

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Understanding Wireless Security

And the Implications for Secure Wireless Network Design

Mark Krischer, Principal Wireless Architect
Asia Pacific, Japan & Greater China
BRKEWN-2104

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 until November 15, 2024



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2104>

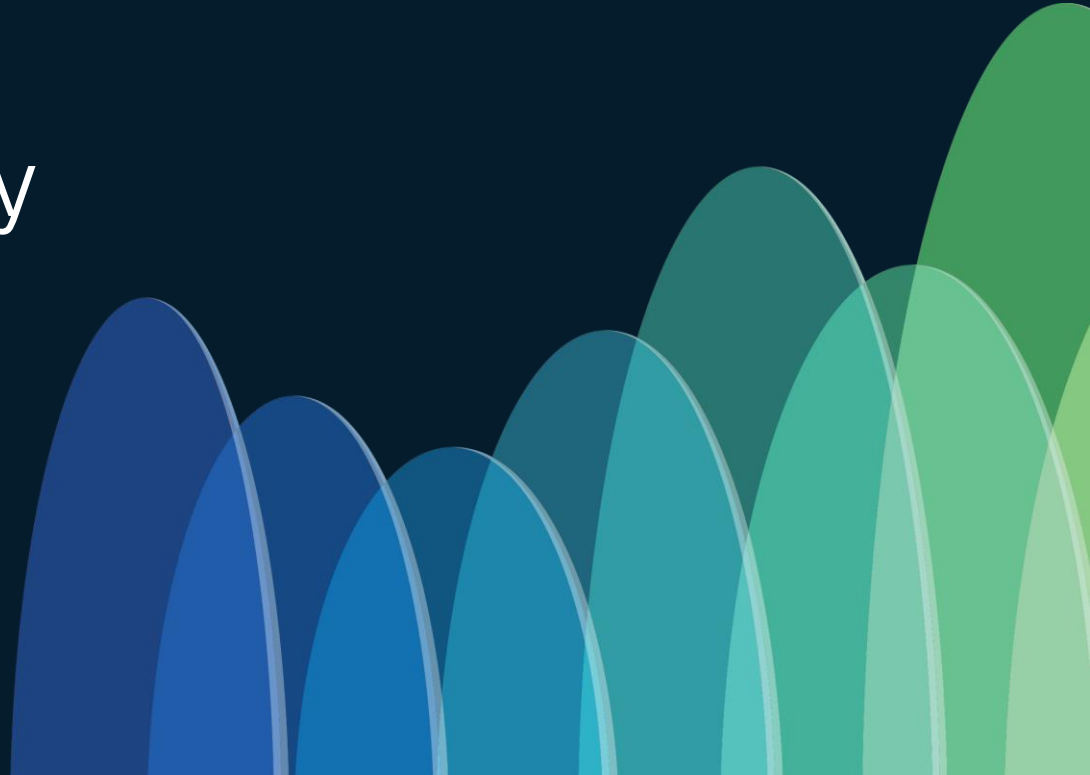


Agenda

- 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



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



Secure the
Air



Secure the
Devices



Secure the
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

Wireless LAN Types



WPA3



- Mandatory for Wi-Fi 6 and Wi-Fi 7 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)

WPA3

FYI

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

802.11 Fundamentals

Authentication



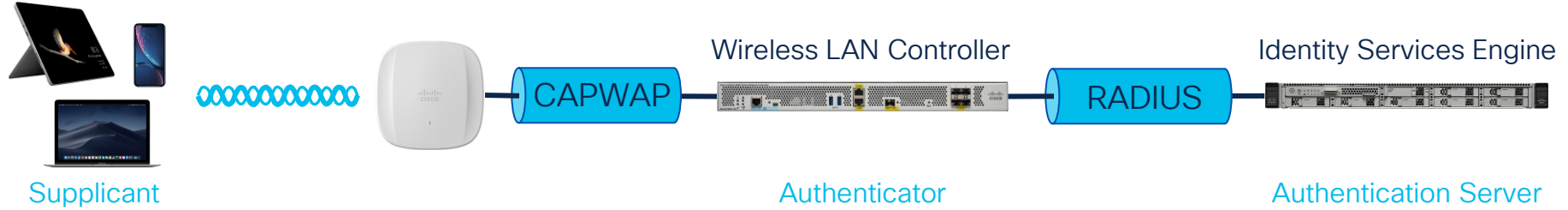
802.11 Fundamentals

Authentication



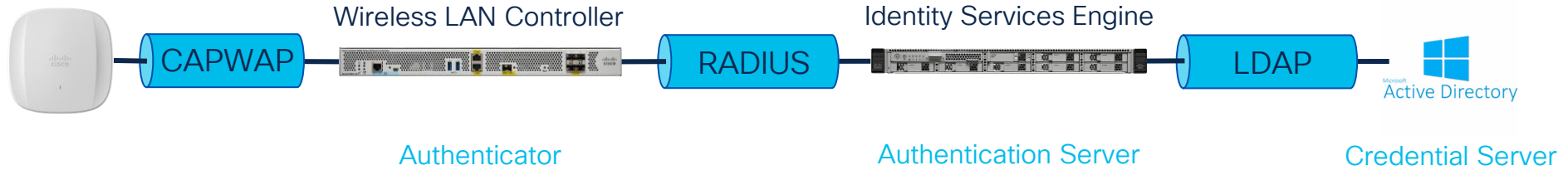
802.11 Fundamentals

Authentication



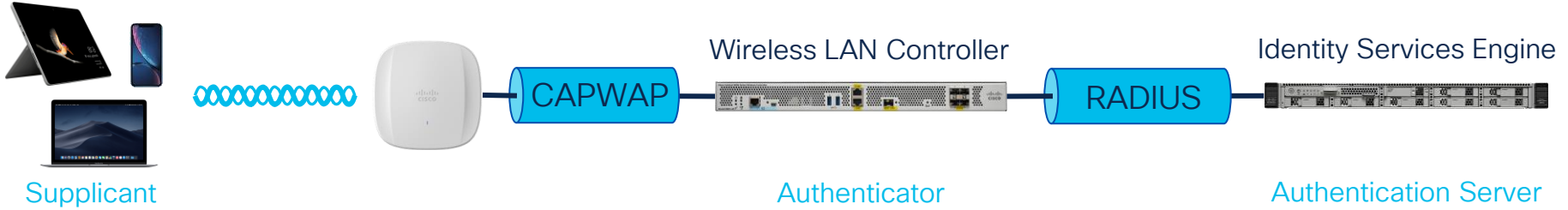
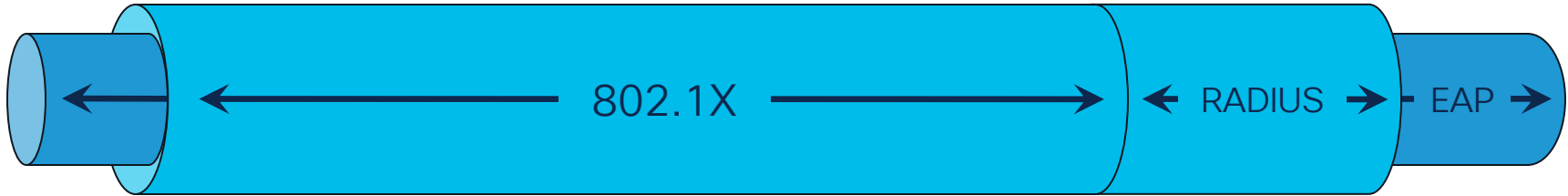
802.11 Fundamentals

Authentication

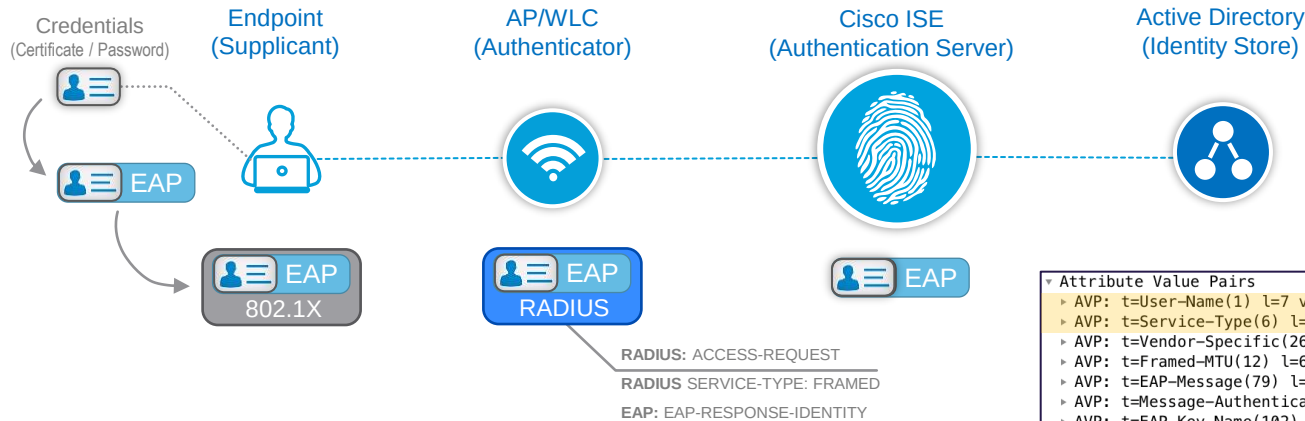


802.11 Fundamentals

Authentication



802.1X



EAP: Extensible Authentication Protocol

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

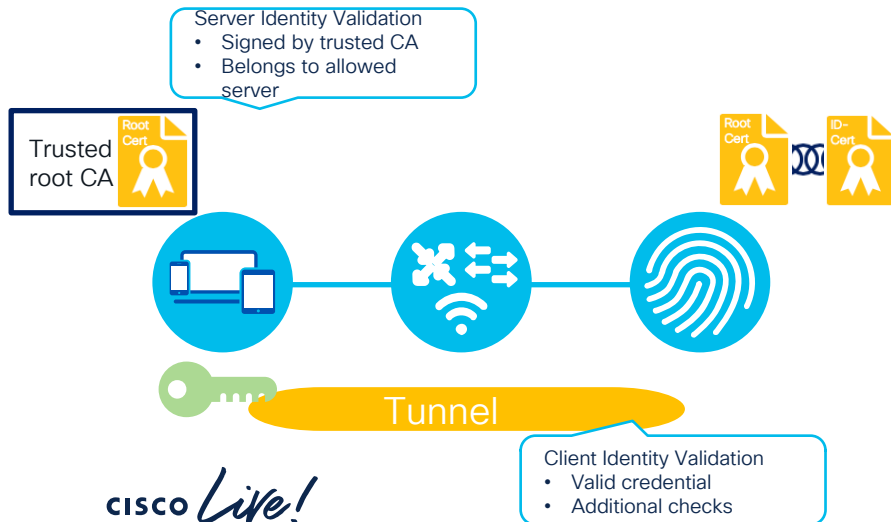
```
Attribute Value Pairs
  AVP: t=User-Name(1) l=7 val=hosuk
  AVP: t=Service-Type(6) l=6 val=Framed(2)
  AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
  AVP: t=Framed-MTU(12) l=6 val=1485
  AVP: t=EAP-Message(79) l=12 Last Segment[1]
  AVP: t=Message-Authenticator(80) l=18 val=10c87be3950f1cec07ae61f4dfad789a
  AVP: t=EAP-Key-Name(102) l=2 val=
  AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
  AVP: t=NAS-IP-Address(4) l=6 val=192.168.201.61
  AVP: t=NAS-Port-Id(87) l=17 val=capwap_90000004
  AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
  AVP: t=NAS-Port(5) l=6 val=8013
  AVP: t=Called-Station-Id(30) l=31 val=38:0e:4d:4a:3b:20:C9800-D0T1X
  AVP: t=Calling-Station-Id(31) l=19 val=08:e6:89:2d:26:4d
  AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
  AVP: t=Vendor-Specific(26) l=35 vnd=ciscoSystems(9)
  AVP: t=NAS-Identifier(32) l=10 val=C9800-CL
```

EAP-PEAP-MSCHAPv2 and EAP-TLS

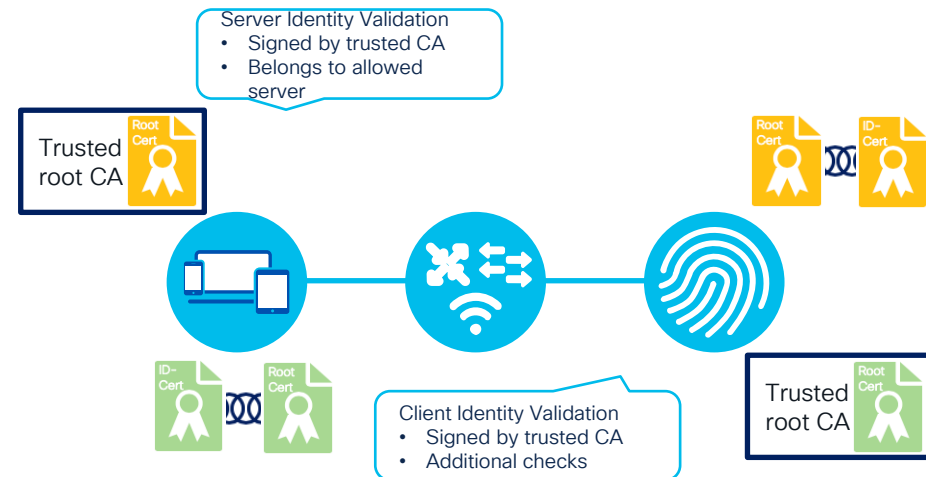


- Both: Use of server certificate
- EAP-TLS: Mutual certificate authentication
- EAP-PEAP: Use of tunnel to encrypt transport

EAP-PEAP-MSCHAPv2

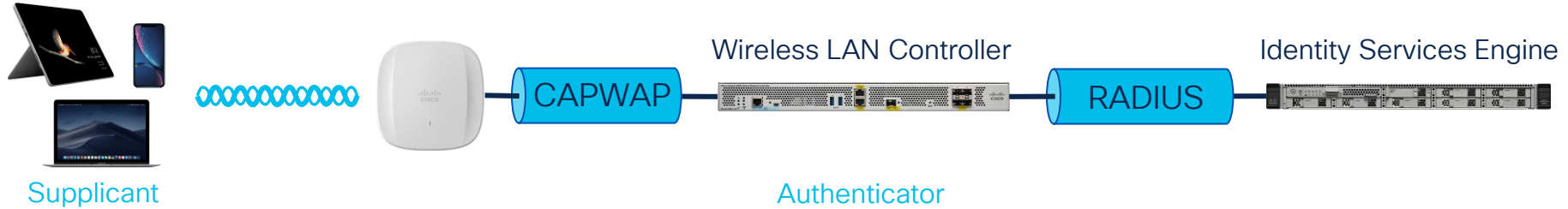
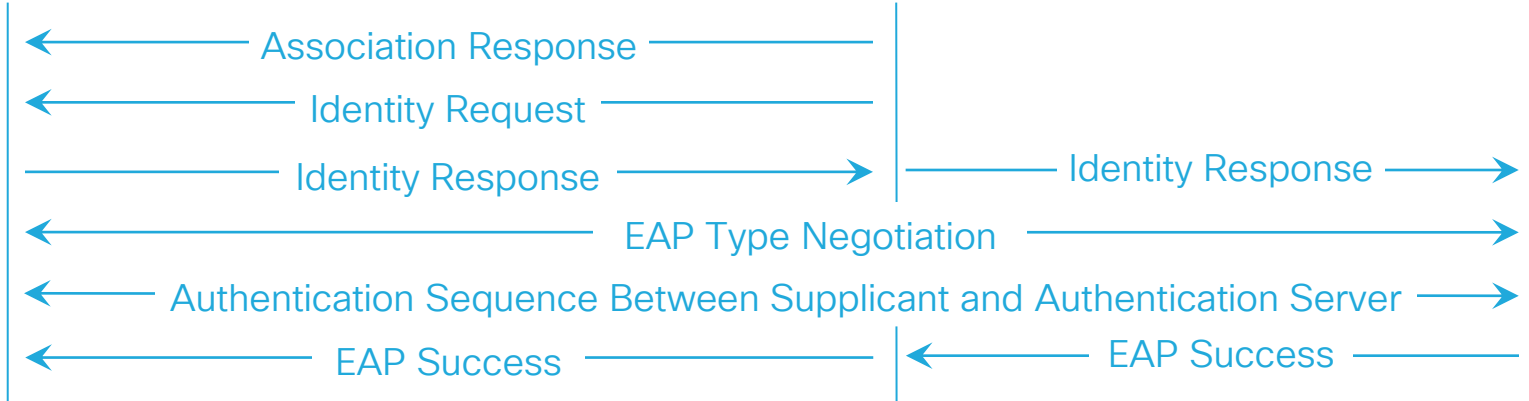


EAP-TLS



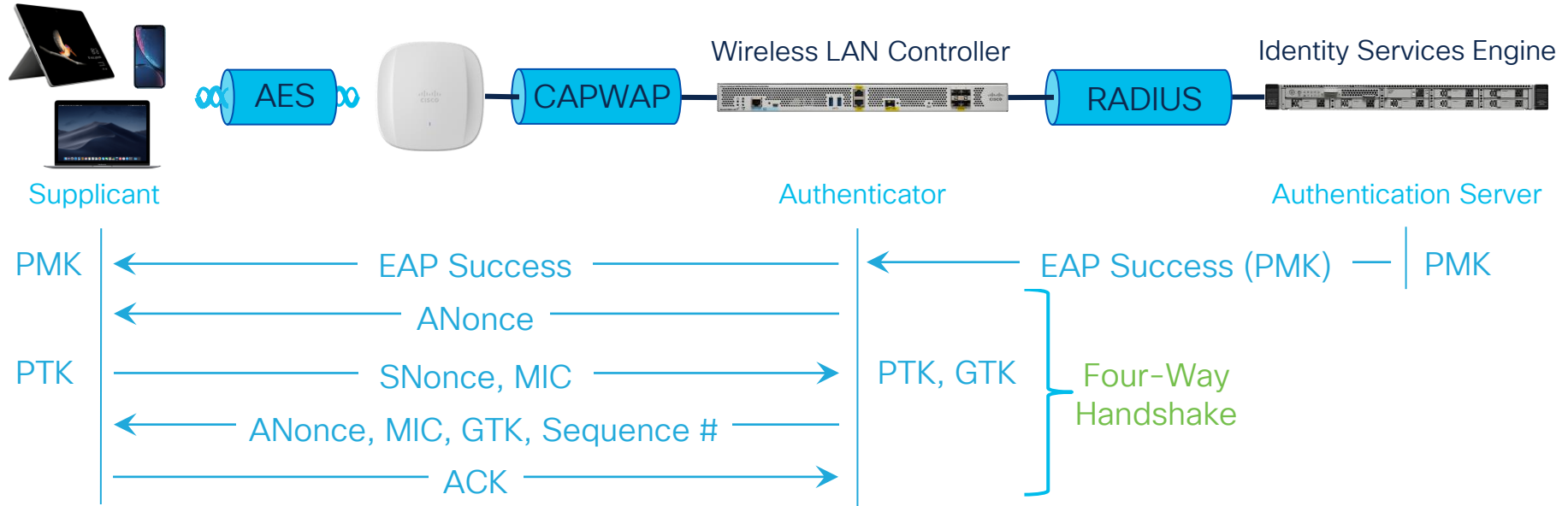
802.11 Fundamentals

Authentication



802.11 Fundamentals

Encryption



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

FlexConnect Support – 192-bit Encryption

Existing

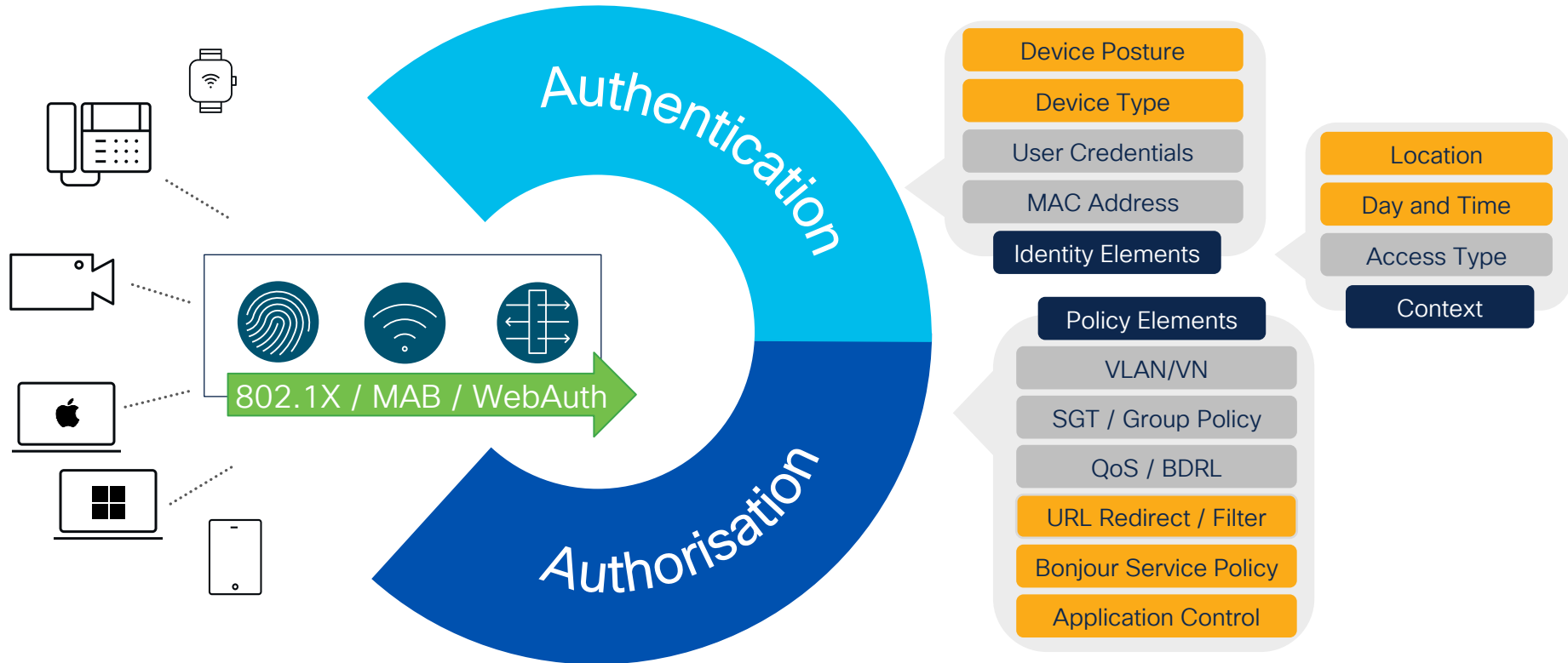
- ❑ Support of AKM Suite-B-192-802.1x(AKM 12) and Suite-B-802.1x(AKM 11) is already supported in Local Mode deployments

New

NEW

- ❑ Starting from IOS-XE 17.15.1, the support of AKM Suite-B-192-802.1x(AKM 12) and Suite-B-802.1x(AKM 11) is available in FlexConnect mode deployments too. Supported in both Central Auth and Local Auth configurations.

Authentication and Authorisation

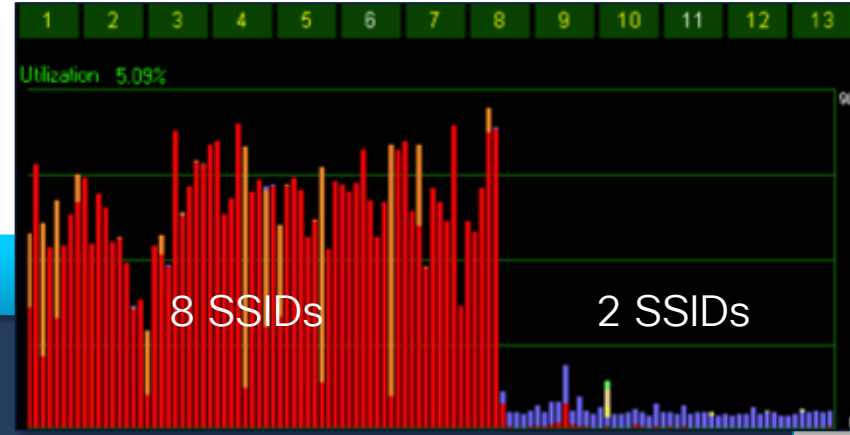


Authorisation

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



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

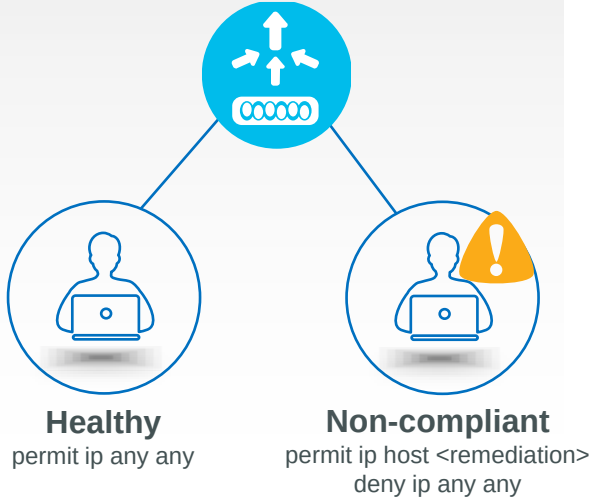
Assigns multiple access characteristics: VLAN, ACL, QoS, Timer, etc.

Authorization Options



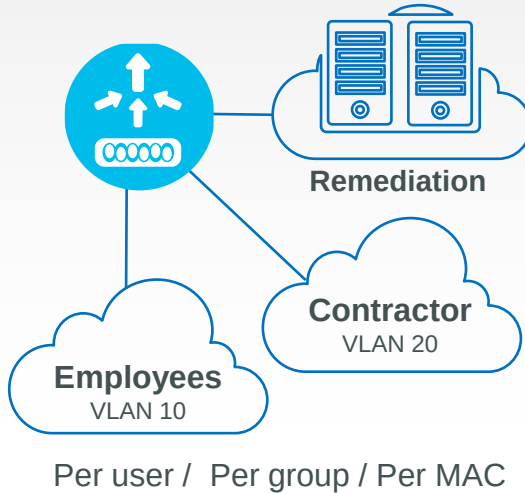
Named ACL

Named ACL



VLANs

Dynamic VLAN Assignments



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: AirSpace Interface Name

vlan 10
name employee
vlan 20
name contractor



RADIUS: Access-Accept
Username = Peter
AirSpace-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"/>	✕

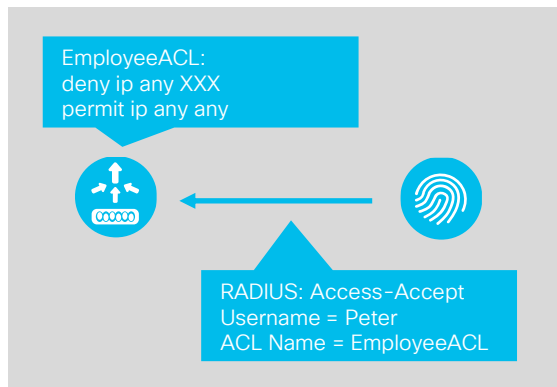
[Add a Named VLAN](#)

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

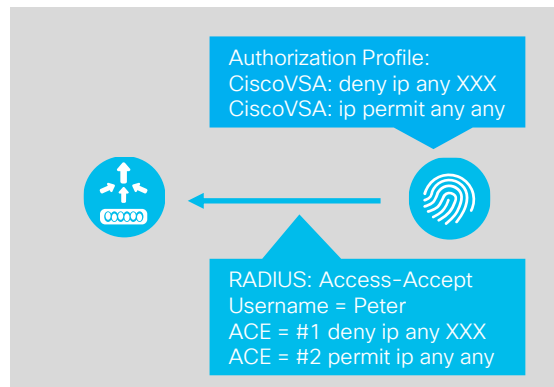
RADIUS Enforced ACLs



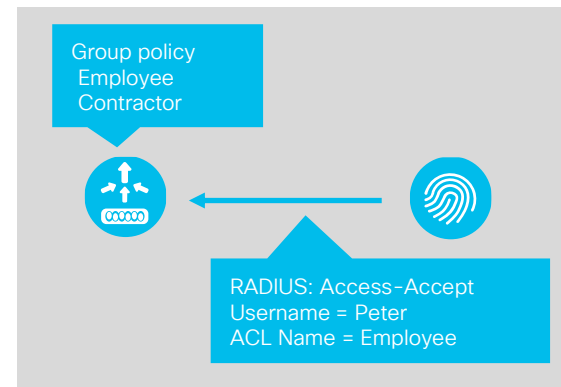
Named ACL



Per-User ACL



Group policy



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



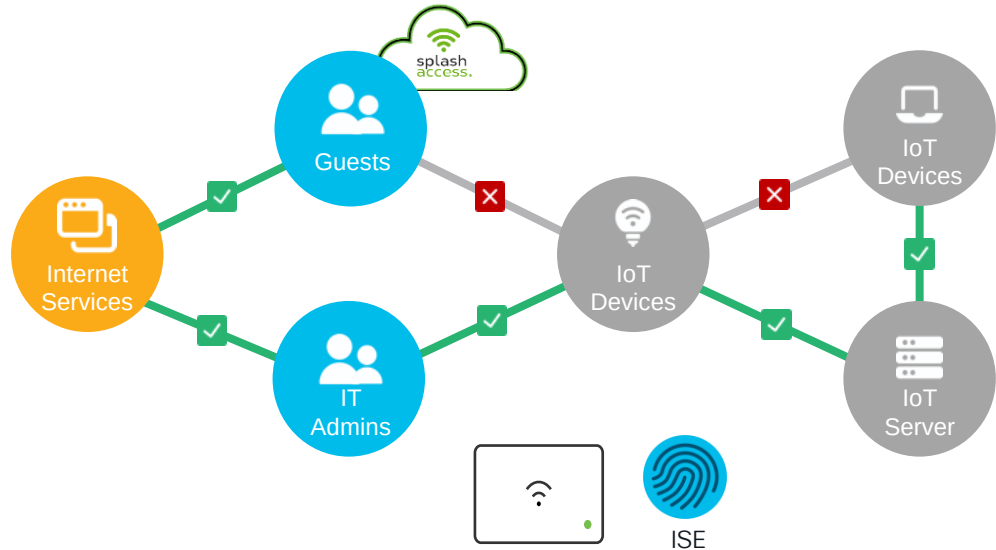
Profiling & Posturing

Classification of unknown endpoints and posture check for compliance



TrustSec

Granular policies using SGTs for micro segmentation



FlexConnect VLAN Override

L3 Authentication



Problem

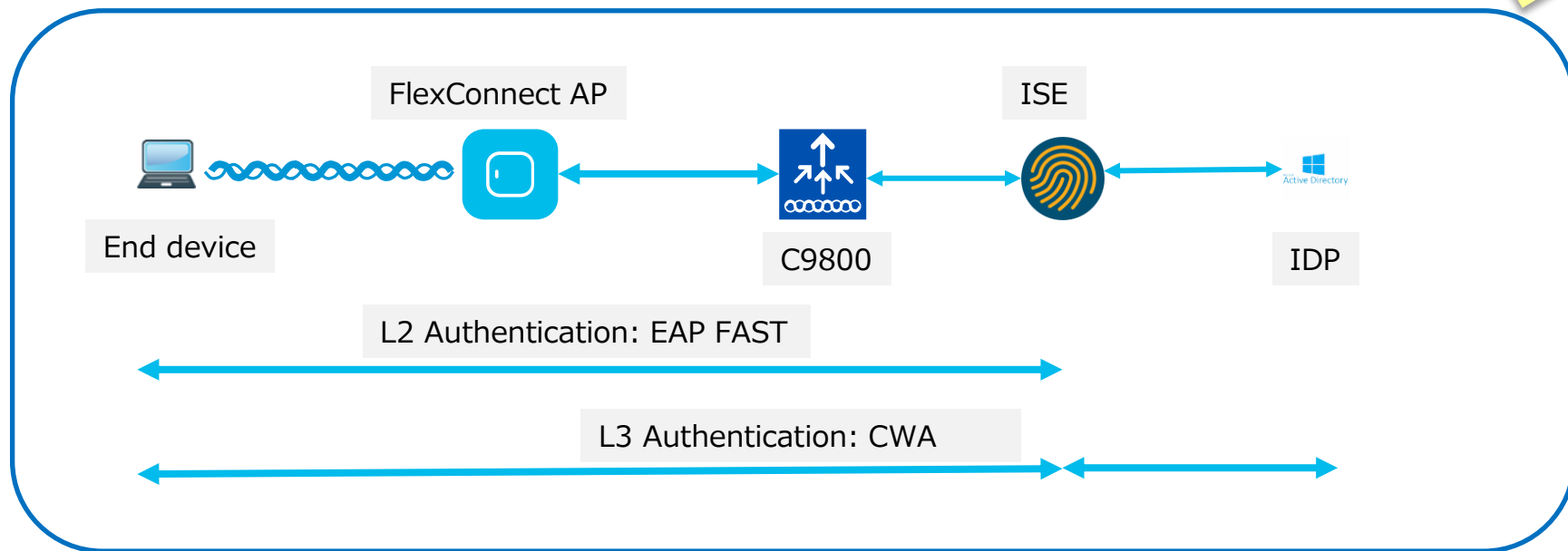
- Prior to 17.14.1:
 - Dynamic VLAN post L3 Authentication in L2+L3 security option is not honored by the WLC and FlexConnect mode AP in Local Switching.
 - Client will be stuck in IP Learn state and be non-operational.

Solution

- Starting 17.14.1, behavior is fixed:
 - User-based VLAN in L2 + L3 authentication in FlexConnect mode for local switching clients is honored.

FlexConnect Topology

FYI



- Supported in all versions of C9800
- Supported in Wave 2, Catalyst Wi-Fi 6 and 6E Access point

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)

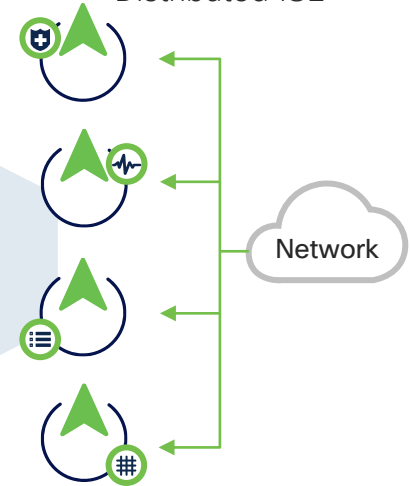
- Makes policy decisions
- RADIUS / TACACS+ Servers



pxGrid Controller (PXG)

- Facilitates sharing of context

Distributed ISE



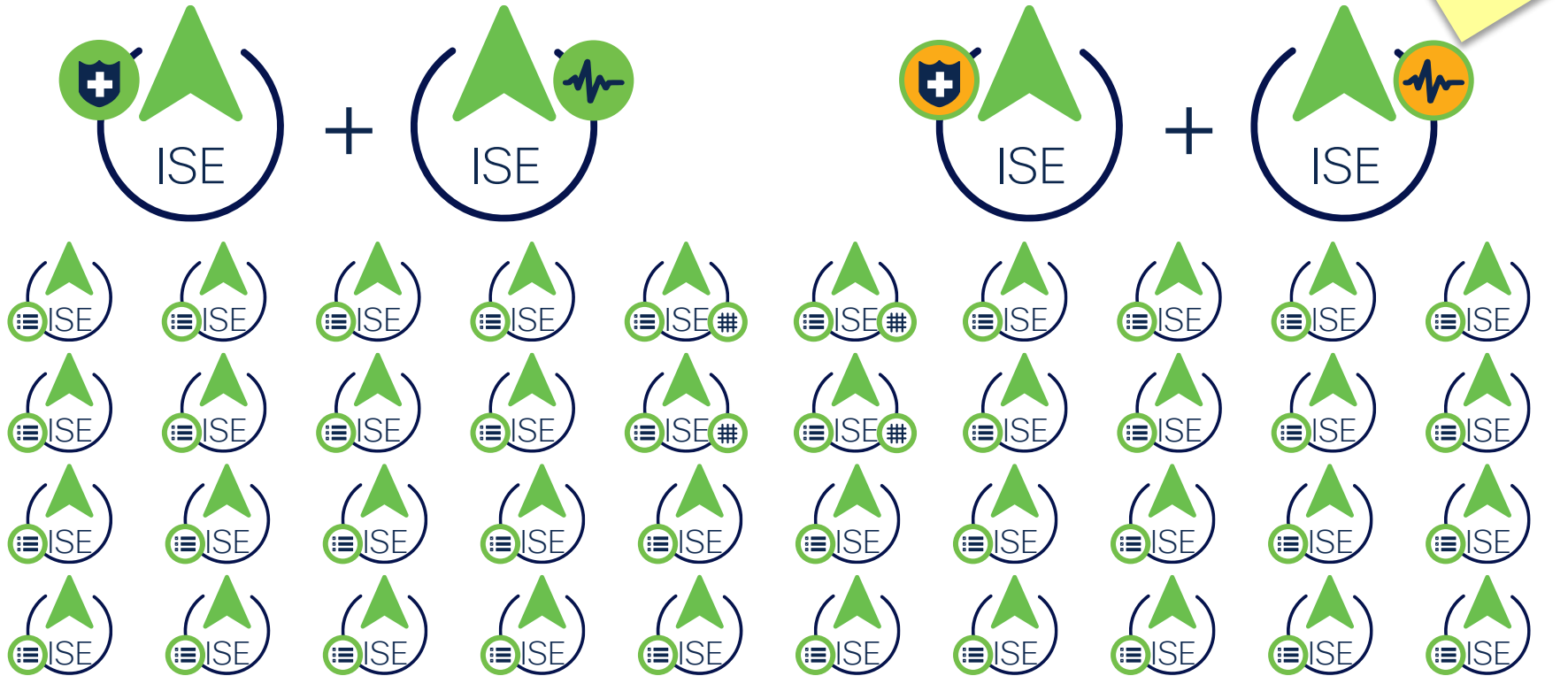
- Standalone provides no redundancy
 - Use for demo, testing, lab

ISE Scaling



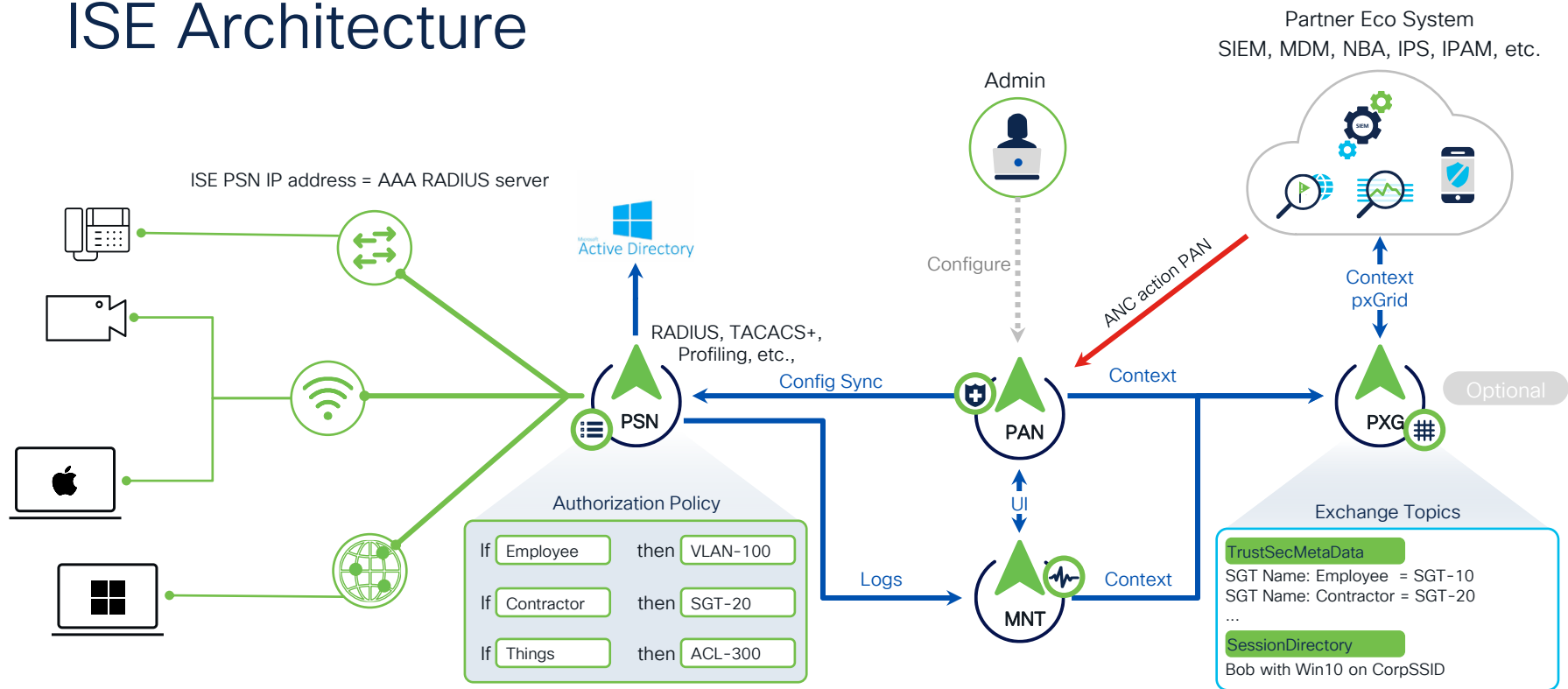
<https://cs.co/ise-scale>

ISE Scaling



<https://cs.co/ise-scale>

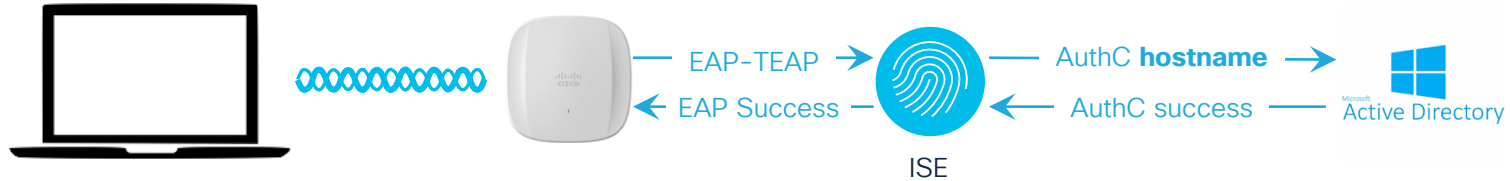
ISE Architecture



<https://cs.co/ise-scale>

Machine Authentication

EAP Chaining with TEAP



EAP-Chaining Result:
User failed and Machine succeeded

Machine Authentication

EAP Chaining with TEAP



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



EAP-Chaining Result:
User and Machine both succeeded

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

On-Prem and Cloud Identity



On-Prem Identity



802.1x, Network Access

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



Cloud Identity

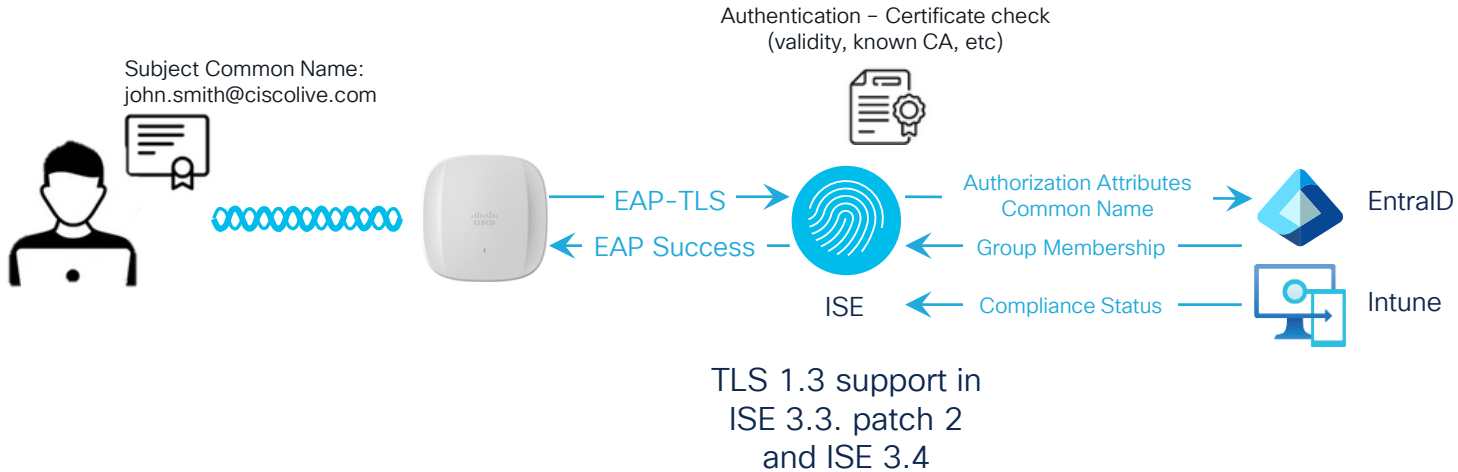
VPN, Application Access



SAMLv2, OpenID Connect



Cloud Identity with EAP-TLS



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

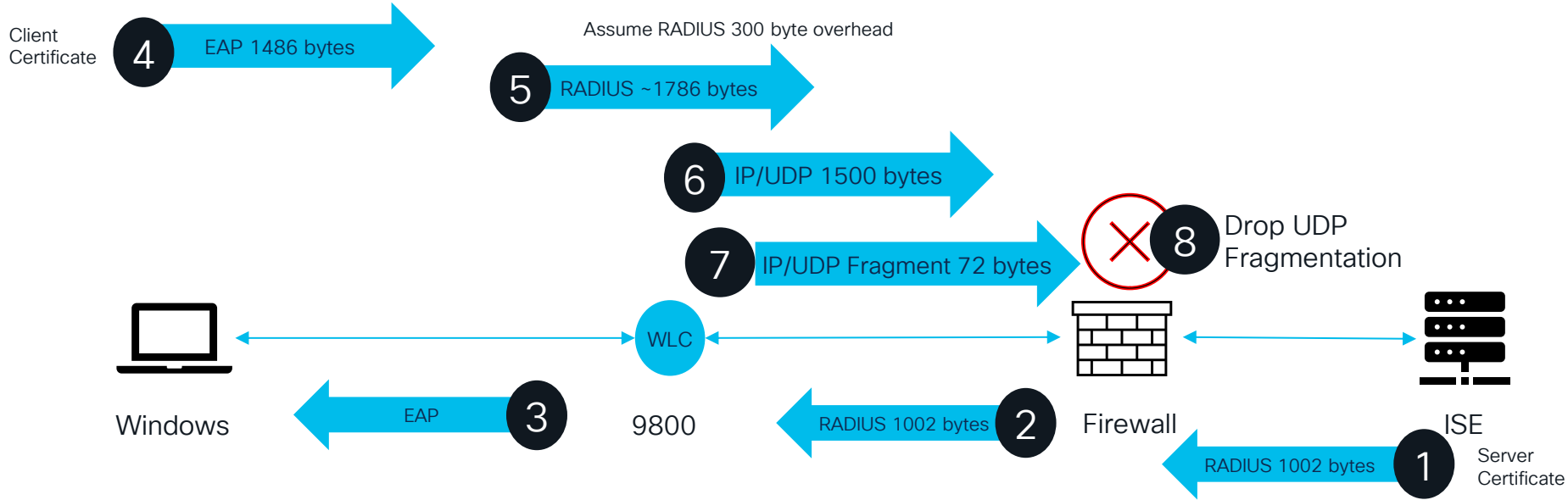
EAP-TLS to RADIUS Fragmentation



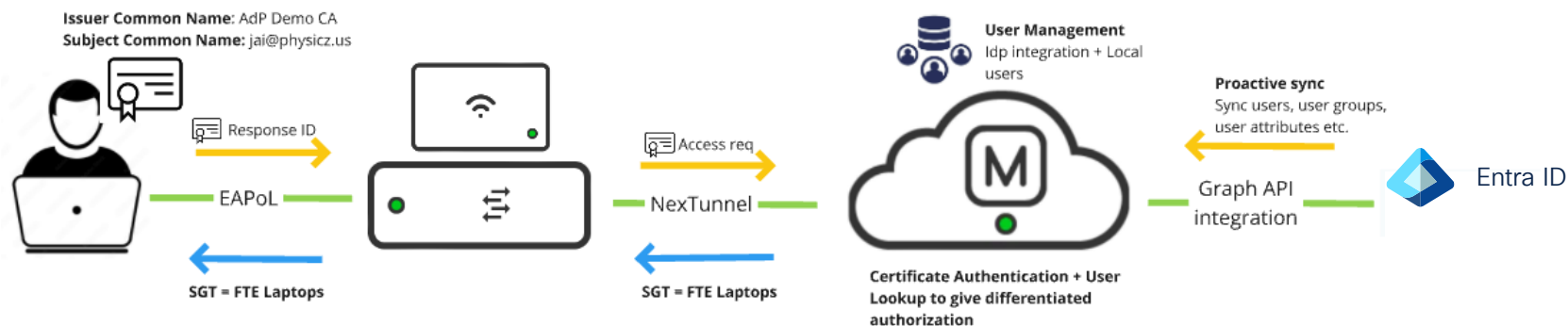
- Potential Solutions:
 - Add a PSN node local with the WLC
 - Enable jumbo packet support on WAN link
 - Change firewall rules to handle packet fragmentation



EAP-TLS to RADIUS Fragmentation



Native Support for Entra ID Based Access Control



Early Access in H1 2025

Secure Fast Roaming Challenges



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

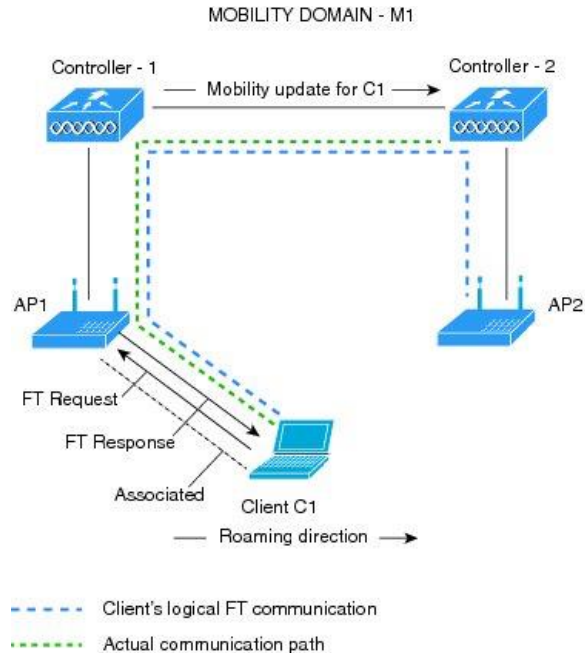
Secure Fast Roaming

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

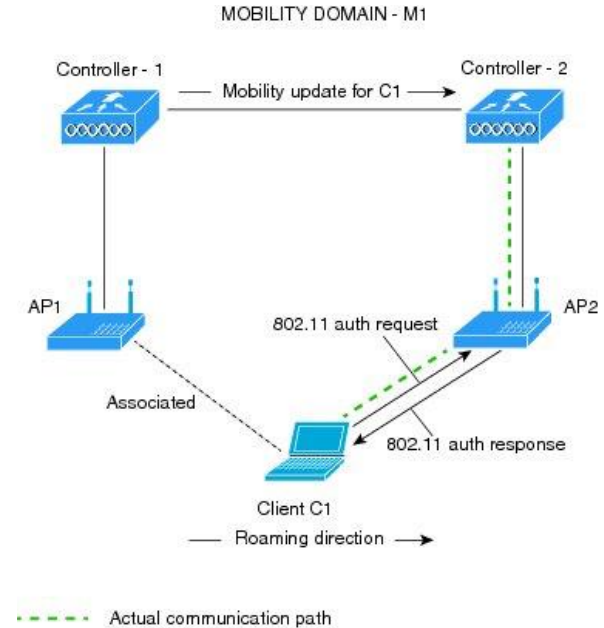


- Client channel scanning and AP selection
 - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
 - 802.11v BSS Transition
- Re-authentication of client device and re-keying
 - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

802.11r Fast Transition



Over the DS

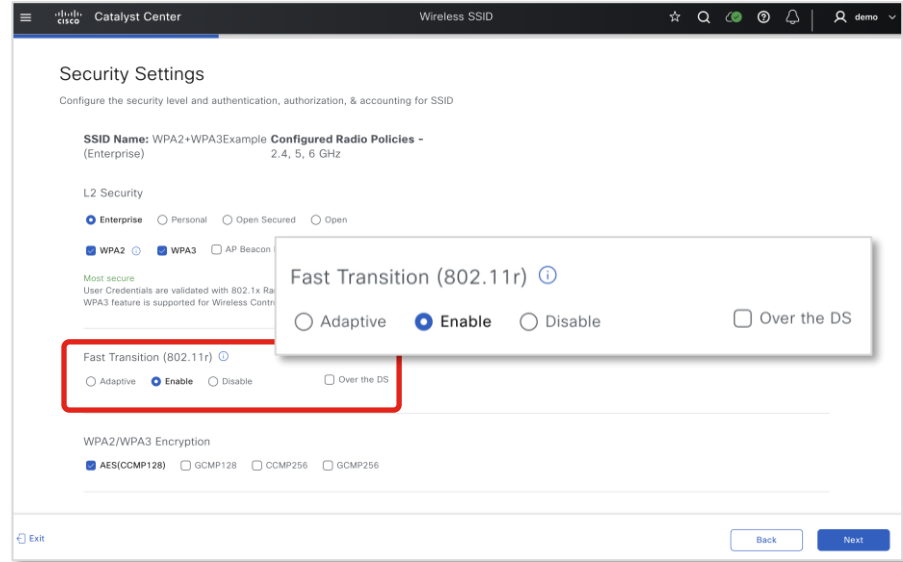


Over the Air

802.11r Fast Transition



- Over the Air is recommended for best client interoperability



Secure Fast Roaming

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



WPA encryption ⓘ

802.11r ⓘ

WPA3 only ▼

☒ Enabled

☐ Adaptive

☐ Disabled

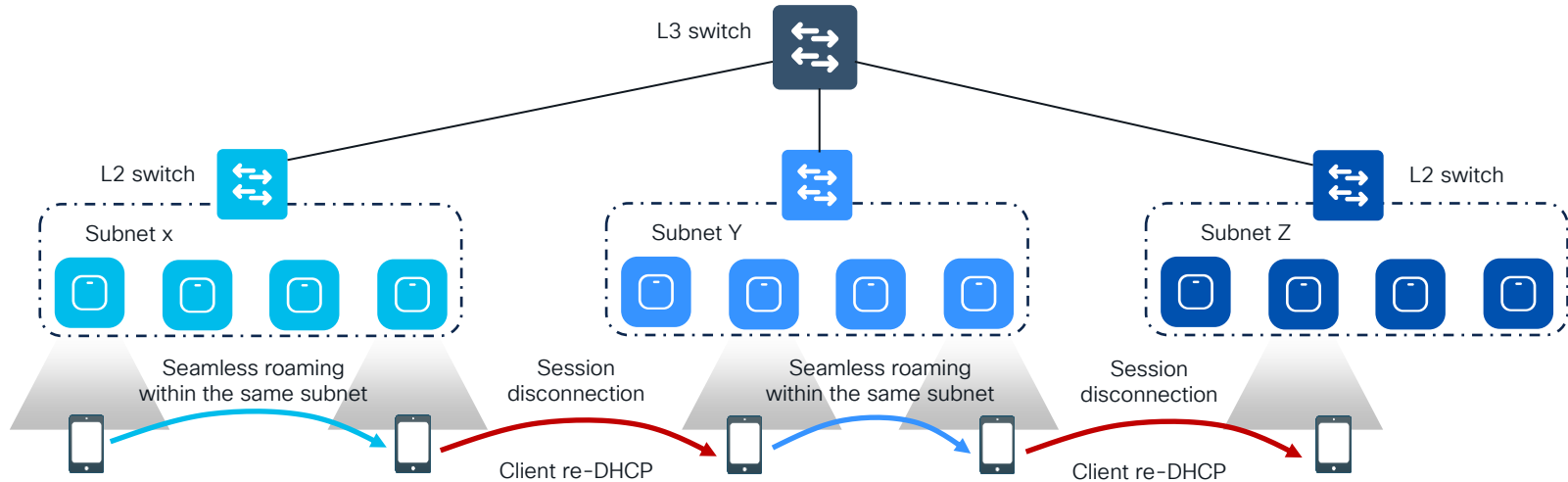
Supported with WPA3 from MR 30

CoA not supported with 802.11r

Seamless Roaming at Scale

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

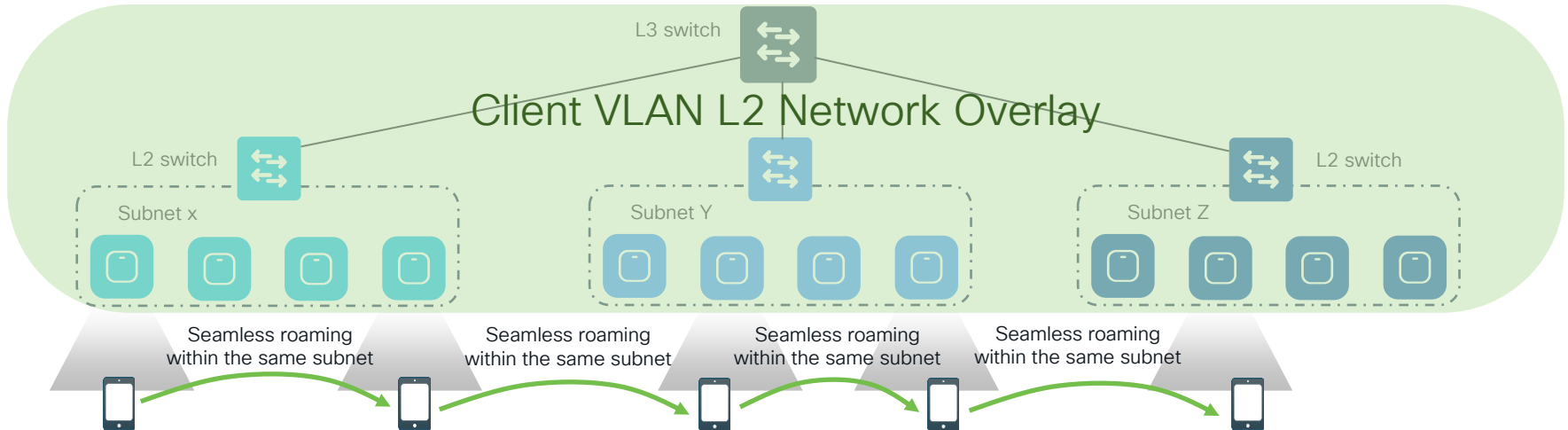
Large broadcast domains do not scale and is counter to networking best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

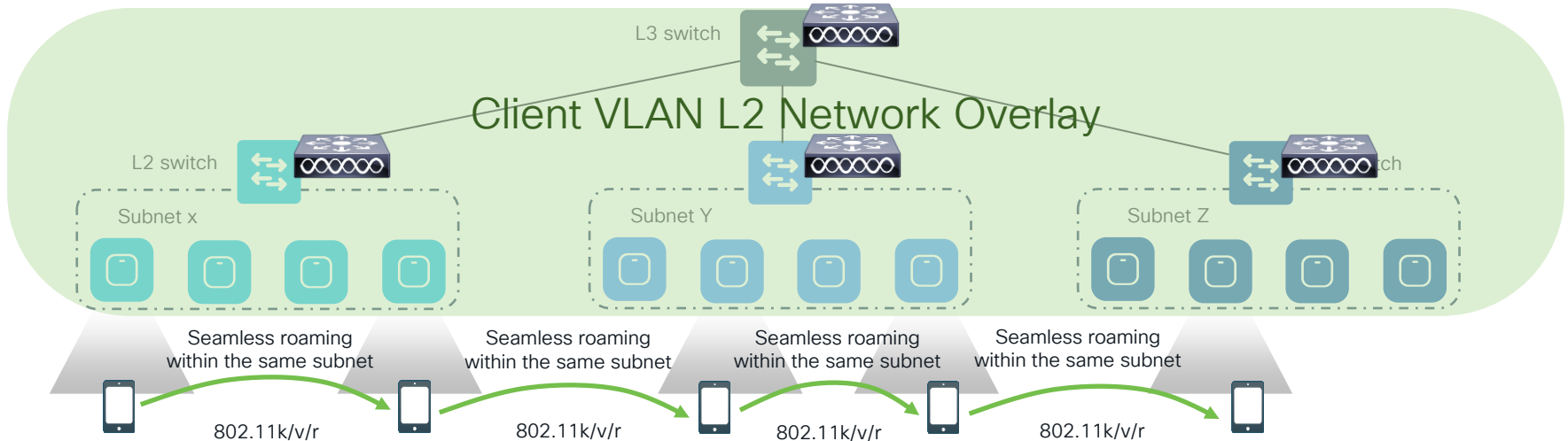
A data termination point is required to roam across L3 boundaries



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

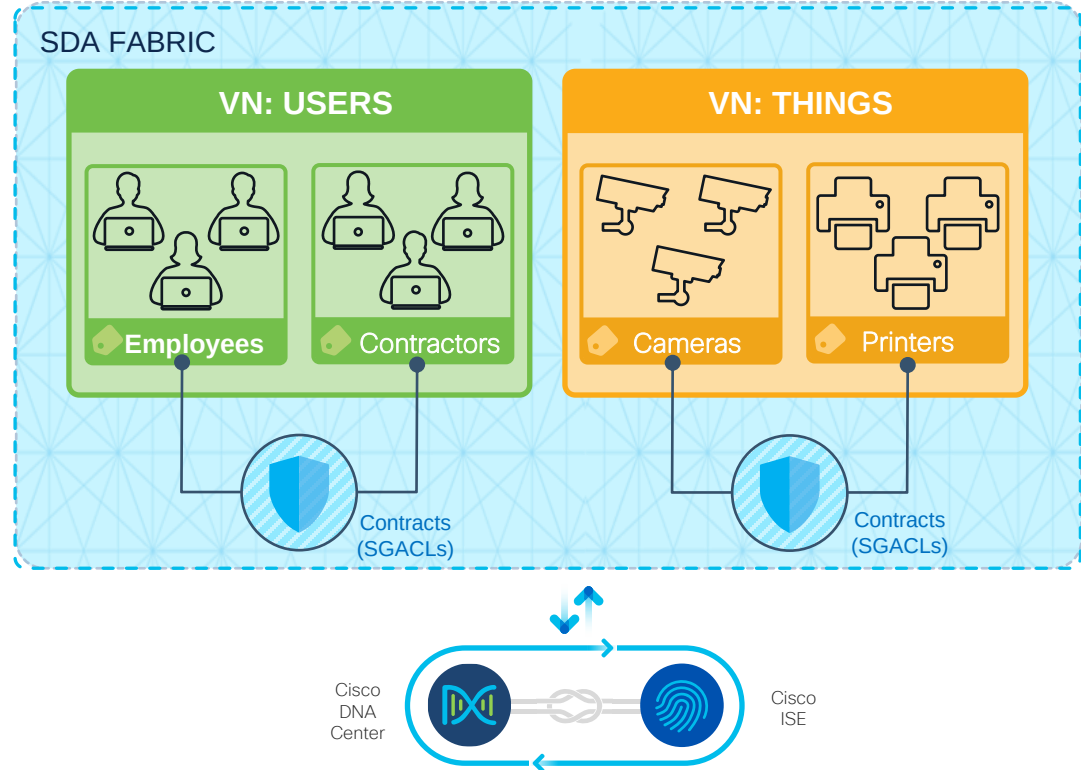


Use cases

Network segmentation with
'Virtual Networks'

Group segmentation with
'Scalable Groups'

Fabric-Native Wireless



Adaptive Policy & Secure Analytics

Informed Policy Creation and Validation

FYI



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



Group based policy and **traffic flow tracking**



TRAFFIC INFORMATION



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

PROTOCOLS

▲ ICMP (11 KB) ...
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](#)

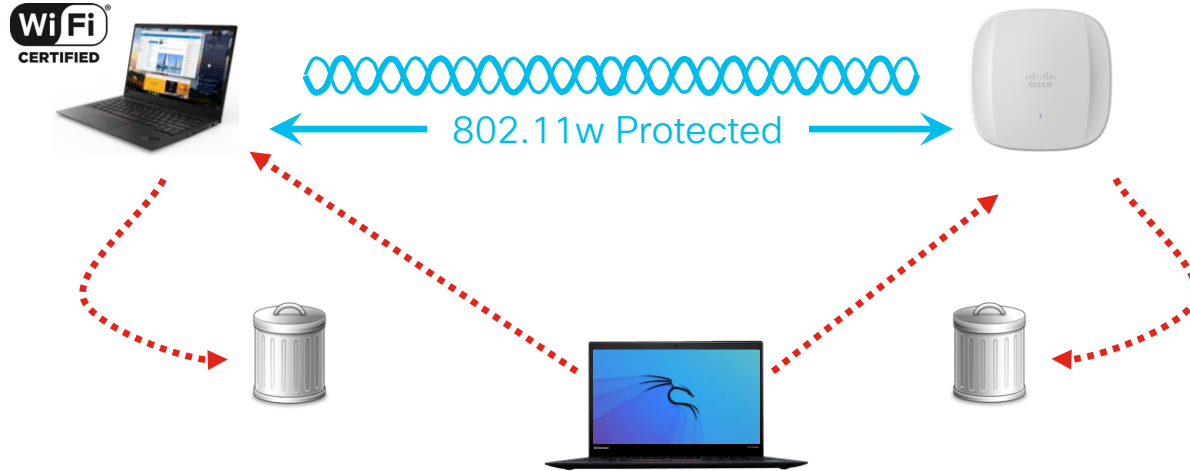
- This was an industry wide issue
 - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
 - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection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

Kr00k Vulnerability



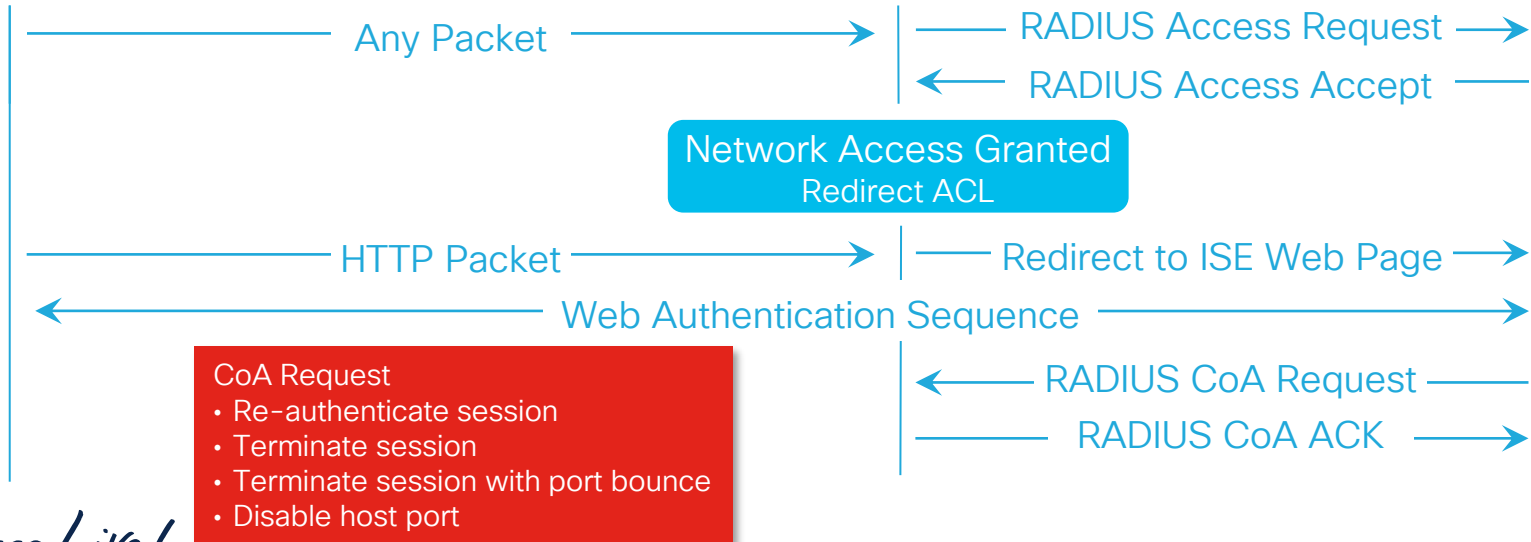
- On February 26th, 2020, researchers Štefan Svorencík and Robert Lipovsky [disclosed a vulnerability in the packet processing of certain Wi-Fi chipsets](#)
- This vulnerability could allow an unauthenticated, adjacent attacker to decrypt Wi-Fi frames without the knowledge of the PTK
- After an affected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

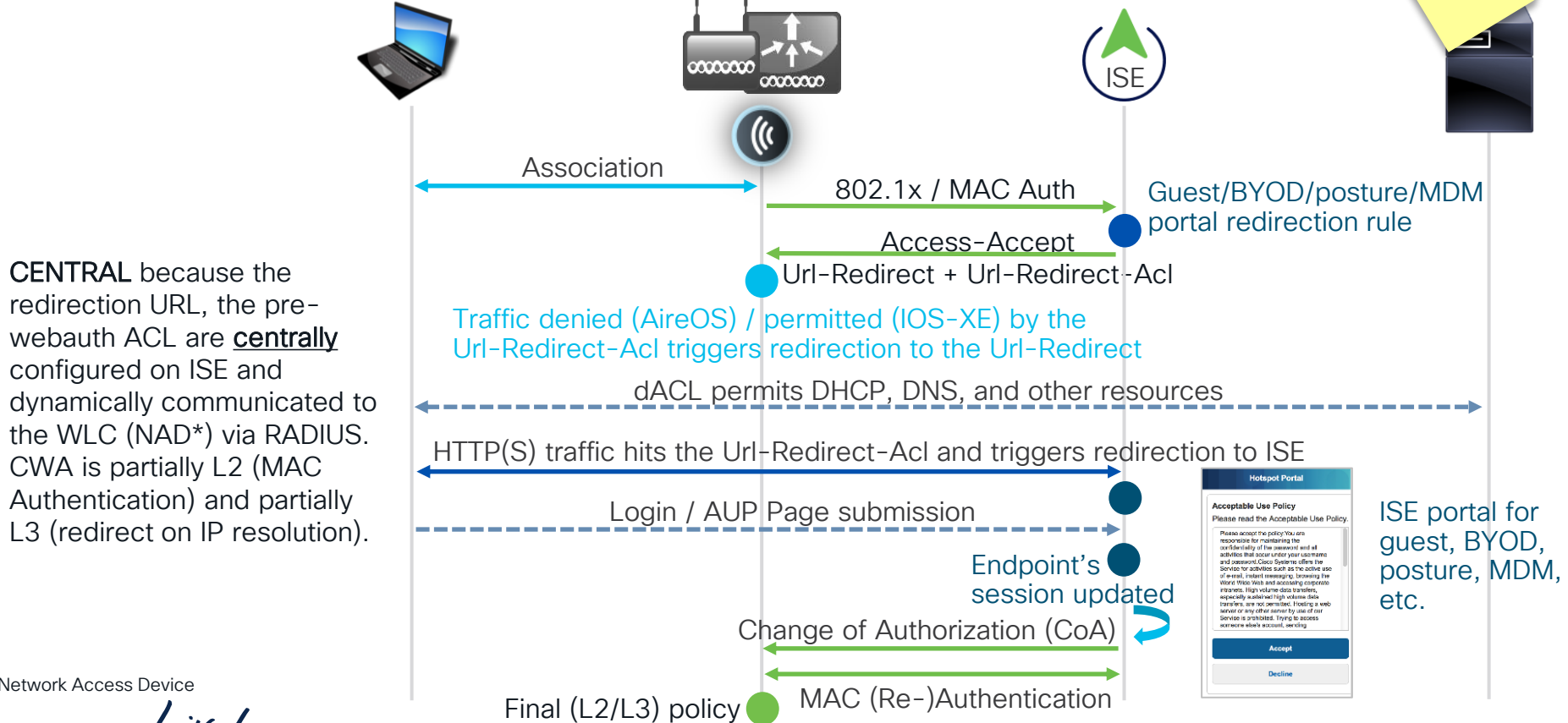
- http://www.gstatic.com/generate_204



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:

1 New Devices Can be Added with a Description

Lost Stolen Edit Delete

Close

2 Devices can be Blacklisted By the User.

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: *

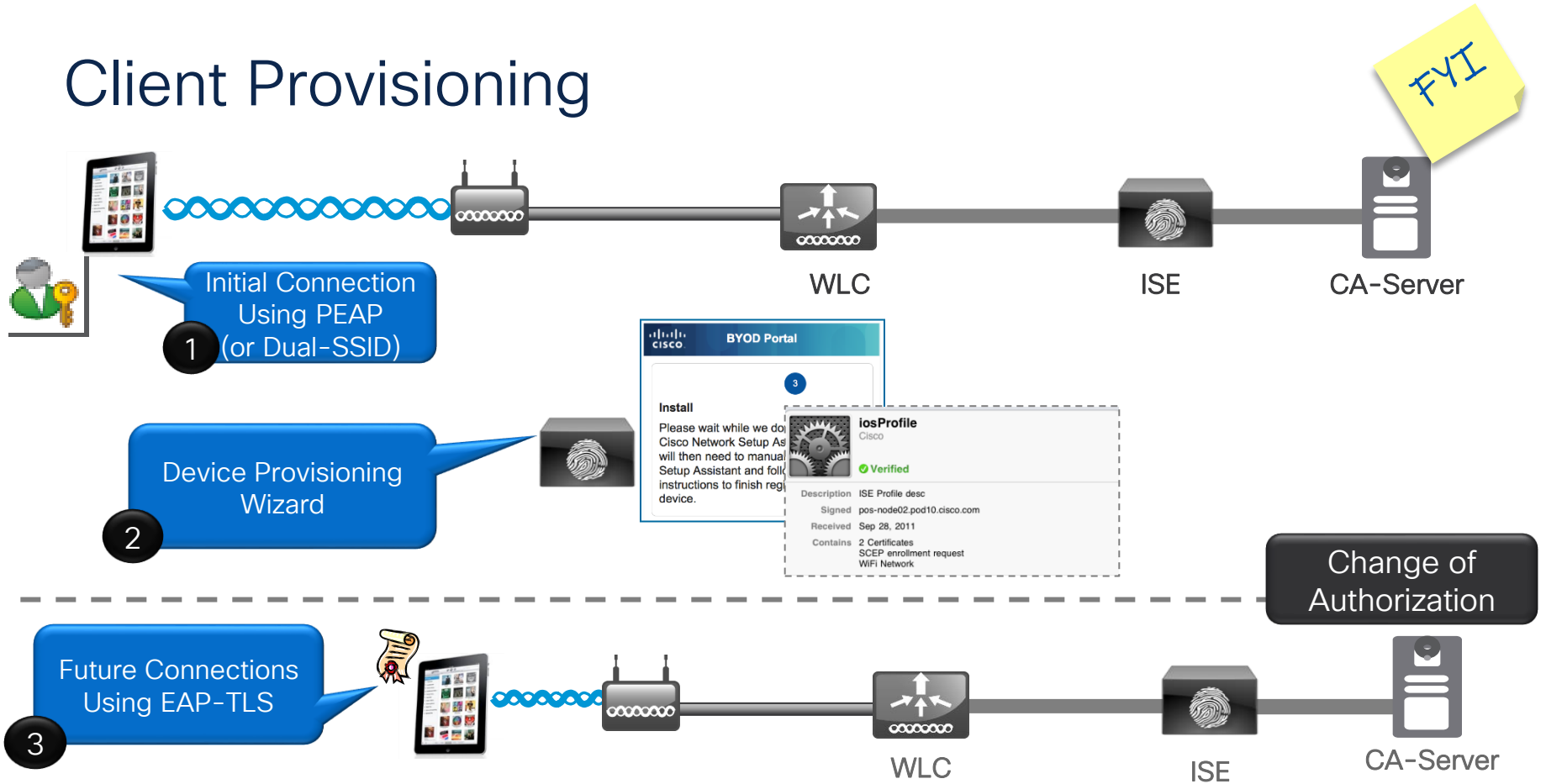
Device ID: *

Description:

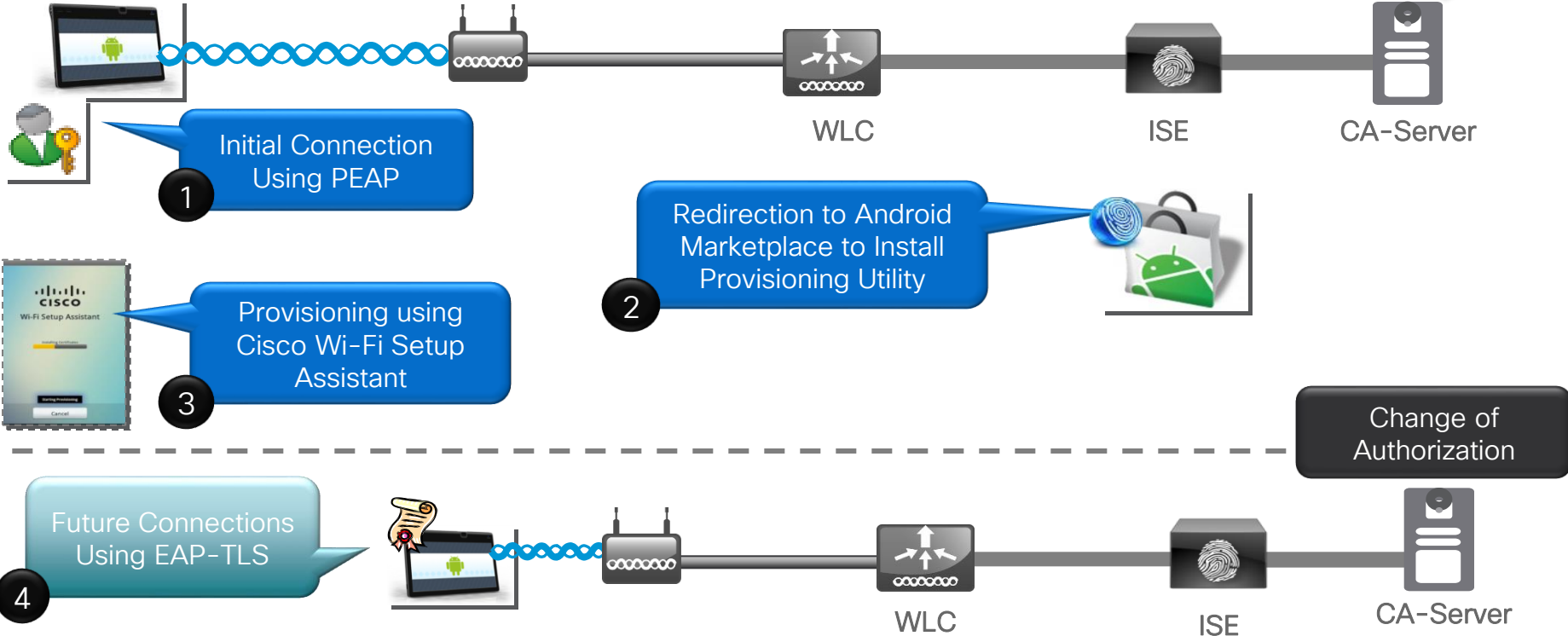
Submit Cancel

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

Client Provisioning



Android Device Provisioning



Client Provisioning Policy

FYI



OS



User



Supplicant

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:

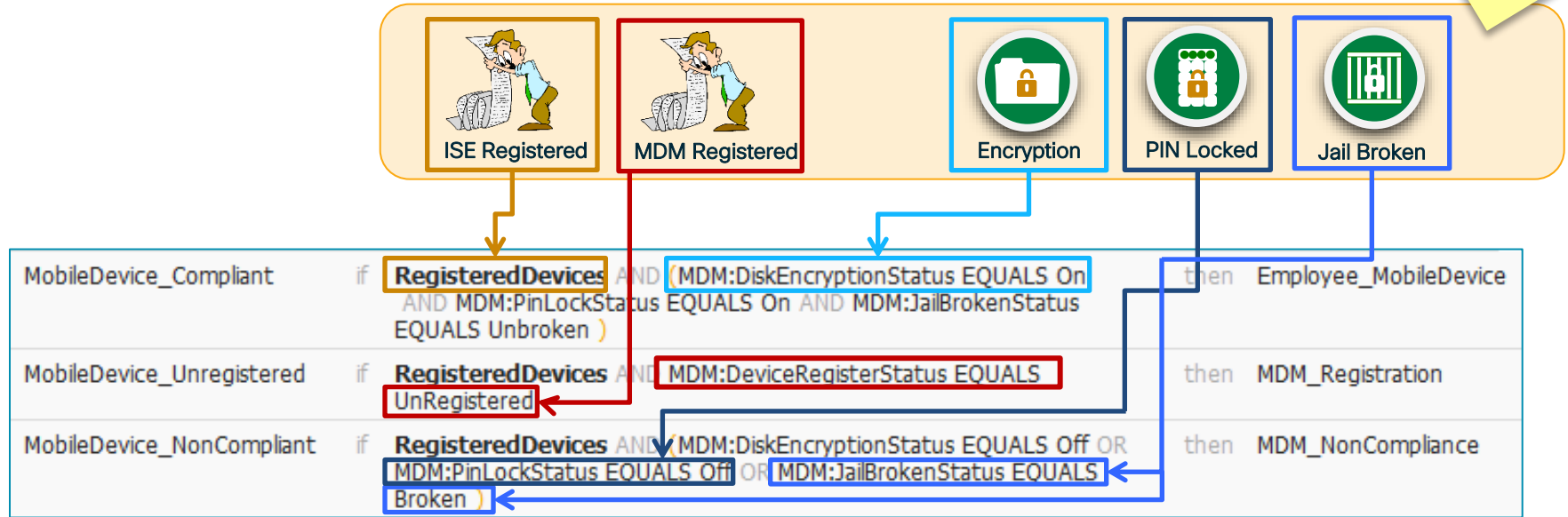
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.

For Native Supplicant Configuration: wizard profile and/or wizard.

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

MDM Integration

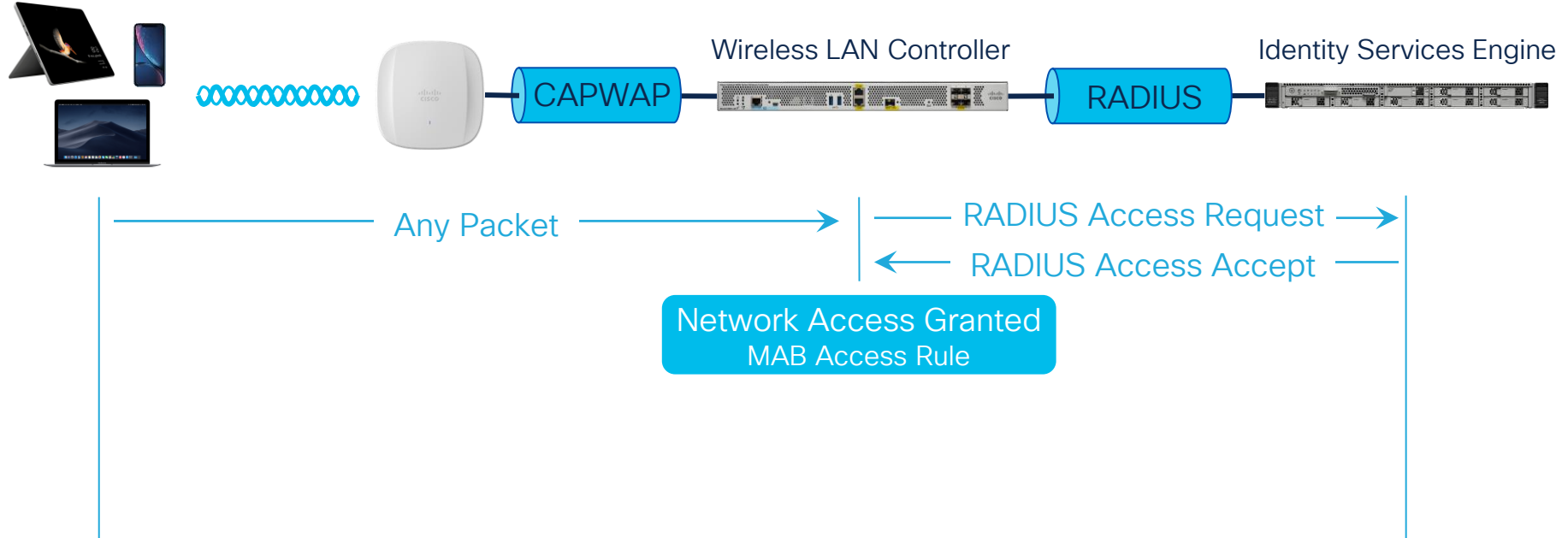
FYI



cisco Live!

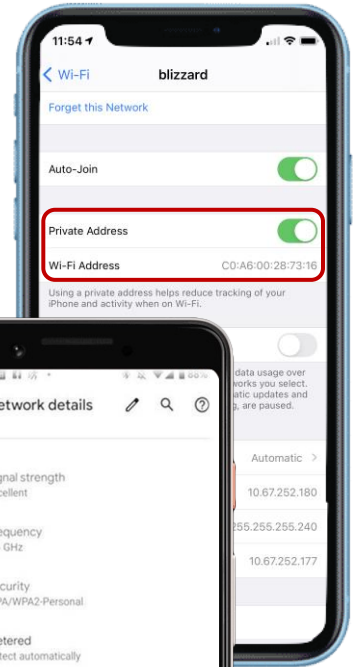
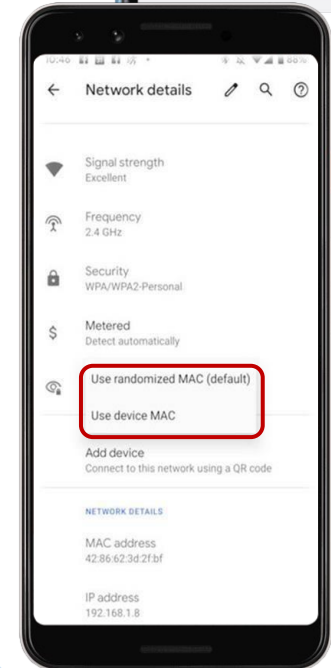
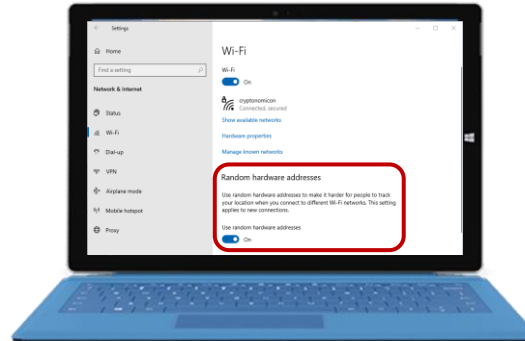
Central Web Authentication

MAC Authentication Bypass

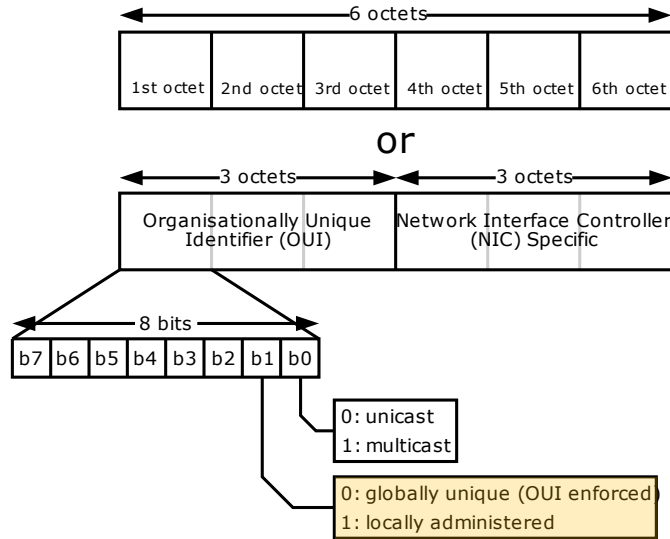


Random MAC and Private Addresses

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



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>

Random MAC Implications



Apple



- **Starting with iOS 14, iPadOS 14, watchOS 7, macOS Sequoia, visionOS**
 - By default, your device improves privacy by using a different MAC address for each Wi-Fi network. This unique MAC address is your device's private Wi-Fi address, which it uses for that network only.
 - If you erase all content and settings or reset network settings on your device, it uses a different private address the next time it joins the network.
- **Starting with iOS 15, iPadOS 15, watchOS 8, macOS Sequoia, visionOS**
 - If your device hasn't joined the network in 6 weeks, it uses a different private address the next time it joins the network.
 - If you make your device [forget the network](#), it also forgets the private address it used with that network, unless it has been less than 2 weeks since the last time it was made to forget that network.

- **Starting with iOS 18, iPadOS 18, watchOS 11, macOS Sequoia, visionOS 2**
 - The Private Wi-Fi Address feature now offers these settings, which you can change at any time.
- **Off**
 - When set to Off, your device uses its hardware MAC address.
- **Fixed**
 - When set to Fixed, your device uses a private address, but the private address doesn't rotate, regardless of the network's security or length of time since you last joined the network. Your device chooses Fixed by default when joining a new network that uses [WPA2 or stronger security](#).
- **Rotating**
 - When set to Rotating, your device uses a private address that rotates to a different private address every 2 weeks. Your device chooses Rotating by default when joining a new network that uses weak security or no security.

Use private Wi-Fi addresses on Apple devices

Android



- The Android framework uses two types of MAC randomization: [persistent randomization](#) and [non-persistent randomization](#)
- If the user disables MAC randomization, the factory MAC address is used.

[MAC randomization behavior](#)

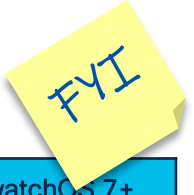
- **Persistent randomization**

- Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does **not** get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.
- Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and let users bypass the login screen as expected, or to enable parental controls.
- For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.

- **Non-persistent randomization**

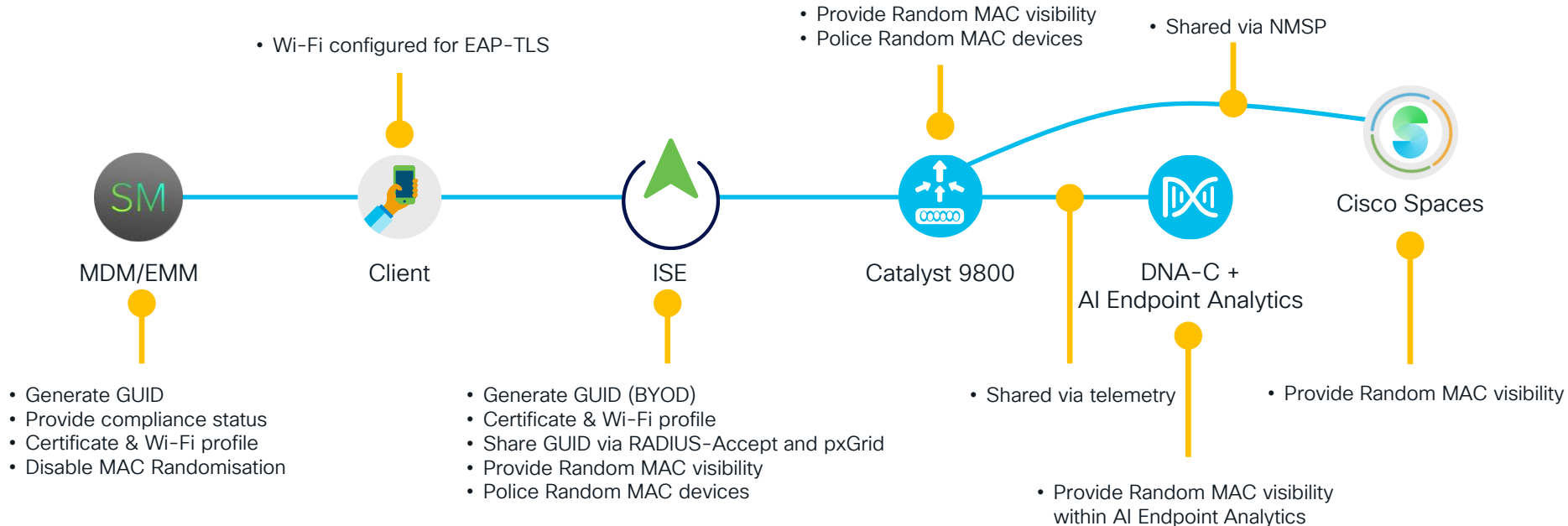
- Under the non-persistent randomization type, which is used for some networks in Android 12 or higher, the Wi-Fi module re-randomizes the MAC address at the start of every connection or the framework uses the existing randomized MAC address to connect to the network. The Wi-Fi module re-randomizes the MAC address in the following situations:
- The DHCP lease duration has expired and more than 4 hours have elapsed since the device last disconnected from this network.
- The current randomized MAC for the network profile was generated more than 24 hours ago. MAC address re-randomization only happens at the start of a new connection. Wi-Fi won't actively disconnect for the purpose of re-randomizing a MAC address.
- If none of these situations apply, the framework uses the previously randomized MAC address to connect to the network.

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

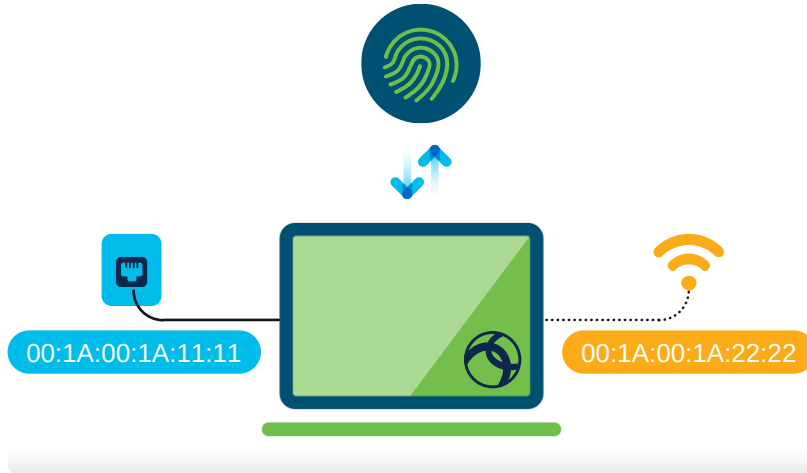
Addressing Random MAC Issues



Unique Device Identifier

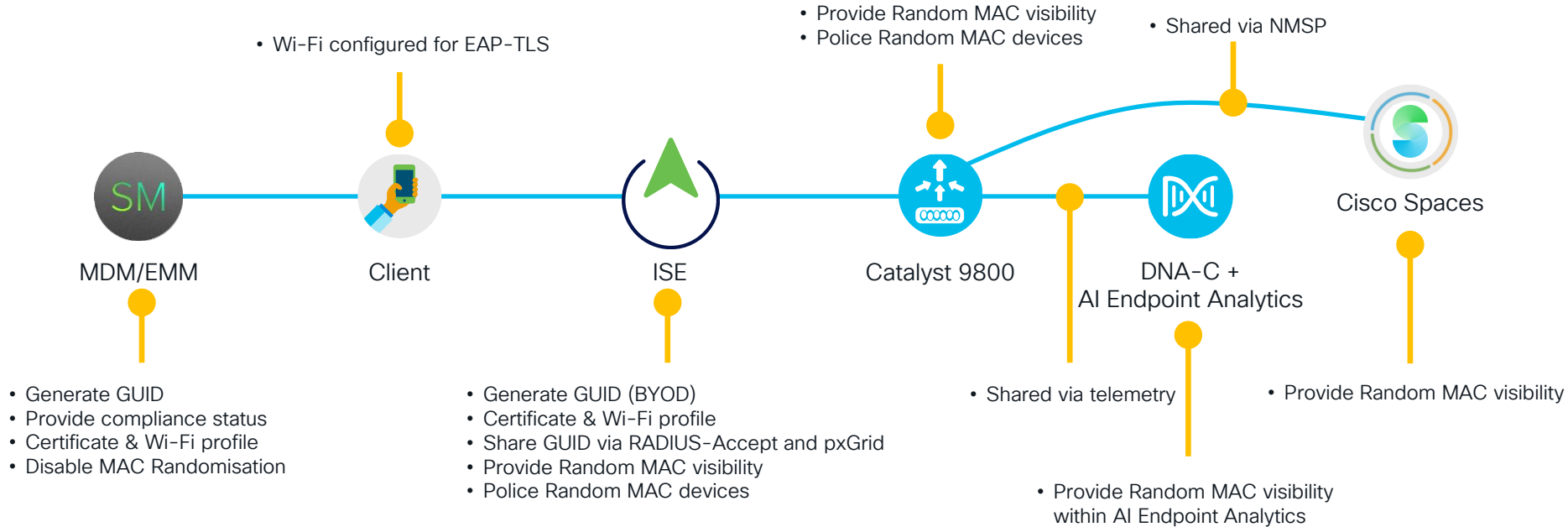


UDID	MAC Address(s)	Compliance
01669b65...05ee93	00:1a:00:1a:11:11 00:1a:00:1a:22:22	✓



- 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



Deny Clients using MAC Randomisation



Catalyst Center Wireless SSID

WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalyst 9800 Controllers version 16.12 & above.

Fast Transition (802.11r) ⓘ

☐ Adaptive ☒ **Enable** ☐ Disable ☐ Over the DS

WPA2/WPA3 Encryption

☒ **AES(CCMP128)** ☐ GCMP128 ☐ CCMP256 ☐ GCMP256

Auth Key Management ⓘ

☐ CCKM ☐ 802.1x (802.1X-SHA1) ☒ **802.1x-SHA256 (802.1X-SHA2)** ☒ **FT + 802.1x**

Authentication, Authorization, and Accounting Configuration

AAA Configured (1)

☒ **AAA Override** ☐ MAC Filtering ☐ Deny RCM Clients ⓘ

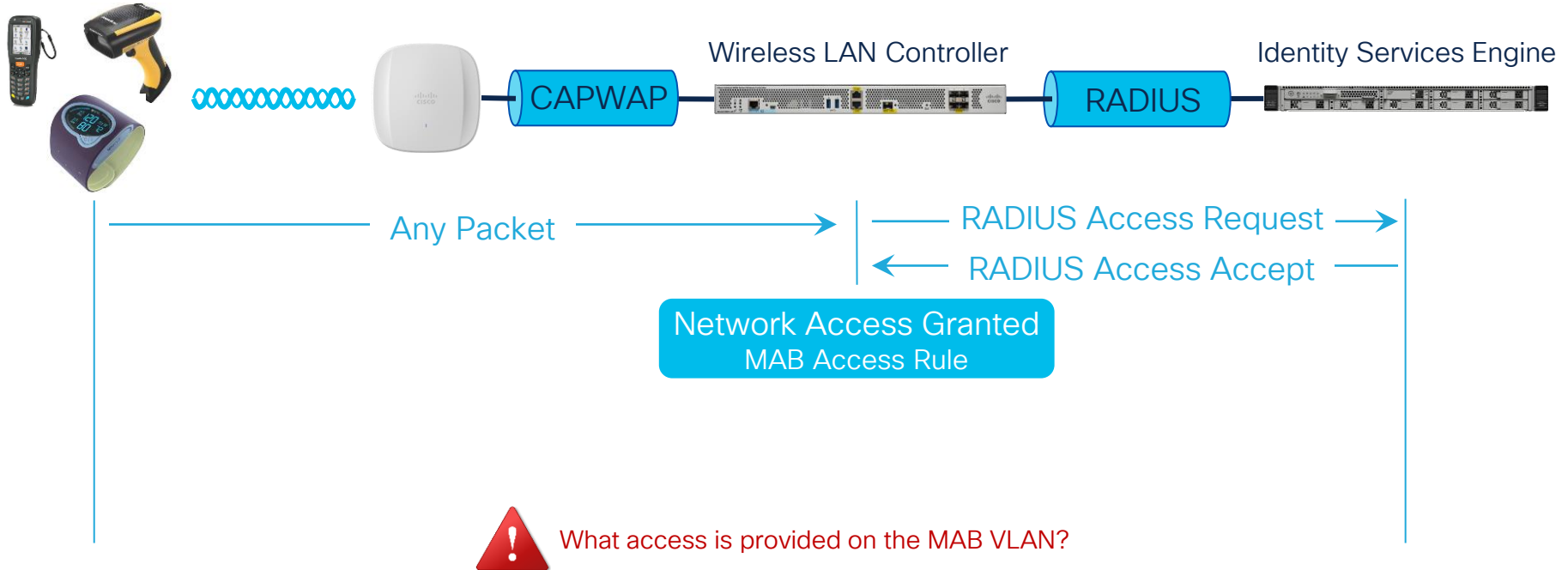
ACL Name is required

☒ **Enable Posture** ⓘ

Exit Back Next

Deny clients using MAC Randomization feature is supported in Catalyst 9800 Controllers with version 17.5 & above, also in Wireless Controllers with version 8.10 MR5 & above.

MAC Authentication Bypass



Wi-Fi Certified Easy Connect

WPA3



Device Provisioning Protocol (DPP)

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



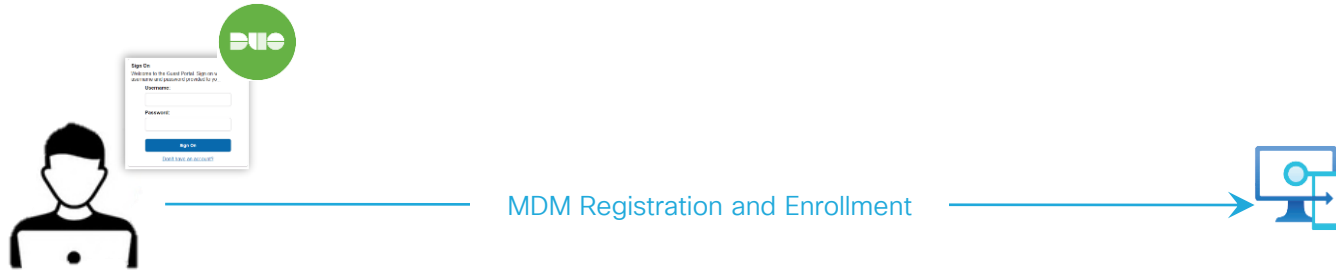
Multi-Factor Authentication



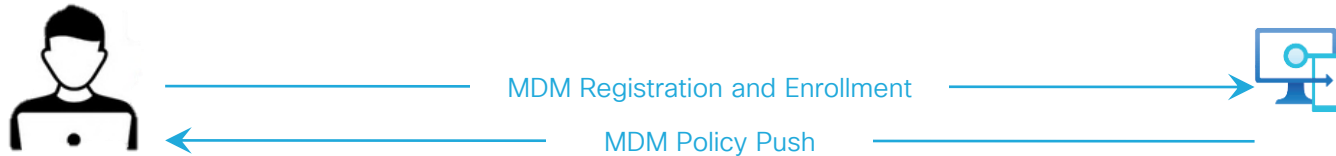
Multi-Factor Authentication



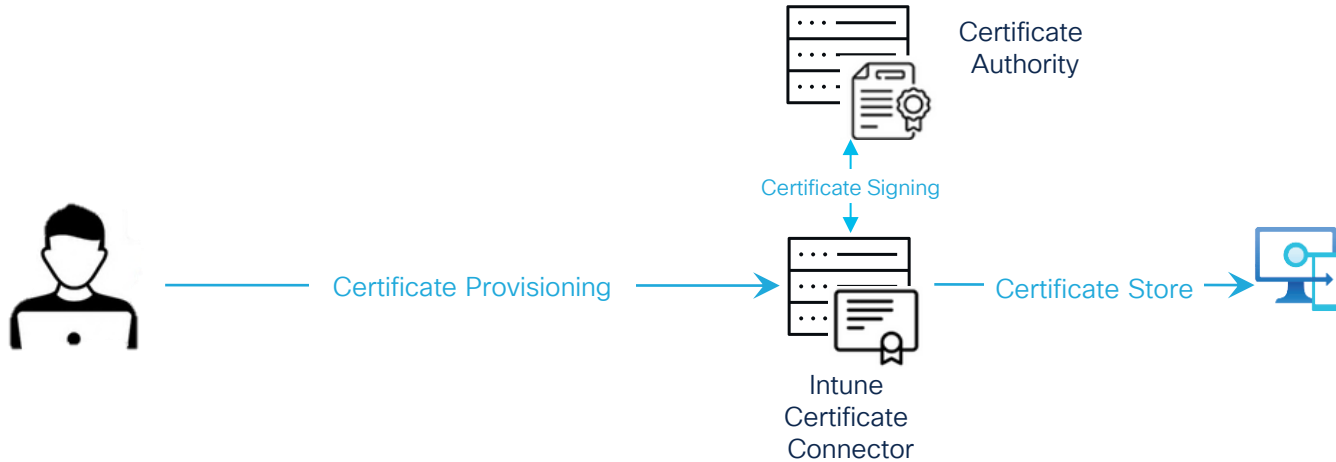
Multi-Factor Authentication



MDM Enrollment



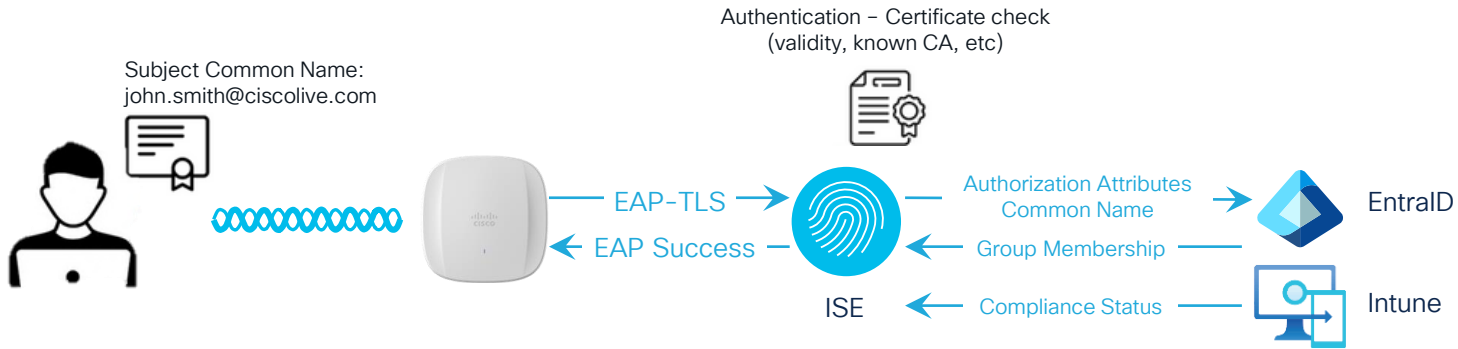
Certificate Provisioning



Certificate Provisioning



Cloud Identity with EAP-TLS



Zero Trust

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

Cyber incident breakdown



- Ransomware

- East/West Traversal
- Authorization
 - Micro-segmentation
- Rapid Threat Containment

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

cisco Live!



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

Access and Identity

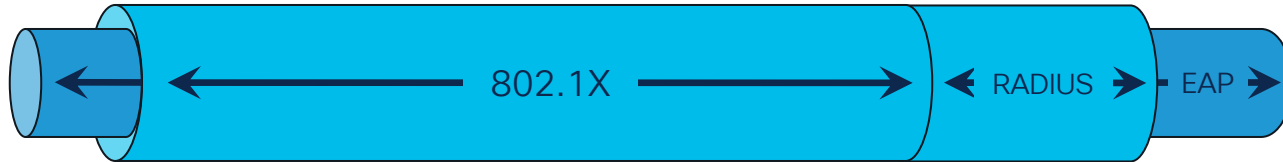
Decoupling Access and Identity

Access



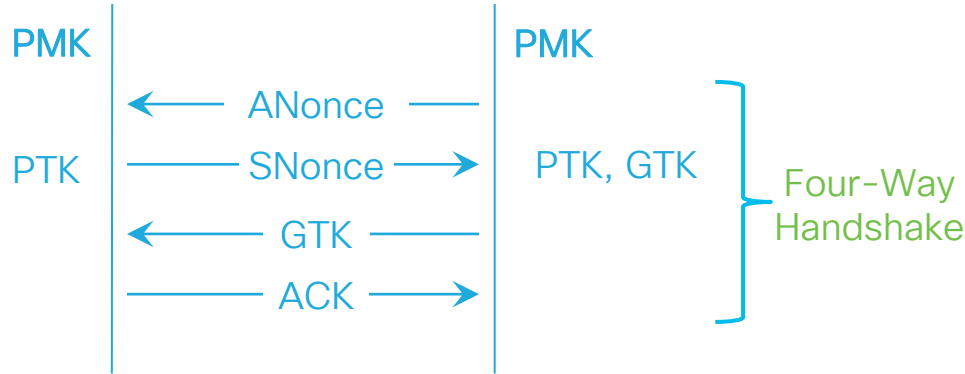
Identity

OpenRoaming



WPA Personal

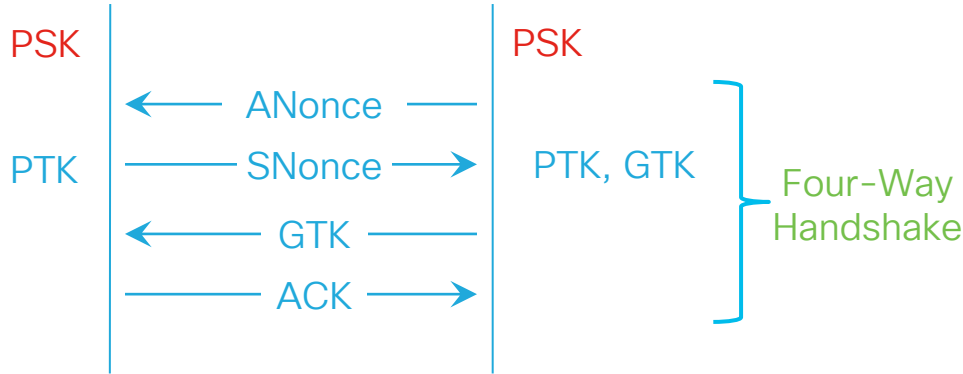
Pre-Shared Key



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

WPA Personal

Pre-Shared Key



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

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years



> Hardware: 12 x RTX 4090 | Password hash: bcrypt

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

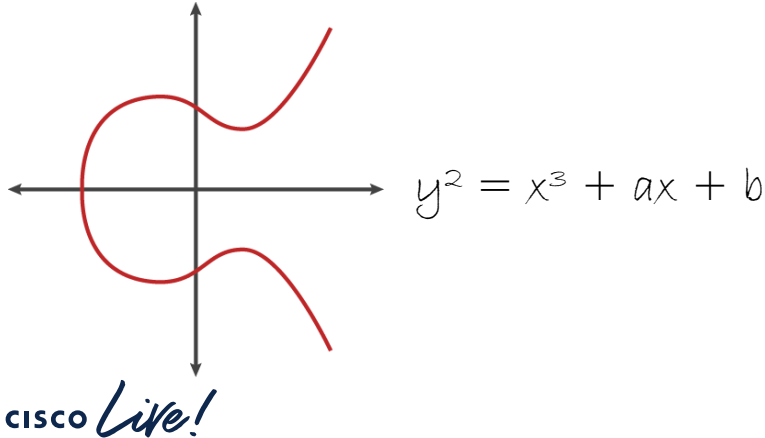
Dragonblood



- 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 password



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 ☐	WPA2 Policy ☐
GTK Randomize ☐	WPA3 Policy ☒
Transition Disable ☒	

Fast Transition

Status Disabled ▼

Over the DS ☐

Reassociation Timeout * 20

WPA2/WPA3 Encryption

AES(CCMP128) ☒	CCMP256 ☐
GCMP128 ☐	GCMP256 ☐

Protected Management Frame

PMF Required ▼

Association Comeback Timer* 1

SA Query Time* 200

Auth Key Mgmt

SAE ☒	FT + SAE ☐
OWE ☐	FT + 802.1x ☐
802.1x-SHA256 ☐	

Anti Clogging Threshold* 1500

Max Retries* 5

Retransmit Timeout* 400

PSK Format Both H2E and HnP

PSK Type Only

Pre-Shared Key* Hunting and Pecking Only

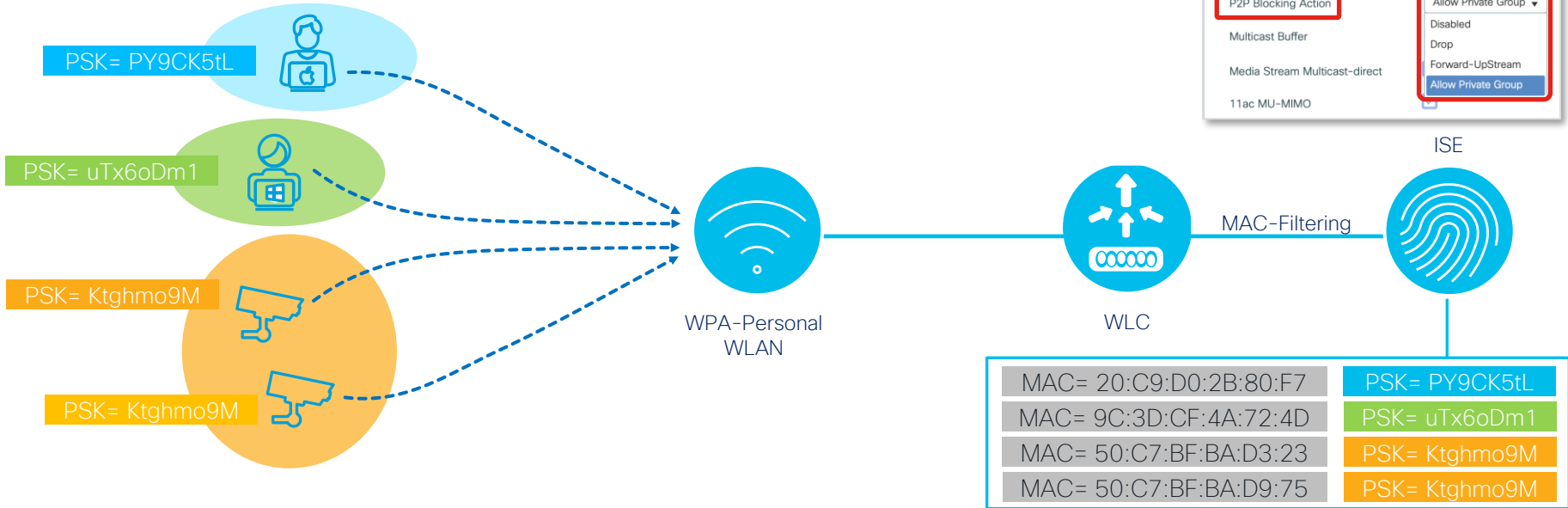
SAE Password Element ⓘ

Hash to Element Only

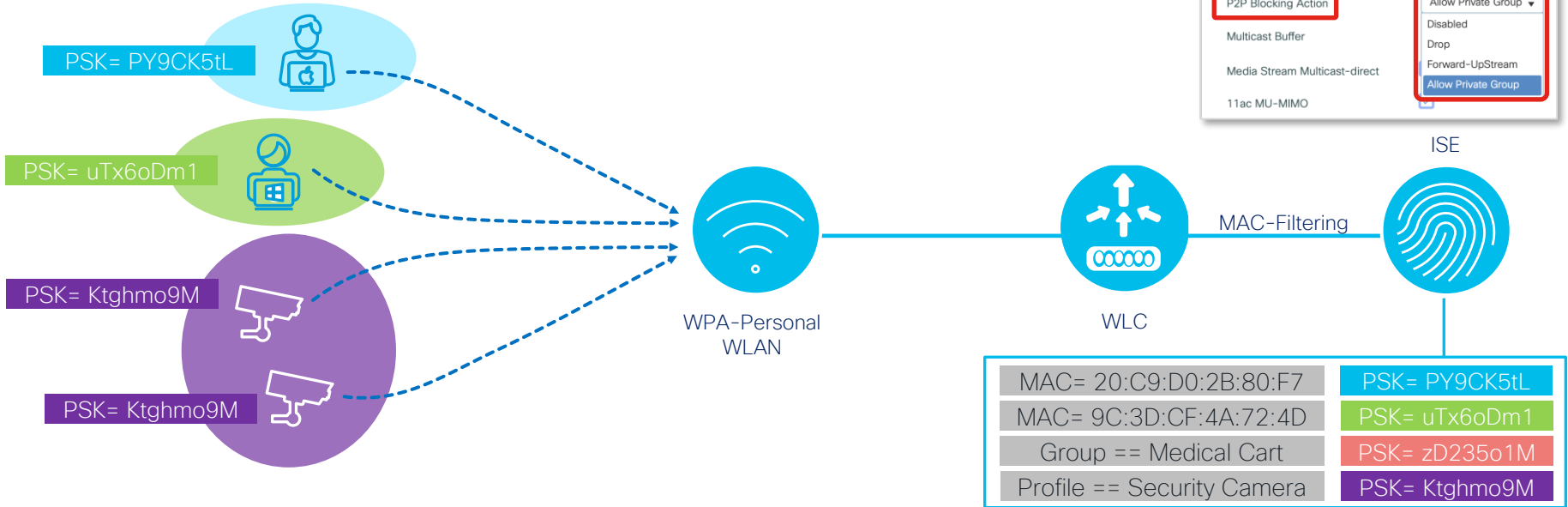
Hash to Element O...



Identity PSK/SAE

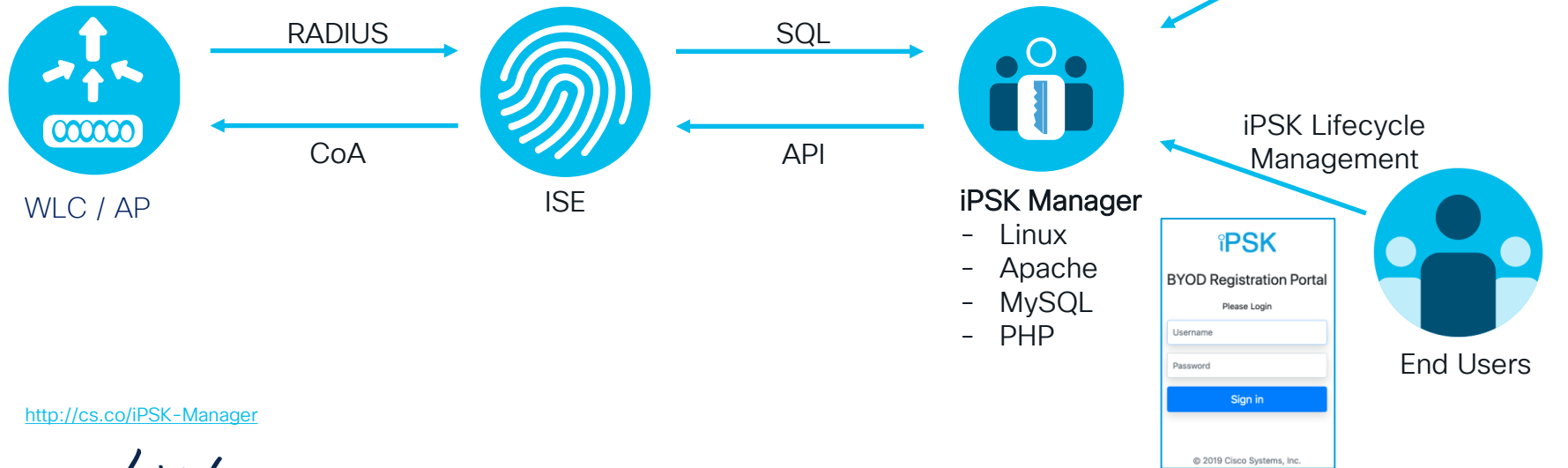


Identity PSK/SAE



<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

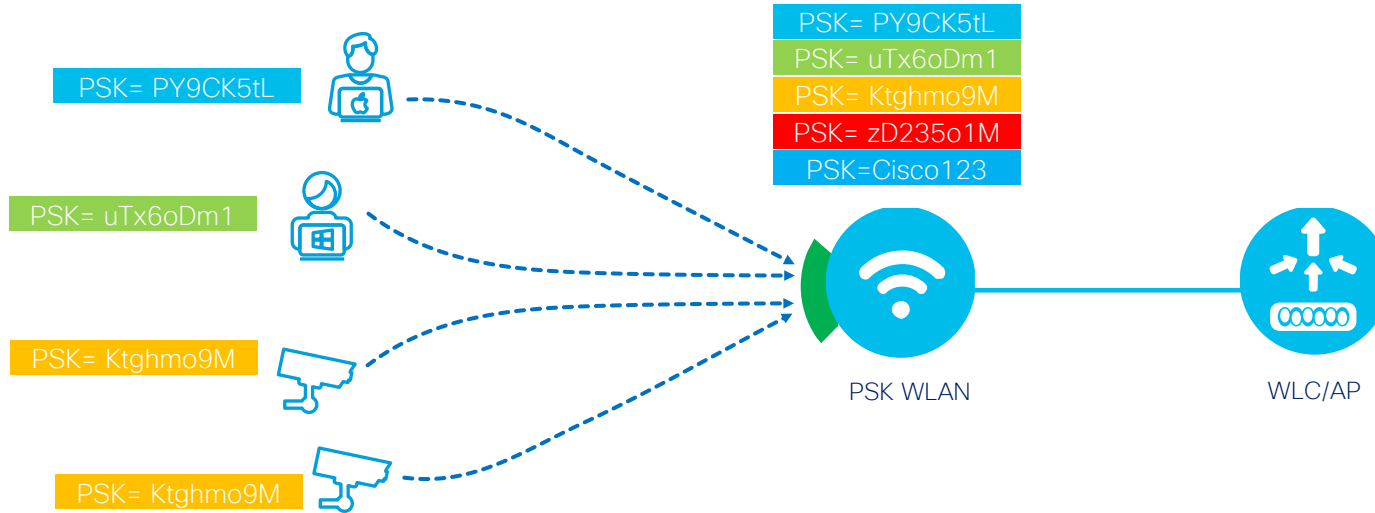
iPSK Manager



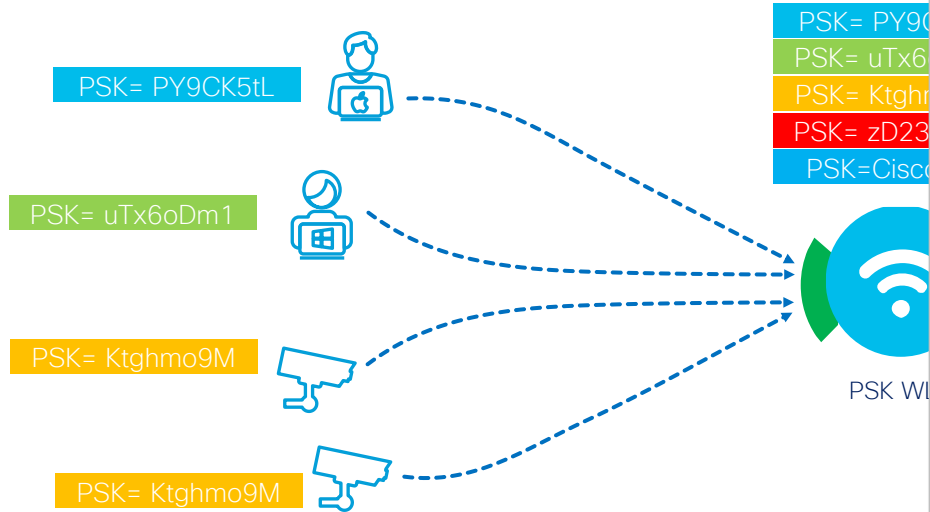
<http://cs.co/iPSK-Manager>

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 ☒

Add Delete

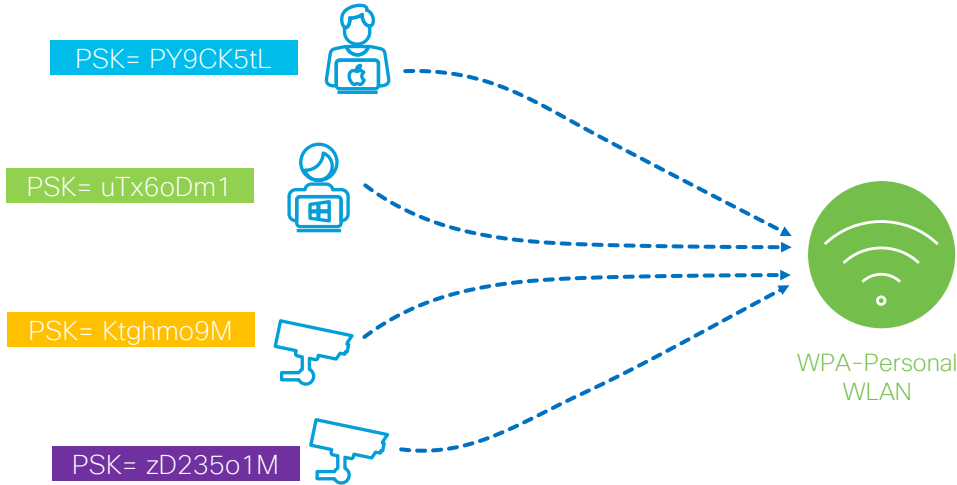
Priority ▼ Key Format ▼ Password Type ▼

Priority * Priority(0-4)
Key Format ASCII
Password Type Unencrypted
Pre-Shared Key*

Cancel Apply

FYI

Identity PSK without RADIUS



Wi-Fi Personal Network (WPN) ⓘ

WPA encryption

Segment clients so that they can only communicate with other devices using the same Identity PSK

Enabled Disabled

WPA2 only ▾

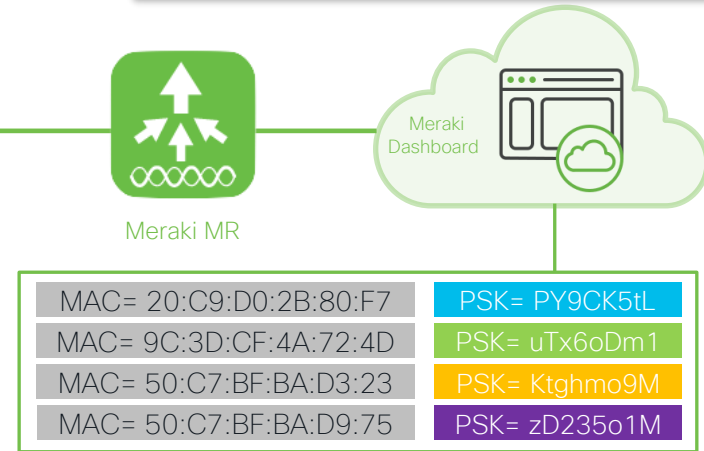
Identity PSK without RADIUS

Devices are assigned a group policy based on its passphrase

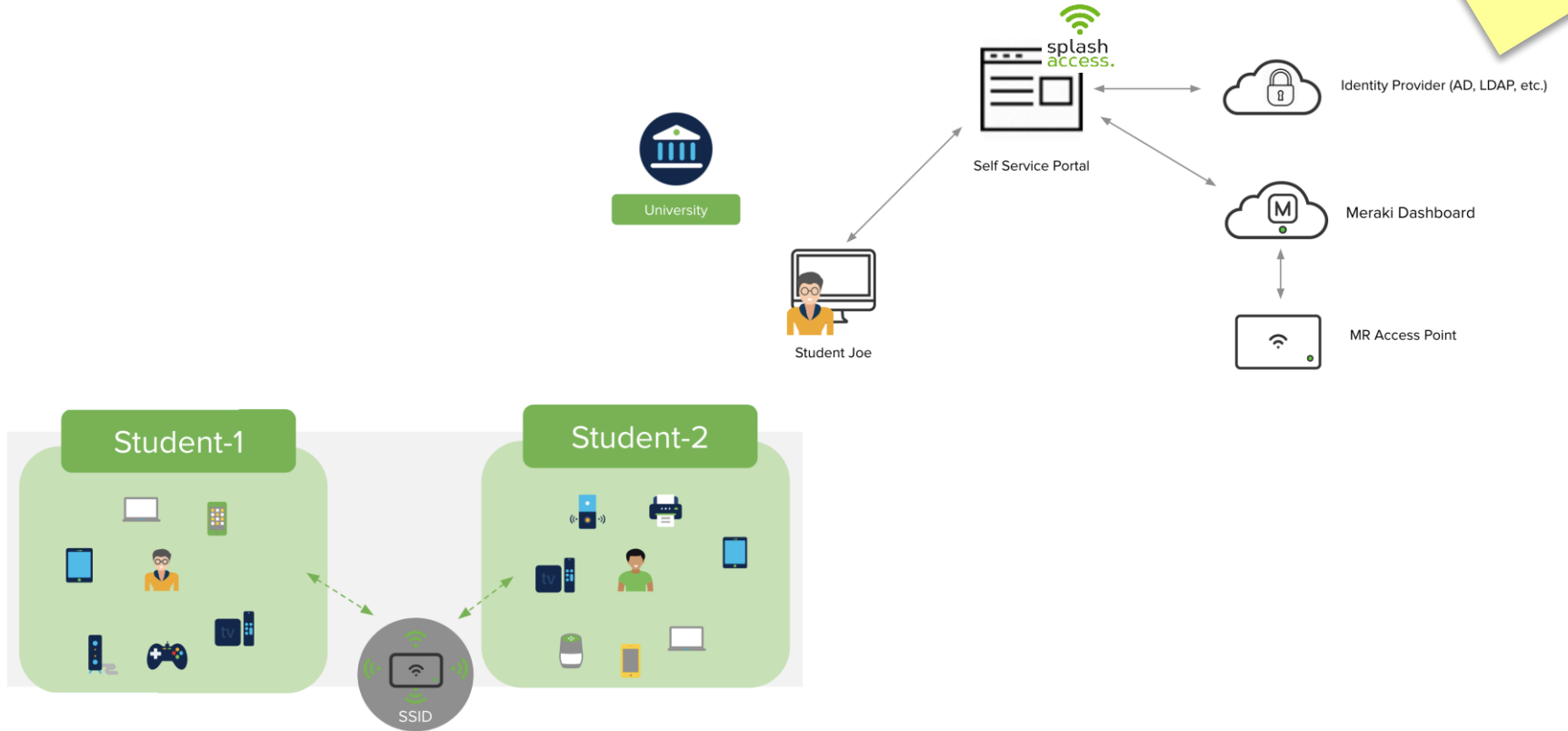
0

Search Identity PSKs... 3 Identity PSKs Add Delete

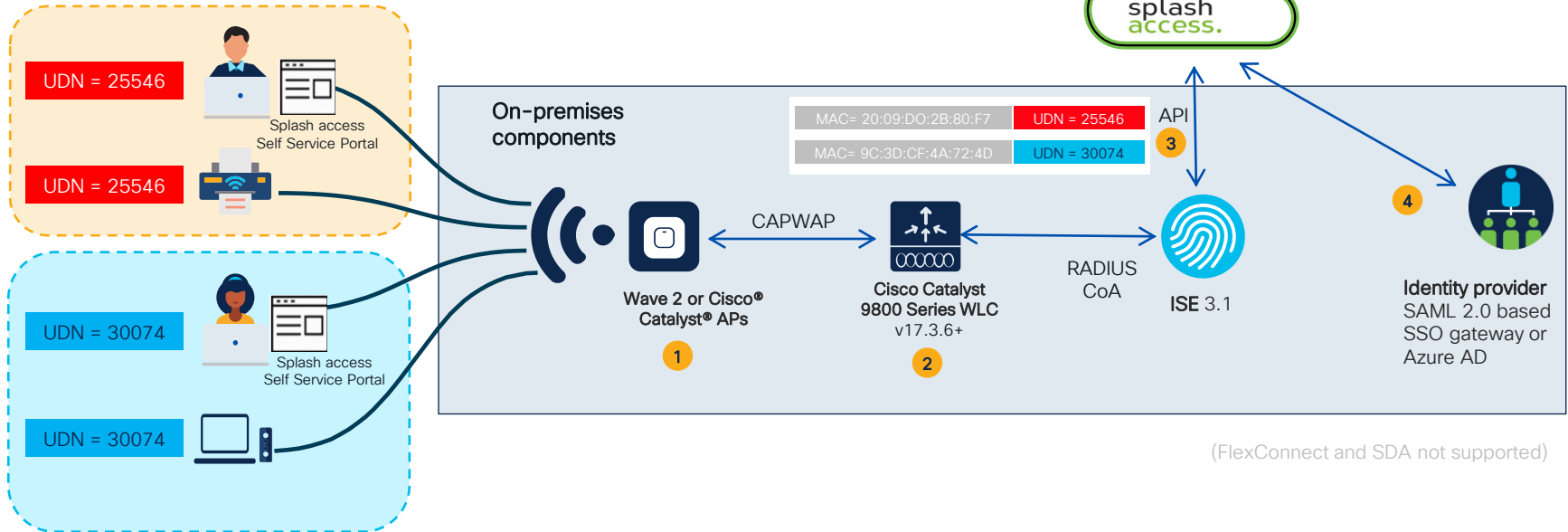
☐	Name ▲	Pre-Shared Key	Group Policy
☐	Cameras		Camera Policy
☐	Scanners		Scanner Policy
☐	POS		POS Policy



Wi-Fi Personal Network



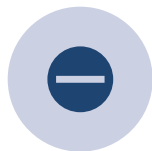
User Defined Network+



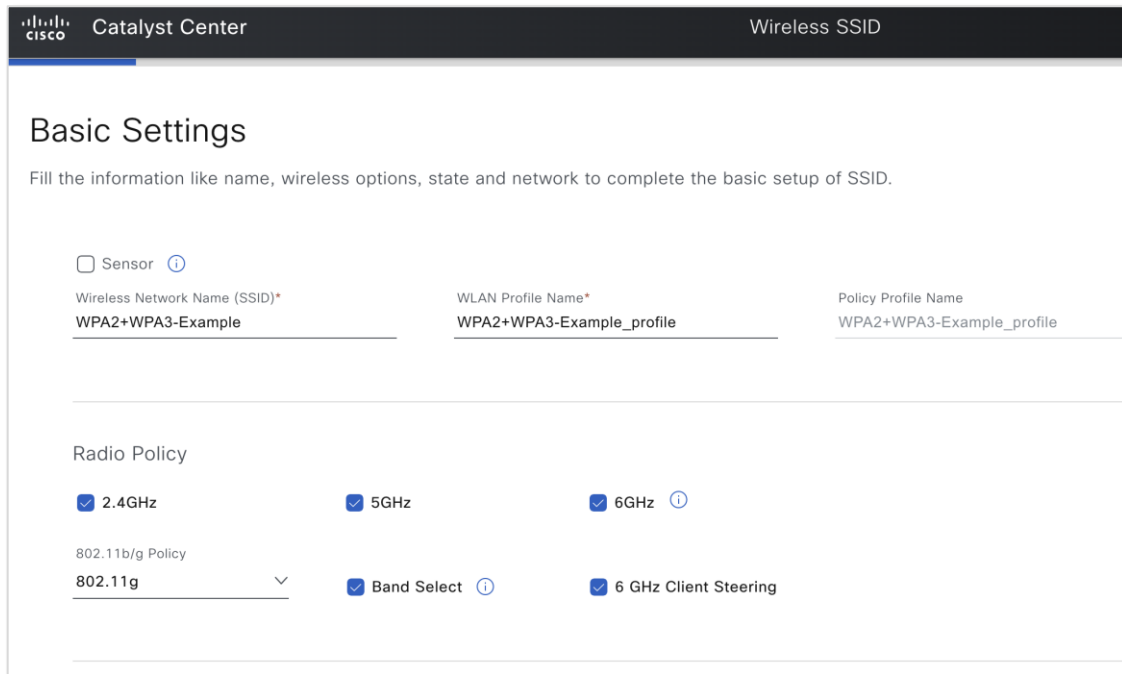
Security Implications of 6GHz



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



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



The screenshot shows the 'Basic Settings' section of the Cisco Catalyst Center 'Wireless SSID' configuration page. It includes fields for 'Wireless Network Name (SSID)*', 'WLAN Profile Name*', and 'Policy Profile Name'. Below these is the 'Radio Policy' section with checkboxes for 2.4GHz, 5GHz, and 6GHz. The 6GHz checkbox is checked. There is also a section for '802.11b/g Policy' with a dropdown menu set to '802.11g' and checkboxes for 'Band Select' and '6 GHz Client Steering', both of which are checked.

Cisco Catalyst Center Wireless SSID

Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID.

☐ Sensor ⓘ

Wireless Network Name (SSID)* WLAN Profile Name* Policy Profile Name

WPA2+WPA3-Example WPA2+WPA3-Example_profile WPA2+WPA3-Example_profile

Radio Policy

☒ 2.4GHz ☒ 5GHz ☒ 6GHz ⓘ

802.11b/g Policy

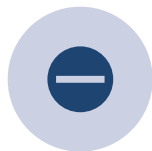
802.11g ▼ ☒ Band Select ⓘ ☒ 6 GHz Client Steering

From IOS-XE 17.12.1

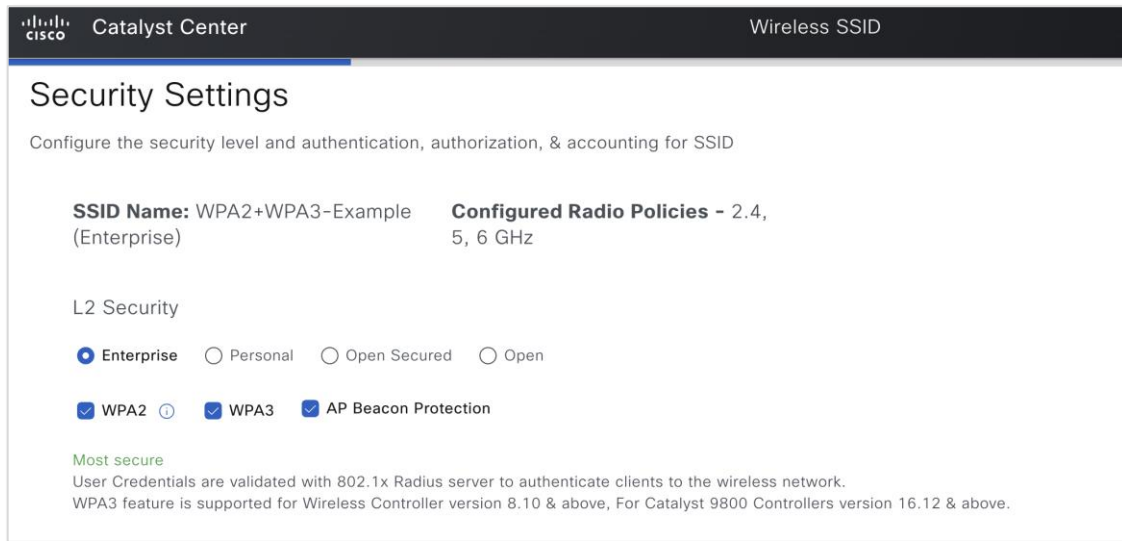
Security Implications of 6GHz



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



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

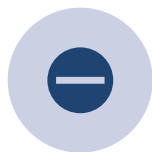


From IOS-XE 17.12.1

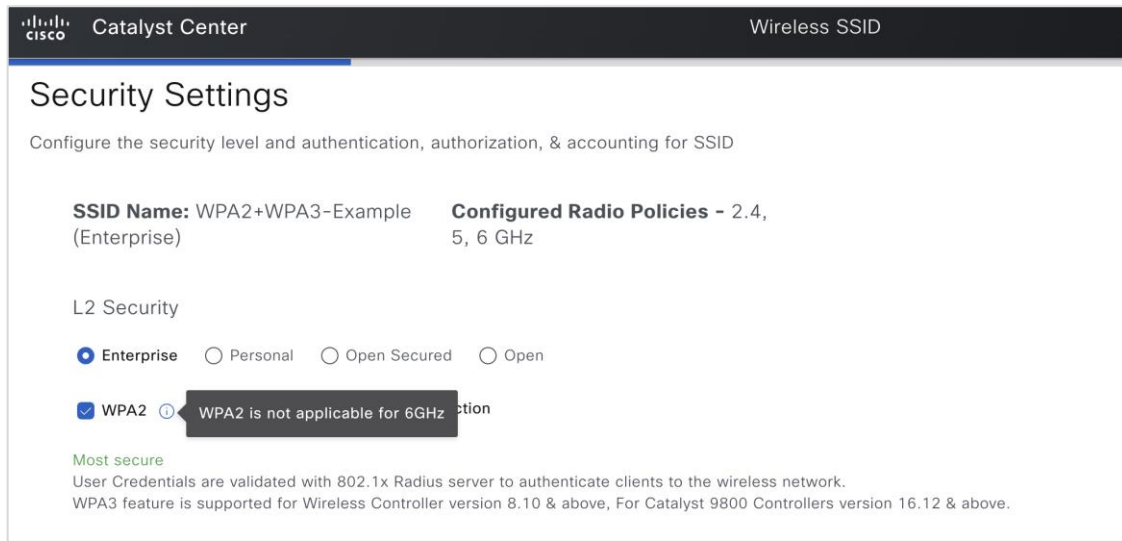
Security Implications of 6GHz



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



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

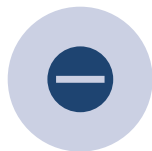


From IOS-XE 17.12.1

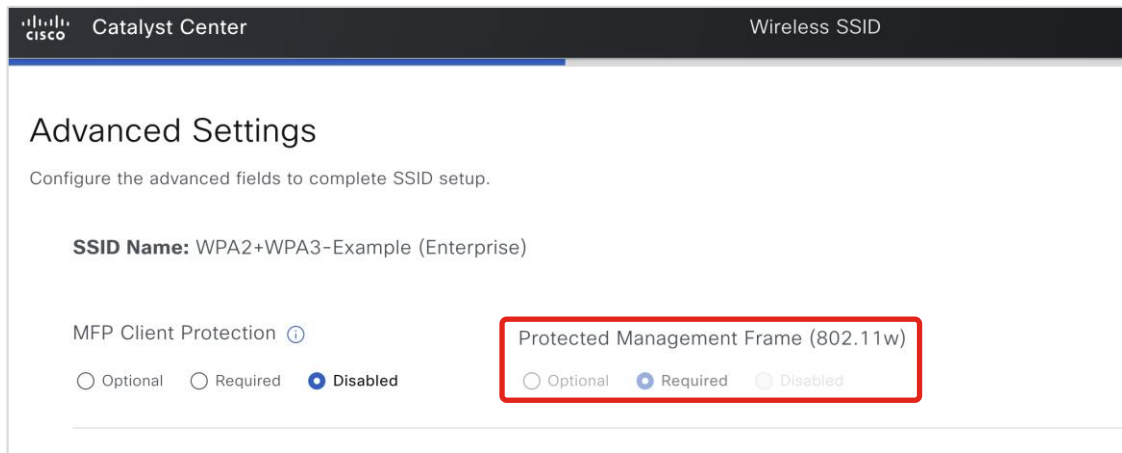
Security Implications of 6GHz



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



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



Security Implications of 6GHz

FYI

General Security Advanced

Profile Name* employee

SSID* employee

WLAN ID* 5

Status **ENABLED**

Broadcast SSID **ENABLED**

Radio Policy ⓘ

[Show slot configuration](#)

6 GHz

Status **ENABLED** ⓘ

- ✗ WPA2 Disabled
- ✓ WPA3 Enabled
- ✓ Dot11ax Enabled

5 GHz

Status **ENABLED**

2.4 GHz

Status **ENABLED**

802.11b/g Policy 802.11g only ▼



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



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

Security Implications of 6GHz



General Security Advanced Add To Policy Tags

Profile Name* enterprise

SSID* enterprise

WLAN ID* 8

Status **ENABLED**

Broadcast SSID **ENABLED**

Radio Policy ⓘ

Show slot configuration

6 GHz

Status **ENABLED**

✓ WPA3 Enabled

✓ Dot11ax Enabled

5 GHz

Status **ENABLED**

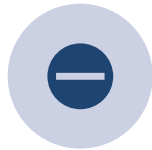
2.4 GHz

Status **ENABLED**

802.11b/g Policy 802.11b/g ▼



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

FYI



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



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

General Security Advanced Add To Policy Tags

Profile Name* enterprise Radio Policy ⓘ

SSID* enterprise

General Security Advanced Add To Policy Tags

WLAN Layer2 Layer3 AAA

Status ☐ WPA + WPA2 ☒ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☐ None

Broch MAC Filtering ☐ Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐ WPA2 Policy ☒ WPA3 Policy ☒ GTK Randomize ☐ Transition Disable ☐

WPA2/WPA3 Encryption

AES(CCMP128) ☒ CCMP256 ☐ GCMP128 ☐ GCMP256 ☐

Protected Management Frame

PMF Optional

Association Comeback Timer* 1

Fast Transition

Status Adaptive Ena...

Over the DS ☐

Reassociation Timeout * 20

Auth Key Mgmt

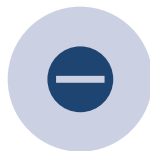
802.1X ☒ PSK ☐ CCKM ☐ SAE ☐ FT + SAE ☐ OWE ☐ FT + 802.1X ☐ FT + PSK ☐ 802.1X-SHA256 ☒ PSK-SHA256 ☐



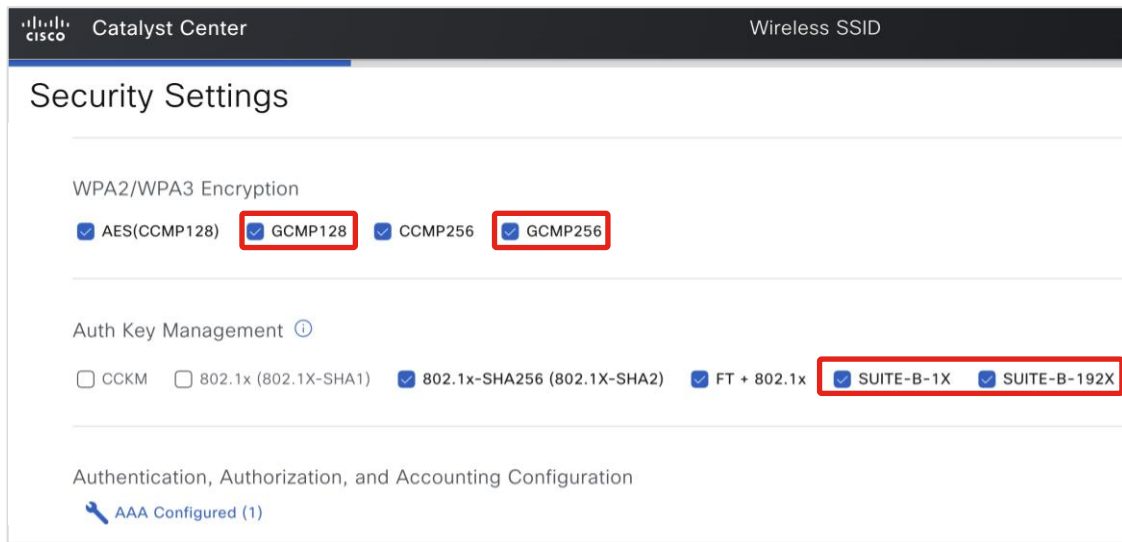
Security Implications of Wi-Fi 7



Wi-Fi 7 brings new AKM and cipher suites for OWE and SAE



These are mandatory for support of Wi-Fi 7 MCS rates and MLO



Wi-Fi 7 Security



- Wi-Fi 7 brings new AKM support for WPA3-SAE and new increased ciphers for OWE & SAE
- WPA3 / OWE mandatory for EHT (11be MCS rates) & MLO

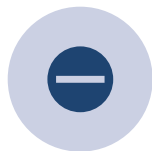
Older	Wi-Fi 6E (6 GHz)	Wi-Fi 7
Open	OWE (AKM: 18) (Cipher: CCMP 128)	OWE (AKM: 18) (Cipher: CCMP 128 or GCMP 256)
WPA2/WPA3 Transition/ WPA3-SAE(Personal), PMF Optional (WPA 2 - AKM - 2, 4 & 6) (WPA 3 - AKM - 8 & 9) (Cipher: CCMP 128 or AES)	WPA3-SAE (Personal), PMF Mandatory (AKM: 8 & 9) (Cipher: CCMP 128 or AES)	WPA3-SAE (Personal), PMF Mandatory (AKM: 24 & 25) (Cipher: CCMP128 or GCMP 256)
WPA/WPA3 Transition/ WPA3-SAE Enterprise, PMF Optional (AKM 1, 3 & 5, 11 & 12) (Cipher: AES, CCMP 128, GCMP128 GCMP256)	WPA3 Enterprise, PMF Mandatory (AKM: 3, 5, 11 & 12) (Cipher: GCMP 128 & GCMP 256)	WPA3 Enterprise, PMF Mandatory (AKM: 3, 5, 11 & 12) (Cipher: GCMP 128 & GCMP 256)

Cipher: GCMP 256 – Better Encryption & Speed; AKM: Better security

Security Implications of 6GHz



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



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

Security *WPA3 Transition Mode Enterprise with 0 RADIUS servers*

WPA encryption ⓘ WPA3 Transition Mode ▾

802.11w ⓘ ☐ Enabled (allow unsupported clients)
☒ Required (reject unsupported clients)
☐ Disabled (never use)

Mandatory DHCP Enabled Disabled

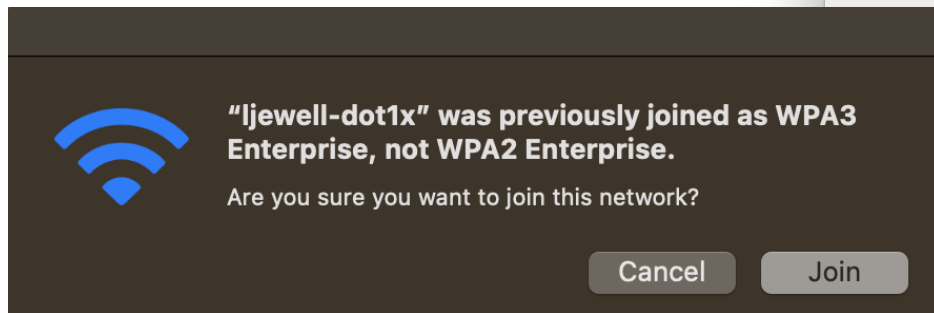
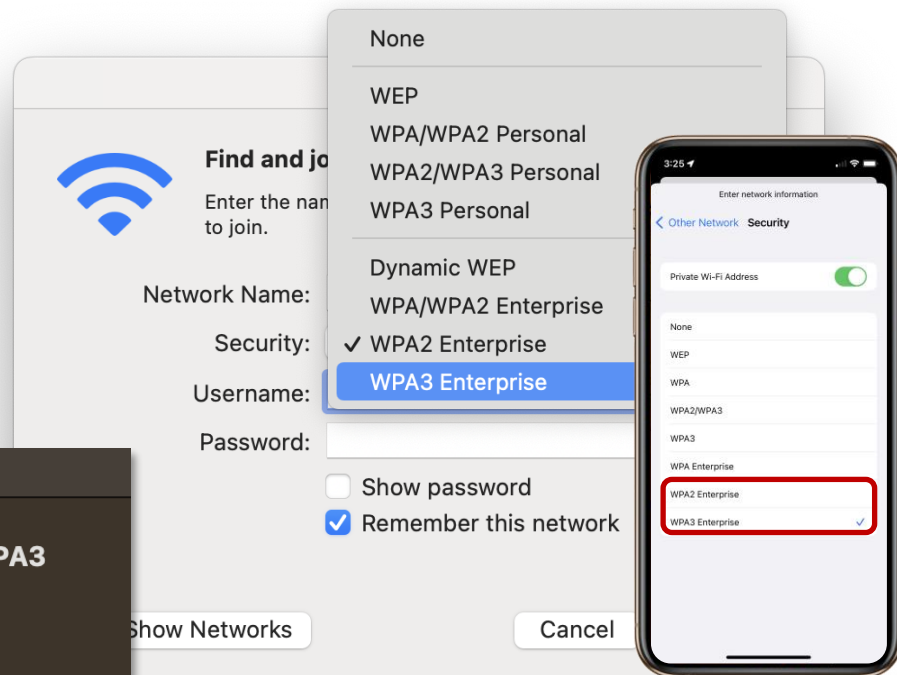
Advanced WPA3 settings *(Cipher and AKM suite settings)* ▾

ⓘ Certain Cipher suite and AKMs are required for capable APs to operate in 802.11be (Wi-Fi 7) mode. Please refer to [documentation](#) for more details.

From Meraki 31.X

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

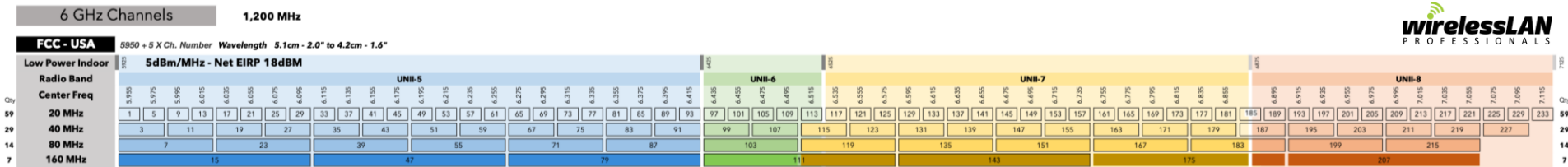
- Manually created client device profiles must select WPA2 *or* WPA3
- Only one profile for a given SSID is permitted



6GHz AP Discovery Challenges

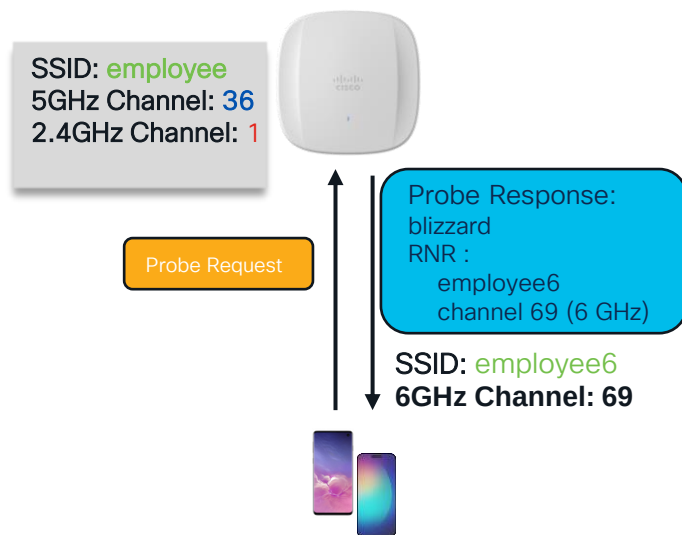


- There are a total of 59x 20MHz channels in the 6GHz band
- Wi-Fi clients can only send Probe Requests on 20MHz channels
- It would take 6 seconds to passively scan all 59 channels



Reduced Neighbour Report (RNR)

Wi-Fi 6E and Wi-Fi 7



- 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 and Wi-Fi 7



- 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 and Wi-Fi 7

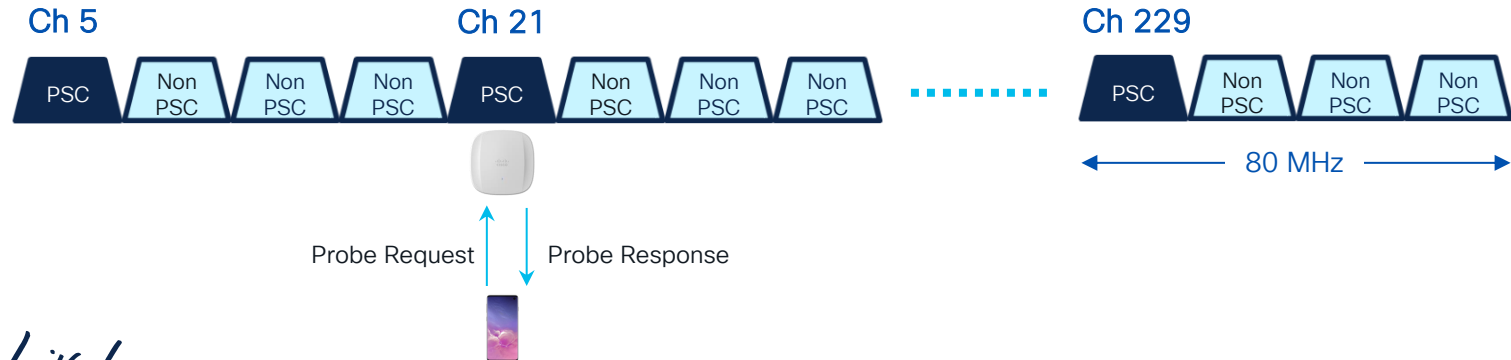
- Broadcast probe response transmitted every 20ms
- Contains detailed information as in the beacon
- Carries multiple BSSIDs
- Reduces probe request overhead
- UBPR is not as widely adopted as FILS
- FILS and UBPR are mutually exclusive

Probe Restrictions in 6GHz

Wi-Fi 6E and Wi-Fi 7



- 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



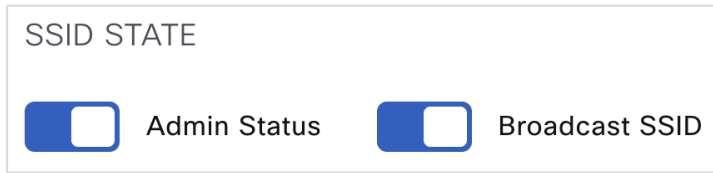
Wi-Fi 6E and Wi-Fi 7

- 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 provide no real 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

Interoperability and Compliance



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



Supported



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



Not supported and no release planning



* Mandatory for WPA3-Personal compliance

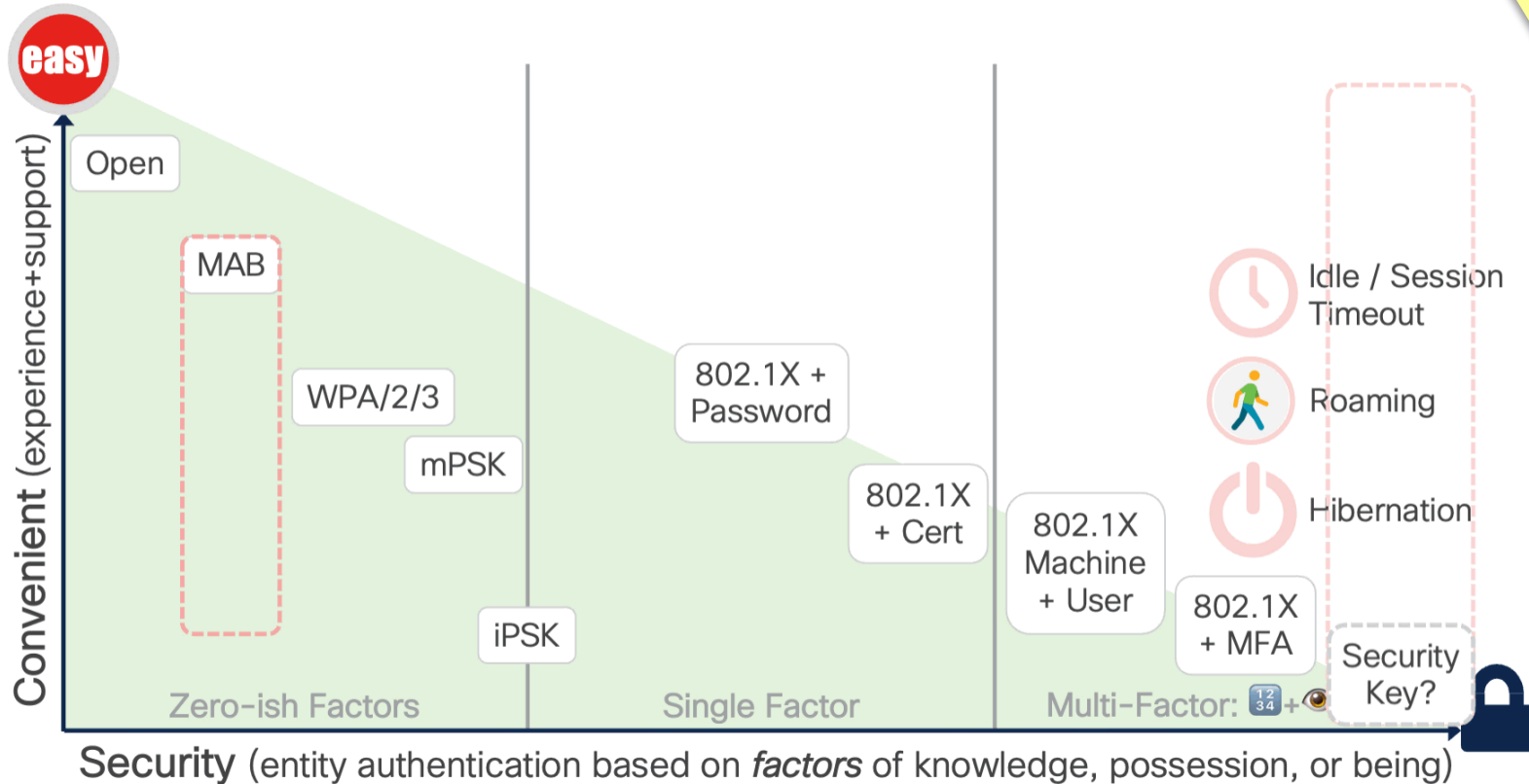
WPA3

New Requirements

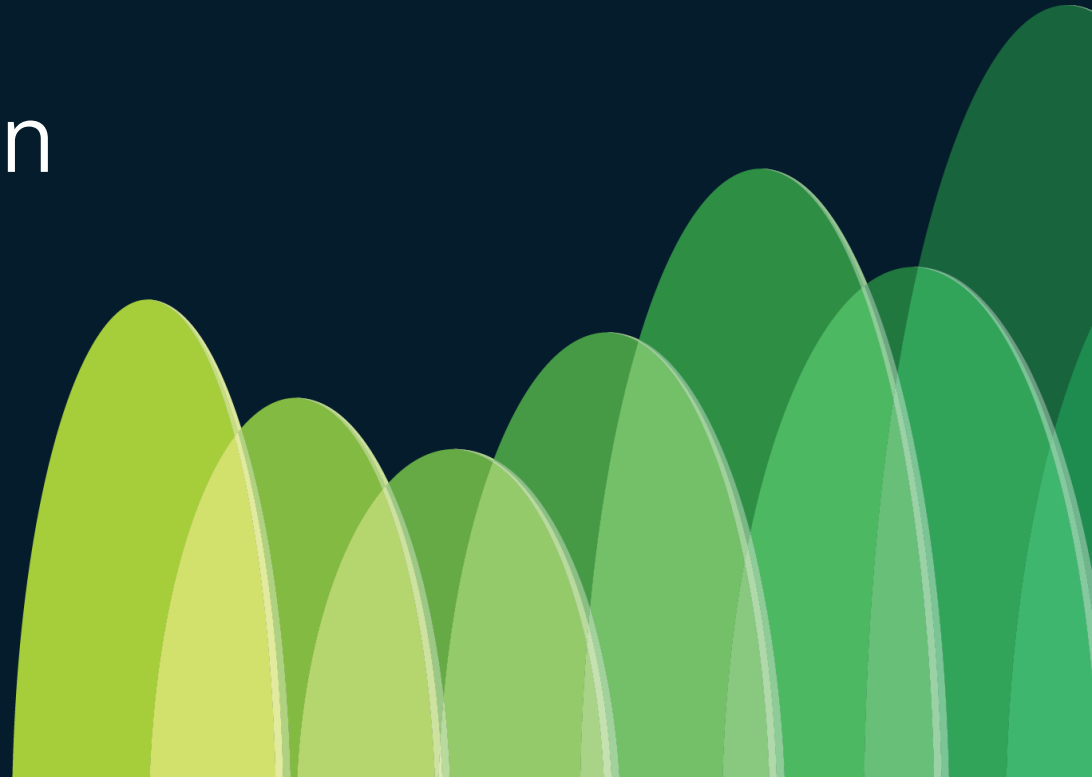


Features	Catalyst (Local)	Catalyst (Flexconnect)	Meraki
WPA3 FT-802.1X-SuiteB-192bit + AES-GCMP256 (Microsoft and Zebra ASK)	✗	✗	✓
AKM FT-802.1X-SHA384(22) and 802.1X-SHA384(23) Support	✗	✗	✗
SAE iPSK Central Auth support	✓	✗	✗
WGB WPA3 Support for COS AP	✗	✗	N/A
SAE-PK Support	✗	✗	TBD
WPA3 Enterprise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

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

Threat 360: Mac CE:9C:1E:ED:6D:F0

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
High	sjc14rogueule	UNKNOWN	Active	Open	Nov 2, 2024 1:56 PM

Location: Global/San Jose/Building 14/Floor1

Detections (3) Clients (0)

Detecting AP	Detecting AP Site	Adhoc	Rogue SSID	Rogue AP MLD MAC	RSSI (dBm)	Channels	Radio Type (B...
SJC14-F1-9164-3	Global/San Jose/Building 14/Floor1	No	thunderstorm	-	-56	149	802.11ax/be(6GHz)

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/catalyst-center-rogue-management-application/2-3-7/quick-start-guide/b_rogue_management_qsg_2_3_7/rogue_management_chapter_01.html

Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies

Signature	Default Threshold	Configured Threshold	Time Interval(In Seconds)	Forensic Capture
Association flood	15	Range: 7 - 45 15	1	☒
Authentication Failure Flood	150	Range: 75 - 450 150	10	☒
Authentication flood	15	Range: 7 - 45 15	1	☒
Beacon Flood	30000	Range: 15000 - 90000 30000	10	☒
Block Ack Flood	1000	Range: 500 - 3000 1000	10	☒
Broadcast probe	1000			☒

aWIPS and Forensic Capture Enablement



aWIPS ⓘ



Forensic Capture ⓘ

The image displays the Cisco Catalyst Center interface for Rogue and aWIPS management. The main view shows a list of threats (365) with columns for Threat Level, MAC Address, and Type. A sidebar on the right provides detailed definitions for various attacks, including CTS Flood, RTS Flood, EAPOL logoff flood, Deauthentication broadcast, Deauthentication flood, EAPOL-Start V1 Flood, PS Poll Flood, Fuzzed Probe Response, Fuzzed Probe Request, Invalid MAC OUI frame, Authentication Failure Flood, Malformed Association Request, AirDrop Session, Block Ack Flood, and Probe Response Flood. A 'Client Exclusion Policies' panel is also visible, listing policies such as 'Excessive 802.11 Association Failures', 'Excessive 802.1X Authentication Failures', 'Excessive 802.1X Authentication Timeout', 'IP Theft or IP Reuse', and 'Excessive Web Authentication Failures'. Each policy has a toggle switch and a link to view details.

Rogue and WIPS Reporting and APIs



Catalyst Center Reports

Generated Reports | **Report Templates** | Usage Insights

All

AI Endpoint Analytics

Access Point

Audit Log

Client

Compliance

Configuration Archive

ExoX

Executive Summary

Group Communication Summary

Group Pair Communication Analytics

Inventory

Licensing

Long Term

Network Devices

Rogue and aWIPS

SWIM

Security Advisories

Telemetry

Rogue and aWIPS
New Threat

This report provides for the detailed information about the new rogue AP's and aWIPS threats that are seen in the network.

CSV TDE JSON

Rogue and aWIPS
Rogue Additional Detail

This report provides additional information of the rogue threats with details at BSSID level. The additional information includes

CSV TDE JSON

Rogue and aWIPS
Threat Detail

This report provides for the detailed information about the rogue AP's and aWIPS threats that are seen in the network.

CSV TDE JSON

Catalyst Center Platform / Developer Toolkit

APIs Integration Flows Event Notifications

Search

Authentication

Cisco DNA Center System

Connectivity

Ecosystem Integrations

Event Management

Integrations

Know Your Network

Applications

Clients

Compliance

Devices

ExoX

Issues

Security Advisories

Sensors

Sites

Topology

Users

Operational Tasks

Policy

Site Management

System

System Settings

Security Advisories

Method	Name	Description	URL
GET	Get Advisories Summary	Retrieves summary of advisories on the network.	/security-advisory/advisory/aggregate
GET	Get Advisories List	Retrieves list of advisories on the network.	/security-advisory/advisory
GET	Get Advisory Device Detail	Retrieves advisory device details for a device.	/security-advisory/device/\${deviceid}
GET	Get Devices Per Advisory	Retrieves list of devices for an advisory.	/security-advisory/advisory/\${advisoryid}/device
GET	Get Advisories Per Device	Retrieves list of advisories for a device.	/security-advisory/device/\${deviceid}/advisory

Sensors

Method	Name	Description	URL	Actions
POST	Create sensor test template	Intent API to create a SENSOR test template with a new SSD, existing SSD, or both new and existing SSD.	/sensor	↗
DELETE	Delete sensor test	Intent API to delete an existing SENSOR test template.	/sensor	↗
PUT	Duplicate sensor test template	Intent API to duplicate an existing SENSOR test template.	/sensorTestTemplate	↗
PUT	Edit sensor test template	Intent API to deploy, schedule, or edit an existing SENSOR test template.	/AssuranceScheduleSensorTest	↗

Catalyst Center Platform / Developer Toolkit

APIs Integration Flows Event Notifications

Search

Authentication

Cisco DNA Center System

Connectivity

Ecosystem Integrations

Event Management

Integrations

Know Your Network

Applications

Clients

Compliance

Devices

ExoX

Issues

Security Advisories

Sensors

Sites

Topology

Users

Operational Tasks

Policy

Site Management

System

System Settings

Devices

Method	Name	Description	URL	Actions
GET	Get Allowed Mac Address	Intent API to fetch all the allowed mac addresses in the system.	/security/threats/rogue/allowed-list	↗
POST	Threat Summary	The Threat Summary for the Rogues and aWIPS.	/security/threats/summary	↗
GET	Get Threat Types	Intent API to fetch all threat types defined.	/security/threats/type	↗
GET	Get Allowed Mac Address Count	Intent API to fetch the count of allowed mac addresses in the system.	/security/threats/rogue/allowed-list/count	↗
DELETE	Remove Allowed Mac Address	Intent API to remove the threat mac address from allowed list.	/security/threats/rogue/allowed-list/\${macAddress}	↗
POST	Threat Detail Count	The details count for the Rogue and aWIPS threats.	/security/threats/details/count	↗
POST	Add Allowed Mac Address	Intent API to add the threat mac address to allowed list.	/security/threats/rogue/allowed-list	↗
GET	Get Threat Levels	Intent API to fetch all threat levels defined.	/security/threats/level	↗
POST	Threat Details	The details for the Rogue and aWIPS threats.	/security/threats/details	↗
POST	The Trend analytics data for the network Device in the specified time range.	The Trend analytics data for the network Device in the specified time range. The data is grouped based on the trend time interval, other input parameters like...	/smc/dataapi/v1/networkDevices/\${deviceid}/trendAnalytics	↗
GET	Get Chassis Details for Device	Returns chassis details for given device ID.	/network-device/\${deviceid}/chassis	↗

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 9178
- Catalyst 9176
- Catalyst 9136
- Catalyst 9166
- Catalyst 9164
- Catalyst 9162
- Catalyst 9130
- Catalyst 9120



Rogue Access Points

- A **Rogue AP** is any AP which is not part of our infrastructure
 - Most of them will be legitimate
 - Some of them may be malicious
- Correctly differentiating between the two is critical

Rogue Detection and Configuration

Detect Access Points that have been installed on a secure network without explicit authorization from a system administrator and configure rogue general configuration parameters



Rogue Detection

Minimum RSSI (dBm)*

-90

Value should be in range -128 and -70.

Transient Interval (seconds)*

0

Value should be 0 or from 120 to 1800.

Report Interval (seconds)*

10

Value should be in range 10 and 300.

General

Client Exclusion Policies

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 Alarm Threshold.



1

Allowed List

AP MAC addresses that are in the allowed list are known AP and so are not considered as malicious.

Friendly

Friendly APs belong to one wireless controller and are seen as a Rogue AP by another wireless controller, where both wireless controllers are managed by Catalyst Center.

Neighbor

Neighbor APs are Rogue APs with signal strength less than or equal to -75dBm and are not broadcasting any corporate SSIDs.

Rogue AP Enhancements



Existing

- ❑ Current Rogue Classification and Containment entries in C9800 is limited to 625

New

- ❑ This scale limit is adequate for some deployments
- ❑ Starting 17.13.1, the scale number of Rogue Classification and Containment entries is increased from 625 to 10000

Rogue Scale - Configuration



Following Classification and Containment entries are extended from 625 to 10000

Configuration:

```
C9800(config)# wireless wps rogue ap friendly <MAC> state {internal|external}
C9800(config)# wireless wps rogue ap malicious <MAC> state {alert|contain}
C9800(config)# wireless wps rogue ap unclassified <MAC> state {alert|contain}
C9800(config)# wireless wps rogue client contain <MAC> <containment_level>
```

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
```

Cisco Catalyst Centre Threat Levels

Informational

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

Potential

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

High

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

Rogue 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

Add Rogue General Configuration

This capability allows to configure Rogue general configuration and client exclusions policies.

Design Name*

Lock all

General

Client Exclusion Policies

Rogue Detection Security Level.

CUSTOM

Expiration timeout for Rogue APs (seconds).

Validate Rogue Clients against AAA.

Validate Rogue APs against AAA.

Rogue Polling Interval (seconds).

Detect and Report Adhoc Networks.

aWIPS Profiles

- Create custom aWIPS profiles to focus on key concerns and customise when to perform automatic forensic capture

Edit aWIPS Profile

Profile Name
CustomaWIPSProfile

Signatures (27)

Search Table

Reset to Default

Signature	Default Threshold	Configured Threshold	Time Interval(In Seconds)	Forensic Capture
Airdrop Session	NA		NA	☐
Association flood	15	14	1	☐
Authentication Failure Flood	150	150	10	☐
Authentication flood	15	15	1	☐
Beacon Flood	30000	30000	10	☐
Block Ack Flood	1000	1000	10	☐
Broadcast probe	1000	1000	10	☐

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 is critical

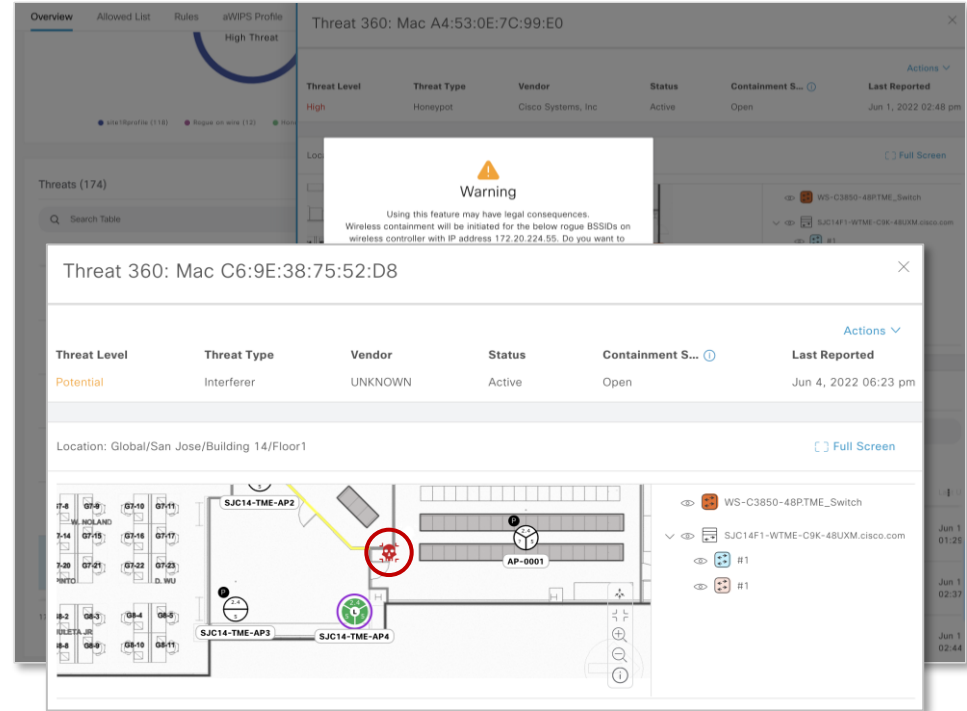
The screenshot displays the Cisco Meraki dashboard interface. A warning dialog box is centered on the screen, titled "Warning" with an orange triangle icon. The text inside the dialog reads: "Using this feature may have legal consequences. Wireless containment will be initiated for the below rogue BSSIDs on wireless controller with IP address 172.20.224.55. Do you want to continue?". Below the text, there is a "Rogue BSSID" label and two input fields 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 shows the "Threats (174)" list with columns for Threat Level, MAC Address, and Type. The selected threat is "High" with MAC address "A4:53:0E:7C:99:E0" and Type "HoneyPot". To the right, the "Threat 360" details for this threat are visible, showing Threat Level as "High", Threat Type as "HoneyPot", Vendor as "Cisco Systems, Inc", Status as "Active", and Containment Status as "Open". Below this, a table lists associated devices with columns for Device Name, Location, ID, Vendor, Model, and Status. The table shows three entries for "SJC14-TME-AP6", "SJC14-TME-AP4", and "SJC14-TME-AP4", all with "Inactive" status.

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

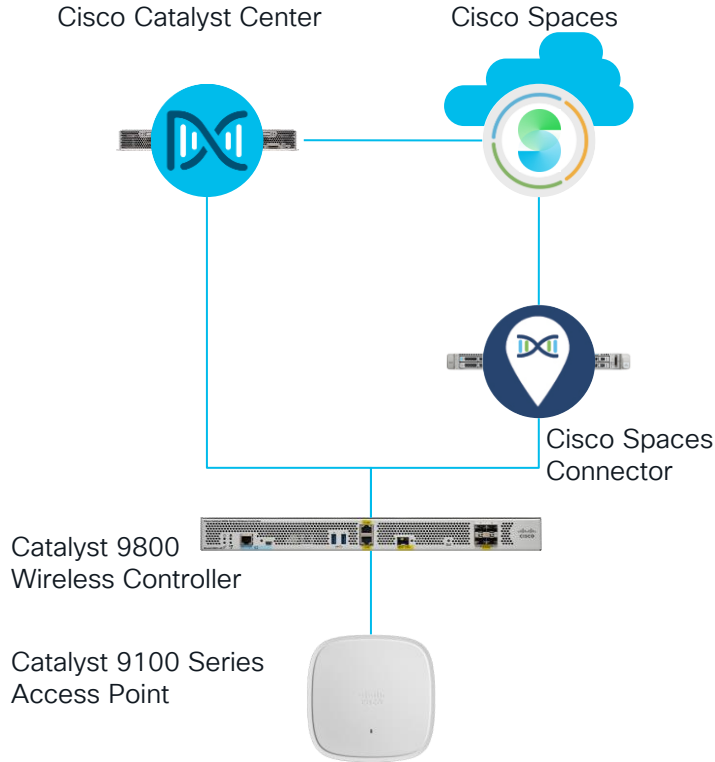
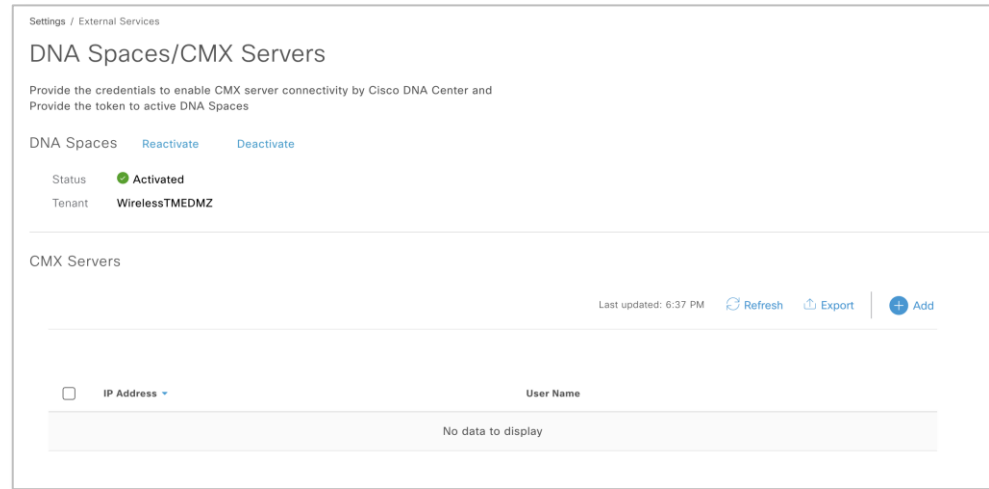
Device Name	Location	ID	Vendor	Model	Status
SJC14-TME-AP6	Global/San Jose/Building 14/Floor1	No	IDNAS Demo	OpenRoaming	Inactive
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNA Spaces	Demo LAN	Active
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo		Active

Rogue AP Containment

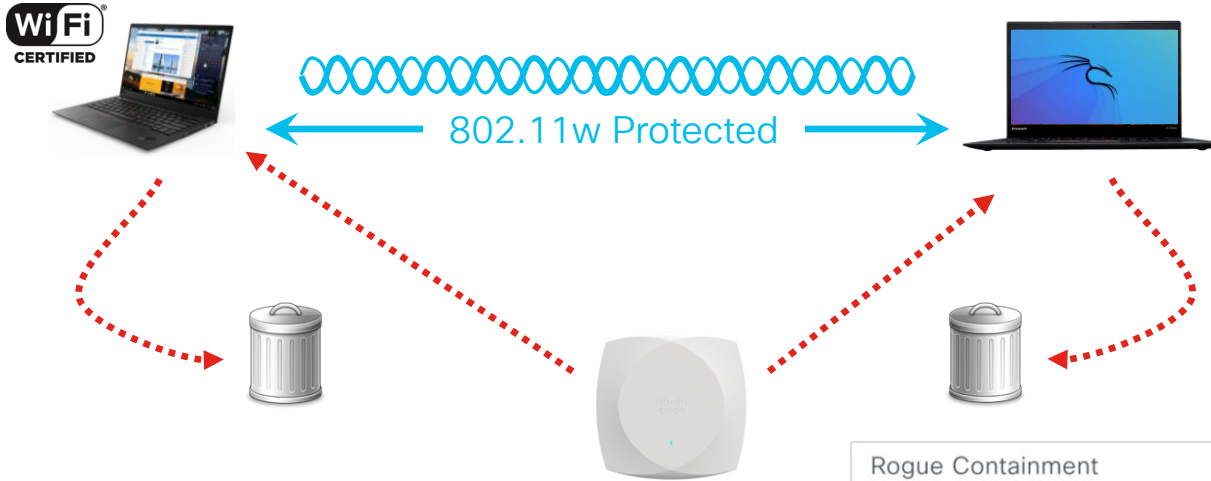
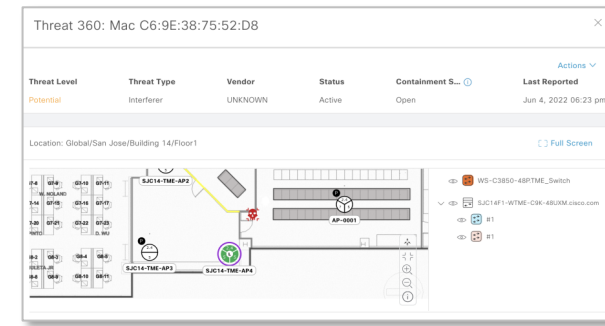
- How do we contain Rogue APs?
 - Containment is a spoofed 802.11 disassociation/deauthentication request attack
- How does WPA3 affect Rogue AP containment?
 - 802.11w will change how we can mitigate Rogue AP related threats
 - The ability to physically locate rogues is critical



Enabling Location Services



Rogue Containment with WPA3



Rogue Containment

Contain the detected rogues in 6GHz



PMF Denial



PMF Denial is supported from IOS-XE version 17.12 and above

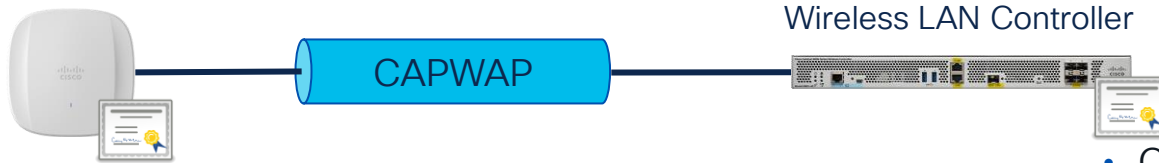
Rogue on Wire

- 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

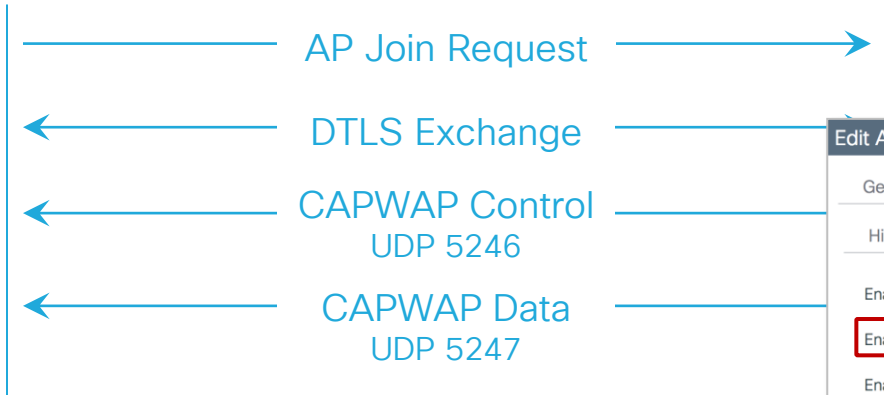
The screenshot displays the Cisco aWIPS interface. On the left, the 'High Threat Summary' section shows 'Active High Threats (14)' with a circular gauge indicating 14 threats. Below this, a table lists threats with columns for Threat Level, MAC Address, and Type. The threat with MAC 6A:3A:0E:53:A6:E9 is highlighted as 'High' and 'Rogue on wire'.

The main panel shows the details for 'Threat 360: Mac 6A:3A:0E:53:A6:E9'. It includes a table with columns: Threat Level (High), Threat Type (Rogue on wire), Vendor (UNKNOWN), Status (Active), and Containment Status (Open). An 'Actions' menu is visible, with 'Shutdown Switchport' highlighted. Below the table, a floor plan diagram shows the location of the threat (SJC14-TME-AP9) and the switch (WS-C3850-48PTME_Switch). A table at the bottom provides details for the switch port, including 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), and Last Updated (Jun 5, 2022 09:40 am).

Securing AP to Controller Communication



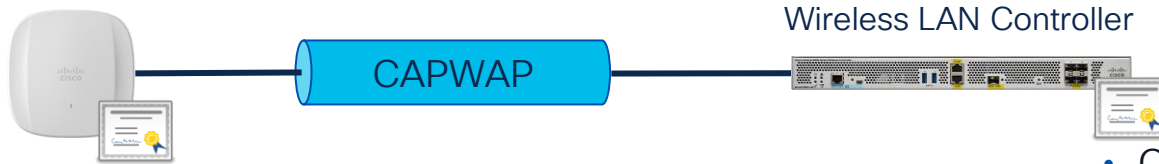
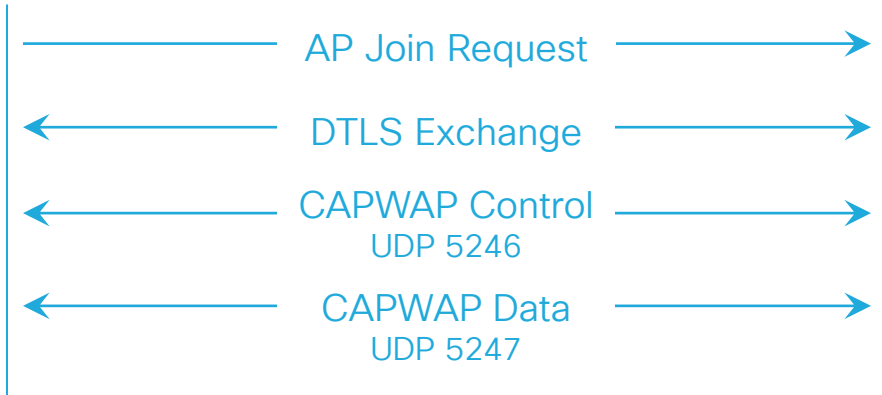
- CAPWAP Control encrypted by default
- CAPWAP Data encapsulated but not encrypted by default



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 Disable					
Preferred Mode Disable					

Securing AP to Controller Communication



- CAPWAP Control encrypted by default
- CAPWAP Data encapsulated but not encrypted by default
 - Except for Office Extend AP (OEAP) Mode

Securing AP Switch Port Access



802.1x
← Authentication (EAP-FAST) →



How do we bootstrap configure the AP?

The screenshot shows the 'Add AP Join Profile' configuration window with the 'Management' tab selected. The 'Credentials' sub-tab is active, showing fields for 'Dot1x Username', 'Dot1x Password', and 'Dot1x Password Type'. The 'Dot1x Password Type' is set to 'clear'. There are 'Cancel' and 'Apply to Device' buttons at the bottom.

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

Create Rogue rule

Choose the threat level and conditions for your rule ⓘ

Threat Level

☒ High ☐ Potential ☐ Informational

☐ Enable Auto-Containment **BETA** ⓘ

Match Any ▼ of the following conditions. ⓘ

Add Condition ^

SSID

RSSI

Encryption Condition

Minimum Rogue Client Count

FYI



Warning

Using this feature may have legal consequences. Wireless containment will be initiated for the rogue rules which have Auto-Containment enabled.

Cancel

Ok

Cisco Catalyst Center Security Advisories



Cisco DNA Center 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 Advisories

SUMMARY

- > Scan Criteria
- > Scan Status
- > Device Family (5)
- > Image Version (16)
- > Sites (48)
- > Advisory Impact

Devices (64)

[Filter](#) [Tag](#)

☐	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



Cisco DNA Center Tools / Security Advisories

Click [here](#) to access customized security advisories

ADVISORIES
2 Critical 39 High 28 Medium

SCAN CRITERIA
5 Software Version

Devices Advisories

SUMMARY
> Scan Criteria
> Scan Status
> Device Family (5)
> Image Version (16)
> Sites (48)
> Advisory Impact

Devices (64)
Filter Tag
Device Name
ASR1K_TME.ASR
SJC14F1-WTME
c9800-40-TMED
SpacesWLC
Spirent_WLC.cise

SJC14F1-WTME-C9K-48UXM.cisco.com (172.20.224.109)
Reachable Uptime: 25 days 7 hrs 10 mins
Run Commands View 360 Last updated: 3:10 PM Refresh

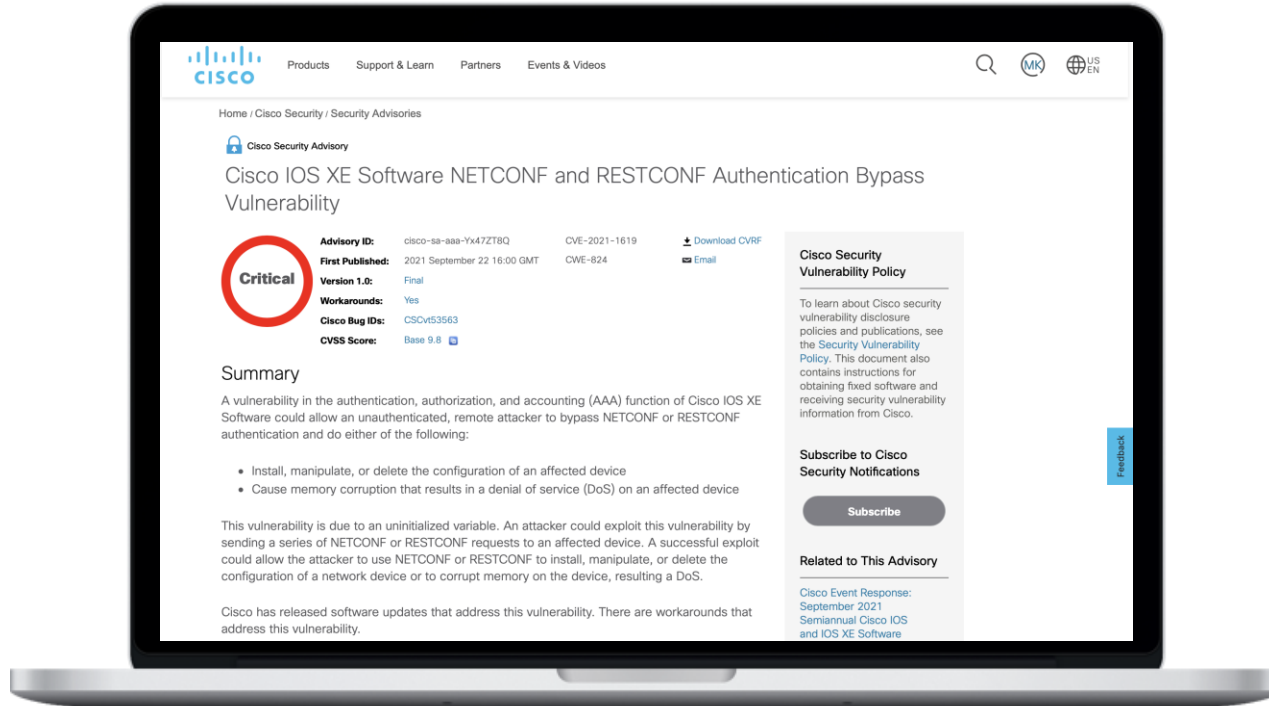
Details Advisories Configuration

Advisories (69) Active Suppressed

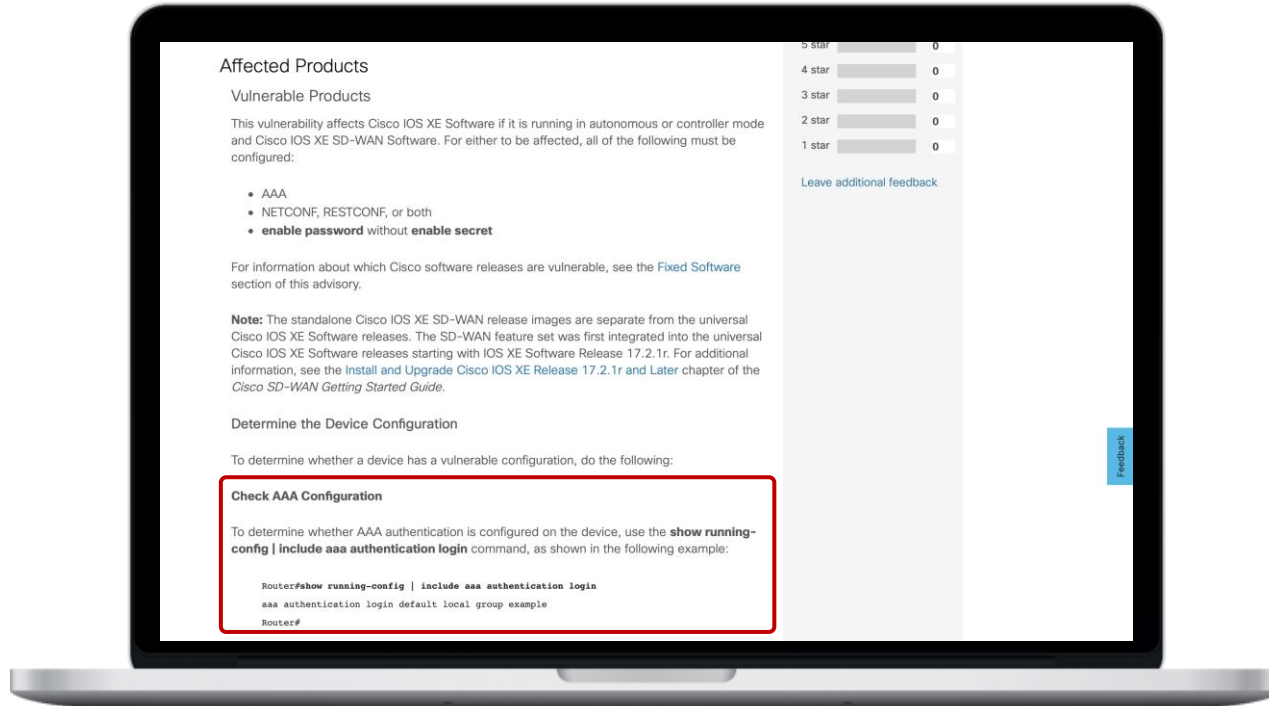
Filter 0 Selected Suppress Advisory

Advisory ID	Advisory Title	CVSS Score	Impact	Fix
cisco-sa-aaa-Yx47ZT8Q	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability	9.8	Critical	16.9.8 16.9.8
cisco-sa-telnetd-EFJeZPx	Telnet Vulnerability Affecting Cisco Products: June 2020	9.8	High	16.9.6
cisco-sa-ioxPE-KgGvCAf9	Cisco IOx for IOS XE Software Privilege Escalation Vulnerability	9.8	Critical	N/A

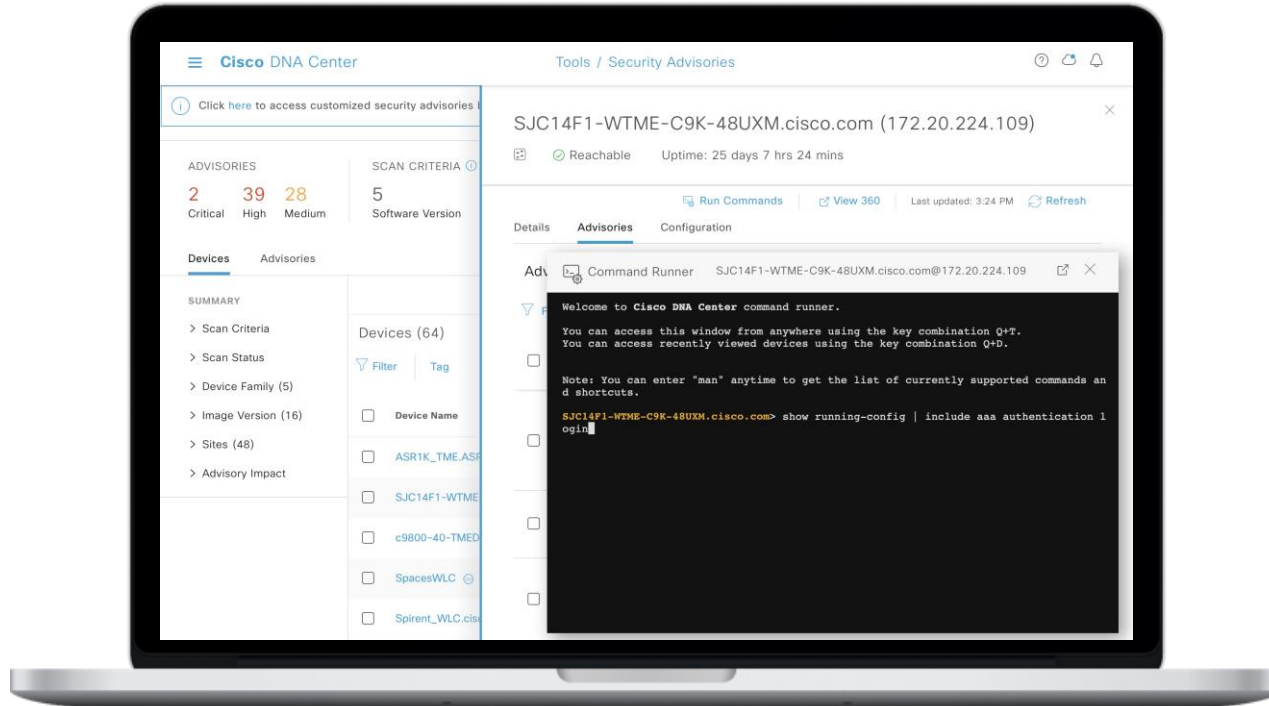
Cisco Catalyst Center Security Advisories



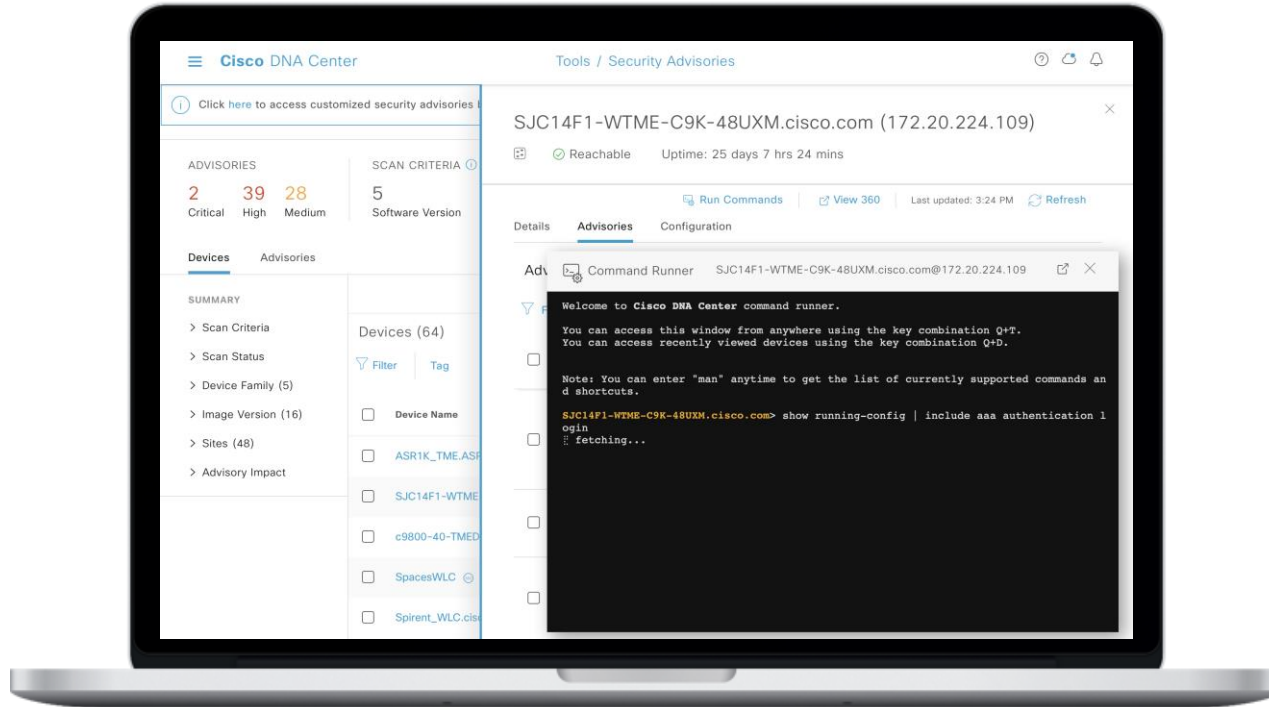
Cisco Catalyst Center Security Advisories



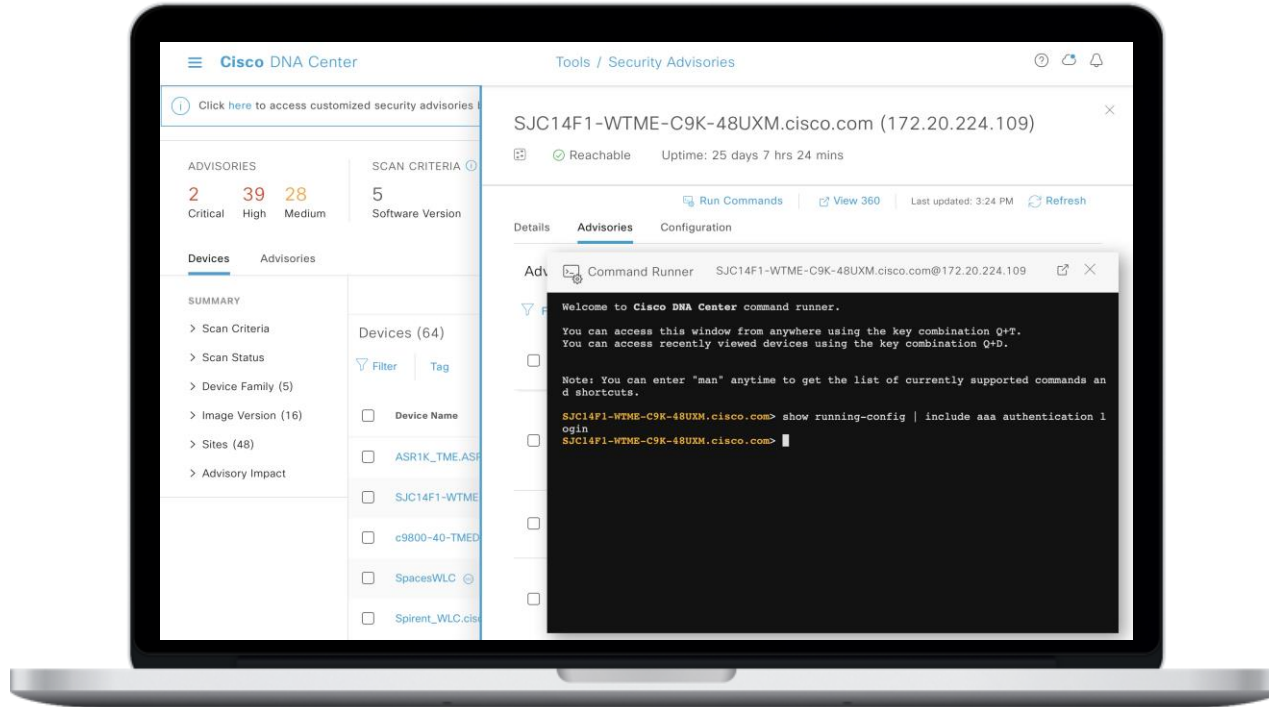
Cisco Catalyst Center Security Advisories



Cisco Catalyst Center Security Advisories



Cisco Catalyst Center Security Advisories



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

CISCO *Live!*

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 web interface. At the top, there's a navigation bar with tabs: 'Configure', 'Rogue SSIDs 24', 'Other SSIDs 595', 'Spoofs 31', 'Malicious broadcasts 0', and 'Packet floods 0'. A yellow sticky note with 'FYI' is placed in the top right corner. The main section is titled '24 rogue SSIDs' with a sub-header 'seen for the last 2 hours'. Below this is a search bar and a list of SSIDs. Two modal windows are open for editing containment settings. The first modal, 'Edit SSID containment', shows a list of SSIDs on the left and a 'Select a containment type' section with four buttons: 'Whitelist', 'Contain', 'Alert', and 'Uncontain'. The second modal, 'Edit Broadcast MAC containment', also shows a list of MAC addresses on the left and the same 'Select a containment type' section. Both modals have 'Confirm' and 'Cancel' buttons at the bottom right. At the bottom of the interface, there's a '10 results' indicator and a list of specific rogue SSIDs with their signal strengths.

Air Marshal

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

24 rogue SSIDs ¹ seen for the last 2 hours ▼

Edit ▼ Search...

☐ **SSID ▲** **Edit SSID containment**

☐ AXE BL testing

☐ IT Test WiFi

☐ j-bond-2-owe

☐ j-bond-3-sae

☐ j-bond-5-1x

☐ j-bond-8-owe-8 (and 2 others) ago ago LAN

☐ j-p1-bond-2-owe **Edit Broadcast MAC containment**

☐ j-p1-bond-3-sae

☐ j-p1-bond-4-sae

☐ Meraki Setup

Select a containment type

Whitelist Contain Alert Uncontain

Confirm Cancel

10 ▼ results

Confirm Cancel

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

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.

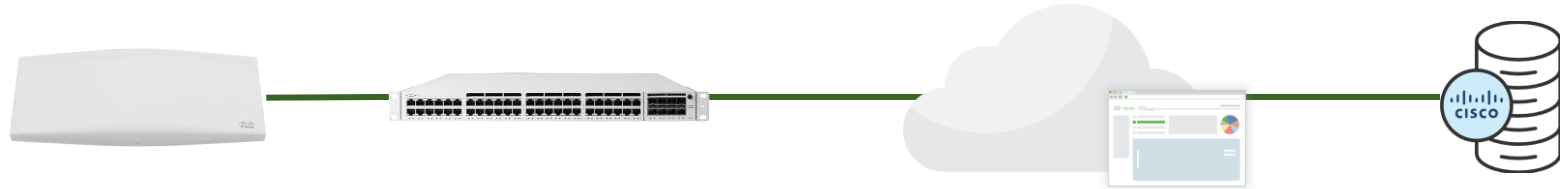
Add a match

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

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

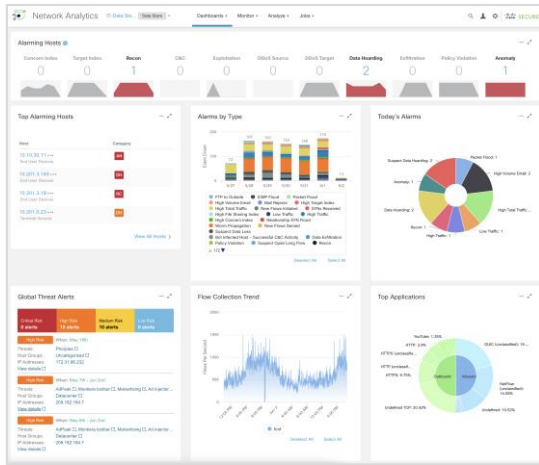
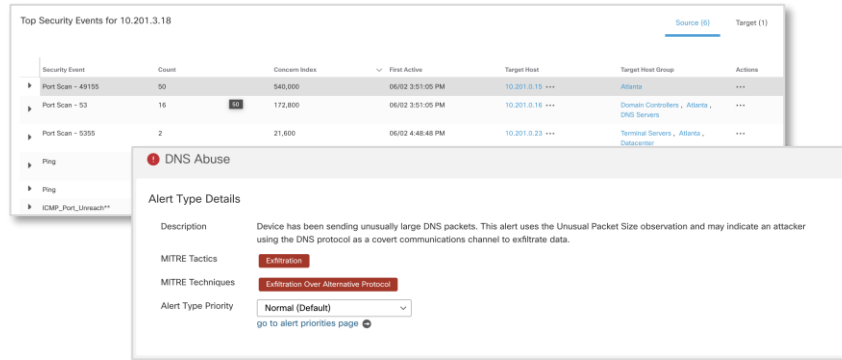
Network as a Sensor and Enforcer



Netflow

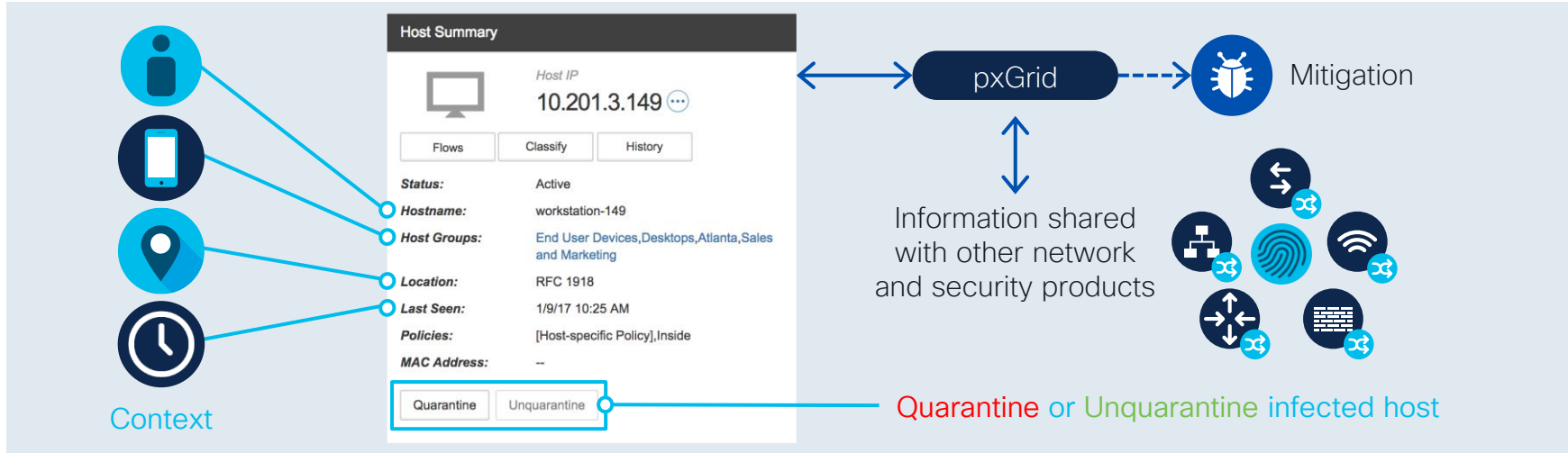


Malware detection and
cryptographic compliance
on Secure Network Analytics



Network as an Enforcer

Rapid Threat Containment



Identity Services Engine



Secure Network Analytics
Management Console

DNS Layer Protection

Cisco Umbrella

- Native integration with Cisco Umbrella to provide DNS layer protection and filtering

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Select an Umbrella policy to apply. ⓘ

Cisco Umbrella account

Umbrella key

Umbrella secret

Store your secret securely. We won't display it again after you save these changes.

Policy Name
Default Policy

Applied to All Identities

Security Setting Applied: Default Settings
Command and Control Callbacks, Malware, Phishing Attacks, plus 1 more will be blocked.
No integration is enabled.
[Edit](#) [Disable](#)

Content Setting Applied: Default Settings
No categories will be blocked.
[Edit](#) [Disable](#)

No Application Settings Applied
[Enable](#)

2 Destination Lists Enforced
1 Block List
1 Allow List
[Edit](#)

File Analysis Not Enabled
File Inspection Not Enabled
[Edit](#)

Custom Block Page Applied
Default Settings
[Edit](#)

Advanced Settings

☒ **Enable Intelligent Proxy**
Gain visibility into threats, c

☐ **SSL Decryption**
Enabling SSL decryption
Turning on SSL decryption

☐ **Enforce SafeSearch**
Enforce SafeSearch for queries

ALLOW-ONLY MODE

☒ **Allow-Only Mode**
In this mode, access to internet

LOGGING

☒ **Log All Requests**

☐ **Log Only Security Events**
Log and report on only those r

☐ **Don't Log Any Requests**
Note: No requests will be reported for intelligence purposes.

Security Settings
Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

Select Setting

Categories To Block [EDIT](#)

- ☒ **Malware**
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.
- ☒ **Newly Seen Domains**
Domains that have become active very recently. These are often used in new attacks.
- ☒ **Command and Control Callbacks**
Prevent compromised devices from communicating with attackers' infrastructure.
- ☒ **Phishing Attacks**
Fraudulent websites that aim to trick users into handing over personal or financial information.
- ☒ **Dynamic DNS**
Block sites that are hosting dynamic DNS content.
- ☒ **Potentially Harmful Domains**
Domains that exhibit suspicious behavior and may be part of an attack.
- ☒ **DNS Tunneling VPN**
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
- ☒ **Cryptomining**
Cryptomining allows organizations to control cryptomining access to mining pools and web miners.

[CANCEL](#) [SET & RETURN](#)



Securing the Wireless Network



Secure the
Air



Secure the
Devices



Secure the
Network





Thank you



#CiscoLiveAPJC

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



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



Continue your education



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

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC