Understanding Wireless Security

and the Implications for Secure Wireless Network Design

Mark Krischer
Principal Solutions Engineer

cisco Live !

Session ID: BRKEWN-2104

Cisco Webex App

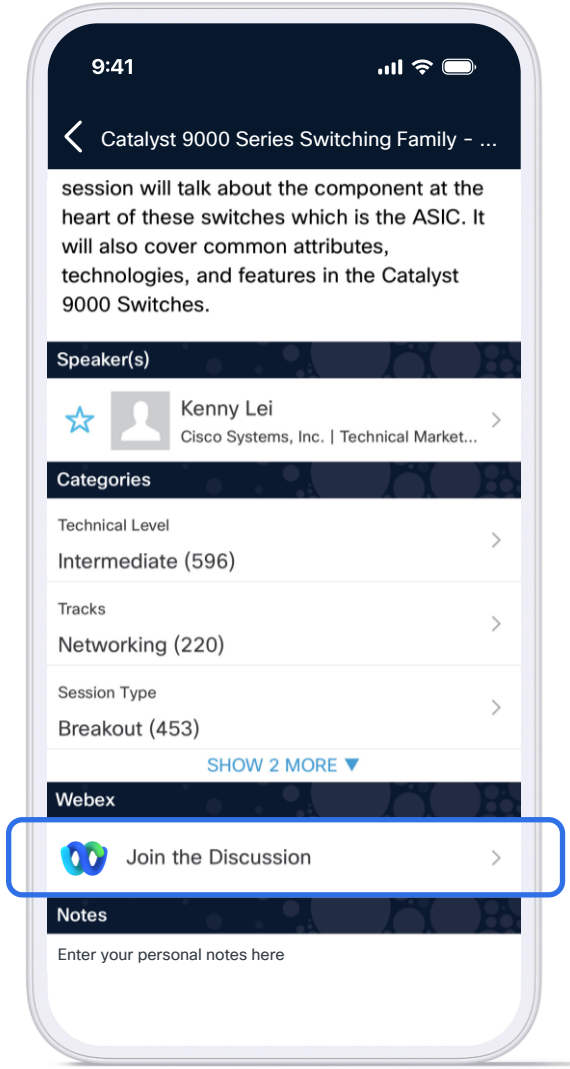
Questions?

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 by the speaker until 14 November 2025.



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

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

1 **Wireless Security Fundamentals**

- WPA3
- Authentication and Authorisation
- Implications of 6GHz

2 **Wireless Intrusion Detection and Prevention**

- Rogue Detection and Mitigation
- Advanced WIPS
- Air Marshal

3 **Network as a Sensor and Enforcer**

© 2025 Cisco and/or its affiliates. All rights reserved.

Wireless Security Fundamentals

cisco Live !

Wireless Attack Surface

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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Securing the Wireless Network

© 2025 Cisco and/or its affiliates. All rights reserved.

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 – Extensible Authentication Protocol)
WPA3	• Wi-Fi Alliance security update • Includes new capabilities and new certification requirements

© 2025 Cisco and/or its affiliates. All rights reserved.

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)

© 2025 Cisco and/or its affiliates. All rights reserved.

802.11 Fundamentals

Authentication

© 2025 Cisco and/or its affiliates. All rights reserved.

802.11 Fundamentals

Authentication

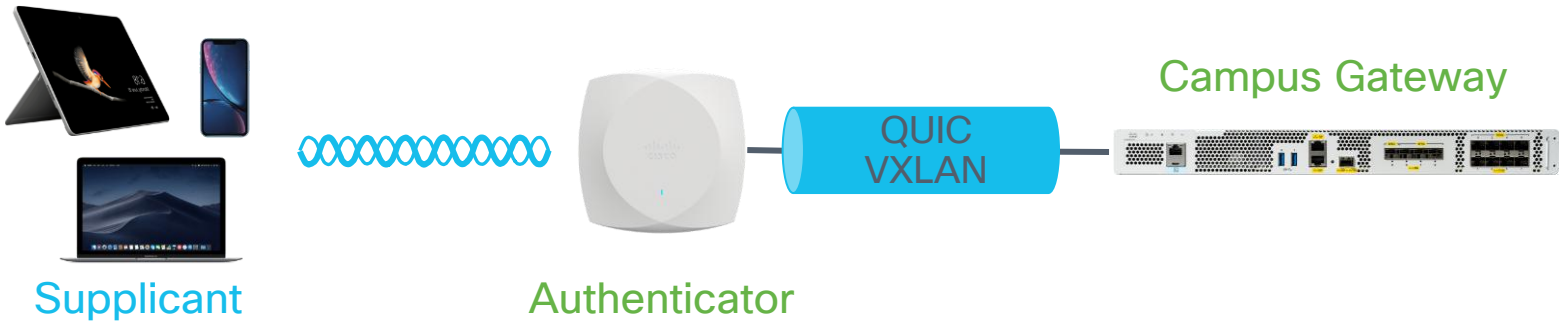
Supplicant

Authenticator

© 2025 Cisco and/or its affiliates. All rights reserved.

802.11 Fundamentals

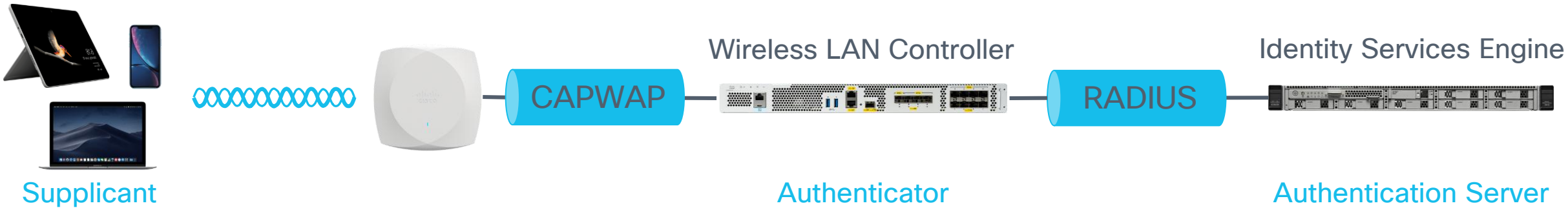
Authentication



© 2025 Cisco and/or its affiliates. All rights reserved.

802.11 Fundamentals

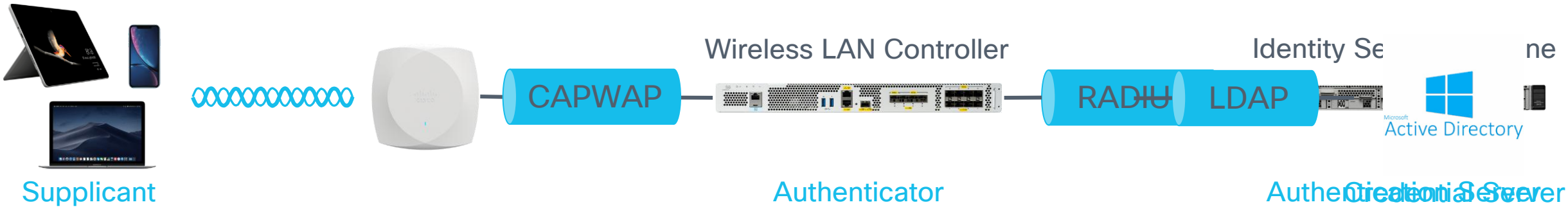
Authentication



© 2025 Cisco and/or its affiliates. All rights reserved.

802.11 Fundamentals

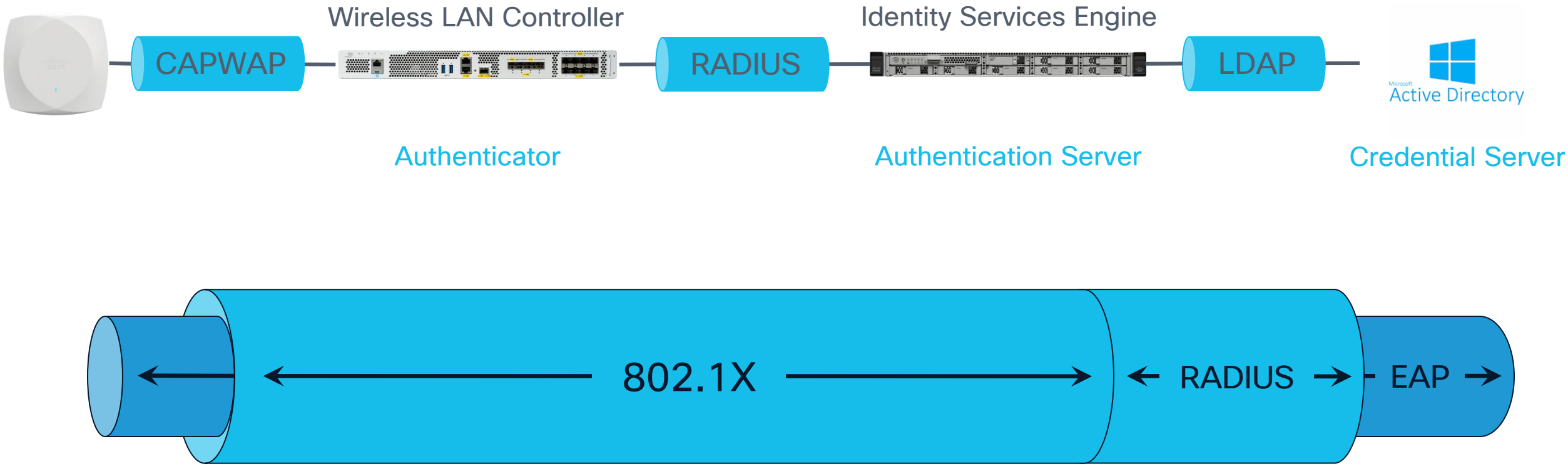
Authentication



© 2025 Cisco and/or its affiliates. All rights reserved.

802.11 Fundamentals

Authentication



© 2025 Cisco and/or its affiliates. All rights reserved.

802.11 Fundamentals

Encryption

AES

CAPWAP

Wireless LAN Controller

RADIUS

Identity Services Engine

Supplicant | Authenticator | Authentication Server

PMK ← EAP Success — EAP Success (PMK) — PMK

← ANonce

PTK → SNonce, MIC

PTK, GTK

← ANonce, MIC, GTK, Sequence #

→ ACK

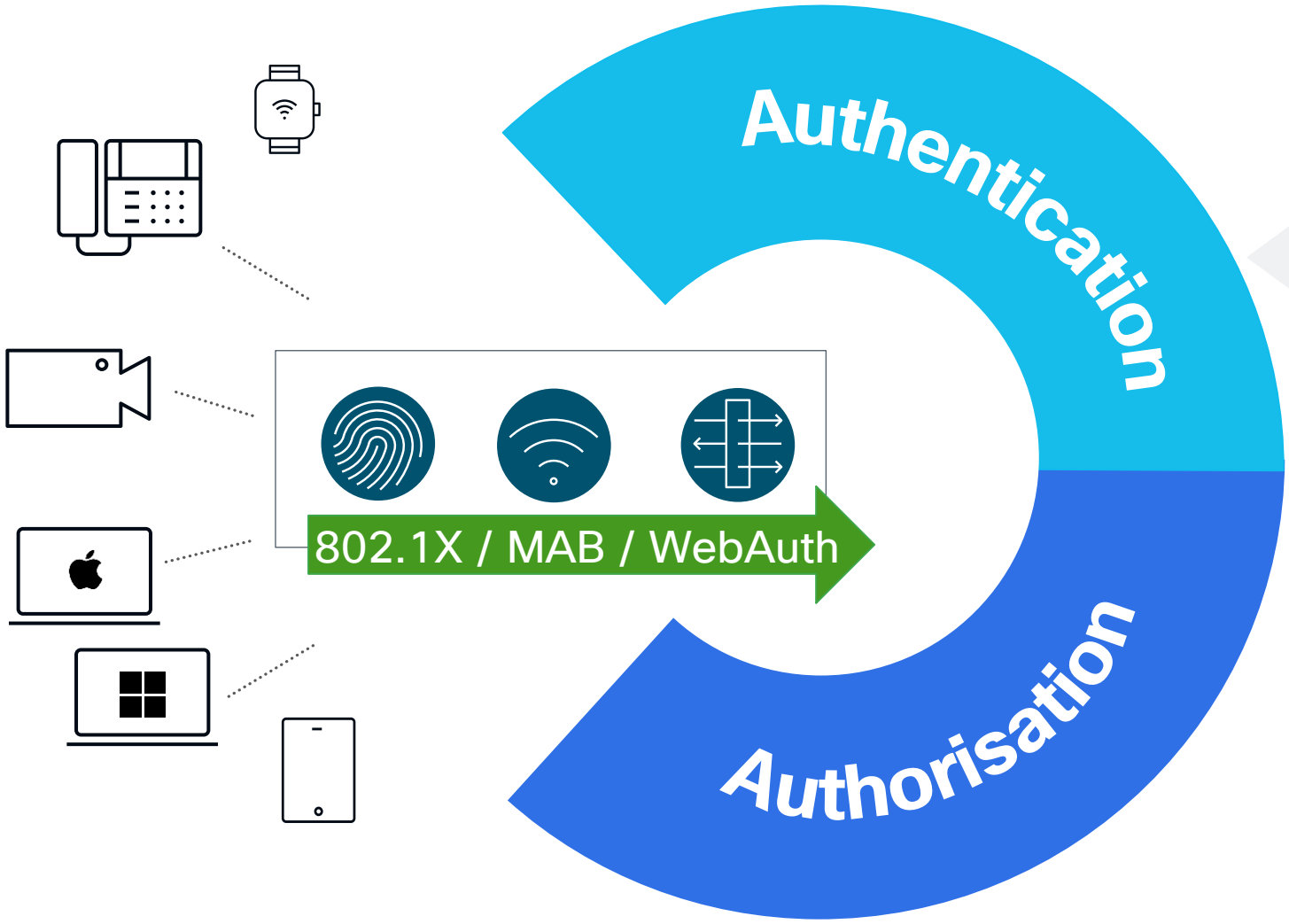
Four-Way Handshake

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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Authentication and Authorisation



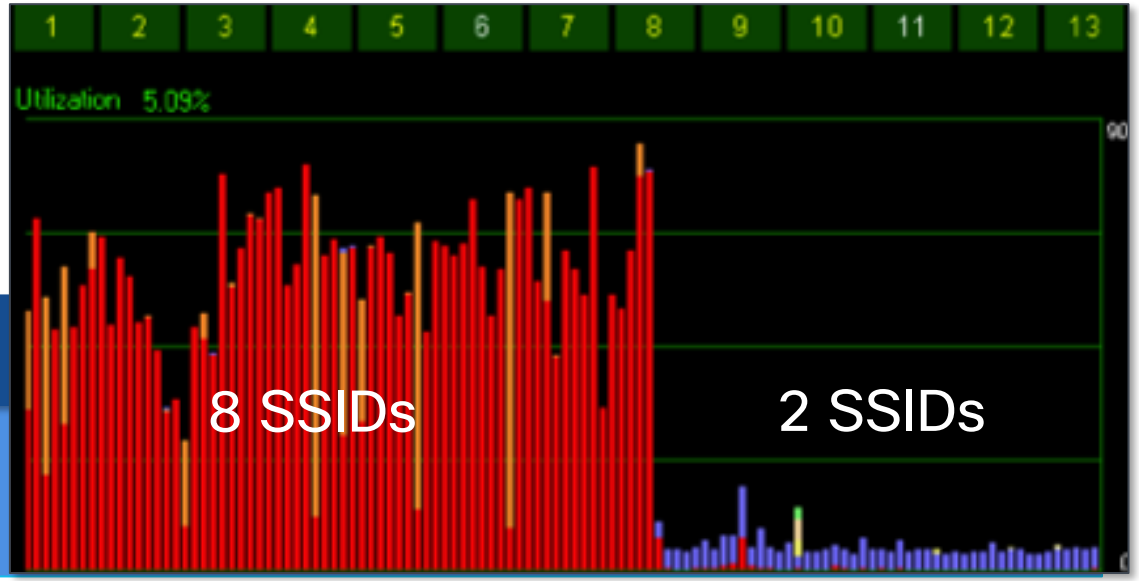
- Device Posture
- Device Type
- User Credentials
- MAC Address
- Identity Elements
  - Location
  - Day and Time
  - Access Type
  - Context

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Authorisation

Network Segmentation



Static VLAN Assignment

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

Dynamic VLAN Assignment

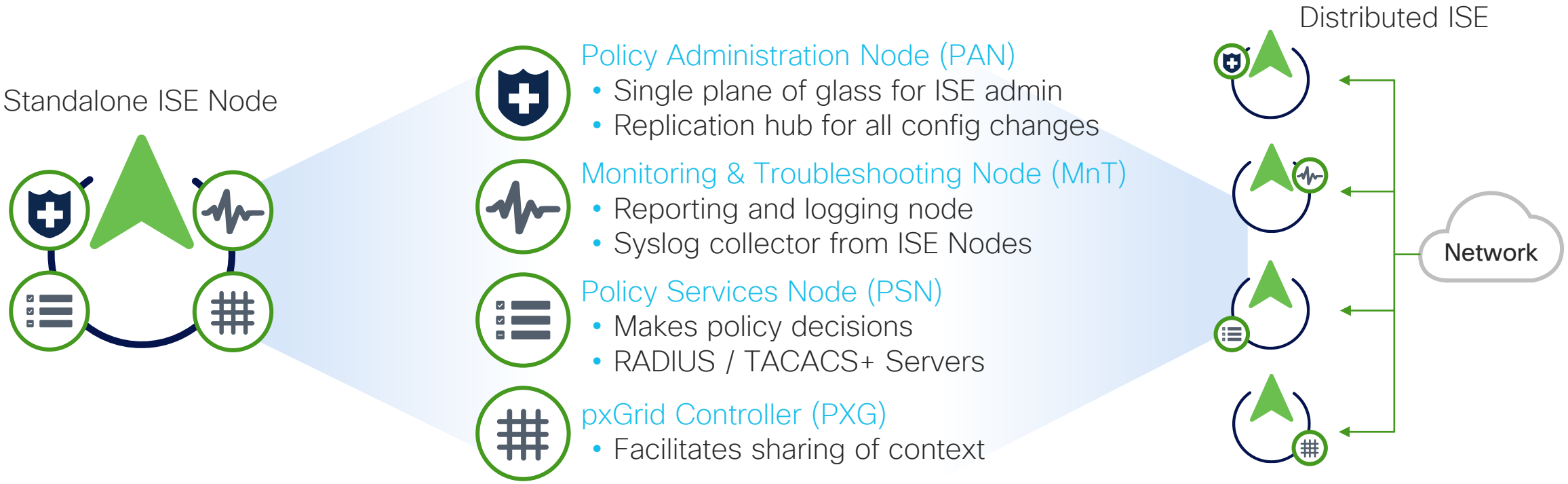
- VLAN based on authentication credentials
- VLAN segregation based on role

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)

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Personas

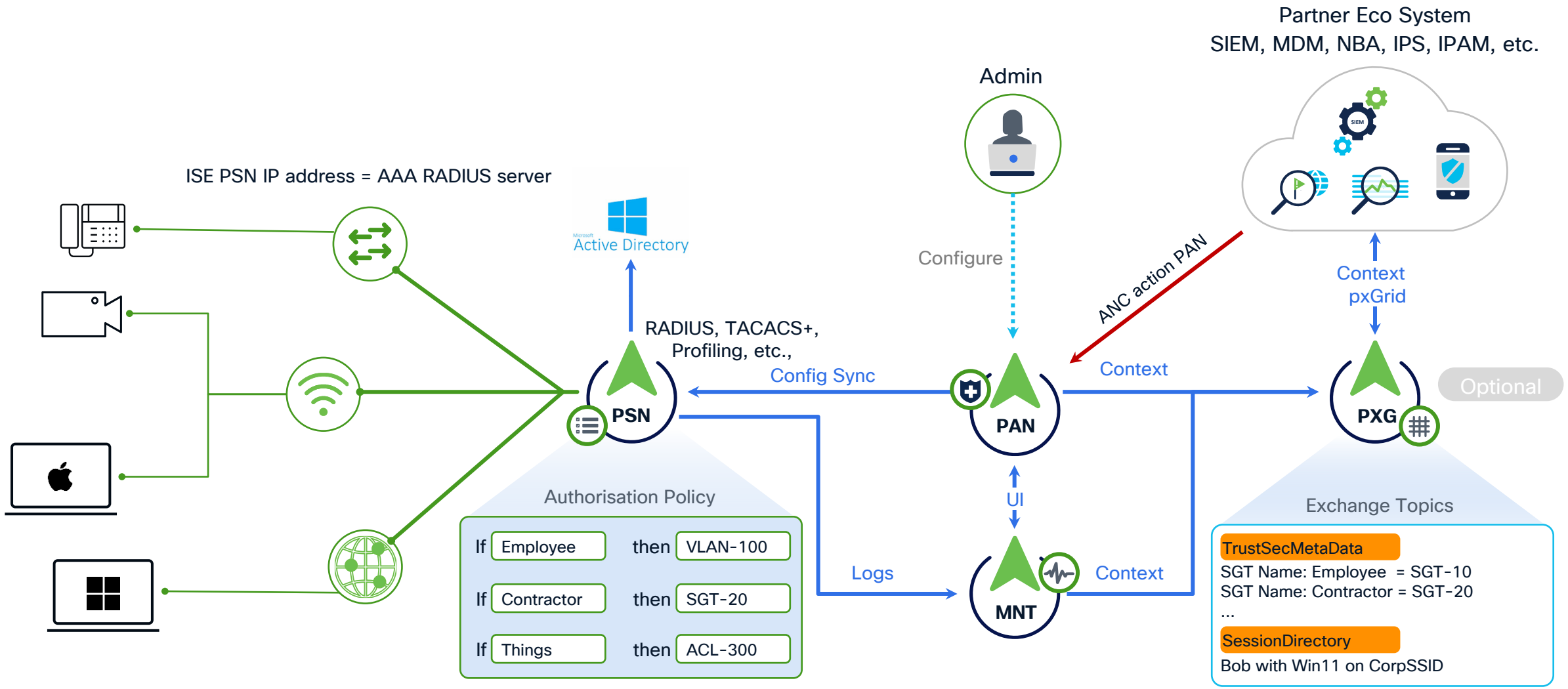


- Standalone provides no redundancy
  - Use for demo, testing, and lab purposes

https://cs.co/ise-scale

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Architecture



© 2025 Cisco and/or its affiliates. All rights reserved.

On-Prem and Cloud Identity

On-Prem Identity

802.1X, Network Access

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

Cloud Identity

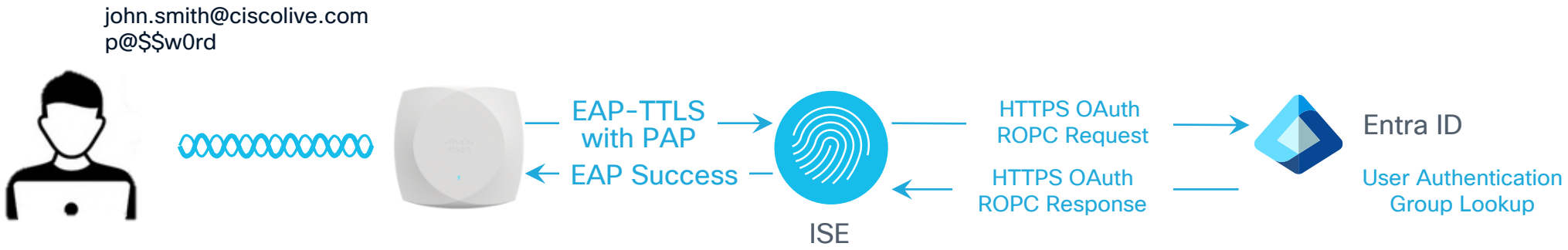
VPN, Application Access

SAMLv2, OpenID Connect

© 2025 Cisco and/or its affiliates. All rights reserved.

Cloud Identity with EAP-TTLS

> ⚠ **Warning**
>
> Microsoft recommends you do *not* use the ROPC flow. In most scenarios, more secure alternatives are available and recommended. This flow requires a very high degree of trust in the application, and carries risks that are not present in other flows. You should only use this flow when other more secure flows aren't viable.



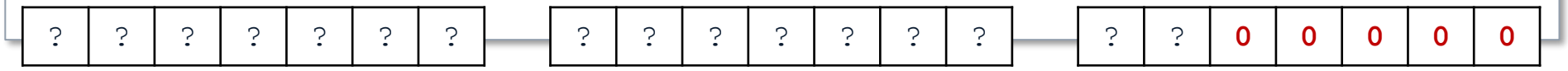
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216182-configure-ise-3-0-rest-id-with-azure-act.html

© 2025 Cisco and/or its affiliates. All rights reserved.

MS-CHAPv2 Brute Force Attack

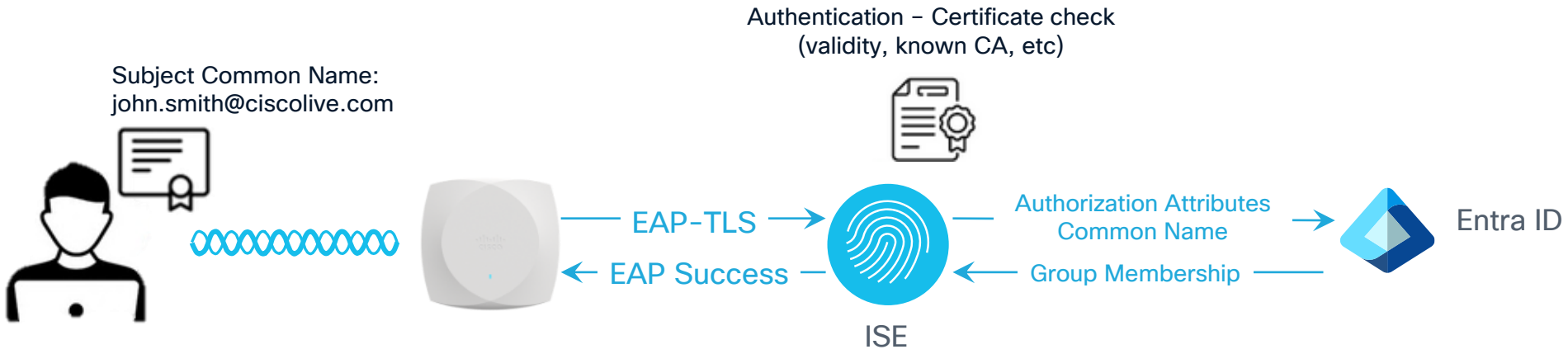
NTHash = MD4(User Password) – 16 byte value

Challenge Response = $DES_{NTHash[1:7]}$ (ChallengeHash) ||
$DES_{NTHash[8:14]}$ (ChallengeHash) ||
$DES_{NTHash[15:21]}$ (ChallengeHash)



© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Apple goto fail Bug

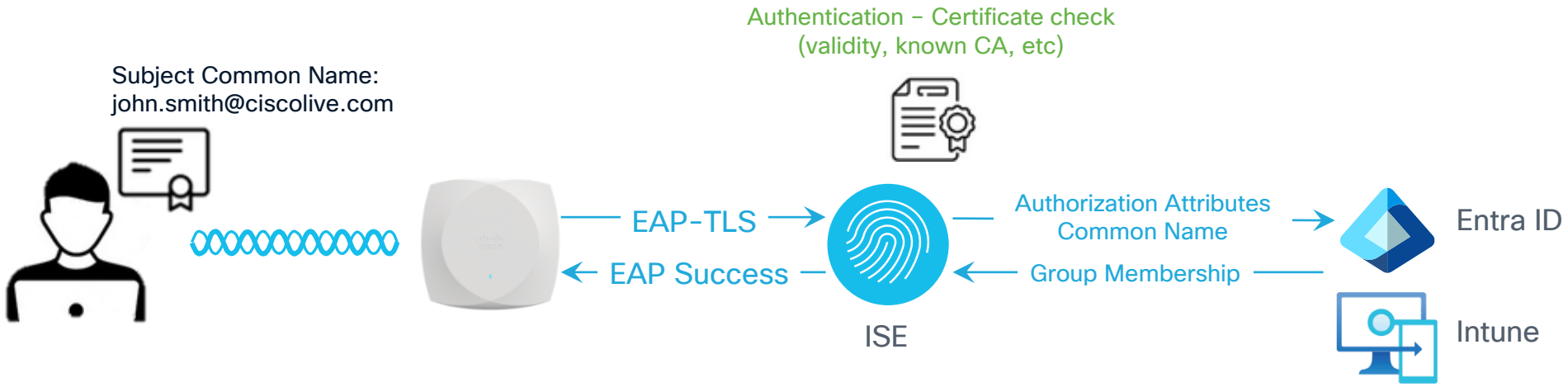
```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
        OSStatus        err;
        ...

        if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
                goto fail;
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail;
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        ...

fail:
        SSLFreeBuffer(&signedHashes);
        SSLFreeBuffer(&hashCtx);
        return err;
}
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Cloud Identity with EAP-TLS

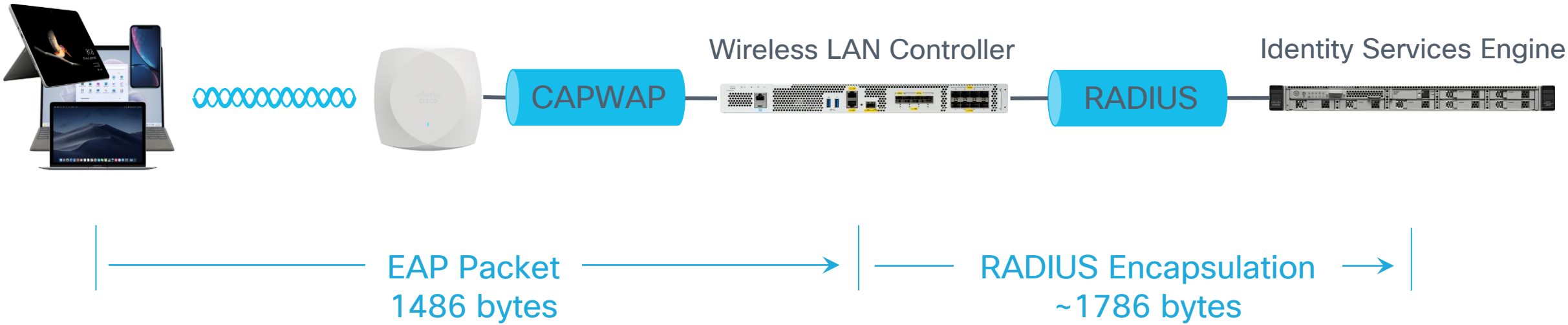


TLS 1.3 support in
ISE 3.3 patch 2 and
ISE 3.4

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

© 2025 Cisco and/or its affiliates. All rights reserved.

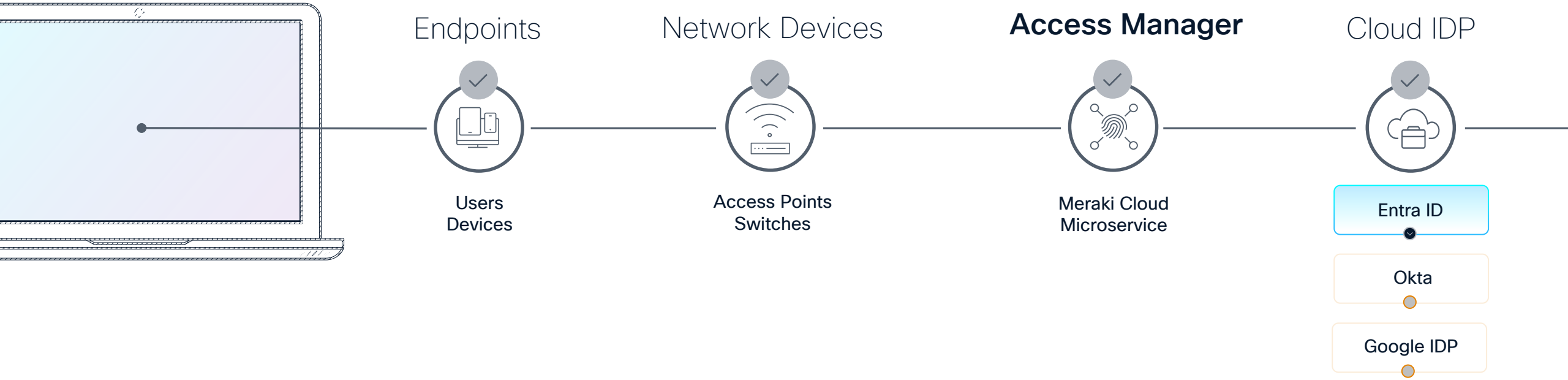
EAP-TLS to RADIUS Fragmentation



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

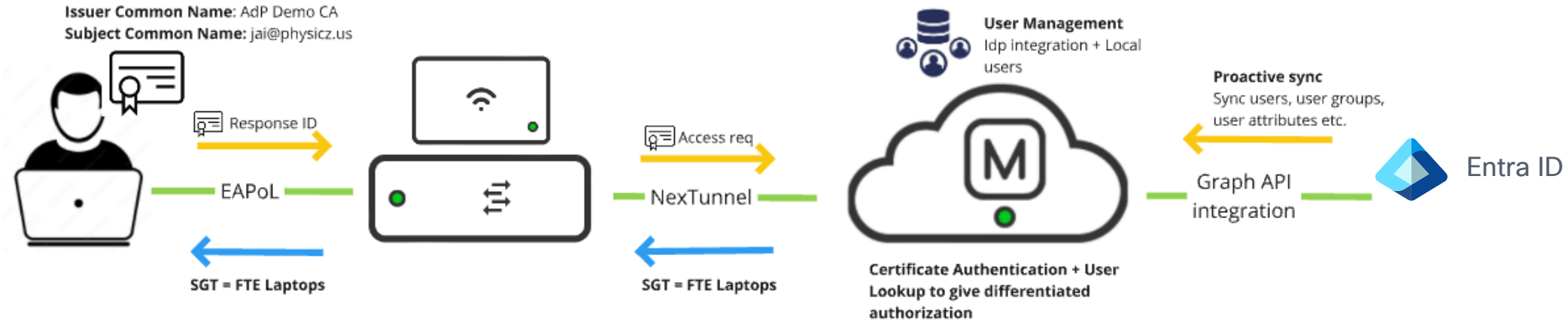
© 2025 Cisco and/or its affiliates. All rights reserved.

Access Manager



© 2025 Cisco and/or its affiliates. All rights reserved.

Access Manager and Entra ID with EAP-TLS

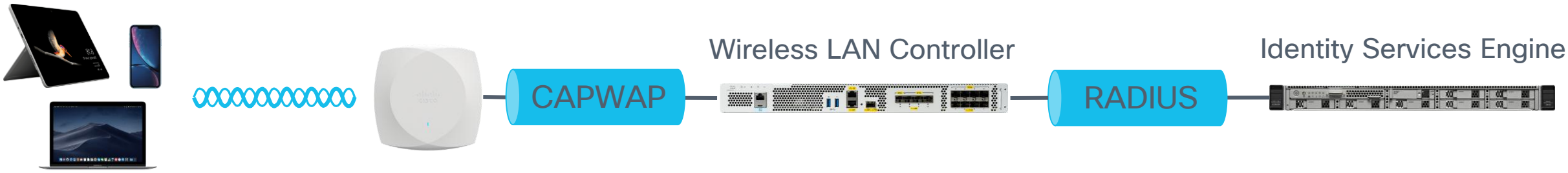


Supplicant | Authenticator | Authentication Server | Credential Server

© 2025 Cisco and/or its affiliates. All rights reserved.

Secure Fast Roaming Challenges

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



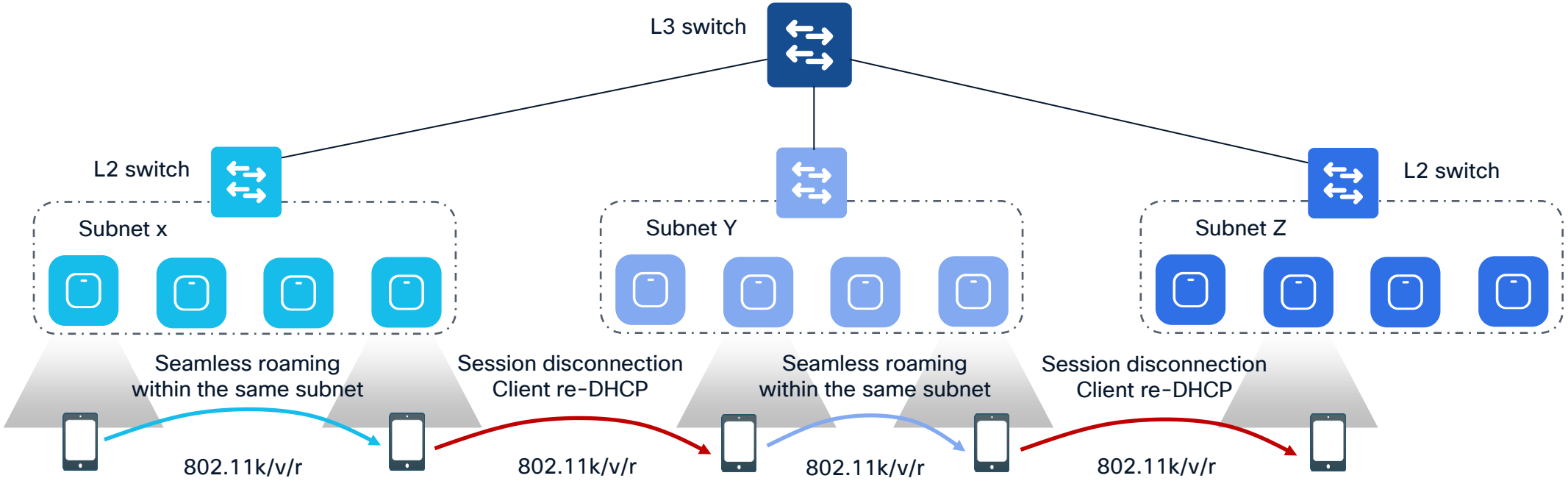
- Client channel scanning and AP selection
  - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
  - 802.11v BSS Transition
- Re-authentication of client device and re-keying
  - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

© 2025 Cisco and/or its affiliates. All rights reserved.

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

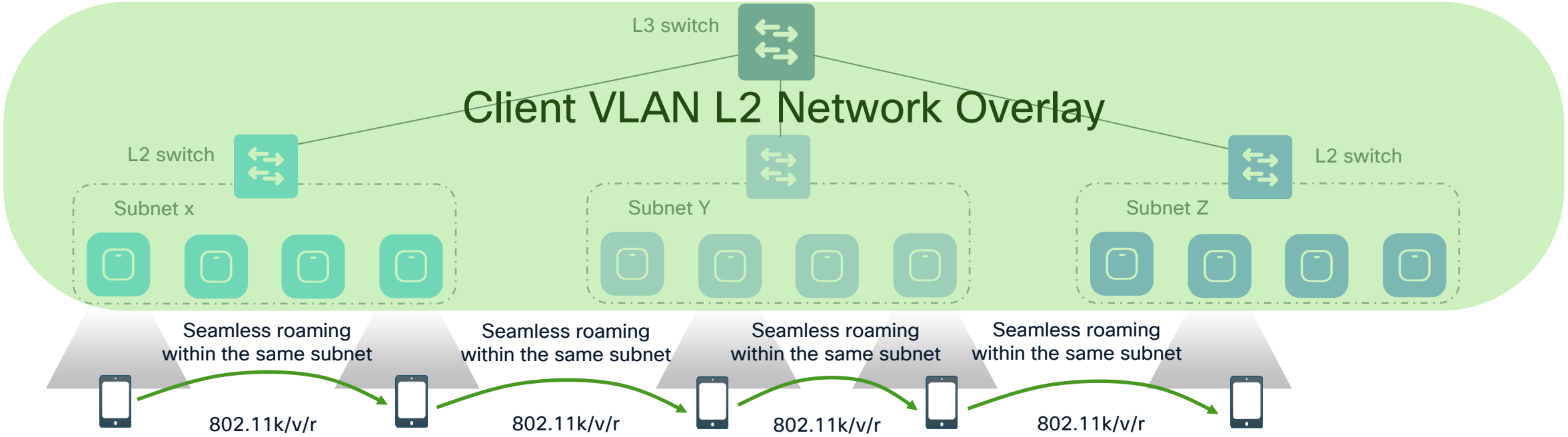


© 2025 Cisco and/or its affiliates. All rights reserved.

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

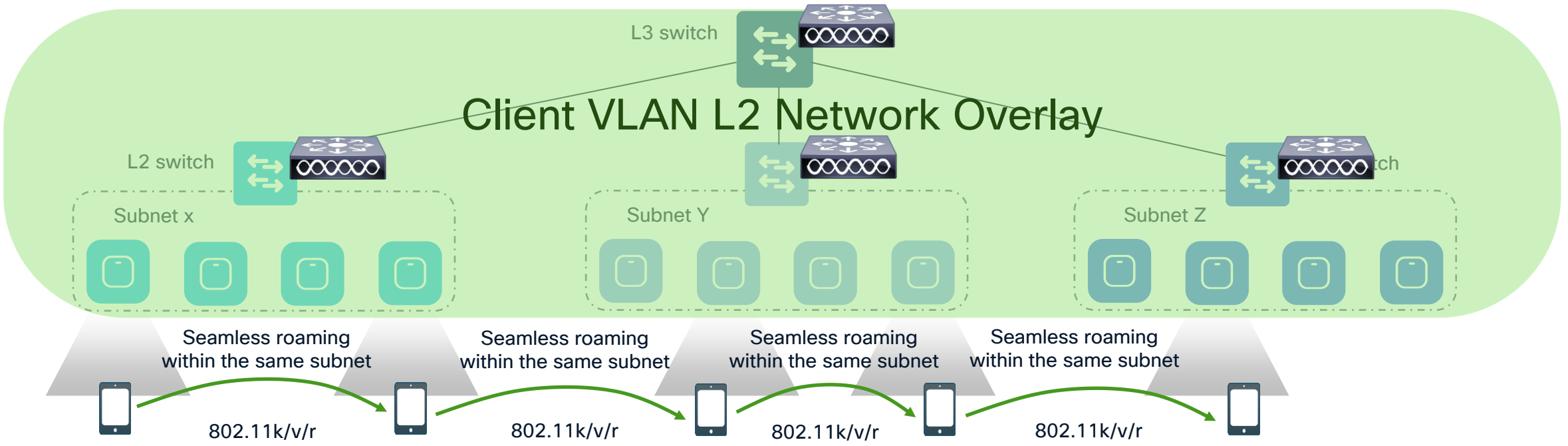


© 2025 Cisco and/or its affiliates. All rights reserved.

Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Key Reinstallation Attack

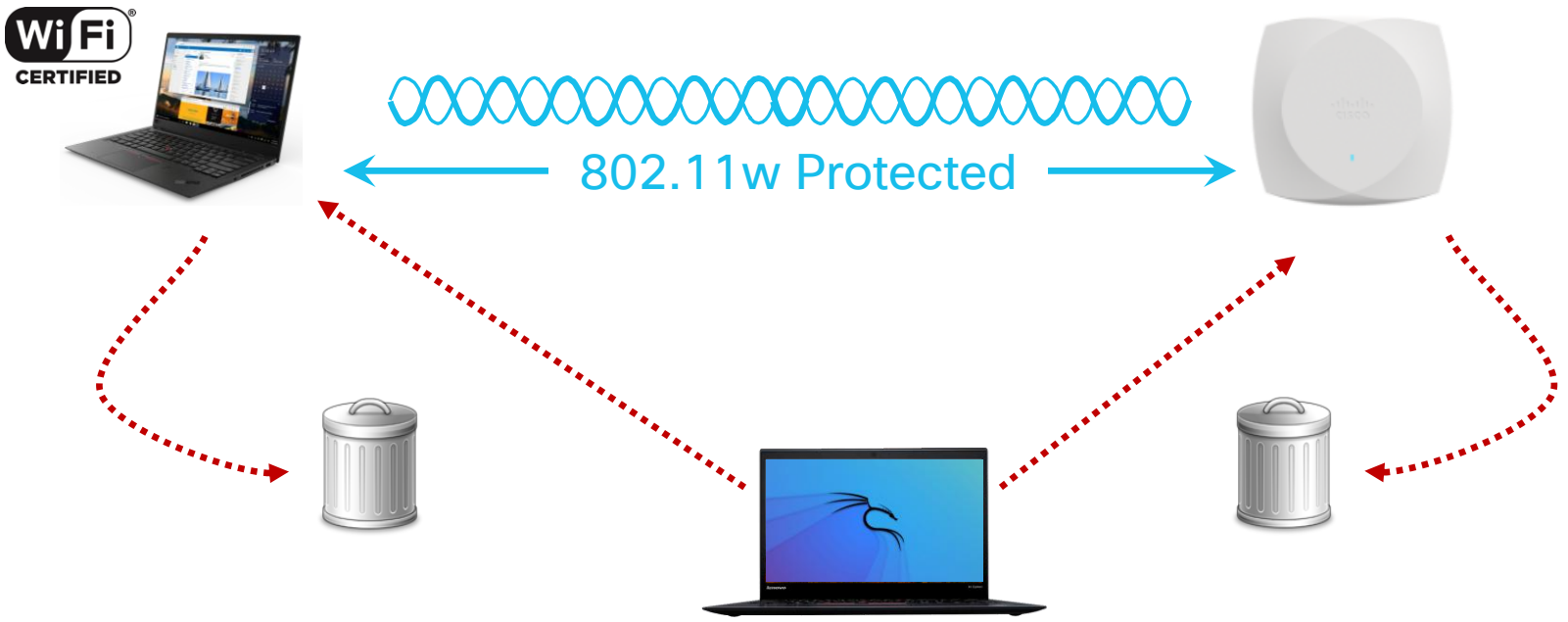
- 10 Vulnerabilities were discovered
  - May allow the reinstallation of keys already in use
- Only 1 impacts Access Points
  - Specific to 802.11r (Fast BSS Transition)
  - CVE-2017-13082

- 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

© 2025 Cisco and/or its affiliates. All rights reserved.

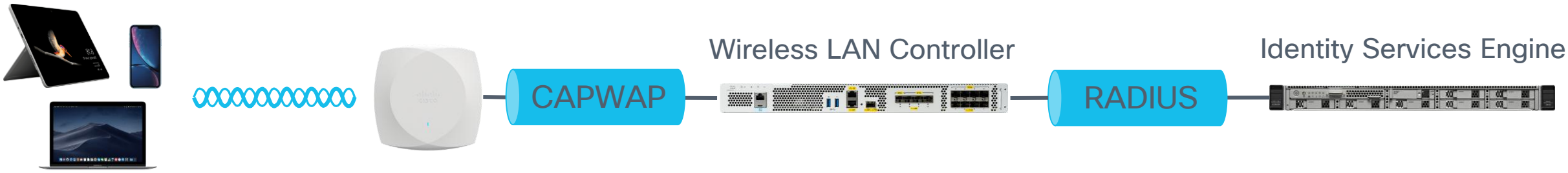
802.11w Protected Management Frames



© 2025 Cisco and/or its affiliates. All rights reserved.

Central Web Authentication

URL Redirect



Any Packet → RADIUS Access Request →

← RADIUS Access Accept

Network Access Granted
Redirect ACL

HTTP Packet → Redirect to ISE Web Page →

← Web Authentication Sequence →

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

← RADIUS CoA Request

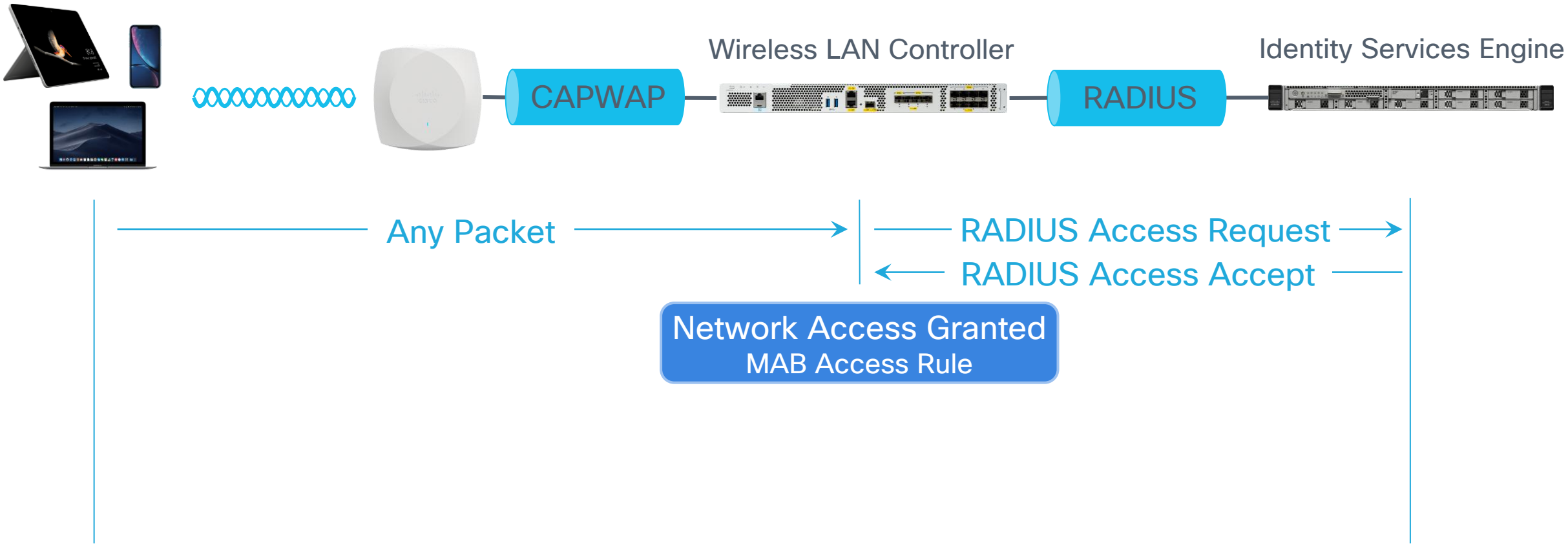
RADIUS CoA ACK →

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Central Web Authentication

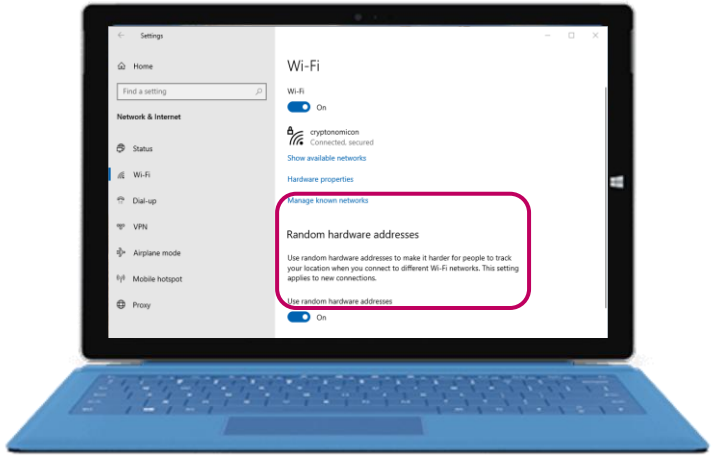
MAC Authentication Bypass

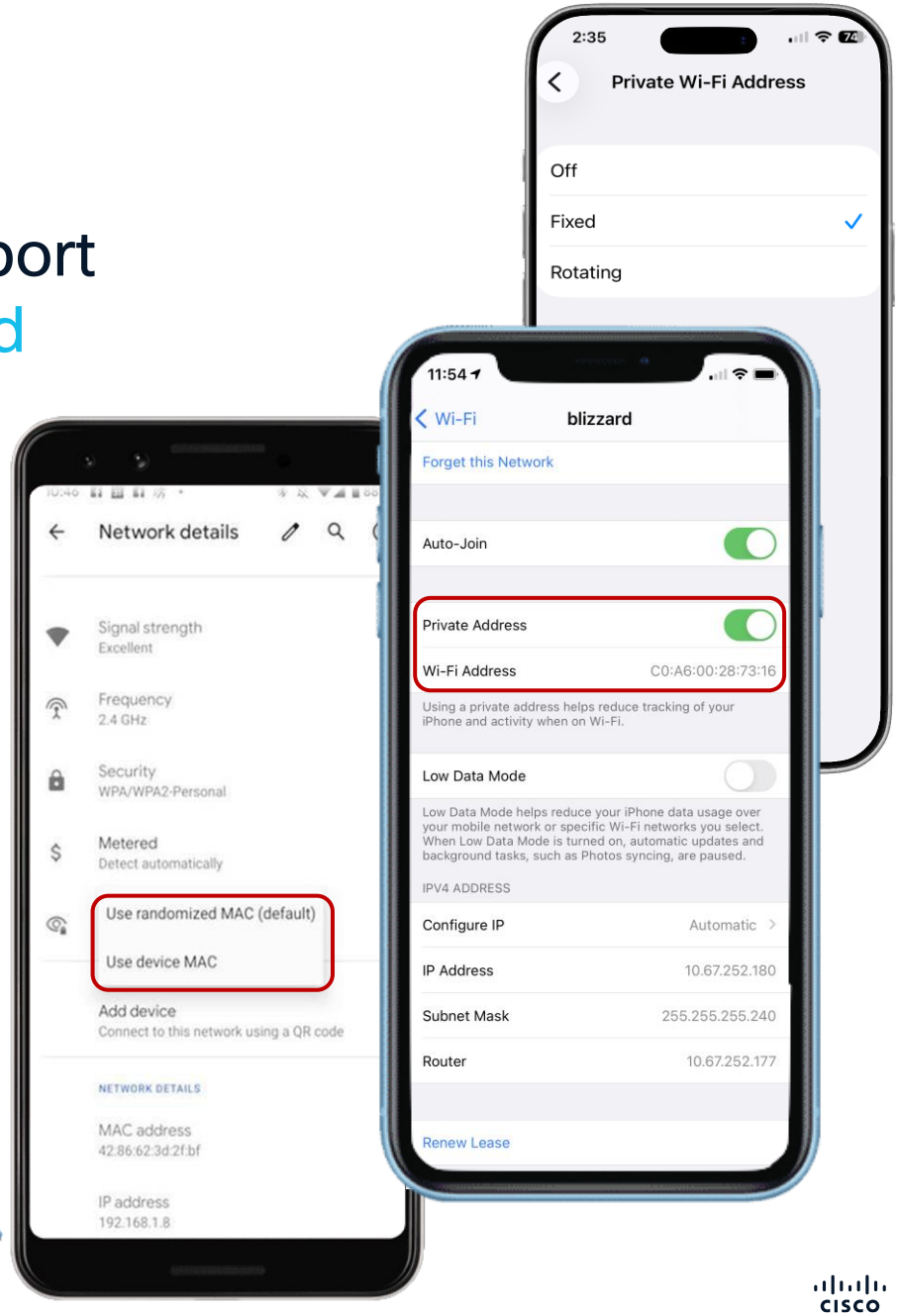


© 2025 Cisco and/or its affiliates. All rights reserved.

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
  - The 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





© 2025 Cisco and/or its affiliates. All rights reserved.

Wi-Fi Certified Enhanced Open

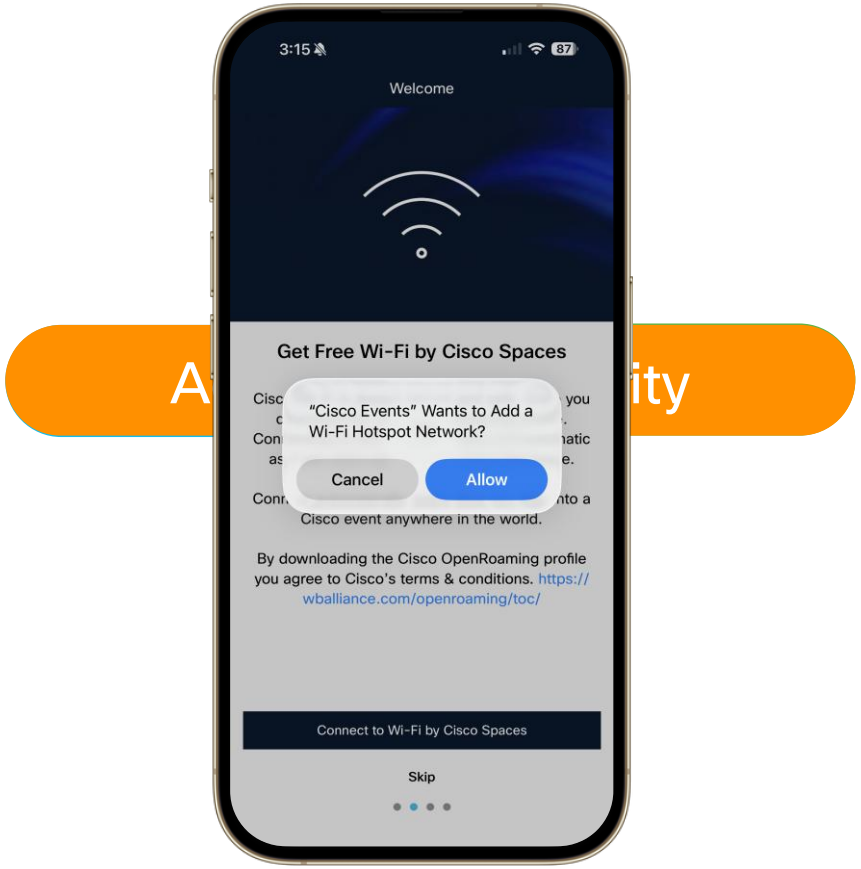
WPA3

- Opp istic Wireless Encryption (OWE)
  - Re ” authentication support
  - Cli ticated Diffie-Hellman Key Exchange to establish a
  - Four-Way Handshake u
  - Supports Protected Management Fr
- Diffie-Hellman is susceptible to MitM attack
  - Would allow the attacker same visibility as on an Open netwo

Man charged over creation of 'evil twin' free WiFi networks to access personal data

© 2025 Cisco and/or its affiliates. All rights reserved.

Decoupling Access and Identity



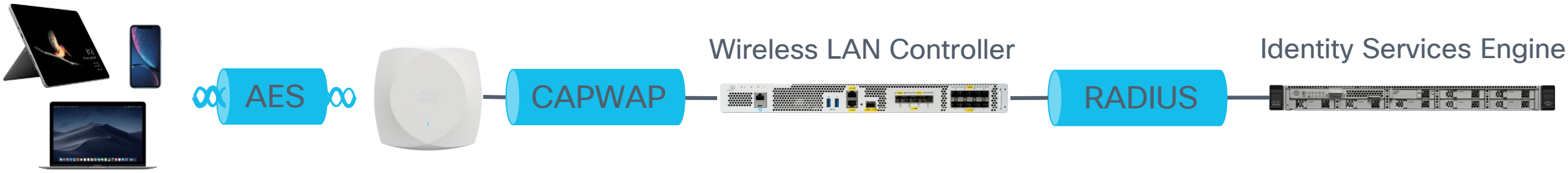
© 2025 Cisco and/or its affiliates. All rights reserved.

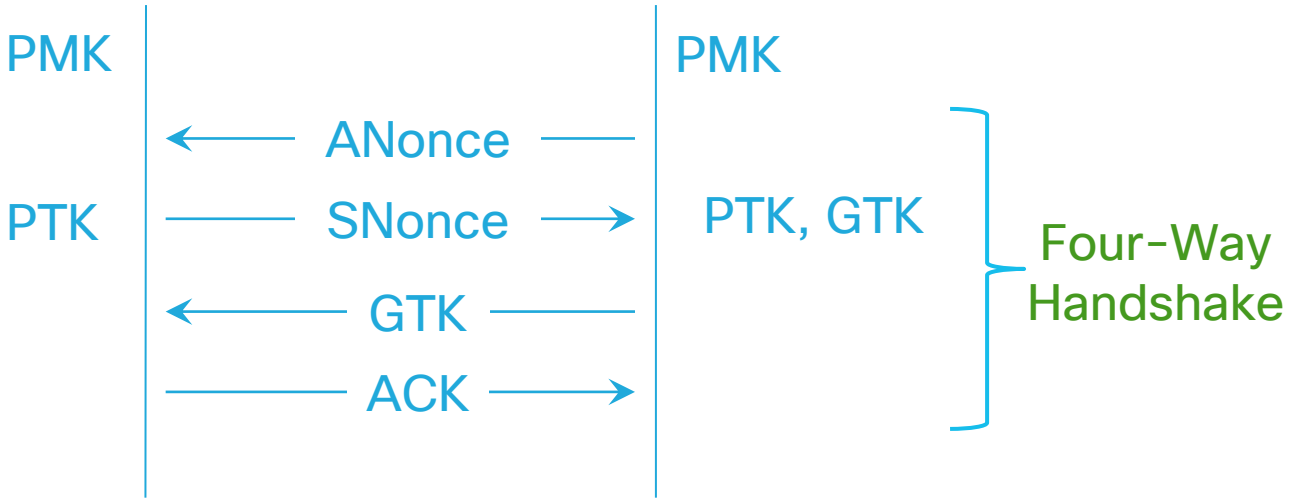
OpenRoaming

© 2025 Cisco and/or its affiliates. All rights reserved.

WPA Personal

Pre-Shared Key



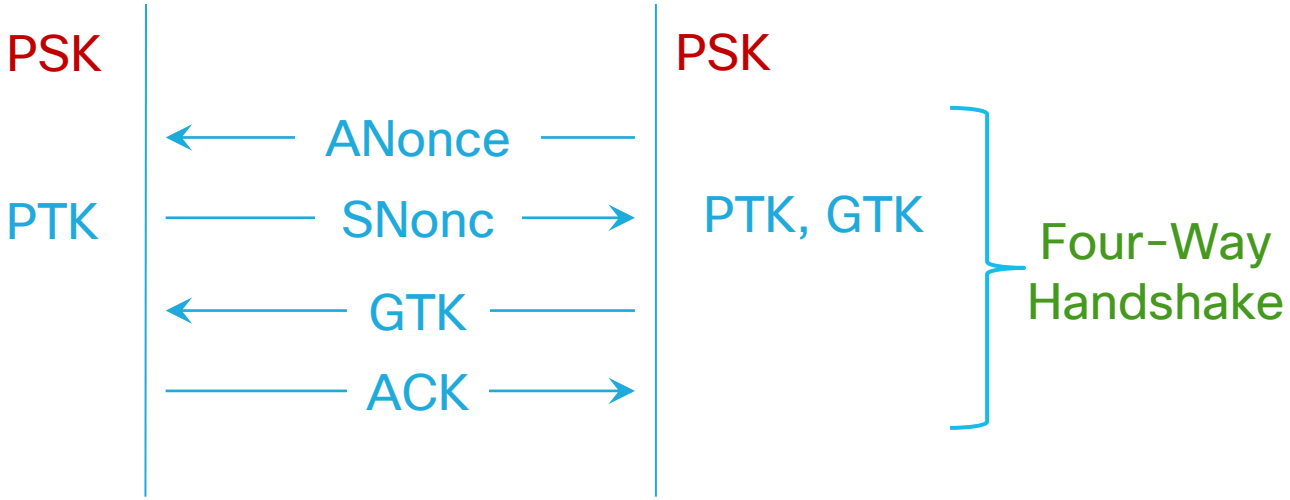


PTK = SHA(PMK + ANonce + SNonce + AP MAC + STA MAC)

© 2025 Cisco and/or its affiliates. All rights reserved.

WPA Personal

Pre-Shared Key



Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

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	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

Read more and download at hivesystems.com/password

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

© 2025 Cisco and/or its affiliates. All rights reserved.

© 2025 Cisco and/or its affiliates. All rights reserved.

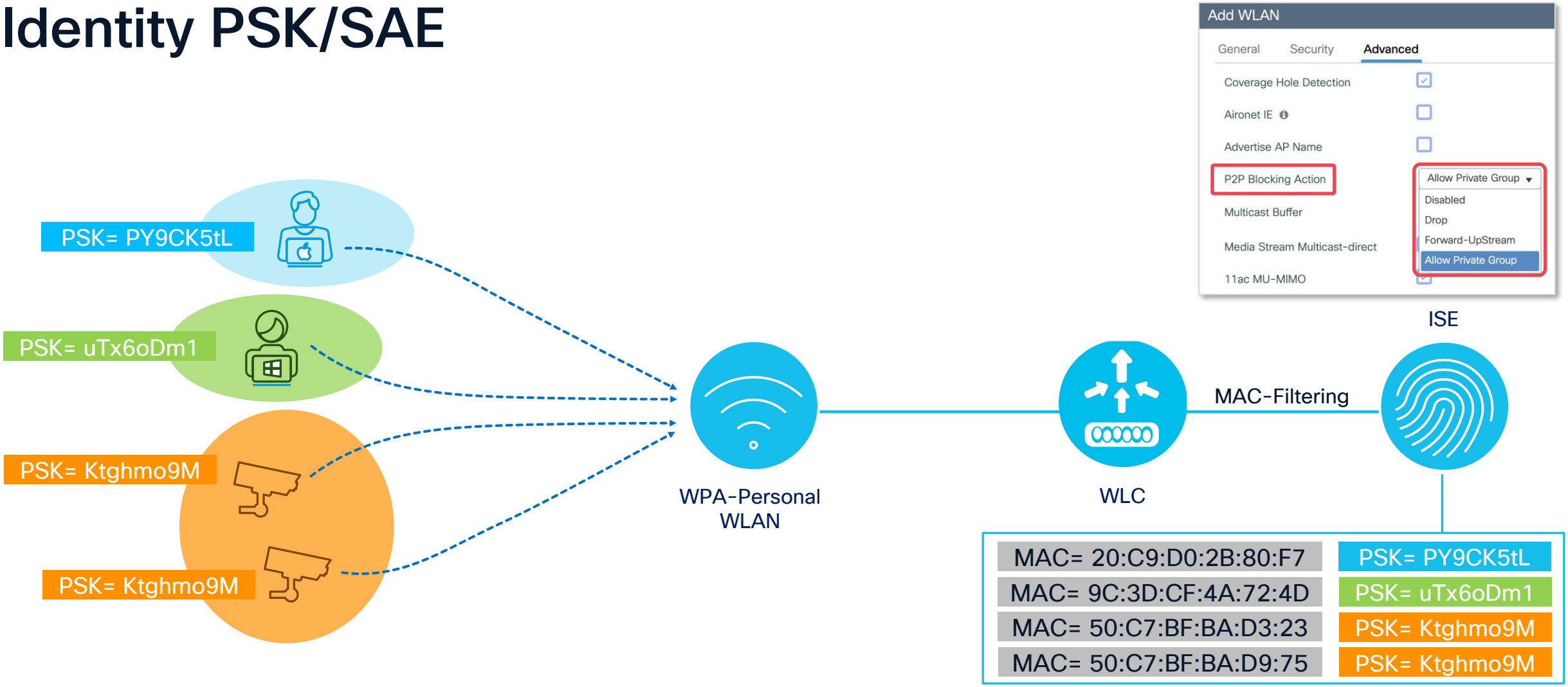
Simultaneous Authentication of Equals

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 attempt to prevent WPA3-Personal clients from downgrading to WPA2-Personal on roams mitigating downgrade attacks

© 2025 Cisco and/or its affiliates. All rights reserved.

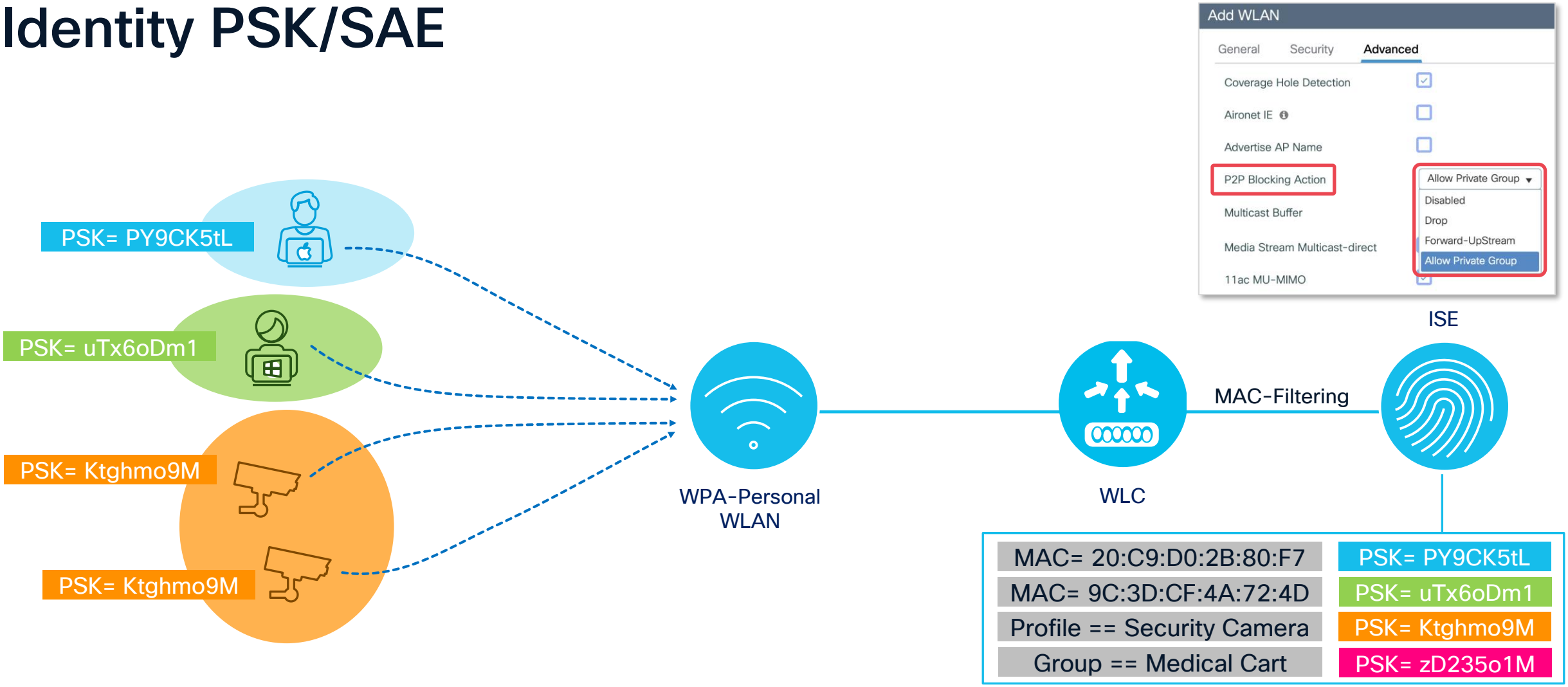
Identity PSK/SAE



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

© 2025 Cisco and/or its affiliates. All rights reserved.

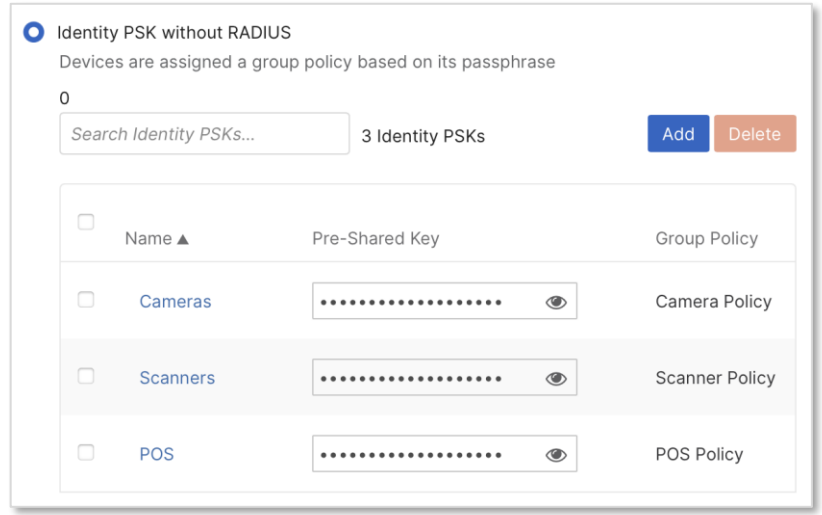
Identity PSK/SAE

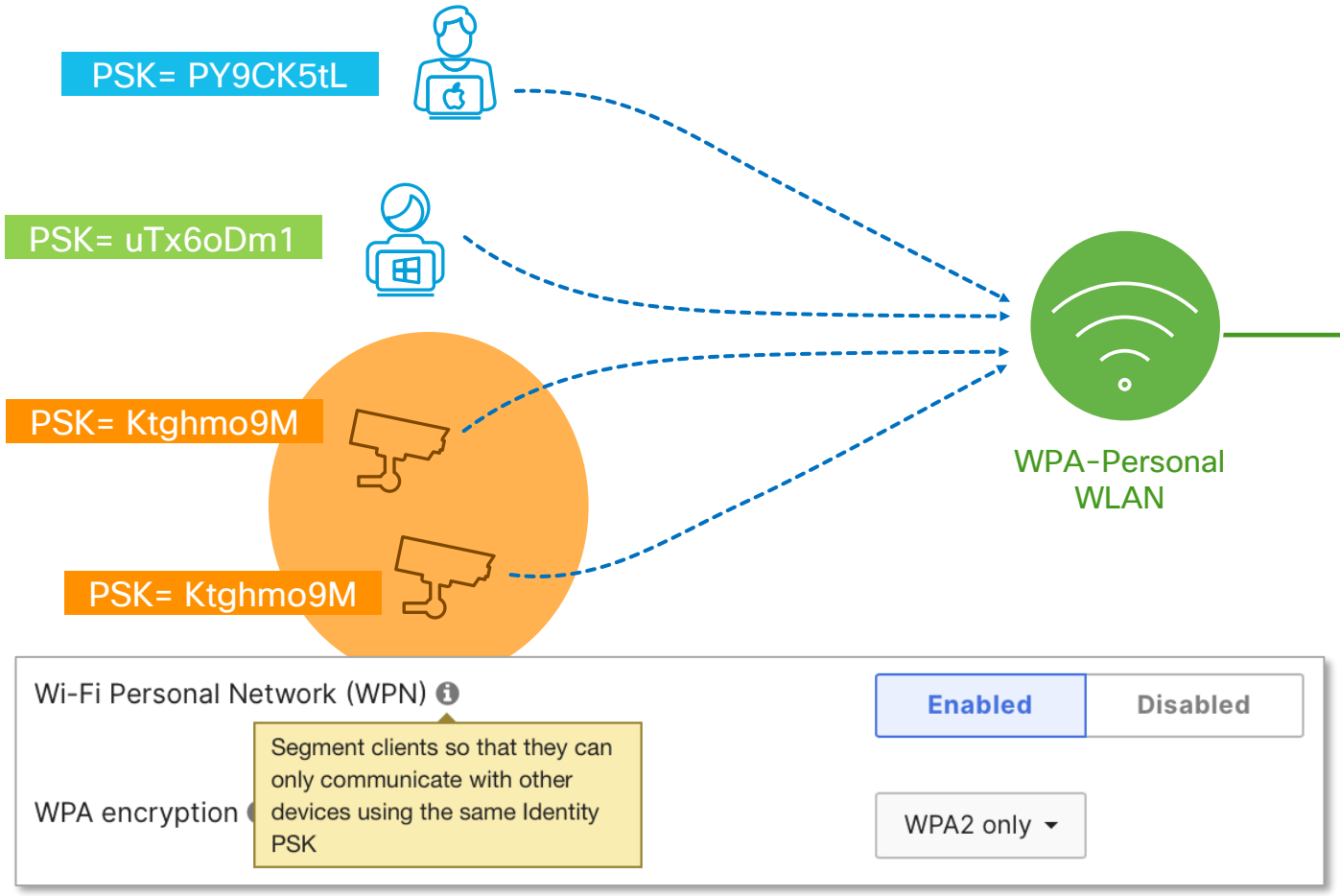


https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

© 2025 Cisco and/or its affiliates. All rights reserved.

Identity PSK without RADIUS





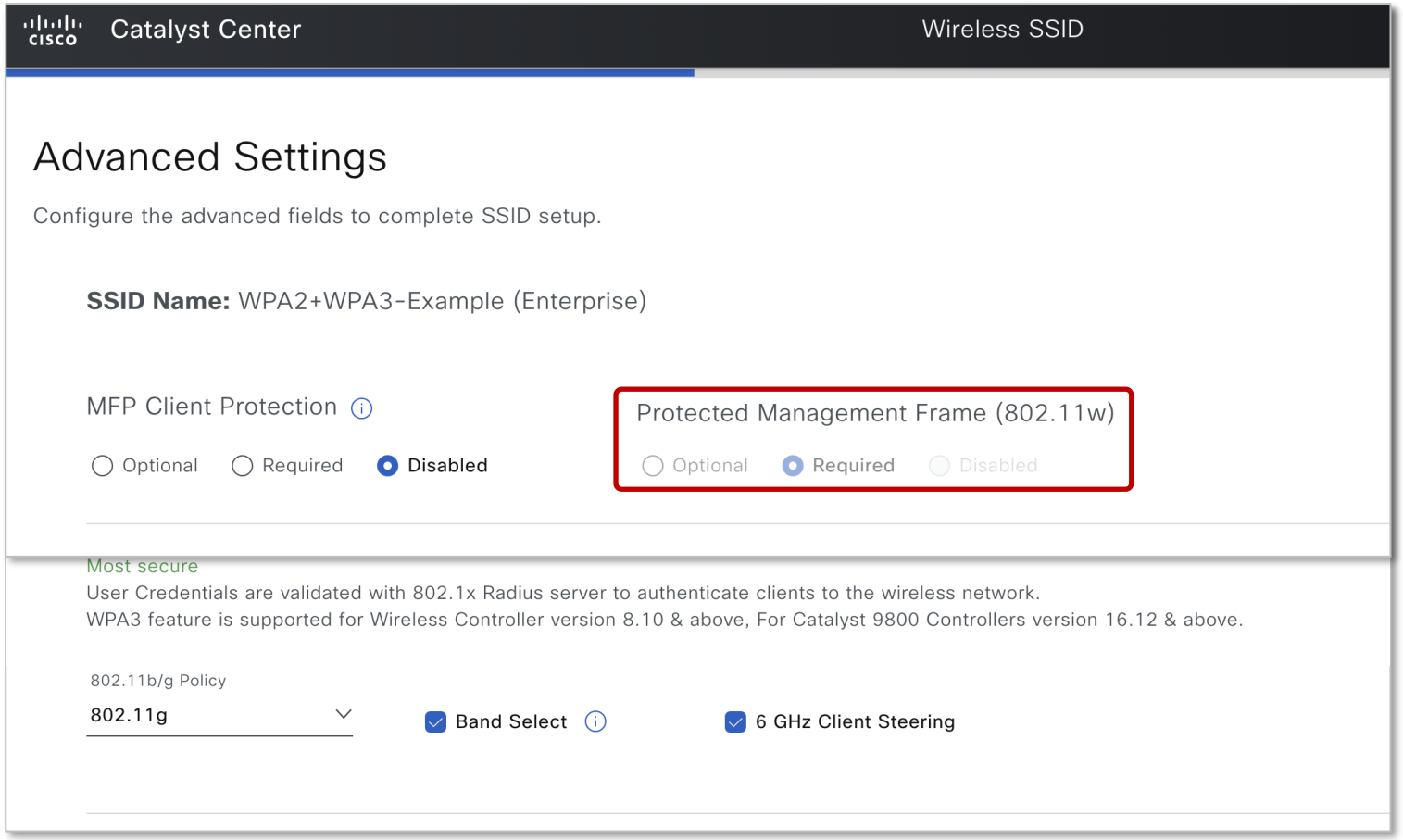
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_Authentication_without_RADIUS

© 2025 Cisco and/or its affiliates. All rights reserved.

Security Implications of 6GHz

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

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



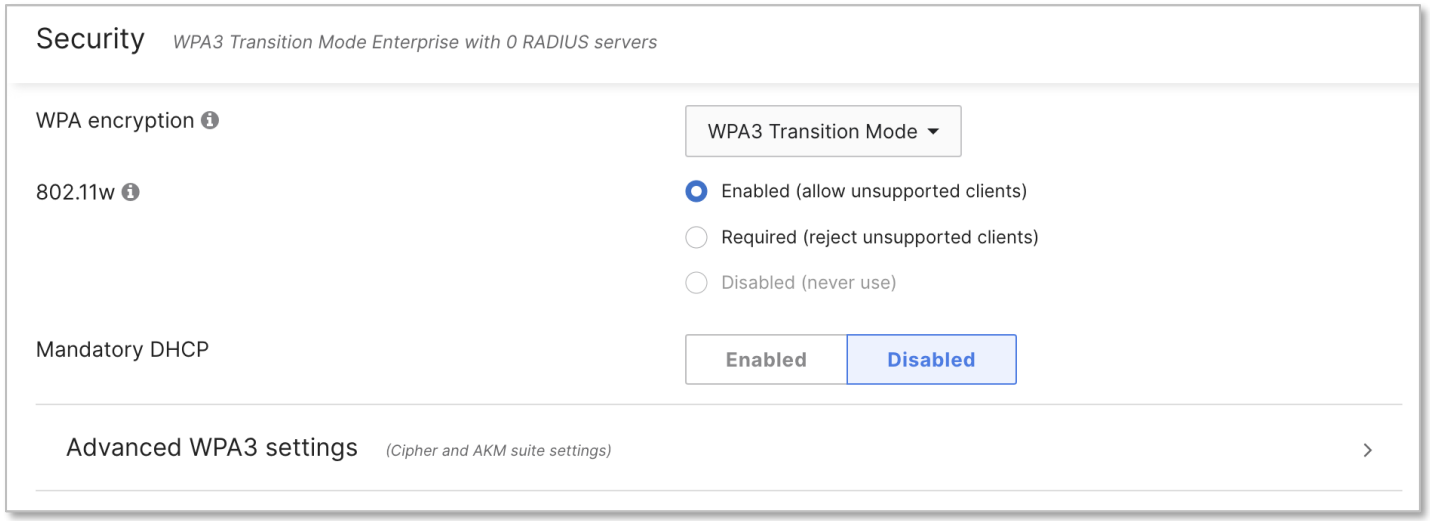
From IOS-XE 17.12.1

© 2025 Cisco and/or its affiliates. All rights reserved.

Security Implications of 6GHz

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

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



From Meraki 31.X

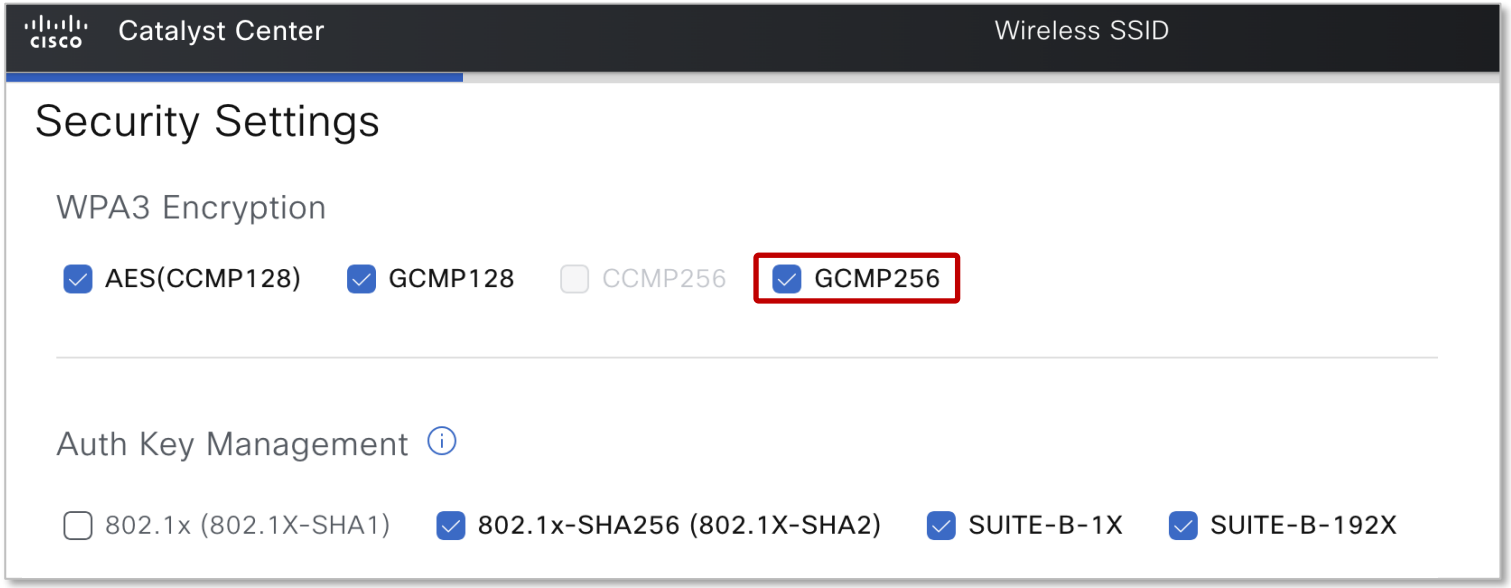
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

© 2025 Cisco and/or its affiliates. All rights reserved.

Security Implications of Wi-Fi 7

Wi-Fi 7 brings new AKM and cipher suite requirements

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



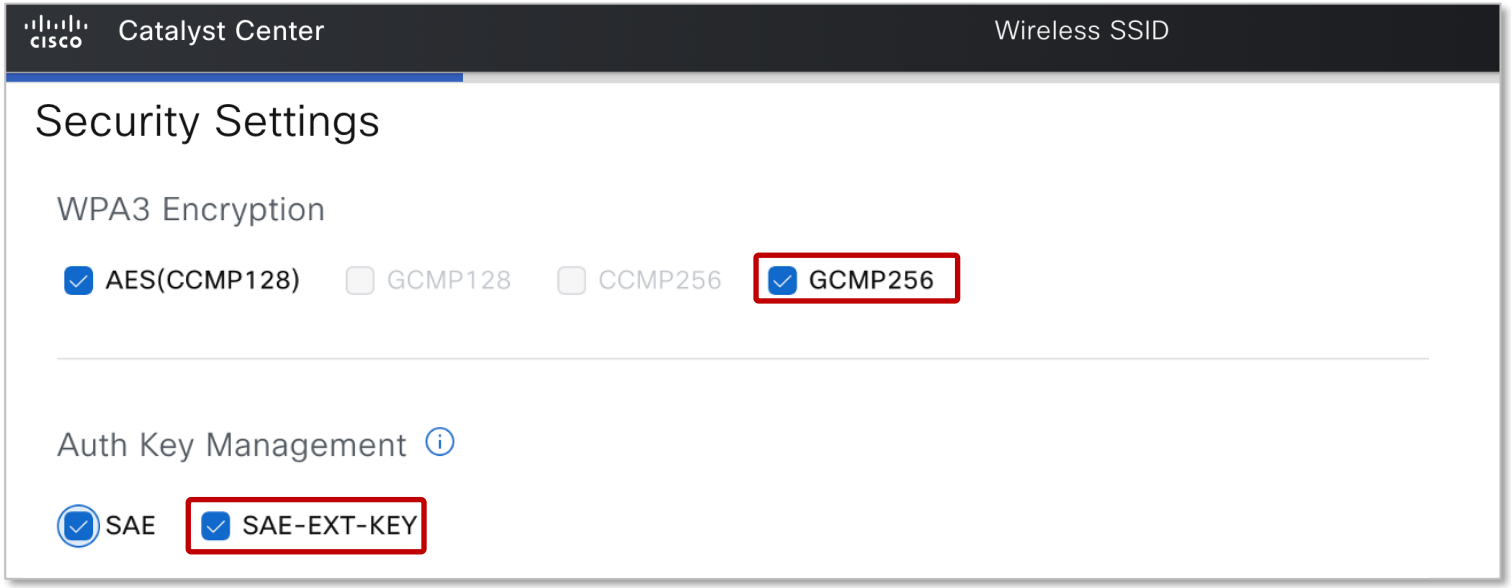
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_wpa3_security_enhancements.html

© 2025 Cisco and/or its affiliates. All rights reserved.

Security Implications of Wi-Fi 7

Wi-Fi 7 brings new AKM and cipher suite requirements

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



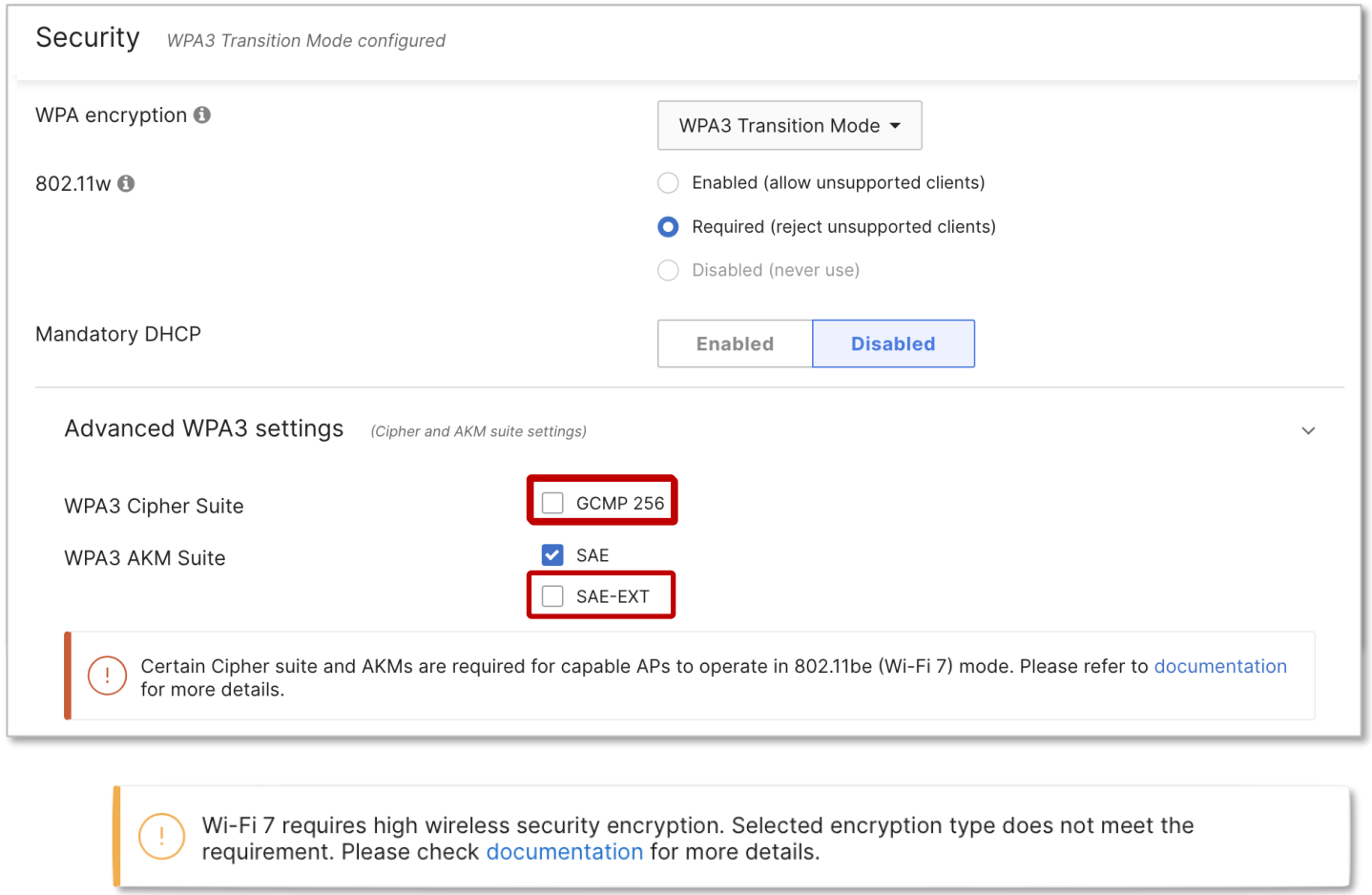
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_wpa3_security_enhancements.html

© 2025 Cisco and/or its affiliates. All rights reserved.

Security Implications of Wi-Fi 7

Wi-Fi 7 brings new AKM and cipher suite requirements

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



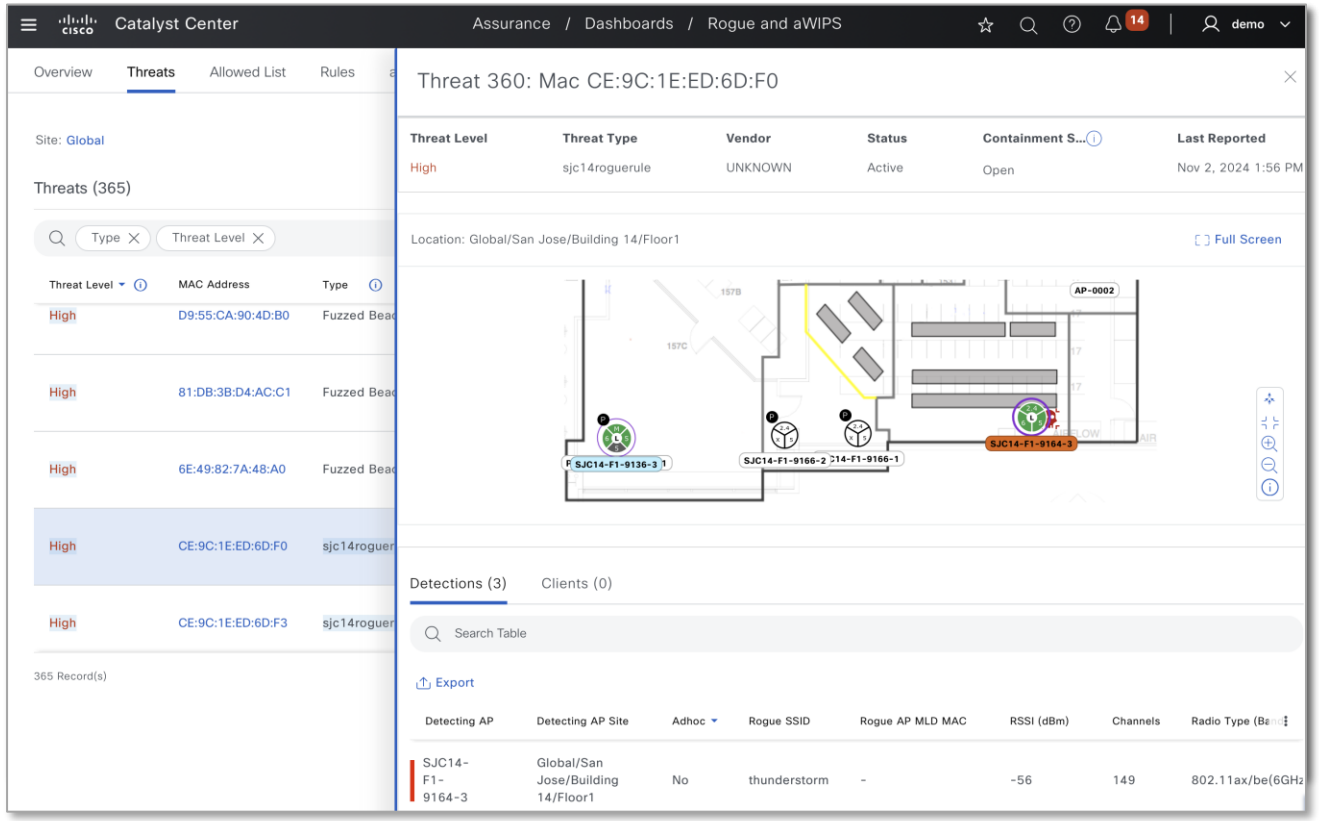
© 2025 Cisco and/or its affiliates. All rights reserved.

Wireless Intrusion Detection and Prevention

cisco Live !

Rogue Detection and Advanced WIPS

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

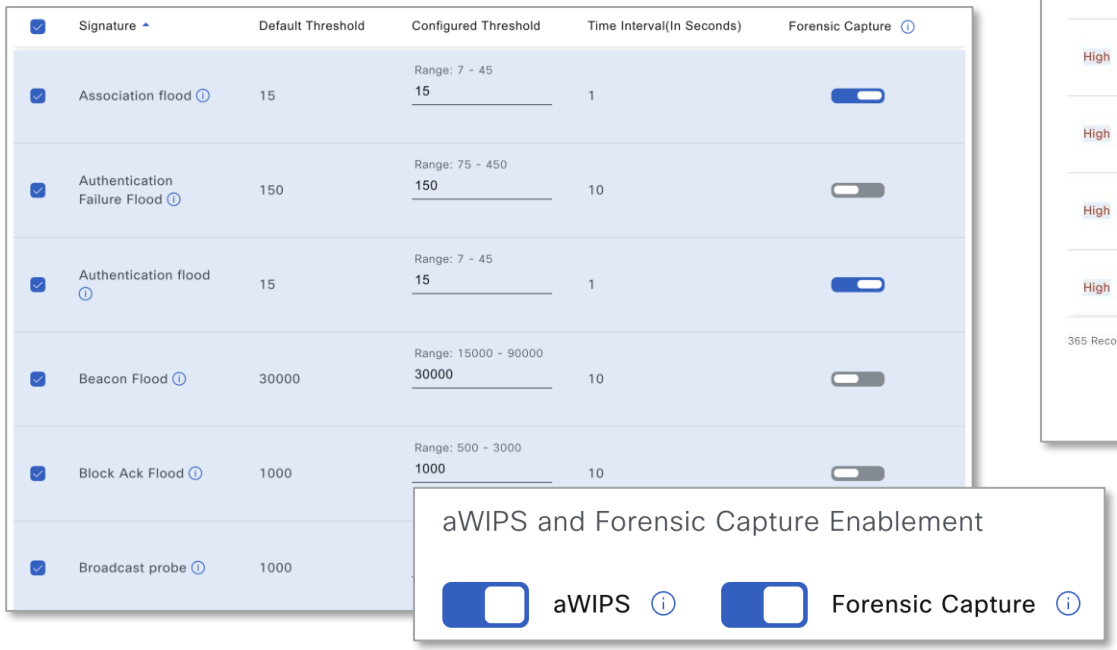


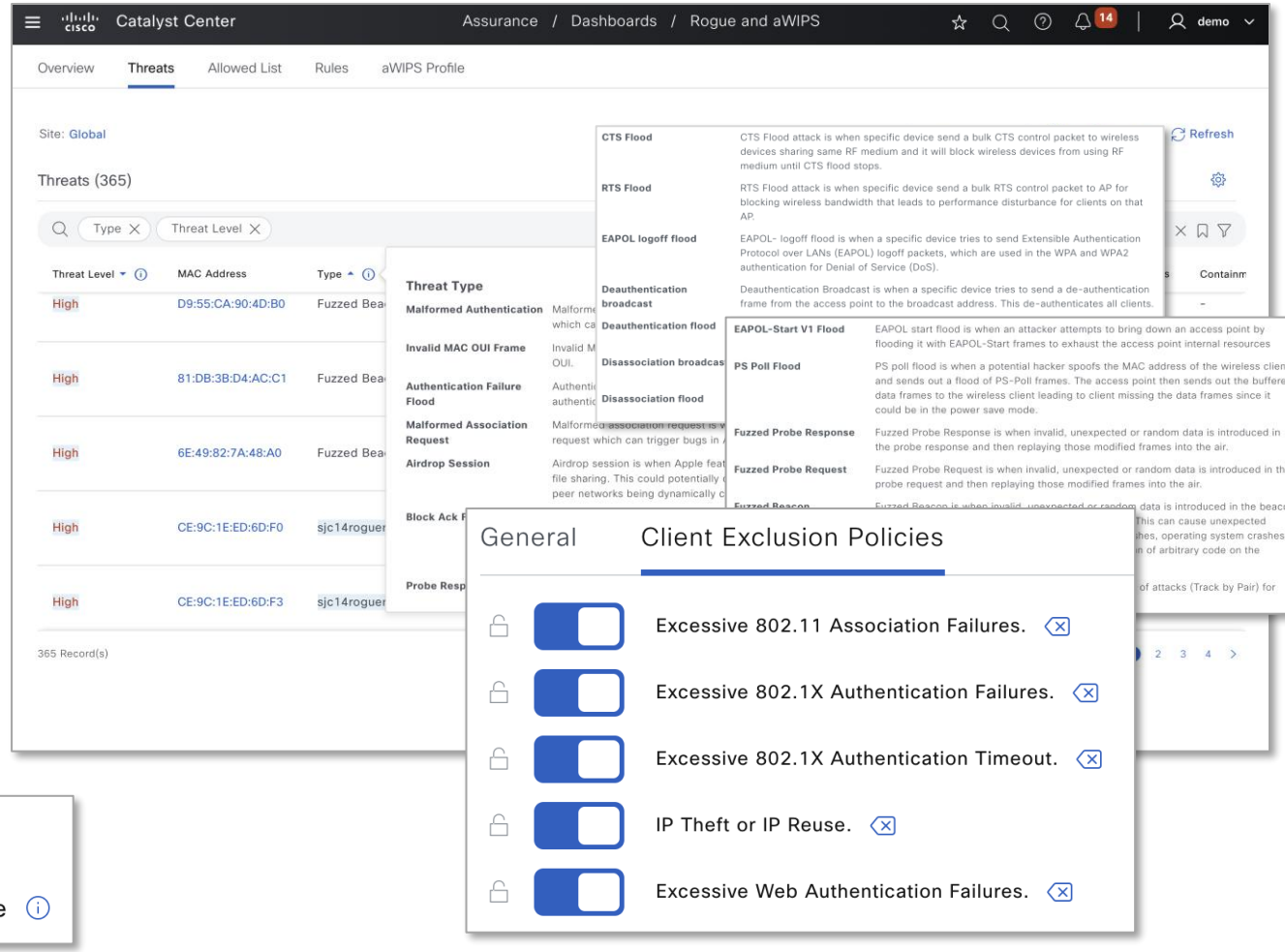
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/catalyst-center-rogue-management-application/2-3-7/quick-start-guide/b_rogue_management_qsg_2_3_7/rogue_management_chapter_01.html

© 2025 Cisco and/or its affiliates. All rights reserved.

Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies

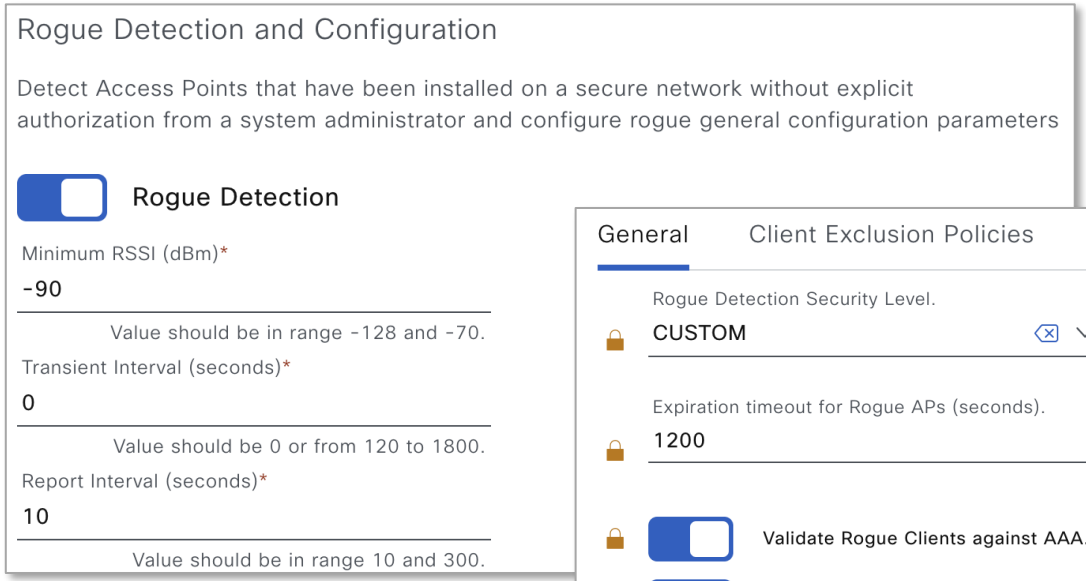


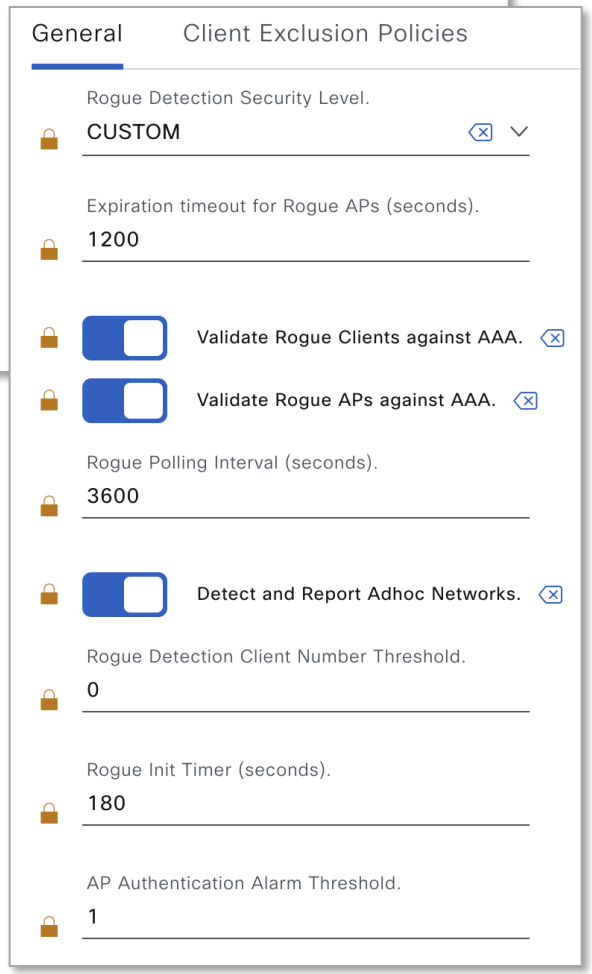


© 2025 Cisco and/or its affiliates. All rights reserved.

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 key

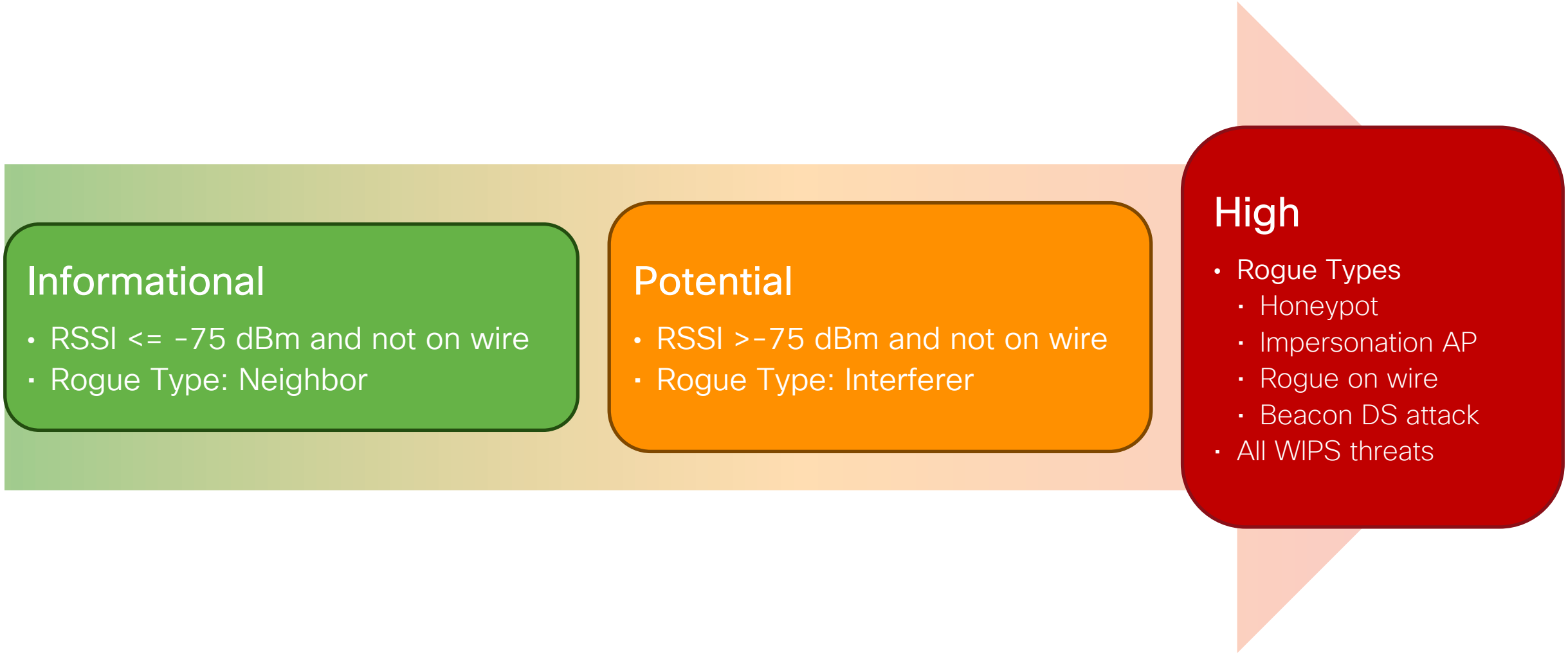




Allowed List	AP MAC addresses that are in the allowed list are known AP and so are not considered as malicious.
Friendly	Friendly APs belong to one wireless controller and are seen as a Rogue AP by another wireless controller, where both wireless controllers are managed by Catalyst Center.
Neighbor	Neighbor APs are Rogue APs with signal strength less than or equal to -75dBm and are not broadcasting any corporate SSIDs.

© 2025 Cisco and/or its affiliates. All rights reserved.

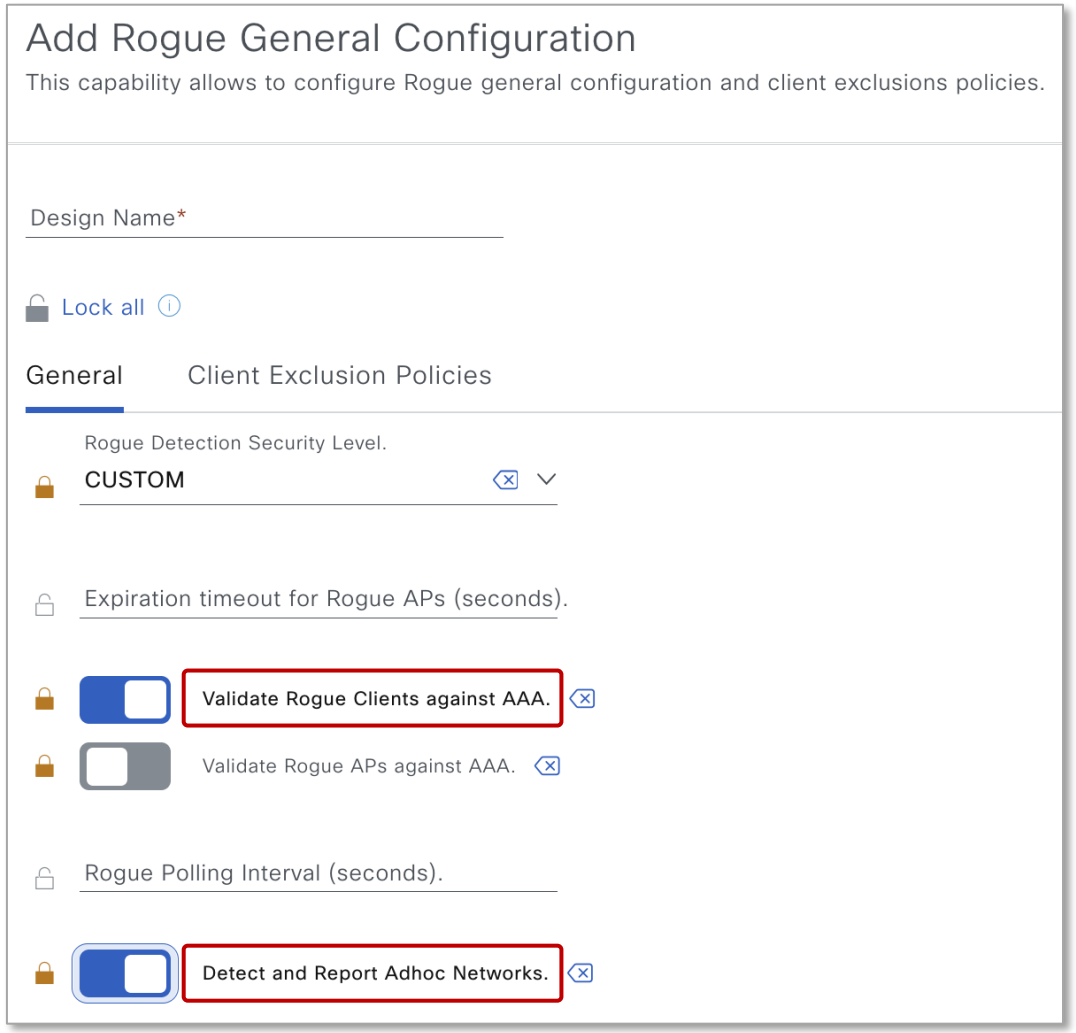
Cisco Catalyst Centre Threat Levels



© 2025 Cisco and/or its affiliates. All rights reserved.

Rogue Clients

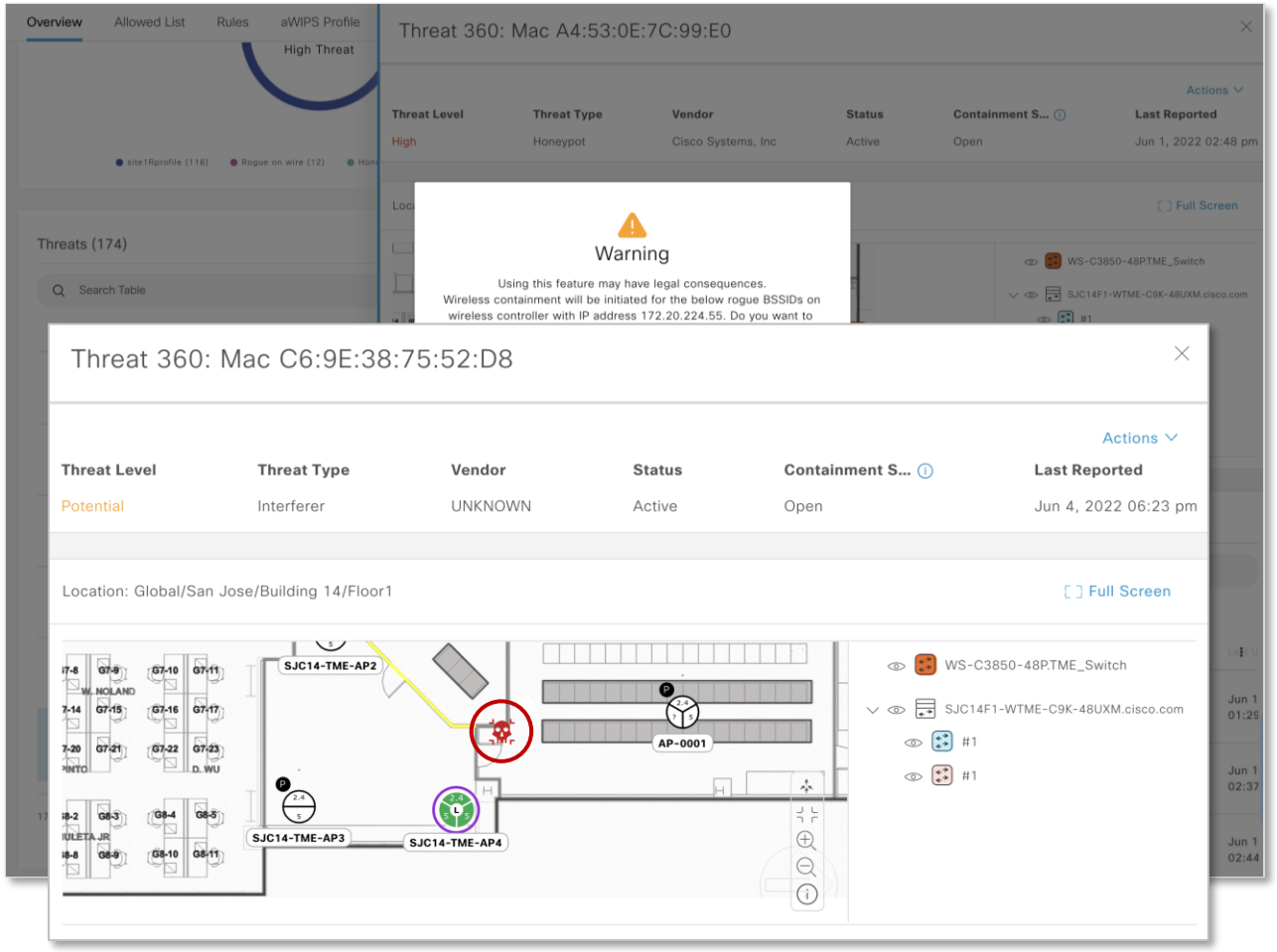
- A Rogue Client is any client which is connected to a Rogue AP
  - What we care about are our clients which have connected to the Rogue AP
  - But this is not necessarily a risk
- Clients may create ad-hoc wireless networks
  - This can be a risk if they have bridged to the wired network



© 2025 Cisco and/or its affiliates. All rights reserved.

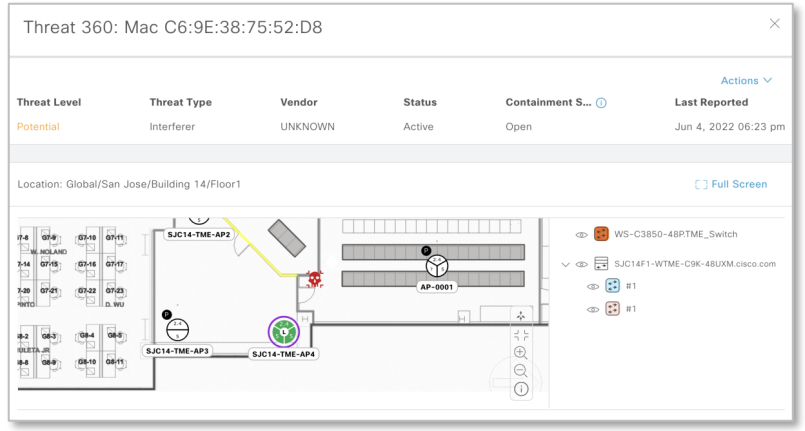
Rogue AP Containment

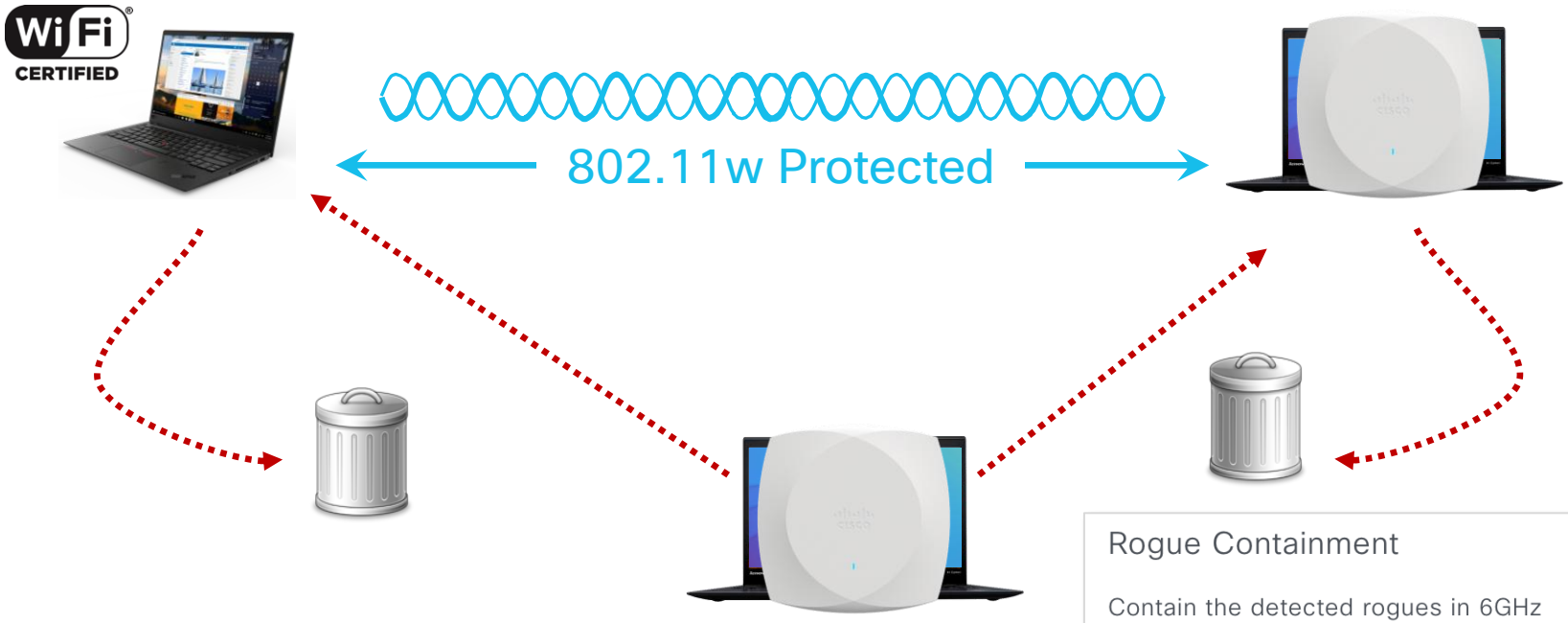
- How do we contain Rogue APs?
  - Containment is a spoofed 802.11 disassociation/deauthentication request attack
- How does WPA3 affect Rogue AP containment?
  - 802.11w will change how we can mitigate Rogue AP related threats
  - The ability to physically locate rogues is critical



© 2025 Cisco and/or its affiliates. All rights reserved.

Rogue Containment with WPA3





Rogue Containment

Contain the detected rogues in 6GHz

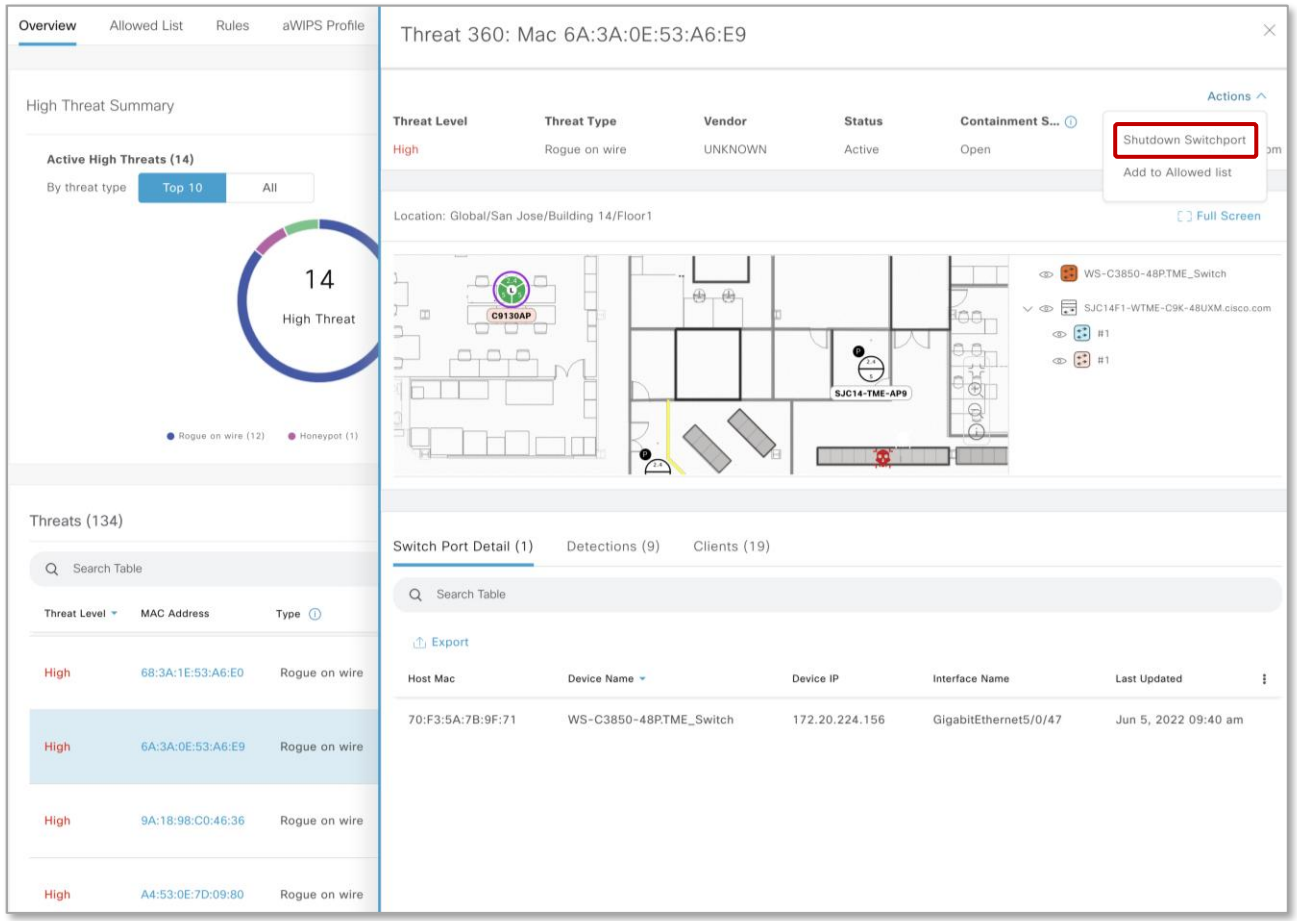
PMF Denial

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Rogue on Wire

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

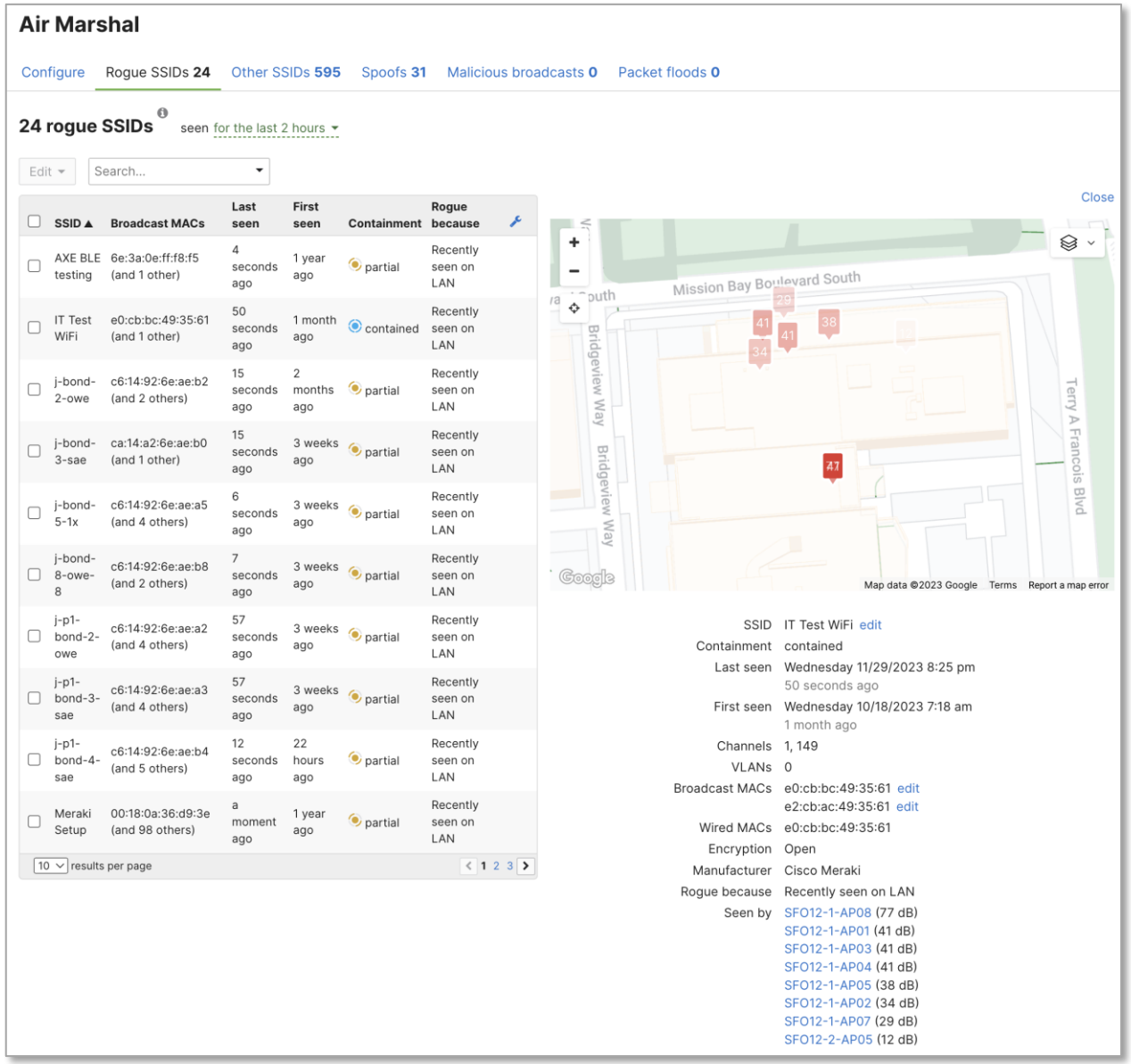


© 2025 Cisco and/or its affiliates. All rights reserved.

Air Marshal

- Rogue AP Detection
  - Rogue Containment
  - Wired Rogue
- WIDS/WIPS
  - Spoofed Management Frames
  - Malicious Broadcasts / DoS
  - Packet Floods
- Rogue detection support has been extended beyond the regulatory domain of the network
  - Alerts are generated for rogue APs broadcasting on unauthorized 2.4 and 5 GHz radio channels

From MR 31.X

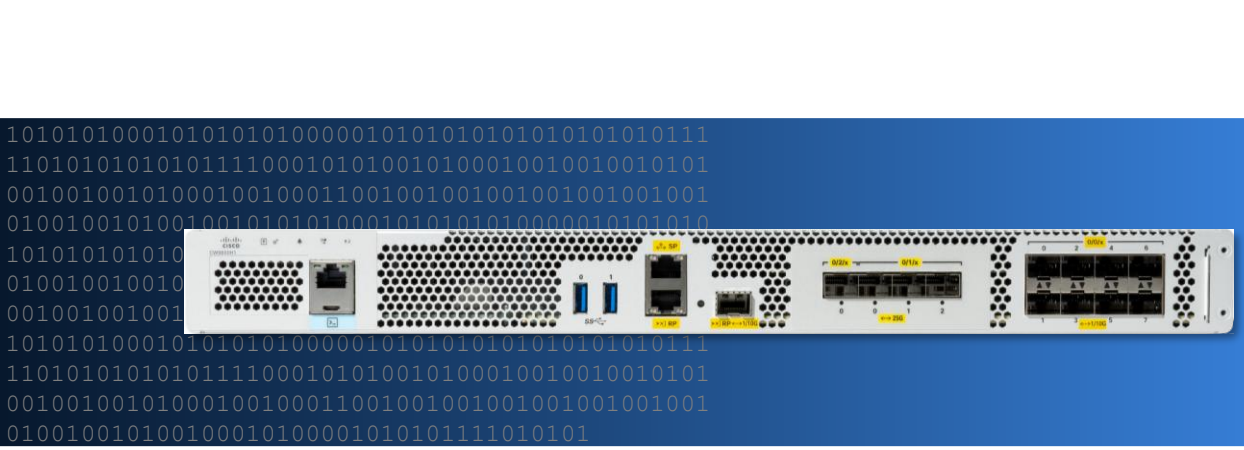


© 2025 Cisco and/or its affiliates. All rights reserved.

Network as a Sensor and Enforcer

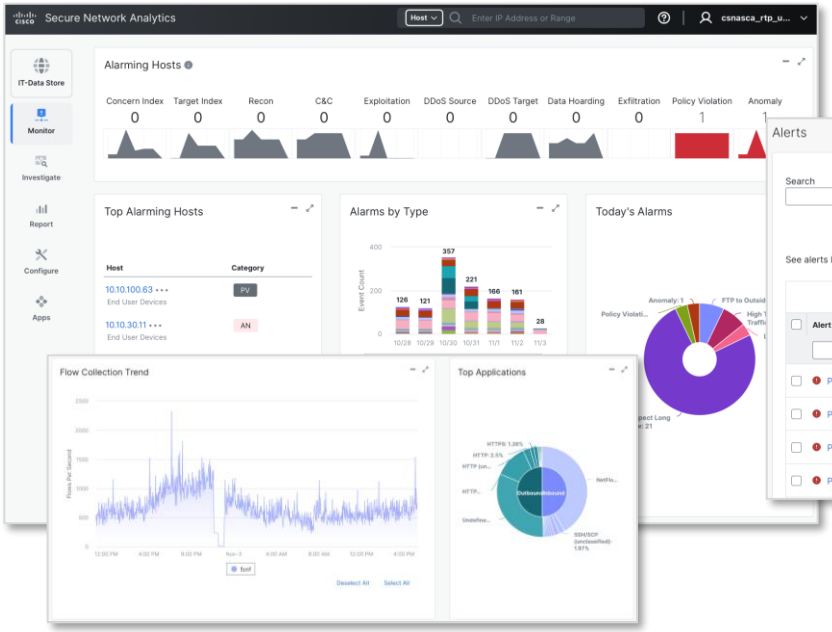
Network as a Sensor

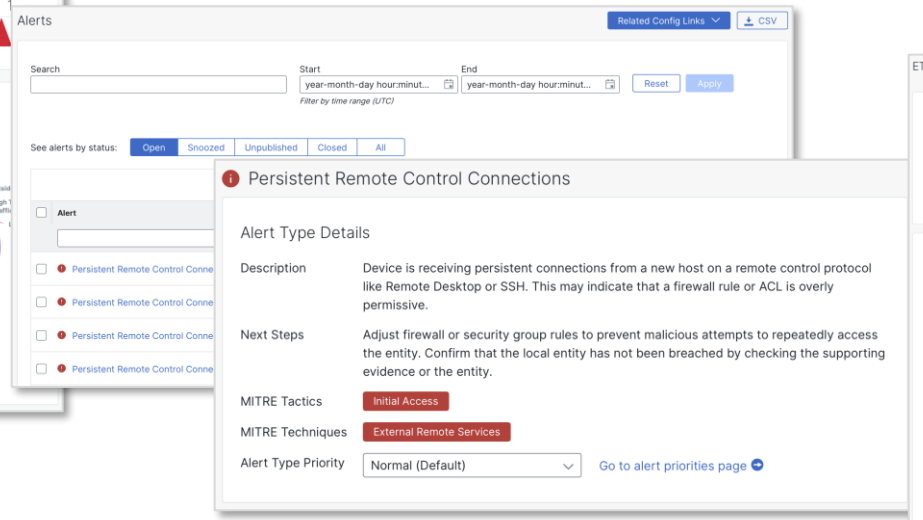
Secure Network Analytics Integration

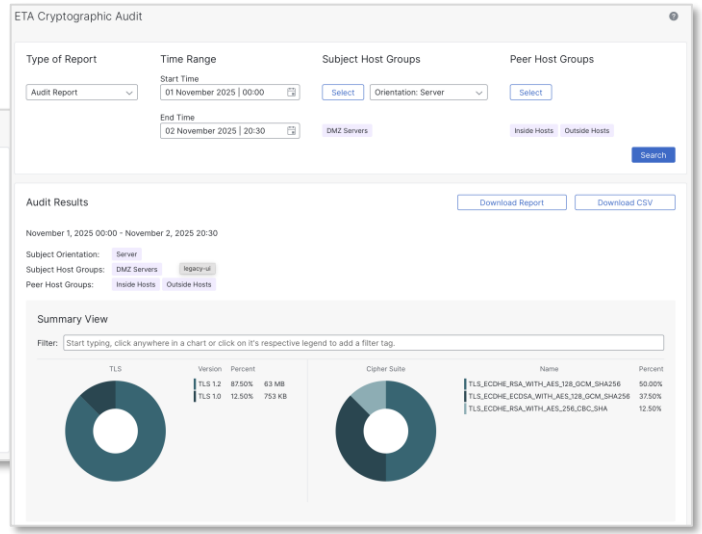


Netflow

Malware detection and cryptographic compliance with Secure Network Analytics



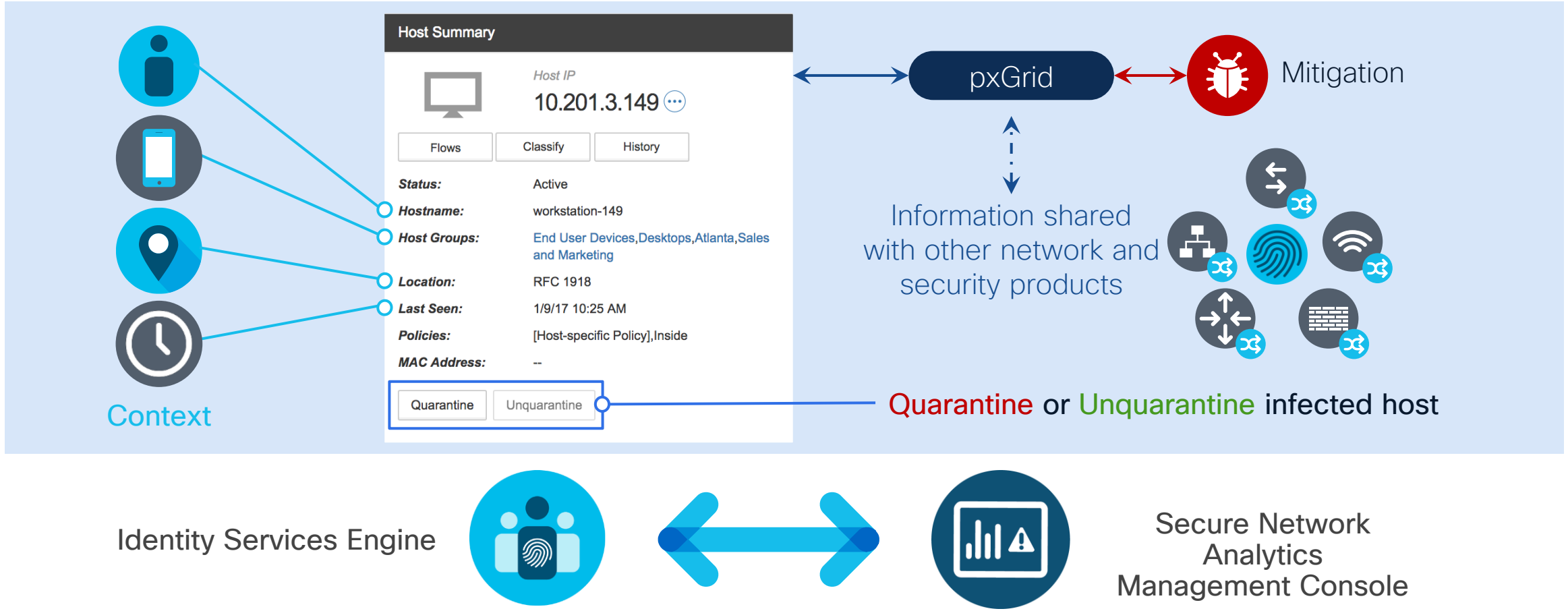




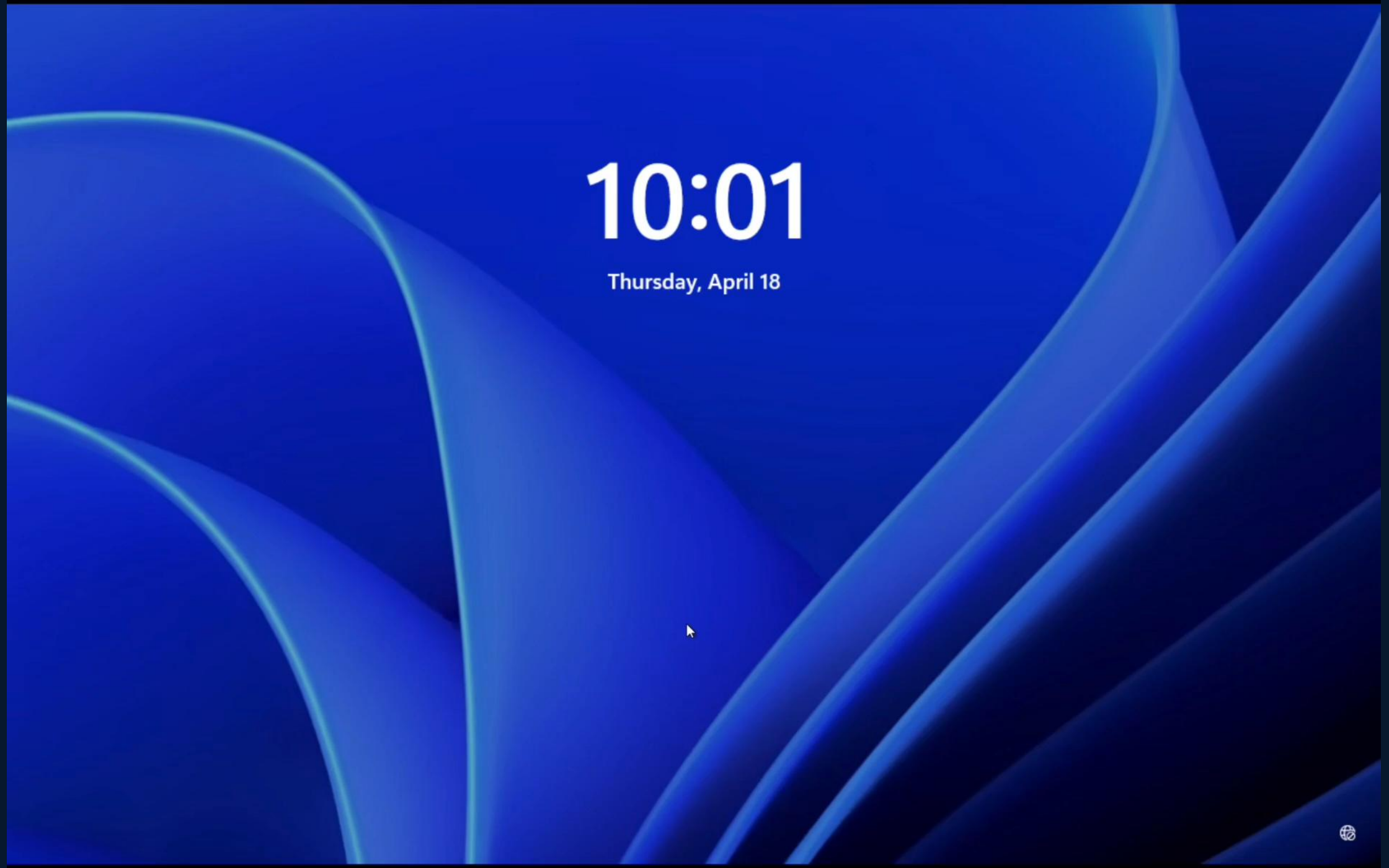
© 2025 Cisco and/or its affiliates. All rights reserved.

Network as an Enforcer

Rapid Threat Containment



© 2025 Cisco and/or its affiliates. All rights reserved.


10:01
Thursday, April 18

Securing the Wireless Network

Secure the Air

Secure the Devices

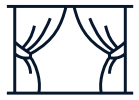
Secure the Network

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Thank you

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

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

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO