



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

## Questions?

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

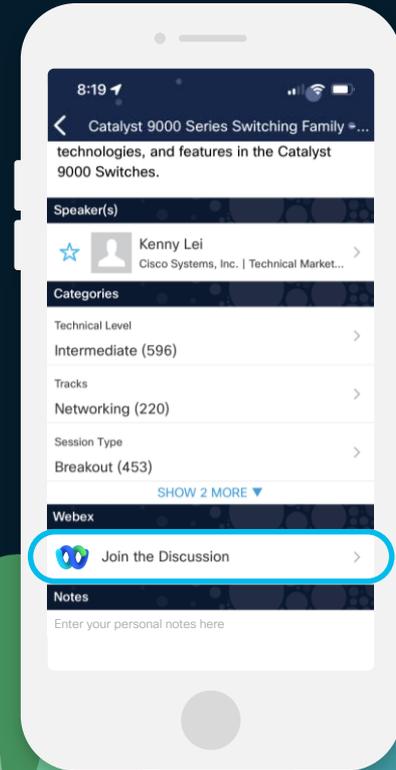
## How

- 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

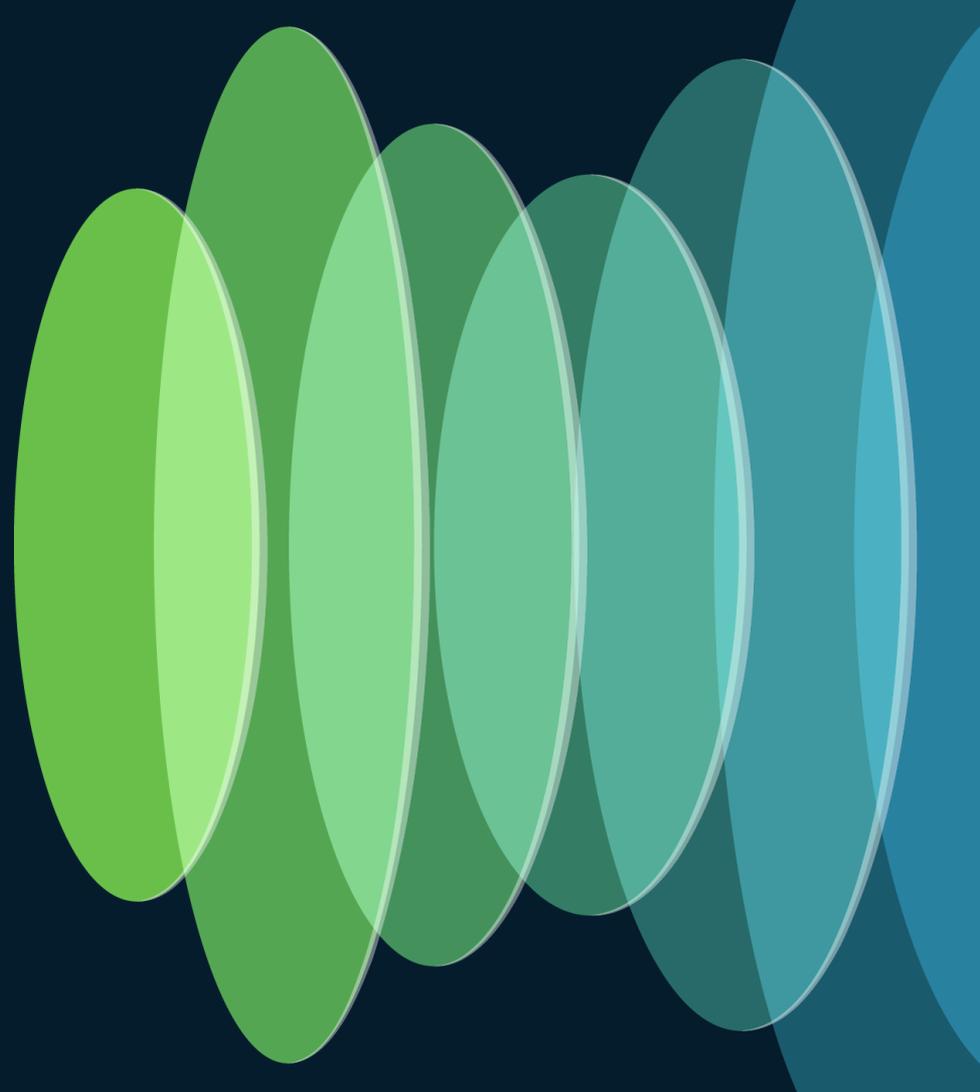
Webex spaces will be moderated by the speaker until June 7, 2024.

**CISCO** *Live!*

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



# Wireless Security Fundamentals



# 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

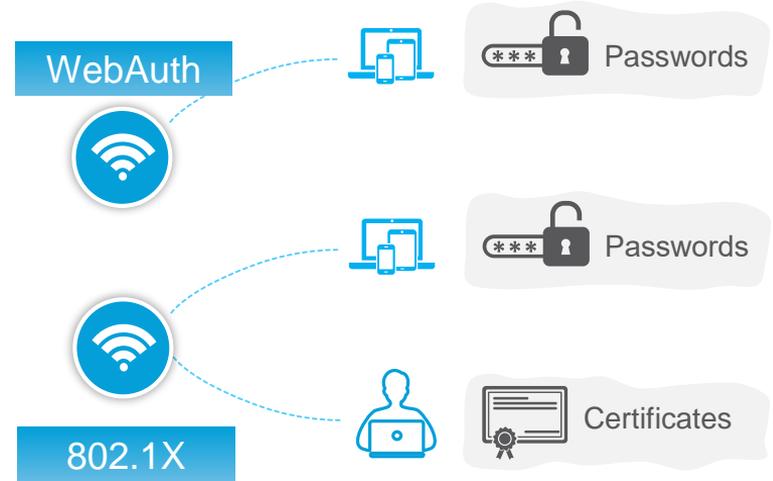
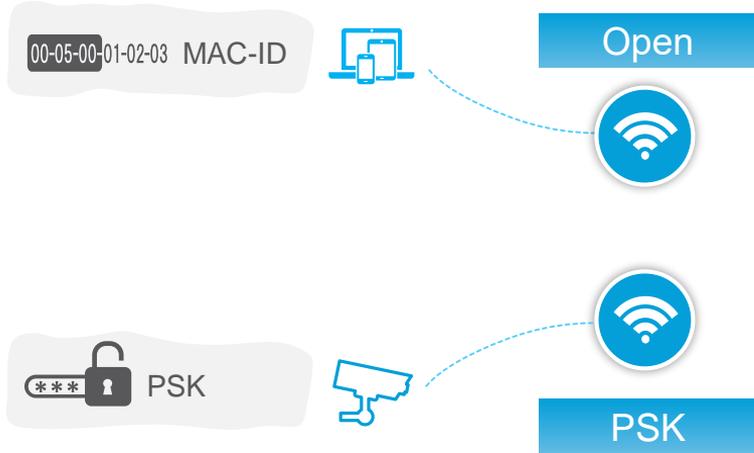
## 802.11w Protected Management Frames Mandatory

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)

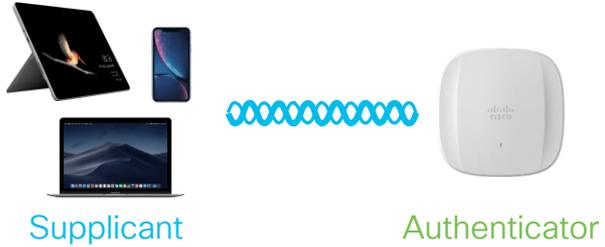
# 802.11 Fundamentals

## Authentication



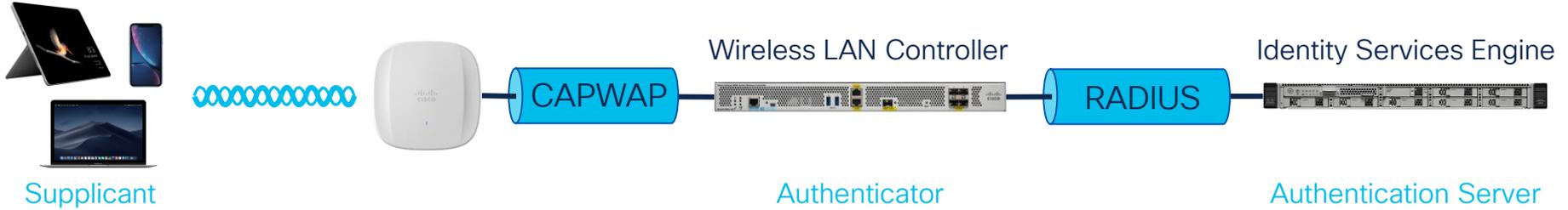
# 802.11 Fundamentals

## Authentication



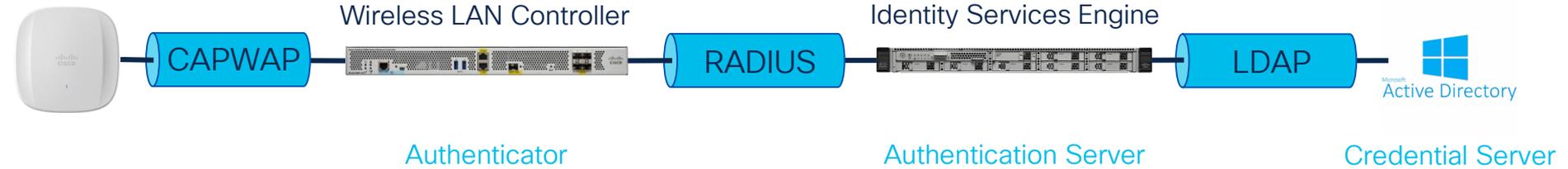
# 802.11 Fundamentals

## Authentication



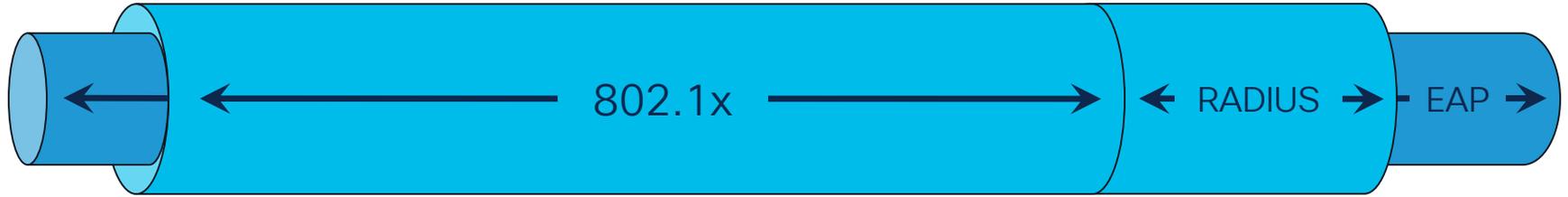
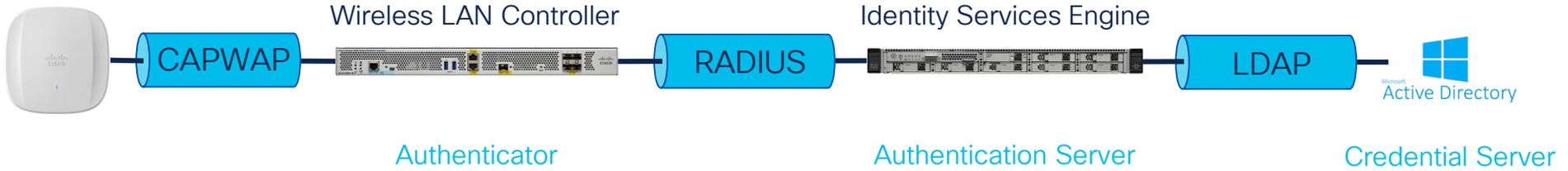
# 802.11 Fundamentals

- Authentication



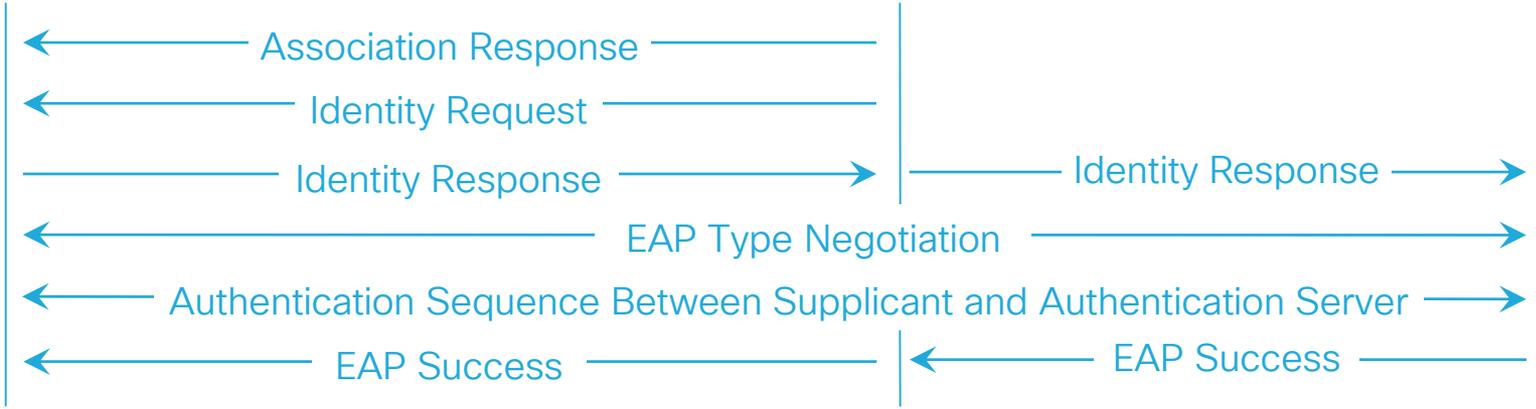
# 802.11 Fundamentals

## Authentication

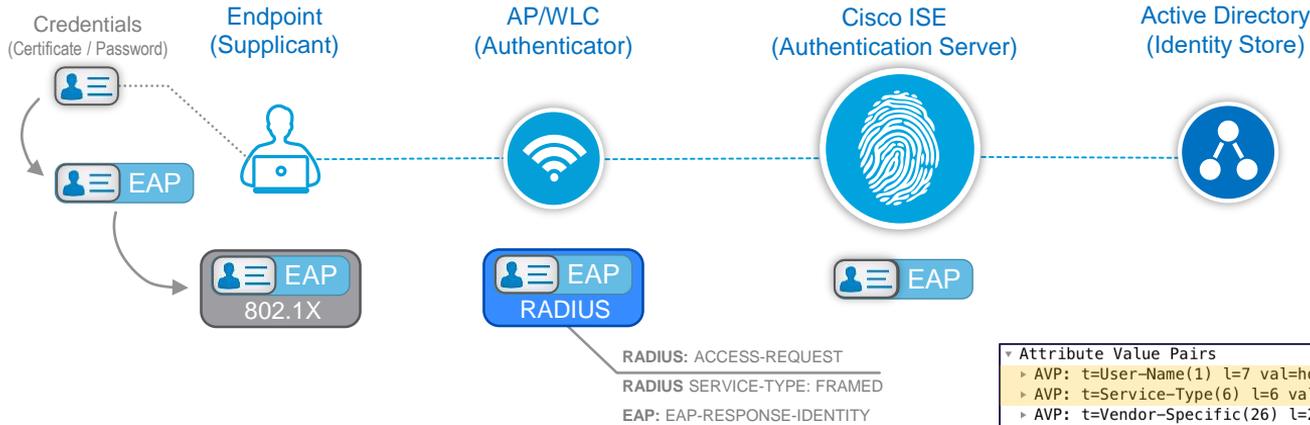


# 802.11 Fundamentals

## Authentication



# 802.1X



EAP: Extensible Authentication Protocol

```
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-D0T1X
  AVP: t=Calling-Station-Id(31) l=19 val=08:e6:89:2d:26:4d
  AVP: t=Vendor-Specific(26) l=12 vnd=Airspace, Inc(14179)
  AVP: t=Vendor-Specific(26) l=35 vnd=ciscoSystems(9)
  AVP: t=NAS-Identifier(32) l=10 val=C9800-CL
```

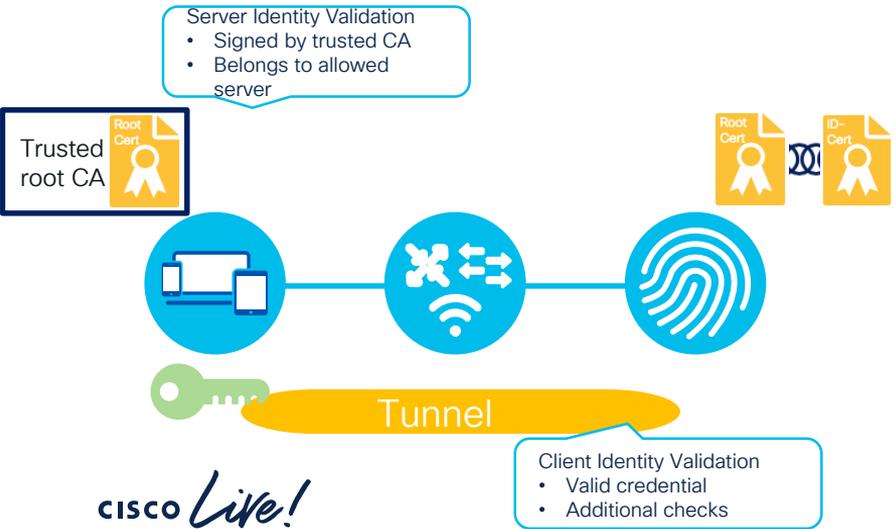
**Supplicant:** Software running on the client that provides credentials to the authenticator (Network Device).

# EAP-PEAP-MSCHAPv2 and EAP-TLS

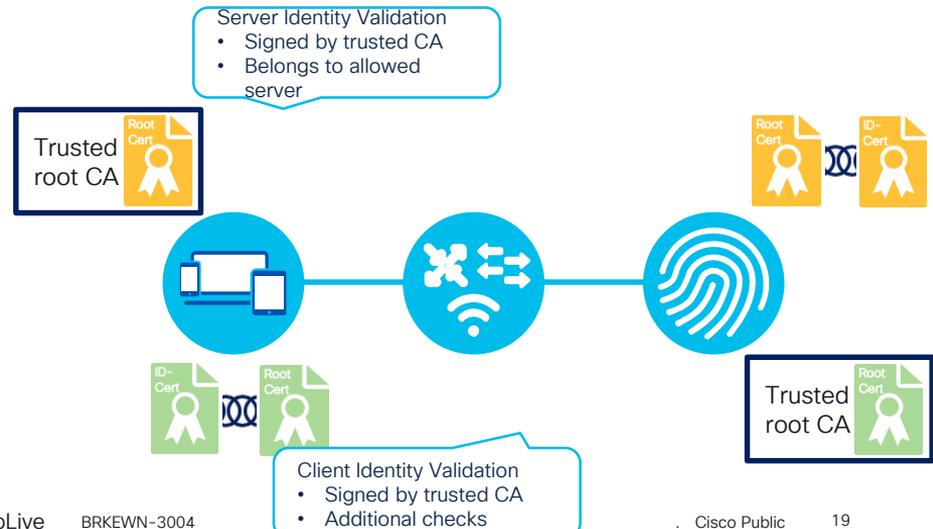


- Both: Use of server certificate
- EAP-TLS: Mutual certificate authentication
- EAP-PEAP: Use of tunnel to encrypt transport

## EAP-PEAP-MSCHAPv2

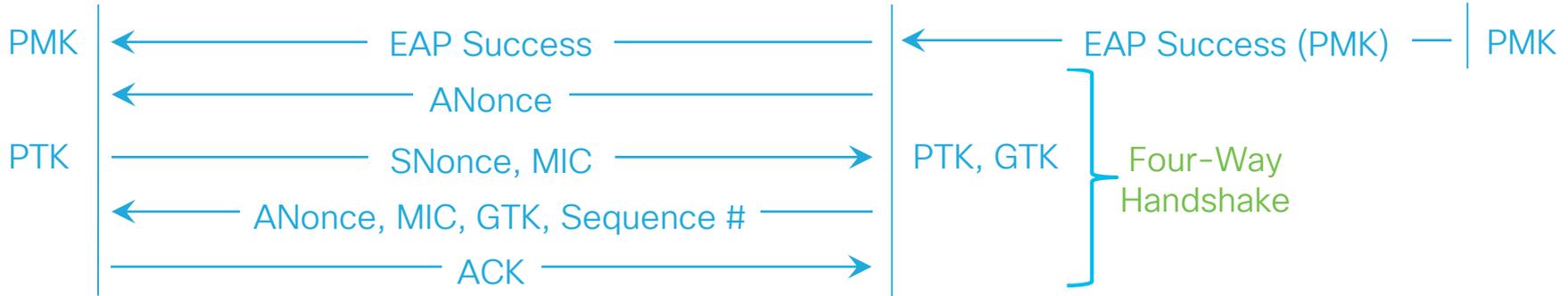
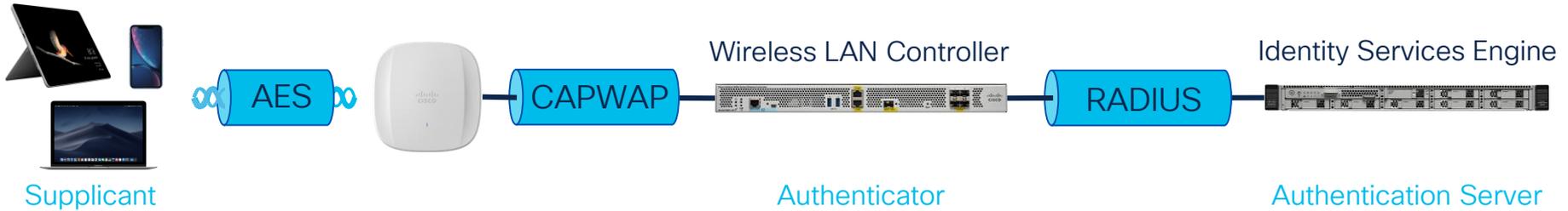


## EAP-TLS



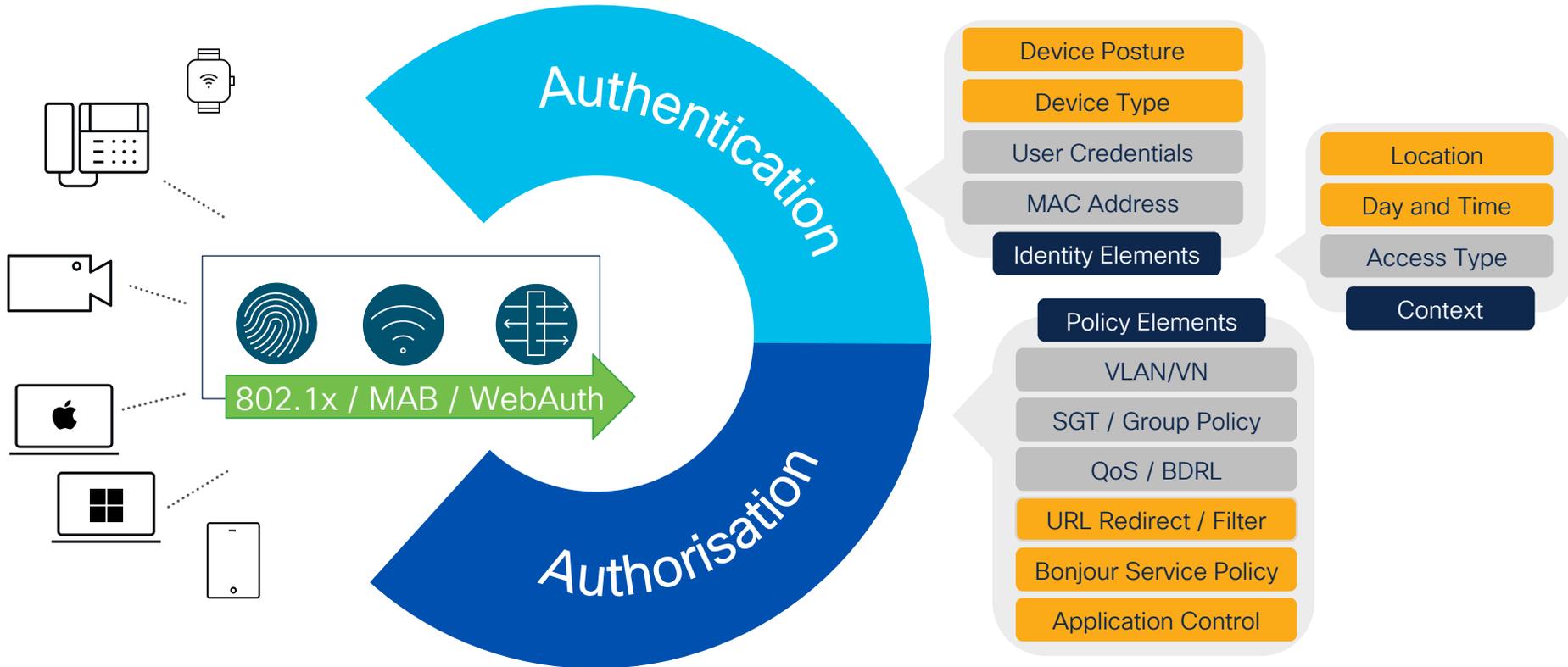
# 802.11 Fundamentals

## Encryption



$$\text{PTK} = \text{SHA}(\text{PMK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$$

# Authentication and Authorisation

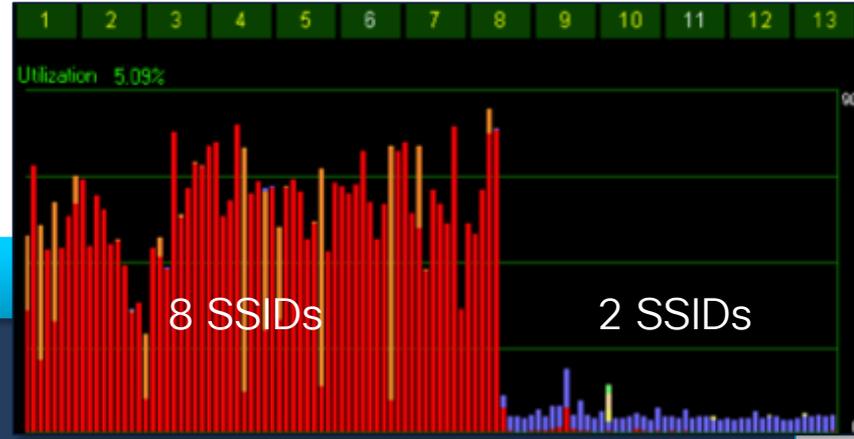


# Authorisation

## 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

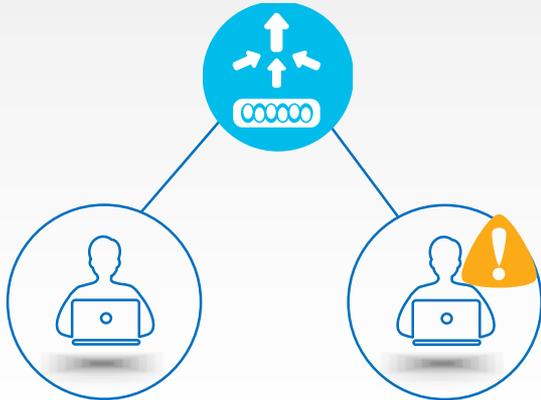
- Security based on TrustSec Scalable Group Tags instead of source and destination addresses
- ACLs applied at the packet level with enforcement across the network (or network fabric)

# Authorization Options



## Named ACL

Named ACL



**Healthy**

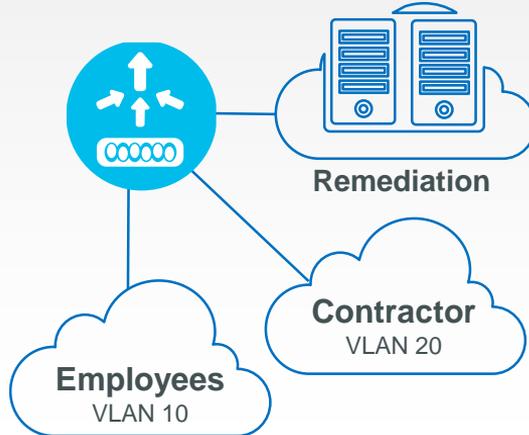
permit ip any any

**Non-compliant**

permit ip host <remediation>  
deny ip any any

## VLANs

Dynamic VLAN Assignments



**Employees**

VLAN 10

**Contractor**

VLAN 20

**Remediation**

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

```
vlan 10
name employee
vlan 20
name contractor
```



```
RADIUS: Access-Accept
Username = Peter
Tunnel-Private-Group-ID = 10
Tunnel-Type = VLAN
Tunnel-Medium-Type = 802
```

## VSA: AireSpace Interface Name

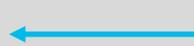
```
vlan 10
name employee
vlan 20
name contractor
```



```
RADIUS: Access-Accept
Username = Peter
AireSpace-Interface-Name
= employee
```

## Group policy

```
Group policy
Employee
Contractor
```



```
RADIUS: Access-Accept
Username = Peter
ACL Name = Employee
```

# 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	<input type="text" value="employee"/>	<input type="text" value="200,220,300-310"/>	✕

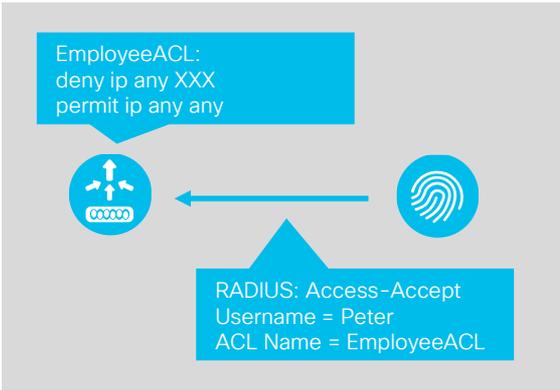
[Add a Named VLAN](#)

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

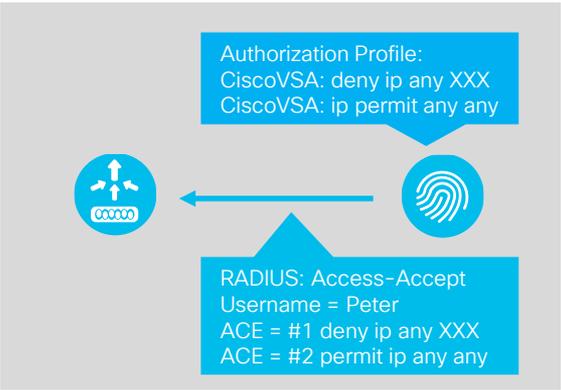
# RADIUS Enforced ACLs



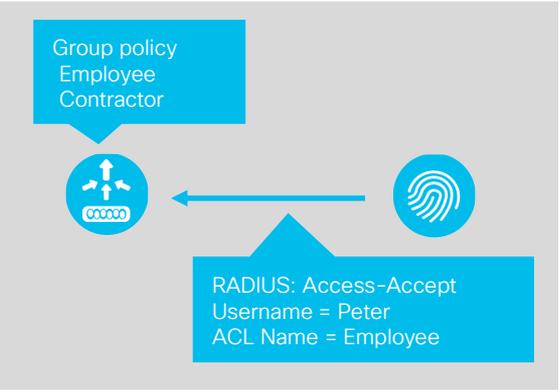
## Named ACL



## 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



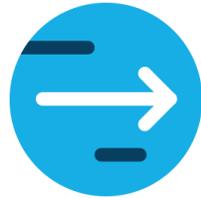
## Calendar Profile

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



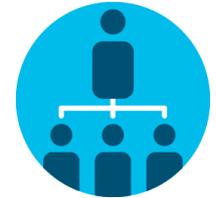
## mDNS Profile

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



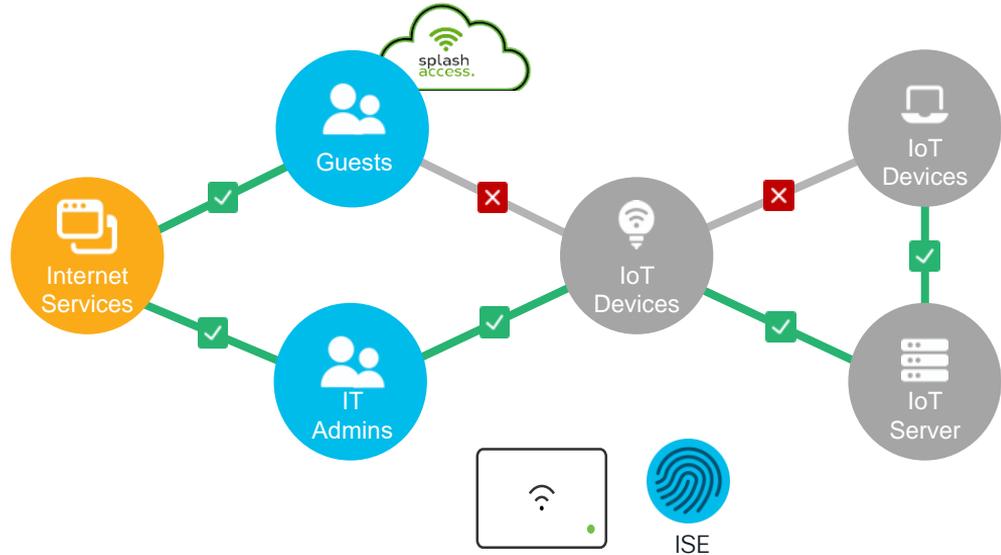
## Profiling & Posturing

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

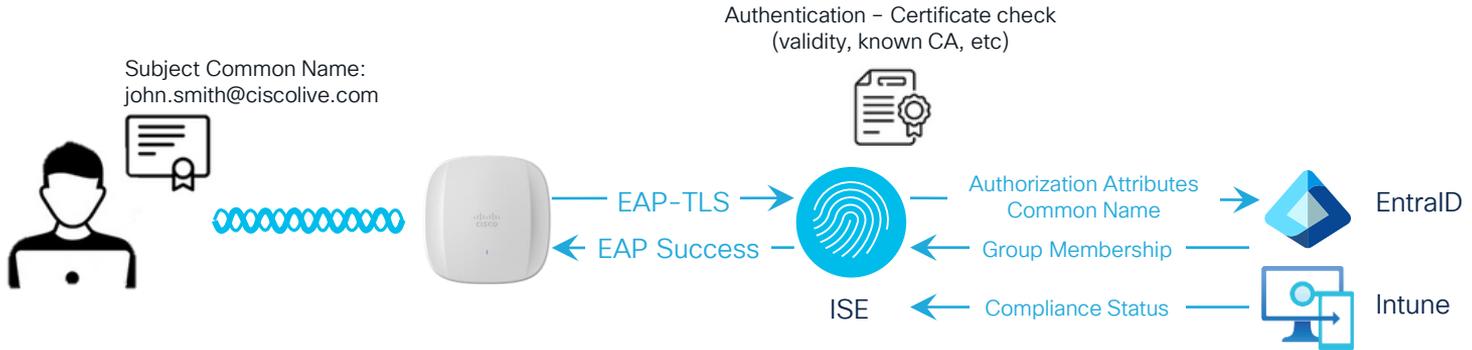
VPN, Application Access



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-h1d-76840754>

# ISE Personas

Standalone ISE Node



## Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all config changes



## Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes



## Policy Services Node (PSN)

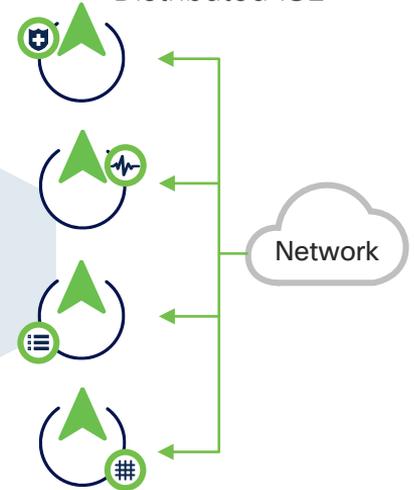
- Makes policy decisions
- RADIUS / TACACS+ Servers



## pxGrid Controller (PXG)

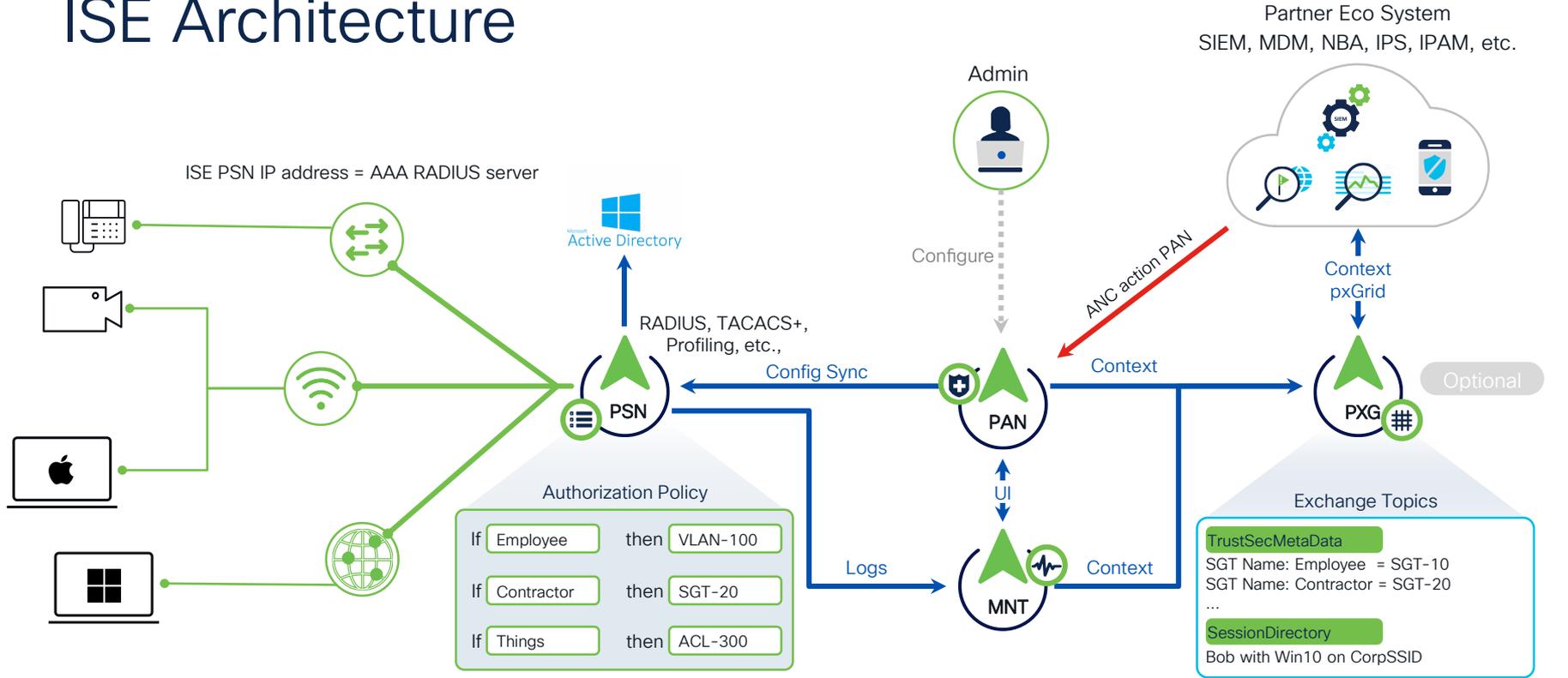
- Facilitates sharing of context

Distributed ISE



- 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

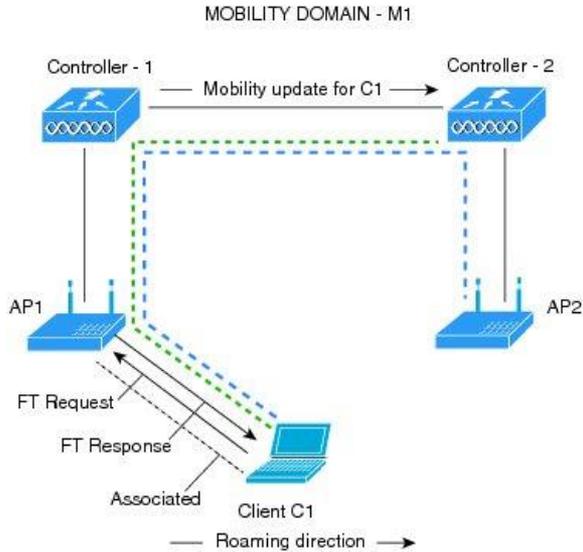
802.11k/v/r and Wi-Fi Agile Multiband



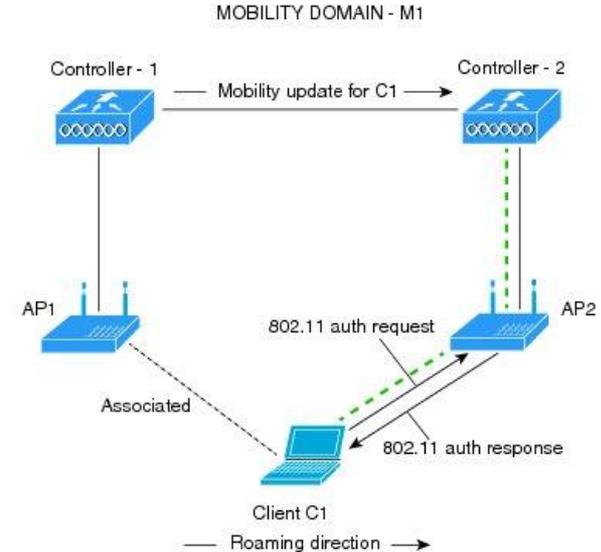
- Client channel scanning and AP selection
  - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
  - 802.11v BSS Transition

- 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

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

**WPA Parameters**

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input type="checkbox"/>		

**Fast Transition**

Status

Over the DS

Reassociation Timeout

**WPA2/WPA3 Encryption**

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

**Protected Management Frame**

PMF

**Auth Key Mgmt**

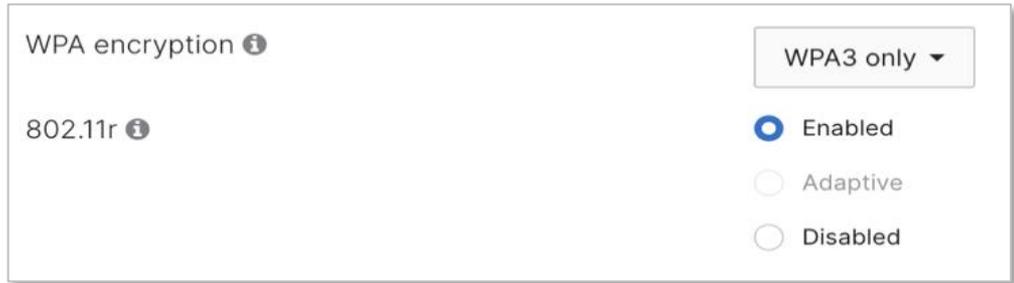
802.1x	<input type="checkbox"/>	PSK	<input type="checkbox"/>
CCKM	<input type="checkbox"/>	SAE	<input type="checkbox"/>
OWE	<input type="checkbox"/>	FT + 802.1x	<input checked="" type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>		

**MPSK Configuration**



# Secure Fast Roaming

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

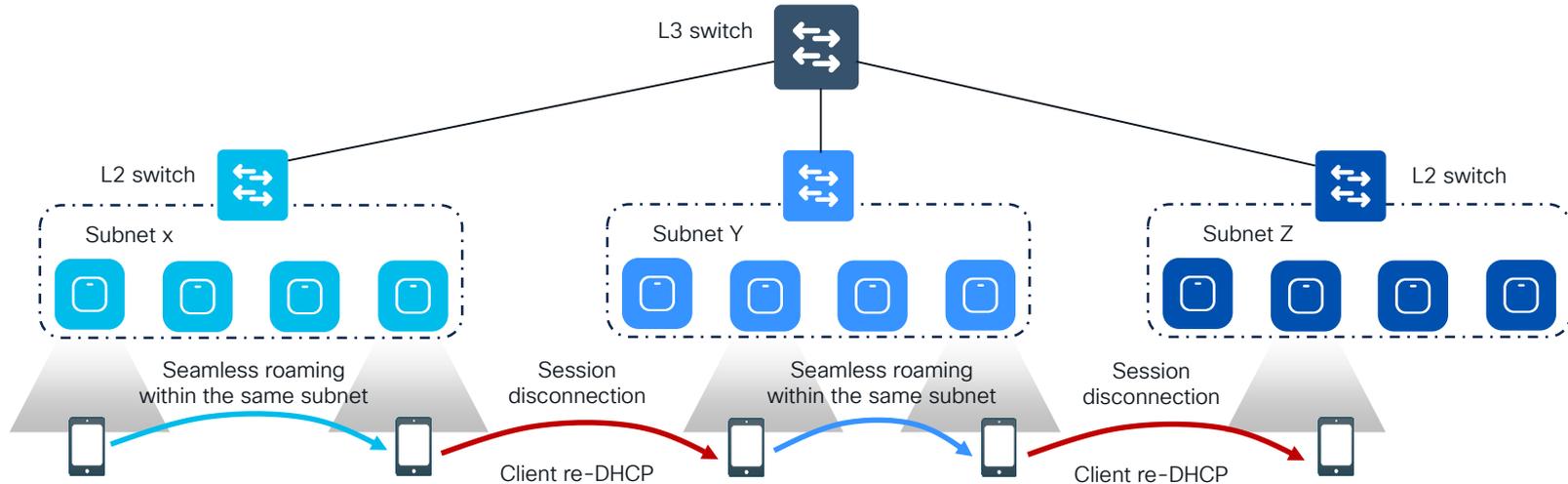


From MR 30

# Seamless Roaming at Scale

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

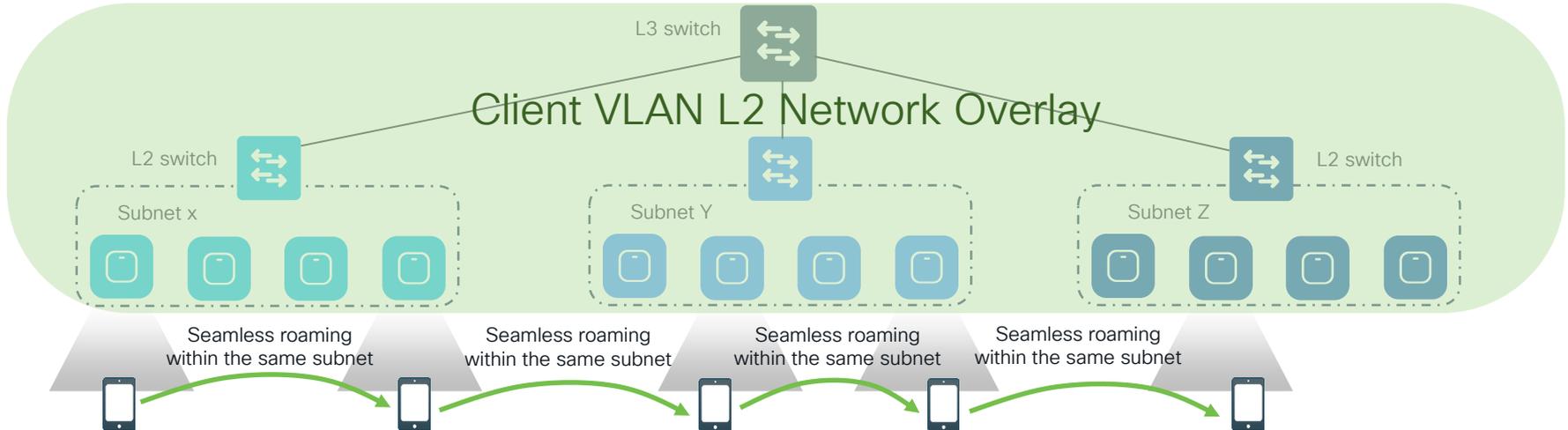
Large broadcast domains do not scale and is counter to networking best practice



# Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

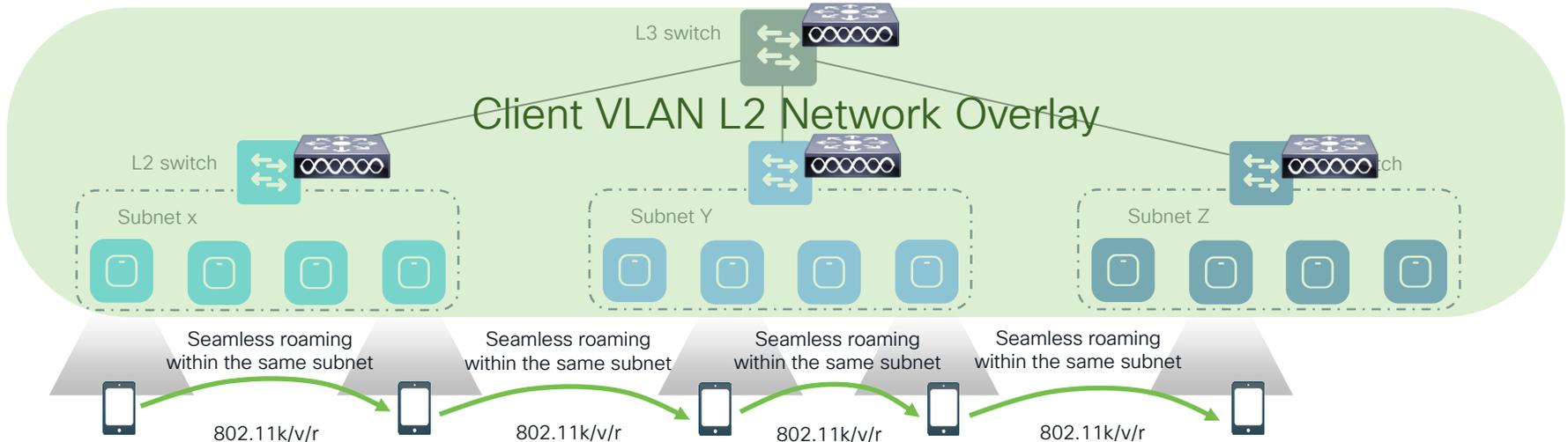
A data termination point is required to roam across L3 boundaries



# 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

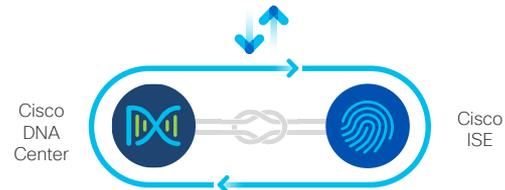
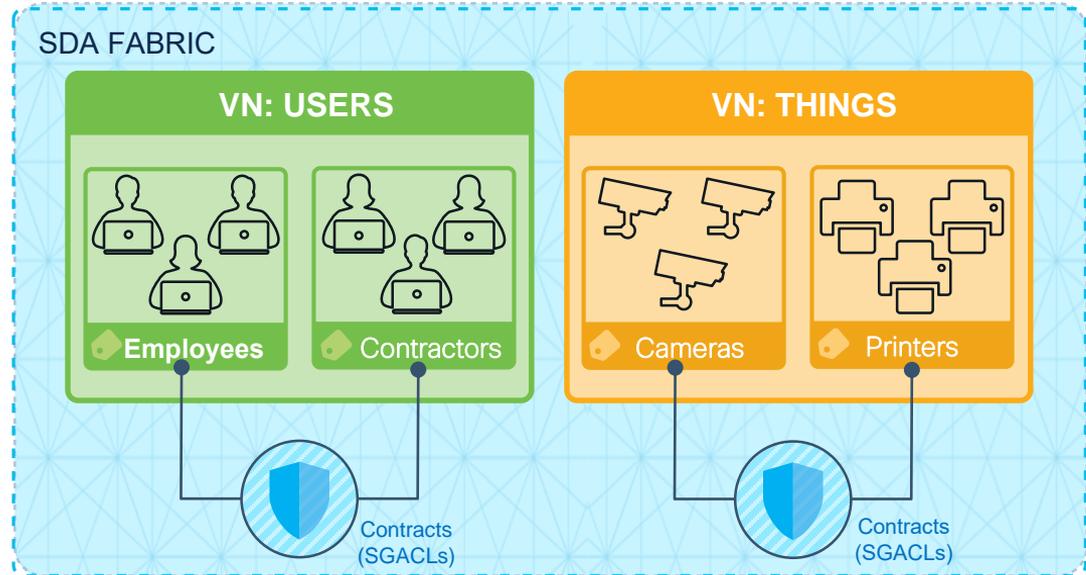


### Use cases

Network segmentation with 'Virtual Networks'

Group segmentation with 'Scalable Groups'

Fabric-Native Wireless



# Adaptive Policy & Secure Analytics

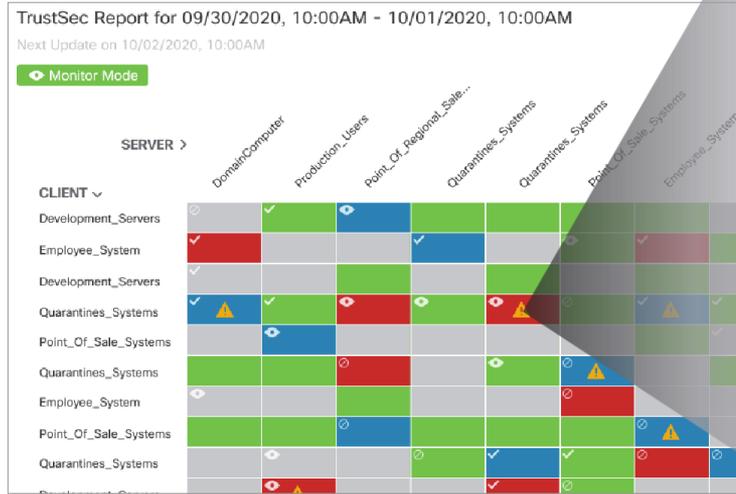
Informed Policy Creation and Validation



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



Group based policy and **traffic flow tracking**



**TRAFFIC INFORMATION**

Traffic Volume:  
Start: ...  
End: ...

**PROTOCOLS**

- ▲ ICMP (11KB) ...
- ▲ TCP (2.5GB) ...
- ▲ UDP (0.6MB) ...

**PORTS**

- 22/SSH (320MB) ...
- 80/HTTP (100MB) ...
- ▲ 443/HTTPS (2GB) ...
- ▲ 54180 (52MB) ...

[View Flows](#)  
[View Offending Traffic Flows](#)

**ISE DATA**

**ISE Policy**  
Enabled ✓

**SECURITY GROUP ACLS**

Name: DevProdCommunication  
IP Version: IP Agnostic  
ACEs: Deny IP  
permit tcp eq 80  
permit tcp eq 22



# 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](#)

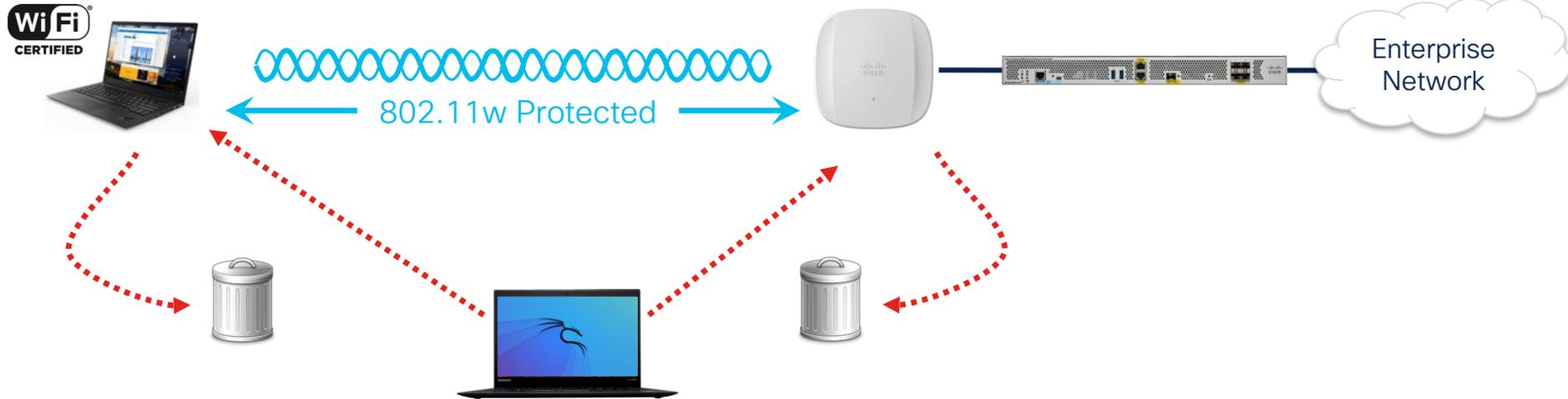
- This was an industry wide issue
  - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
  - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection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

# Kr00k Vulnerability



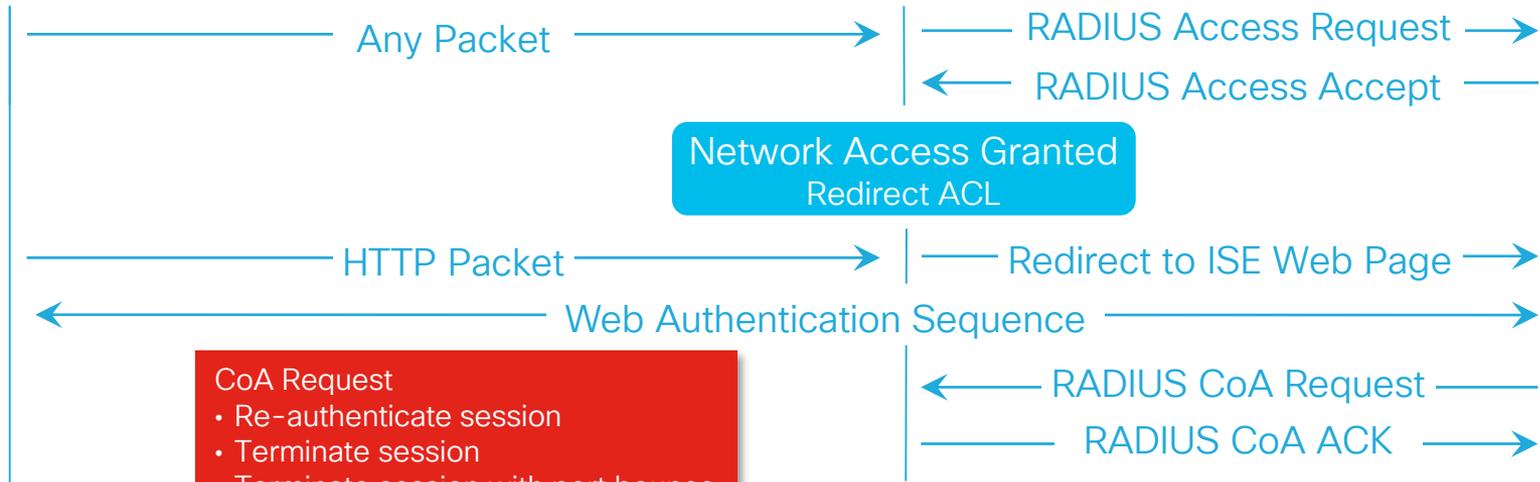
- On February 26th, 2020, researchers Štefan Svorencík and Robert Lipovsky [disclosed a vulnerability in the packet processing of certain Wi-Fi chipsets](#)
- This vulnerability could allow an unauthenticated, adjacent attacker to decrypt Wi-Fi frames without the knowledge of the PTK
- After an affected 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



# 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



Windows

- <http://www.msftncsi.com/ncsi.txt>



Google Devices

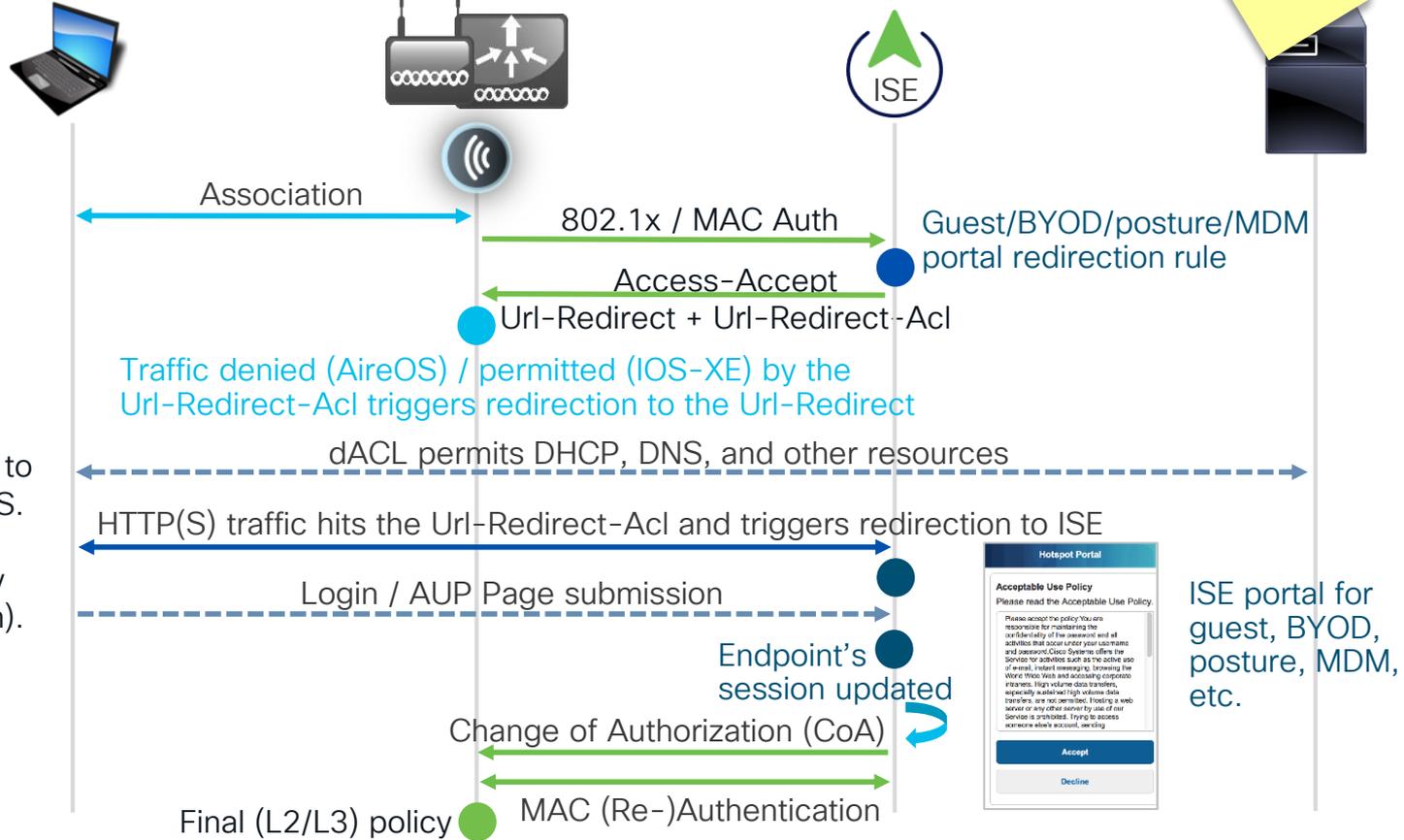
- [http://www.gstatic.com/generate\\_204](http://www.gstatic.com/generate_204)



Apple Devices

- <http://captive.apple.com/hotspot-detect.html>

# 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



**CISCO** My Devices Portal

Select an operation you would like to perform on your device.

Device status:  
Device name:  
Device ID:  
Description:

**Lost** **Stolen**

**Edit** **Delete**

**Close**

2  
Devices can be Blacklisted By the User.

1  
New Devices Can be Added with a Description

**CISCO** My Devices Portal

**Add Device**  
To add a new device, enter the device ID, which displays on your device as the MAC address. The device ID consists of 6 alphanumeric number pairs separated by colons such as AA:BB:CC:11:22:33.

Device name: \*

Device ID: \*

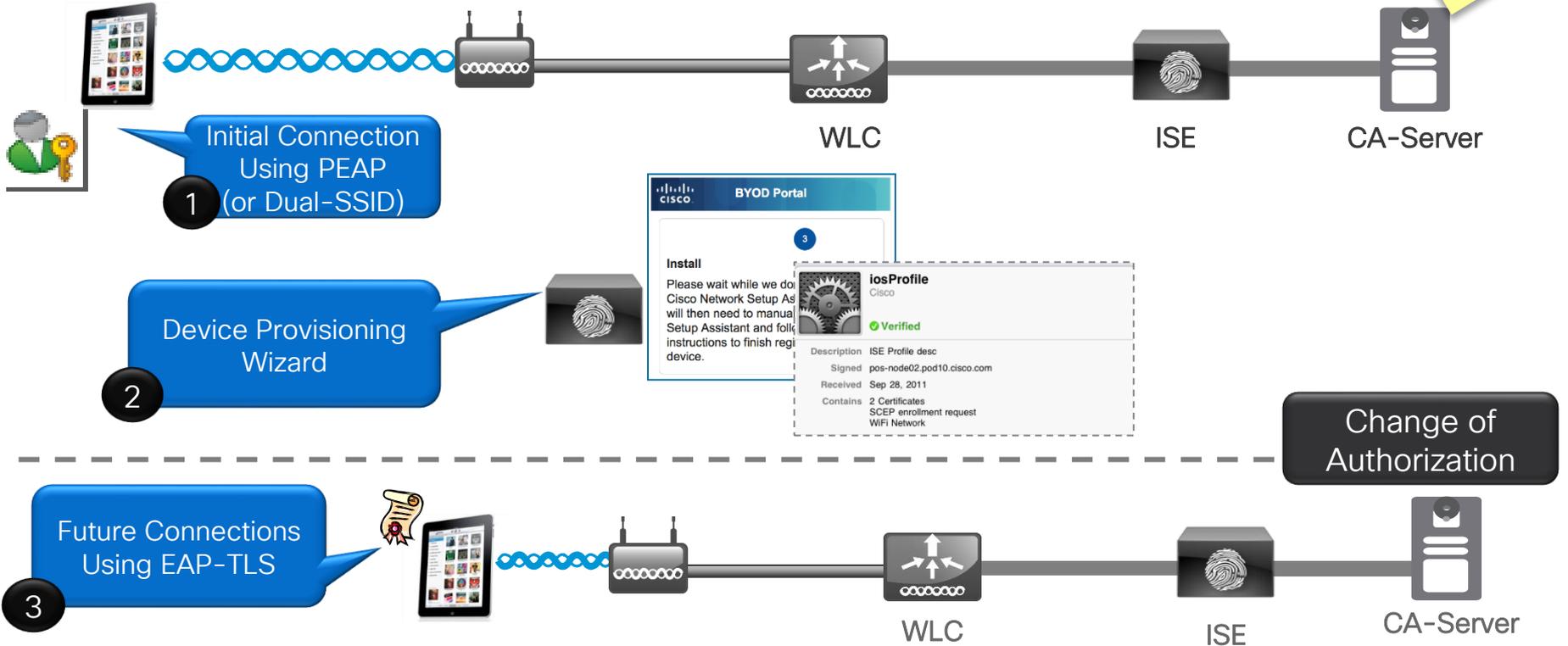
Description:

**Submit** **Cancel**

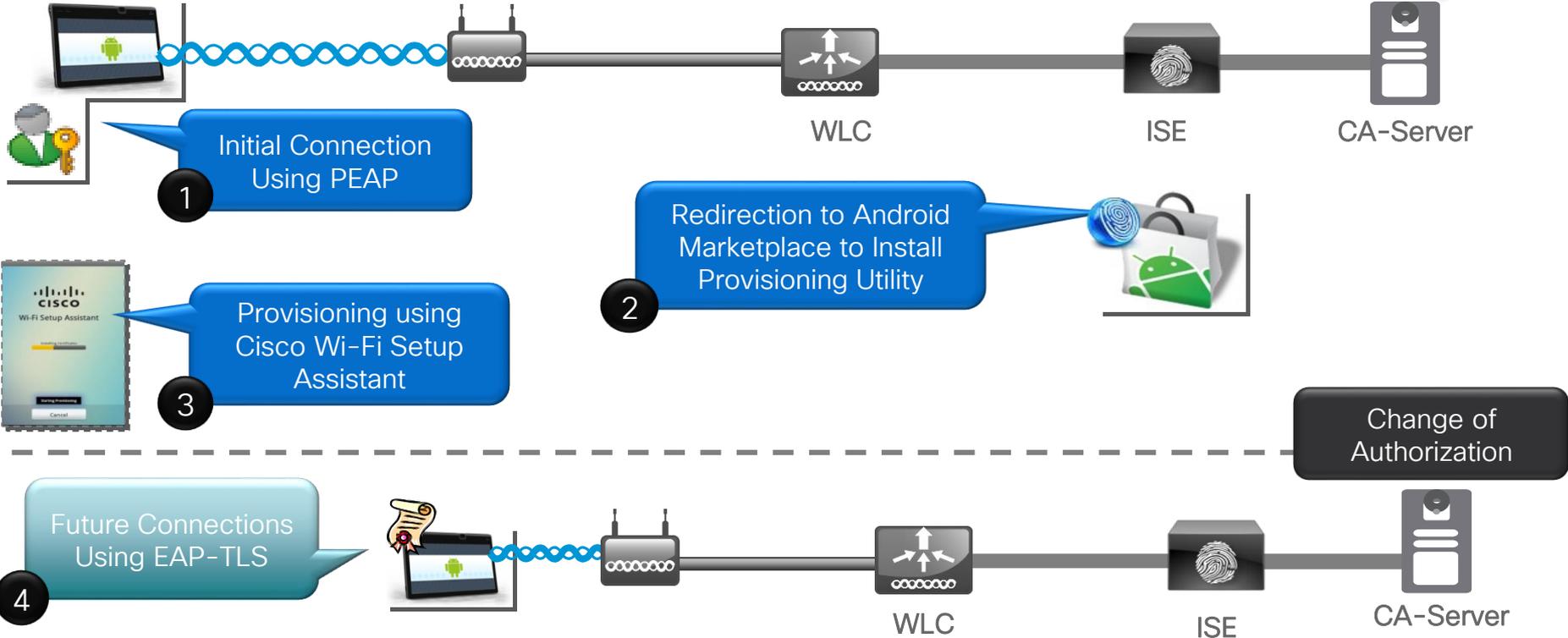
3  
Devices Can be Self-Registered, Up to an Administrator Defined Limit

# Client Provisioning

FYI



# Android Device Provisioning



# Client Provisioning Policy



## 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
<input checked="" type="checkbox"/> IOS	If Any and	Mac iOS All	AD1:ExternalGroups EQUALS cts.I...	WiFi_Profile
<input checked="" type="checkbox"/> Android	If Any and	Android	AD1:ExternalGroups EQUALS cts.I...	WiFi_Profile
<input checked="" type="checkbox"/> WinThings	If Any and	Windows...	AD1:ExternalGroups EQUALS cts.I...	WinSPWizard 1.0.0.14 And WiFi_Profile
<input checked="" type="checkbox"/> MAC-OSX	If Any and	Mac OSX	AD1:ExternalGroups EQUALS cts.I...	MacOsXSPWizard 1.0.0.6 And WiFi_Profile

# MDM Integration

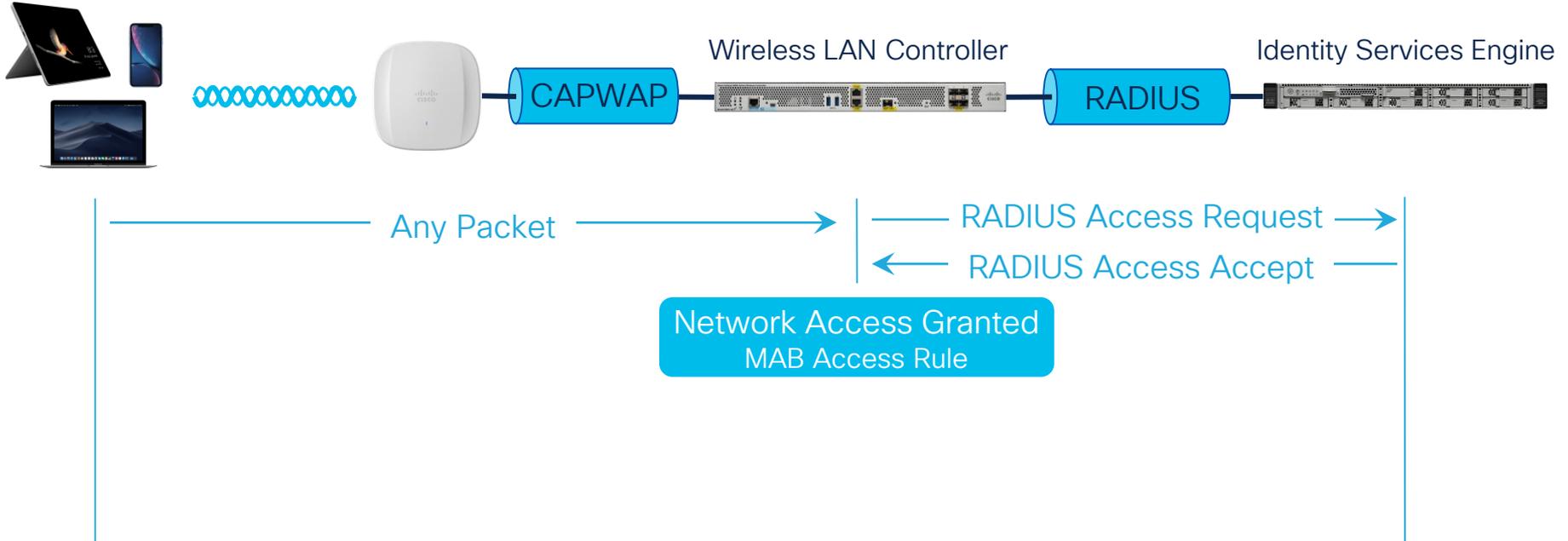


MobileDevice_Compliant	if <b>RegisteredDevices</b> AND ( MDM:DiskEncryptionStatus EQUALS On AND MDM:PinLockStatus EQUALS On AND MDM:JailBrokenStatus EQUALS Unbroken )	then Employee_MobileDevice
MobileDevice_Unregistered	if <b>RegisteredDevices</b> AND <b>MDM:DeviceRegisterStatus EQUALS UnRegistered</b>	then MDM_Registration
MobileDevice_NonCompliant	if <b>RegisteredDevices</b> AND ( MDM:DiskEncryptionStatus EQUALS Off OR MDM:PinLockStatus EQUALS Off OR <b>MDM:JailBrokenStatus EQUALS Broken</b> )	then MDM_NonCompliance

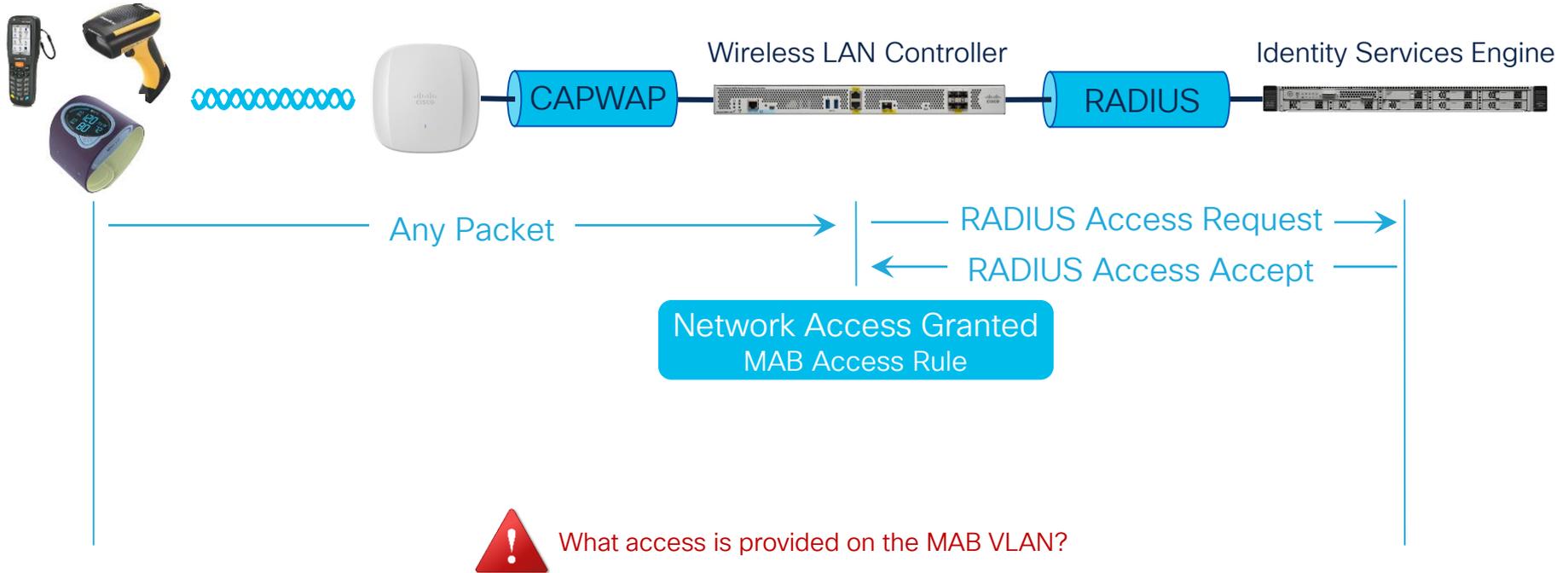


# Central Web Authentication

## MAC Authentication Bypass



# MAC Authentication Bypass



What access is provided on the MAB VLAN?

# Wi-Fi Certified Easy Connect

## WPA3



## Device Provisioning Protocol (DPP)

- 3 Phases

- Bootstrapping

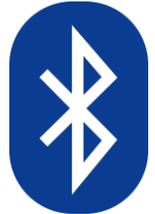
- Obtains the public key of new device

- Authentication and Provisioning

- Public key is used to create a secure tunnel for credential exchange

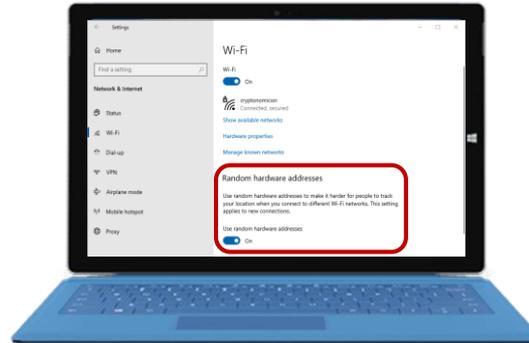
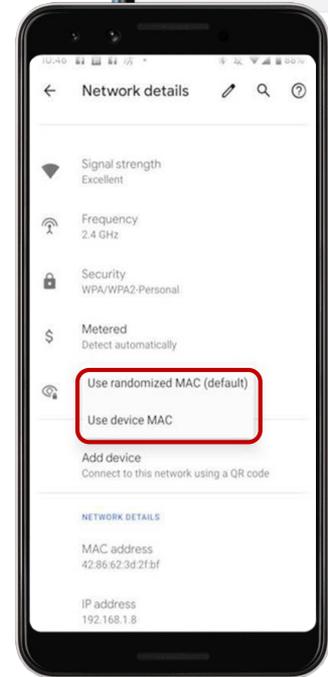
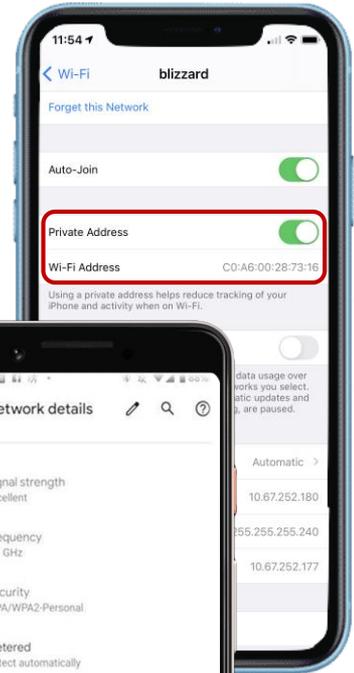
- Network Access

- 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



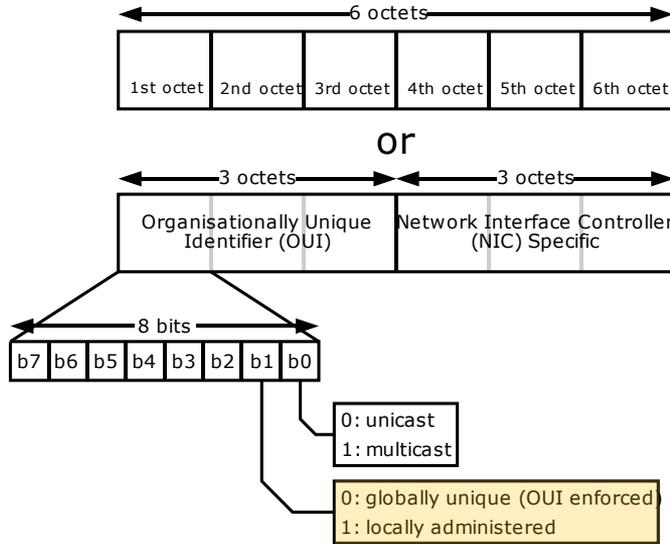
	Windows 10+	Android 10+	iOS 14+, iPadOS 14+, watchOS 7+
Randomization enabled by default	No	Yes	Yes
Same random MAC used for subsequent connection	Yes	Yes	Yes
Randomization saved between device reboot	Yes	Yes	Yes
Random MAC saved when Wi-Fi profile recreated	No	Yes	Yes
Randomization per day and/or per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



 <p>Profiling</p>	 <p>BYOD</p>	 <p>Whitelisting</p>	 <p>MDM Flow</p>	 <p>Guest</p>
 <p>Location lookup</p>	 <p>User Defined Network</p>	 <p>Endpoint Analytics</p>	 <p>Forensics</p>	 <p>Quarantine</p>

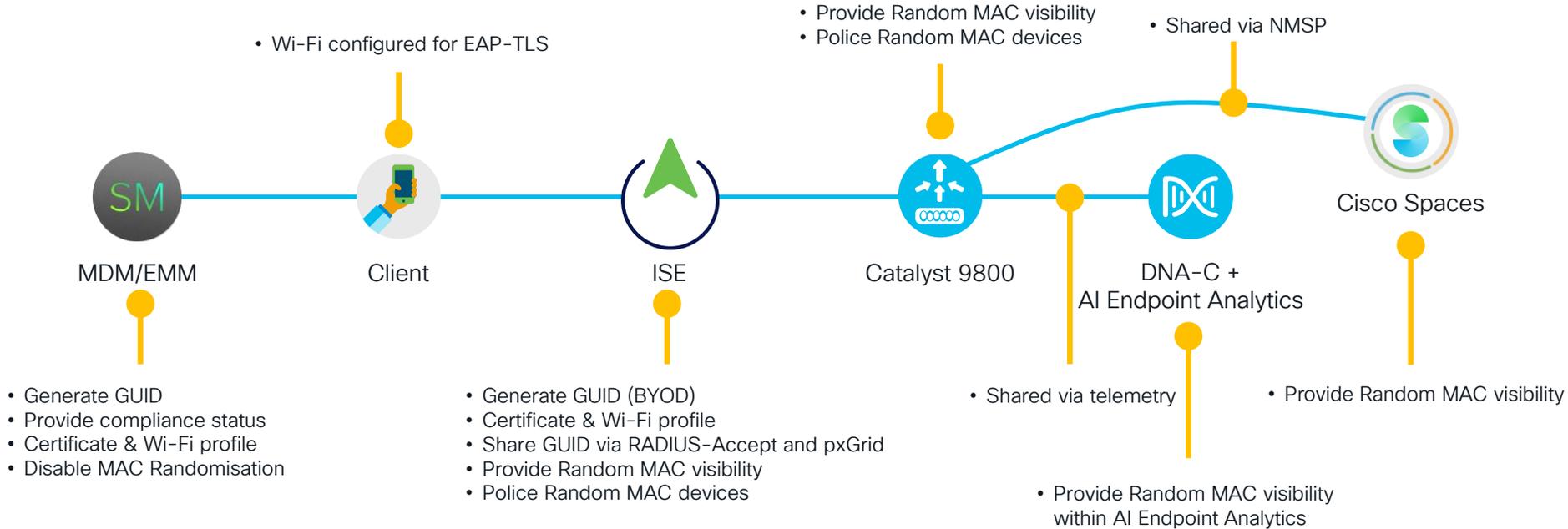
# Detecting Random MAC Addresses



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>

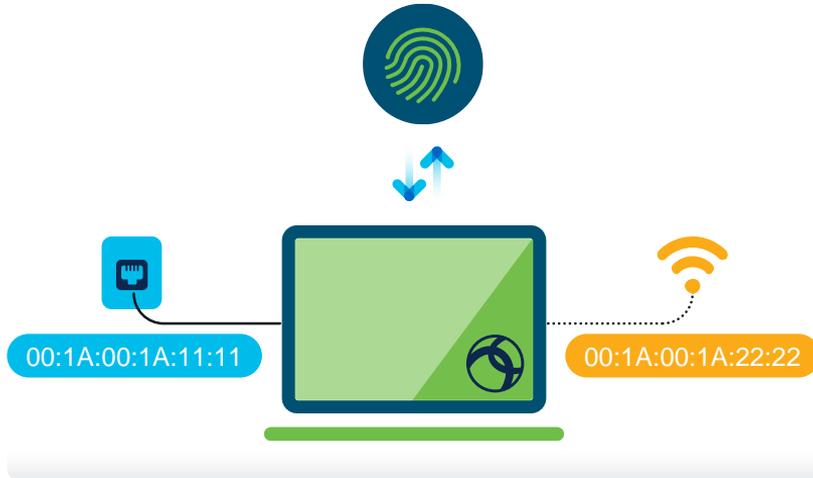
# Addressing Random MAC Issues



# Unique Device Identifier

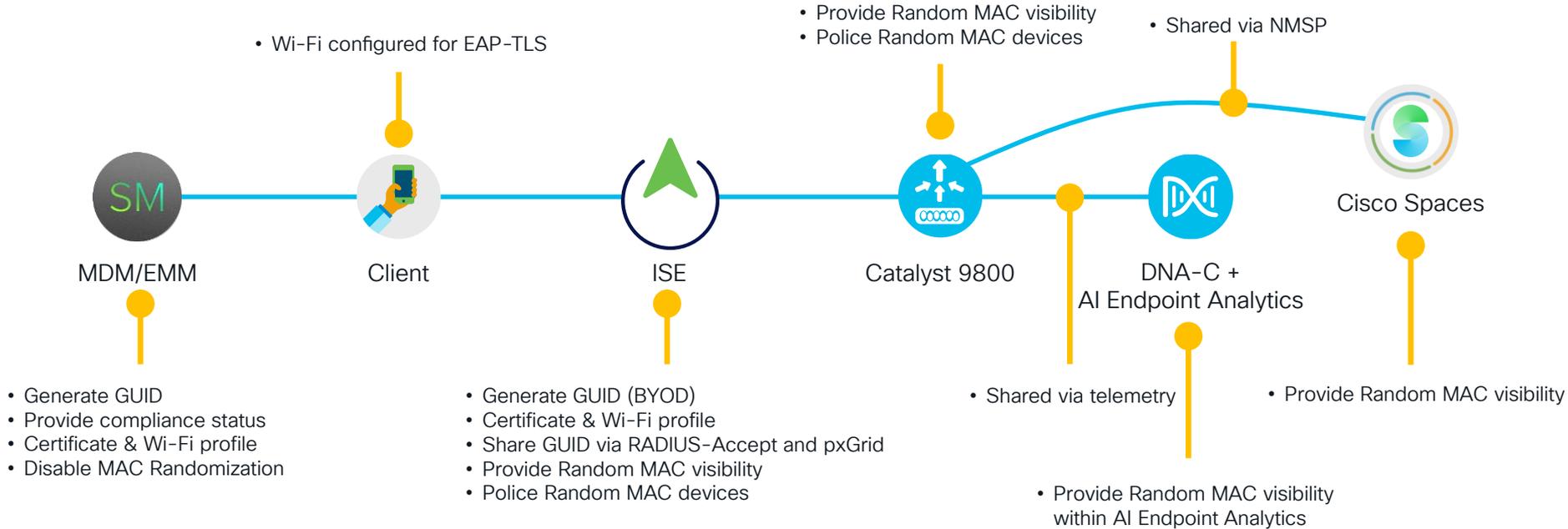


UDID	MAC Address(s)	Compliance
01669b65...05ee93	00:1a:00:1a:11:11 00:1a:00:1a:22:22	✓



- 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 and AnyConnect 4.7

# Globally Unique Identifier



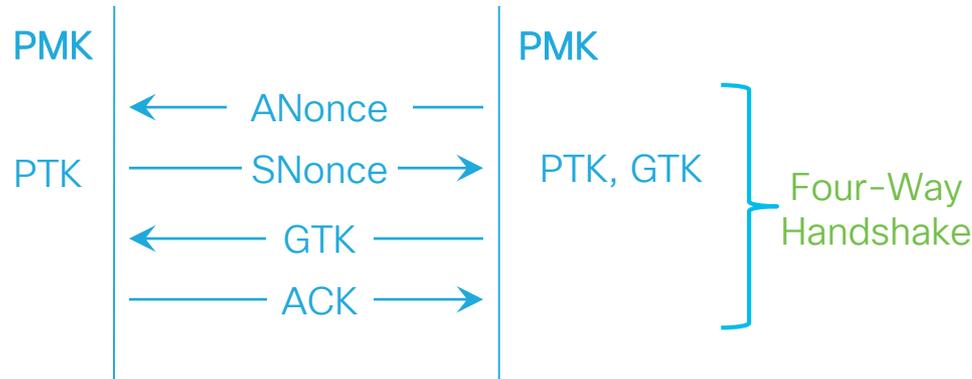
# WPA Personal

## Pre-Shared Key



# WPA Personal

## Pre-Shared Key

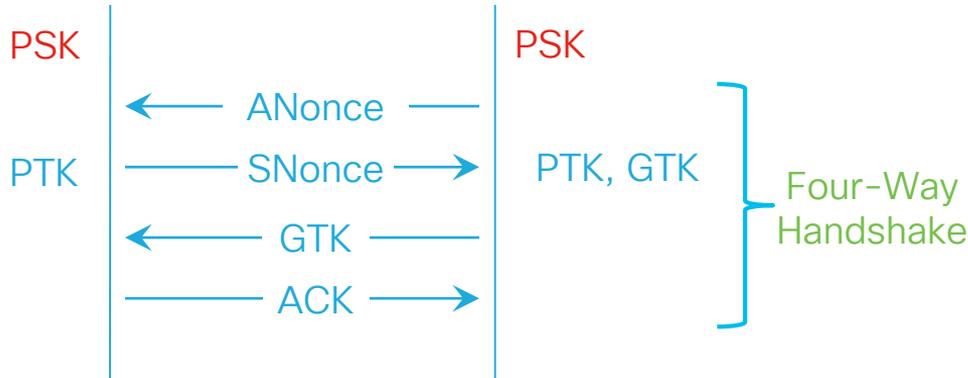


$$\text{PTK} = \text{SHA}(\text{PMK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$$

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

# WPA Personal

## Pre-Shared Key



$PTK = \text{SHA}(\text{PSK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$

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



# 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

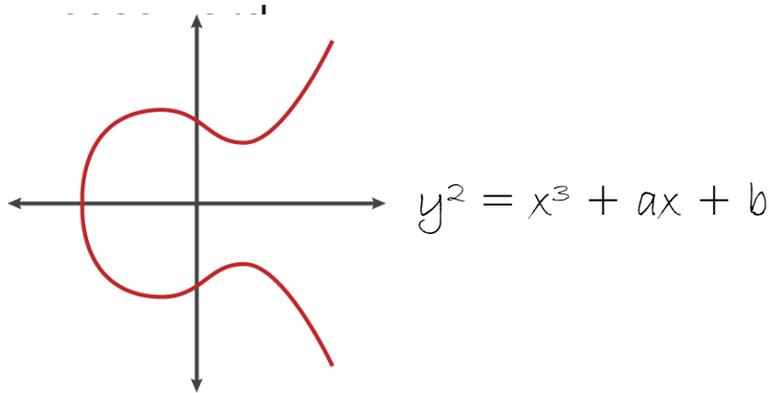
# Dragonblood



- 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

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



Edit WLAN

General Security Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP

MAC Filtering  Authorization List\* ipsk ⓘ

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input checked="" type="checkbox"/>		

Fast Transition

Status Disabled ▾

Over the DS

Reassociation Timeout\* 20

WPA2/WPA3 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

Protected Management Frame

PMF Required ▾

Association Comeback Timer\* 1

SA Query Time\* 200

Auth Key Mgmt

SAE	<input checked="" type="checkbox"/>	FT + SAE	<input type="checkbox"/>
OWE	<input type="checkbox"/>	FT + 802.1x	<input type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>		

Anti Clogging Threshold\* 1500

Max Retries\* 5

Retransmit Timeout\* 400

PSK Format Both H2E and HnP

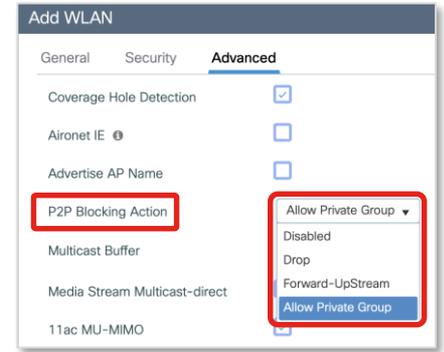
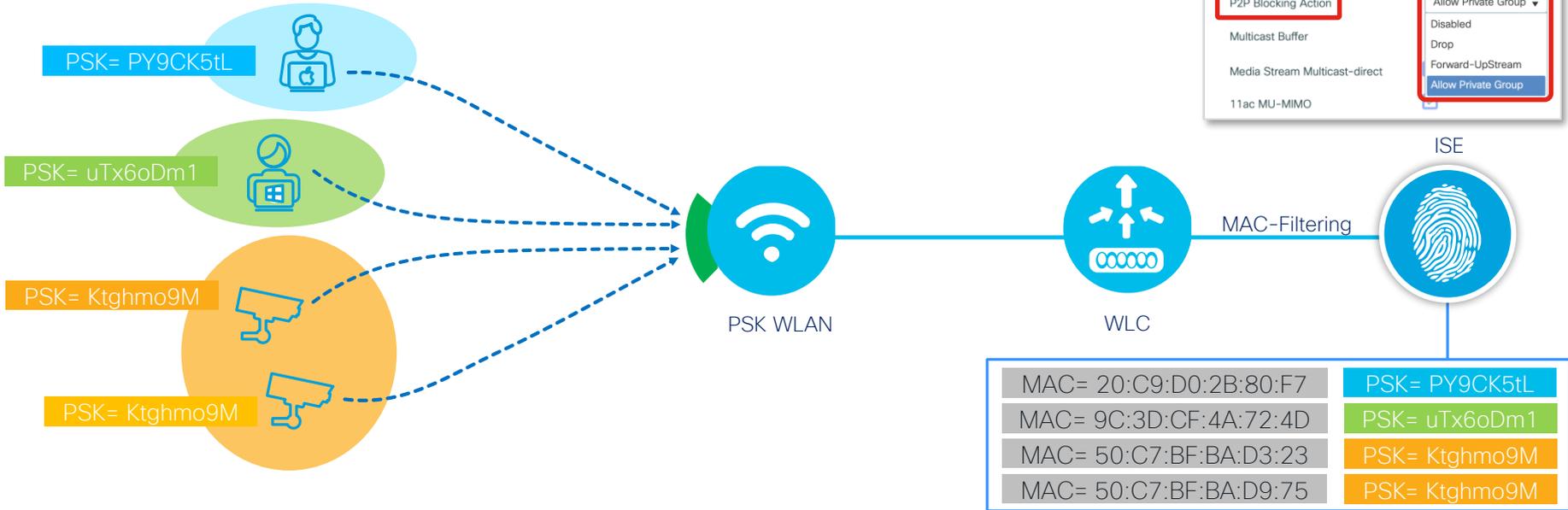
PSK Type Hash to Element Only

Pre-Shared Key\* Hunting and Pecking Only

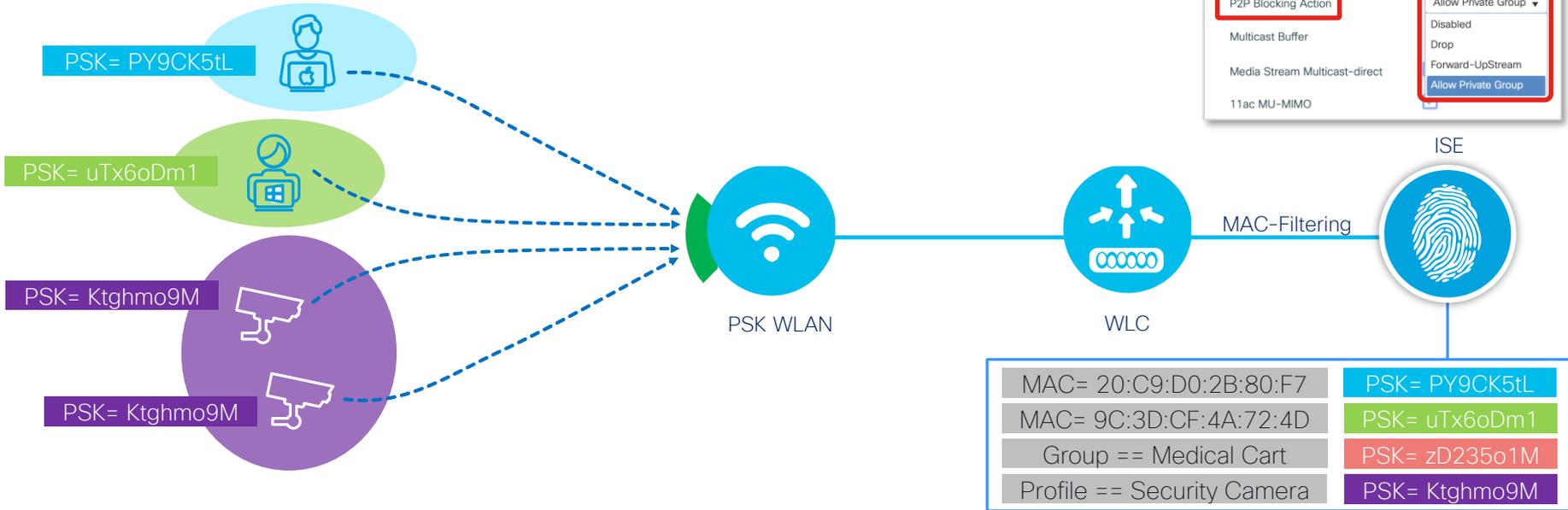
SAE Password Element ⓘ

Hash to Element O...

# Identity PSK/SAE

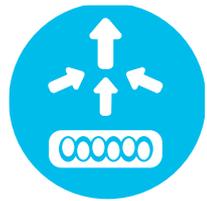


# Identity PSK/SAE

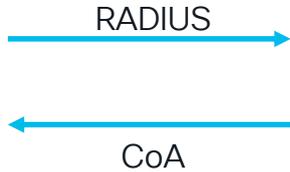


<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>  
[https://documentation.meraki.com/MR/Encryption\\_and\\_Authentication/IPSK\\_with\\_RADIUS\\_Authentication](https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication)

# iPSK Manager



WLC / AP



ISE



iPSK Manager

- Linux
- Apache
- MySQL
- PHP

Administration

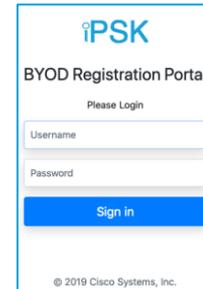


Admin

iPSK Lifecycle Management



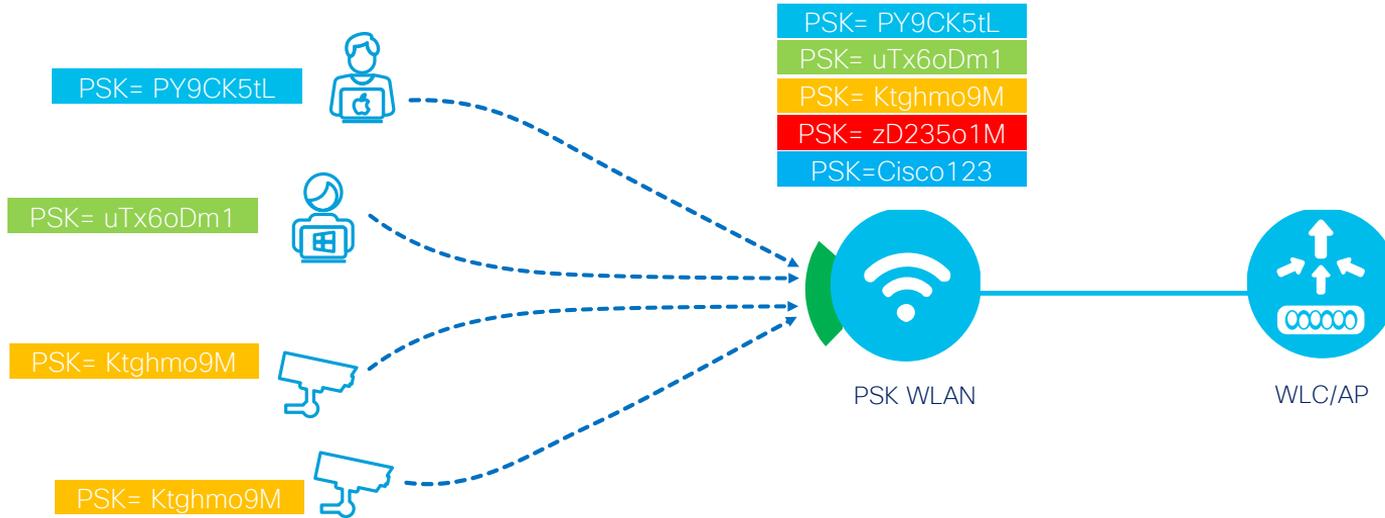
End Users



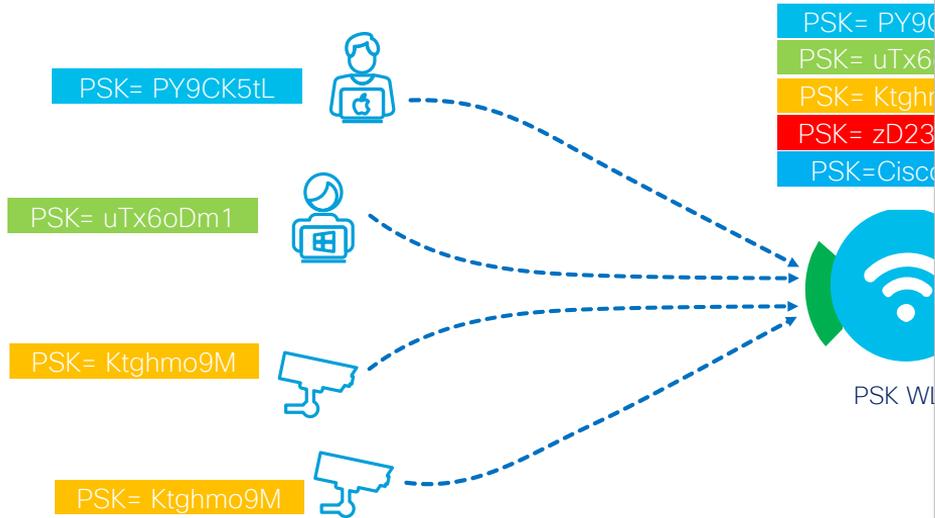
<http://cs.co/iPSK-Manager>

**CISCO** Live!

# Multi Pre-Shared Key



# Multi Pre-Shared Key



Edit WLAN

General Security Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP

MAC Filtering  Authorization List\* mpsk ⓘ

Lobby Admin Access

WPA Parameters

WPA Policy  WPA2 Policy

GTK Randomize  OSEN Policy

WPA2 Encryption

AES(CCMP128)  CCMP256

GCMP128  GCMP256

Protected Management Frame

PMF Disabled

Fast Transition

Status Disabled

Over the DS

Reassociation Timeout \* 20

Auth Key Mgmt

802.1x  PSK

Easy-PSK  CCKM

FT + 802.1x  FT + PSK

802.1x-SHA256  PSK-SHA256

PSK Format ASCII

PSK Type Unencrypted

Pre-Shared Key\* .....

MPSK Configuration

Enable MPSK

Priority \* Priority(0-4)

Key Format ASCII

Password Type Unencrypted

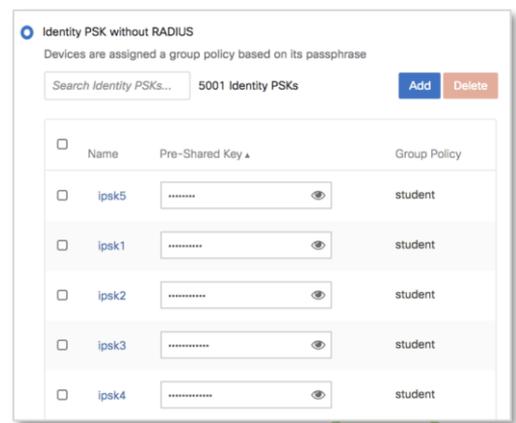
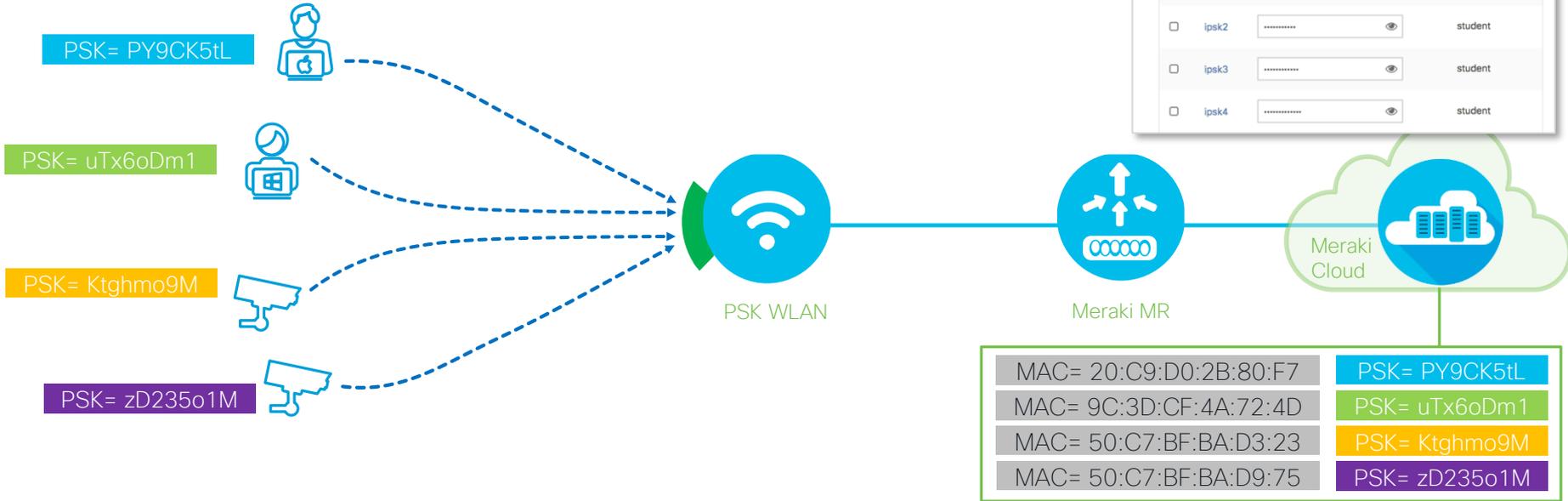
Pre-Shared Key\*

Cancel Apply

Priority Key Format Password Type

FYI

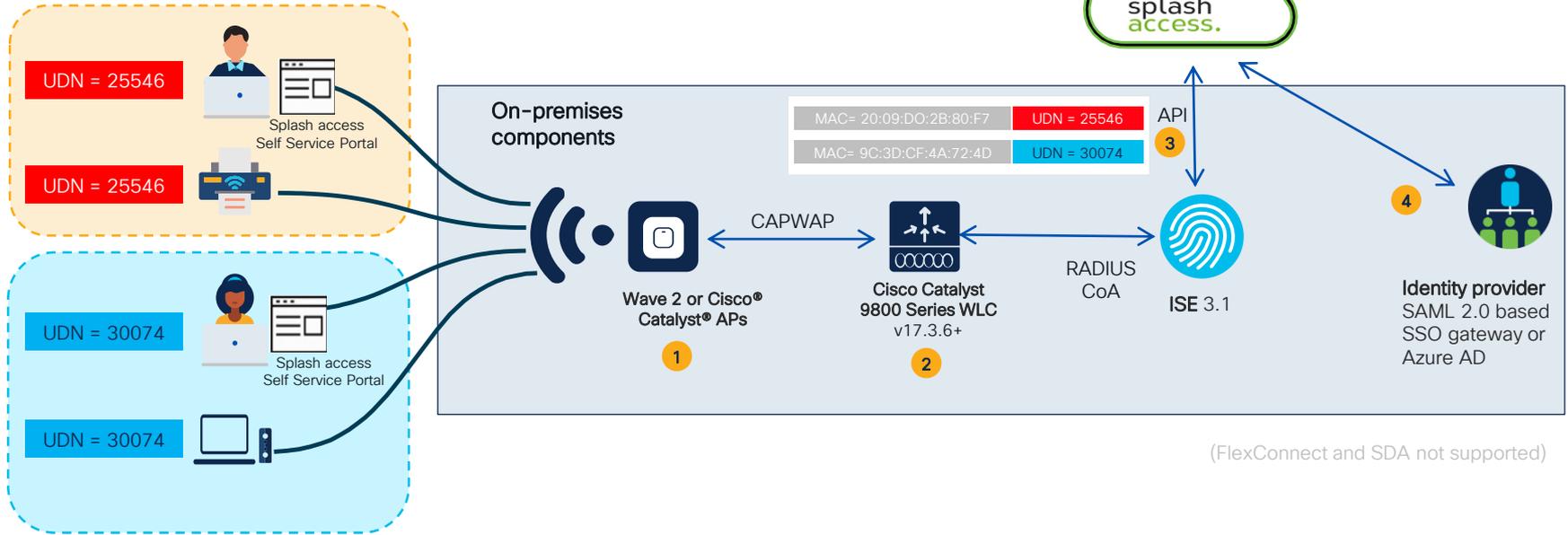
# Identity PSK without RADIUS



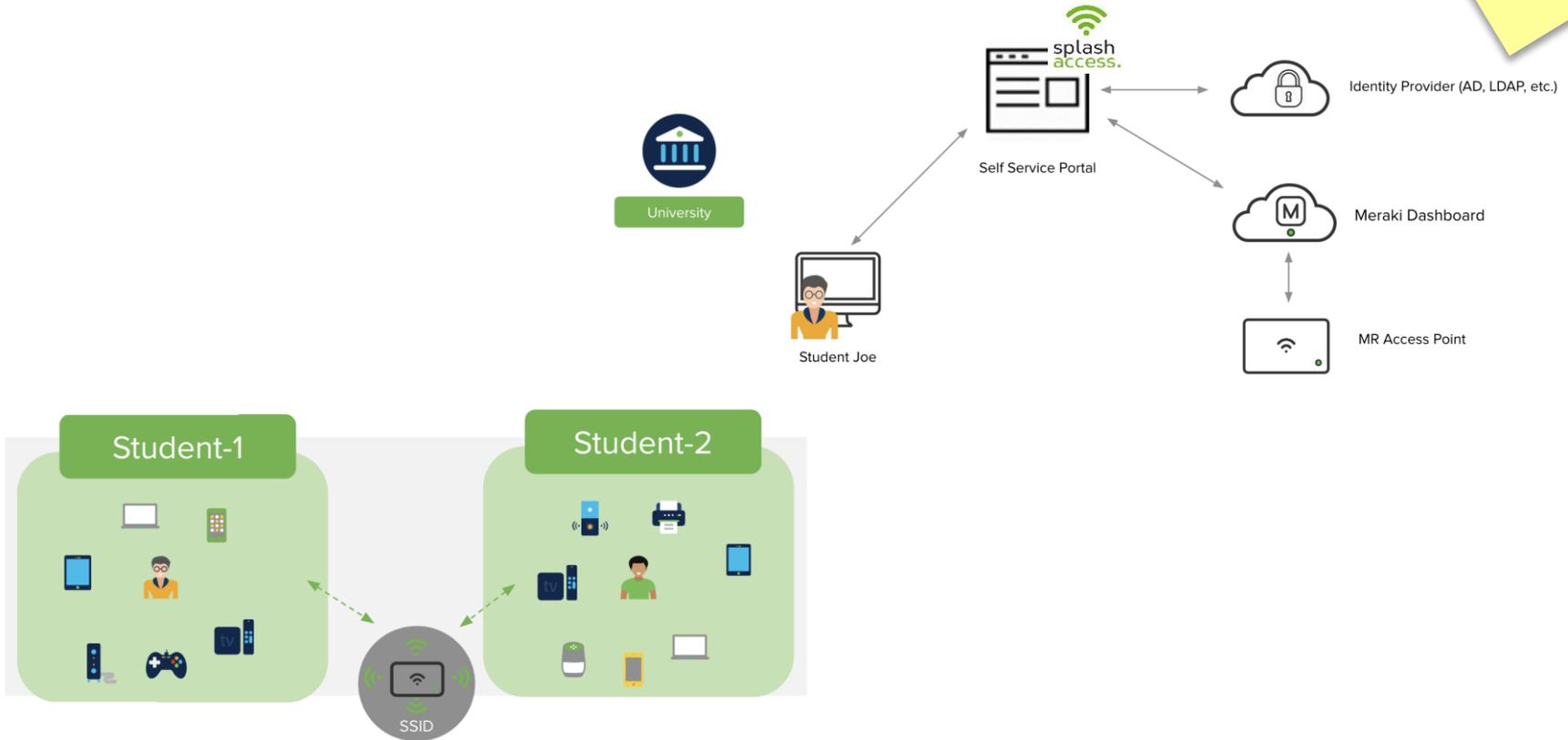
# User Defined Network+



UDN with Splash access supported on central switching SSID



# Wi-Fi Personal Network

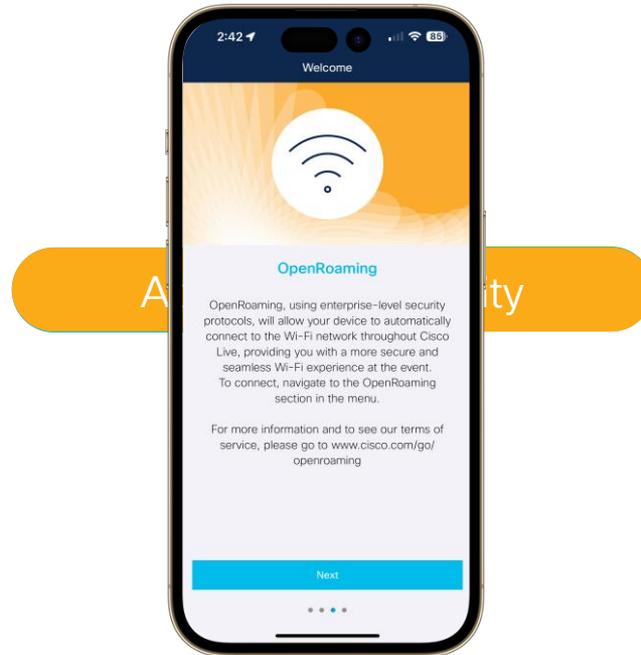




# Wi-Fi Certified Enhanced Open WPA3

- 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

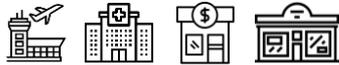
# Decoupling Access and Identity



# OpenRoaming



Access >



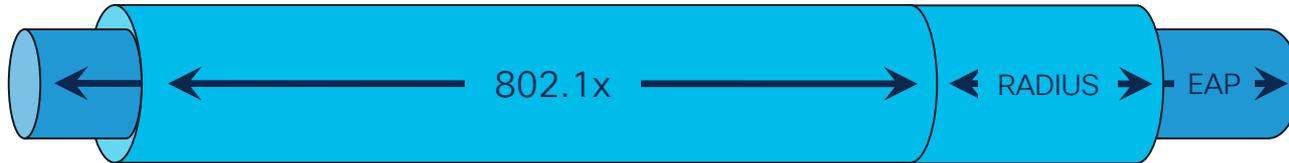
Wireless Network Discovery



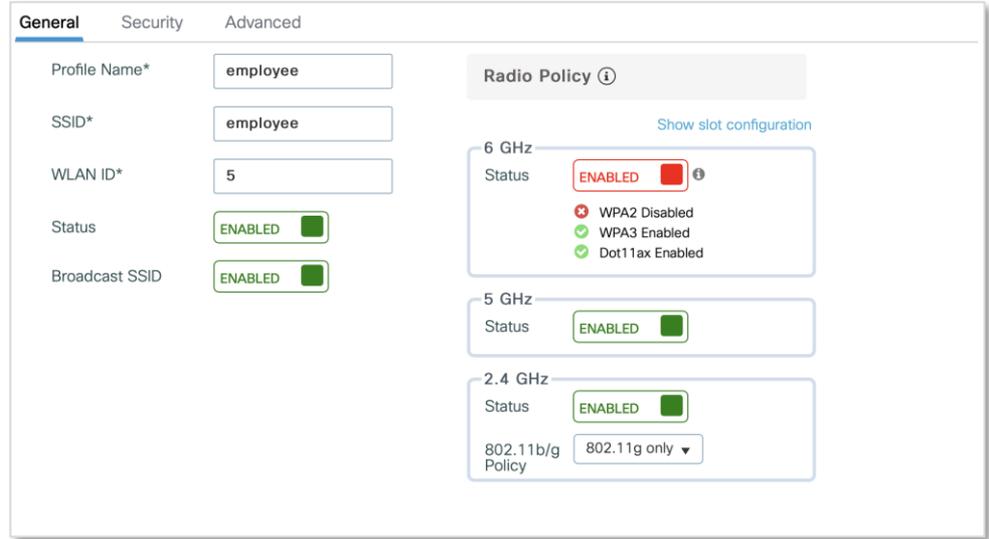
< Identity



Unique Identity



# Security Implications of 6GHz

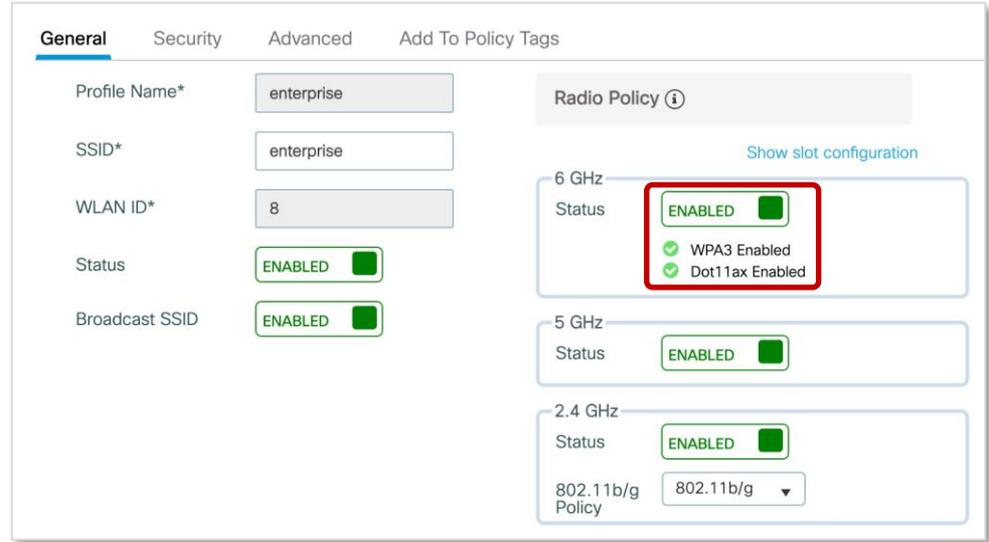


WPA3 and OWE are **mandatory** for 6GHz



WPA2 and Open are **not** supported on 6GHz

# Security Implications of 6GHz



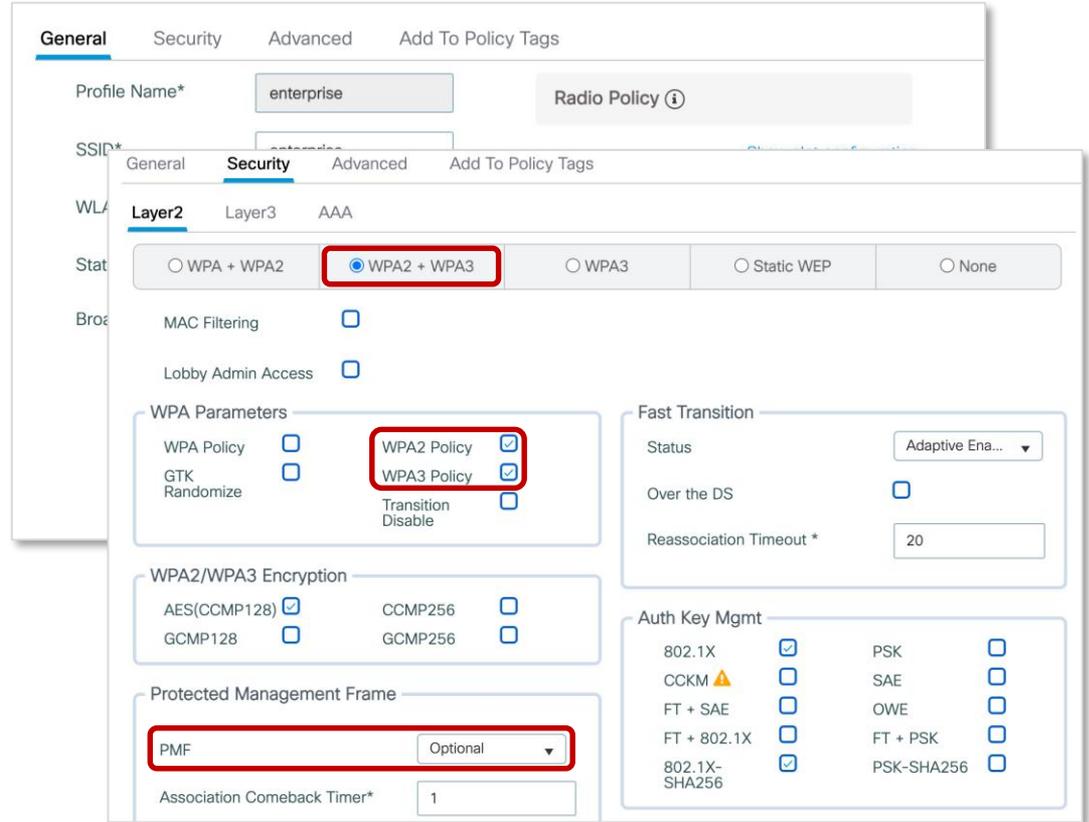
WPA3 and OWE are **mandatory** for 6GHz



WPA2 and Open are **not** supported on 6GHz

From IOS-XE 17.12.1

# Security Implications of 6GHz

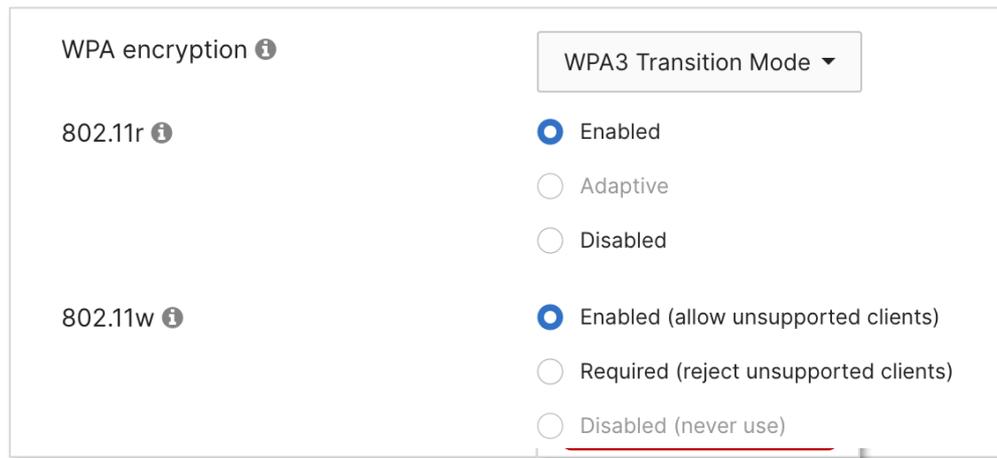


WPA3 and OWE are **mandatory** for 6GHz



WPA2 and Open are **not** supported on 6GHz

# Security Implications of 6GHz



WPA3 and OWE are **mandatory** for 6GHz

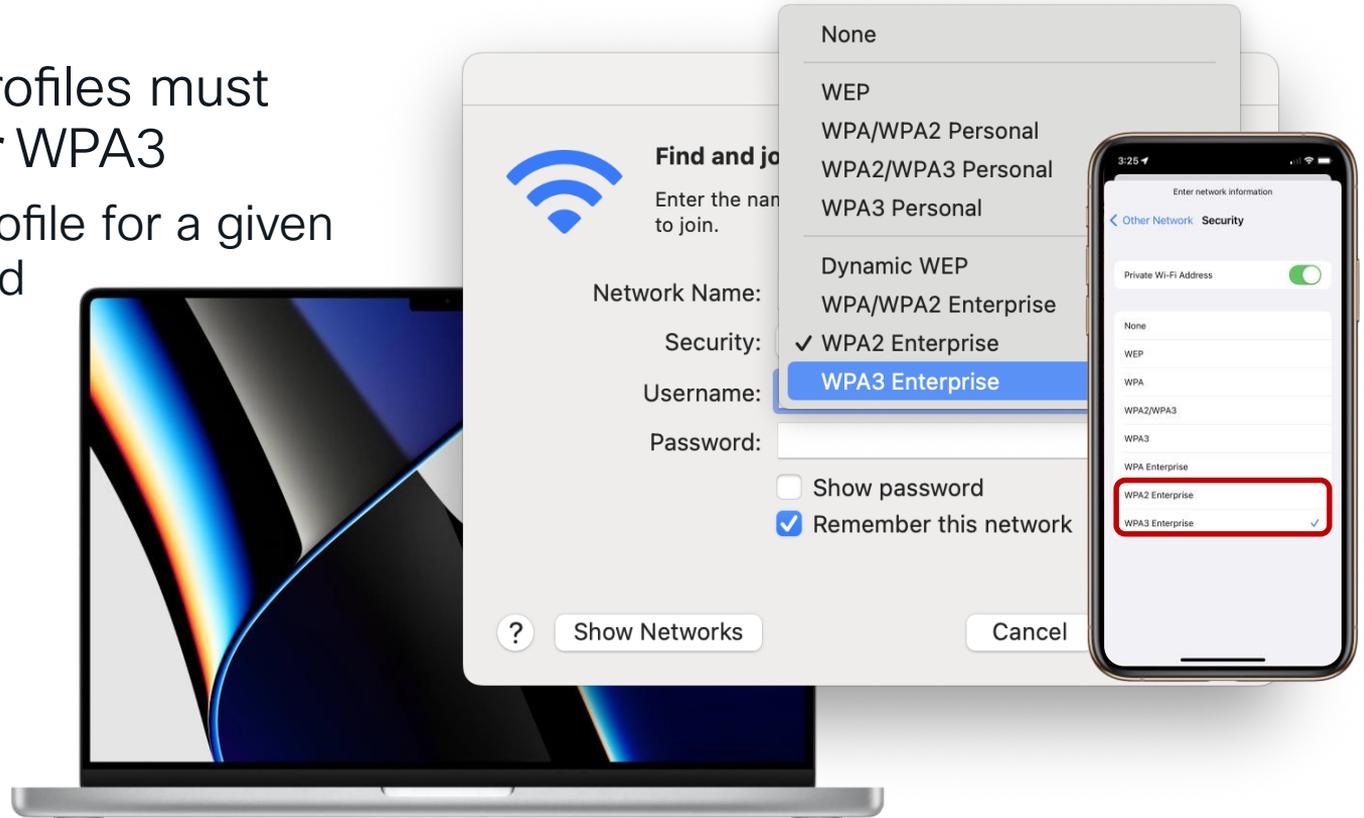


WPA2 and Open are **not** supported on 6GHz

From MR 31.X

# 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

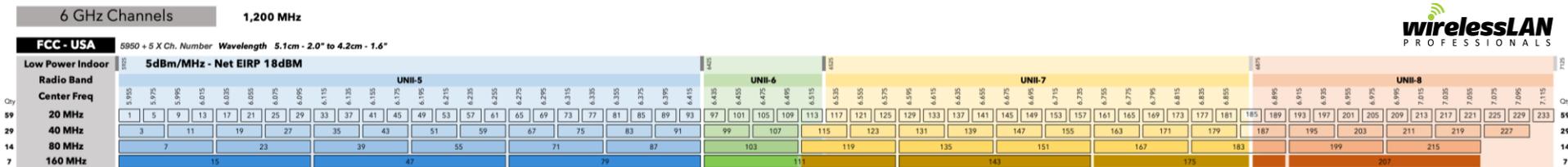


# AP Discovery Challenges

## Wi-Fi 6E

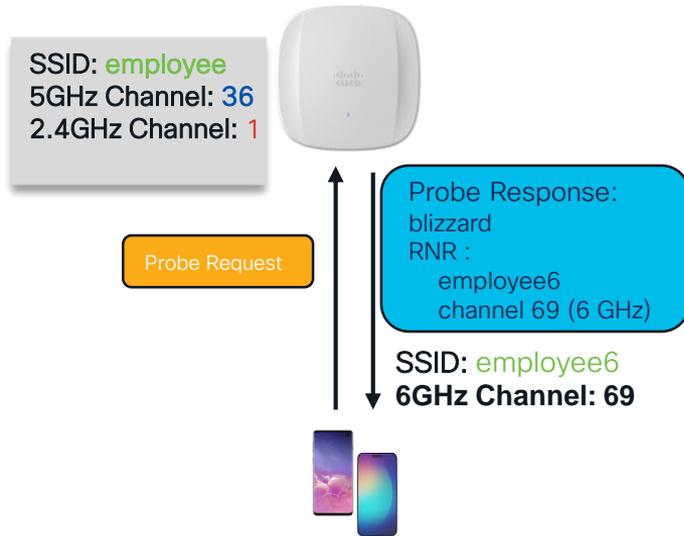


- There are a total of 59x 20MHz channels in the 6GHz band
- Wi-Fi clients can only send Probe Requests on 20MHz channels
- It would take 6 seconds to passively scan all 59 channels



# 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)

FYI

## Wi-Fi 6E

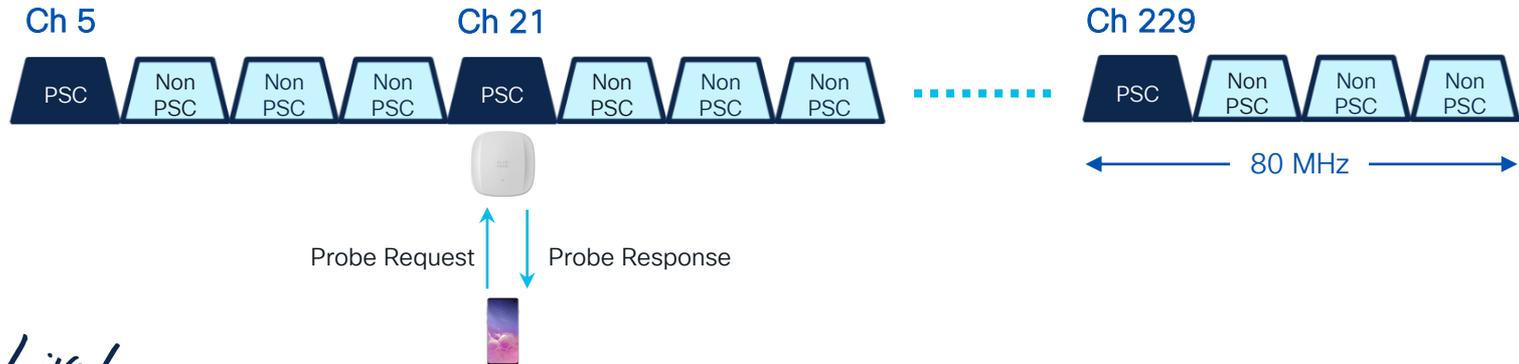
- Broadcast probe response transmitted every 20ms
- Contains detailed information as in the beacon
- Carries multiple BSSIDs
- Reduces probe request overhead
- UBPR is not as widely adopted as FILS
- FILS and UBPR are mutually exclusive

# 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



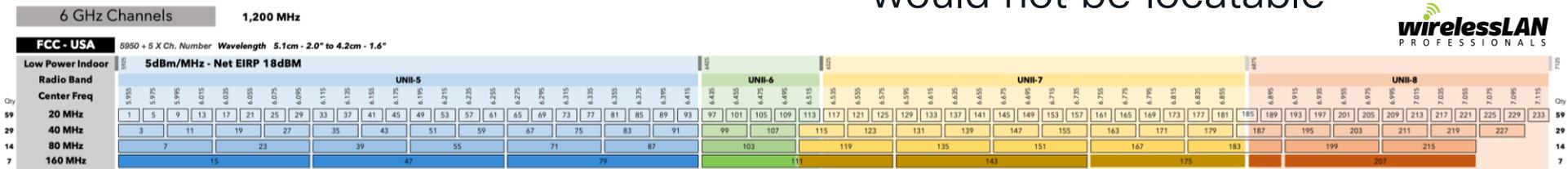
## Wi-Fi 6E

- 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

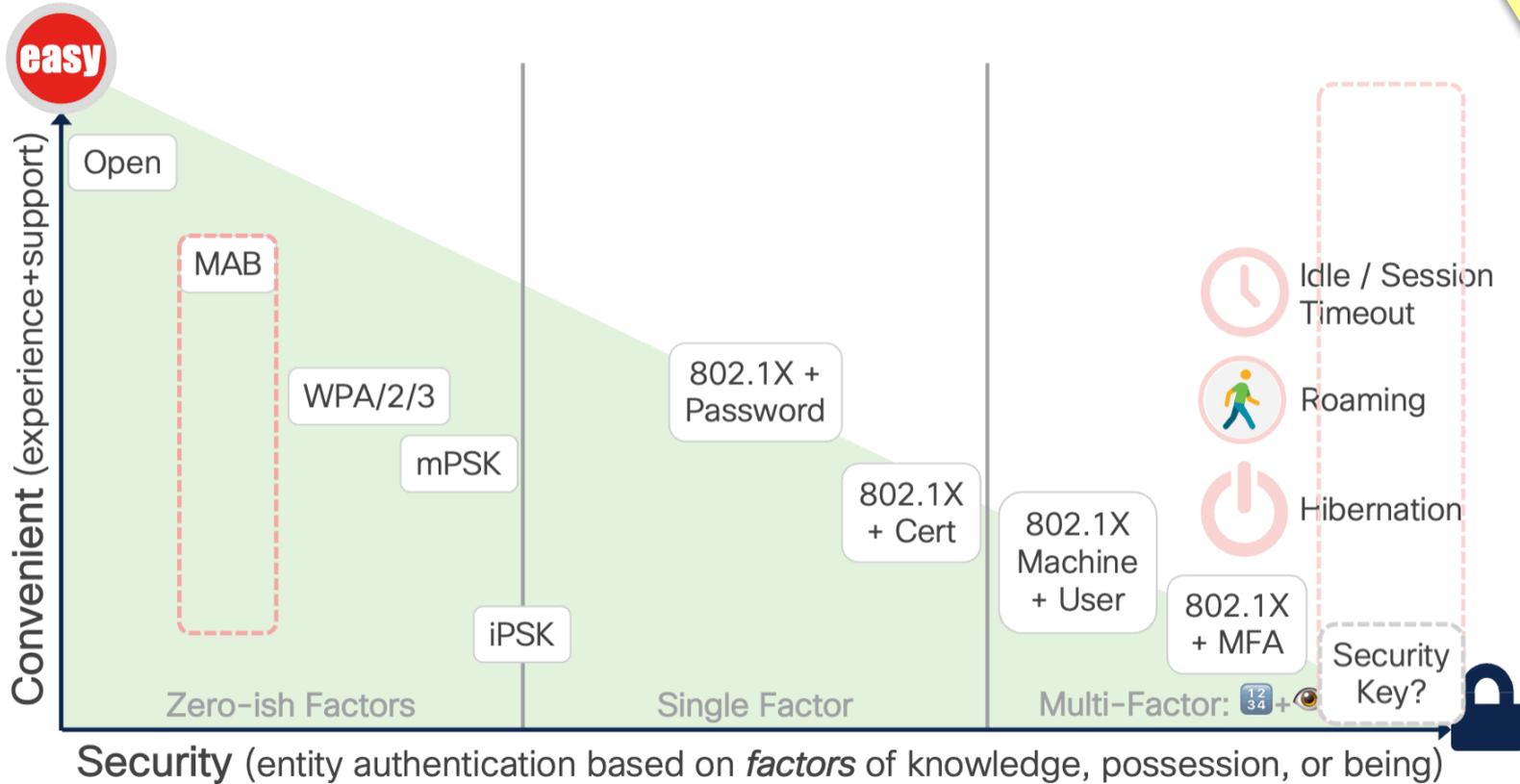
# WPA3

## New Requirements

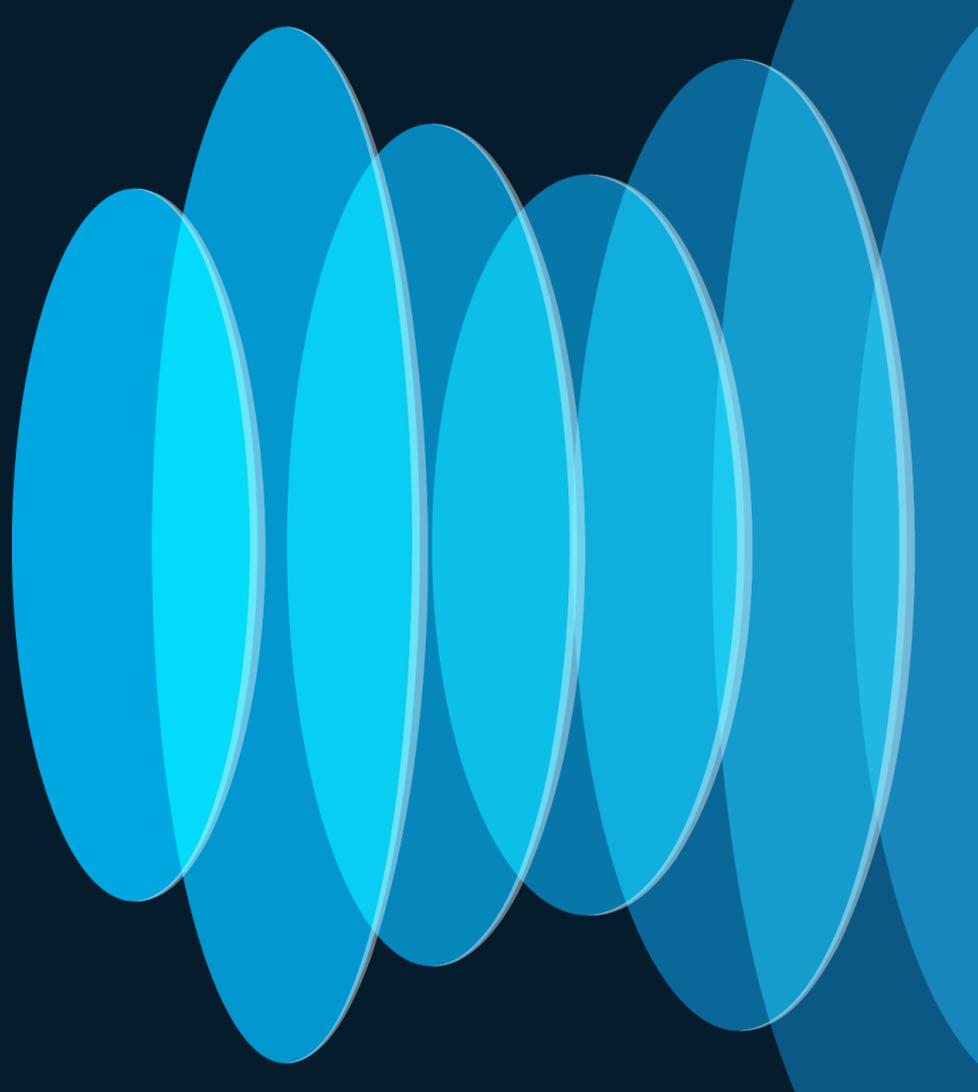


Features	Catalyst (Local)	Catalyst (Flexconnect)	Meraki
WPA3 FT-802.1X-SuiteB-192bit + AES-GCMP256 (Microsoft and Zebra ASK)	×	×	<input checked="" type="checkbox"/>
AKM FT-802.1X-SHA384(22) and 802.1X-SHA384(23) Support	×	×	×
SAE iPSK Central Auth support	<input checked="" type="checkbox"/>	×	×
WGB WPA3 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)	×	×	<input checked="" type="checkbox"/>
AKM FT-802.1X-SHA384(22) and 802.1X-SHA384(23) Support	×	×	×
SAE iPSK Central Auth support	<input checked="" type="checkbox"/>	×	×

# Network Access Security Spectrum



# Wireless Intrusion Detection and Prevention



# 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

**High Threat Summary**

Active High Threats (135)

By threat type: Top 10, All

135 High Threat

Threats (176)

Threat Level	MAC Address	Type
High	A4:53:0E:7D:09:80	Rogue on wire
High	9A:18:98:C0:46:36	Rogue on wire
High	A4:53:0E:7D:16:60	Honeypot
High	A4:53:0E:7D:38:80	Honeypot
High	A4:53:0E:7D:42:A0	Honeypot

**Threat 360: Mac A4:53:0E:7D:42:A0**

Threat Level: High, Threat Type: Honeypot, Vendor: Cisco Systems, Inc, Status: Active, Containment S...: Open, Last Reported: Jun 1, 2022 02:06 pm

Location: Global/San Jose/Building 14/Floor1

Detections (18) Clients (0)

Detecting AP	Detecting AP Site	Adhoc	Rogue SSID	RSSI (dBm)	Channels	Radio Type (Band)	State	Last Reported
SJC14-TME-AP9	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo	-50	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 01:45
Traffic_Assurance_01	Global/San Jose/Building 14/Floor1	No	DNA Spaces Sensors LAN	-70	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 02:06
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo	-71	60	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:02

[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](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

The dashboard displays the following statistics:

- TOTAL ROGUE THREATS: 197
- TOTAL AWIPS THREATS: 79
- TOTAL UNIQUE ROGUE CLIENTS: 5
- ROGUES CONTAINED: 7

High Threats Summary: Active High Threats (99)

Threat Type	Severity	Policy	Status
AP Impersonation	High	Predefined	Active
Association Flood	High	Predefined	Active
Authentic Fuzzed Beacon	High	Predefined	Active
Authentic Fuzzed Probe Request	High	Predefined	Active
Beacon D Fuzzed Probe Response	High	Predefined	Active
Beacon F Honeypot	High	Predefined	Active
Beacon W Interferer	Potential	Predefined	Active
Block Ack Invalid MAC OUI Frame	High	Predefined	Active
Broadcas Malformed Association Request	High	Predefined	Active
CTS Flood Malformed Authentication	High	Predefined	Active
CTS Virtu Neighbor	Informational	Predefined	Active
Deauthen Probe Response Flood	High	Predefined	Active
Deauthen PS Poll Flood	High	Predefined	Active
Disassoci Re-Association Request Flood	High	Predefined	Active
Disassoci Rogue on Wire	High	Predefined	Active
EAPOL L RTS Flood	High	Predefined	Active
RTS Virtual Carrier Sense Attack	High	Predefined	Active

Configuration > Security > Wireless Protection Policies

Rogue Policies   Rogue AP Rules   **Client Exclusion Policies**

- Select all events
- Excessive 802.11 Association Failures
- Excessive 802.1X Authentication Failures
- Excessive 802.1X Authentication Timeout
- IP Theft or IP Reuse
- Excessive Web Authentication Failures

Captures (11)

Alarm ID	Capture Filename	Last Updated
226034	A0F8497EC066_80211_1622535114913083.pcap	Jun 7, 2022 06:38 am
226035	A0F8497EC066_80211_1622535145905580.pcap	Jun 7, 2022 06:38 am
226036	A0F8497EC066_80211_1622535176916025.pcap	Jun 7, 2022 06:38 am
PLS06-AP3800-01	A0F8497EC066_80211_1622535238913731.pcap	Jun 7, 2022 06:38 am
PLS06-AP3800-01	A0F8497EC066_80211_1622535424906239.pcap	Jun 7, 2022 06:38 am

aWIPS and Forensic Capture Enablement

aWIPS is supported for Catalyst 9800 Controllers and eCA devices. aWIPS can be enabled/ disabled on WLC physically managed site location Note: aWIPS is not applicable for Remote TeleWorker sites.

- Enable aWIPS
- Enable Forensic Capture

# Rogue and WIPS Reporting and APIs



The screenshot shows the Cisco DNA Center Reports page. The left sidebar lists various report categories, with 'Rogue and aWIPS' highlighted. The main content area displays two report templates: 'Rogue and aWIPS New Threat' and 'Rogue and aWIPS Threat Detail'. Each template includes a brief description and options to generate the report in CSV, TDE, or JSON format.

The screenshot shows the Cisco DNA Center Platform / Developer Toolkit page. The left sidebar lists various API categories, with 'Devices' highlighted. The main content area displays a table of APIs related to Rogue and aWIPS reporting.

Method	Name	Description	URL	Actions
GET	Get Allowed Mac Address <sup>Intent</sup>	Intent API to fetch all the allowed mac addresses in the system.	/security/threats/rogue/allowed-list	...
POST	Threat Summary <sup>Intent</sup>	The Threat Summary for the Rogues and aWIPS	/security/threats/summary	...
GET	Get Threat Types <sup>Intent</sup>	Intent API to fetch all threat types defined.	/security/threats/type	...
GET	Get Allowed Mac Address Count <sup>Intent</sup>	Intent API to fetch the count of allowed mac addresses in the system.	/security/threats/rogue/allowed-list/count	...
DELETE	Remove Allowed Mac Address <sup>Intent</sup>	Intent API to remove the threat mac address from allowed list.	/security/threats/rogue/allowed-list/\${macAddress}	...
POST	Threat Detail Count <sup>Intent</sup>	The details count for the Rogue and aWIPS threats	/security/threats/details/count	...
POST	Add Allowed Mac Address <sup>Intent</sup>	Intent API to add the threat mac address to allowed list.	/security/threats/rogue/allowed-list	...
GET	Get Threat Levels <sup>Intent</sup>	Intent API to fetch all threat levels defined.	/security/threats/level	...
POST	Threat Details <sup>Intent</sup>	The details for the Rogue and aWIPS threats	/security/threats/details	...

# Access Point Scanning Options



## 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



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

Configuration > Radio Configurations > CleanAir

5 GHz Band | 2.4 GHz Band

General | Trap Configuration

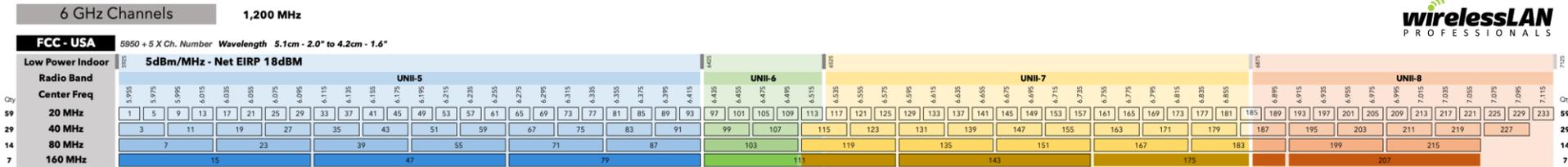
Enable CleanAir

Enable SI

Report Interferers

Available Interference Types: WiFi Inverted, WiFi Invalid Channel

Interference Types to detect: TDD Transmitter, Jammer, Continuous Transmitter, DECT-like Phone



# 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

The image shows two overlapping screenshots of a Cisco configuration interface. The top screenshot is titled "Add AP Join Profile" and shows the "Security" tab. Under the "Rogues" section, "Rogue Detection" is checked, "Rogue Detection Minimum RSSI" is set to -90, and "Rogue Detection Transient Interval (seconds)" is set to 0. The bottom screenshot is titled "Configuration > Security > Wireless Protection Policies" and shows the "Rogue AP Rules" tab. Under the "General" section, "Rogue Detection Security Level" is set to Custom, "Expiration timeout for Rogue APs (seconds)\*" is 1200, "Validate Rogue Clients against AAA" is unchecked, "Validate Rogue APs against AAA" is unchecked, "Rogue Polling Interval (seconds)" is 3600, "Detect and Report Adhoc Networks" is checked, "Rogue Detection Client Number Threshold\*" is 0, "Rogue Init Timer (seconds)\*" is 180, "AP Authentication" is unchecked, "AP Authentication Alarm Threshold\*" is 1, and "Syslog Notification" is unchecked. Under the "Auto Contain" section, "Auto Containment Level" is set to 1, "Auto Containment only for Monitor Mode APs" is unchecked, "Using our SSID" is checked, "Valid client on Rogue AP" is unchecked, and "Adhoc Rogue AP" is unchecked. Under the "MFP Configuration" section, "Global MFP State" is unchecked, "AP Impersonation Detection" is unchecked, and "MFP Key Refresh Interval (hours)\*" is 24.

# 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

Configuration > Security > Wireless Protection Policies

Rogue Policies | Rogue AP Rules | Client Exclusion Policies

General

Rogue Detection Security Level: Custom

Expiration timeout for Rogue APs (seconds)\*: 1200

Validate Rogue Clients against AAA:

Validate Rogue APs against AAA:

Rogue Polling Interval (seconds): 3600

Detect and Report Adhoc Networks:

Rogue Detection Client Number Threshold\*: 0

Rogue Init Timer (seconds)\*: 180

AP Authentication:

AP Authentication Alarm Threshold\*: 1

Syslog Notification:

Auto Contain

Auto Containment Level: 1

Auto Containment only for Monitor Mode APs:

Using our SSID:

Valid client on Rogue AP:

Adhoc Rogue AP:

MFP Configuration

Global MFP State:

AP Impersonation Detection:

MFP Key Refresh Interval (hours)\*: 24

Apply

# Cisco Catalyst Centre Threat Levels

## Informational

- RSSI  $\leq$  -75 dBm and not on wire
- Rogue Type: Neighbor

## Potential

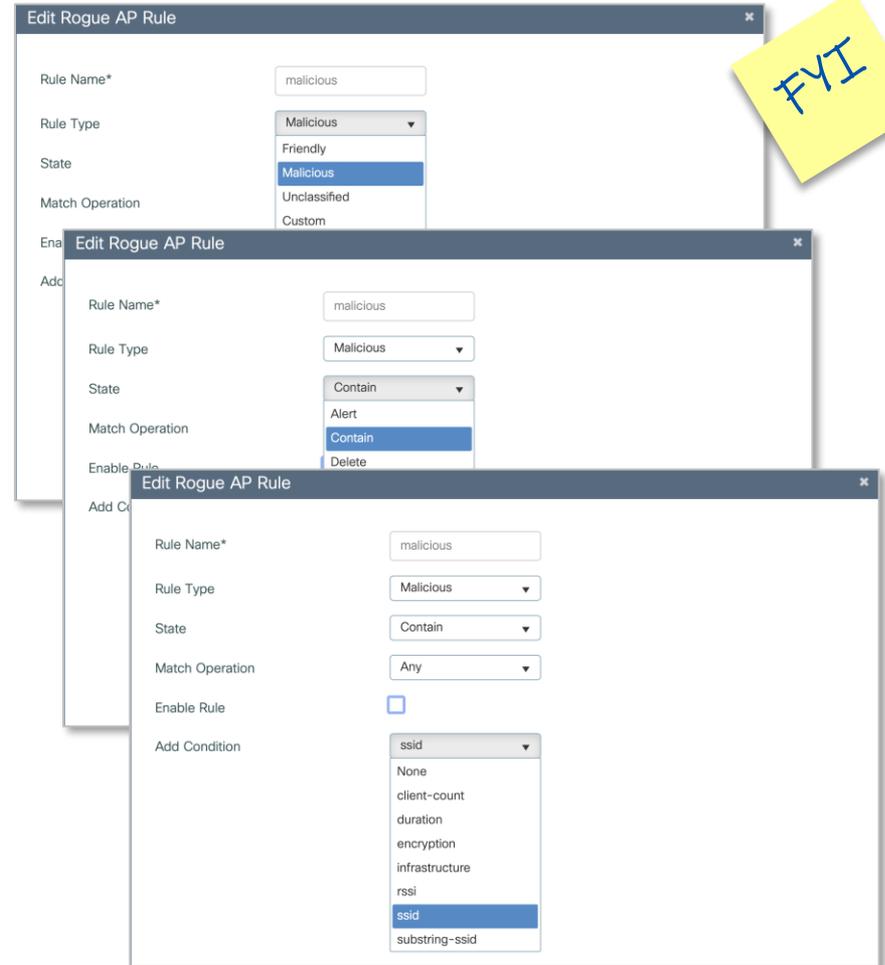
- RSSI  $>$  -75 dBm and not on wire
- Rogue Type: Interferer

## 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 on Wire

- Matching Algorithms
  - MAC Address  $\pm 3/\pm 2/\pm 1$
  - 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

The screenshot displays the Cisco DNA Center Assurance interface for a 'Rogue and aWIPS' dashboard. The main view shows a 'High Threat Summary' with 14 active high threats, categorized by type: Rogue on wire (12) and Honeyport (1). A circular gauge indicates the total count of 14 high threats. Below this, a table lists threats, with the top entry highlighted: Threat Level: High, MAC Address: 6A:3A:0E:53:A6:E9, Type: Rogue on wire.

The detailed view for Threat 360 (Mac 6A:3A:0E:53:A6:E9) shows a 'High' threat level, 'Rogue on wire' type, 'UNKNOWN' vendor, 'Active' status, and 'Open' containment status. It includes a floor plan visualization of the location (Global/San Jose/Building 14/Floor1) with a red circle highlighting the 'SJC14-TNE-AP3' device. A table below the floor plan shows 'Switch Port Detail (1)' with one entry: Host Mac: 70:F3:5A:7B:9F:71, Device Name: WS-C3850-48PTME\_Switch, Device IP: 172.20.224.156, Interface Name: GigabitEthernet5/0/47, Last Updated: Jun 5, 2022 09:40 am.

# Rogue on Wire

- Matching Algorithms
  - MAC Address  $\pm 3/\pm 2/\pm 1$
  - 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

Cisco DNA Center Assurance / Dashboards / Rogue and aWIPS

Threat 360: Mac 6A:3A:0E:53:A6:E9

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
High	Rogue on wire	UNKNOWN	Active	Open	Jun 5, 2022 03:23 pm

Location: Global/San Jose/Building 14/Floor1

Threats (134)

Threat Level	MAC Address	Type
High	68:3A:1E:53:A6:E0	Rogue on wire
High	6A:3A:0E:53:A6:E9	Rogue on wire
High	9A:18:98:C0:46:36	Rogue on wire
High	A4:53:0E:70:09:80	Rogue on wire

Switch Port Detail (1) Detections (9) **Clients (19)**

MAC Address	Gateway MAC	Rogue AP MAC	IP Address	Last Heard
70:F3:5A:7B:FD:F1	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.100	Jun 5, 2022 03:23 pm
70:F3:5A:7B:FD:31	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.90	Jun 5, 2022 03:23 pm
70:F3:5A:7B:FC:11	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.99	Jun 5, 2022 03:14 pm
70:F3:5A:7B:FA:11	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.80	Jun 5, 2022 03:23 pm
70:F3:5A:7B:F9:71	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.105	Jun 5, 2022 03:23 pm

# Rogue on Wire

- Matching Algorithms
  - MAC Address  $\pm 3/\pm 2/\pm 1$
  - 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

The screenshot displays the Cisco DNA Center Assurance dashboard for a 'Rogue and aWIPS' threat. The main view shows a 'High Threat Summary' with 14 active high threats. A circular gauge indicates 14 high threats, with a legend for 'Rogue on wire (12)' and 'Honeypot (1)'. Below this is a table of threats, with the selected threat 'Threat 360: Mac 6A:3A:0E:53:A6:E9' highlighted. The details for this threat are shown in a right-hand pane, including a table of threat information, a floor plan visualization, and a table of switch port details.

Threat Level	Threat Type	Vendor	Status	Containment S...
High	Rogue on wire	UNKNOWN	Active	Open

Switch Port Detail (1)	Detections (9)	Clients (19)		
Host Mac	Device Name	Device IP	Interface Name	Last Updated
70:F3:5A:7B:9F:71	WS-C3850-48PTME_Switch	172.20.224.156	GigabitEthernet5/0/47	Jun 5, 2022 09:40 am

# Securing AP Switch Port Access



802.1x  
← Authentication (EAP-FAST) →



How do we bootstrap configure the AP?

Management

Dot1x Credentials

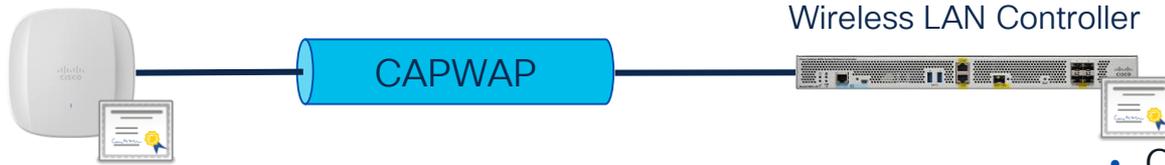
Dot1x Username:

Dot1x Password:

Dot1x Password Type:

Buttons: Cancel, Apply to Device

# Securing AP to Controller Communication



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



Edit AP Join Profile

General Client **CAPWAP** AP Management Rogue AP

High Availability **Advanced**

Enable VLAN Tagging

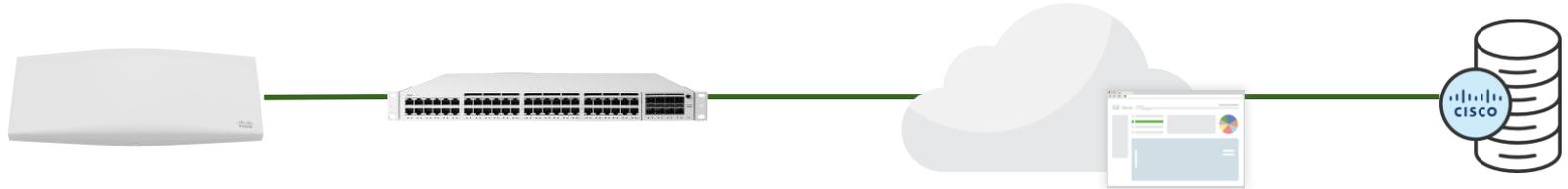
**Enable Data Encryption**

Enable Jumbo MTU

Link Latency

Preferred Mode

# SecurePort



MR connected to MS

MR requests certificate from Cisco PKI

MS authorizes port based on configured profile

1

2

3

4

5

MS permits Meraki dashboard connection for MR

MR authenticates with acquired certificate

# Rogue AP Containment

- How do we contain Rogue APs?

The screenshot displays the Cisco DNA Center interface for Rogue and aWIPS management. The main view shows a threat entry for 'Threat 360: Mac A4:53:0E:7C:99:E0' with a 'High' threat level and 'Honeypot' type. The interface includes a map of the physical location (Global/San Jose/Building 14/Floor1) showing the placement of various access points (AP-0001, SJC14-TME-AP1 through AP4) and a switch (WS-C3850-48RTME\_Switch). A 'Start Containment' button is highlighted in red in the top right corner of the threat details panel.

**Threats (174)**

Threat Level	MAC Address	Type
High	A4:53:0E:7D:35:80	Honeypot
High	A4:53:0E:7D:38:80	Honeypot
High	A4:53:0E:7C:CC:00	Honeypot
High	A4:53:0E:7D:5B:20	Honeypot
High	A4:53:0E:7C:86:80	Honeypot
High	A4:53:0E:7C:99:E0	Honeypot

**Detections (28)**

Detecting AP	Detecting AP Site	Adhoc	Rogue SSID	RSSI (dBm)	Channels	Radio Type (Band)	State	Time
SJC14-TME-AP6	Global/San Jose/Building 14/Floor1	No	IDNAS Demo OpenRoaming	-71	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 01:25
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNA Spaces Demo LAN	-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:37
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo	-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:44

# Rogue AP Containment

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

The screenshot displays the Cisco DNA Center interface for Rogue and aWIPS. A warning dialog is open, titled "Warning", with a yellow triangle icon. The text reads: "Using this feature may have legal consequences. Wireless containment will be initiated for the below rogue BSSIDs on wireless controller with IP address 172.20.224.95. Do you want to continue?". Below the text, there are two input fields for "Rogue BSSID" containing the MAC addresses "A4:53:0E:7C:99:E0" and "A4:53:0E:7C:99:E3". At the bottom of the dialog, there are "No" and "Yes" buttons. The background interface shows a table of threats and a table of APs.

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
High	Honeypot	Cisco Systems, Inc	Active	Open	Jun 1, 2022 02:48 pm

RSSI (dBm)	Channels	Radio Type (Band)	State	
-71	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 01:25
-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:37
-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:44

# Rogue AP Containment

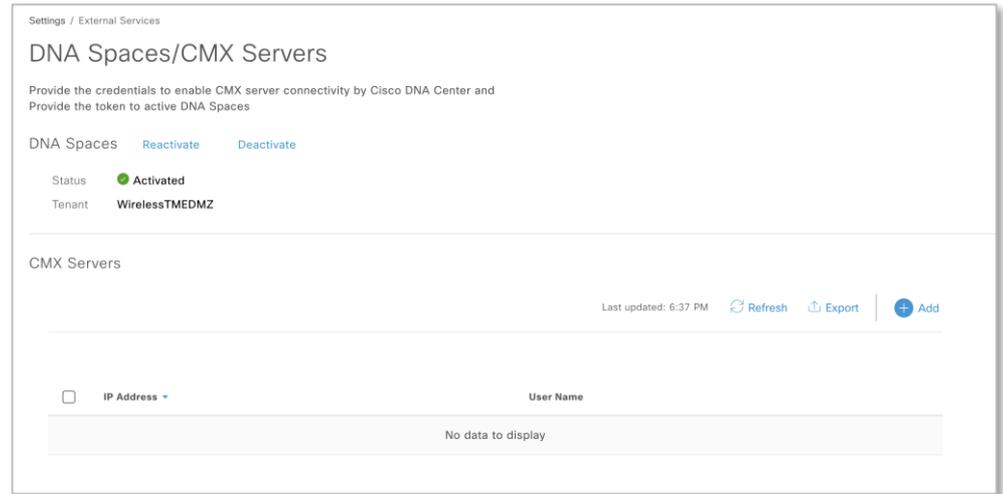
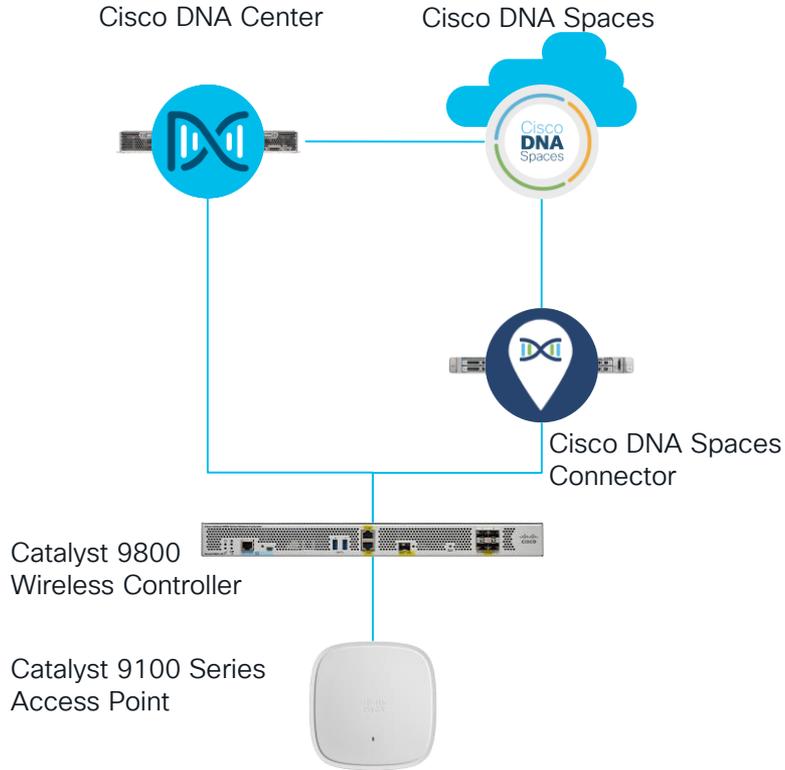
- How do we contain Rogue APs?
  - Containment is a spoofed 802.11 disassociation/deauthentication request attack
- How does WPA3 affect Rogue AP containment?
  - 802.11w will change how we can mitigate Rogue AP related threats
  - The ability to physically locate rogues will be key

The screenshot displays the Cisco DNA Center interface for Rogue and aWIPS. The main view shows a threat entry for 'Threat 360: Mac A4:53:0E:7C:99:E0' with a 'High' threat level and 'HoneyPot' threat type. A warning dialog box is overlaid, stating: 'Warning: Using this feature may have legal consequences. Wireless containment will be initiated for the below rogue BSSIDs on wireless controller with IP address 172.20.224.95. Do you want to...'

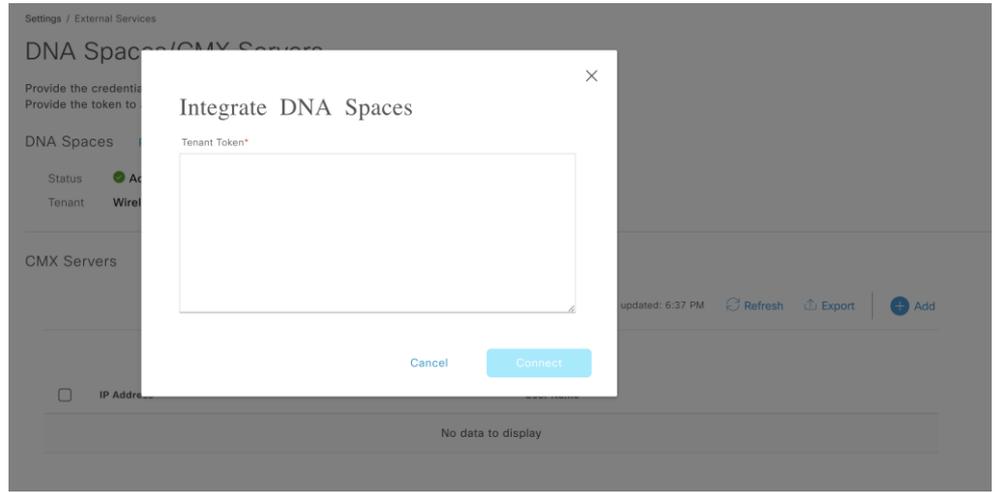
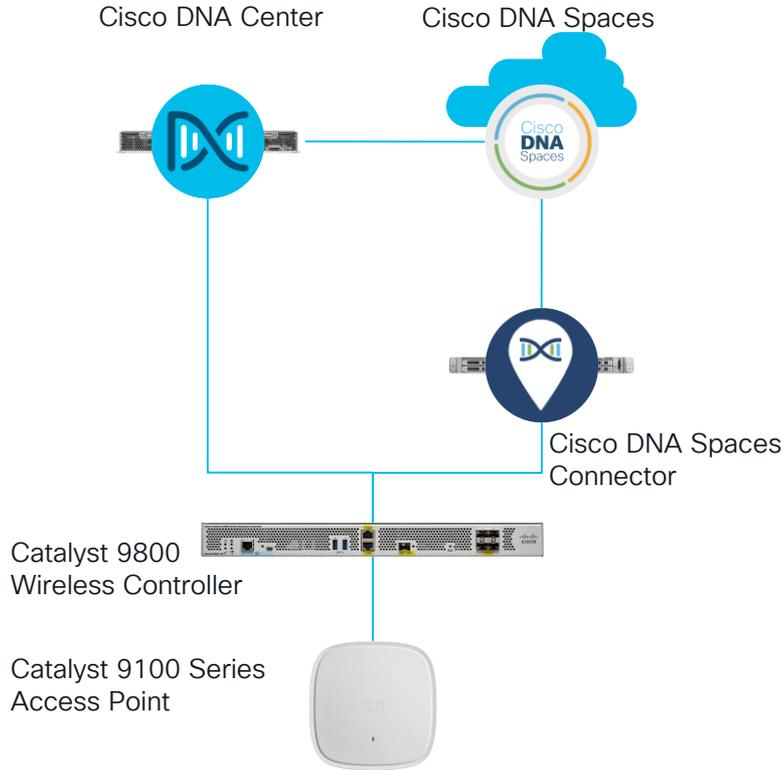
Below the warning, another threat entry is shown for 'Threat 360: Mac C6:9E:38:75:52:D8' with a 'Potential' threat level and 'Interferer' threat type. The interface includes a table with columns for Threat Level, Threat Type, Vendor, Status, Containment Status, and Last Reported.

The bottom section shows a floor plan for 'Global/San Jose/Building 14/Floor1' with several APs labeled: SJC14-TME-AP2, SJC14-TME-AP3, SJC14-TME-AP4, and AP-0001. A red circle highlights a specific location on the floor plan.

# Enabling Location Services



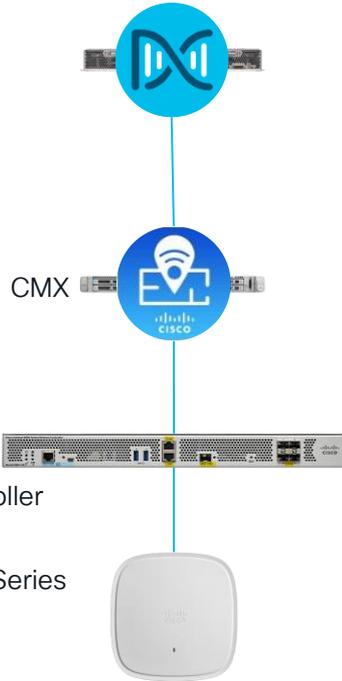
# Enabling Location Services



# Enabling Location Services



Cisco DNA Center



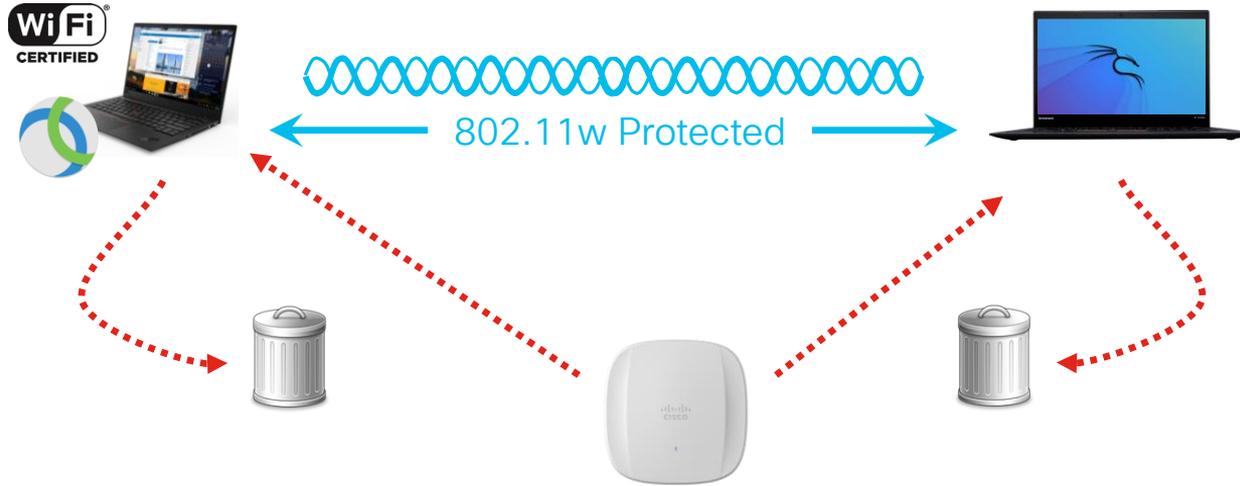
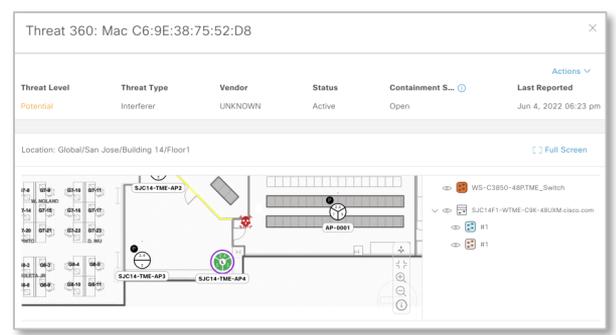
Catalyst 9800  
Wireless Controller

Catalyst 9100 Series  
Access Point

The screenshot shows the 'Settings / External Services' page in Cisco DNA Center. The main section is titled 'DNA Spaces/CMX Servers' and includes instructions: 'Provide the credentials to enable CMX server connectivity by Cisco DNA Center and Provide the token to active DNA Spaces'. Below this, there are tabs for 'DNA Spaces' with 'Reactivate' and 'Deactivate' options. The 'Status' is 'Activated' (indicated by a green dot) and the 'Tenant' is 'WirelessTMEDMZ'. A table for 'CMX Servers' is shown with columns for 'IP Address' and 'User Name', but it is empty with the message 'No data to display'. On the right, a modal window titled 'Add CMX Server' is open, containing input fields for 'IP Address\*', 'User Name\*', 'Password\*', 'SSH User Name\*', and 'SSH Password\*'. At the bottom of the modal are 'Cancel' and 'Add' buttons.



# 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

Configuration > Security > Wireless Protection Policies

Rogue Policies | Rogue AP Rules | Client Exclusion Policies

**General** | **Auto Contain** | Apply

Rogue Detection Security Level	Custom	Auto Containment Level	1
Expiration timeout for Rogue APs (seconds)*	1200	Auto Containment only for Monitor Mode APs	<input type="checkbox"/>
<b>Validate Rogue Clients against AAA</b>	<input type="checkbox"/>	<b>Using our SSID</b>	<input type="checkbox"/>
Validate Rogue APs against AAA	<input type="checkbox"/>	<b>Valid client on Rogue AP</b>	<input type="checkbox"/>
Rogue Polling Interval (seconds)	3600	<b>Adhoc Rogue AP</b>	<input type="checkbox"/>
Detect and Report Adhoc Networks	<input checked="" type="checkbox"/>	<b>MFP Configuration</b>	
Rogue Detection Client Number Threshold*	0	Global MFP State	<input type="checkbox"/>
Rogue Init Timer (seconds)*	180	AP Impersonation Detection	<input type="checkbox"/>
AP Authentication	<input type="checkbox"/>	MFP Key Refresh Interval (hours)*	24
AP Authentication Alarm Threshold*	1		
Syslog Notification	<input type="checkbox"/>		

# Air Marshal

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

### Air Marshal

Configure **Rogue SSIDs 24** Other SSIDs 595 Spoofs 31 Malicious broadcasts 0 Packet floods 0

**24 rogue SSIDs** seen for the last 2 hours

Edit Search...

<input type="checkbox"/>	SSID ▲	Broadcast MACs	Last seen	First seen	Containment	Rogue because
<input type="checkbox"/>	AXE BLE testing	6e:3a:0e:ff:f8:f5 (and 1 other)	4 seconds ago	1 year ago	partial	Recently seen on LAN
<input type="checkbox"/>	IT Test WiFi	e0:cb:bc:49:35:61 (and 1 other)	50 seconds ago	1 month ago	contained	Recently seen on LAN
<input type="checkbox"/>	j-bond-2-owe	c6:14:92:6e:ae:b2 (and 2 others)	15 seconds ago	2 months ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-bond-3-sae	ca:14:a2:6e:ae:b0 (and 1 other)	15 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-bond-5-1x	c6:14:92:6e:ae:a5 (and 4 others)	6 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-bond-8-owe-8	c6:14:92:6e:ae:b8 (and 2 others)	7 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-p1-bond-2-owe	c6:14:92:6e:ae:a2 (and 4 others)	57 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-p1-bond-3-sae	c6:14:92:6e:ae:a3 (and 4 others)	57 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-p1-bond-4-sae	c6:14:92:6e:ae:b4 (and 5 others)	12 seconds ago	22 hours ago	partial	Recently seen on LAN
<input type="checkbox"/>	Meraki Setup	00:18:0a:36:d9:3e (and 98 others)	a moment ago	1 year ago	partial	Recently seen on LAN

10 results per page < 1 2 3 >

Map data ©2023 Google Terms Report a map error

SSID **IT Test WiFi** edit

Containment contained

Last seen Wednesday 11/29/2023 8:25 pm  
50 seconds ago

First seen Wednesday 10/18/2023 7:18 am  
1 month ago

Channels 1, 149

VLANs 0

Broadcast MACs e0:cb:bc:49:35:61 edit  
e2:cb:ac:49:35:61 edit

Wired MACs e0:cb:bc:49:35:61

Encryption Open

Manufacturer Cisco Meraki

Rogue because Recently seen on LAN

Seen by SFO12-1-AP08 (77 dB)  
SFO12-1-AP01 (41 dB)  
SFO12-1-AP03 (41 dB)  
SFO12-1-AP04 (41 dB)  
SFO12-1-AP05 (38 dB)  
SFO12-1-AP02 (34 dB)  
SFO12-1-AP07 (29 dB)  
SFO12-2-AP05 (12 dB)

# Air Marshal

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

The screenshot displays the Air Marshal interface with the following components:

- Navigation:** Configure, Rogue SSIDs 24, Other SSIDs 595, Spoofs 31, Malicious broadcasts 0, Packet floods 0.
- Header:** 24 rogue SSIDs seen for the last 2 hours.
- Modal: Edit SSID containment**
  - Search bar and Edit dropdown.
  - Checkboxes for various SSIDs: AXE BL testing, IT Test WiFi, j-bond-2-owe, j-bond-3-sae, j-bond-5-1x, j-bond-8-owe-8, j-p1-bond-2-owe, j-p1-bond-3-sae, j-p1-bond-4-sae, Meraki Setup.
  - Select a containment type:** Whitelist, Contain, Alert, Uncontain.
  - Buttons: Confirm, Cancel.
- Table of Rogue SSIDs:**

SSID	MAC	Age	Visibility	Location
(and 2 others)		ago		LAN
j-p1-bond-2-owe	c6:14:92:6e:ae:a2 (and 4 others)	57 seconds ago	3 weeks ago	partial Recently seen on LAN
j-p1-bond-3-sae	c6:14:92:6e:ae:a3 (and 4 others)	57 seconds ago	3 weeks ago	partial Recently seen on LAN
j-p1-bond-4-sae	c6:14:92:6e:ae:b4 (and 5 others)	12 seconds ago	22 hours ago	partial Recently seen on LAN
Meraki Setup	00:18:0a:36:d9:3e (and 98 others)	a moment ago	1 year ago	partial Recently seen on LAN
- Details for IT Test WiFi:**
  - SSID: IT Test WiFi
  - Containment: contained
  - Last seen: Wednesday 11/29/2023 8:25 pm, 50 seconds ago
  - First seen: Wednesday 10/18/2023 7:18 am, 1 month ago
  - Channels: 1, 149
  - VLANs: 0
  - Broadcast MACs: e0:cb:bc:49:35:61, e2:cb:ac:49:35:61
  - Wired MACs: e0:cb:bc:49:35:61
  - Encryption: Open
  - Manufacturer: Cisco Meraki
  - Rogue because: Recently seen on LAN
  - Seen by: SFO12-1-AP08 (77 dB), SFO12-1-AP01 (41 dB), SFO12-1-AP03 (41 dB), SFO12-1-AP04 (41 dB), SFO12-1-AP05 (38 dB), SFO12-1-AP02 (34 dB), SFO12-1-AP07 (29 dB), SFO12-2-AP05 (12 dB)

# Air Marshal

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

The screenshot displays the Cisco Air Marshal interface. At the top, there are navigation tabs: "Configure", "Rogue SSIDs 24", "Other SSIDs 595", "Spoofs 31", "Malicious broadcasts 0", and "Packet floods 0". Below this, a section titled "24 rogue SSIDs" is visible, with a search bar and a filter for "seen for the last 2 hours". A modal window titled "Edit Broadcast MAC containment" is open, showing a list of SSIDs on the left and a configuration panel on the right. The configuration panel includes a "Select a containment type" section with buttons for "Whitelist", "Contain", "Alert", and "Uncontain", and "Confirm" and "Cancel" buttons at the bottom. The SSID list includes entries like "AXE BL testing", "IT Test WiFi", and several "j-bond-2-owe" and "j-p1-bond-2-owe" entries with their respective MAC addresses and last seen times. A detailed view of the "IT Test WiFi" entry is shown on the right, including its containment status, last and first seen times, channels, broadcast MACs, wired MACs, encryption, manufacturer, and rogue cause.

SSID	MAC	Last seen	First seen	Channels	Broadcast MACs	Wired MACs	Encryption	Manufacturer	Rogue because	Seen by
AXE BL testing										
IT Test WiFi		11/29/2023 8:25 pm	10/18/2023 7:18 am	1, 149	e0:cb:bc:49:35:61	e0:cb:bc:49:35:61	Open	Cisco Meraki	Recently seen on LAN	SFO12-1-AP08 (77 dB) SFO12-1-AP01 (41 dB) SFO12-1-AP03 (41 dB) SFO12-1-AP04 (41 dB) SFO12-1-AP05 (38 dB) SFO12-1-AP02 (34 dB) SFO12-1-AP07 (29 dB) SFO12-2-AP05 (12 dB)
j-bond-2-owe	c6:14:92:6e:ae:a2	57 seconds ago	3 weeks ago							
j-p1-bond-2-owe	c6:14:92:6e:ae:a3	57 seconds ago	3 weeks ago							
j-bond-3-sae	c6:14:92:6e:ae:a3	57 seconds ago	3 weeks ago							
j-p1-bond-3-sae	c6:14:92:6e:ae:a3	57 seconds ago	3 weeks ago							
j-bond-4-sae	c6:14:92:6e:ae:b4	12 seconds ago	22 hours ago							
j-p1-bond-4-sae	c6:14:92:6e:ae:b4	12 seconds ago	22 hours ago							
Meraki Setup	00:18:0a:36:d9:3e	a moment ago	1 year ago							

# Air Marshal

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

Should clients be able to connect to rogue SSIDs by default? ⓘ

Allow clients to connect to rogue SSIDs by default

Rogue SSIDs will only be contained if you specify them in the containment list below. The setting is appropriate when you have either non-Meraki access points or Meraki access points from other Organizations on your LAN.

Block clients from connecting to rogue SSIDs by default

Your Meraki access points will block clients from connecting to all rogue SSIDs by default. This setting is appropriate when you have all Meraki access points at your site and is better for security. You can allow connections to individual SSIDs by using the Allow list below.

SSID Block list ⓘ

These rules will apply to SSIDs seen on and off the LAN.

Add a match

SSID Allow list ⓘ

Rogue or Other SSIDs matching these rules will be accessible for clients, overriding your default block policy and any that you've Blocked.

Meraki won't send alerts about SSIDs matching rules on the Allow list.

Add a match

SSID alerting ⓘ

Rogue or Other SSIDs matching these rules (but not a rule in the SSID Allow list) will trigger an email or syslog alert, if configured. Meraki won't prevent clients from connecting to these SSIDs.

Add a match

# 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



Tools / Security Advisories

Click [here](#) to access customized security advisories based on your device configuration, powered by CX Cloud.

ADVISORIES: 2 Critical, 39 High, 28 Medium

SCAN CRITERIA: 5 Software Version, 0 Custom, 0 Advanced

Re-scan Network

Settings

Devices (64)

Device Name	IP Address	Advisories	Platform	Image Version
ASR1K_TME.ASR1K_TME	172.20.224.132	69	C1111-8P	16.9.4
SJC14F1-WTME-C9K-48UXM.cisco.com	172.20.224.109	69	C9300-48UXM	16.9.4
c9800-40-TMEDNAC.cisco.com	172.20.224.55	0	C9800-40-K9	17.8.1
SpacesWLC	172.20.226.210	0	C9800-CL-K9	17.9.20220411:075
Spirent_WLC.cisco.com	172.20.224.56	0	C9800-40-K9	17.7.20210815:031

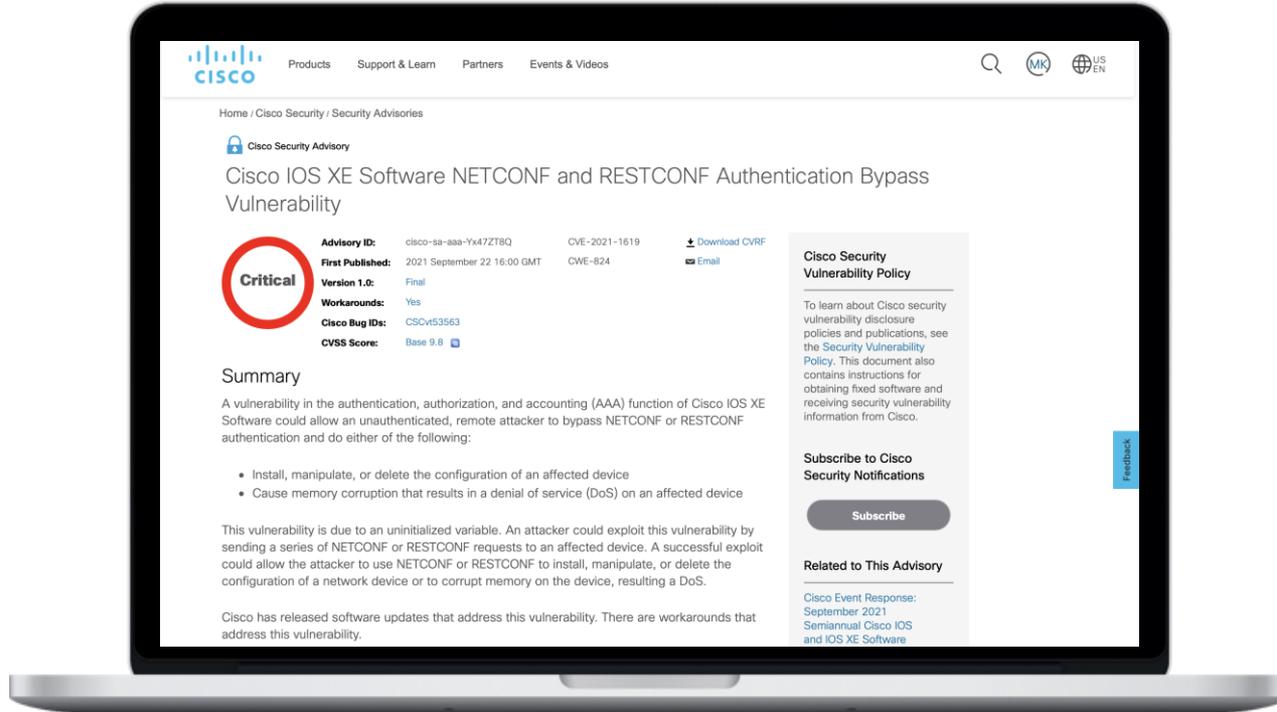
# Cisco Catalyst Center Security Advisories



The screenshot displays the Cisco DNA Center interface for Security Advisories. The main content area shows details for device SJC14F1-WTME-C9K-48UXM.cisco.com (172.20.224.109), which is reachable and has an uptime of 25 days 7 hrs 10 mins. A table lists 69 advisories, with one highlighted in a red box:

Advisory ID	Advisory Title	CVSS Score	Impact	Fix Version
<a href="#">cisco-sa-aaa-Yx47ZT8Q</a>	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability	9.8	Critical	16.9.8
<a href="#">cisco-sa-tenetd-EFJrEzPx</a>	Telnet Vulnerability Affecting Cisco Products: June 2020	9.8	High	16.9.6
<a href="#">cisco-sa-ioxPE-KgGvCAf9</a>	Cisco IOx for IOS XE Software Privilege Escalation Vulnerability	9.8	Critical	N/A

# Cisco Catalyst Center Security Advisories



# Cisco Catalyst Center Security Advisories



**Affected Products**

**Vulnerable Products**

This vulnerability affects Cisco IOS XE Software if it is running in autonomous or controller mode and Cisco IOS XE SD-WAN Software. For either to be affected, all of the following must be configured:

- AAA
- NETCONF, RESTCONF, or both
- **enable password** without **enable secret**

For information about which Cisco software releases are vulnerable, see the [Fixed Software](#) section of this advisory.

**Note:** The standalone Cisco IOS XE SD-WAN release images are separate from the universal Cisco IOS XE Software releases. The SD-WAN feature set was first integrated into the universal Cisco IOS XE Software releases starting with IOS XE Software Release 17.2.1r. For additional information, see the [Install and Upgrade Cisco IOS XE Release 17.2.1r and Later](#) chapter of the [Cisco SD-WAN Getting Started Guide](#).

**Determine the Device Configuration**

To determine whether a device has a vulnerable configuration, do the following:

**Check AAA Configuration**

To determine whether AAA authentication is configured on the device, use the **show running-config | include aaa authentication login** command, as shown in the following example:

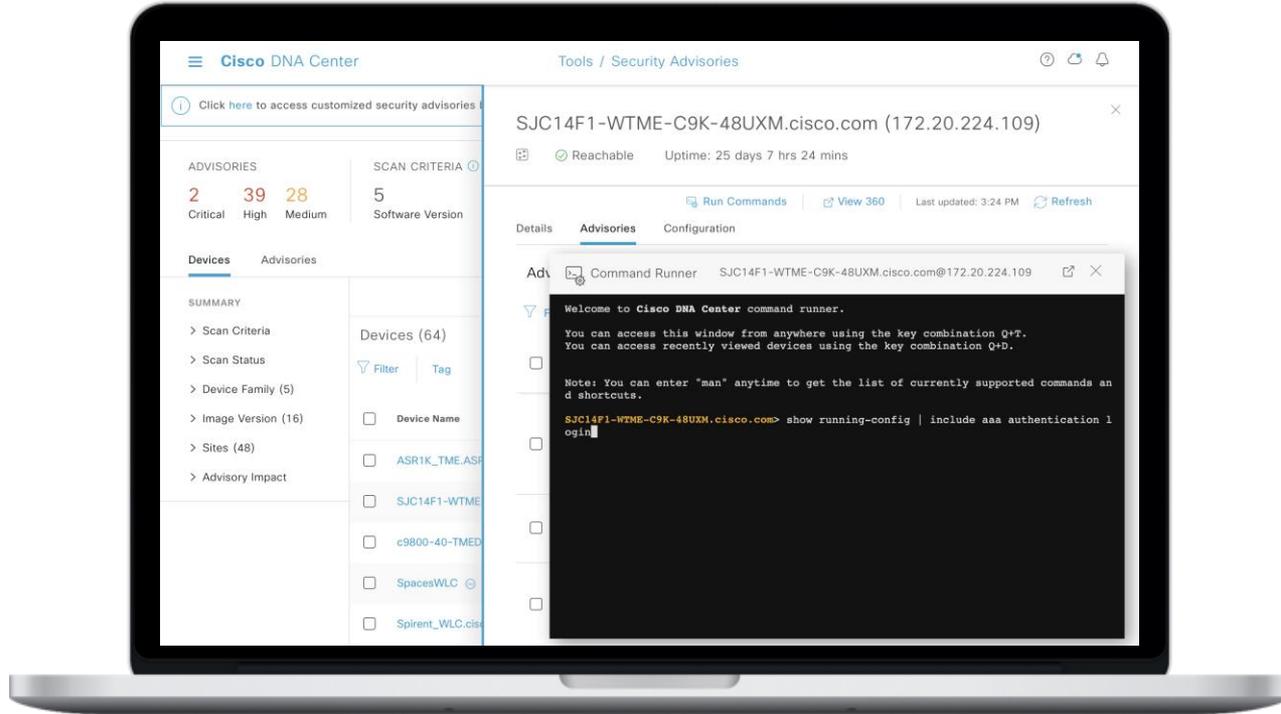
```
Router#show running-config | include aaa authentication login
aaa authentication login default local group example
Router#
```

5 star 0  
4 star 0  
3 star 0  
2 star 0  
1 star 0

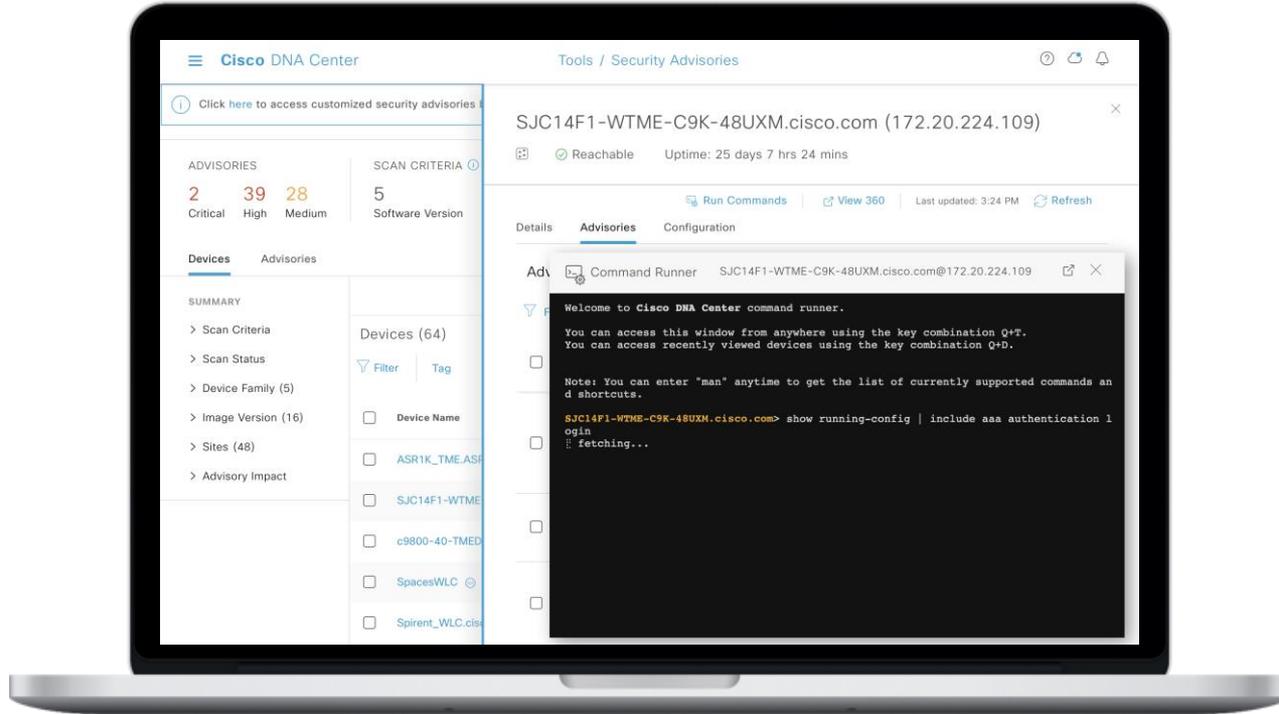
[Leave additional feedback](#)

[Feedback](#)

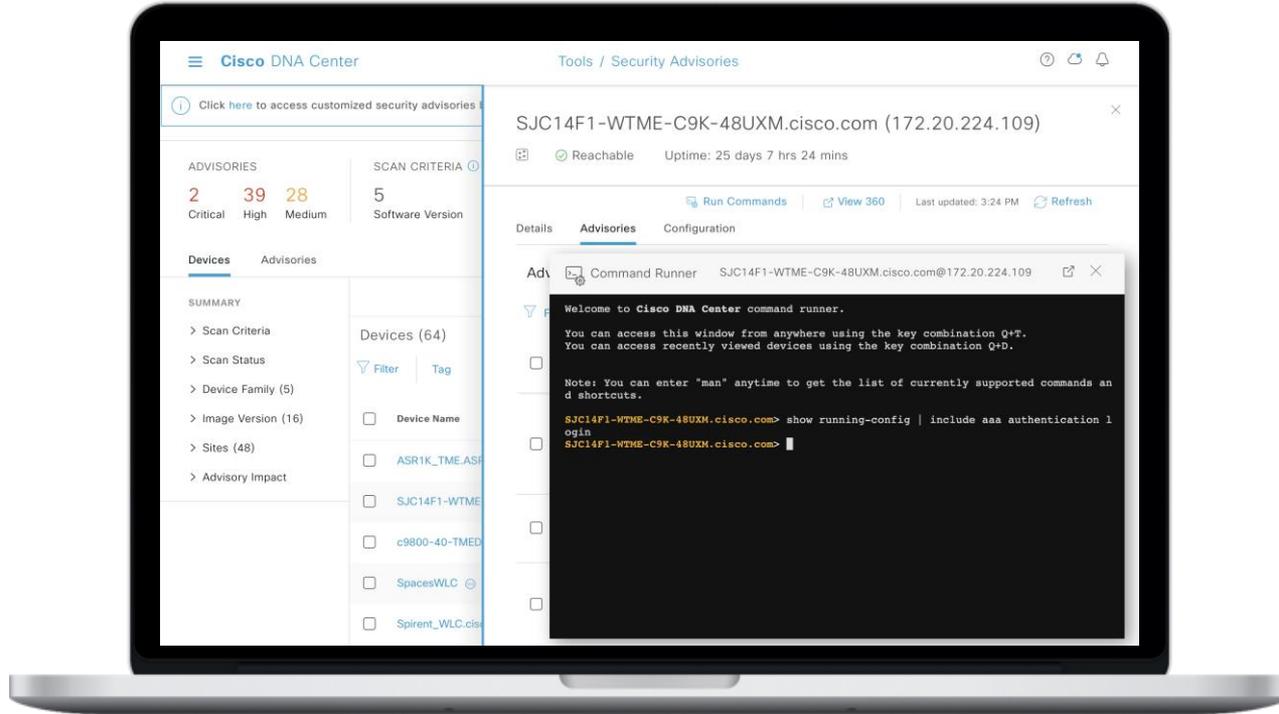
# Cisco Catalyst Center Security Advisories



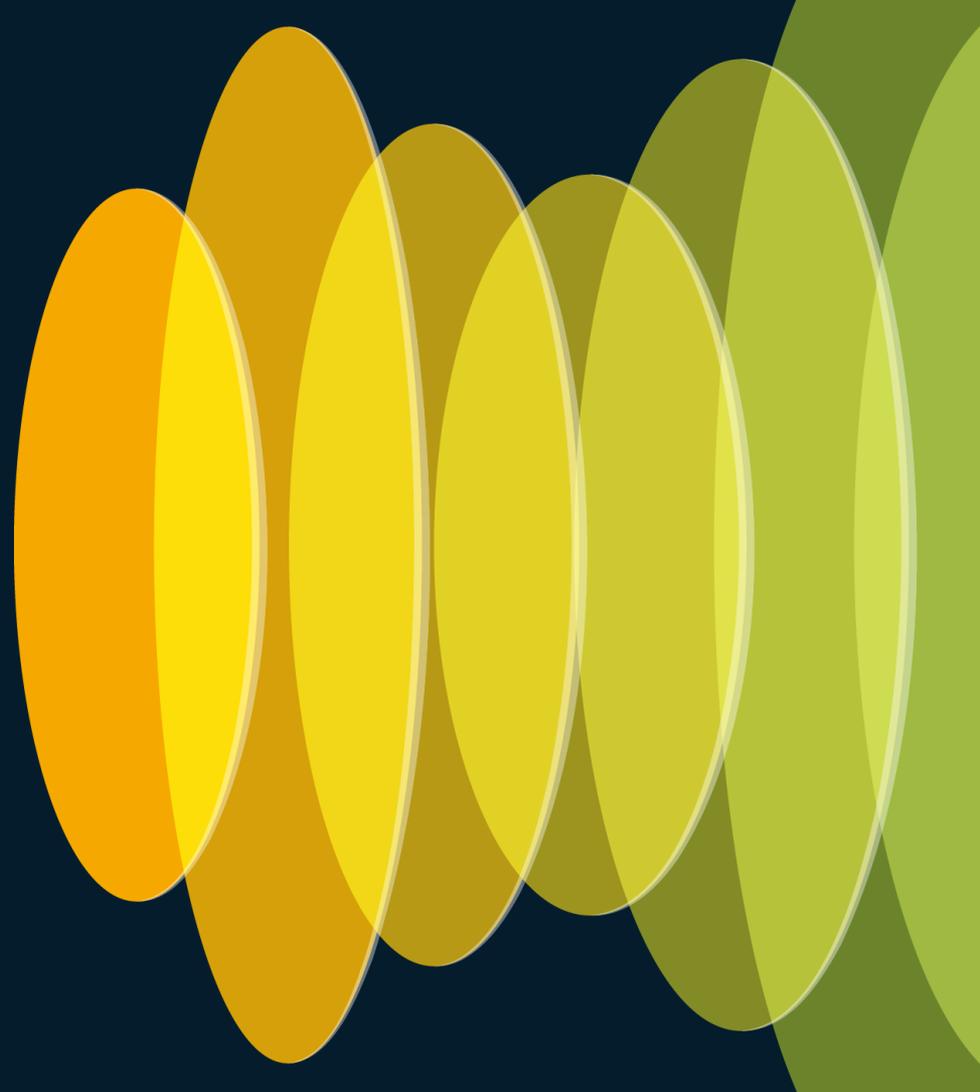
# Cisco Catalyst Center Security Advisories



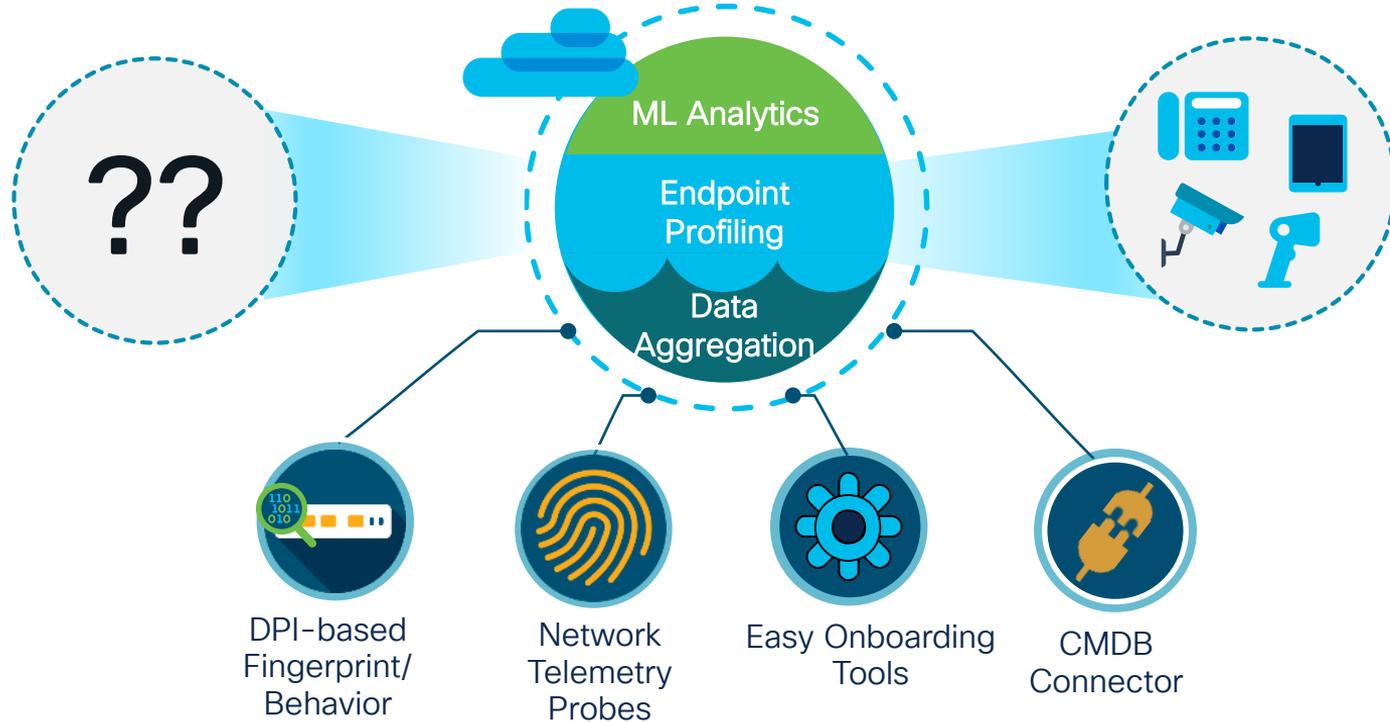
# Cisco Catalyst Center Security Advisories



# Network as a Sensor and Enforcer



# Cisco Catalyst Center AI Endpoint Analytics



# Network as a Sensor

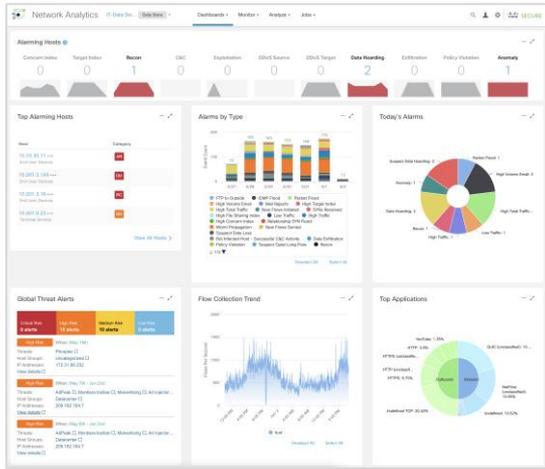
## Secure Network Analytics Integration



Netflow



Malware detection and cryptographic compliance on Cisco Stealthwatch



Top Security Events for 10.201.3.18

Security Event	Count	Concern Index	First Active	Target Host	Target Host Group	Actions
Port Scan - 49195	50	546,000	06/02 3:51:05 PM	10.201.0.16	Atlanta	...
Port Scan - 53	16	172,800	06/02 3:51:05 PM	10.201.0.16	Domain Controllers , Atlanta , DNS Servers	...
Port Scan - 5355	2	21,600	06/02 4:48:48 PM	10.201.0.23	Terminal Servers , Atlanta , Datacenter	...

**DNS Abuse**

**Alert Type Details**

Description: Device has been sending unusually large DNS packets. This alert uses the Unusual Packet Size observation and may indicate an attacker using the DNS protocol as a covert communications channel to exfiltrate data.

MITRE Tactics: **Exfiltration**

MITRE Techniques: **Exfiltration Over Alternative Protocol**

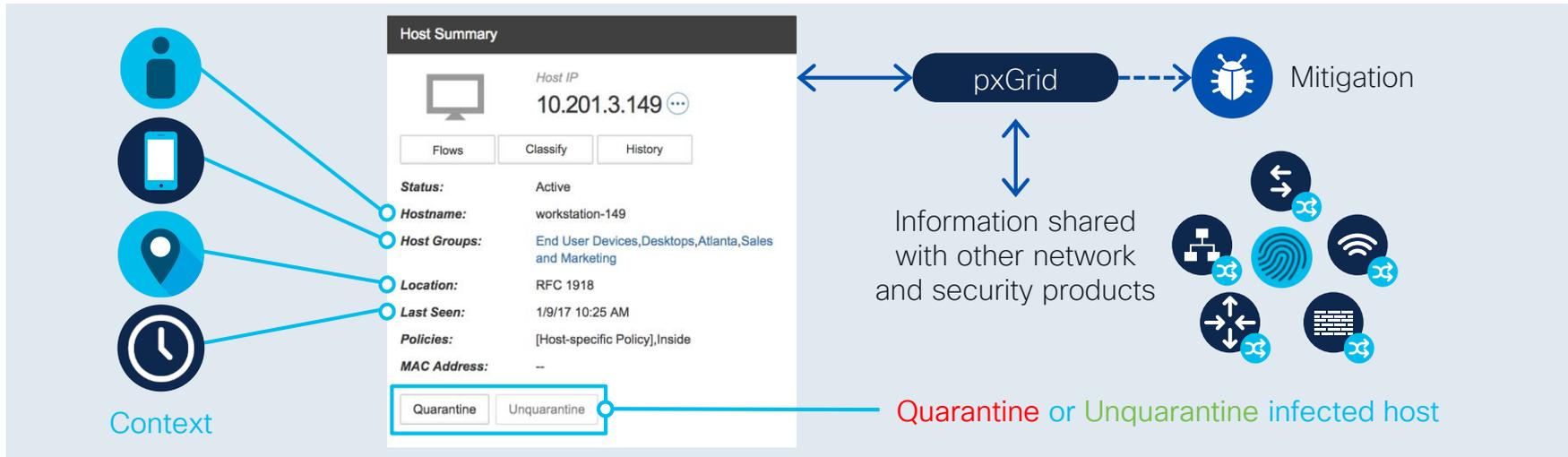
Alert Type Priority: **Normal (Default)**

[go to alert priorities page](#)



# Network as an Enforcer

## Rapid Threat Containment



Identity Services Engine



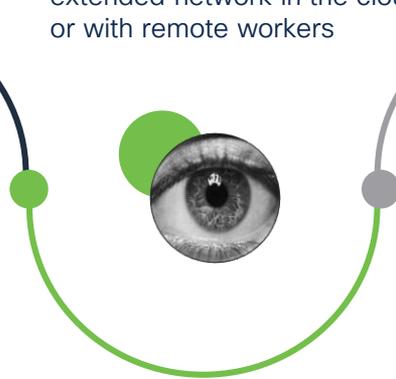
Secure Network Analytics Management Console

# 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



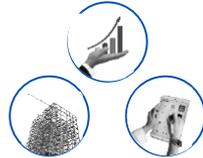
## Encrypted traffic analytics

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



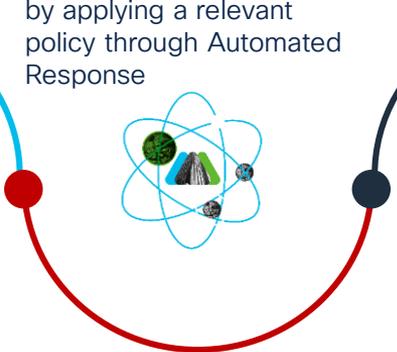
## Smart segmentation

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

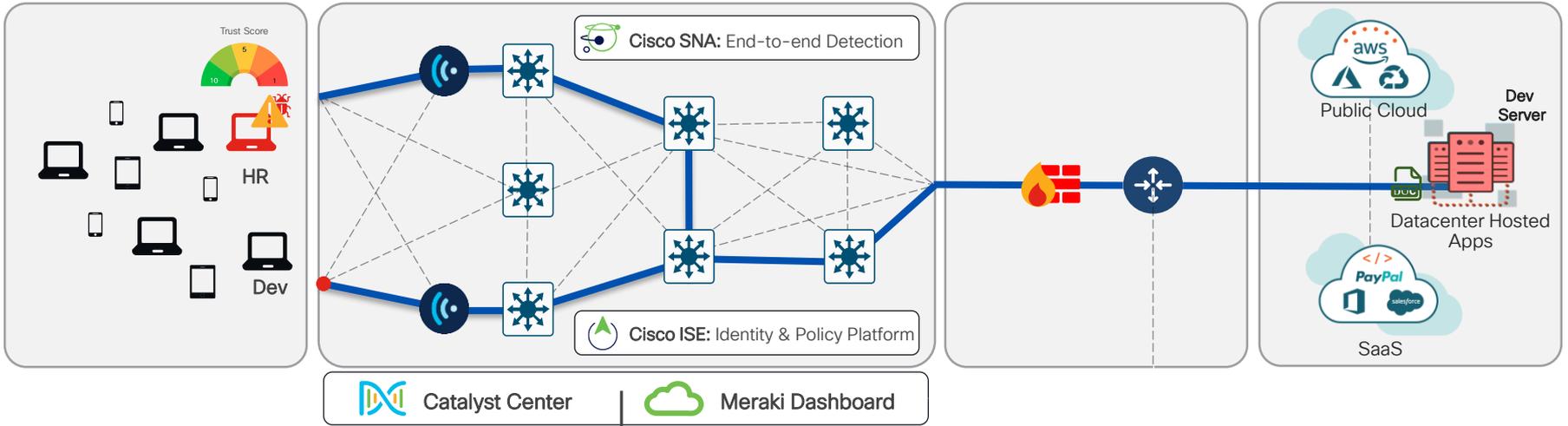


## Immediate threat remediation

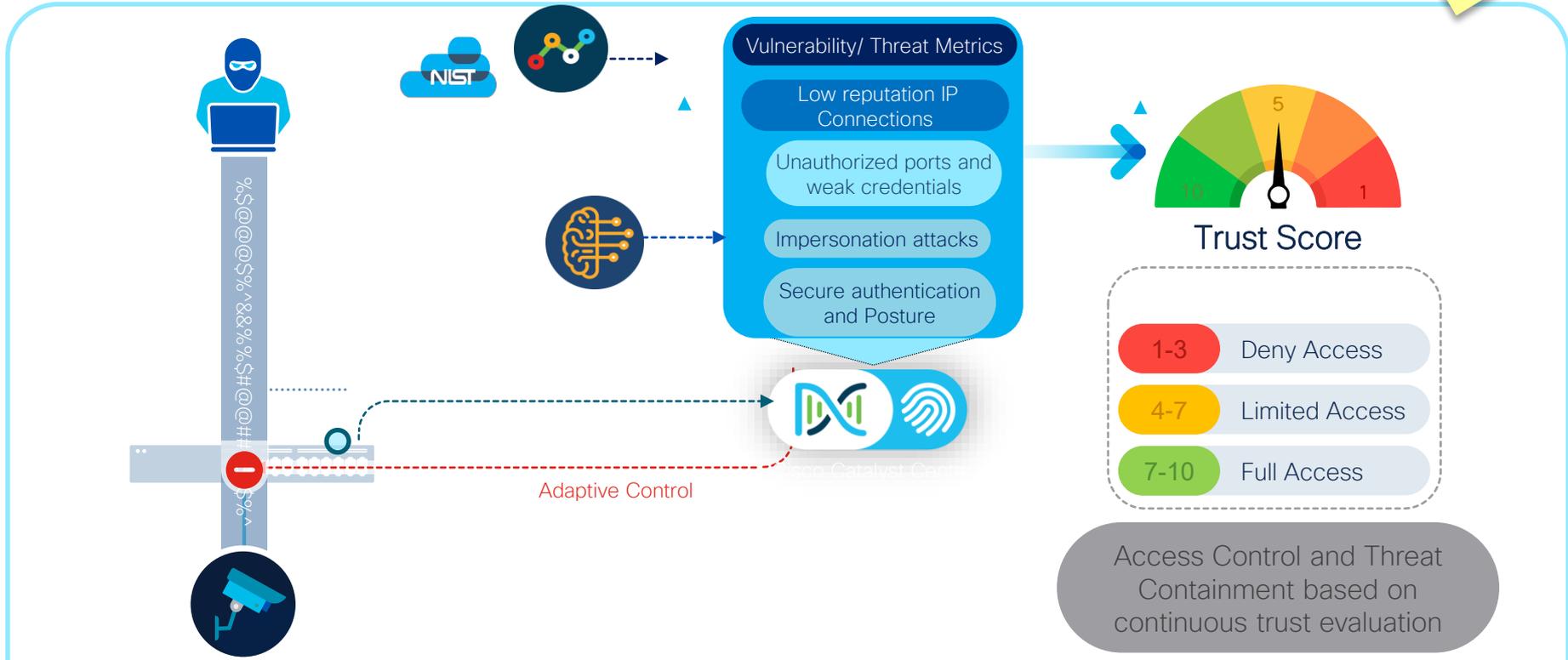
Use the network to remove the infected host by applying a relevant policy through Automated Response



# Compromised Client



# Trust Based Network Access





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)



# 2.2 Trillion

## Threat Artifacts Analyzed Daily

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

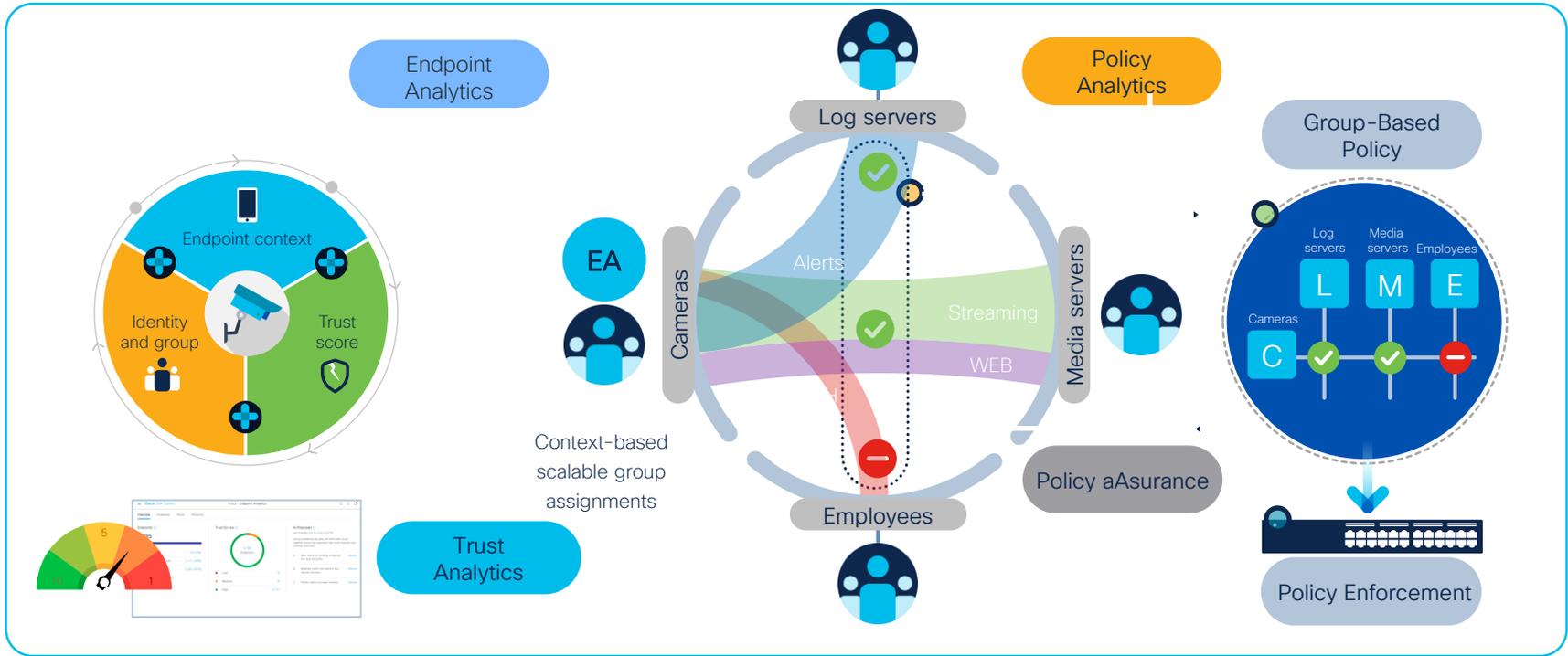


# 11 Billion

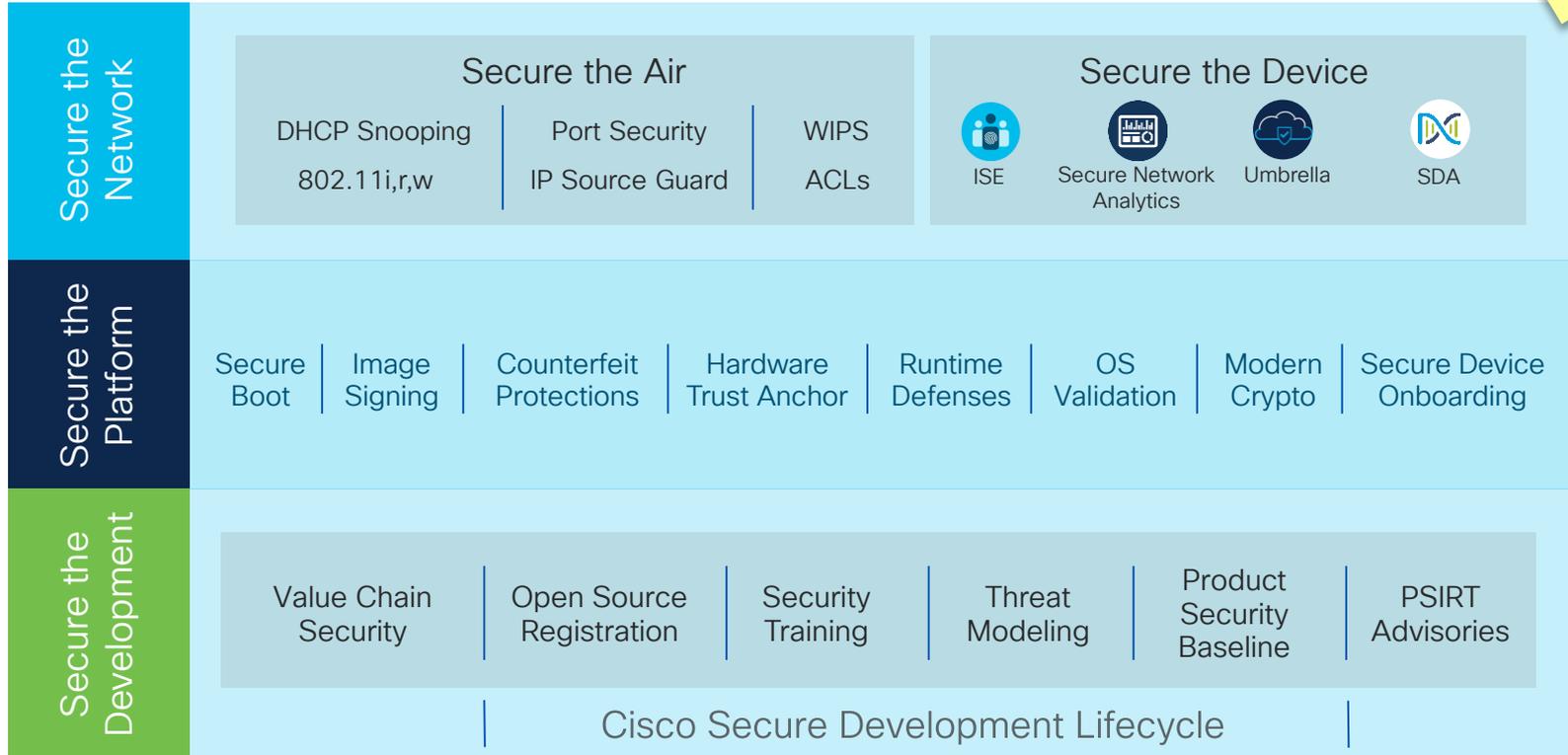
## Threat Responses Initiated Daily

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



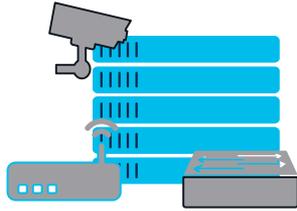
# Secured Infrastructure with Trusted Platform



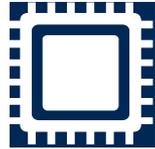
- Secure Boot With ACT2 chip
- Image Signing Authentic OS
- Integrity Verifications Malware Protection
- SUDI Support Two-way trust
- Best-In Class Security Automatic code encryption
- Runtime Defenses 64 bit ASLR



# Trustworthy Solutions



Manufacturing



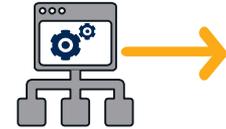
Hardware



BIOS/ROMMON



Software Image



System Booted



Trust Anchor Module w/SUDI



Trust Anchor Module w/SUDI

+



Secure Boot

+



Image Signing



Runtime Defenses

# Cisco Secure Networking



# Securing the Wireless Network





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.

START

Monday, June 3 | 8:30 a.m.

**BRKEWN-2054**

Designing the Right Enterprise Wireless Architecture for Challenging Environments (On-Premises, Cloud, and Hybrid)

Monday, June 3 | 10:30 a.m.

**BRKEWN-2035**

Design your Enterprise Wireless Network with Cisco Meraki

Monday, June 3 | 11:00 a.m.

**BRKENS-2834**

IPv6-Enabled Wireless (Wi-Fi) Access: Design and Deployment Strategies

Tuesday, June 4 | 10:30 a.m.

**BRKEWN-3004**

Understanding Wireless Security and the Implications for Secure Wireless Network Design

Wednesday, June 5 | 10:30 a.m.

**BRKEWN-2926**

Tune Your Cisco Wi-Fi Designs for the Most Demanding Clients and Applications, Boosted with Applied AI

Thursday, June 6 | 9:30 a.m.

**BRKEWN-2658**

Implement and Troubleshoot Cisco Spaces to Deliver Next-Generation Location-Based Solutions

Thursday, June 6 | 1:00 p.m.

**BRKEWN-2037**

OpenRoaming Under the Hood

FINISH

# 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](https://www.CiscoLive.com/on-demand)