

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, triangular rays in various shades of blue and cyan, creating a sunburst effect that spreads across the right half of the image.

cisco *Live!*

Let's go

#CiscoLiveAPJC



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!*

#CiscoLiveAPJC

Cisco Webex App

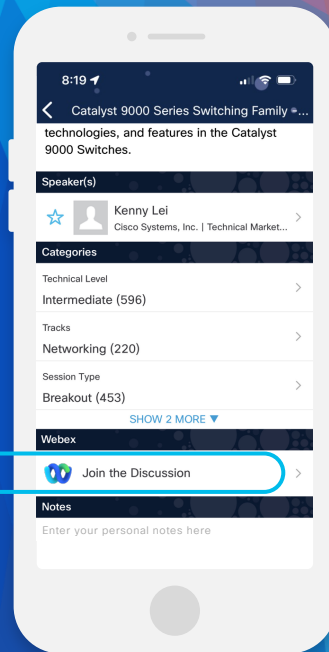
Questions?

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 December 22, 2023.



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

Agenda

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



Wireless Security Fundamentals

“For Carlsberg, networking and security operations are ultimately about the same thing...
ensuring the beer keeps flowing.”

Tal Arad, CISO and Head of Technology, Carlsberg

“Networking and security teams tasked to converge, collaborate”, NetworkWorld

Securing the Wireless Network



Secure the
Air



Secure the
Devices



Secure the
Network

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

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

FYI



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)

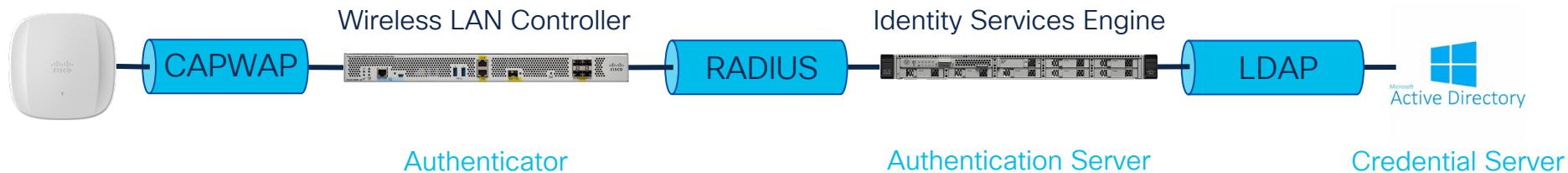
802.11 Fundamentals

Authentication



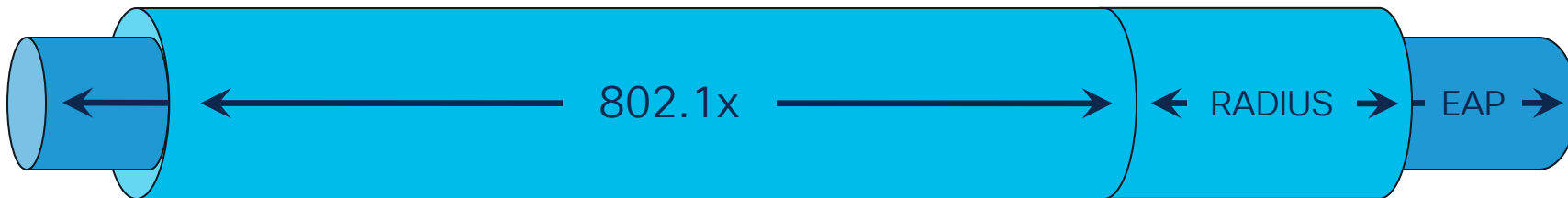
802.11 Fundamentals

- Authentication



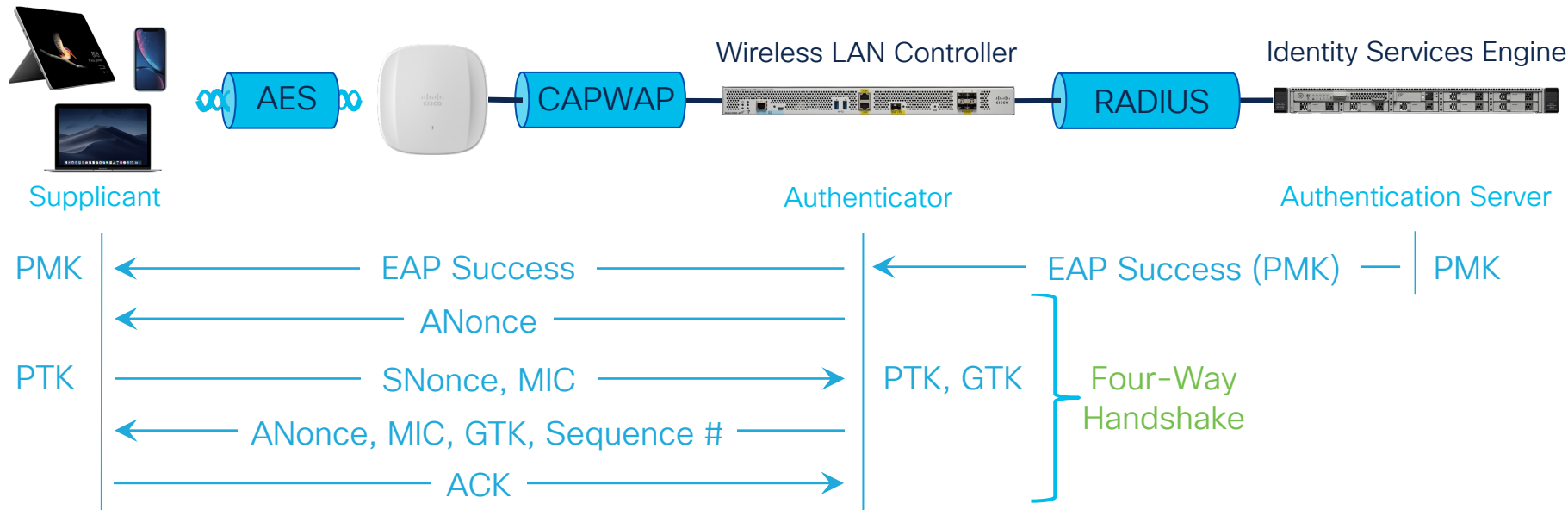
802.11 Fundamentals

- Authentication



802.11 Fundamentals

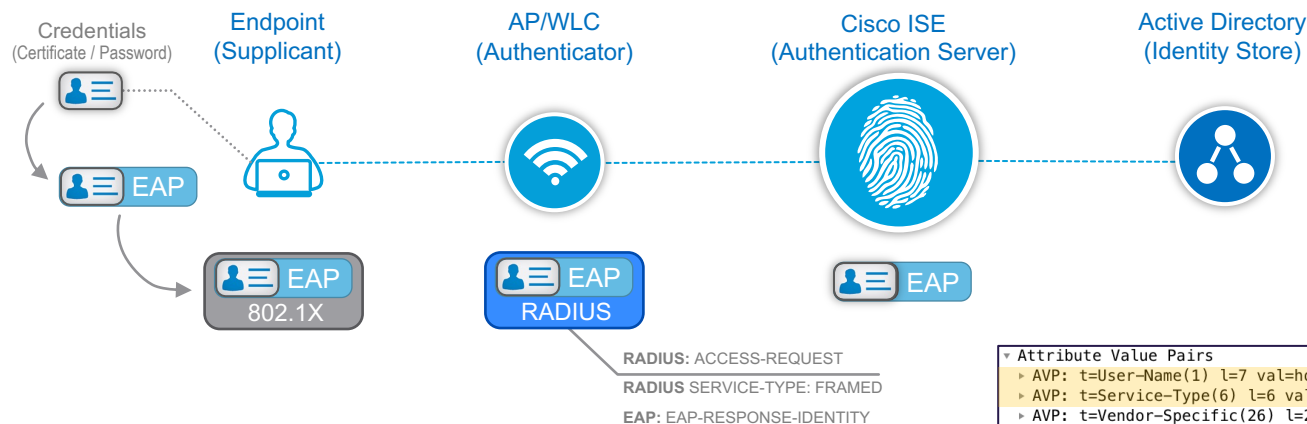
Encryption



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

802.1X

FYI



EAP: Extensible Authentication Protocol

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

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

EAP-PEAP-MSCHAPv2 and EAP-TLS



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

EAP-PEAP-MSCHAPv2

Server Identity Validation

- Signed by trusted CA
- Belongs to allowed server

Trusted root CA



Tunnel

Client Identity Validation

- Valid credential
- Additional checks

EAP-TLS

Server Identity Validation

- Signed by trusted CA
- Belongs to allowed server

Trusted root CA

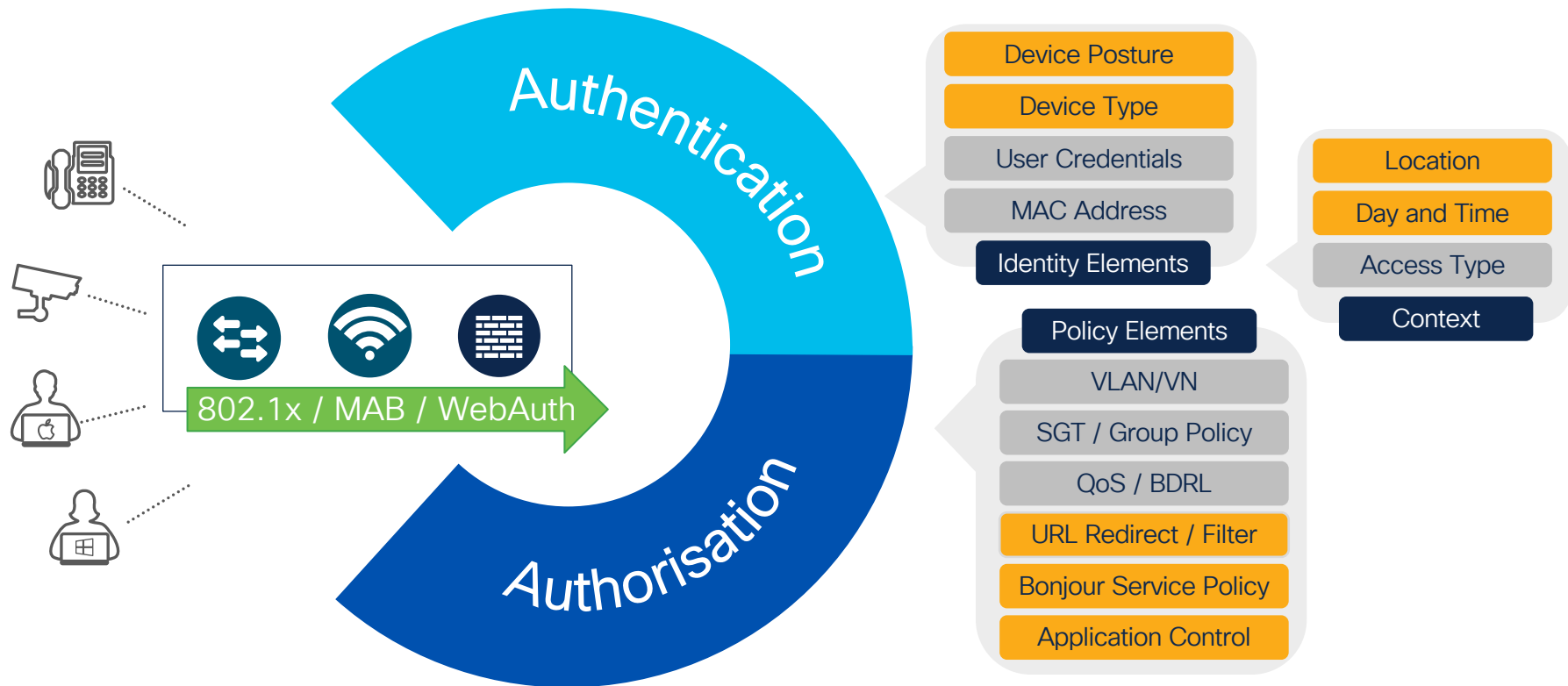


Trusted root CA

Client Identity Validation

- Signed by trusted CA
- Additional checks

Authentication and Authorisation



Authorisation

Network Segmentation

Static VLAN Assignment

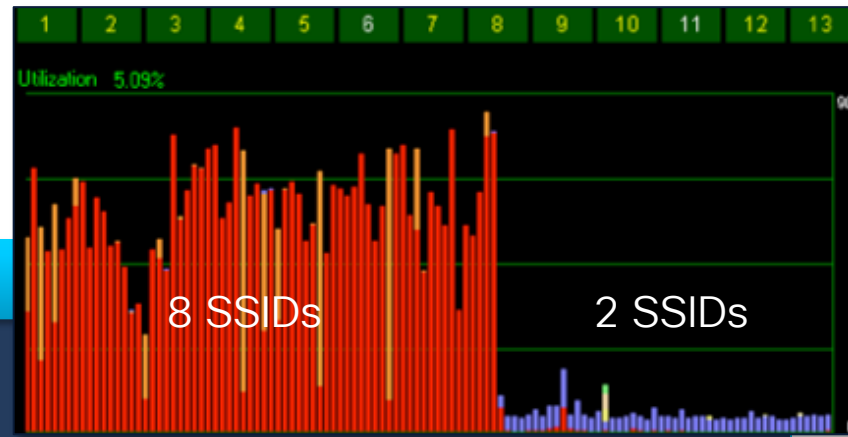
- VLAN based on SSID
- VLAN segregation based on security policy

Dynamic VLAN Assignment

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

TrustSec / Group Based Policy / Software Defined Access

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

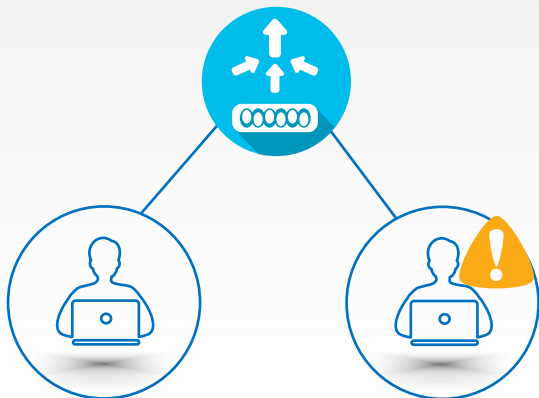


Authorization Options



Named ACL

Named ACL

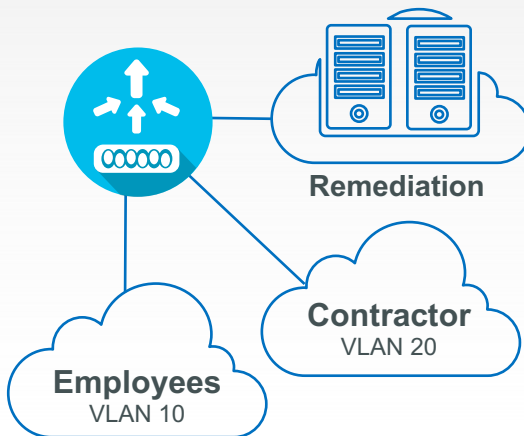


Healthy
permit ip any any

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

VLANs

Dynamic VLAN Assignments



Per user / Per group / Per MAC

SGTs or UDN/WPN ID

User Defined Network
or Scalable Group Tags



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

Dynamic VLAN

FYI

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"/>	✕

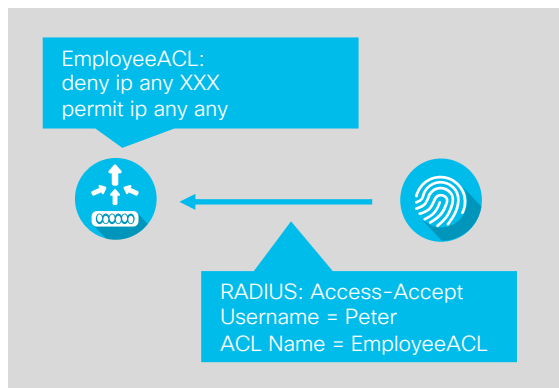
[Add a Named VLAN](#)

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

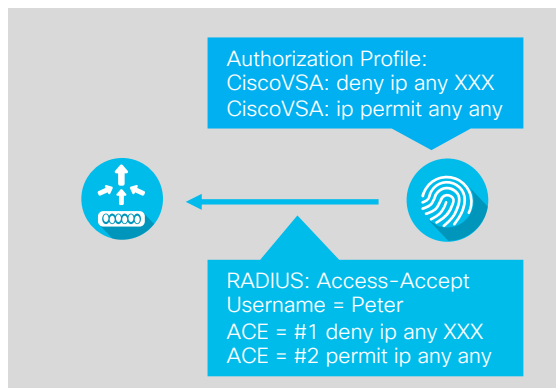
RADIUS Enforced ACLs



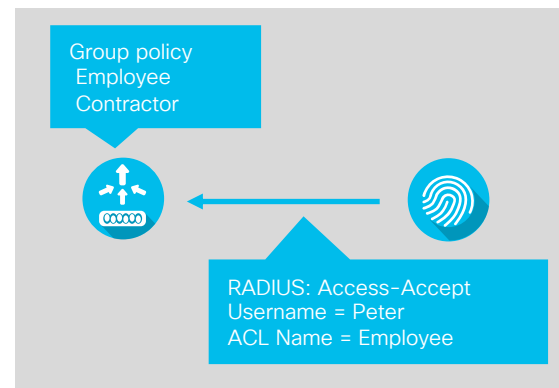
Named ACL



Per-User ACL



Group policy



Additional 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.

Secure Fast Roaming Challenges



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

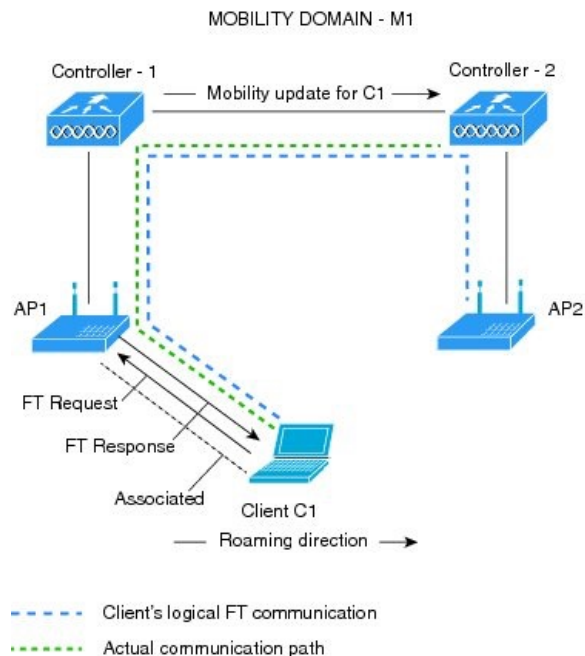
Secure Fast Roaming

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

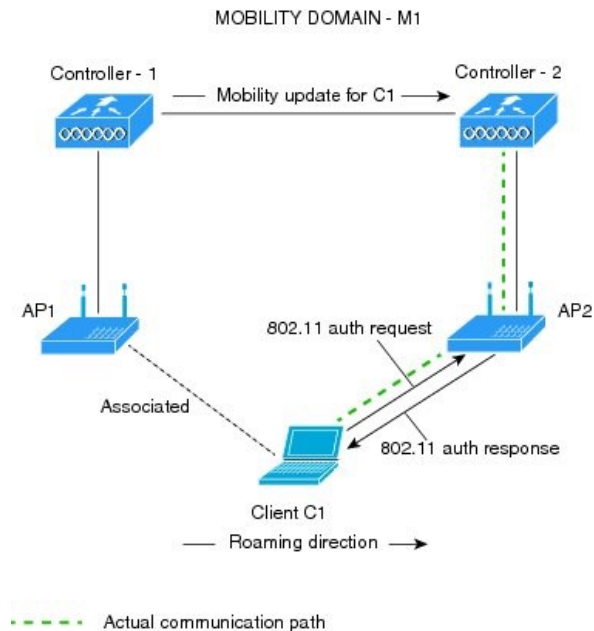


- Client channel scanning and AP selection
 - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
 - 802.11v BSS Transition
- Re-authentication of client device and re-keying
 - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

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

Fast Transition

Status

Over the DS ☐

Reassociation Timeout

WPA2/WPA3 Encryption

AES(CCMP128)	☒	CCMP256	☐
GCMP128	☐	GCMP256	☐

Protected Management Frame

PMF

Auth Key Mgmt

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

MPSK Configuration

WPA3 802.11r Fast Roaming Support



- Network administrators can now configure fast roaming on the network to work with most WPA3 encryption options.
- Supports Fast Transition with the following WPA3 modes:
 - WPA3 Personal
 - WPA3 Only
 - WPA3 Transition Mode
 - WPA3 Enterprise
 - WPA3 Only

The screenshot shows a configuration page for WPA3. It includes sections for 'WPA encryption', '802.11r', '802.11w', and 'Mandatory DHCP'. The '802.11r' section is highlighted with a green box and contains a dropdown menu set to 'WPA3 only' and three radio button options: 'Enabled' (selected), 'Adaptive', and 'Disabled'. The '802.11w' section has three radio button options: 'Enabled (allow unsupported clients)', 'Required (reject unsupported clients)' (selected), and 'Disabled (never use)'. The 'Mandatory DHCP' section has two buttons: 'Enabled' and 'Disabled'.



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](#)

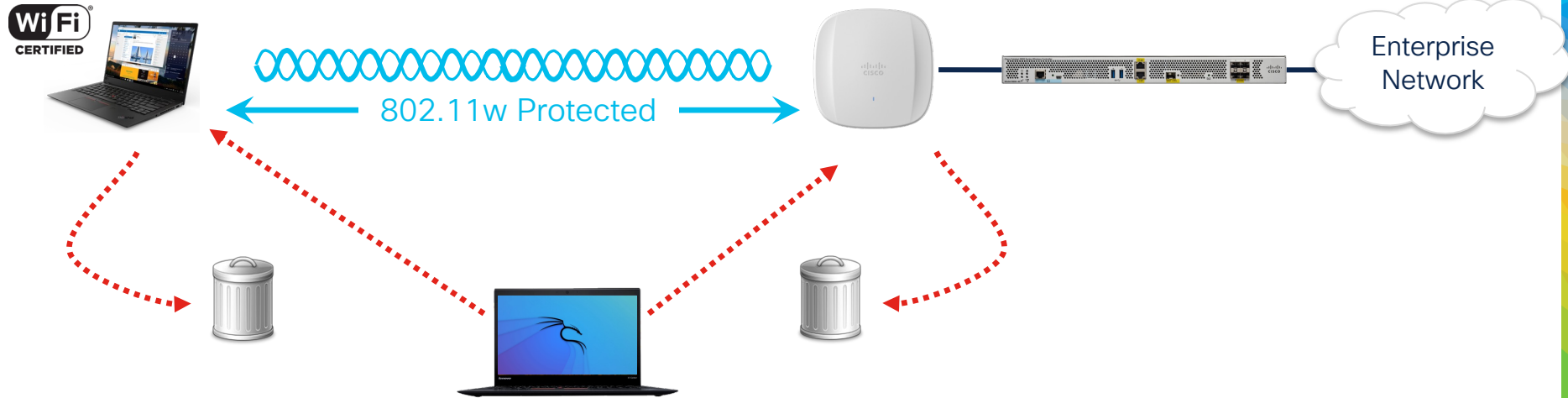
- This was an industry wide issue
 - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
 - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection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

Kr00k Vulnerability

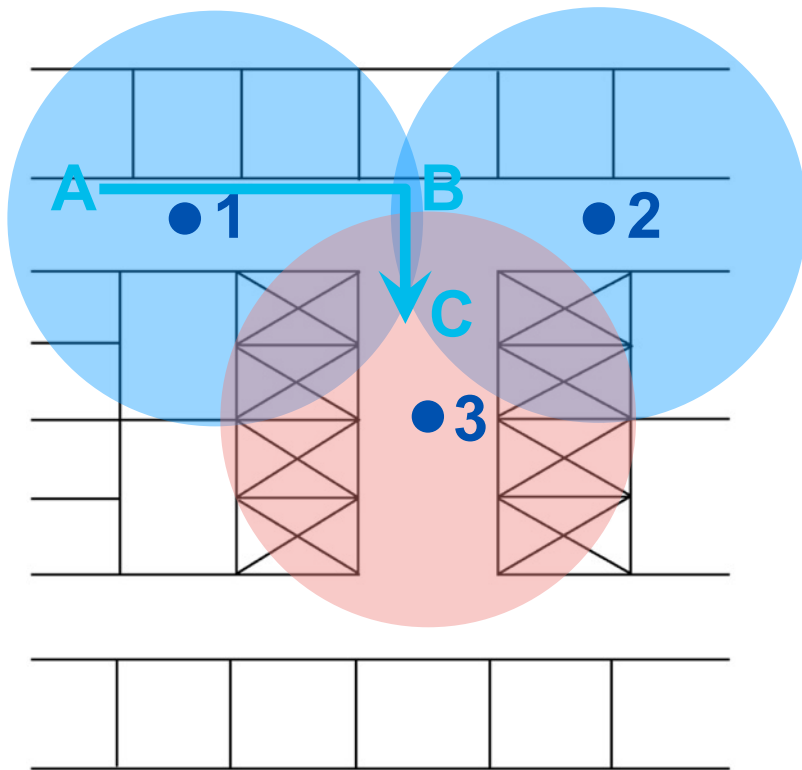
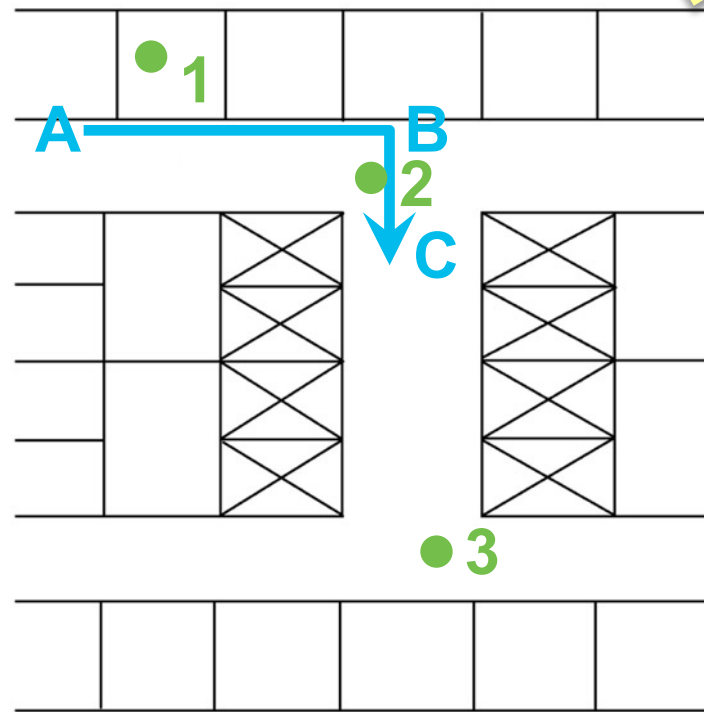


- On February 26th, 2020, researchers Štefan Svorencík and Robert Lipovsky [disclosed a vulnerability in the packet processing of certain Wi-Fi chipsets](#)
- This vulnerability could allow an unauthenticated, adjacent attacker to decrypt Wi-Fi frames without the knowledge of the PTK
- After an affected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



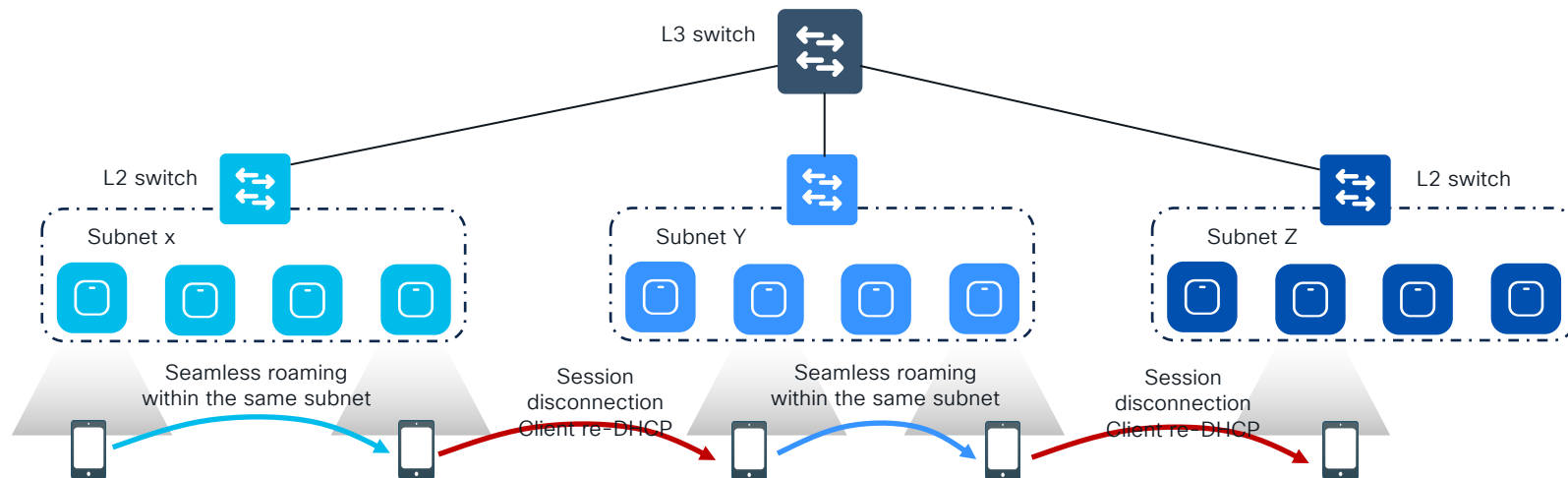
AP Placement and Roaming Optimization



Seamless Roaming at Scale

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

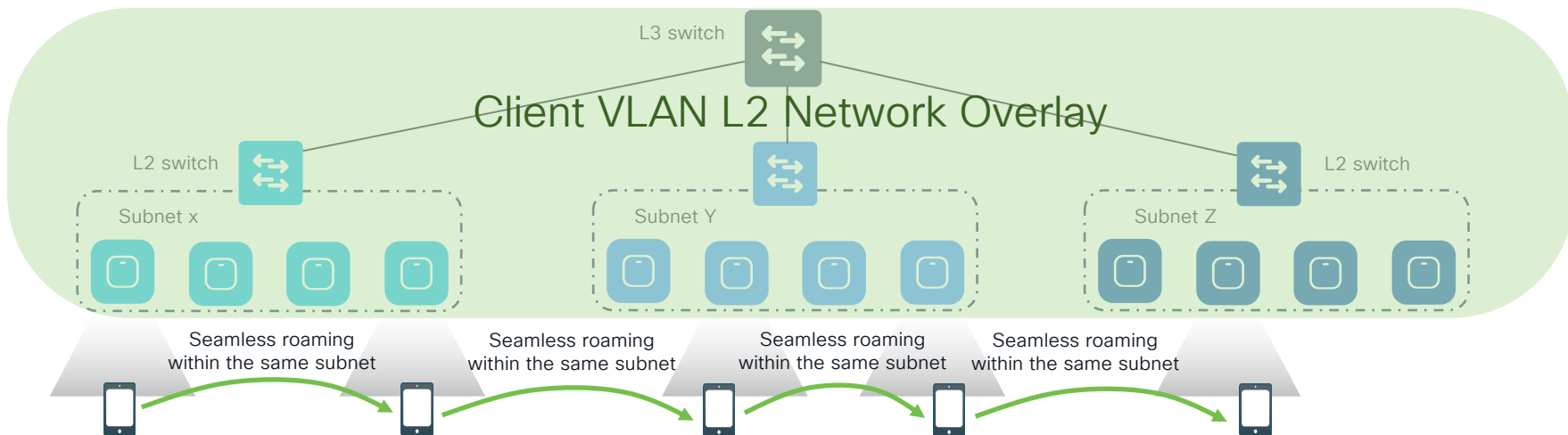
Large broadcast domains do not scale and is counter to networking best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

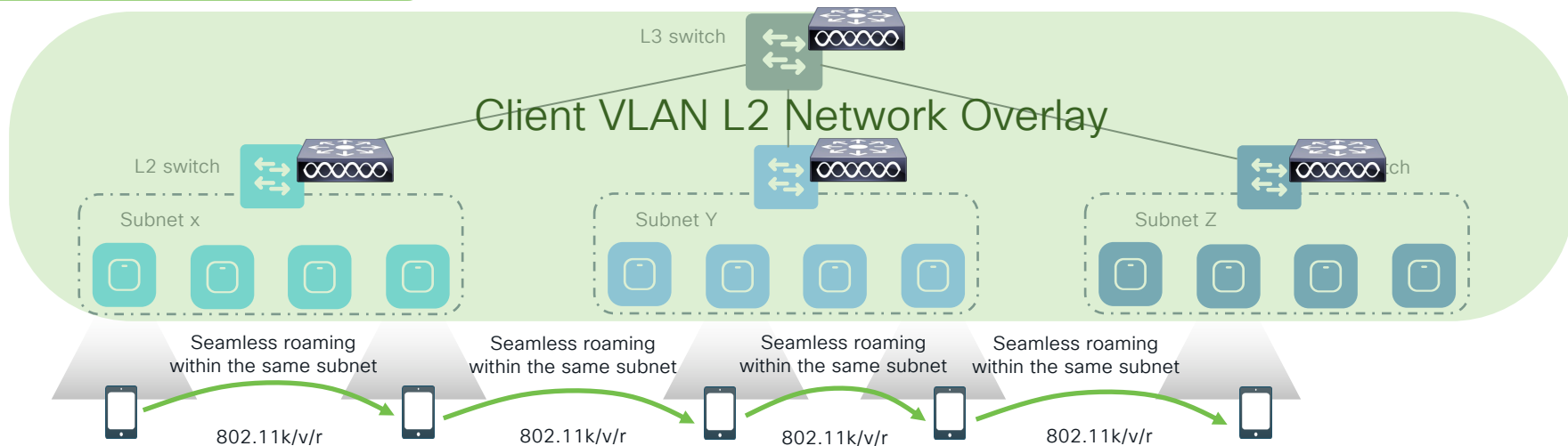
A data termination point is required to roam across L3 boundaries



Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

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



On-Prem and Cloud Identity



On-Prem Identity



802.1x, Network Access

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



Cloud Identity

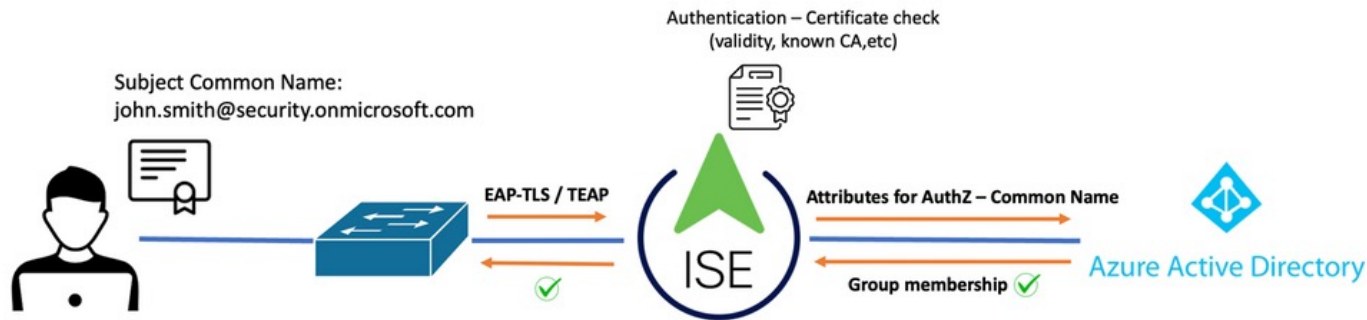
VPN, Application Access



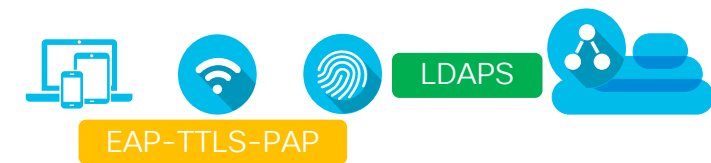
SAMLv2, OpenID Connect



Cloud Identity with EAP-TLS



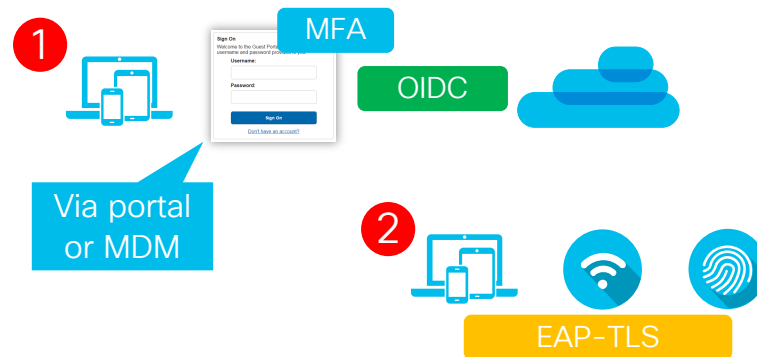
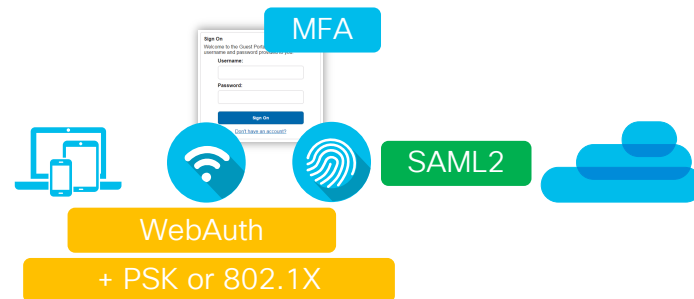
Utilise Cloud Identity for Network Access



TTLS - Tunneled TLS



ROPC - Resource Owner Password Credentials



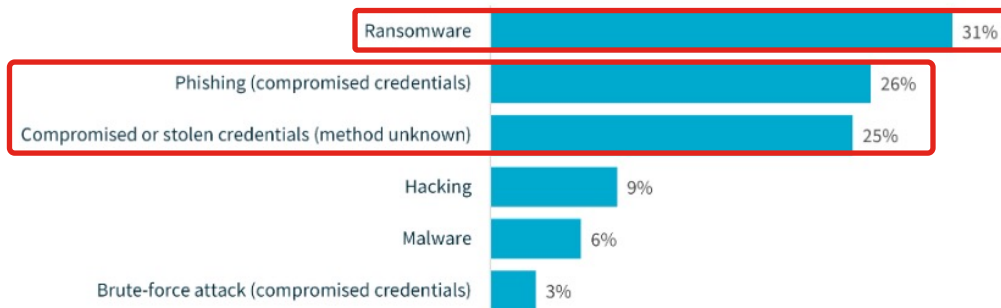
Multi-Factor Authentication



Zero Trust

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

Cyber incident breakdown



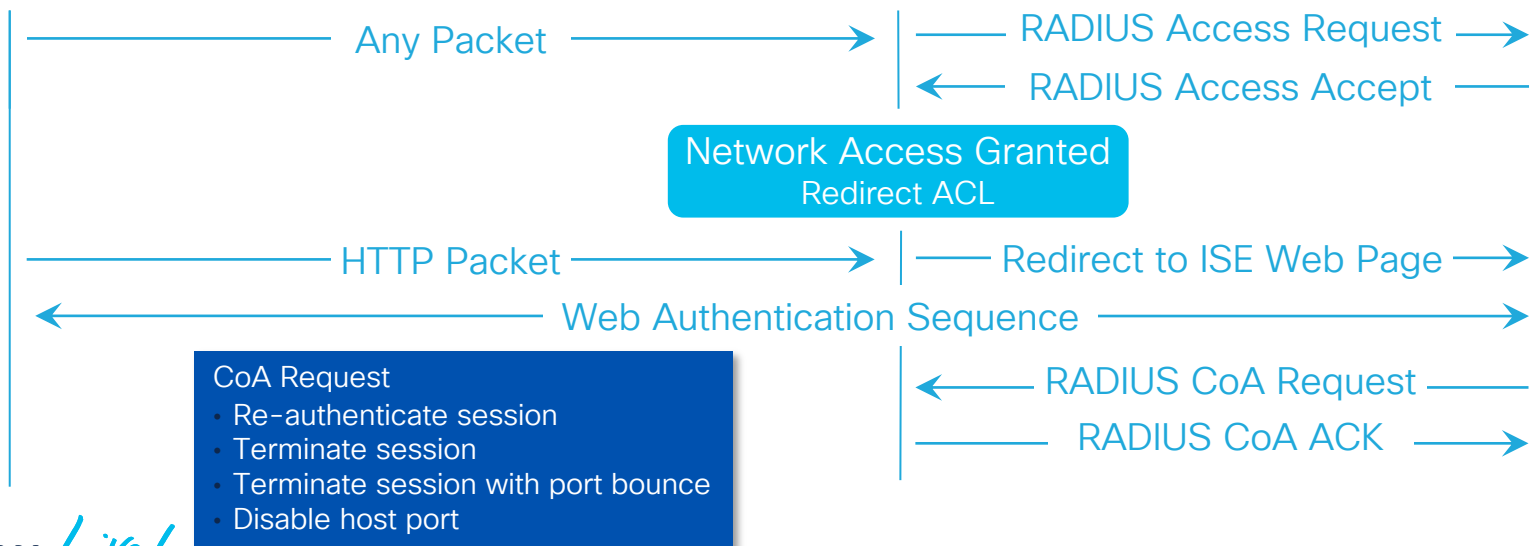
- Ransomware

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

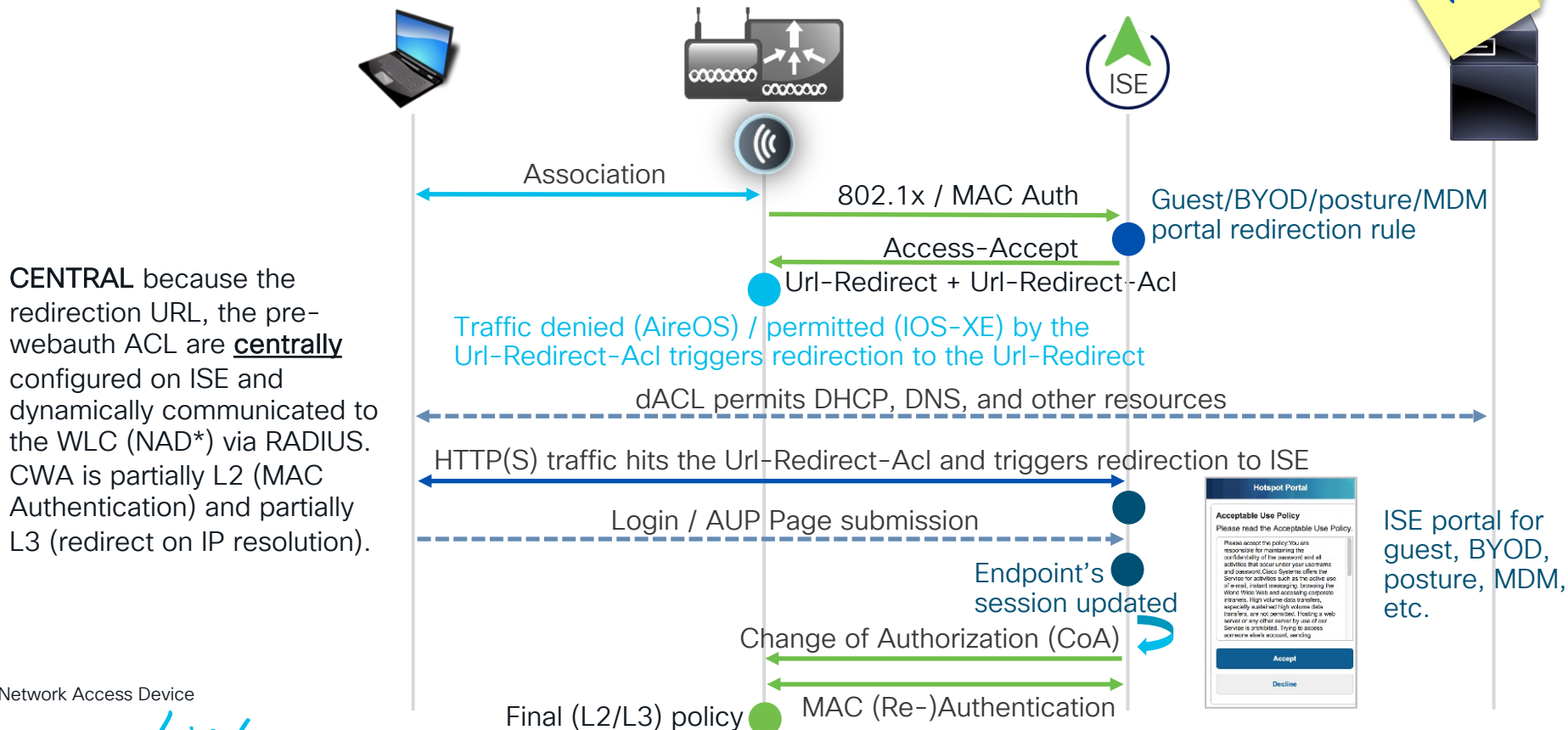
- Phishing and compromised or stolen credentials
 - Username/Password
 - Digital Certificates

Central Web Authentication

URL Redirect



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: *

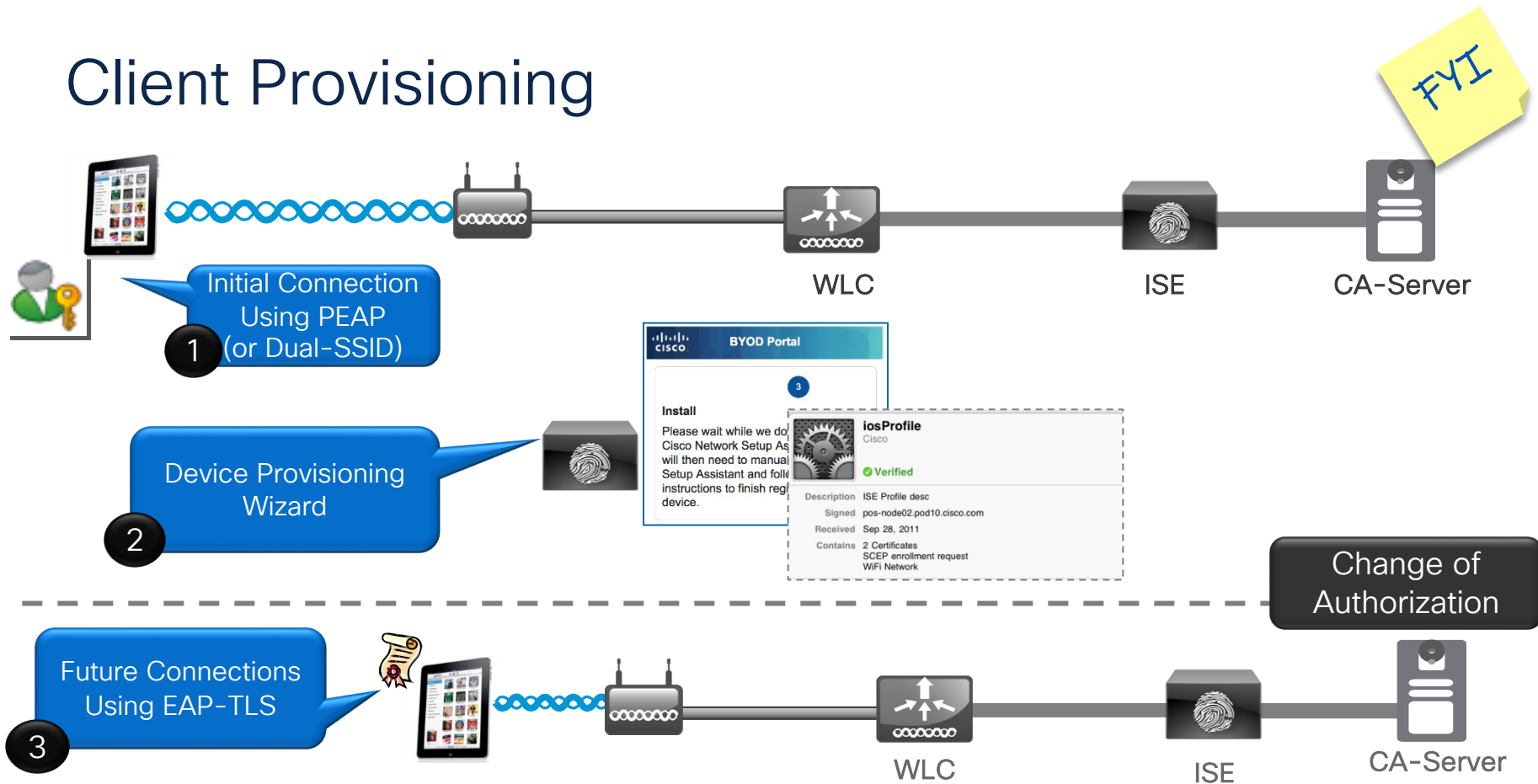
Device ID: *

Description:

Submit **Cancel**

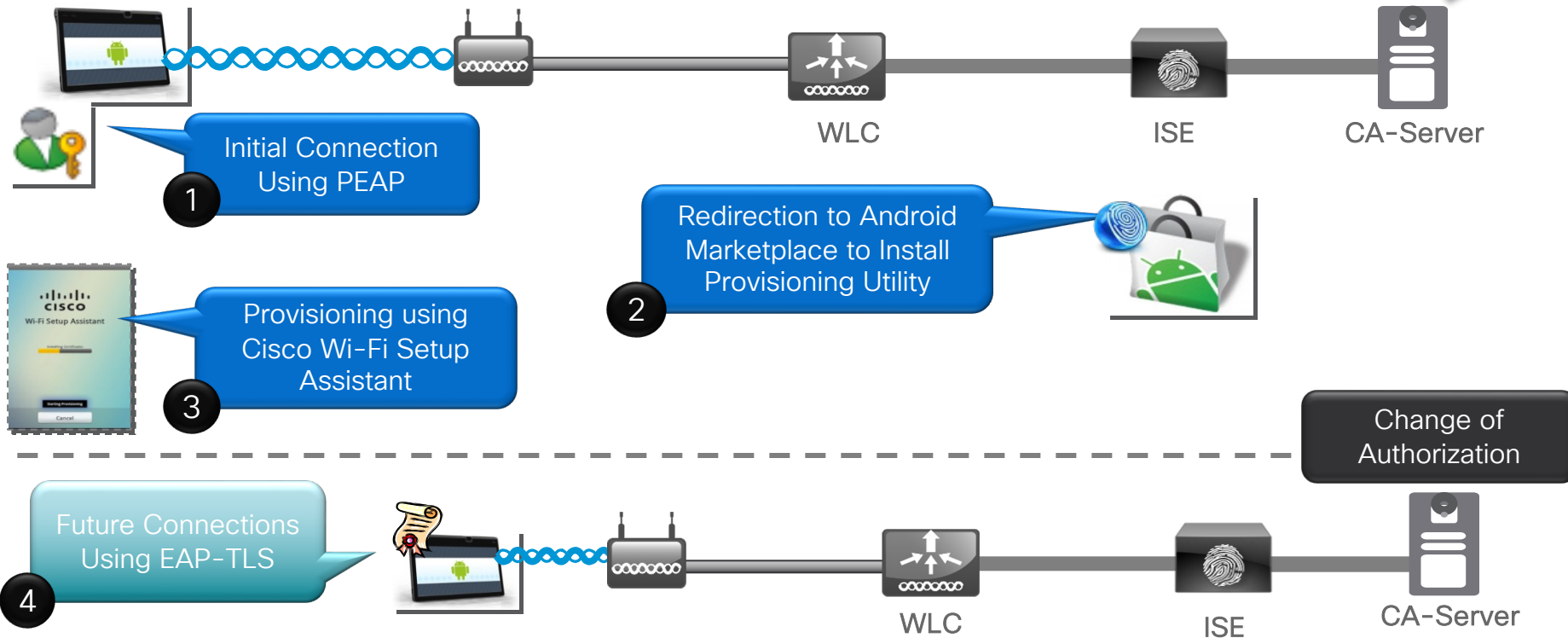
3
Devices Can be Self-Registered, Up to an Administrator Defined Limit

Client Provisioning



Android Device Provisioning

FYI



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:

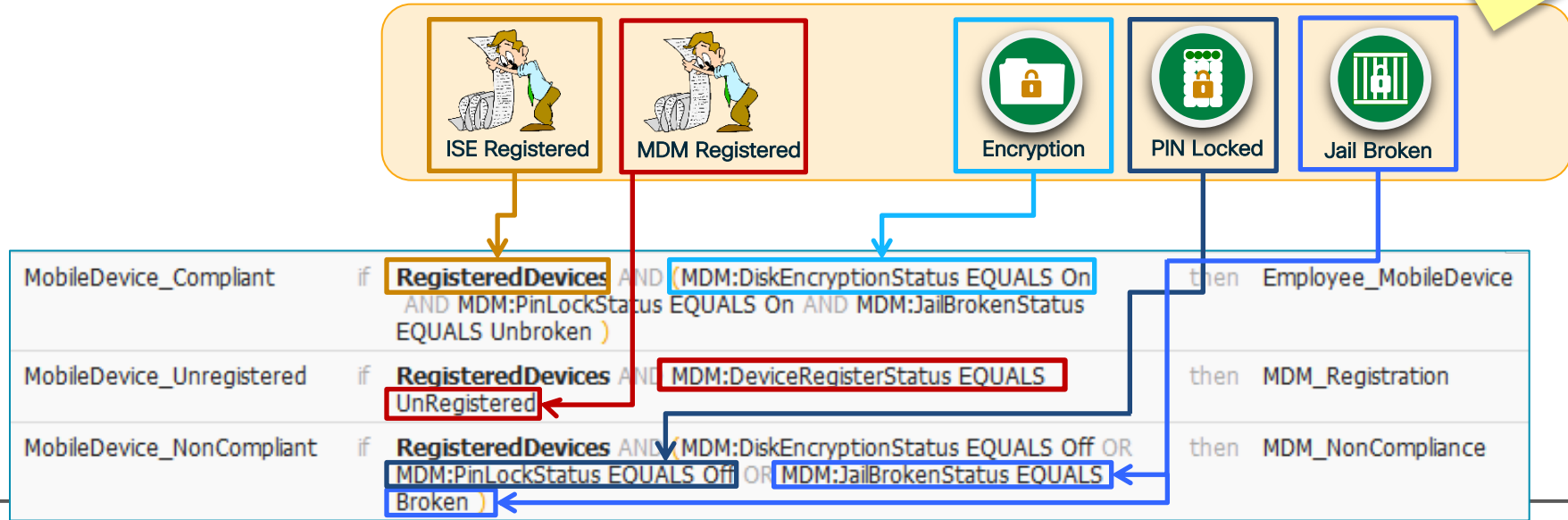
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.

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



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

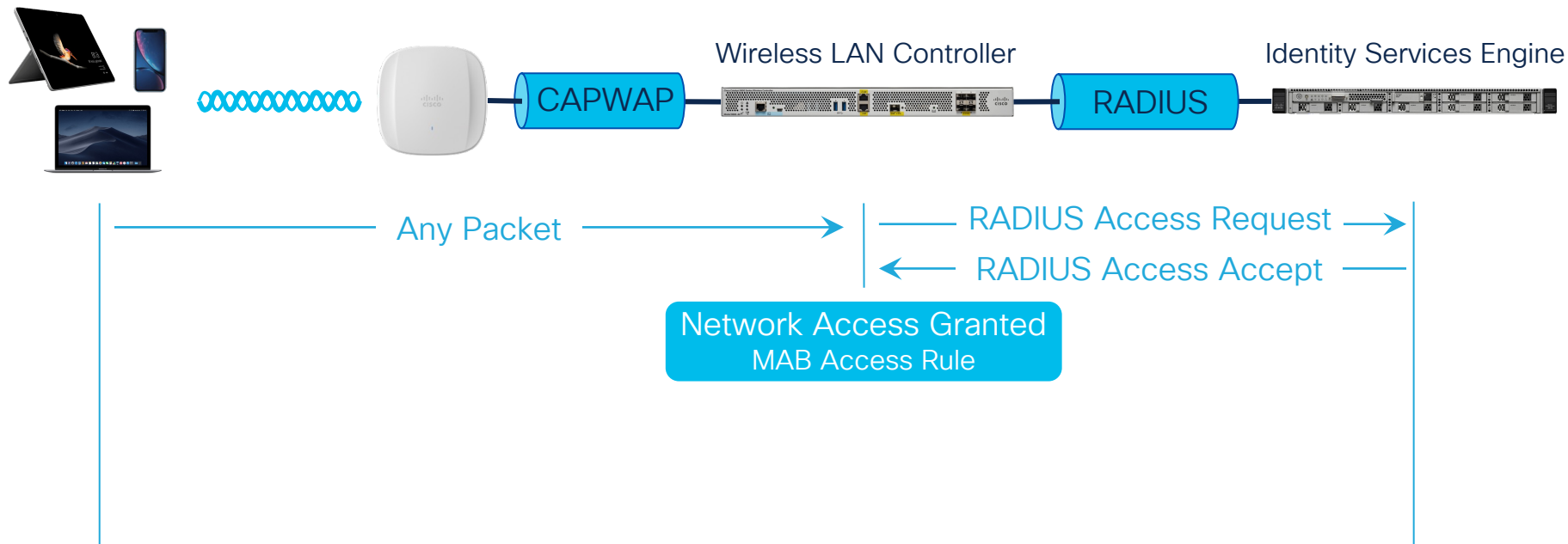


Apple Devices

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

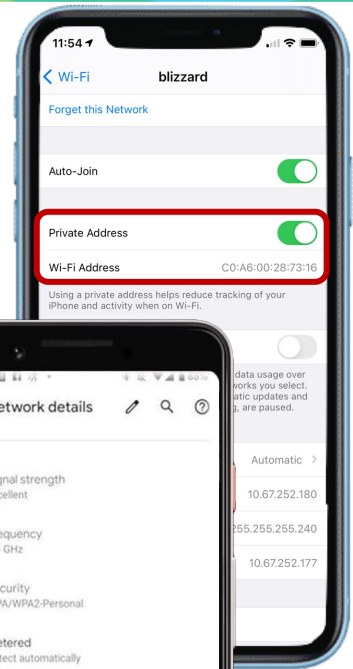
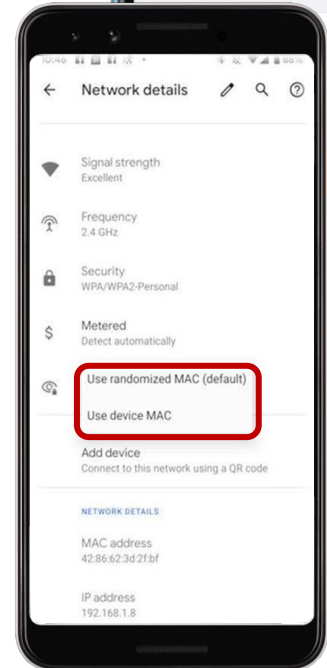
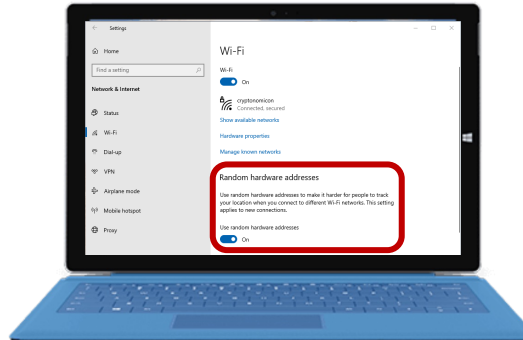
Central Web Authentication

MAC Authentication Bypass



Random MAC and Private Addresses

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



Detailed Implementation

FYI

	Windows 10+	Android 10+	iOS 14+, iPadOS 14+, watchOS 7+
Randomization enabled by default	No	Yes	Yes
Same random MAC used for subsequent connection	Yes	Yes	Yes
Randomization saved between device reboot	Yes	Yes	Yes
Random MAC saved when Wi-Fi profile recreated	No	Yes	Yes
Randomization per day and/or per association	Optional	Optional (Android 11 Developer Mode)	No
Randomization enabled upon upgrade for existing Wi-Fi profile	No	No	Yes
Can be enabled/disabled globally	Yes	No	No
API to control randomization exists	Unknown	Yes (Android 11+)	Yes
Randomization saved between factory reset	No	No	Unknown

Random MAC Implications



Profiling



BYOD



Whitelisting



MDM Flow



Guest



Location lookup



User Defined Network



Endpoint Analytics



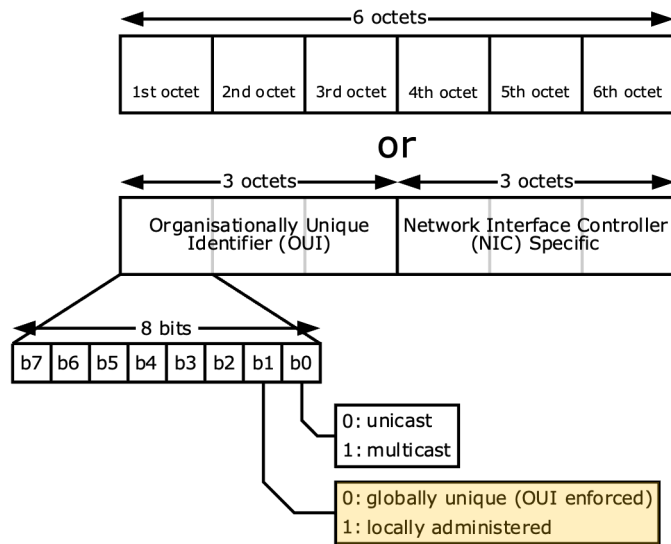
Forensics



Quarantine

Detecting Random MAC Addresses

FYI



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

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

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

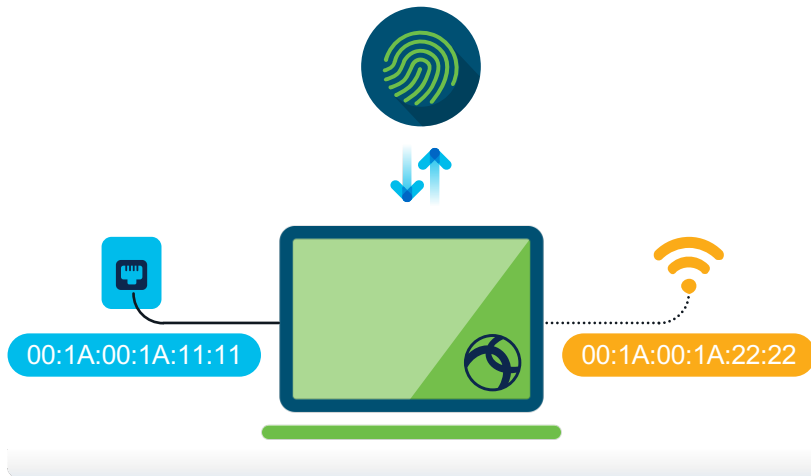
AE-83-37-55-A7-22

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>

Unique Device Identifier

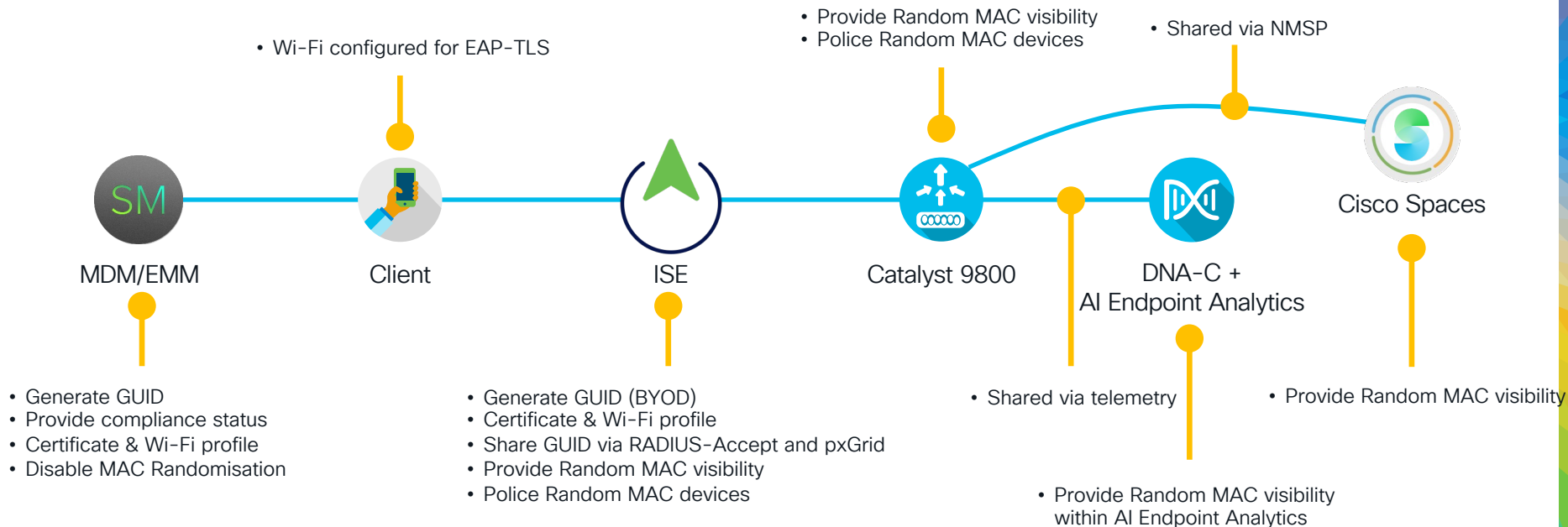


UDID	MAC Address(s)	Compliance
01669b65...05ee93	00:1a:00:1a:11:11 00:1a:00:1a:22:22	✓

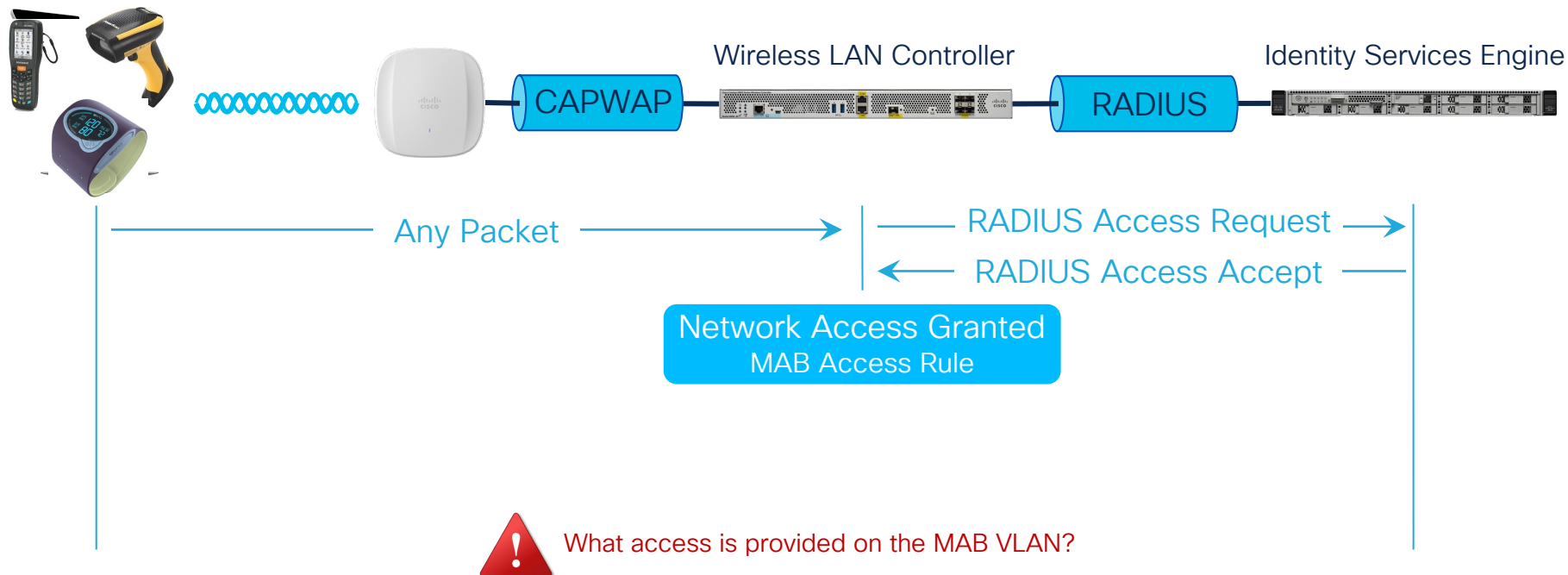


- In open seating environments with docking stations for PCs and Ethernet dongles for Apple MacBooks, lead to a different challenge
 - The same MAC address will be used by different users
- ISE can perform authorization for managed end-points leveraging the laptop UDID (Unique Device Identifier) instead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

Globally Unique Identifier



MAC Authentication Bypass



WPA Personal

Pre-Shared Key

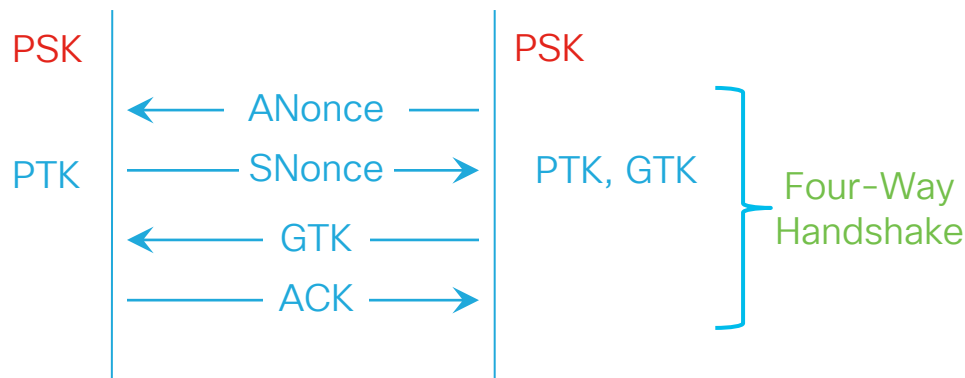


WPA Personal

Pre-Shared Key

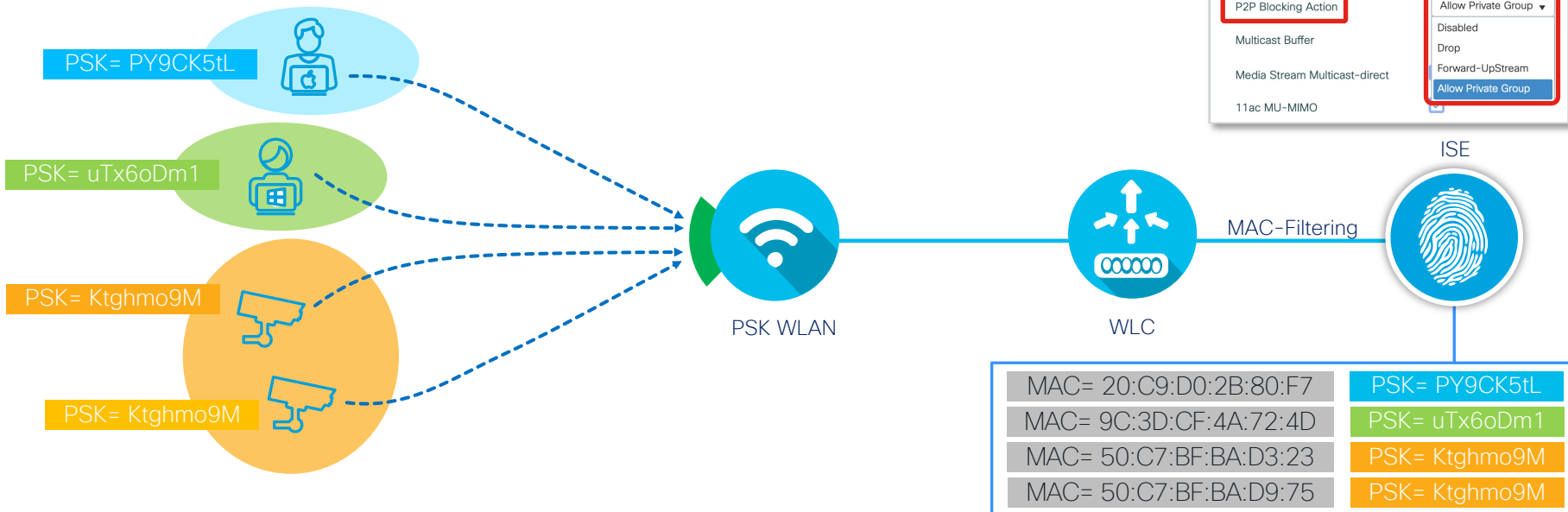


- Offline Attacks
 - Dictionary
 - Rainbow Table
- Strong Passwords Matter



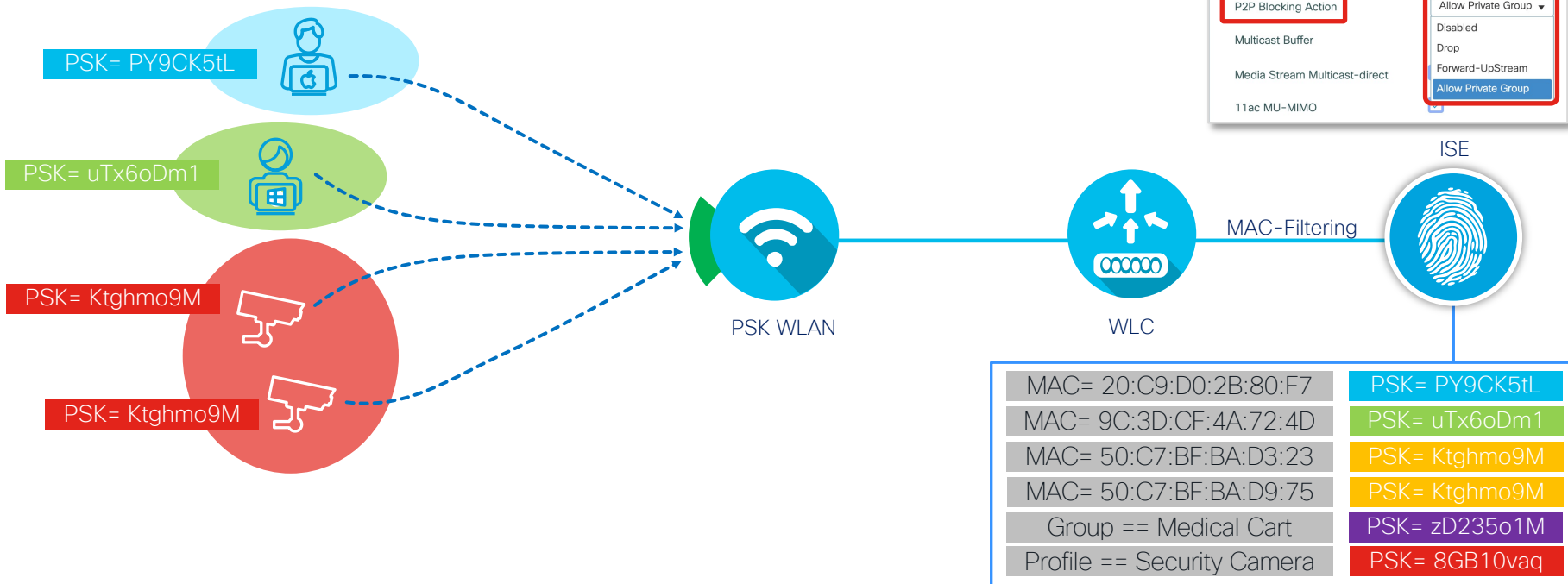
$$PTK = \text{SHA}(\text{PSK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$$

Identity PSK



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

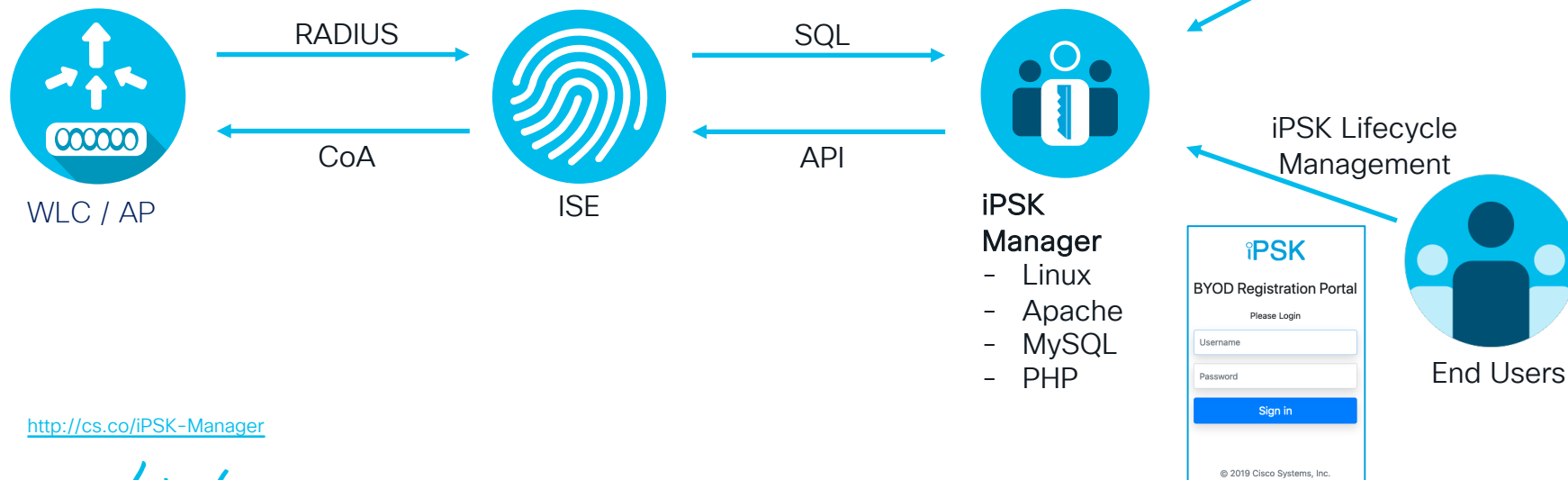
Identity PSK



<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsec-with-ci.html>

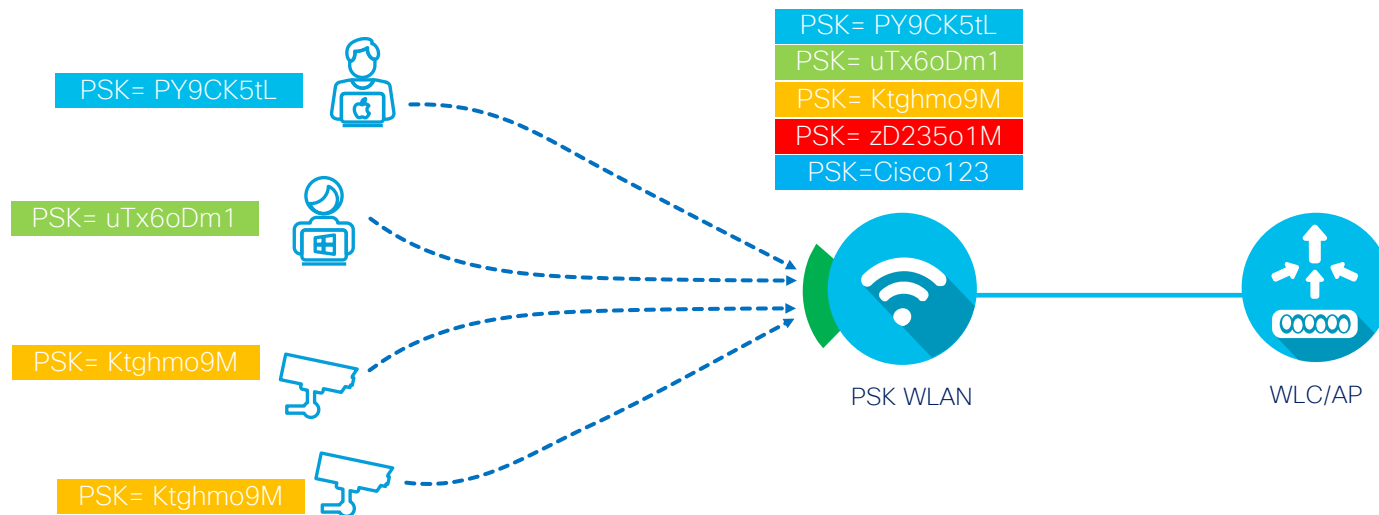
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSec_with_RADIUS_Authentication

iPSK Manager

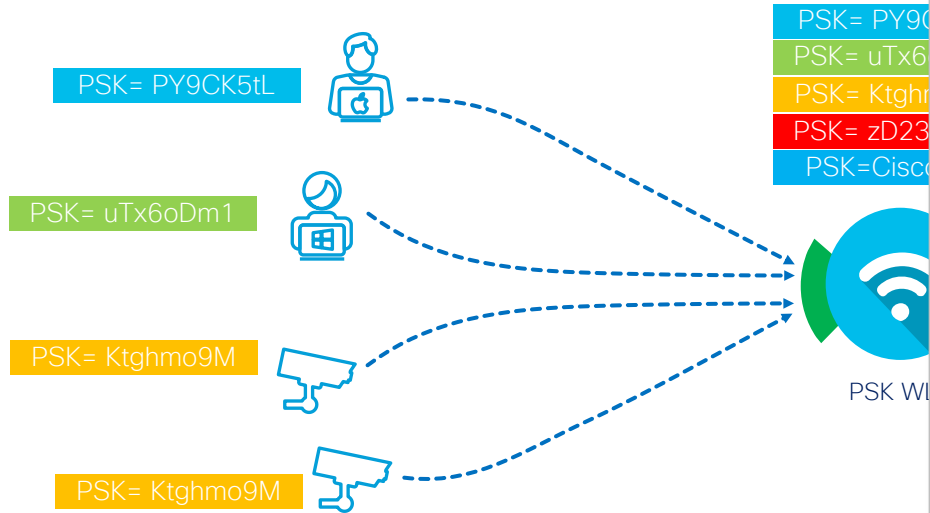


<http://cs.co/iPSK-Manager>

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 ☐	OSN 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 ☐	CCMK ⚠ ☐
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

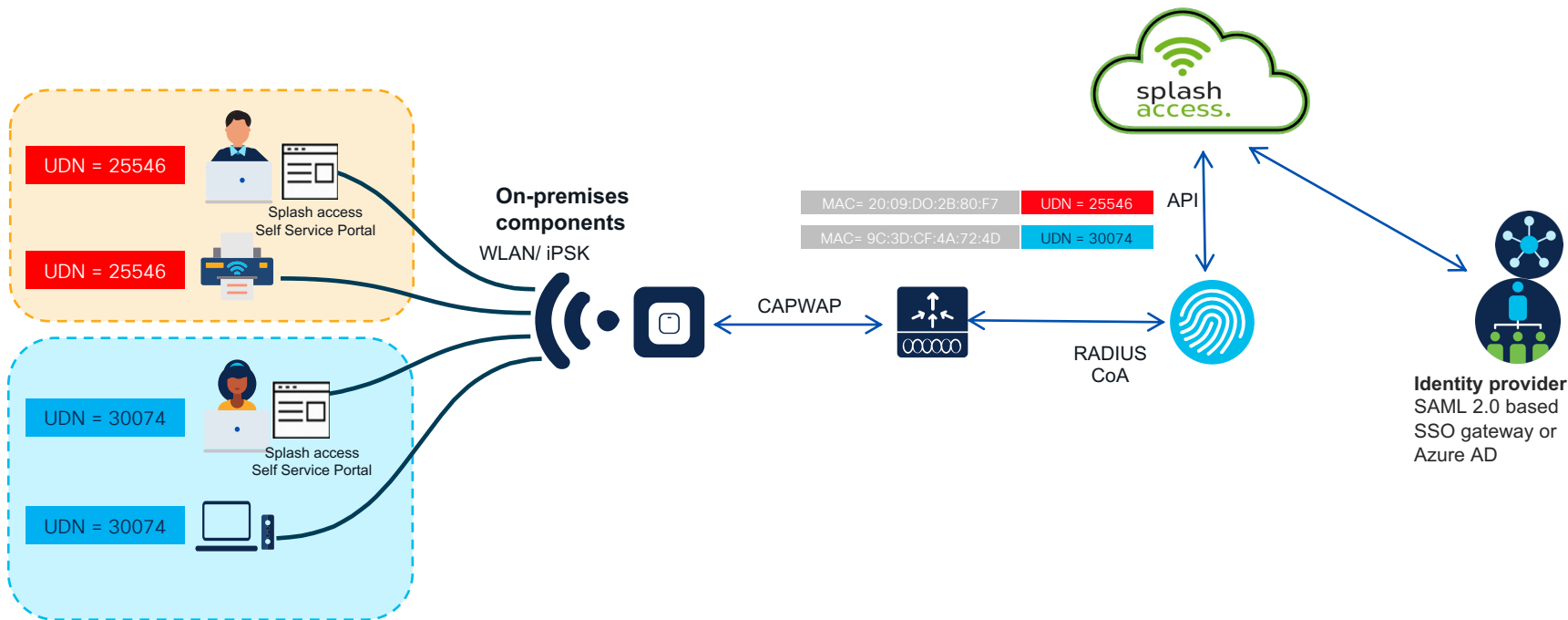
FYI

CISCO *Live!*

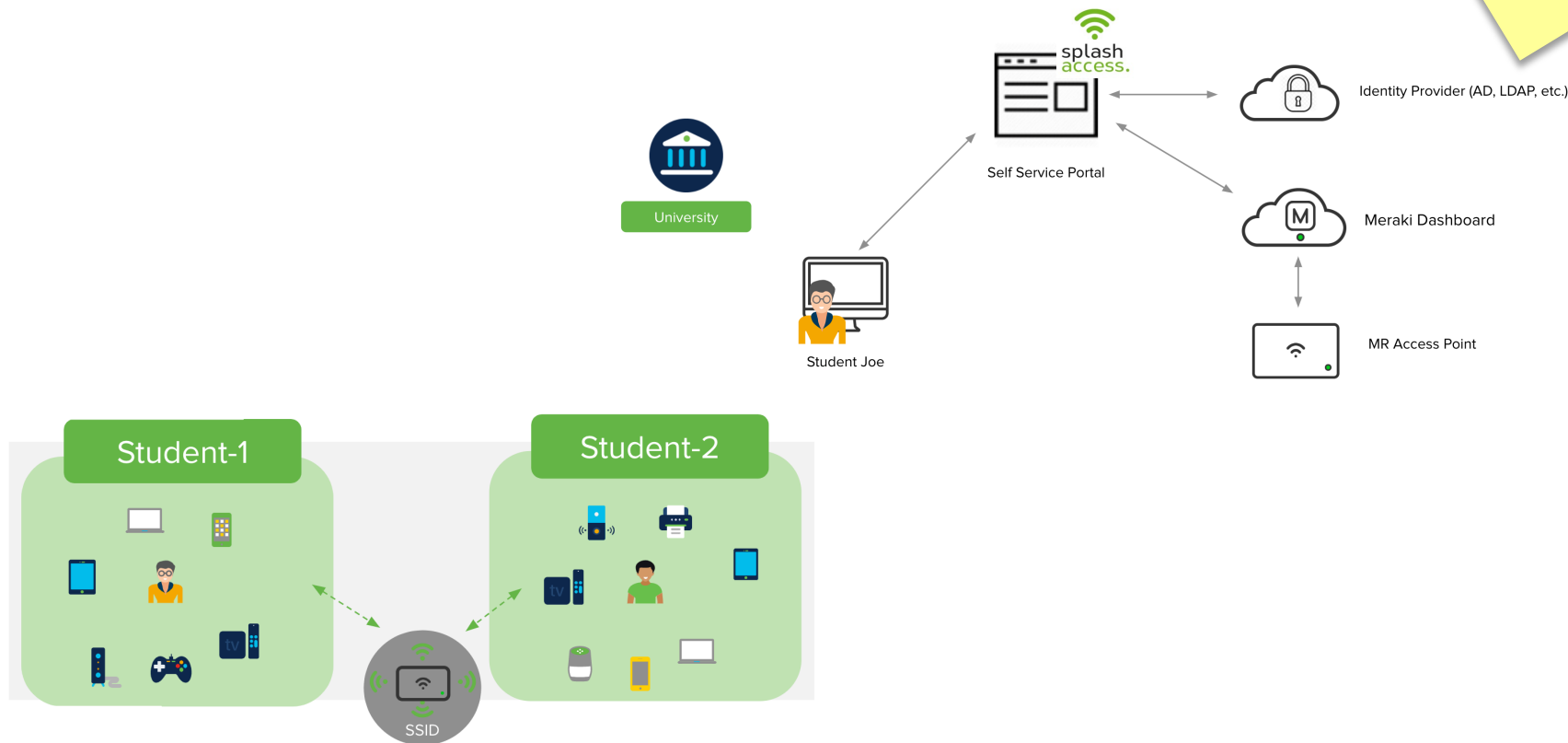


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Defined Network



Wi-Fi Personal Network



Simultaneous Authentication of Equals

WPA3

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

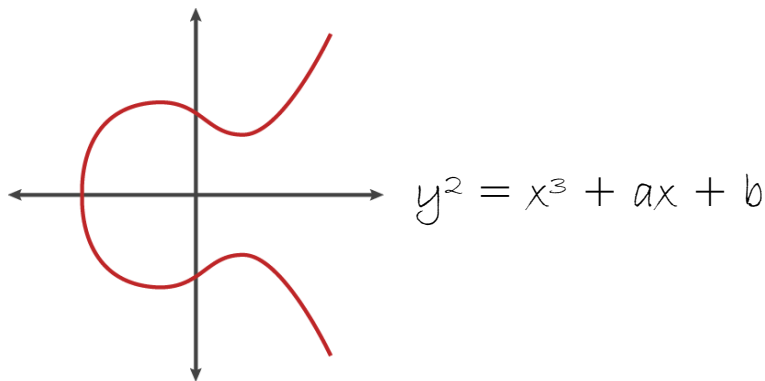
Dragonblood



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

Dragonblood

- 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 ☐ None

MAC Filtering ☒ Authorization List* ⓘ

Lobby Admin Access ☐

WPA Parameters

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

WPA2/WPA3 Encryption

AES(CCMP128) ☒	CCMP256 ☐
GCMP128 ☐	GCMP256 ☐

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS ☐

Reassociation Timeout *

Auth Key Mgmt

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

Anti Clogging Threshold*

Max Retries*

Retransmit Timeout*

PSK Format

PSK Type

Pre-Shared Key*

SAE Password Element ⓘ

FYI

Wi-Fi Certified Enhanced Open

WPA3

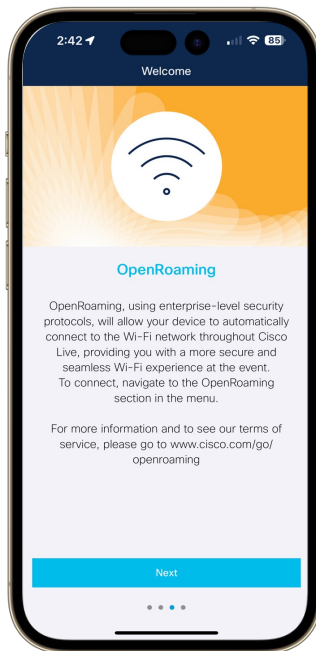
- Opportunistic Wireless Encryption (OWE)
 - Replaces 802.11 “open” authentication support
 - Client and AP perform an unauthenticated Diffie-Hellman Key Exchange to establish a PMK
 - Four-Way Handshake used as normal
 - Supports Protected Management Frames
- Diffie-Hellman is susceptible to MitM attacks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

Decoupling Access and Identity

Access and Identity

Decoupling Access and Identity

Access



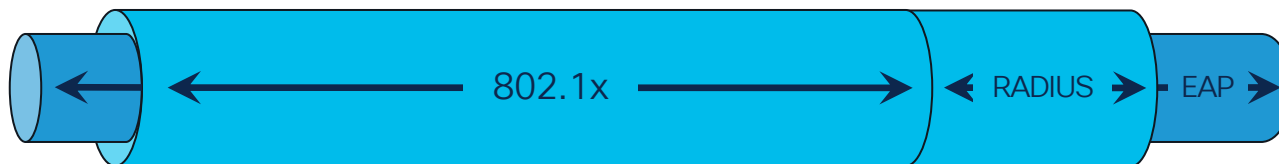
Identity

OpenRoaming



Wireless Network Discovery

Unique Identity



Wi-Fi 6E Security



WPA3 and OWE are **mandatory** for Wi-Fi 6E



WPA2 and Open are **not** supported on 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

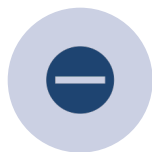
Status **ENABLED**

802.11b/g Policy 802.11b/g ▼

Wi-Fi 6E Security



WPA3 and OWE are **mandatory** for Wi-Fi 6E



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

General Security Advanced Add To Policy Tags

Profile Name* enterprise Radio Policy ⓘ

SSID* enterprise Show slot configuration

General Security Advanced Add To Policy Tags

Layer2 Layer3 AAA

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

MAC Filtering ☐

Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐ WPA2 Policy ☒

GTK Randomize ☐ WPA3 Policy ☒

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 ☐

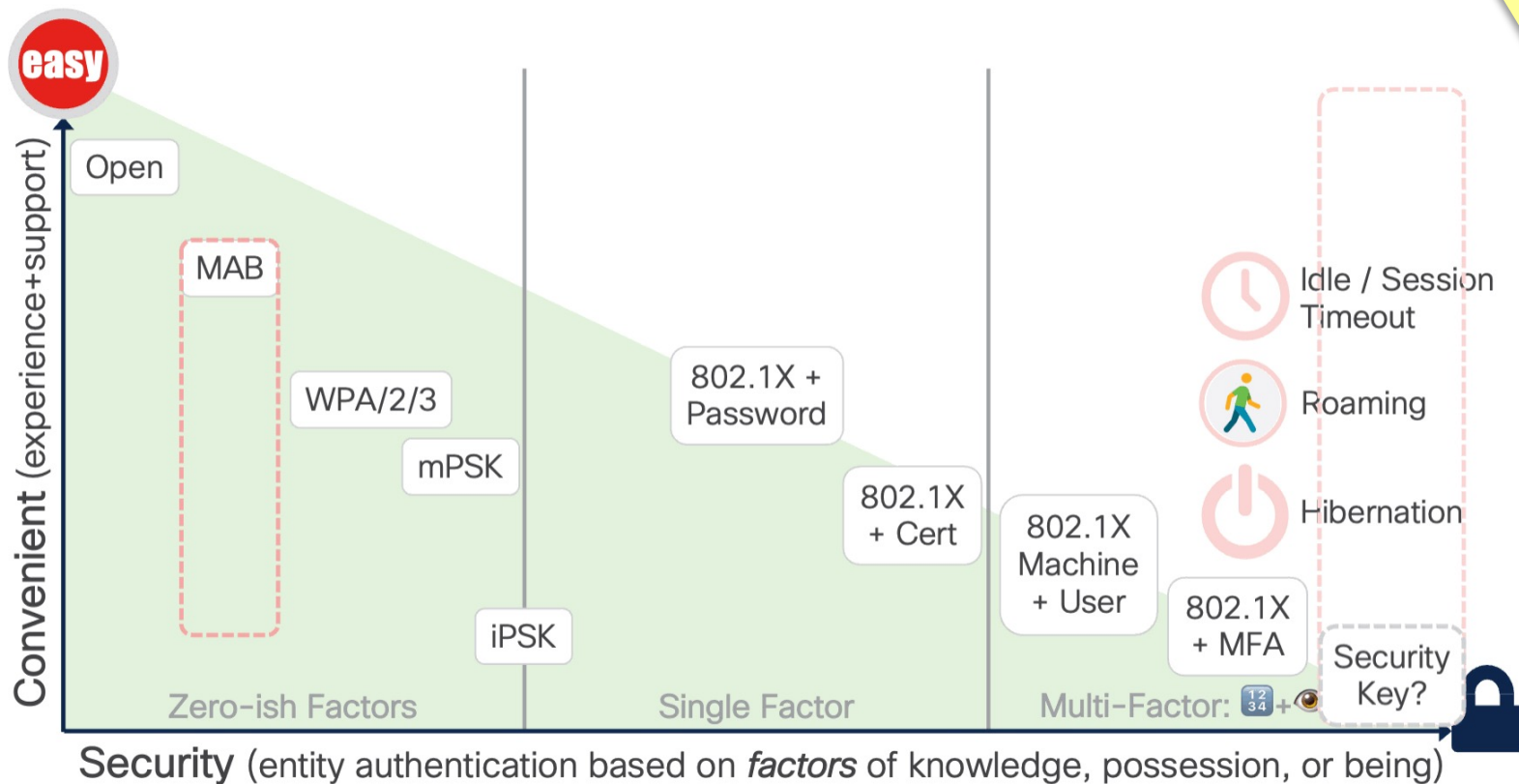
802.1X-SHA256 ☒ PSK-SHA256 ☐

Wi-Fi 6E Security

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



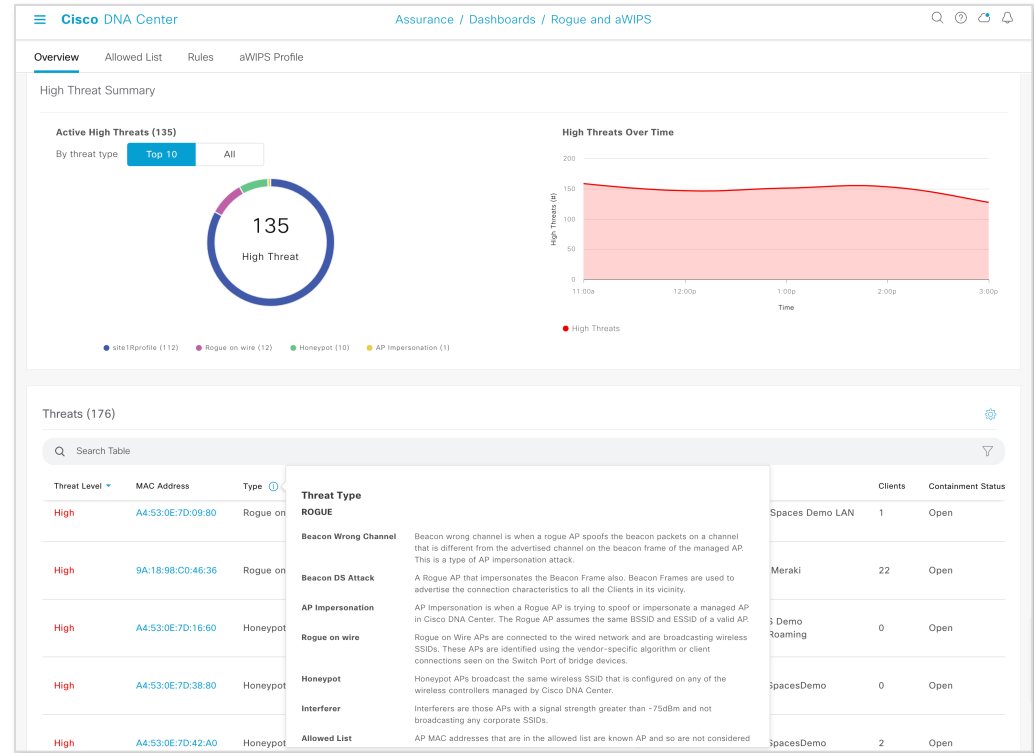
Network Access Security Spectrum



Rogue Detection and Advanced WIPS

Rogue Detection and Advanced WIPS

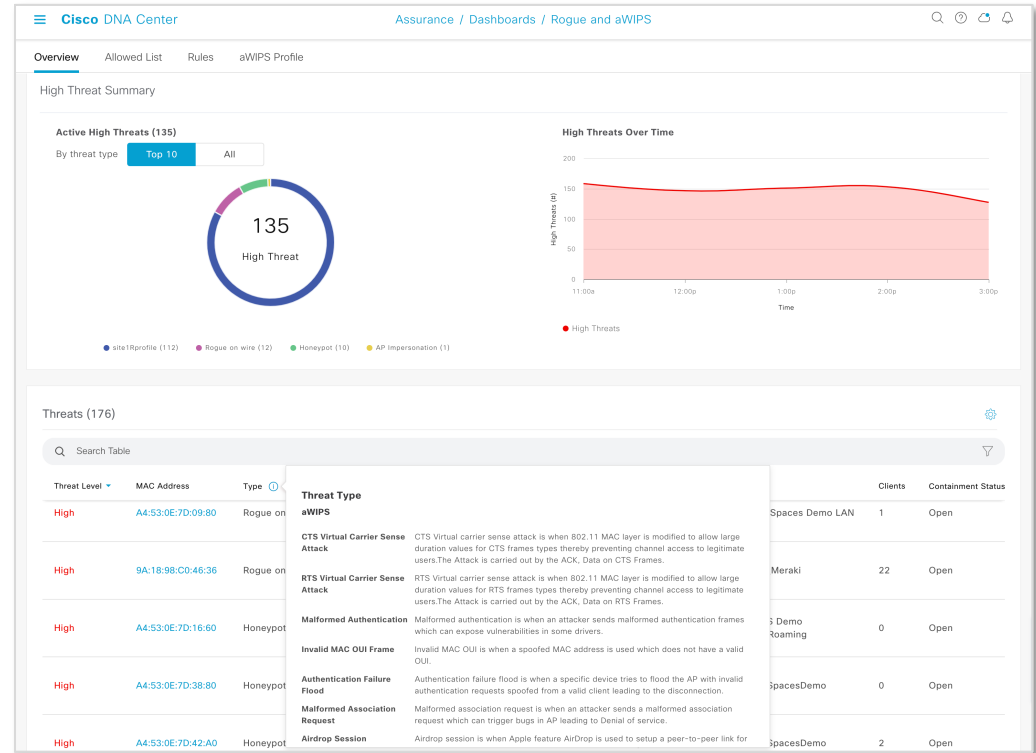
- Centralized wireless threat management
- Rogue detection
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



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

Rogue Detection and Advanced WIPS

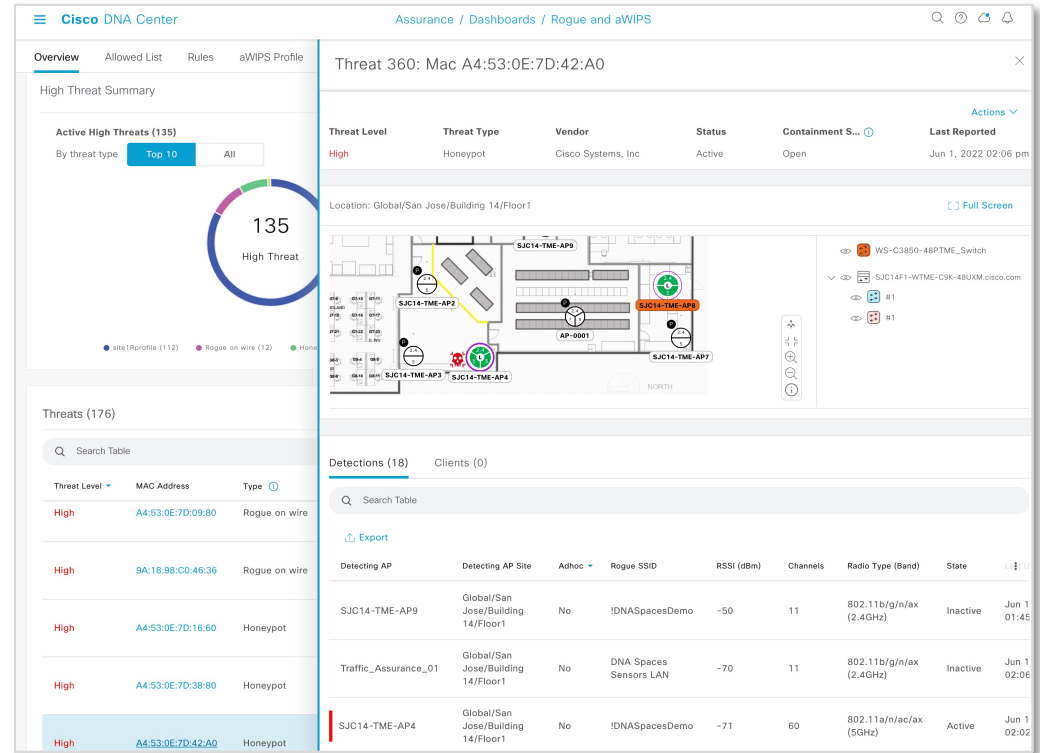
- Centralized wireless threat management
- Rogue detection
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



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

Rogue Detection and Advanced WIPS

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



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

Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies

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 Save Reset

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 ⓘ

Overview Threats Allowed List Rules aWIPS Profile

Site: Global May 7, 2022 8:26 PM - May 8, 2022 8:26 PM Last 24 hours Refresh Actions

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

High Threats Summary

Active High Threats (99)

By Threat Type

99 High Threat

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
Broadcast	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

Rogue and WIPS Reporting and APIs



Cisco DNA Center Reports

Generated Reports Report Templates Usage Insights

All

AI Endpoint Analytics

Access Point

Client

Compliance

Configuration Archive

EoX

Executive Summary

Group Communication Summary

Group Pair Communication Analytics

Inventory

Licensing

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 TDL JSON

Generate

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 TDL JSON

Generate

Cisco DNA Center Platform / Developer Toolkit

APIs Integration Flows Event Notifications

Search API

Devices

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

FYI

- 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 ☒

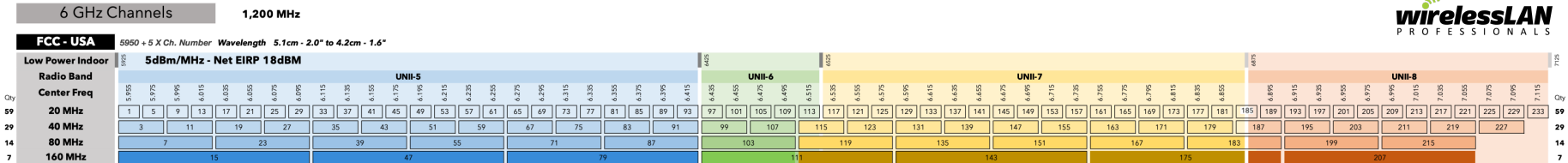
Report Interferers ☒

Available Interference Types

WiFi Inverted
WiFi Invalid Channel

Interference Types to detect

TDD Transmitter
Jammer
Continuous Transmitter
DECT-like Phone



wirelessLAN
PROFESSIONALS

CISCO Live!

Rogue Access Points

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

The screenshot shows the 'Add AP Join Profile' configuration window with the 'Security' tab selected. The window has tabs for General, Client, CAPWAP, AP, Management, Security, ICap, and QoS. The 'Rogues' section contains the following settings:

Setting	Value
Rogue Detection	☒
Rogue Detection Minimum RSSI	-90
Rogue Detection Transient Interval (seconds)	0
Rogue Detection Report Interval (seconds)	10
Rogue Containment Automatic Rate Selection	☐
Auto Containment on FlexConnect Standalone	☐

The 'aWIPS' section contains the following settings:

Setting	Value
aWIPS Enable	☒
Forensic Enable	☐

At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

Rogue Access Points

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

The screenshot displays the 'Add AP Join Profile' configuration window, specifically the 'Security' tab. The 'Rogues' section is active, showing settings for Rogue Detection (checked), Rogue Detection Minimum RSSI (-90), and Rogue Detection Transient Interval (seconds) (0). Below this, the 'Wireless Protection Policies' section is visible, with 'Rogue AP Rules' selected. The 'General' tab for Rogue AP Rules shows settings for Rogue Detection Security Level (Custom), Expiration timeout for Rogue APs (seconds)* (1200), Validate Rogue Clients against AAA (unchecked), Validate Rogue APs against AAA (unchecked), Rogue Polling Interval (seconds) (3600), Detect and Report Adhoc Networks (checked), Rogue Detection Client Number Threshold* (0), Rogue Init Timer (seconds)* (180), AP Authentication (unchecked), AP Authentication Alarm Threshold* (1), and Syslog Notification (unchecked). The 'Auto Contain' tab shows settings for Auto Containment Level (1), Auto Containment only for Monitor Mode APs (unchecked), Using our SSID (checked), Valid client on Rogue AP (unchecked), Adhoc Rogue AP (unchecked), MFP Configuration (unchecked), Global MFP State (unchecked), AP Impersonation Detection (unchecked), and MFP Key Refresh Interval (hours)* (24). The 'Using our SSID' checkbox is highlighted with a red box.

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 DNA 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 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

The image displays three overlapping screenshots of the 'Edit Rogue AP Rule' configuration window. A yellow sticky note with 'FYI' is in the top right corner.

- Top Window:** Shows 'Rule Name*' as 'malicious' and 'Rule Type' as 'Malicious'. The 'State' dropdown is open, showing options: Friendly, Malicious (selected), Unclassified, and Custom.
- Middle Window:** Shows 'Rule Name*' as 'malicious' and 'Rule Type' as 'Malicious'. The 'State' dropdown is open, showing options: Contain (selected), Alert, and Delete.
- Bottom Window:** Shows 'Rule Name*' as 'malicious' and 'Rule Type' as 'Malicious'. The 'State' dropdown is open, showing options: Contain (selected), Alert, and Delete. The 'Enable Rule' checkbox is unchecked. The 'Add Condition' dropdown is open, showing options: None, client-count, duration, encryption, infrastructure, rssi, ssid (selected), and substring-ssid.

Rogue Notification Triggers



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

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

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

Rogue AP Containment

- How do we contain Rogue APs?
 - Containment is a spoofed 802.11 disassociation/deauthentication request attack
- 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 management. The top navigation bar shows 'Cisco DNA Center' and 'Assurance / Dashboards / Rogue and aWIPS'. The main content area is divided into several sections:

- Overview:** Shows a summary of threats, including a 'High Threat' indicator.
- Threats (174):** A table listing detected threats. The selected threat is 'Threat 360: Mac A4:53:0E:7C:99:E0'.
- Threat Details:** A detailed view of the selected threat, including its level (High), type (HoneyPot), vendor (Cisco Systems, Inc), status (Active), and containment status (Open). A 'Start Containment' button is highlighted.
- Location:** A map showing the physical location of the threat, labeled 'Global/San Jose/Building 14/Floor1'.
- Detections (28):** A table listing detected threats, including their AP ID, location, and status.

Threat Level	Threat Type	Vendor	Status	Containment Status
High	HoneyPot	Cisco Systems, Inc	Active	Open

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
- 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. A warning dialog box is open, 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 172.20.224.55. Do you want to continue?" The dialog lists two Rogue BSSIDs: A4:53:0E:7C:99:E0 and A4:53:0E:7C:99:E3. Below the dialog, a table lists threats. The threat "SJC14-TME-AP4" is highlighted with a red circle. The table columns include Threat Level, Threat Type, Vendor, Status, Containment Status, and Last Reported.

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

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

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

Rogue AP Containment

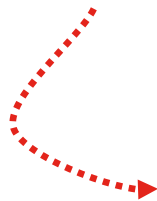
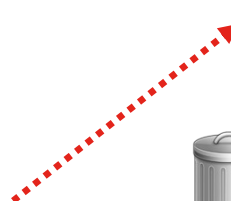
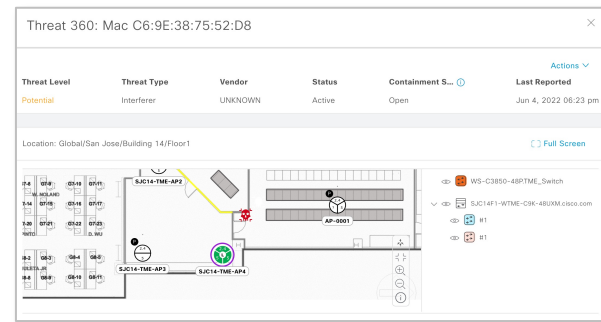
- How do we contain Rogue APs?
 - Containment is a spoofed 802.11 disassociation/deauthentication request attack
- How does WPA3 affect Rogue AP containment?
 - 802.11w will change how we can mitigate Rogue AP related threats
 - The ability to physically locate rogues will be key

The screenshot displays the Cisco DNA Center interface, specifically the 'Assurance / Dashboards / Rogue and aWIPS' section. It shows a table of threats, with a warning dialog box overlaid. The warning states: 'Warning: Using this feature may have legal consequences. Wireless containment will be initiated for the below rogue BSSIDs on wireless controller with IP address 172.20.224.55. Do you want to'. Below the warning, a detailed view for 'Threat 360: Mac C6:9E:38:75:52:D8' is shown, indicating a 'Potential' threat level, 'Interferer' type, and 'UNKNOWN' vendor. The interface also includes a floor plan of a building (Global/San Jose/Building 14/Floor1) with various access points (AP-0001, SJC14-TME-AP2, SJC14-TME-AP3, SJC14-TME-AP4) and switches (WS-C3850-48PTME_Switch, SJC14F1-WTME-C9K-48UXM.cisco.com) marked. A red circle highlights a specific location on the floor plan.

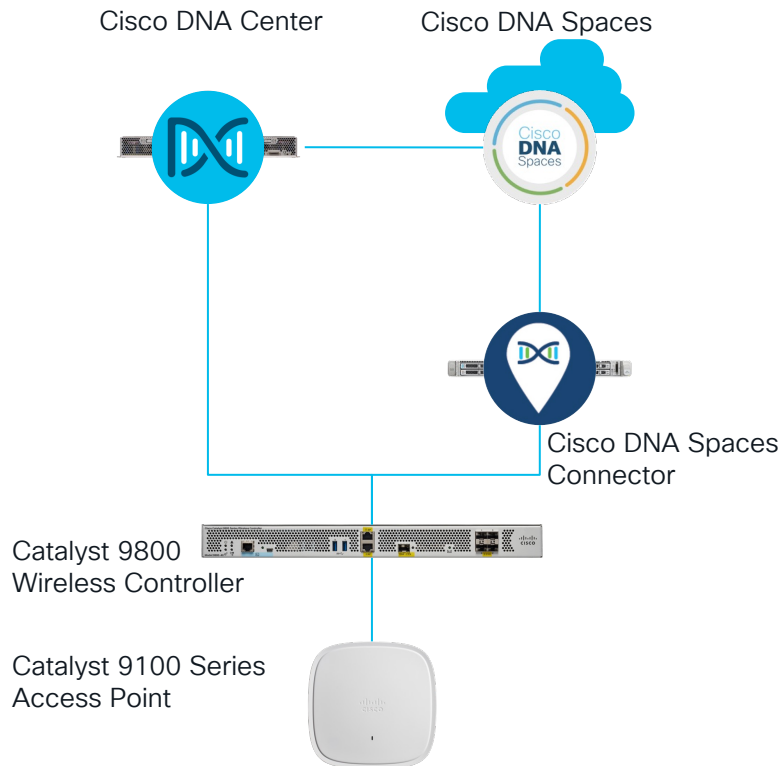
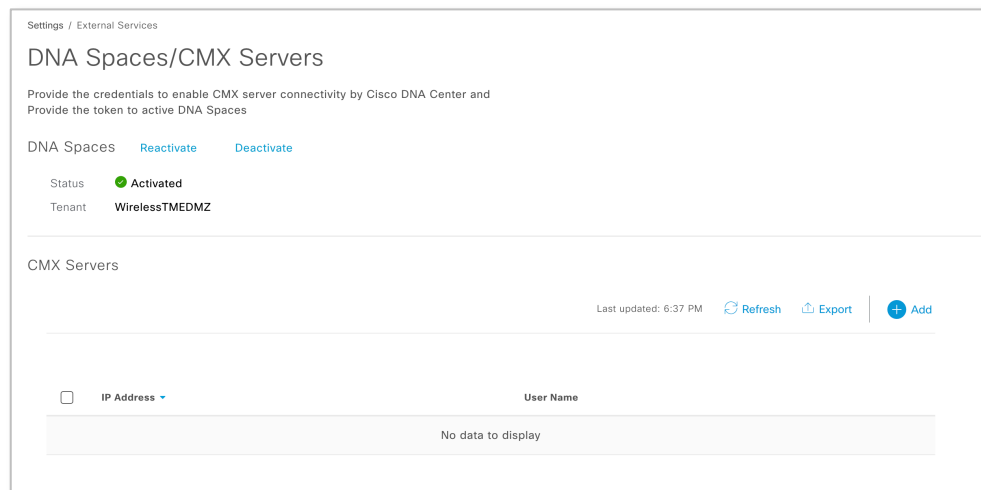
Rogue Containment with WPA3



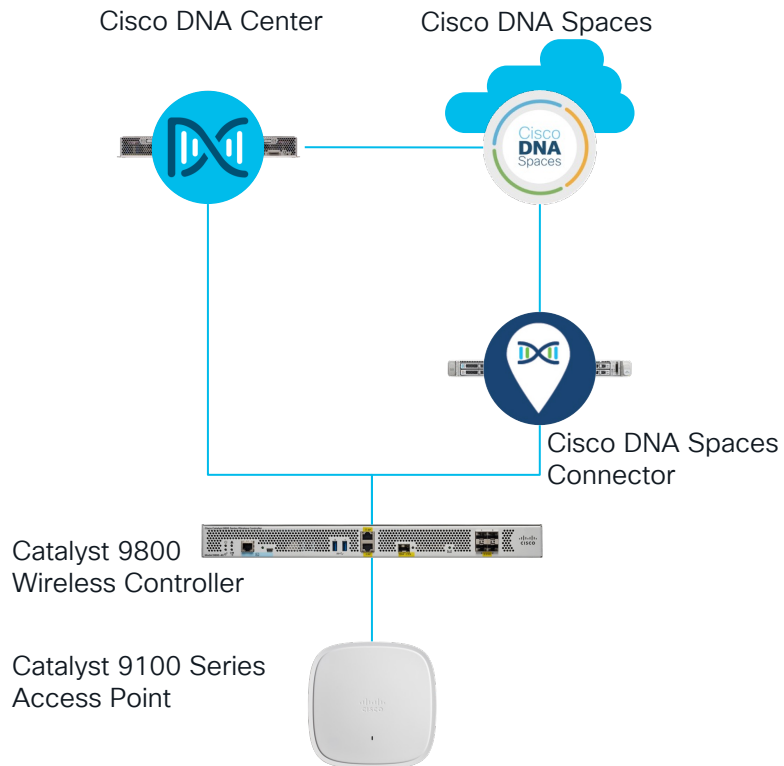
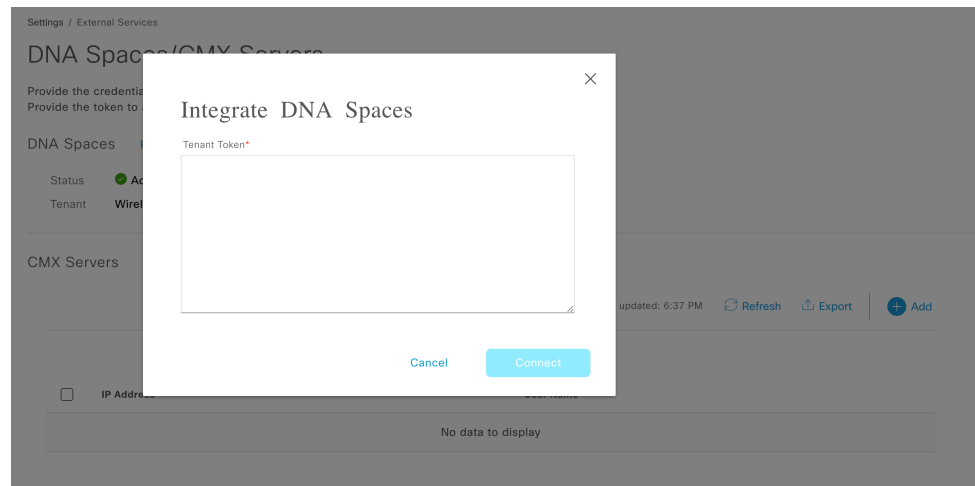
802.11w Protected



Enabling Location Services



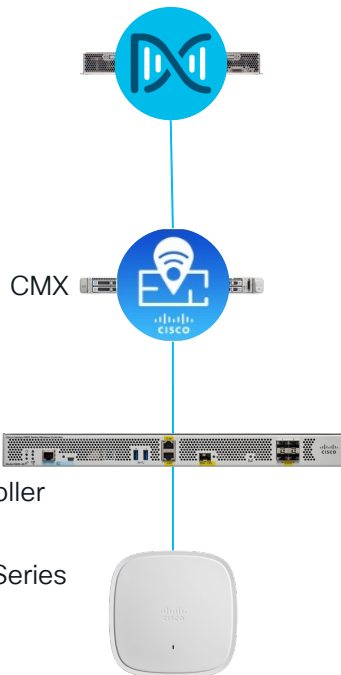
Enabling Location Services



Enabling Location Services



Cisco DNA Center



Settings / External Services

DNA Spaces/CMX Servers

Provide the credentials to enable CMX server connectivity by Cisco DNA Center and Provide the token to active DNA Spaces

DNA Spaces [Reactivate](#) [Deactivate](#)

Status ● **Activated**

Tenant **WirelessTMEDMZ**

CMX Servers

Last updated:

☐	IP Address ▼	User Name
No data to display		

Add CMX Server

IP Address*

User Name*

Password*

SSH User Name*

SSH Password*

[Cancel](#) [Add](#)

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

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

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

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

14 High Threat

● Rogue on wire (12) ● Honeyport (1)

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:7D:09:80	Rogue on wire

Switch Port Detail (1)

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

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

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

Full Screen

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:7D: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

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...
High	Rogue on wire	UNKNOWN	Active	Open

Location: Global/San Jose/Building 14/Floor1

Switch Port Detail (1)

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) →

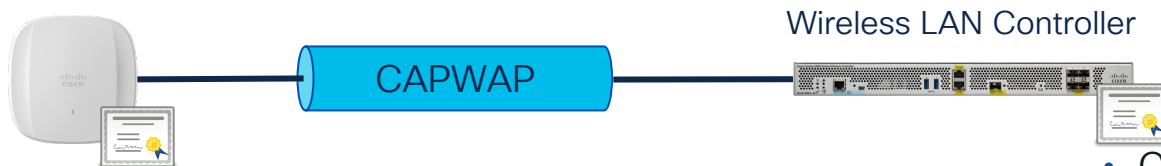


How do we bootstrap configure the AP?

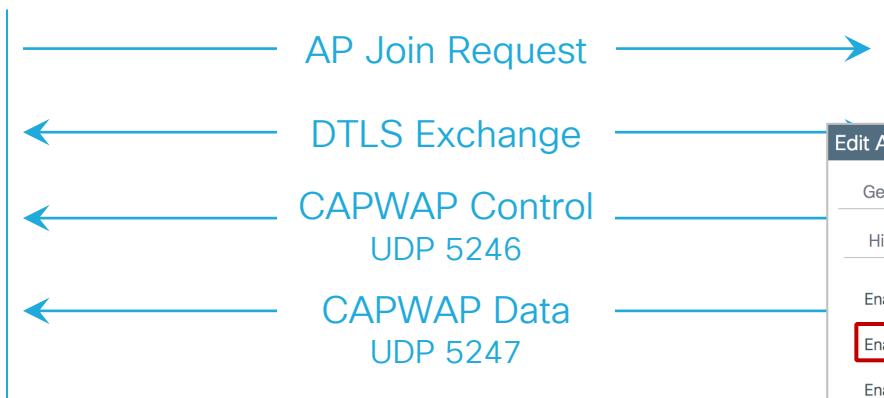
- Pre-Provision before deploying the APs
- Enable 802.1x after bringing up the wireless network

The screenshot shows the 'Add AP Join Profile' configuration window. The 'Management' tab is selected. Under the 'Credentials' sub-tab, the 'Dot1x Credentials' section is visible. It contains three fields: 'Dot1x Username' with a text input field labeled 'Enter dot1x Username', 'Dot1x Password' with a text input field labeled 'Enter Dot1x Password', and 'Dot1x Password Type' with a dropdown menu set to 'clear'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

Securing AP to Controller Communication



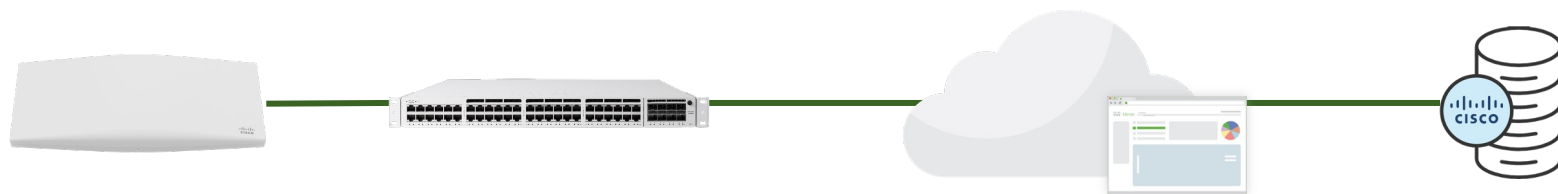
- CAPWAP Control encrypted by default
- CAPWAP Data encapsulated but not encrypted by default



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 <input type="text" value="Disable"/>					
Preferred Mode <input type="text" value="Disable"/>					

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

Air Marshal

- Rogue AP Detection
 - 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...

☐	SSID ▲	Broadcast MACs	Last seen	First seen	Containment	Rogue because	
☐	AXE BLE testing	6e:3a:0e:ff:f8:f5 (and 1 other)	4 seconds ago	1 year ago	🔒 partial	Recently seen on LAN	
☐	IT Test WiFi	e0:cb:bc:49:35:61 (and 1 other)	50 seconds ago	1 month ago	🔒 contained	Recently seen on LAN	
☐	j-bond-2-owe	c6:14:92:6e:ae:b2 (and 2 others)	15 seconds ago	2 months ago	🔒 partial	Recently seen on LAN	
☐	j-bond-3-sae	ca:14:a2:6e:ae:b0 (and 1 other)	15 seconds ago	3 weeks ago	🔒 partial	Recently seen on LAN	
☐	j-bond-5-1x	c6:14:92:6e:ae:a5 (and 4 others)	6 seconds ago	3 weeks ago	🔒 partial	Recently seen on LAN	
☐	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	
☐	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	

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

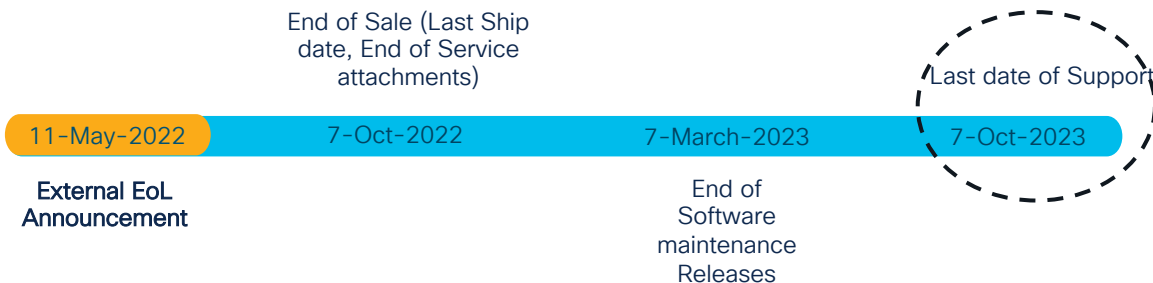
Seen by SFO12-1-AP08 (77 dB)
SFO12-1-AP01 (41 dB)
SFO12-1-AP03 (41 dB)
SFO12-1-AP04 (41 dB)
SFO12-1-AP05 (38 dB)
SFO12-1-AP02 (34 dB)
SFO12-1-AP07 (29 dB)
SFO12-2-AP05 (12 dB)

MSE WIPS End of Life



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

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



Next Steps

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

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

Cisco DNA 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 DNA 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.cis

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

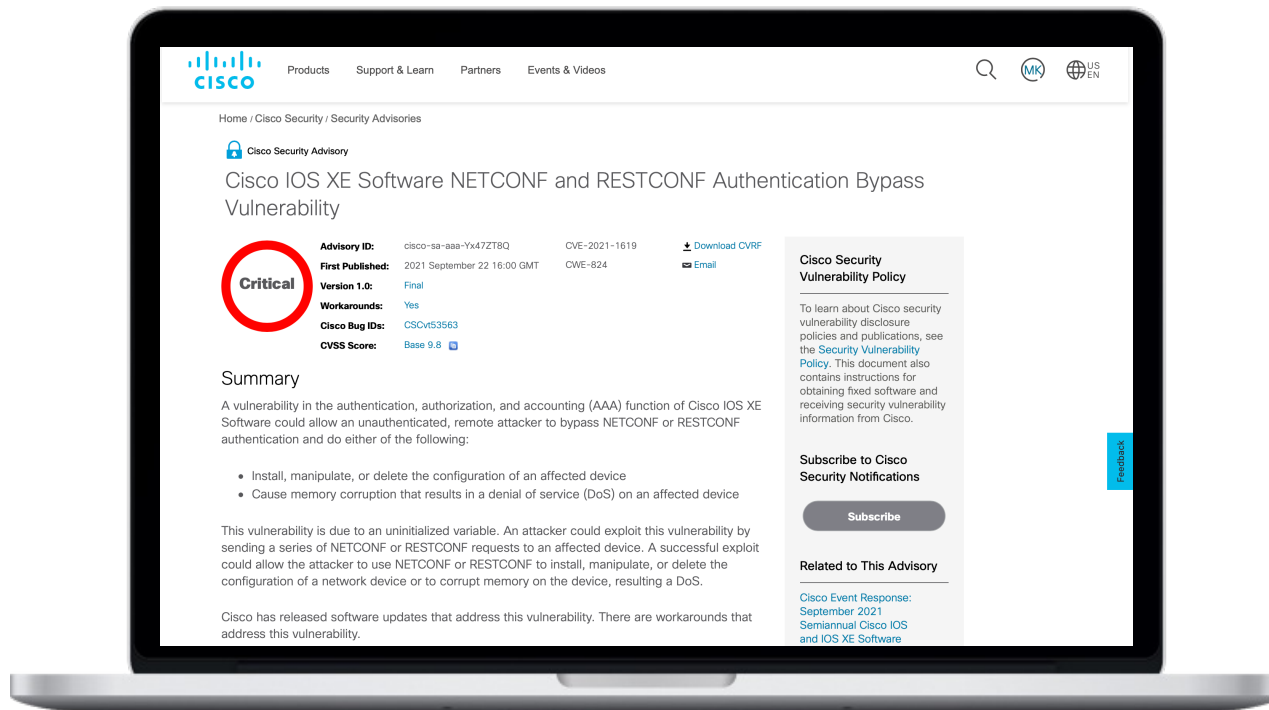
Details Advisories Configuration

Advisories (69) Active Suppressed

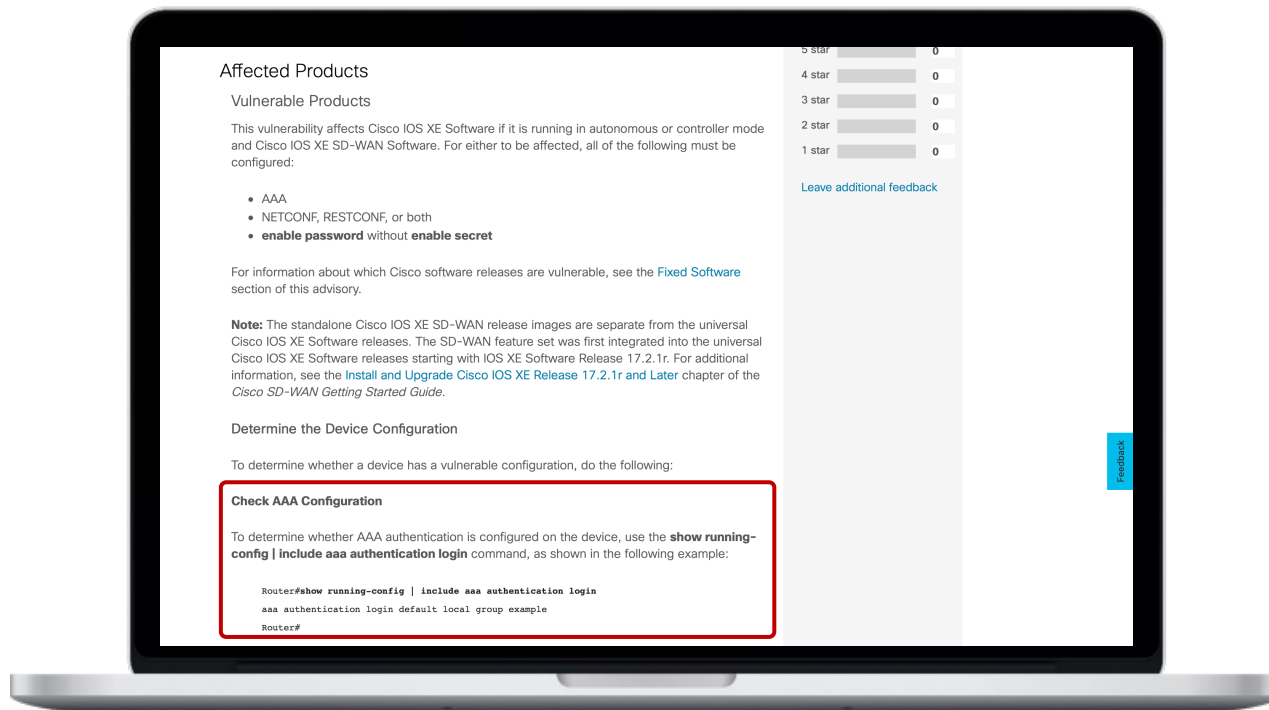
Filter 0 Selected Suppress Advisory

☐	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-EFJrEzPx	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

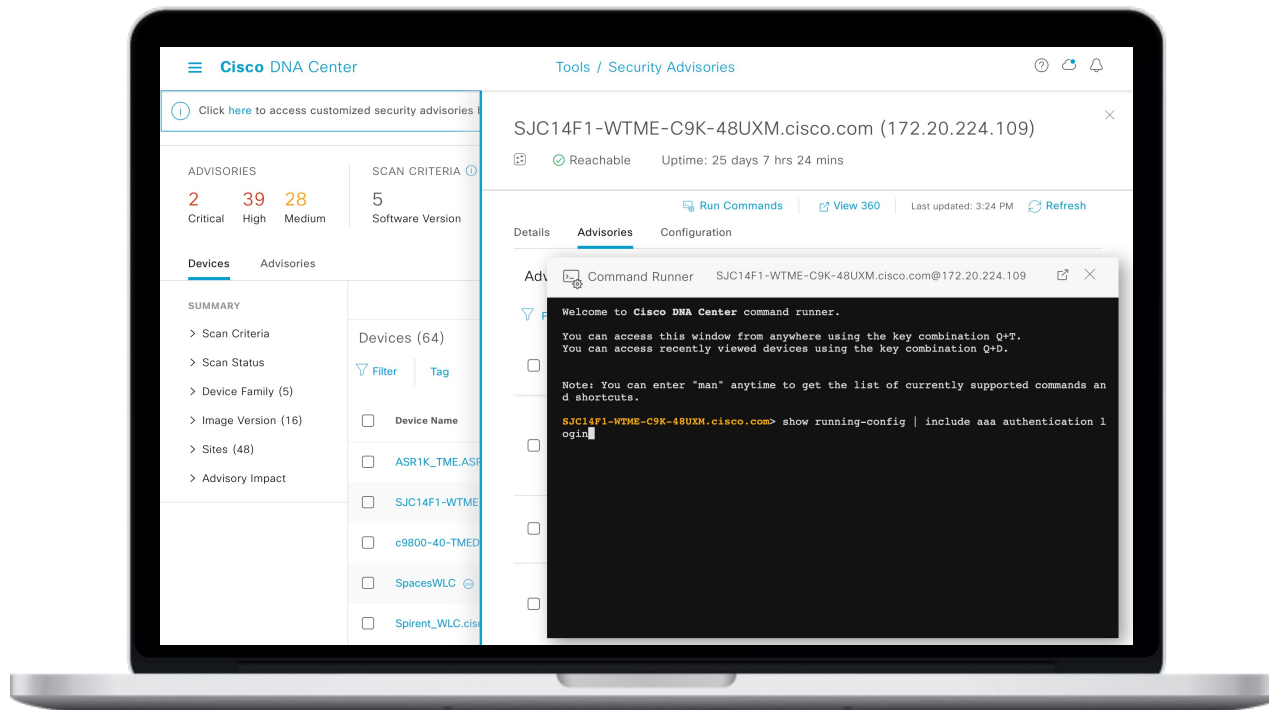
Cisco DNA Center Security Advisories



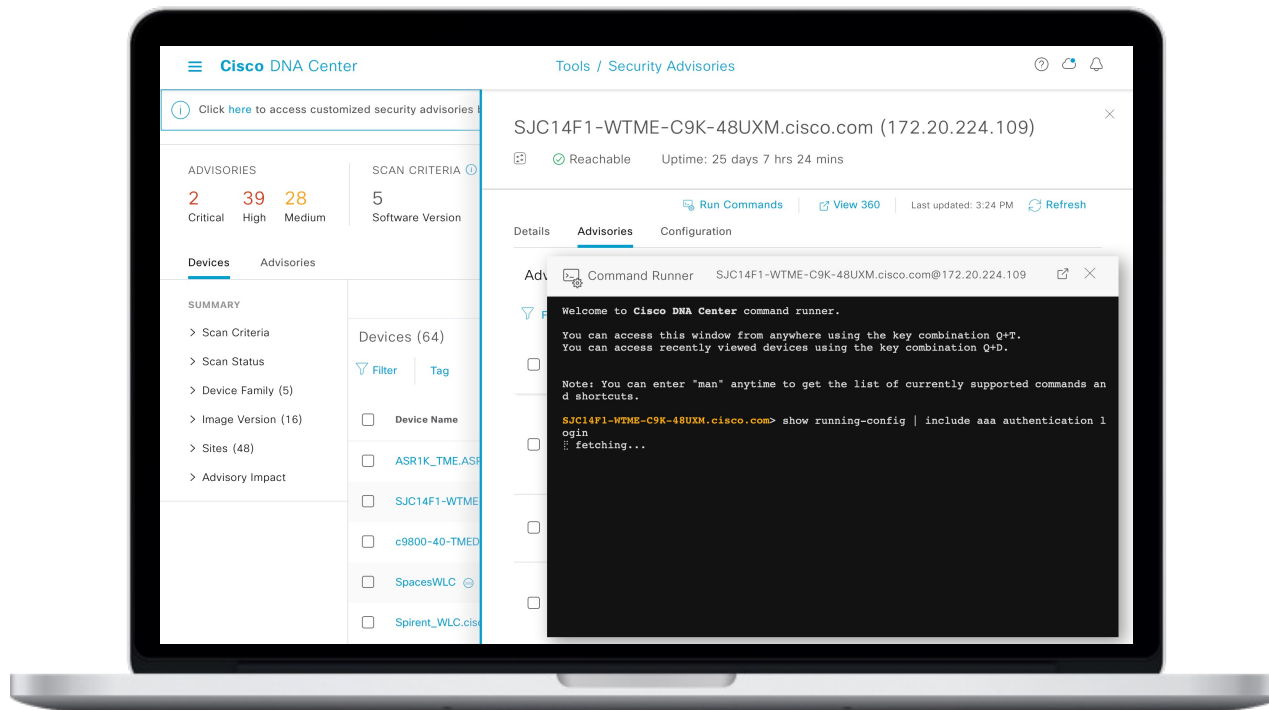
Cisco DNA Center Security Advisories



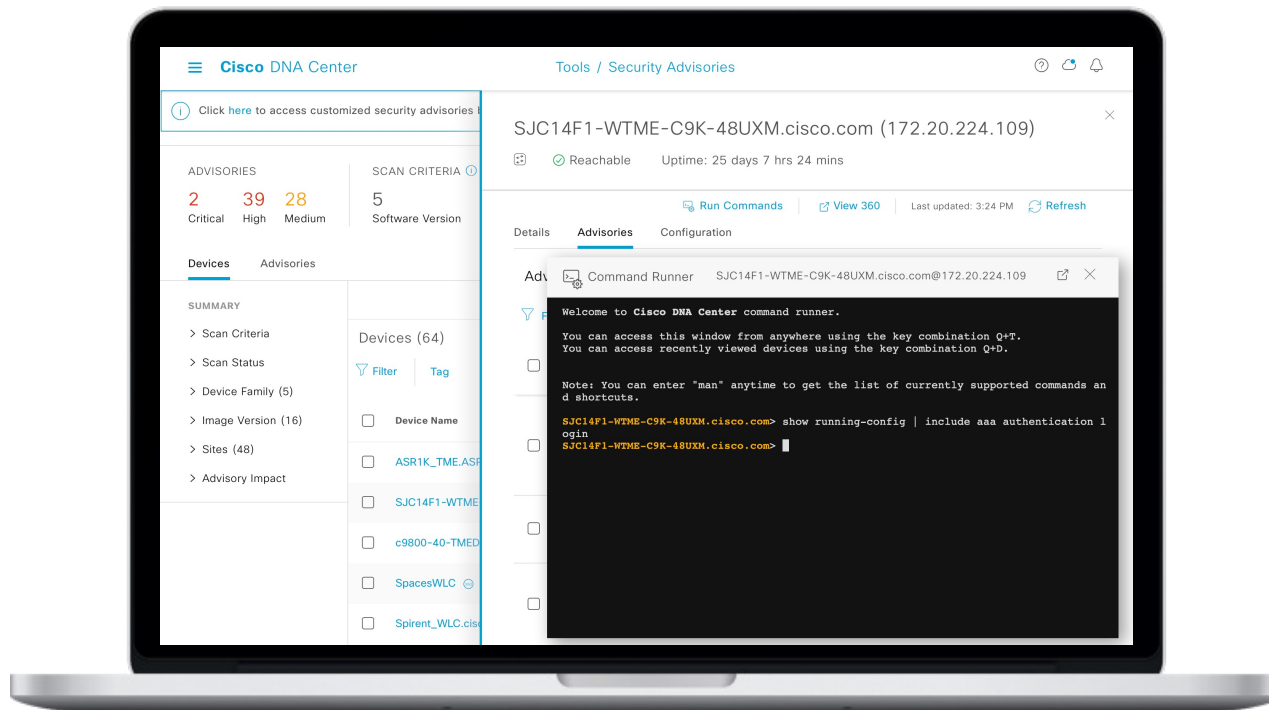
Cisco DNA Center Security Advisories



Cisco DNA Center Security Advisories

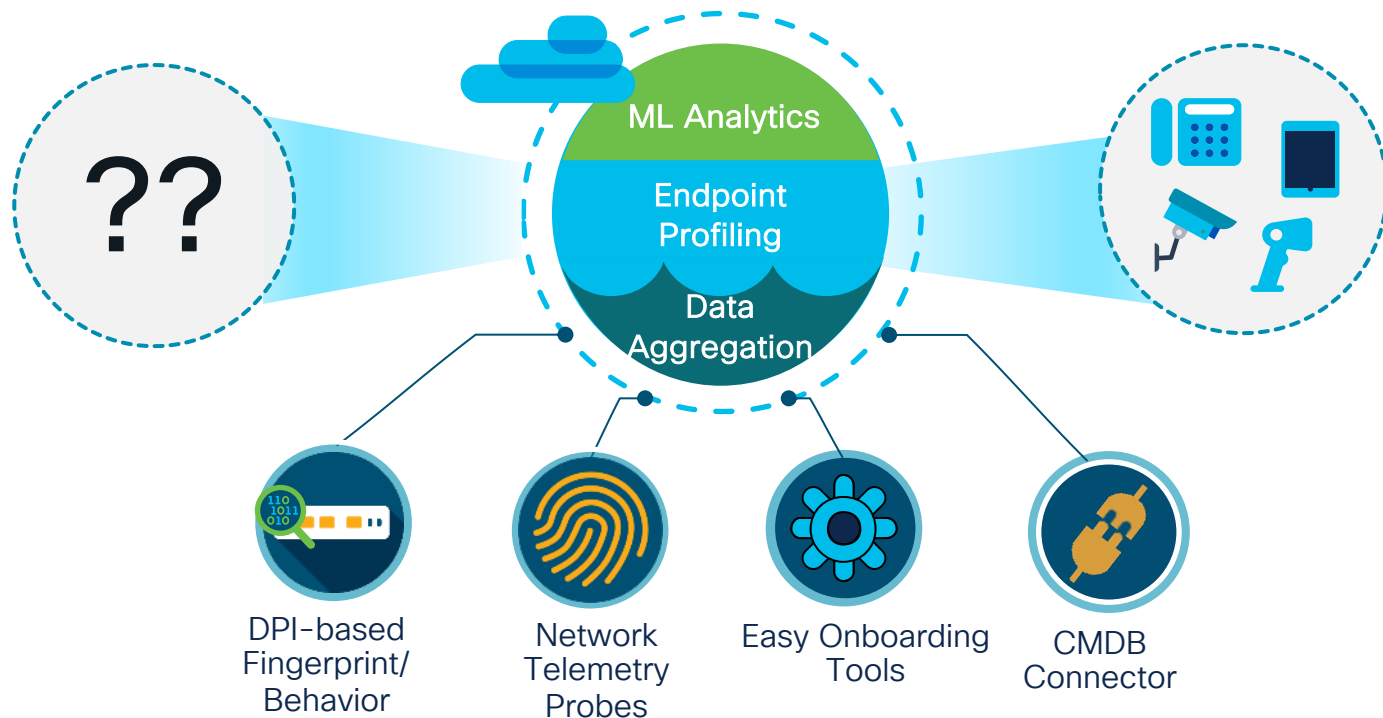


Cisco DNA Center Security Advisories



Cisco DNA Center AI Endpoint Analytics

FYI



Network as a Sensor

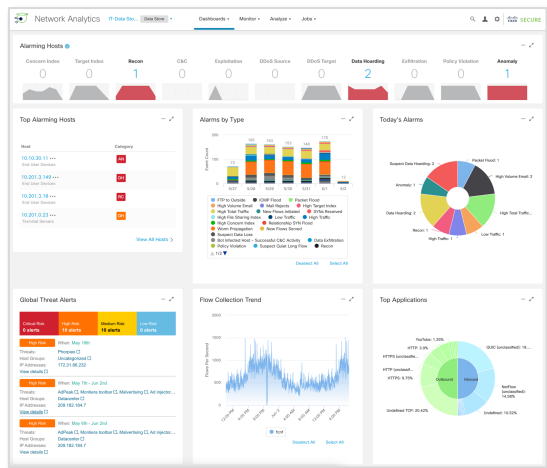
Secure Network Analytics Integration



Netflow



Malware detection and cryptographic compliance on Cisco Stealthwatch



Top Security Events for 10.201.3.18

Security Event	Count	Concom Index	First Active	Target Host	Target Host Group	Actions
Port Scan - 49115	50	\$40,000	06/02 3:51:05 PM	10.201.0.15	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 4:48:43 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**

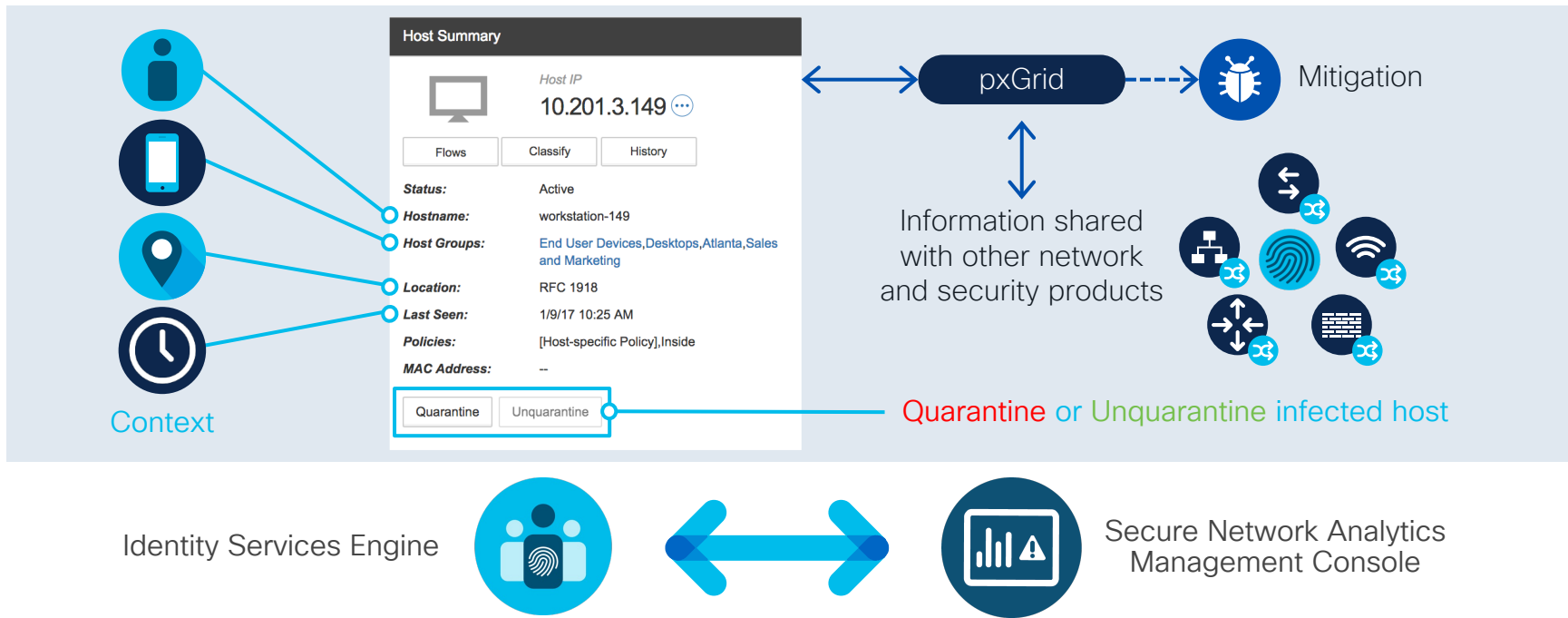
MITRE Techniques: **Exfiltration Over Alternative Protocol**

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

[go to alert priorities page](#)

Network as an Enforcer

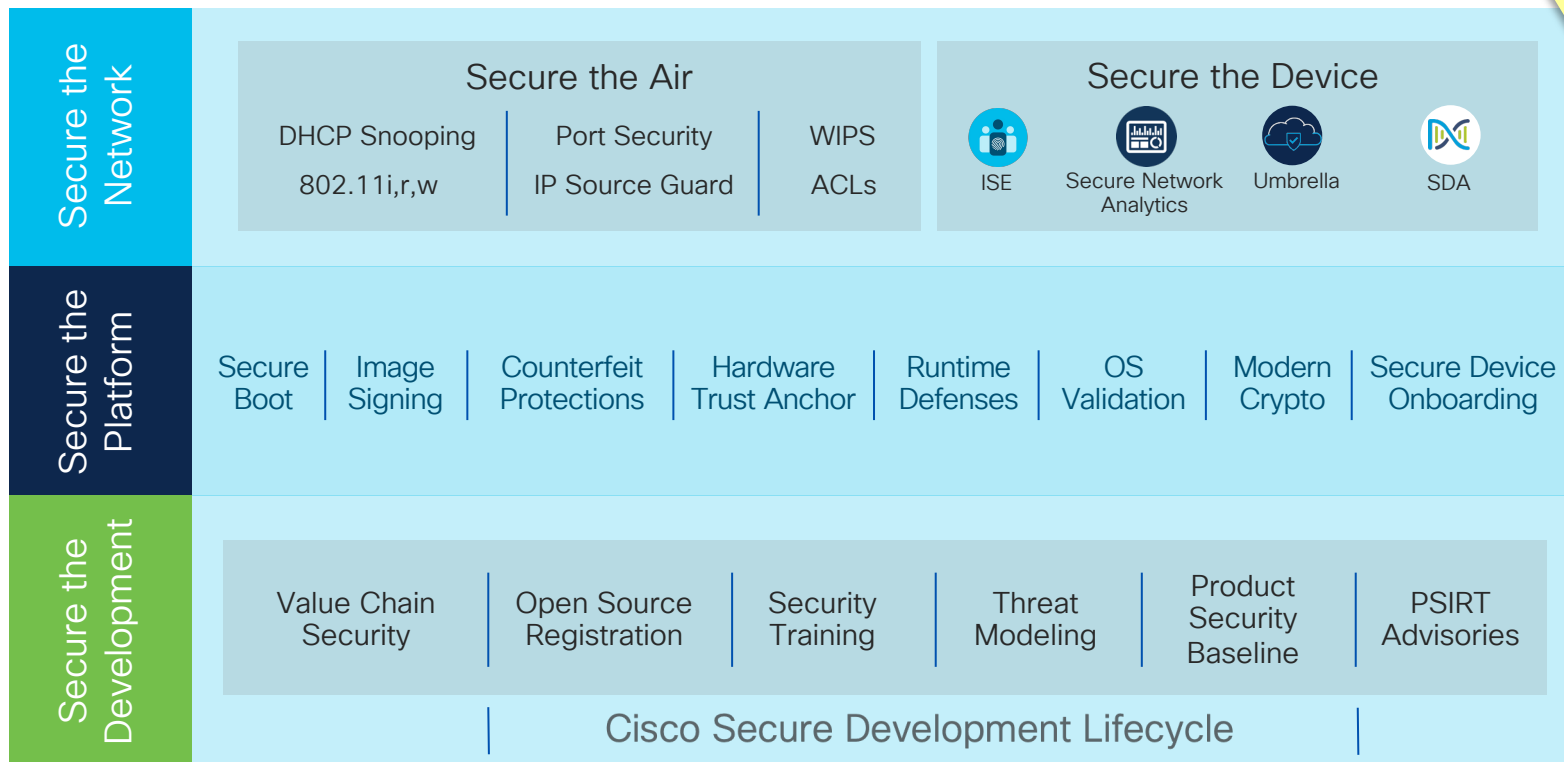
Rapid Threat Containment



Securing the Wireless Network



Trustworthy Systems





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase 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

The background is a vibrant, abstract graphic. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect. The overall composition is dynamic and colorful.

cisco *Live!*

Let's go

#CiscoLiveAPJC