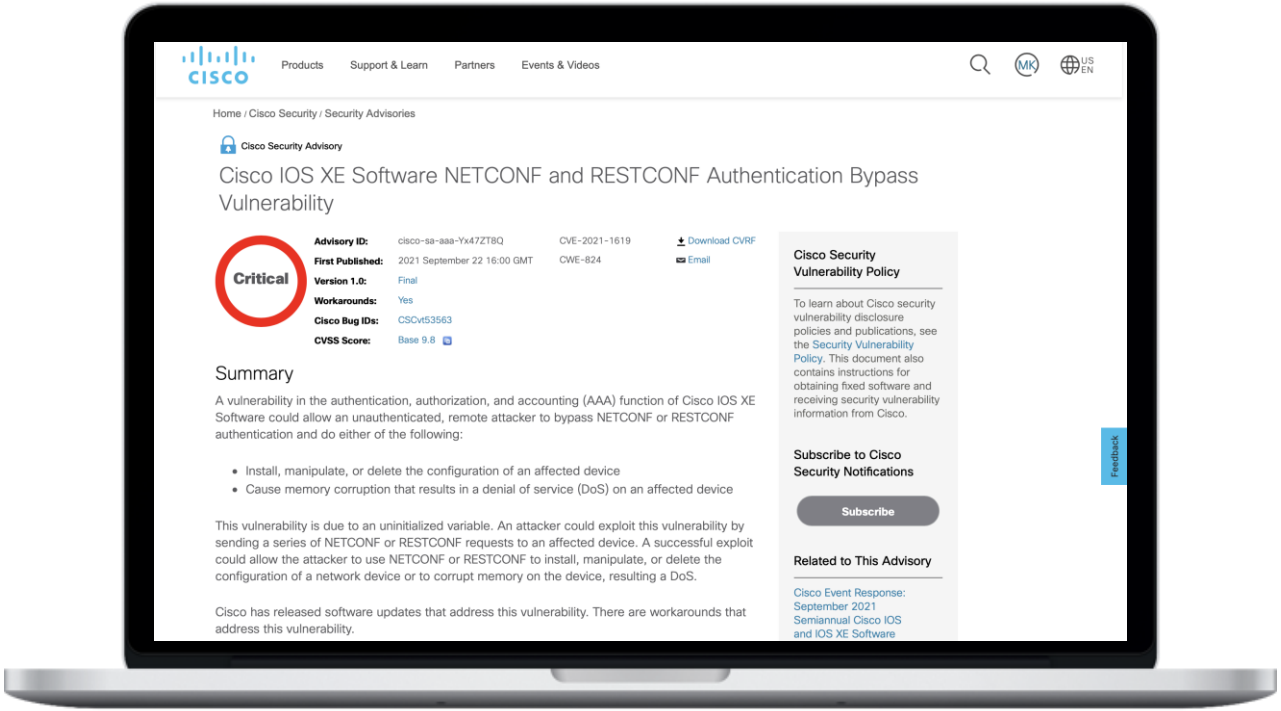
Cisco Catalyst Center Security Advisories



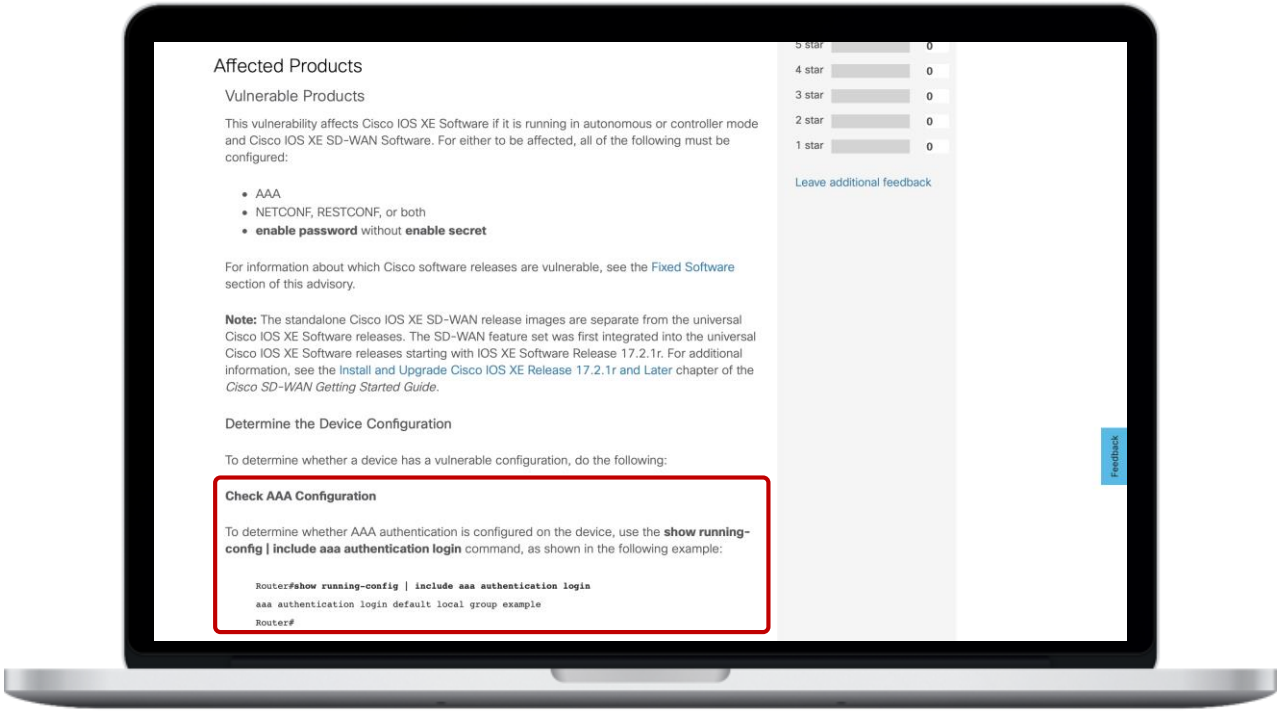
Cisco Catalyst Center Security Advisories



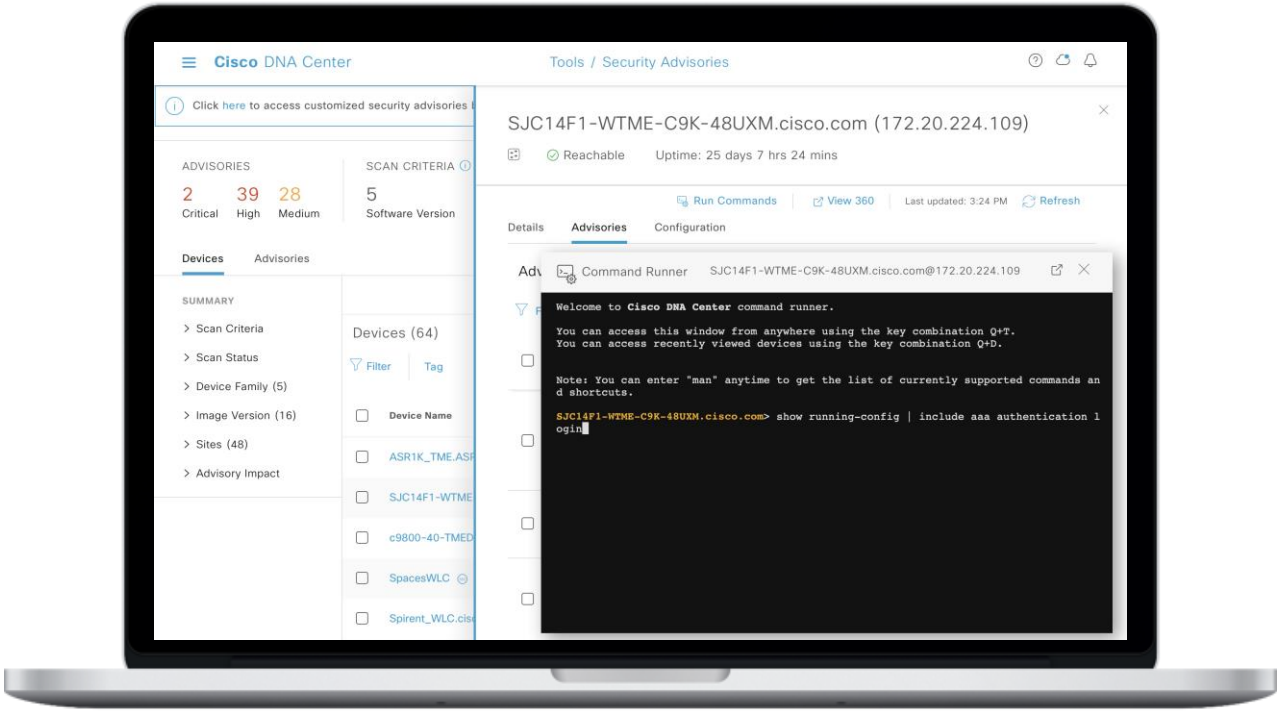
Cisco Catalyst Center Security Advisories



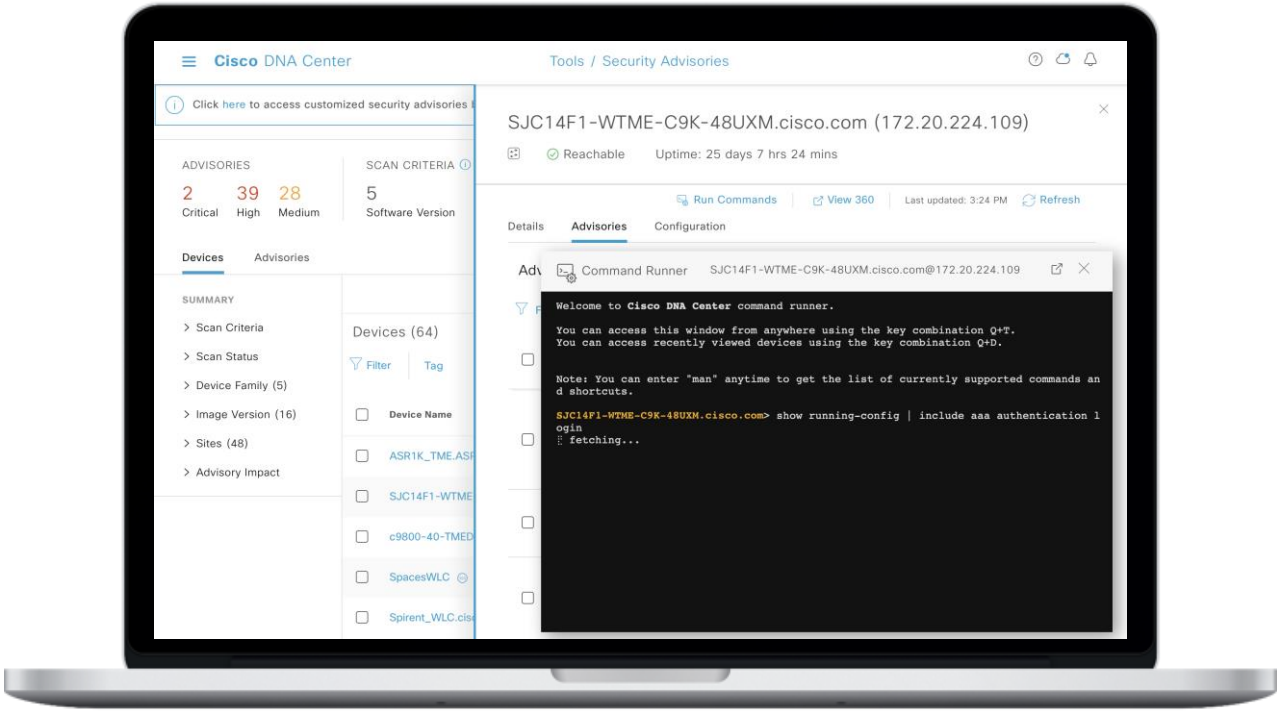
Cisco Catalyst Center Security Advisories



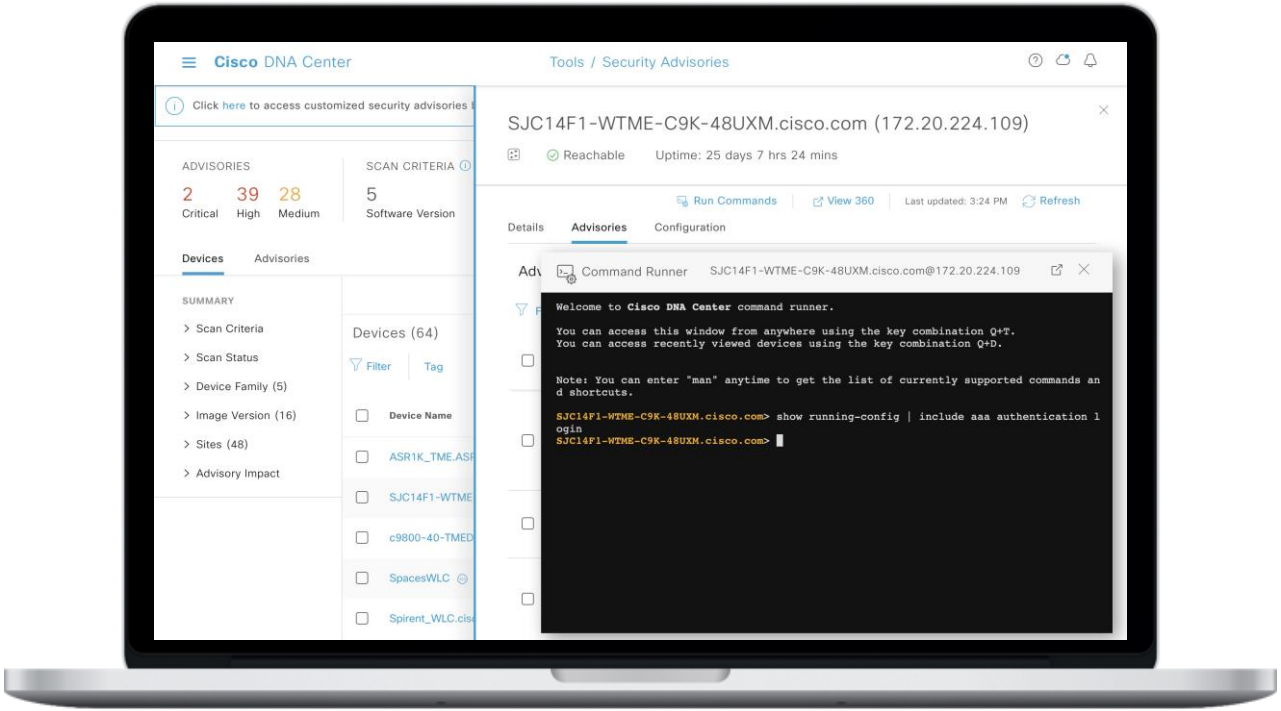
Cisco Catalyst Center Security Advisories



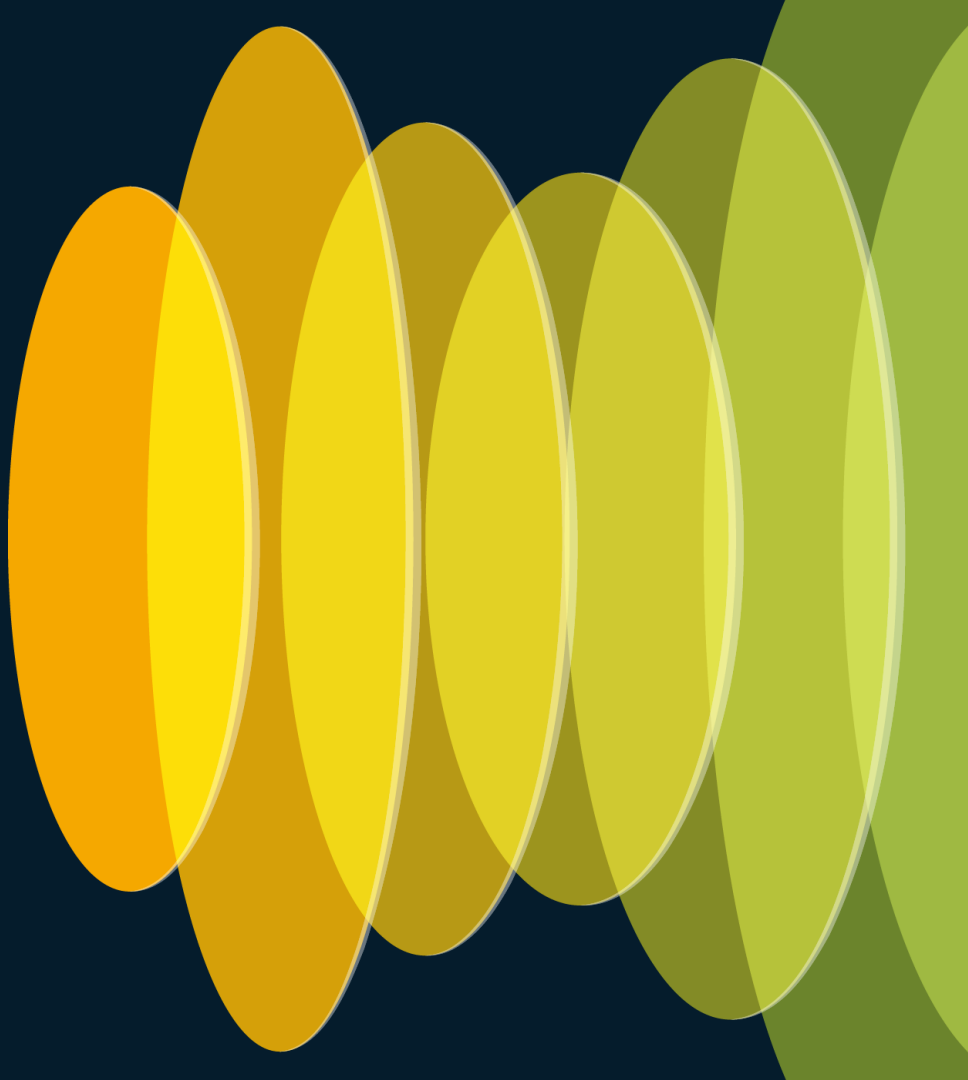
Cisco Catalyst Center Security Advisories



Cisco Catalyst Center Security Advisories

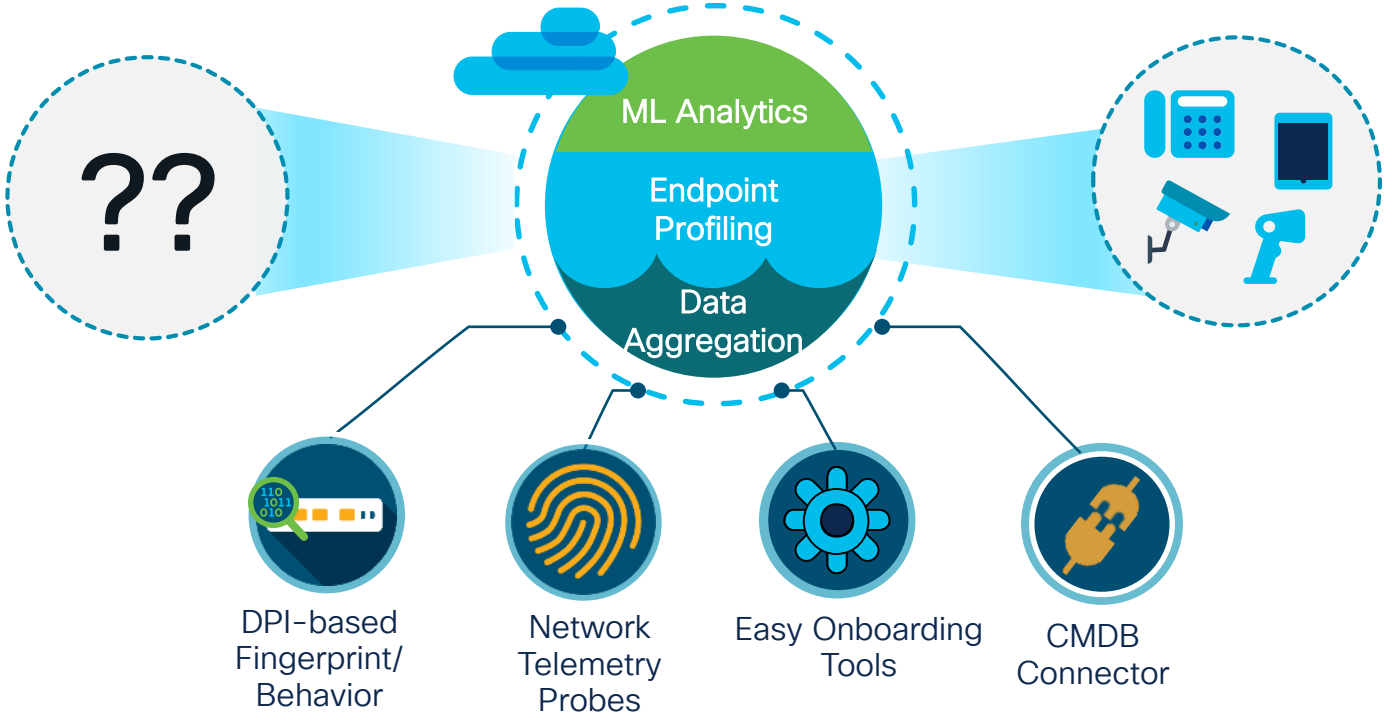


Network as a Sensor and Enforcer



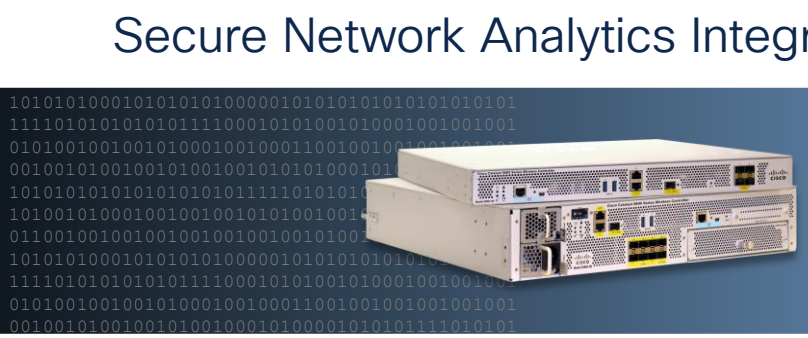
Cisco Catalyst Center AI Endpoint Analytics

FYI



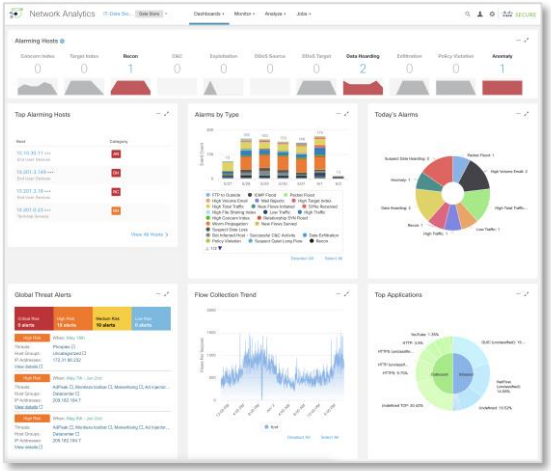
Network as a Sensor

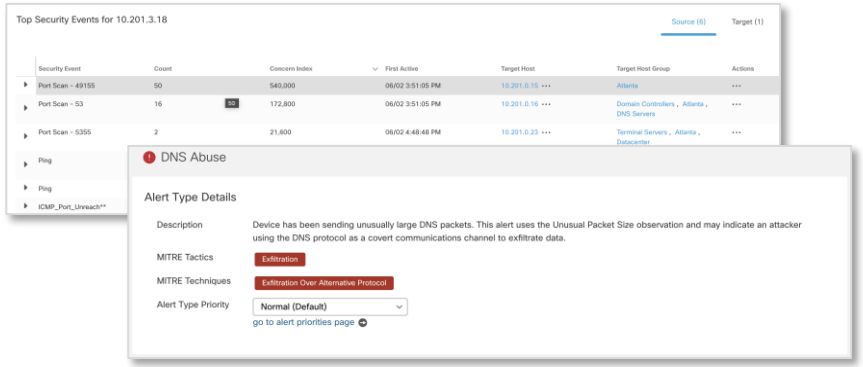
Secure Network Analytics Integration



Netflow

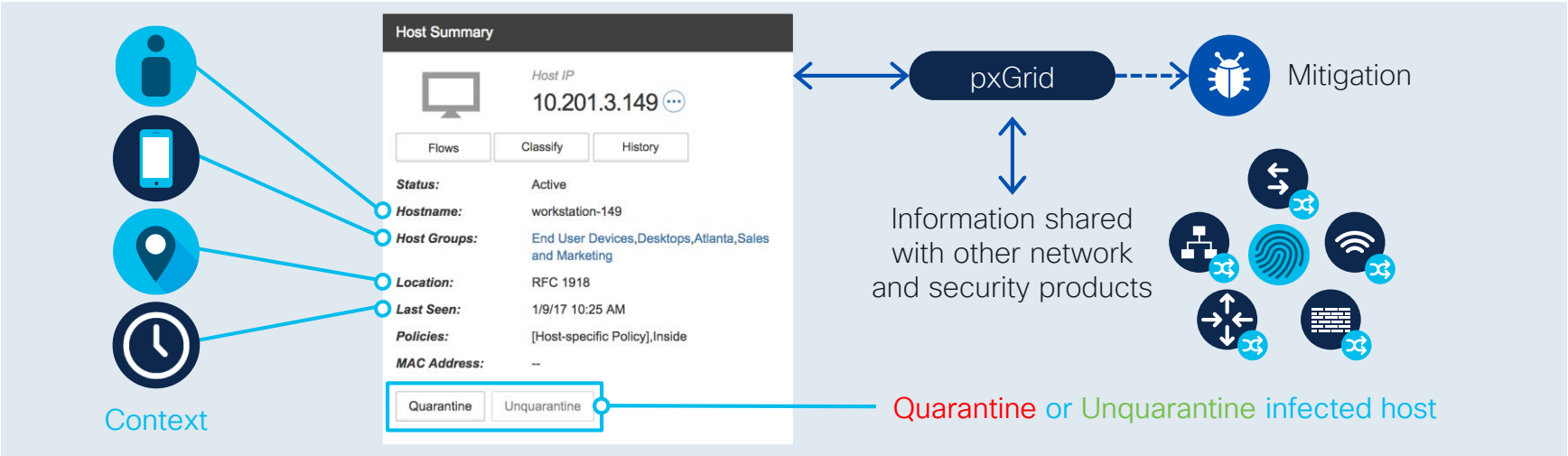
Malware detection and cryptographic compliance on Cisco Stealthwatch





Network as an Enforcer

Rapid Threat Containment



Identity Services Engine

Secure Network Analytics Management Console

Cisco Secure Network Analytics

Visibility everywhere

Analyze enterprise telemetry from any source, provide end to end visibility across the extended network in the cloud or with remote workers

Unique threat detection

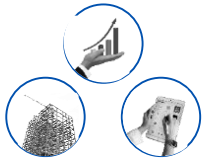
Combination of multi-layer machine learning and behavioral modeling provides the ability to detect inside as well as outside threats

Encrypted traffic analytics

Analyze encrypted traffic to detect malware and ensure policy compliance without decryption

Smart segmentation

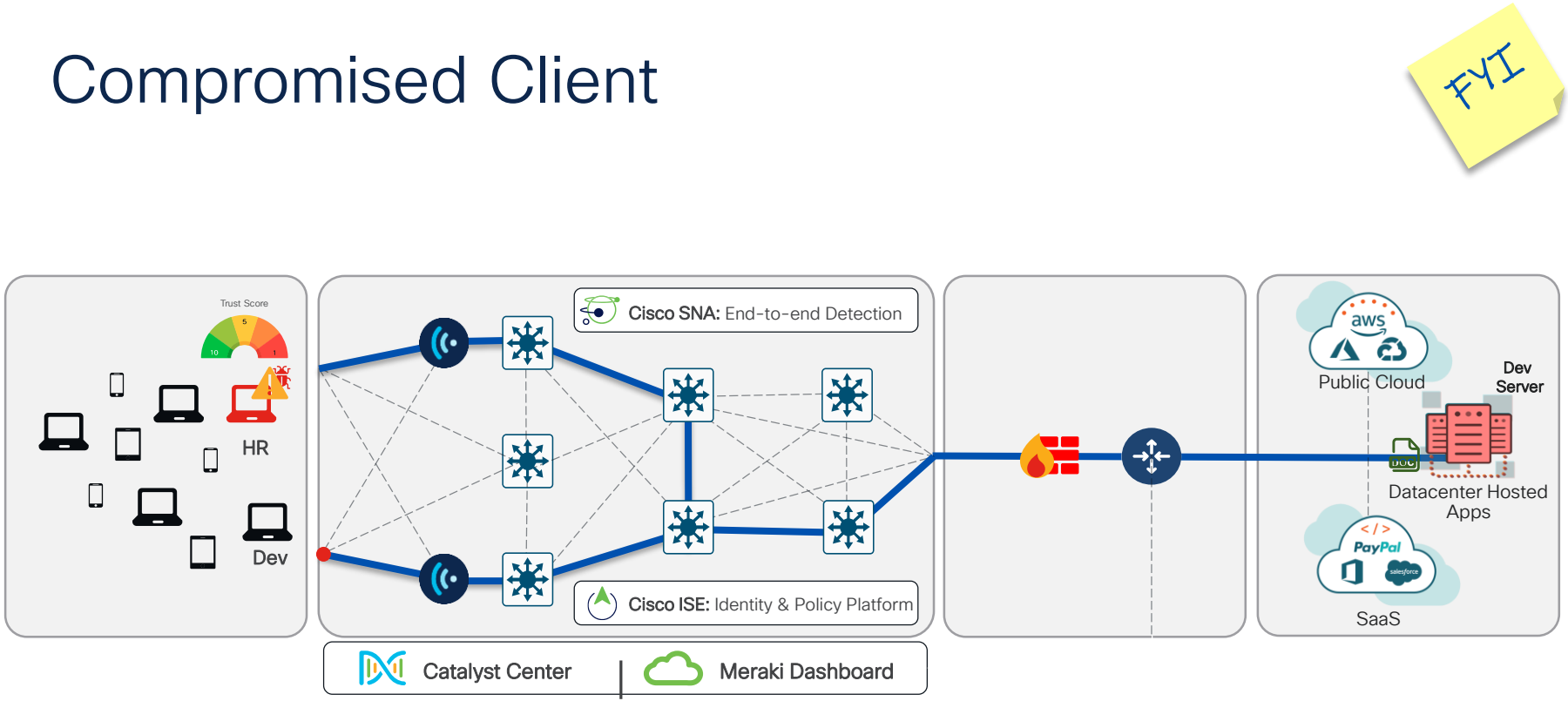
Use logical functional business groups that, monitor the effectiveness of segmentation policies through contextual alarms



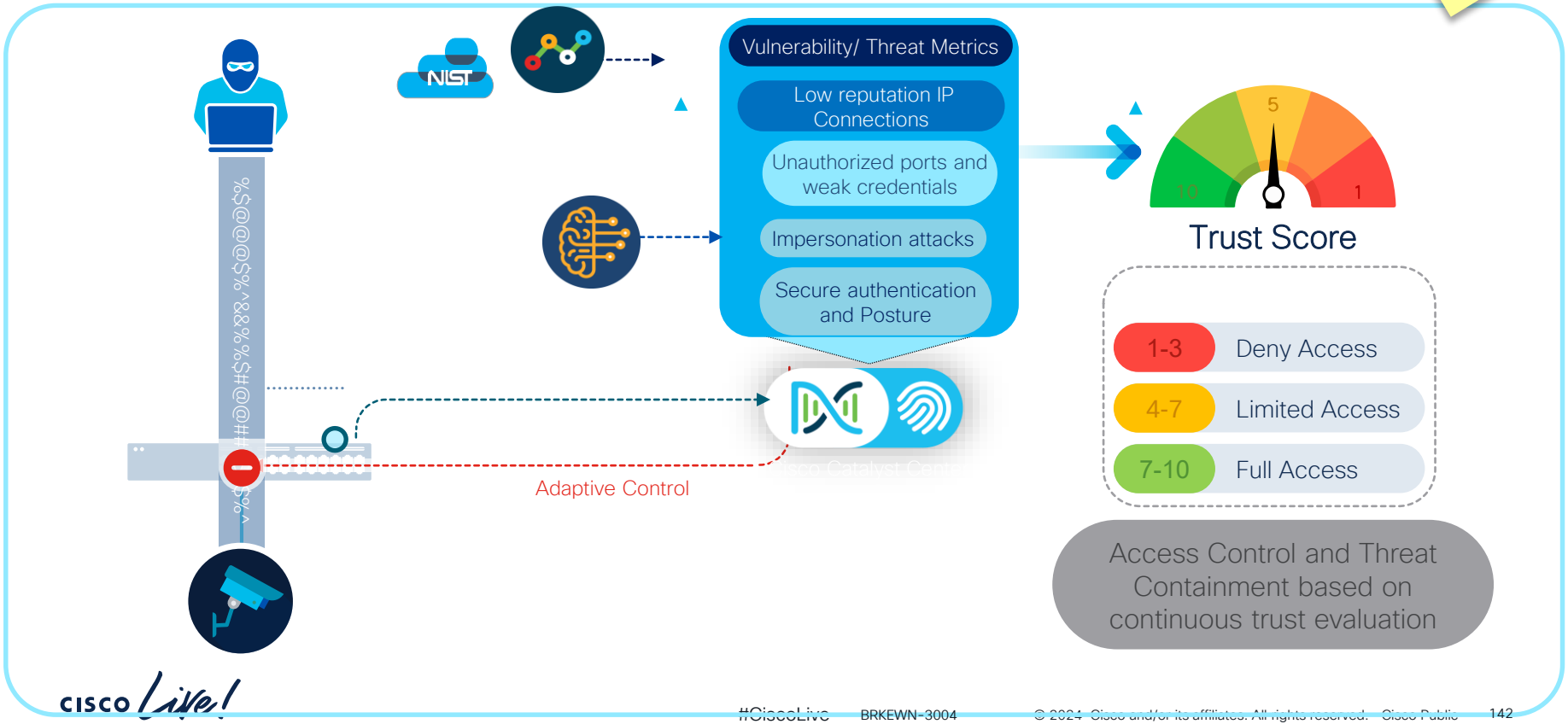
Immediate threat remediation

Use the network to remove the infected host by applying a relevant policy through Automated Response

Compromised Client



Trust Based Network Access




CISCO LOGIN
CISCO
TALOS
Software
Vulnerability Information
Reputation Center
Support
Incident Response
Careers
Blog
Podcasts
About
FYI
Reputation Lookup
Search by IP, domain, or network owner for real-time threat data.
Legitimate Email
Spam
Malware
Click on a marker to see more information.
Email Traffic Overview
As of: Mon Feb 12 2024 12:49:45 GMT+1100 (Australian Eastern Daylight Time)
Google
Keyboard shortcuts
Map data ©2024
500 km
Terms

2.2 Trillion

Threat Artifacts Analyzed Daily

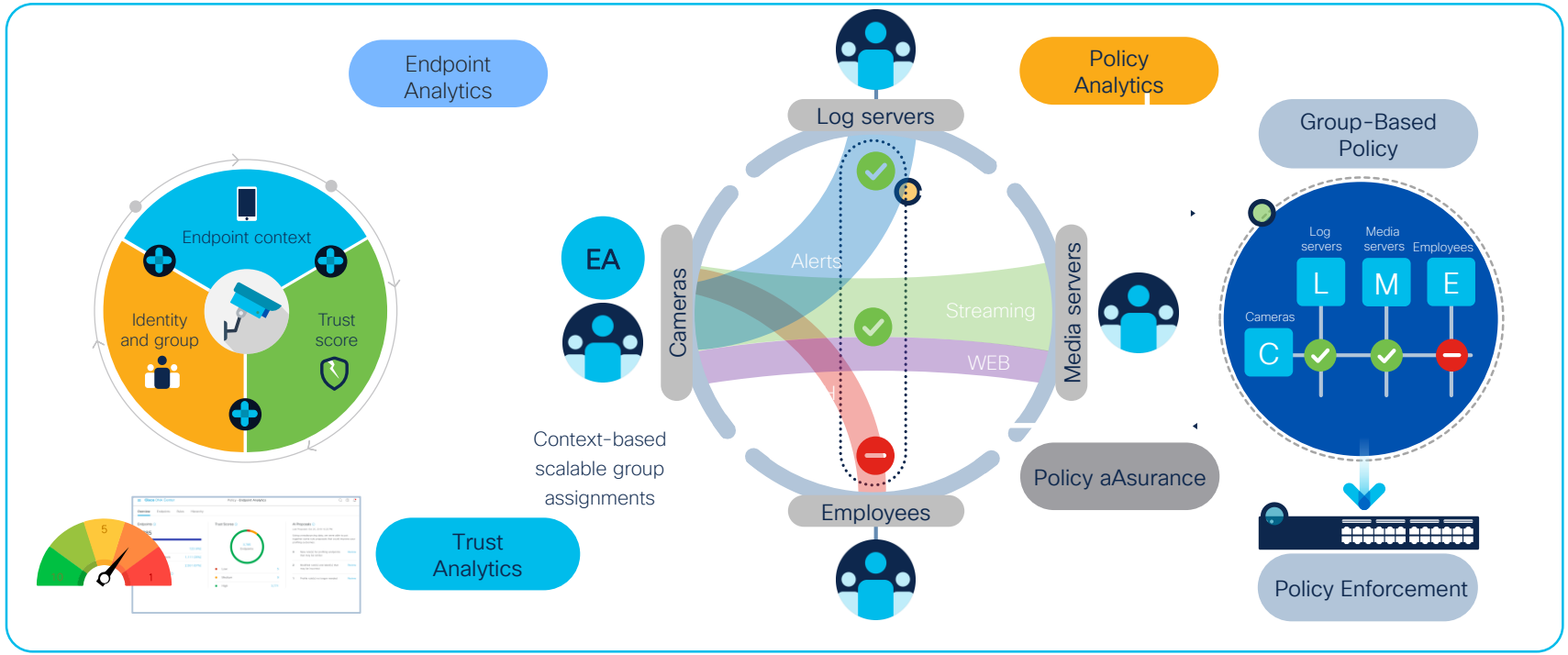
1.9T Email – 200B DNS Entries – 47B Web Redirects – 189M File Artifacts

11 Billion

Threat Responses Initiated Daily

6.7B Rejected Email – 2.7B URLs Blocked – 1.6B DNS Blocks - 100M Vulnerability Exploits
1M Malicious File Blocks – 100K File Convictions

Microsegmentation Based Security



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

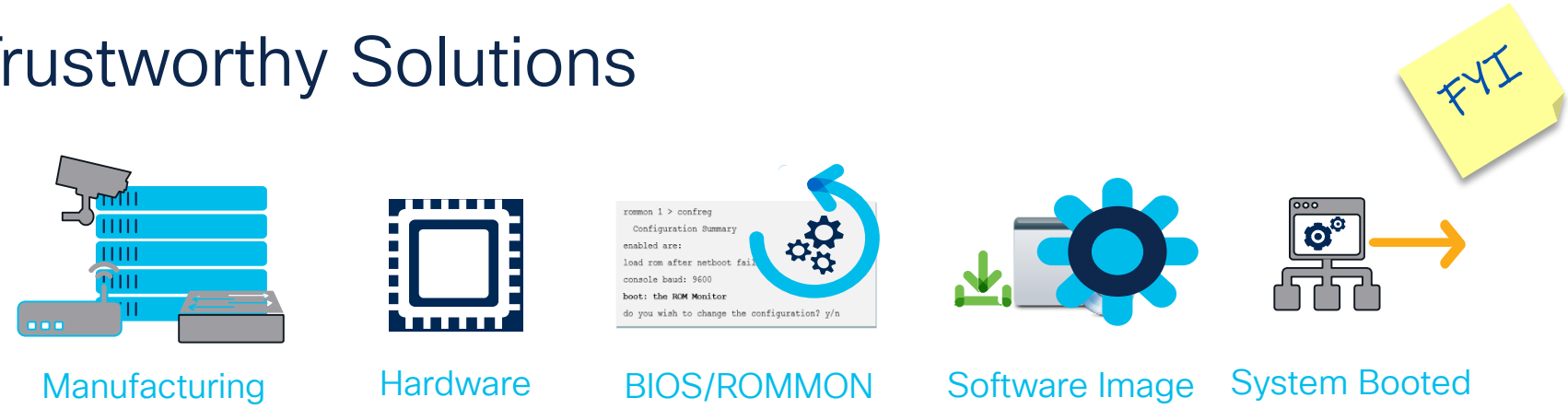
Secured Infrastructure with Trusted Platform

FYI

Secure Boot	With ACT2 chip
Image Signing	Authentic OS
Integrity Verifications	Malware Protection
SUDI Support	Two-way trust
Best-In Class Security	Automatic code encryption
Runtime Defenses	64 bit ASLR

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

Trustworthy Solutions



Cisco Secure Networking

Unauthorised access

Secure Access & Analytics

Zero-Trust Security

- Segmentation
- Policy Enforcement
- Cloud

Security Analytics

- Trust Analytics
- Endpoint Analytics

Ransomware

Secure Data

Traffic Analytics

- Malware Detection
- Umbrella DNS Security
- Compliance

Distributed Firewall

- ASAc on C9000

Eavesdropping

Secure Transport

MACSEC AES 256

- No wire-tapping
- No MITM
- Data Integrity

IPSEC

- 100G HW-based IPSEC
- All untrusted links

Counterfeiting

Secure Infrastructure

Cisco Trustworthy Solutions

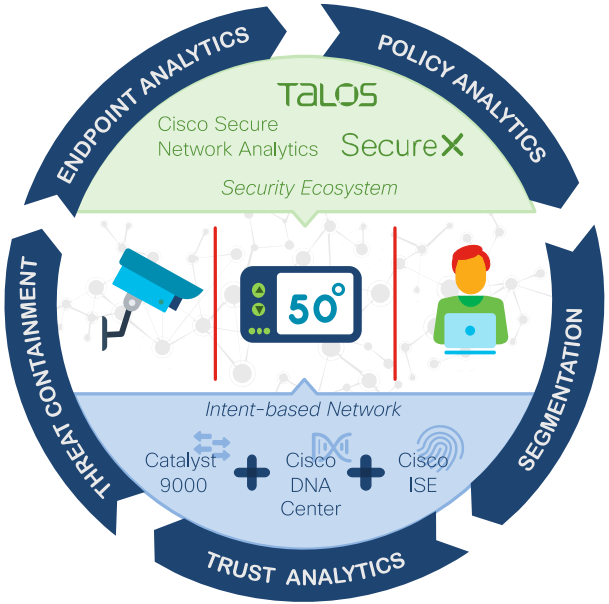
- 2 way trust
- Hardware Authenticity
- Run-time Defence

Securing the Wireless Network

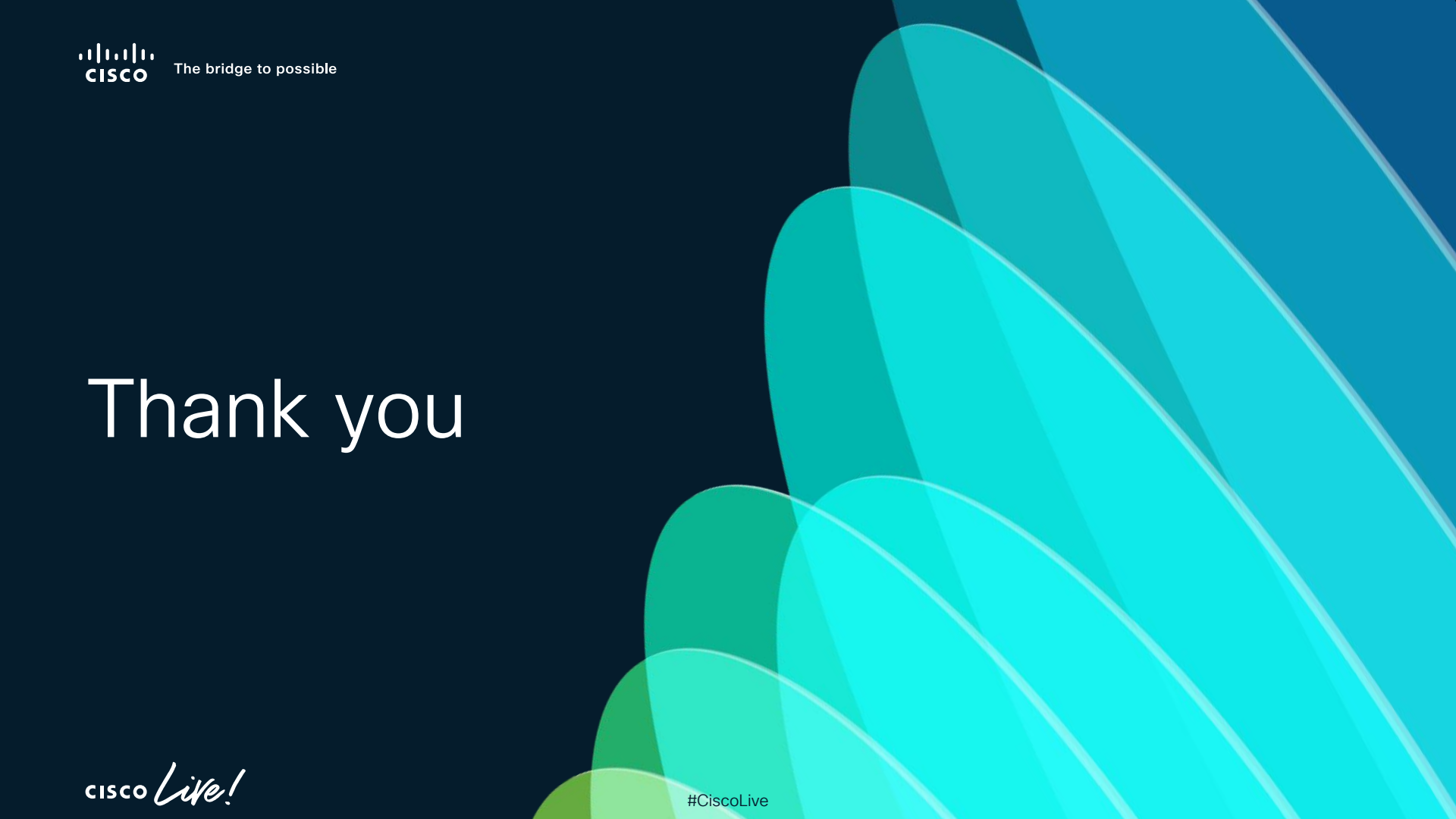
Secure the Air

Secure the Devices

Secure the Network



WPA3


The bridge to possible
Thank you
cisco Live!
#CiscoLive

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

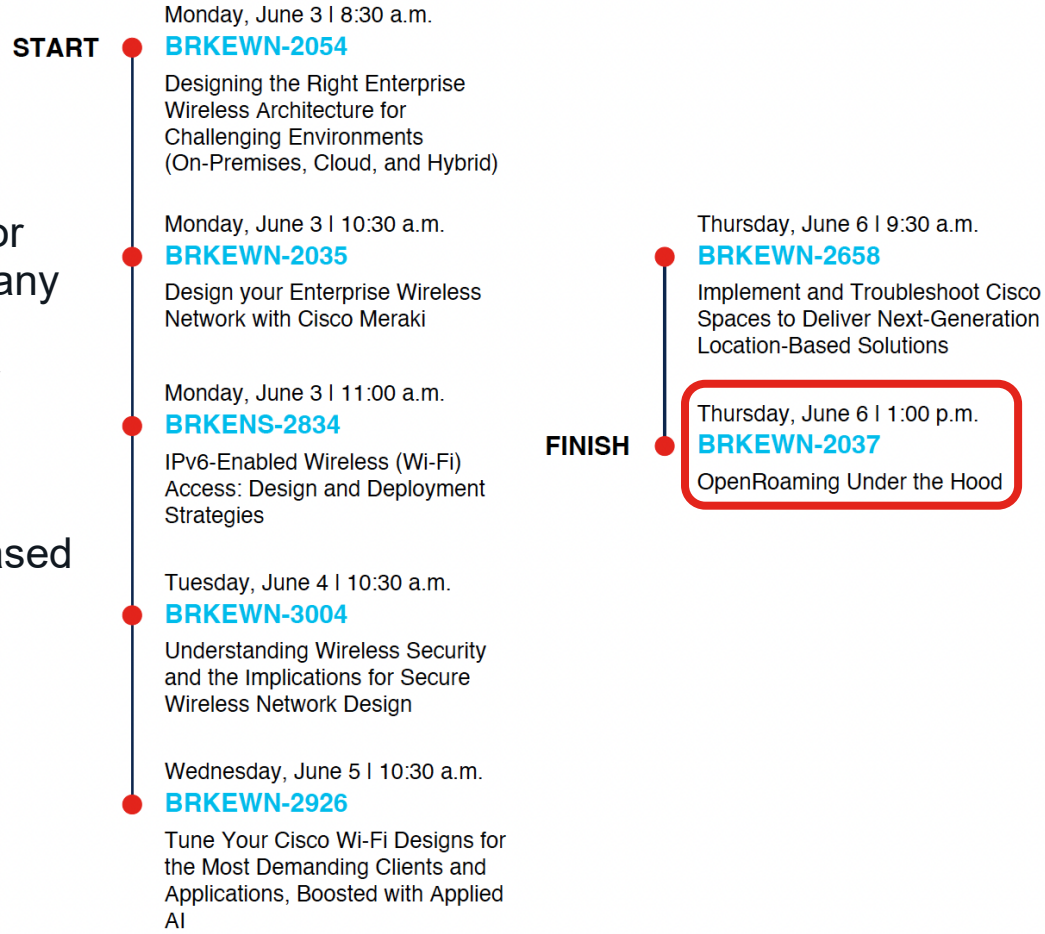
Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Networking

Secure Wireless Design

- Learn about design best practices for Cisco wireless solution, including many security optimizations. You will also learn about energy optimizations for Cisco Wireless deployments.
- Finally you will learn how to enable Smart Workspaces and locations based services that leverage your Cisco Wireless and BLE solution.



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