Secure Your Cisco Wireless Network with Identity Services Engine (ISE)

Rasheed Hamdan - Customer Delivery Engineering Technical Leader
Surendra Reddy Kanala - Customer Experience Customer Success Specialist

BRKEWN-2325

Webex App

Questions?

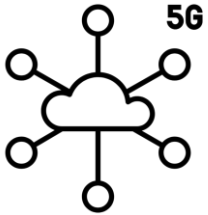
Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

Rasheed Hamdan



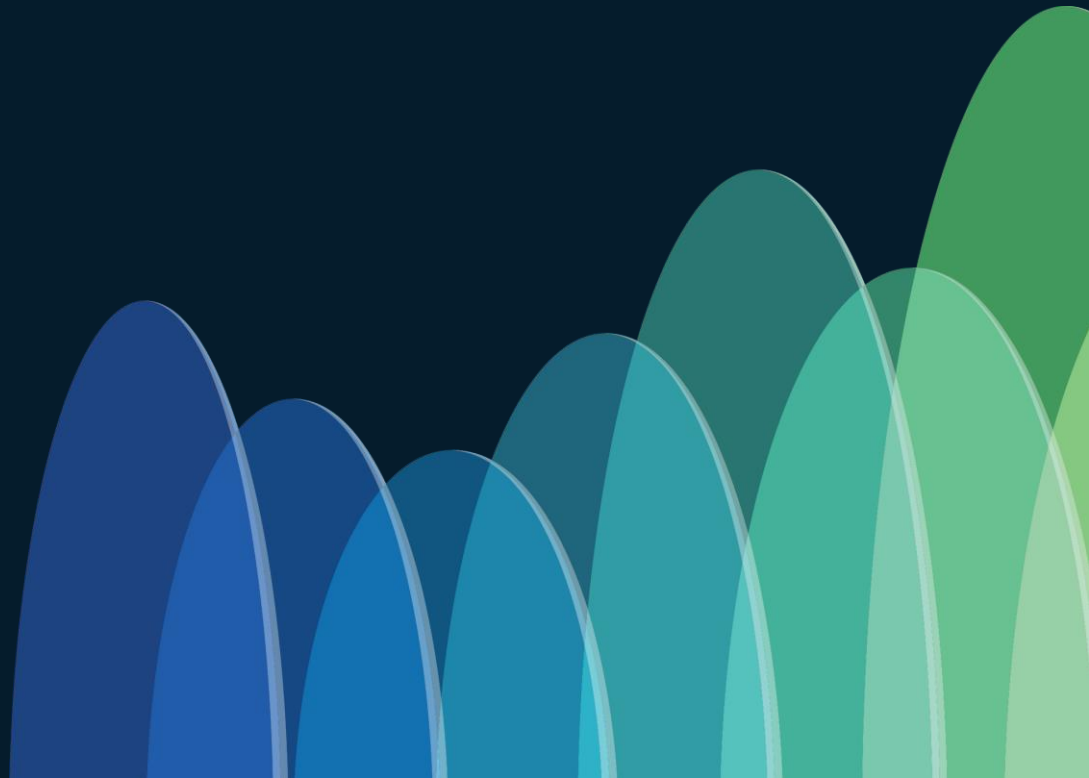
Surendra Reddy Kanala

Cisco Technical Support

Agenda

- Introduction
- Basic Integration with Catalyst and Meraki
- Managing Network Users and Wireless Users
- Optimizing Authentication for Wireless Users
- Network Segmentations and Security Group Tags

Introduction



Why are we here today?

Why ISE?

- Device Administration
- Secure Access
- Guest Access
- Asset Visibility
- Compliance & Posture
- Context Exchange
- Segmentation
- Cisco Catalyst Center
- EMM/MDM
- Threat Containment

ISE Capabilities for Zero Trust from Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / APs
- VPN

Cisco ISE

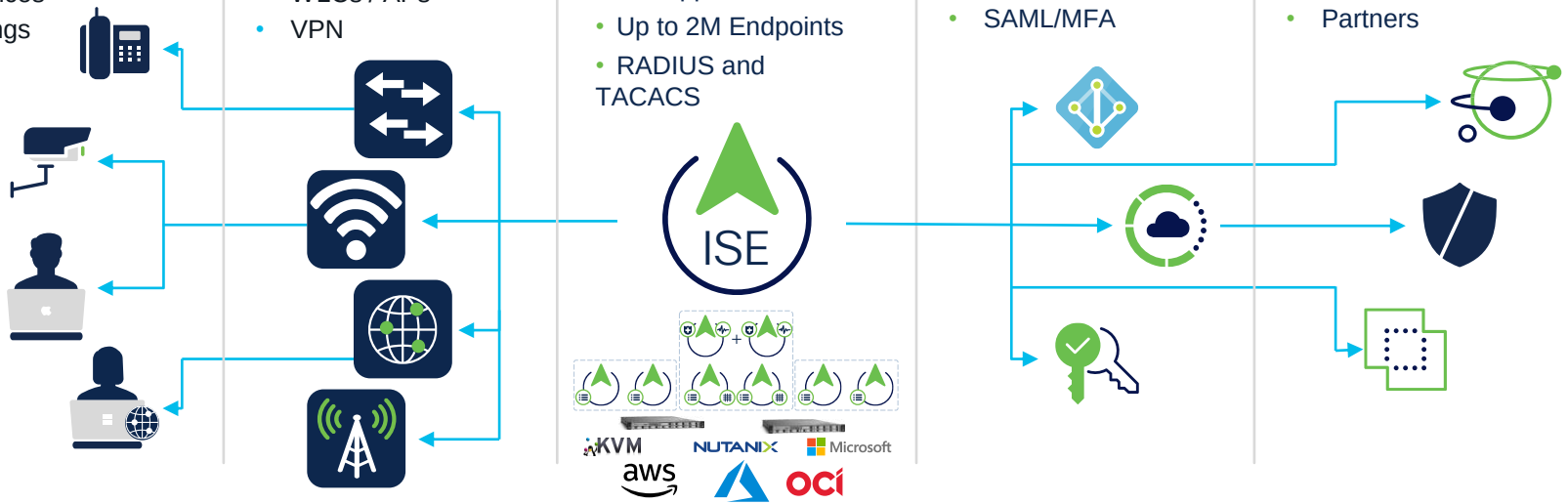
- Shared or Distributed
- VM/Appliance/Cloud
- Up to 2M Endpoints
- RADIUS and TACACS

Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Services

- Cloud Analytics
- Secure Firewall
- Partners



See It | Secure It | Share It

Authorization Options with ISE

URL-Redirect

Provide conditional web redirect when traffic is blocked

QoS

QoS Profile is assigned per endpoint

AVC Profile

Application Visibility Profile is assigned per endpoint

Bandwidth

Control maximum bandwidth and burst rate per endpoint/user

Timer

Control session and idle-timeout

mDNS Profile

Assigns mDNS profile to broker mDNS advertisement

Open DNS

Assigns Open DNS profile to intercept DNS packets for custom response

Roles

Assigns role that includes multiple characteristics: VLAN, ACL, QoS, Timer, etc.

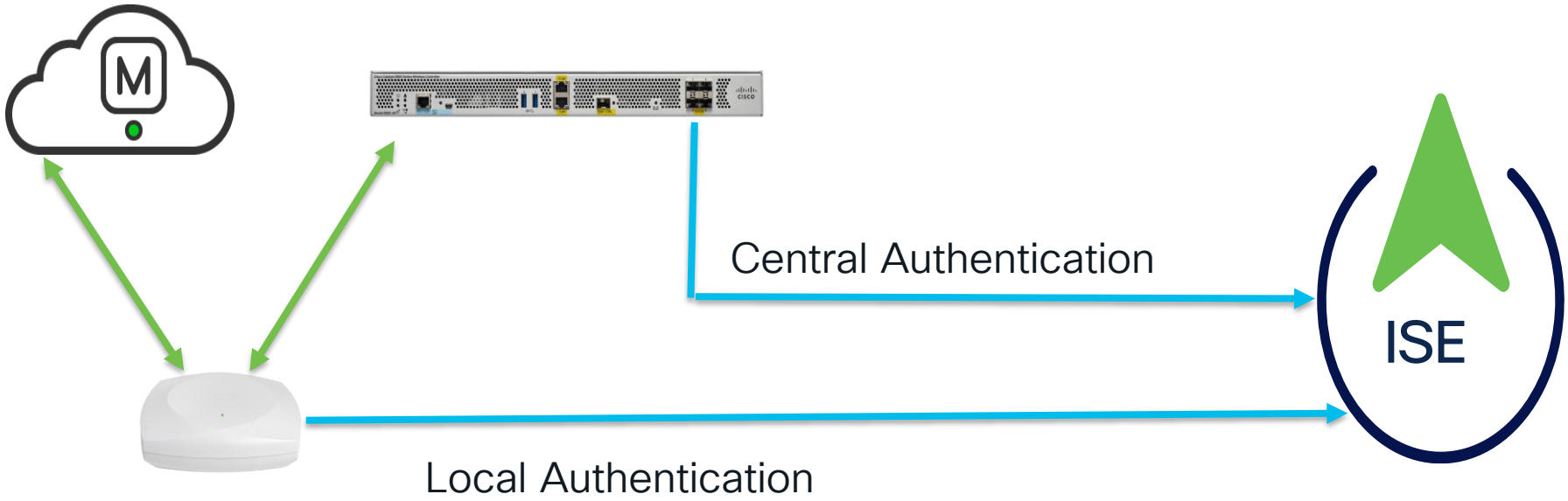
Service Template

Assigns service that includes multiple characteristics: VLAN, ACL, QoS, Timer, etc.

URL-Filter

Controls which FQDNs the endpoint can reach or not

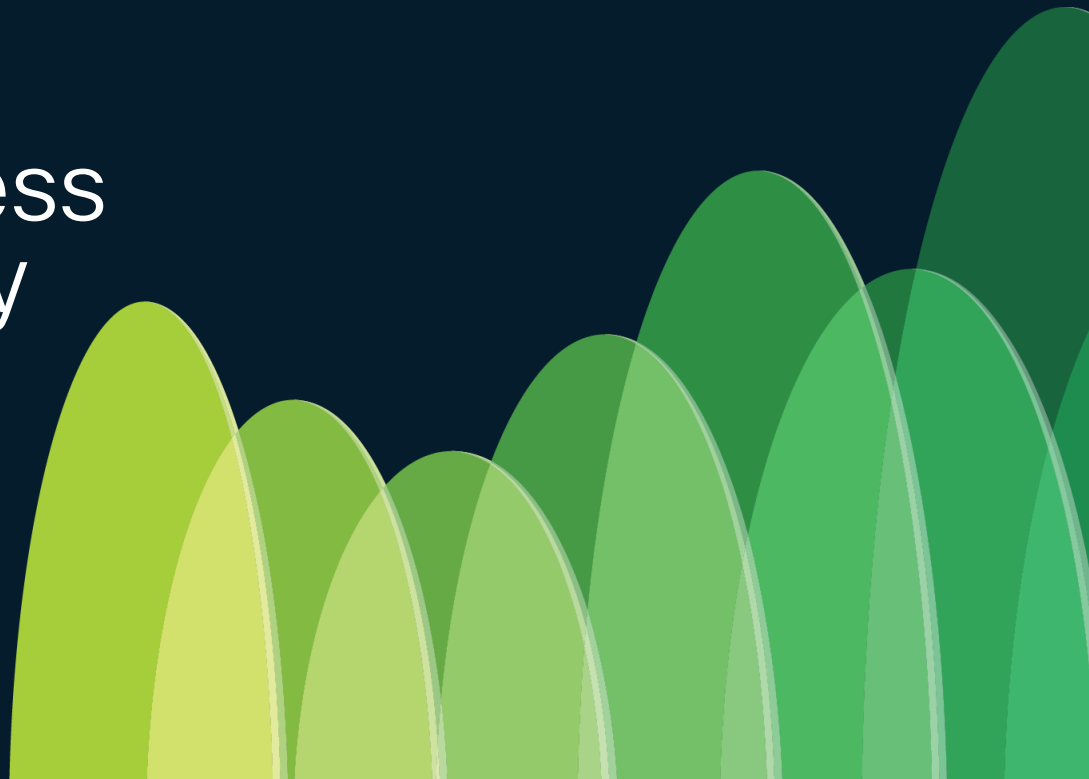
Cisco Wireless Introduction



Integrating ISE with Cisco Wireless

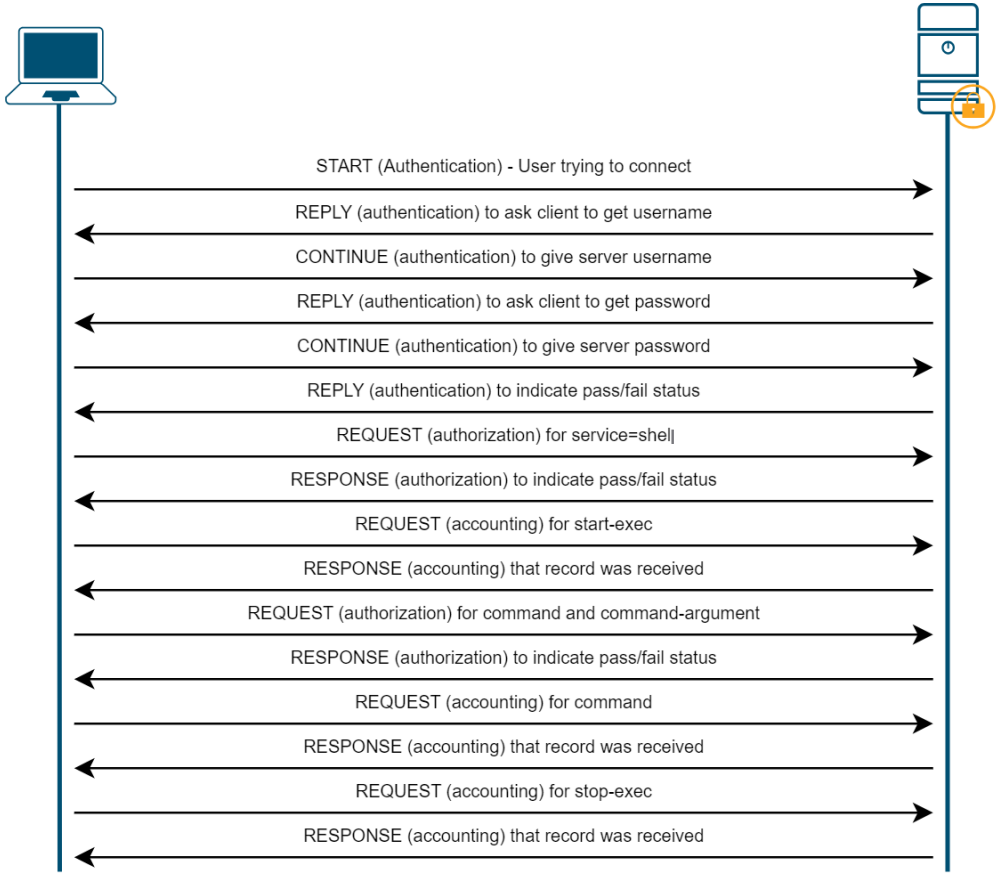
Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redir	CoA	Profiling
Meraki Wireless								
MR20, MR70	✓	✓	✓	✓	–	✓	✓	–
MR28/30H/33/42/42E/52/53/53E/74/84 MR36/36H/44/45/46/46E/55/56/57/76/78/86 CW916x/CW917x	✓	✓	✓	✓	✓ 802.11ac Wave2 or higher. Min 27.6	✓	✓	From R31.2 on 802.11ax+ models
Catalyst								
9800 (All Supported APs)	✓	✓	✓	✓	✓	✓	✓	✓

Managing Wireless Network Security



cisco Live!

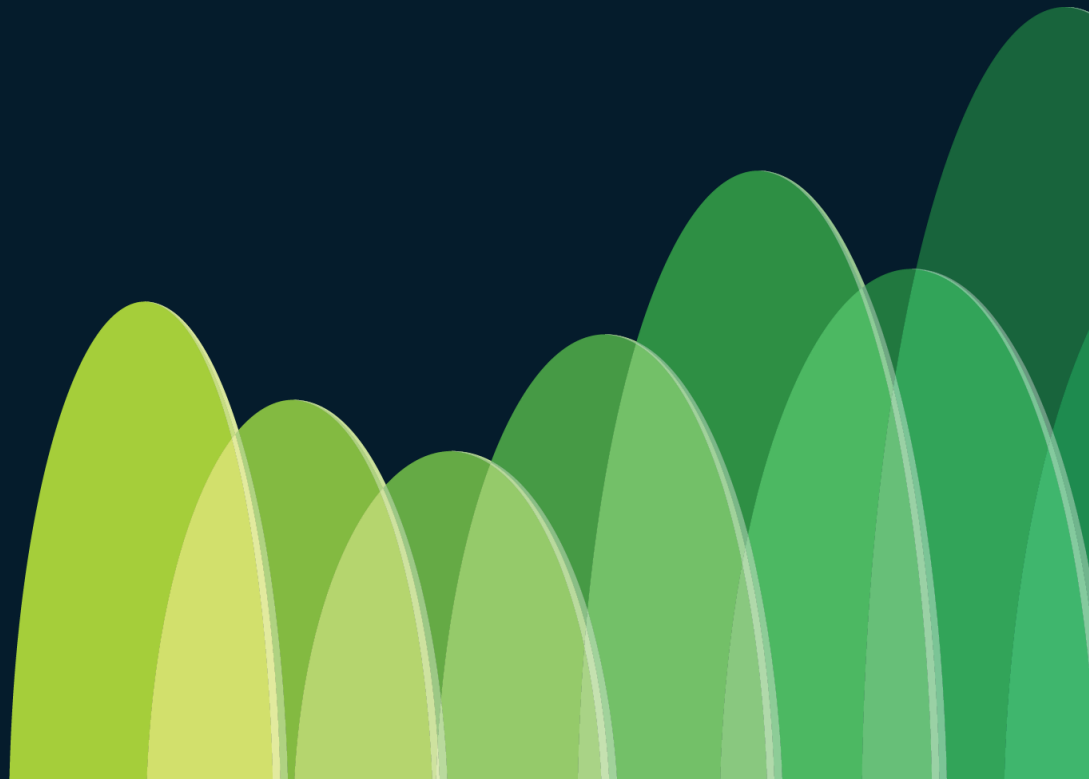
C9800 Network Admins TACACS+ Workflow



C9800 Wireless Users Management

Clients	Authentication	Encryption	SSID
	None	Open	((guest))
	AUP (MAC Filter)	Open	((guest))
	pre-shared key (PSK)	WPA + PSK	((iot))
	psk1 | psk2 | ...	WPA2 + mPSK	((iot))
	xx:xx:xx:xx:xx:xx : psk1 yy:yy:yy:yy:yy:yy : psk2	WPA2 + iPSK	((iot))
	 802.1X	WPA2/3-Ent	((corp))

L2 Authentication

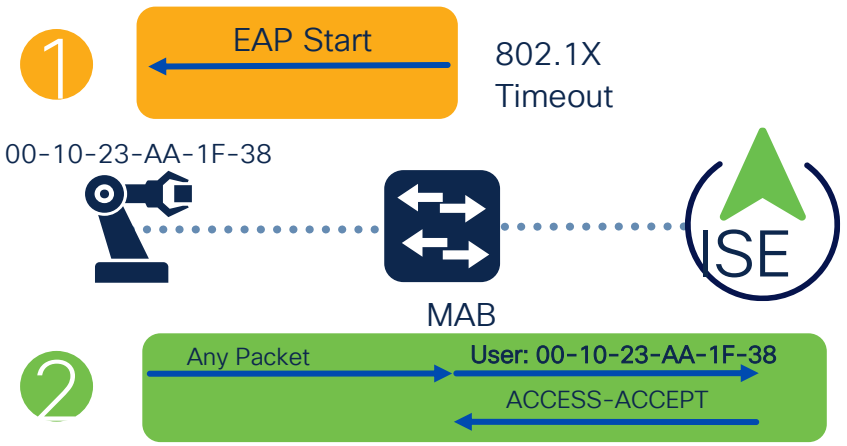


MAB

Endpoints without a configured supplicant fail 802.1X!

```
Attribute Value Pairs
  AVP: l=14 t=User-Name(1): b844d934e871
  AVP: l=24 t=Called-Station-Id(30): 20-bb-c0-67-fd-a0:OPEN
  AVP: l=19 t=Calling-Station-Id(31): b8-44-d9-34-e8-71
  AVP: l=6 t=NAS-Port(5): 4
  AVP: l=6 t=NAS-IP-Address(4): 192.168.202.61
  AVP: l=7 t=NAS-Identifier(32): wlc-1
  AVP: l=12 t=Vendor-Specific(26) v=Airespace, Inc (formerly 'Black Storm Networks')(14179)
  AVP: l=18 t=User-Password(2): Encrypted
  AVP: l=6 t=Service-Type(6): Call-Check(10)
  AVP: l=6 t=Framed-MTU(12): 1300
  AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
  AVP: l=6 t=Tunnel-Type(64) Tag=0x00: VLAN(13)
  AVP: l=6 t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
  AVP: l=4 t=Tunnel-Private-Group-Id(81): 30
  AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
     AVP Type: 26
     AVP Length: 49
     VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8ca3d0000000058a28e54
  AVP: l=30 t=Acct-Session-Id(44): 58a28e54/b8:44:d9:34:e8:71/1
```

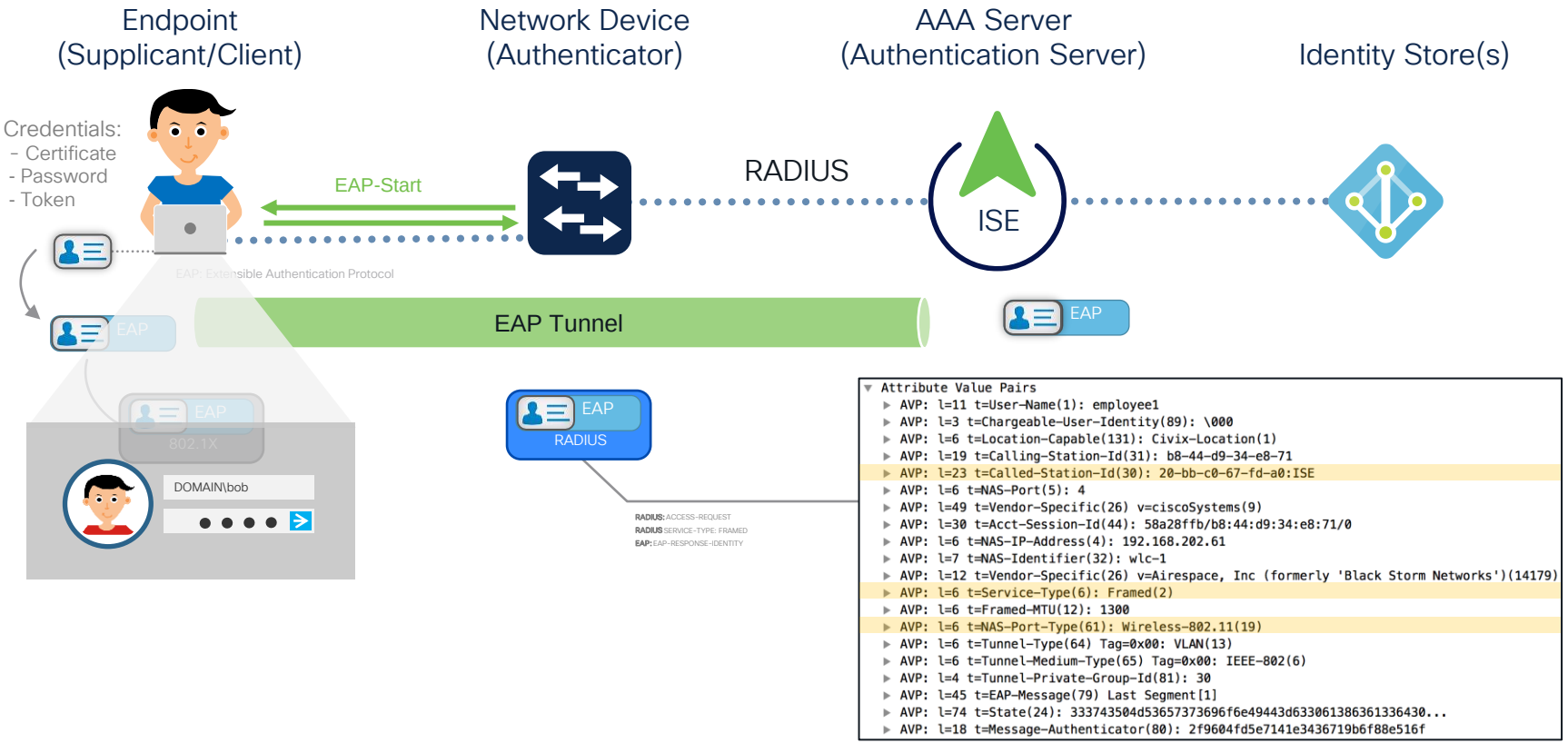
Bypass 802.1X Authentication with a Known MAC



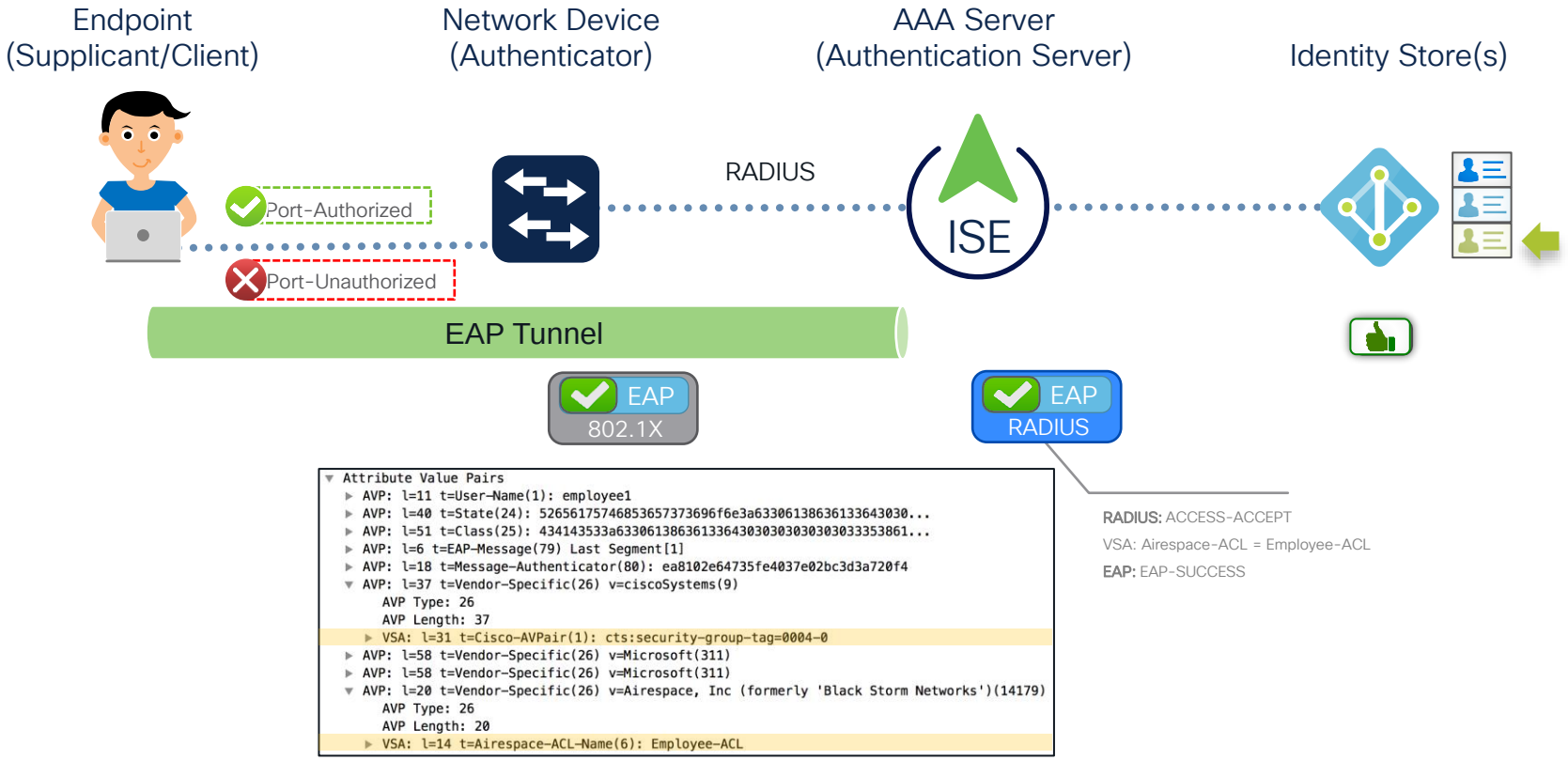
`Radius:Service-Type = Call Check`

MAB requires a MAC address database | ISE builds this database dynamically from discovered endpoints

IEEE 802.1X Fundamentals



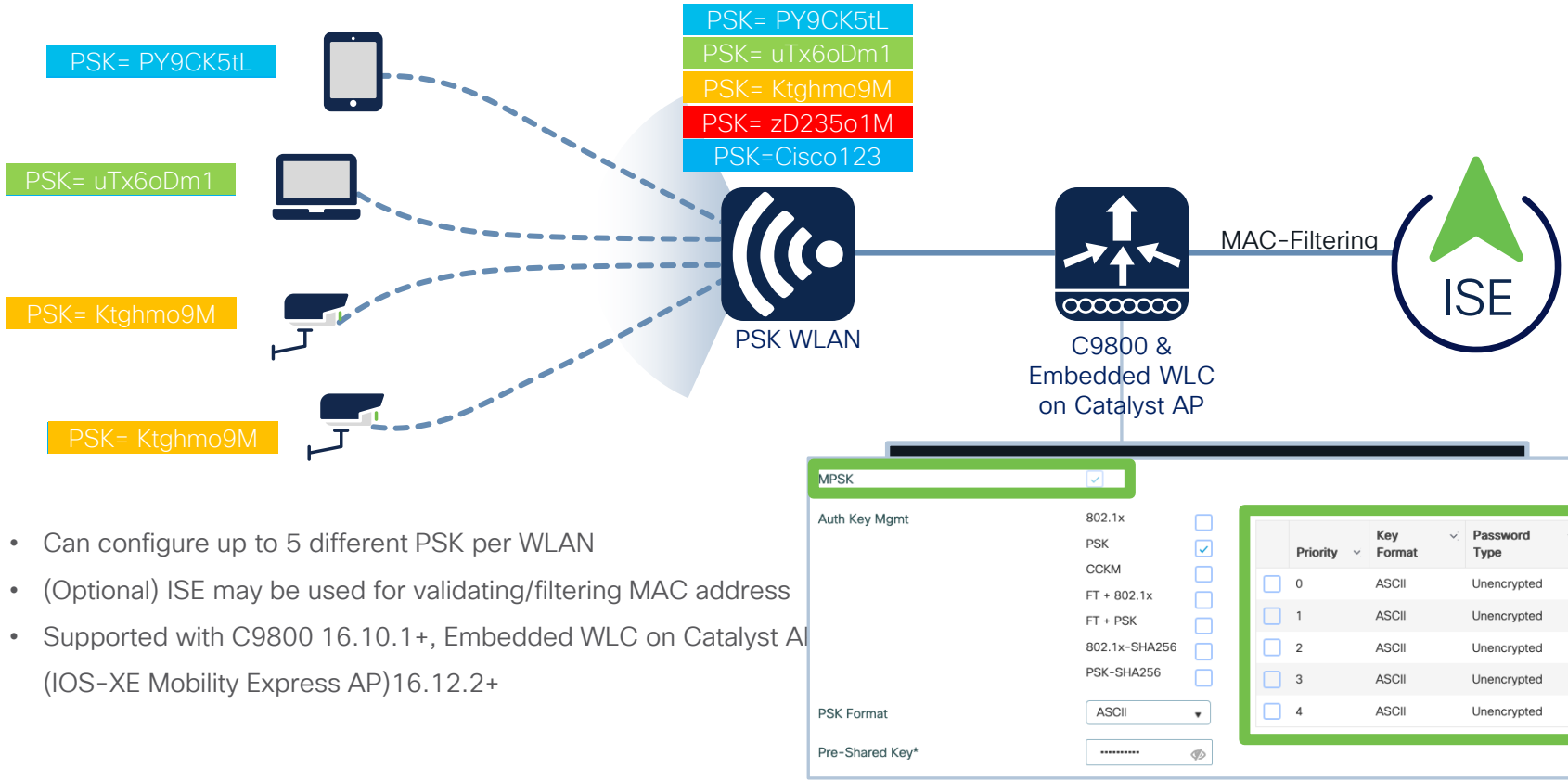
IEEE 802.1X Fundamentals



PSK (Pre-Shared Key) WLAN

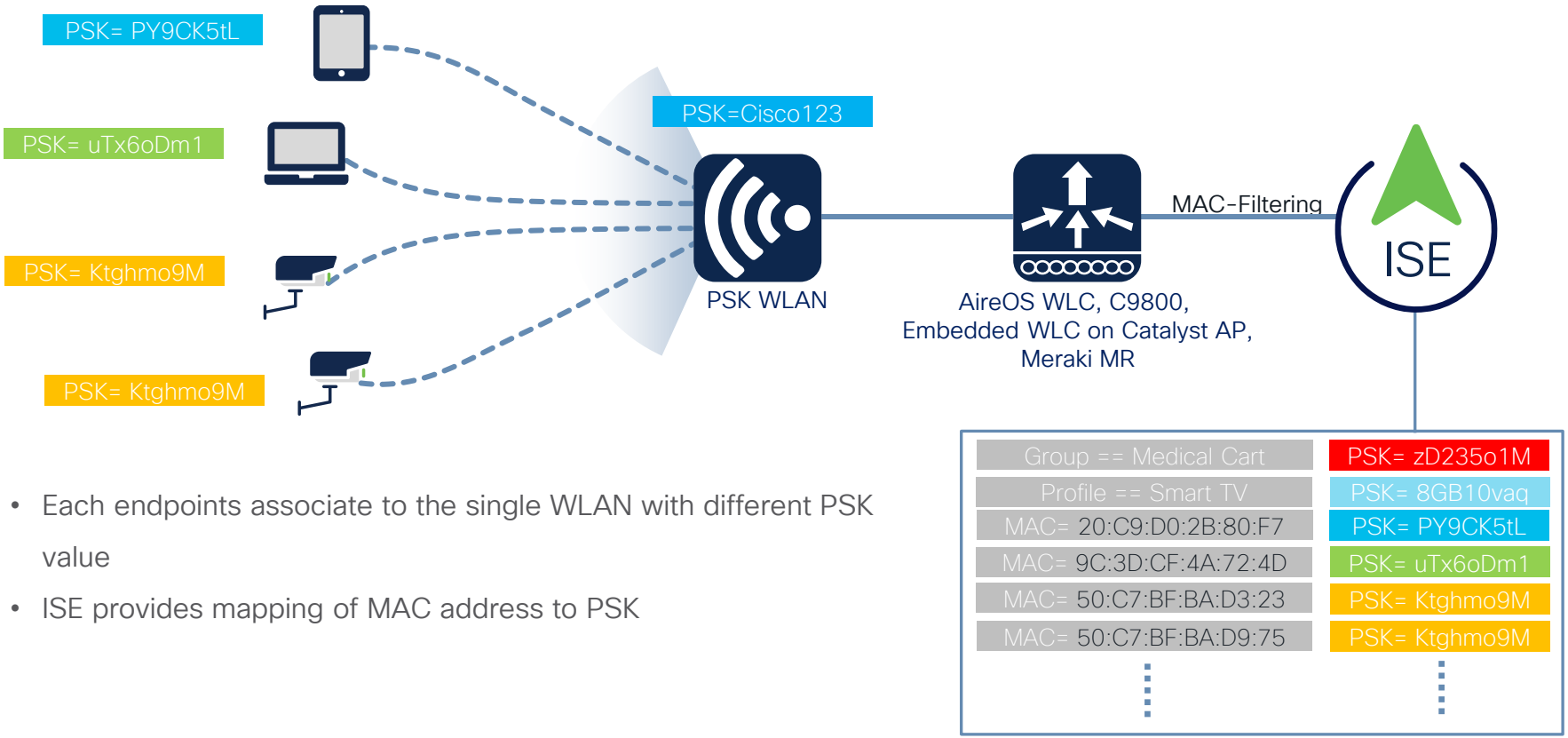
- Each endpoints associate to the single WLAN with same PSK value
- (Optional) ISE may be used for validating/filtering MAC address
- Supported on virtually any wireless product

mPSK (Multi-PSK)



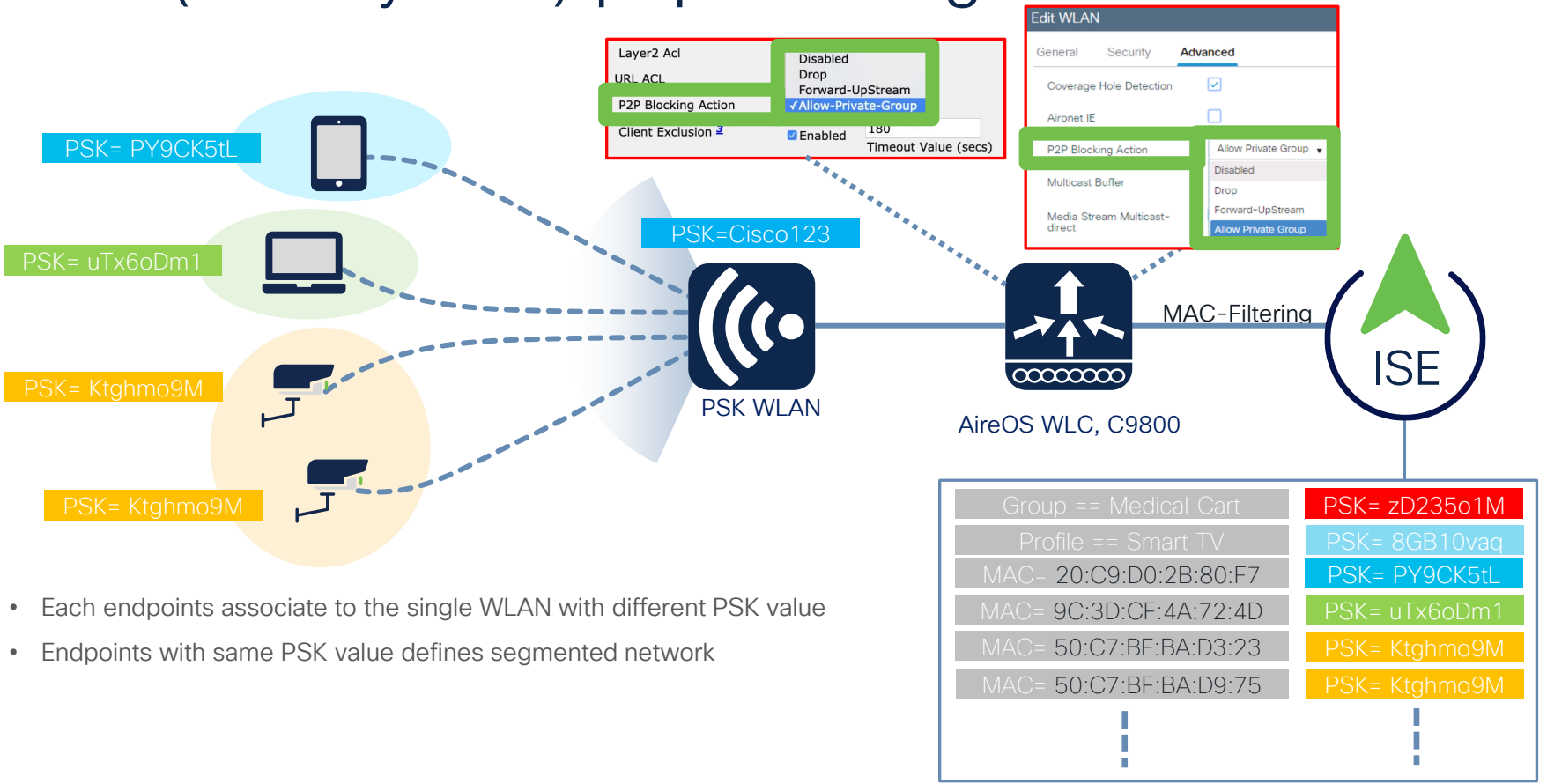
- Can configure up to 5 different PSK per WLAN
- (Optional) ISE may be used for validating/filtering MAC address
- Supported with C9800 16.10.1+, Embedded WLC on Catalyst AI
  (IOS-XE Mobility Express AP)16.12.2+

Identity PSK (iPSK)



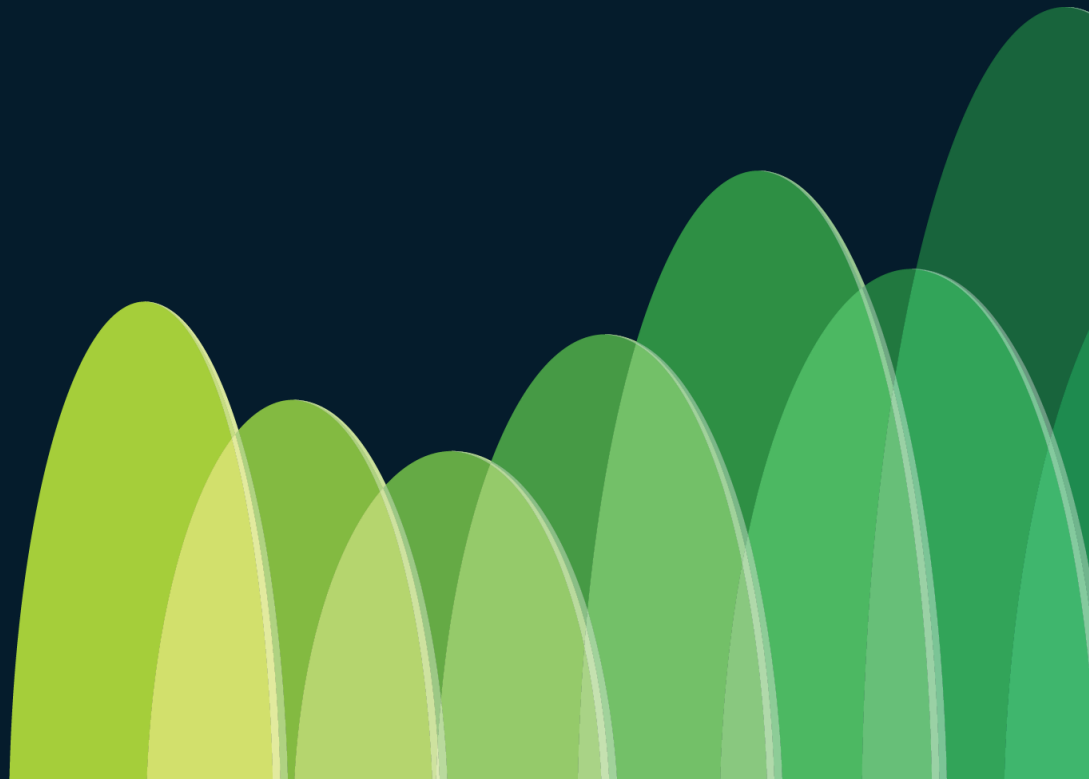
- Each endpoints associate to the single WLAN with different PSK value
- ISE provides mapping of MAC address to PSK

iPSK (Identity PSK) p2p blocking

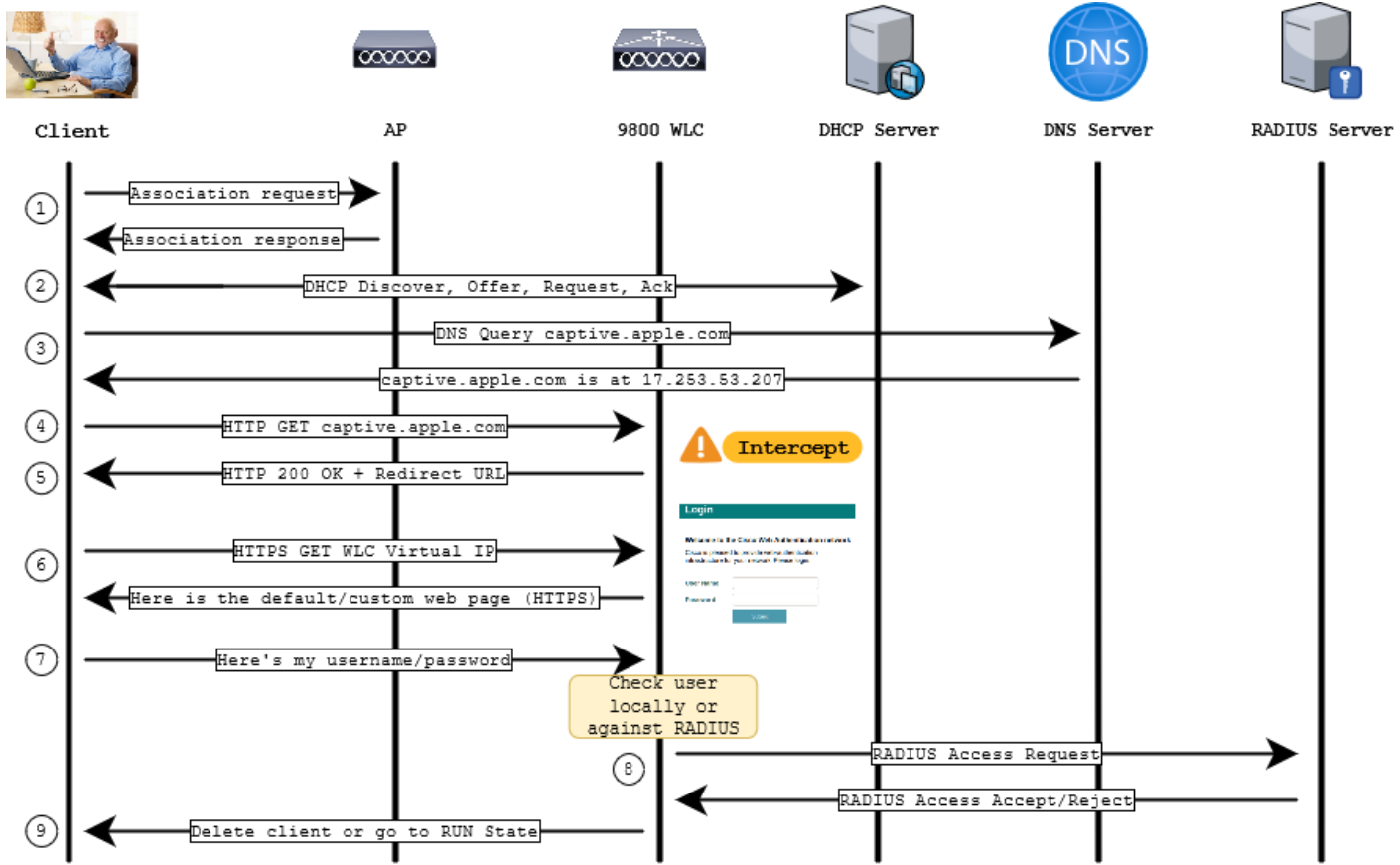


- Each endpoints associate to the single WLAN with different PSK value
- Endpoints with same PSK value defines segmented network

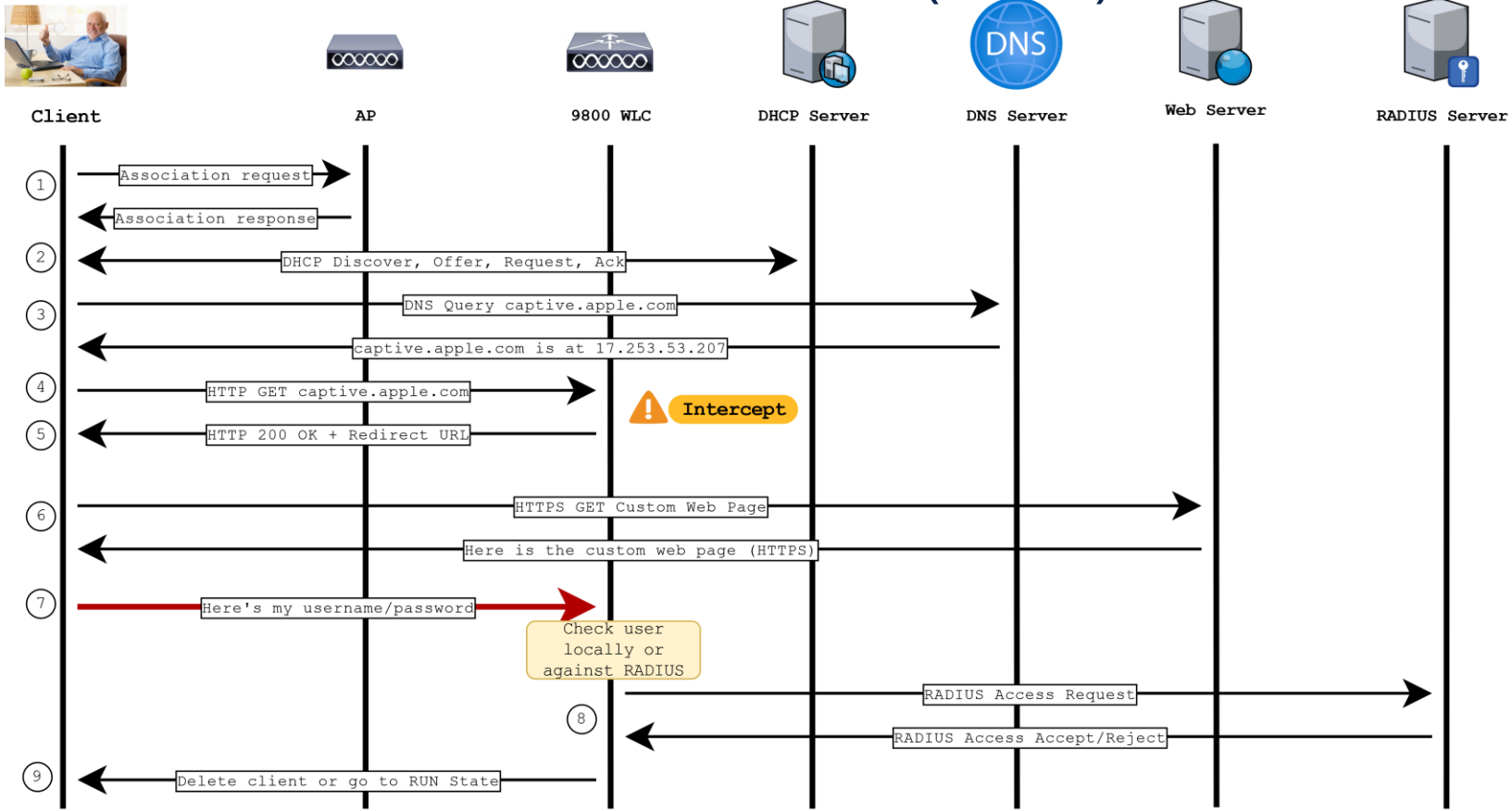
L3 Authentication



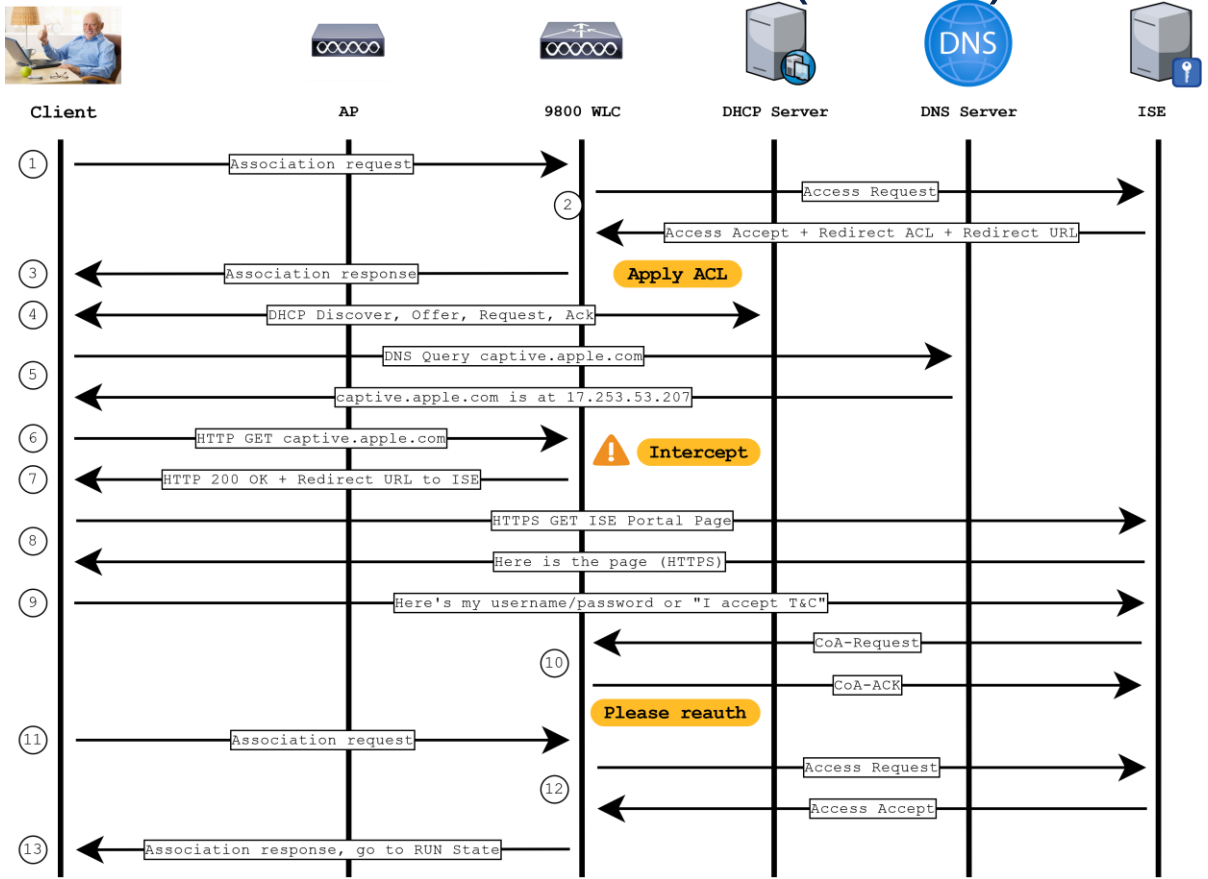
Local Web Authentication (LWA)



External Web Authentication (EWA)



Central Web Authentication (CWA)



ISE Guest Features

1 million

# of supported Guest accounts

EMAIL PRINT SMS

Guest account notification options

Portal language customization

Social Media Login support

API

Manage guest accounts via REST

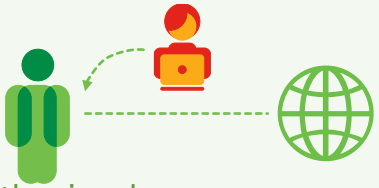
Hotspot

Immediate, un-credentialed Internet access

Self Registered

Self-registration by guests, Sponsors may approve access

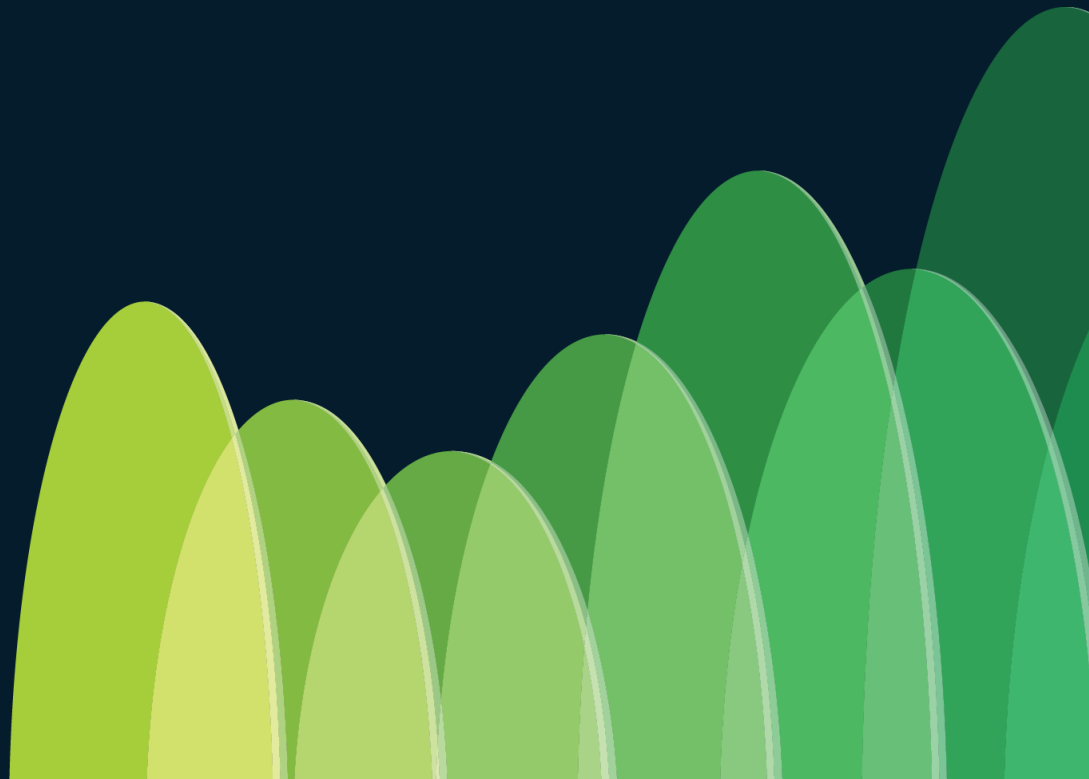
Sponsored Guest Access



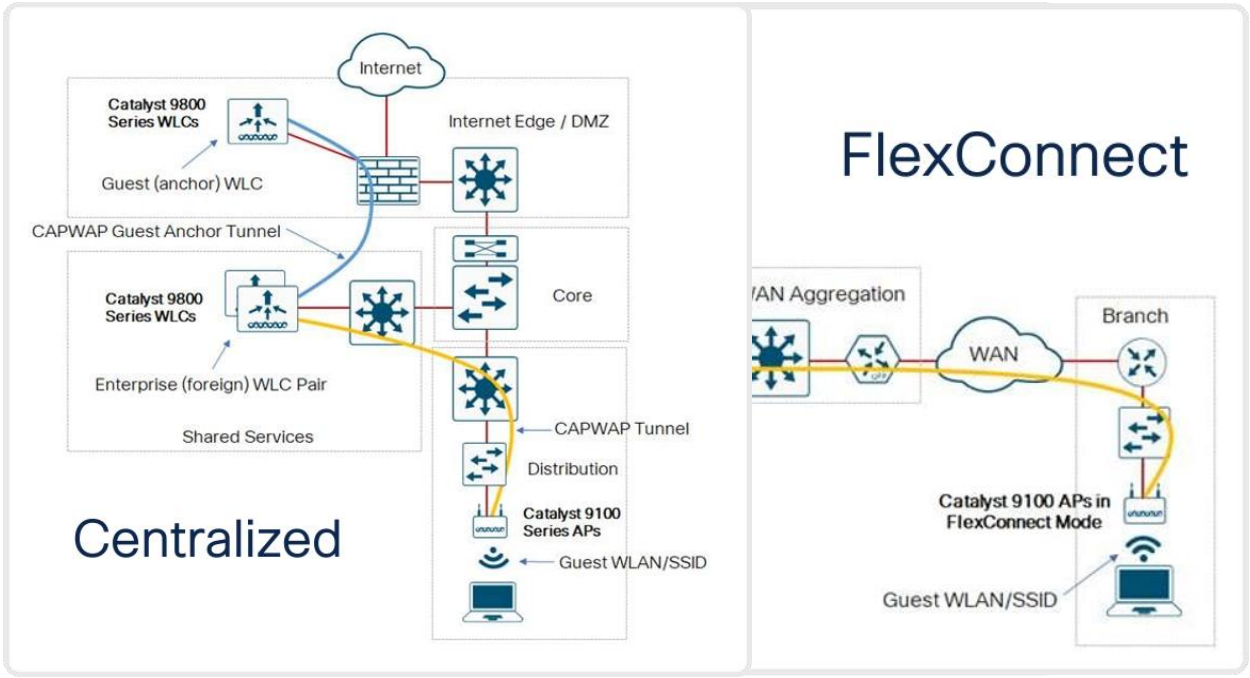
Authorized sponsors create account and share credentials

The 3 types of guest access

Configuration – Catalyst

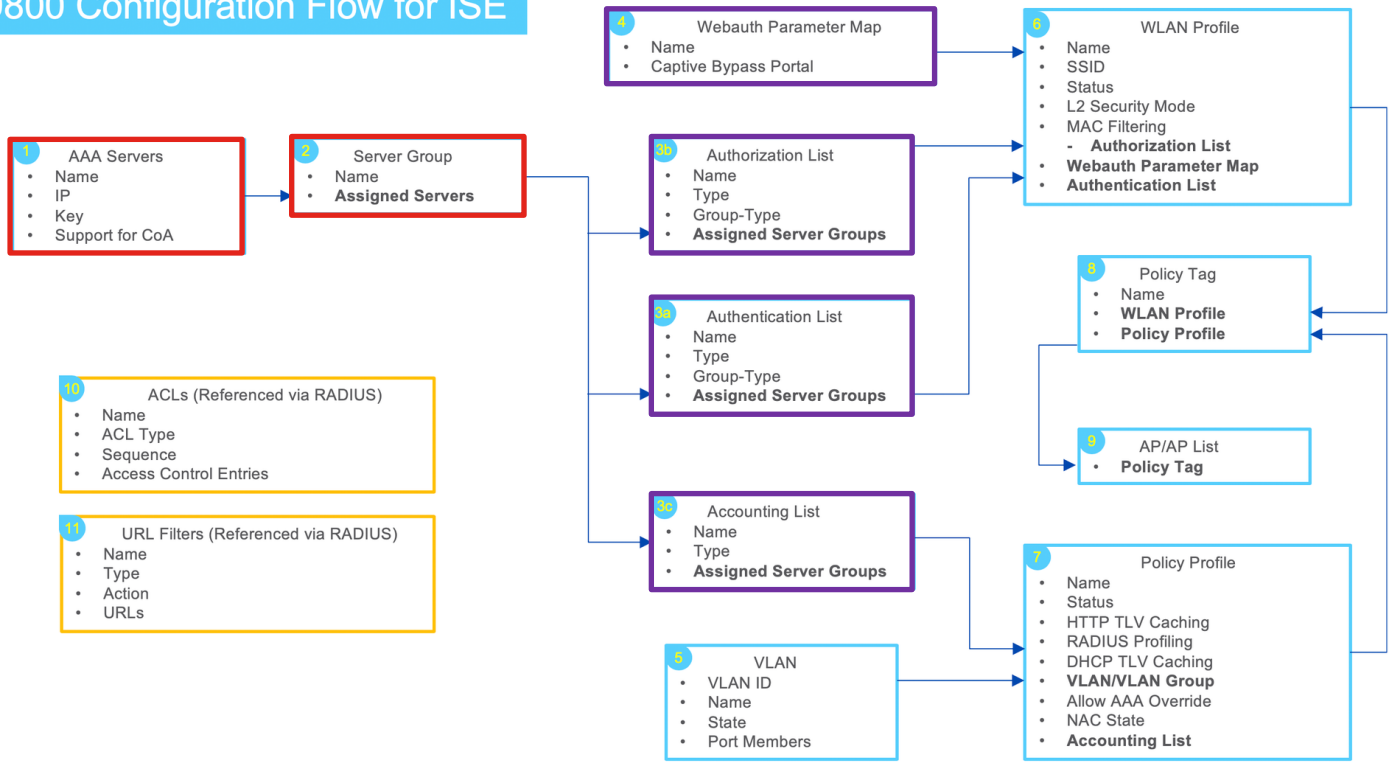


Designing ISE Guest with Catalyst 9800 WLC

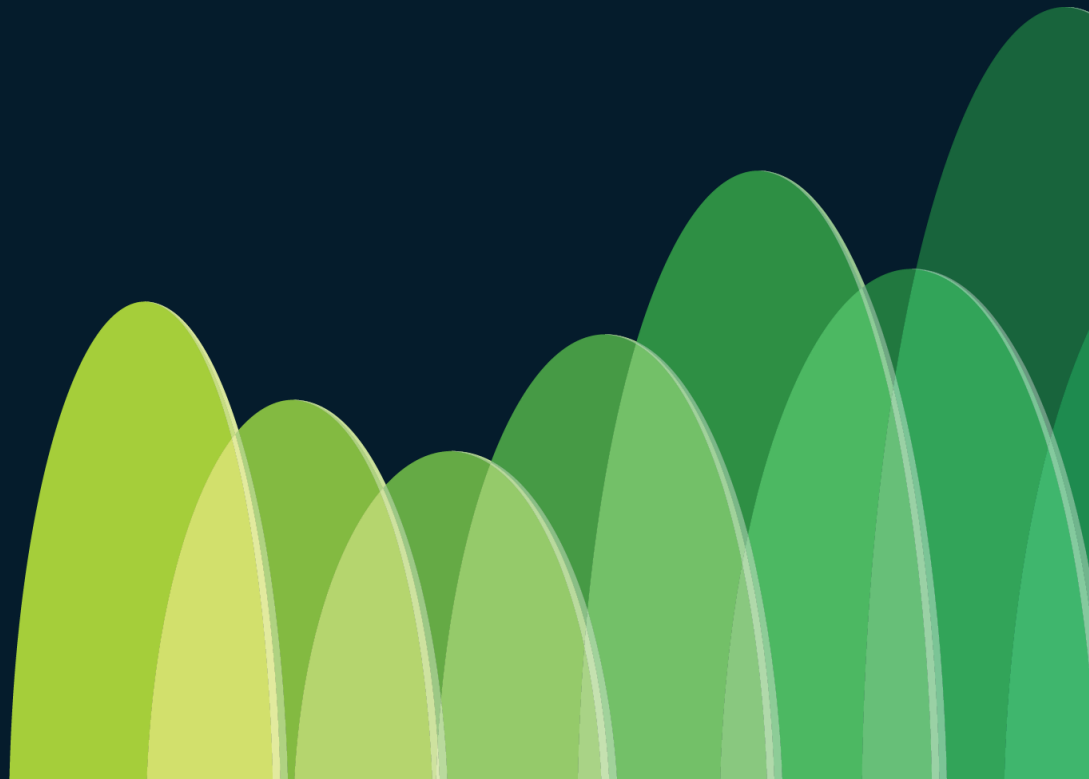


Integrating ISE with Catalyst 9800 WLC

C9800 Configuration Flow for ISE



Meraki

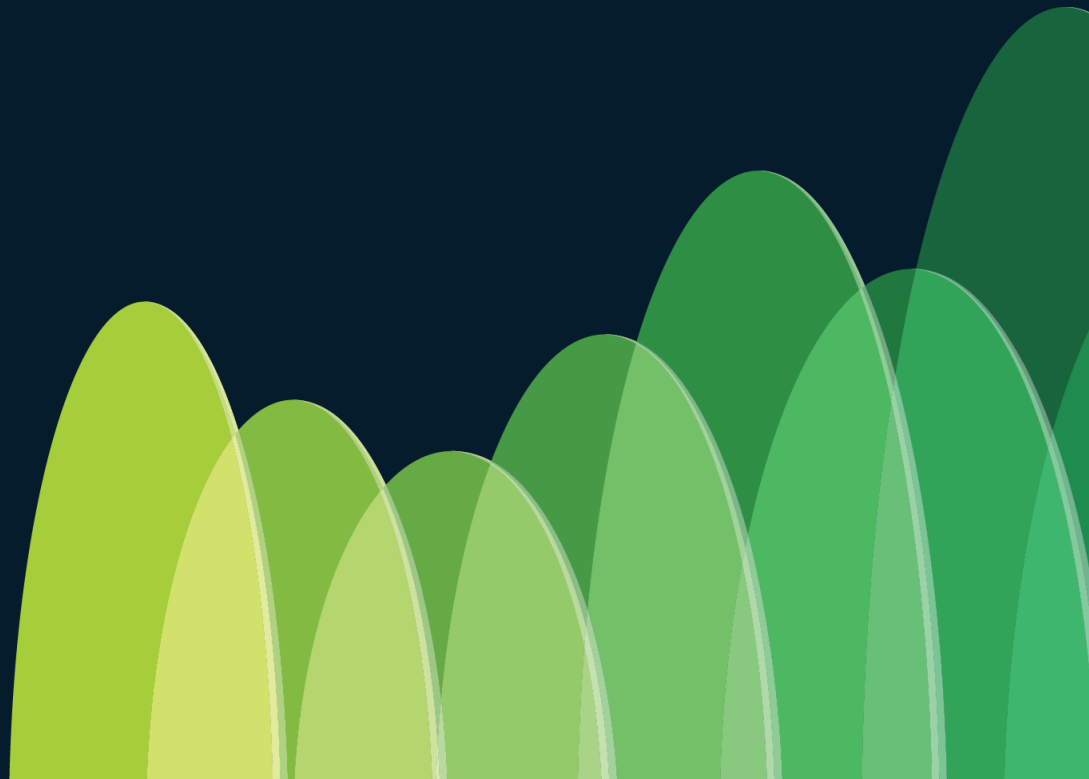


cisco Live!

Why ISE with Meraki for Access Control?

	Meraki	ISE
Multi-Vendor Deployments	Meraki Only	✓
Active Directory Domains	1 per Splash Page / LocalAuth	50
Identity Stores	AD, LDAP, Google Auth	Sequences: AD, Azure AD, LDAP, ODBC, SAML
Centralized, Customizable Portals	Splash Page	✓
Guest: Hotspot/AUP/Click-Thru	✓	✓
Guest: Self-Registered	✓	✓
Guest: Sponsored	✓	✓
Social Logins	Facebook	Facebook
Pay for Access Option	✓	X
MDM	Meraki Systems Manager	Meraki SM + 13 MDM Partners
Context / Security Integrations	Splash Page, WPN	100+ CSTA Partners

Configuration - Meraki



SSIDs

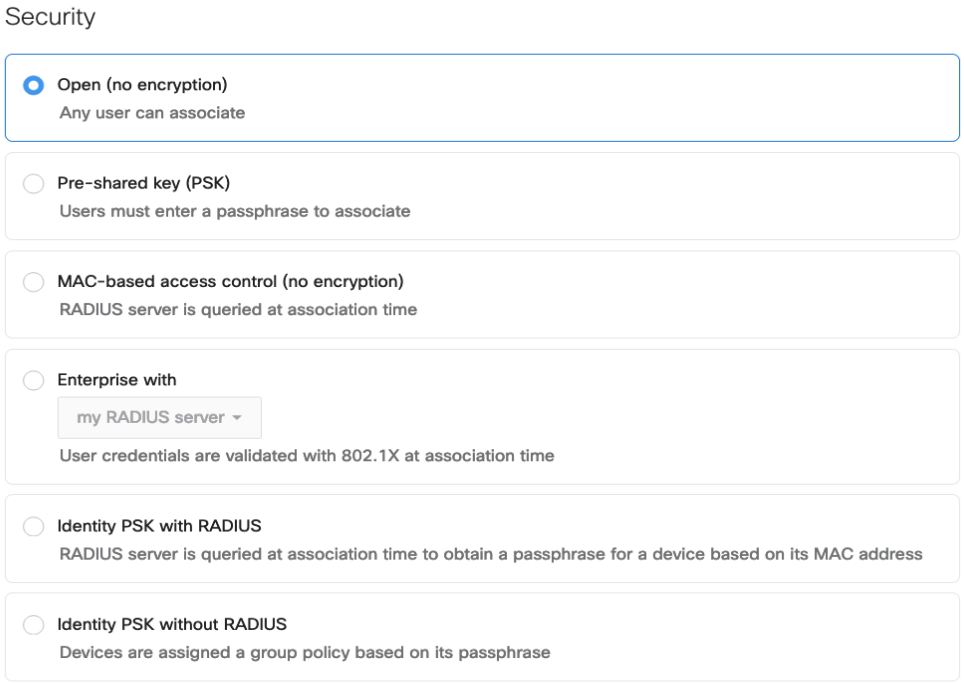
Wireless > Configure > SSIDs

Configuration overview

SSIDs Showing 4 of 15 SSIDs. Show all my SSIDs.

	Unconfigured SSID 0	Unconfigured SSID 2	Unconfigured SSID 3	Unconfigured SSID 4
Enabled	disabled	disabled	disabled	disabled
Name	rename	rename	rename	rename
Access control	edit settings	edit settings	edit settings	edit settings
Encryption	Open	Open	Open	Open
Sign-on method	None	None	None	None
Bandwidth limit	unlimited	unlimited	unlimited	unlimited
Client IP assignment	Meraki DHCP	Meraki DHCP	Meraki DHCP	Meraki DHCP
Clients blocked from using LAN	yes	no	no	no
Wired clients are part of Wi-Fi network	no	no	no	no
VLAN tag	n/a	n/a	n/a	n/a
VPN	Disabled	Disabled	Disabled	Disabled
Splash page				
Splash page enabled	no	no	no	no
Splash theme	n/a	n/a	n/a	n/a

Access Control Options per SSID



Open / Default

Hotspot / Passphrase

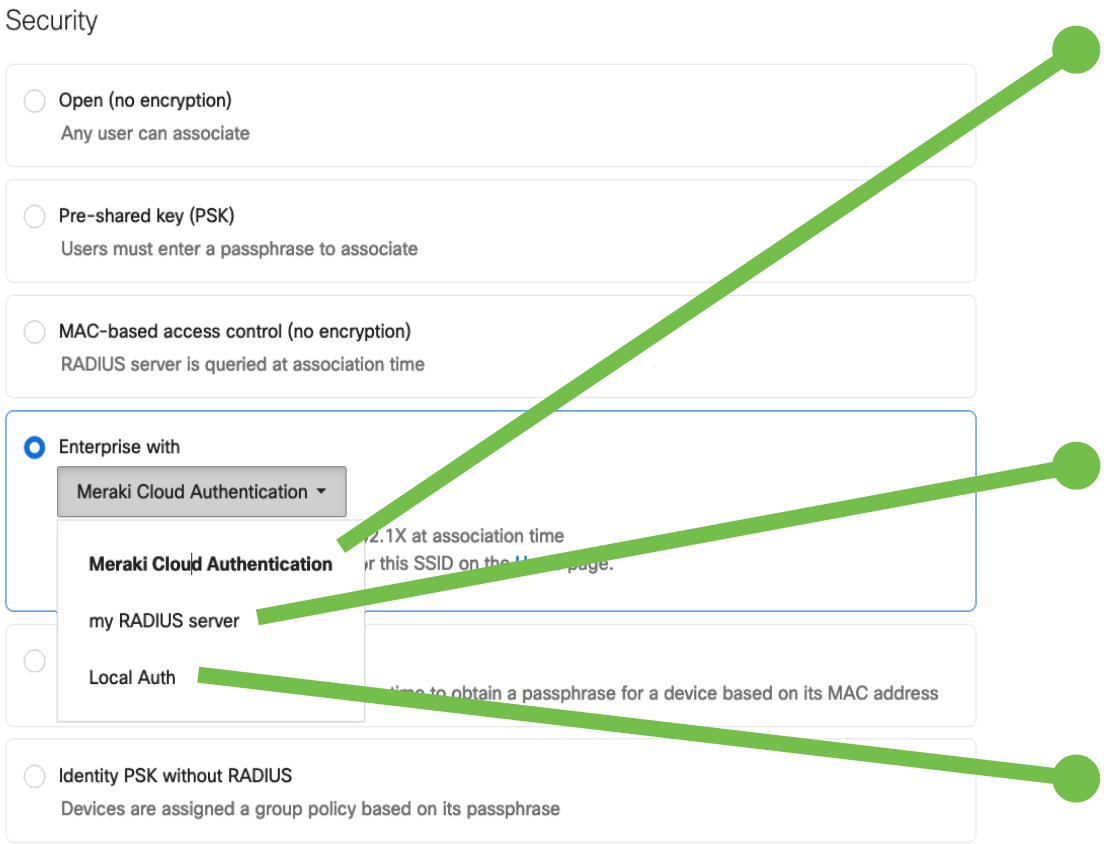
MAB

802.1X

Passphrase per MAC

Policy per Passphrase

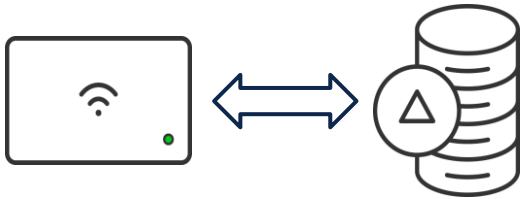
Enterprise Authentication Options per SSID



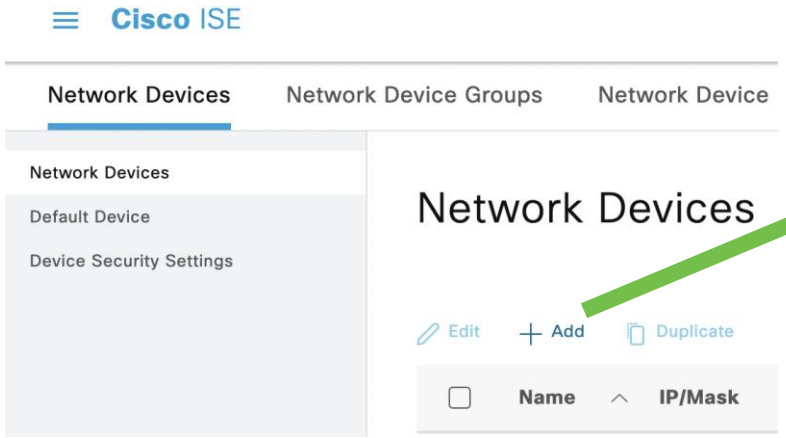
Available for:

- Sign-On Splash page
- WPA2 + 802.1X

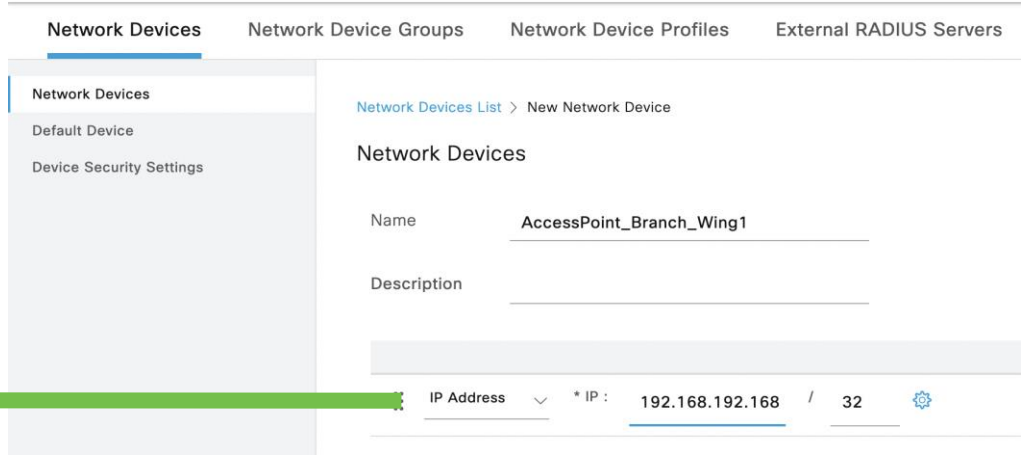
Open
PSK
MAB
Active Directory
LDAP
ODBC
Azure AD
SAML



Adding APs as Network Devices on ISE

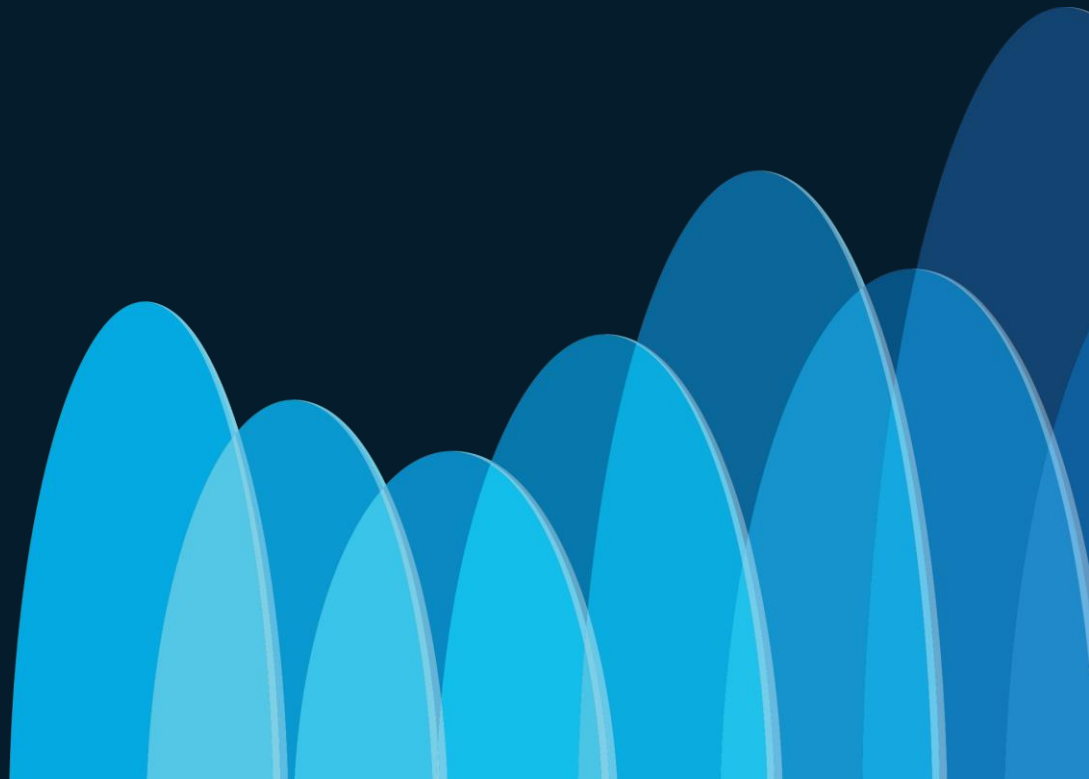


Administration > Network Resources > Network Devices



Add multiple IP Addresses or Address Ranges for ease of configuration!

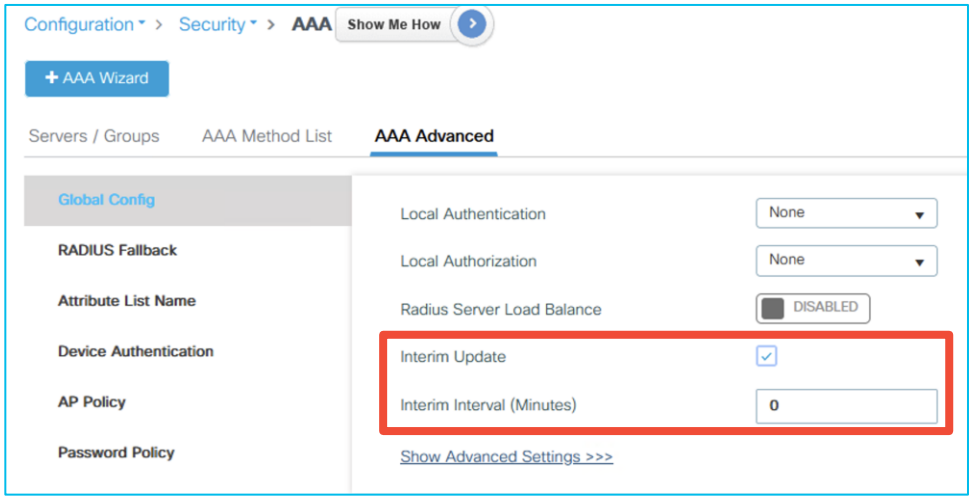
Optimizing Authentication for Wireless Users



cisco Live!

9800 WLC

- Configure Interim-Accounting to send updates on new-info or roam only.

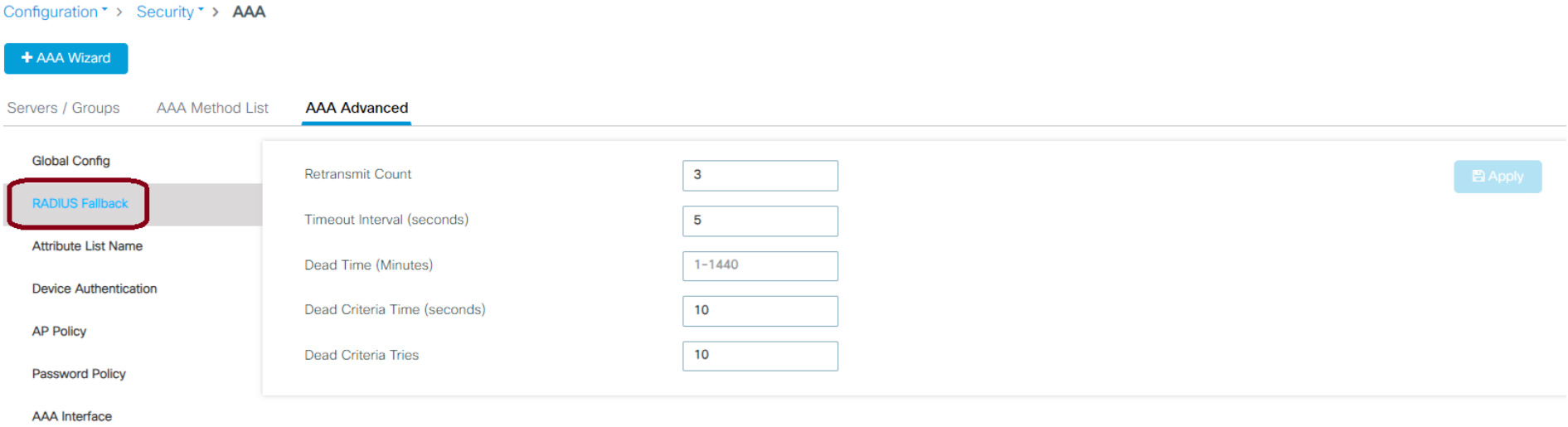


https://community.cisco.com/t5/security-knowledge-base/ise-and-catalyst-9800-series-integration-guide/ta-p/3753060

Number of RADIUS Servers

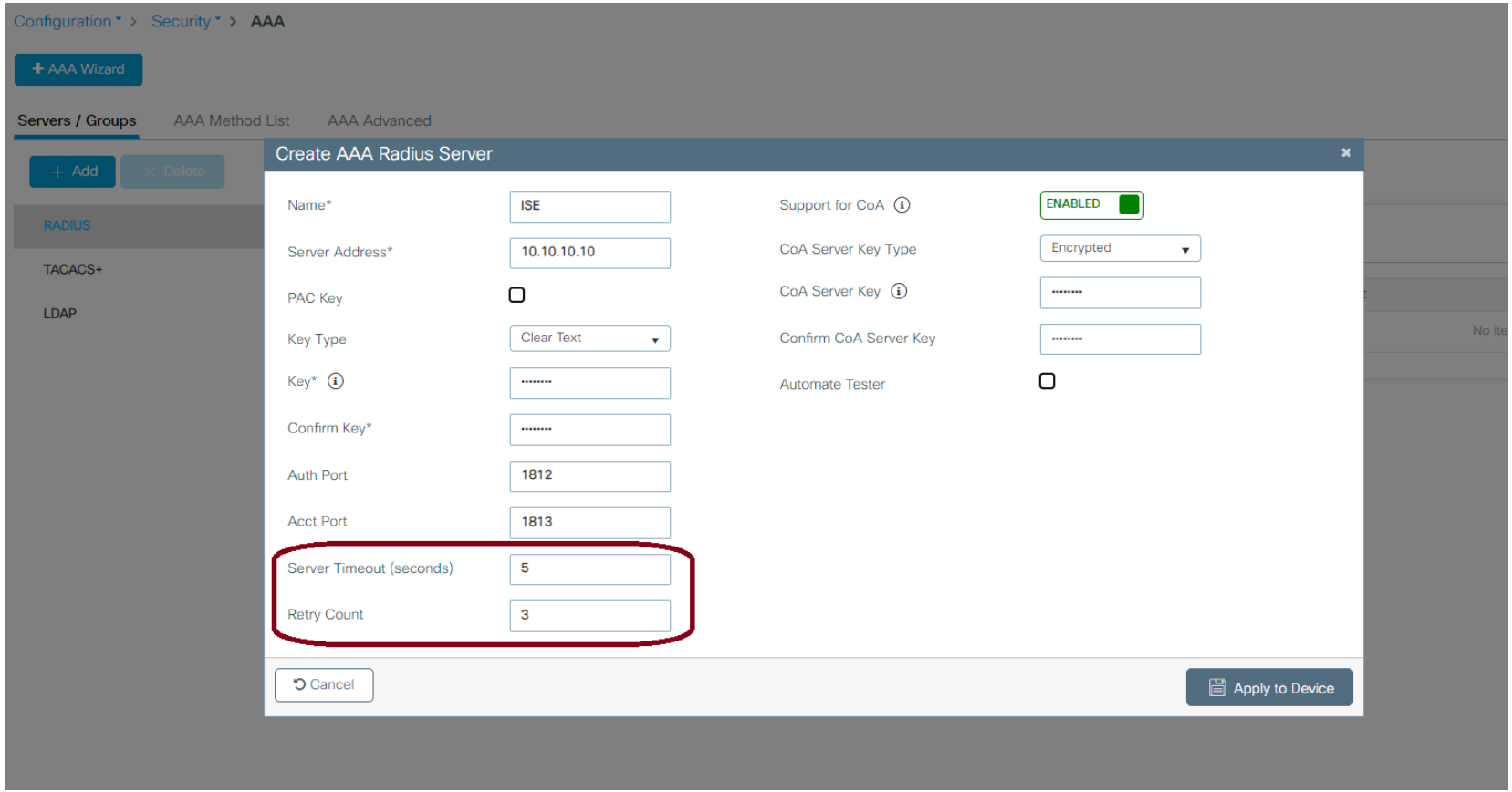
- Keep it to 3 or less
- 3 retries at 5 seconds means 15 seconds per server.
- Devices won't wait long enough to make more worthwhile (inbuilt timers).
- More adds more chance for cascading failures.
- Need more? Add a load balancer!
- Use a dead timer of 10 minutes or more.
  - If all servers are exhausted the top server will be tried before the deadtime expires.

Radius Timers (Global Setting)

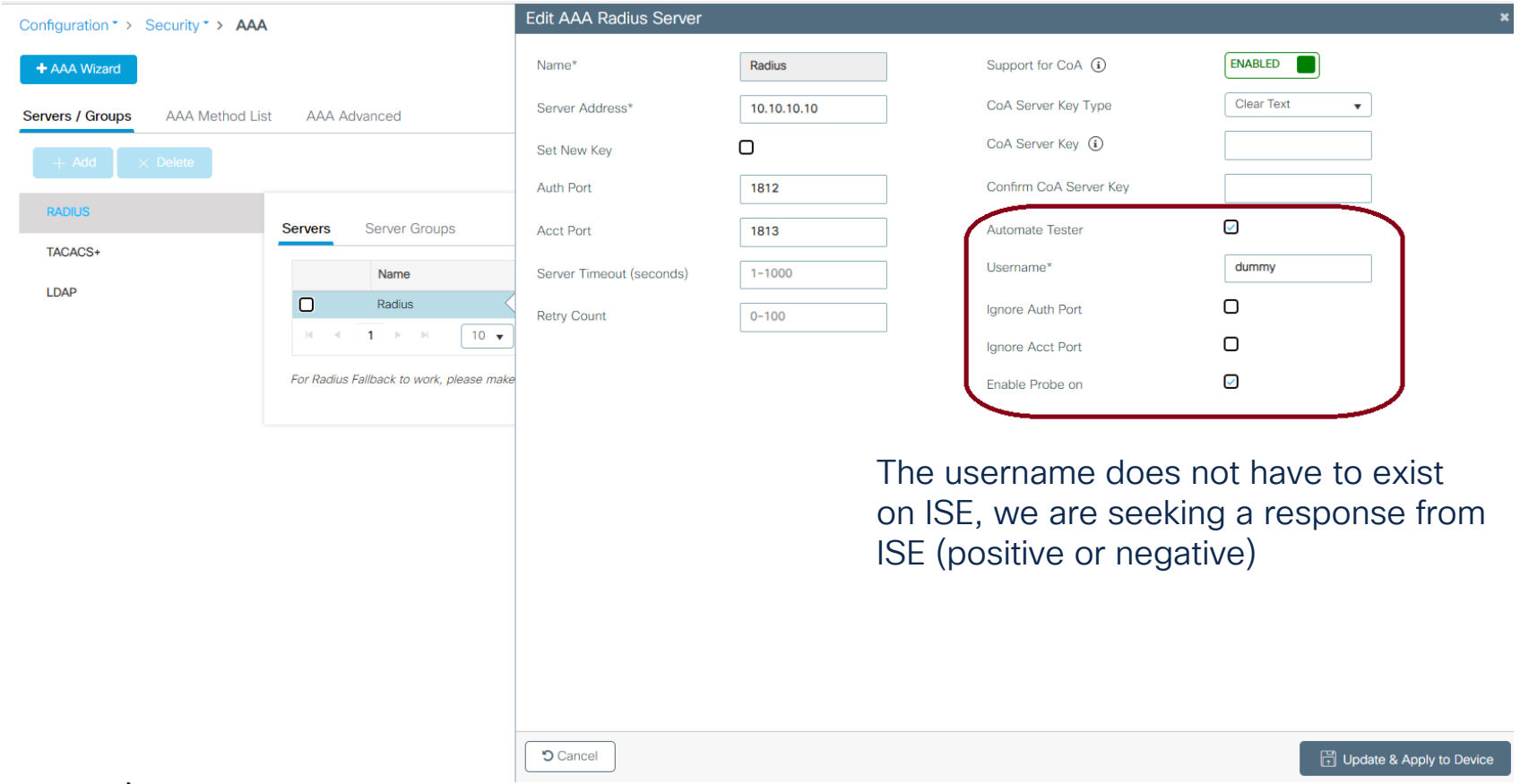


Dead Time = For how long will the server be considered dead.
Dead Criteria Time = How long should the WLC wait before marking it dead once the Dead Criteria Tries have been exhausted.
Dead Criteria Tries = How many tries should the radius requests fail before marking it dead.

Radius Timers (Per Server)

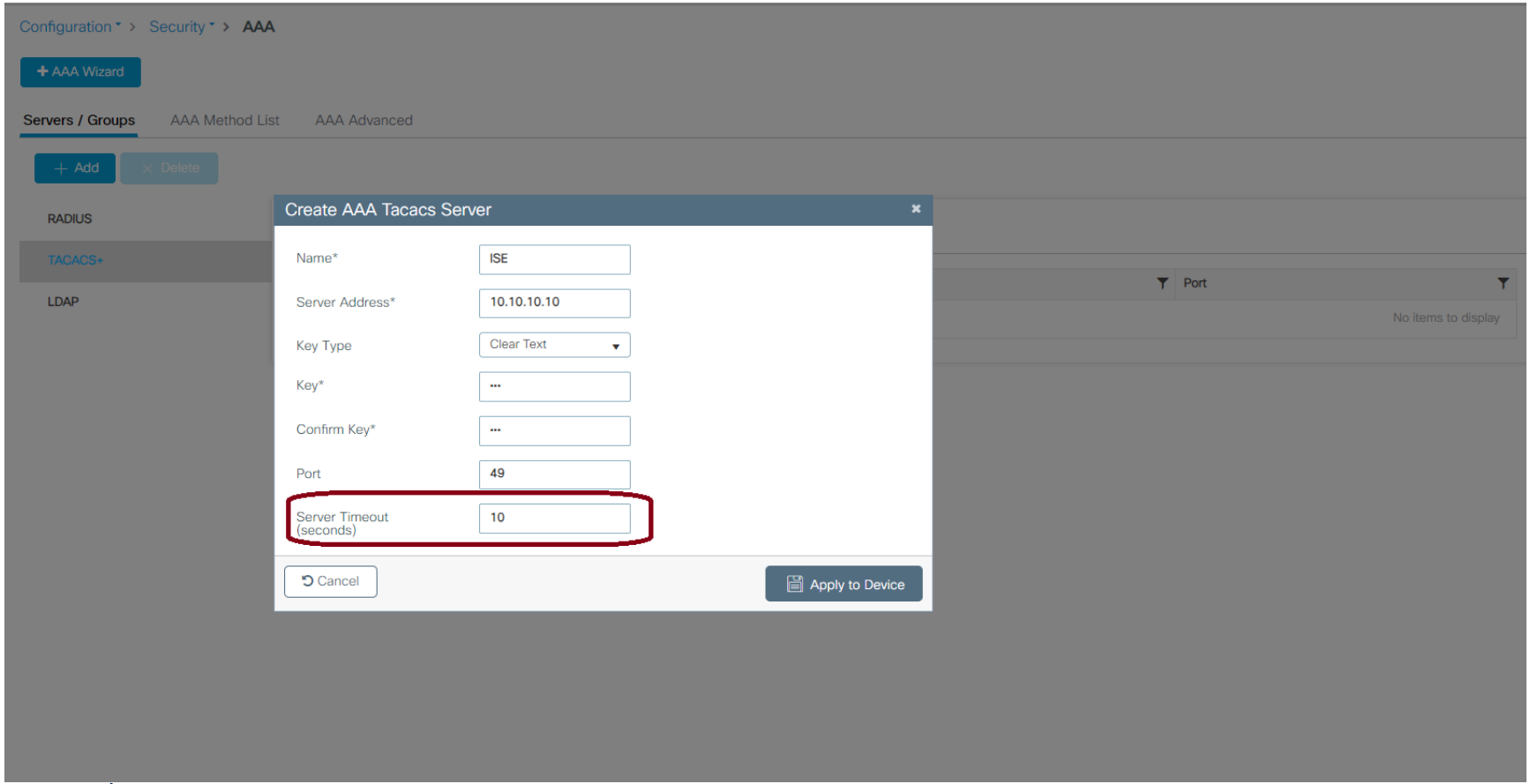


Automate Tested (Per Server)



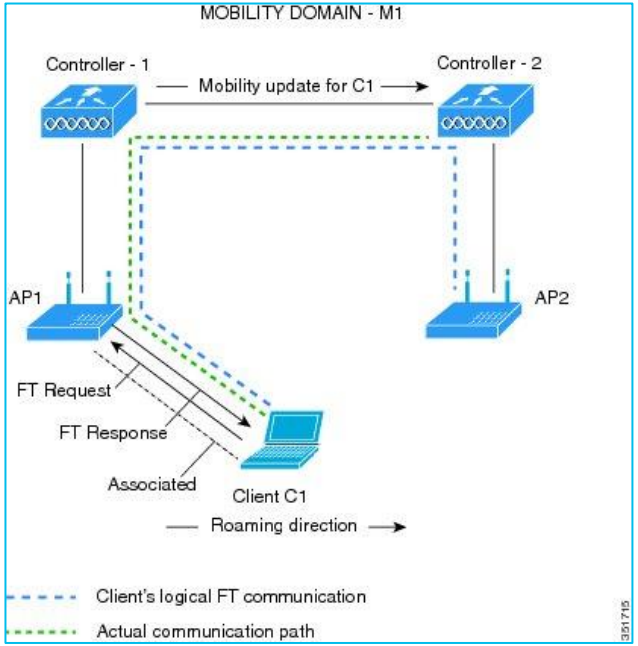
The username does not have to exist on ISE, we are seeking a response from ISE (positive or negative)

TACACS+ Timer



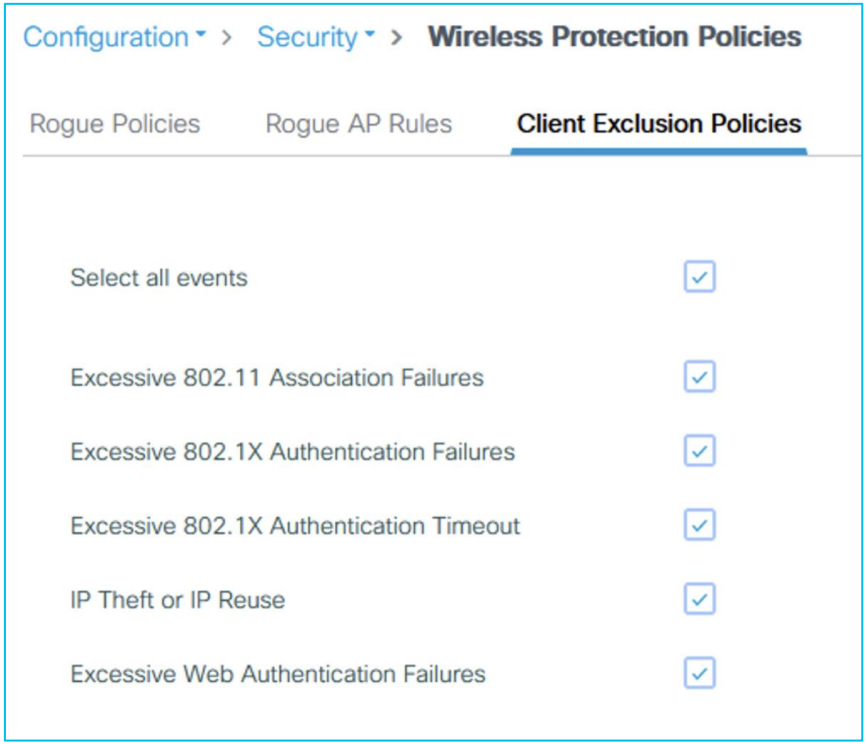
Use Fast BSS Transition (802.11r)

- Allow clients to roam without full 802.1x authentication.
- Supported by:
  - Apple Devices
  - Android Devices (platform and version dependent)
  - Some Windows devices (driver dependent)
- Clients that done support 802.11r work on the same WLAN.
- TAC recommends over-the-air mode.

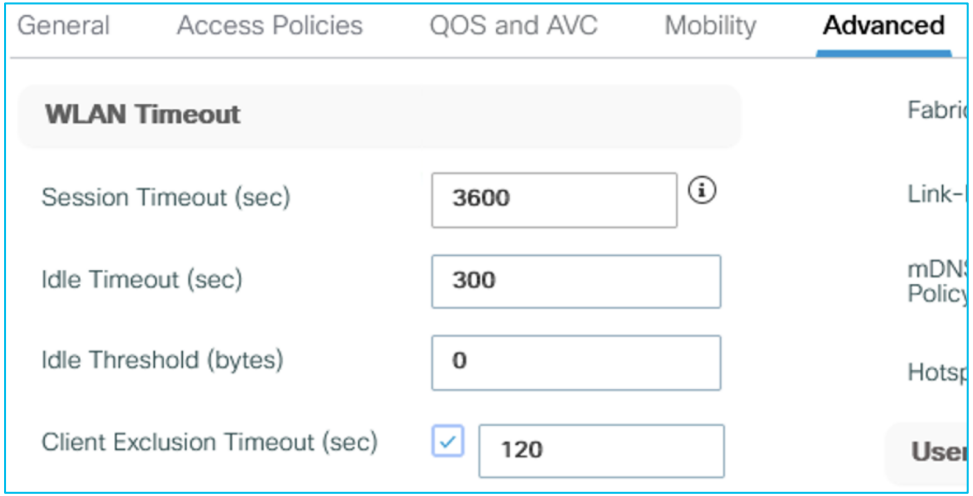


https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-11r-bss-fast-transition.html

9800 WLC Client Exclusions



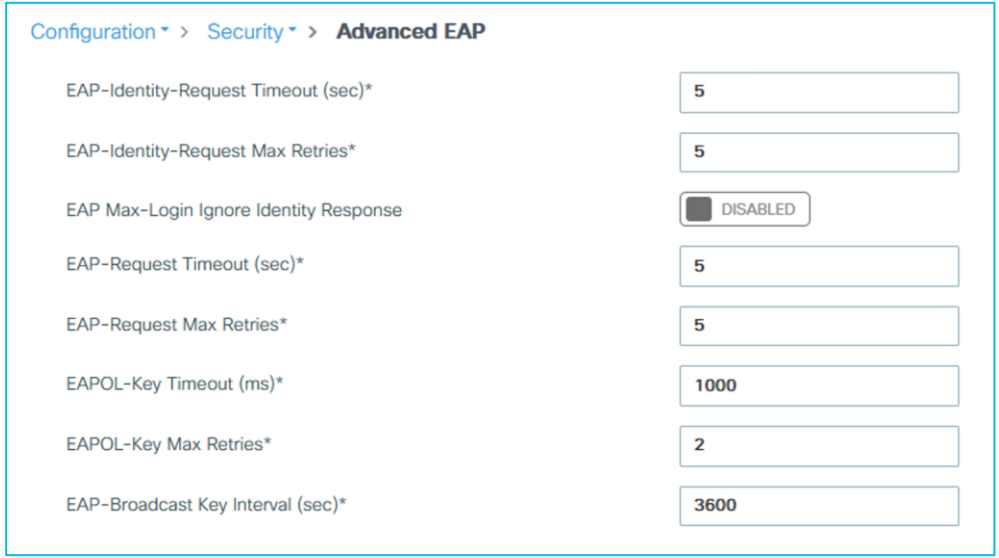
Configuration > Tags & Profiles > Policy



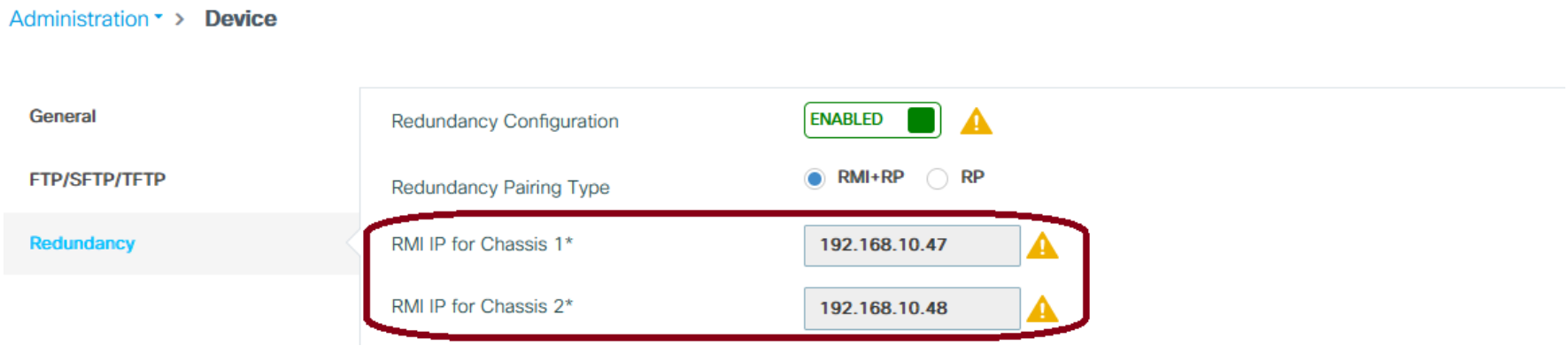
9800 WLC Client Exclusions

Tweaking EAP Timers

- Clients excluded on
  - 6th 802.1x failure
  - 5th 802.1x timeout
- Advanced EAP timers should be tweaked to allow exclusion before client restarts.



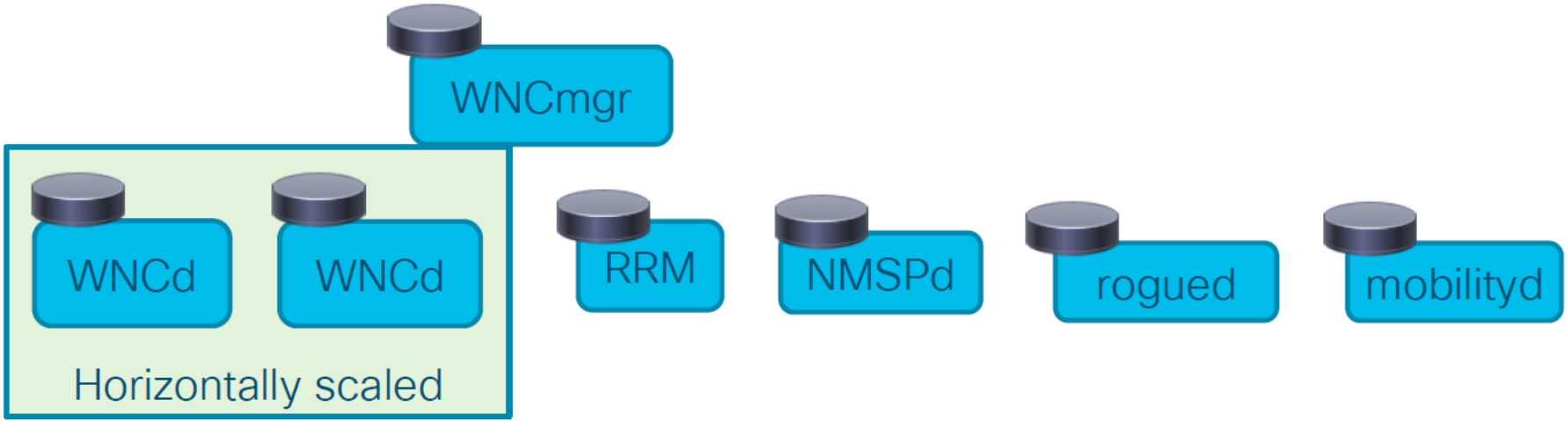
Consideration for C9800 High Avaliability



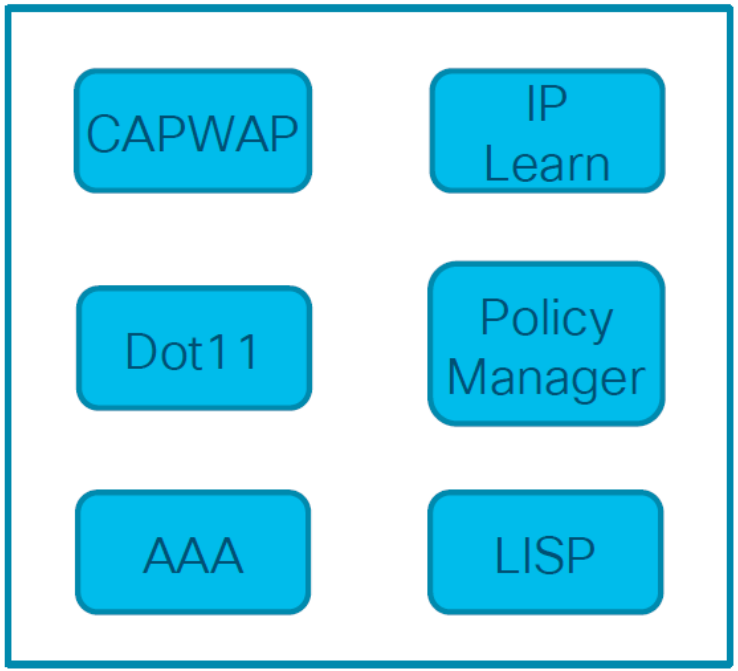
The active controller uses Wireless Management or RMI IP's to initiate AAA requests. Whereas the standby controller uses the RMI IP to initiate AAA requests. Thus, the RMI IPs must be added in AAA servers for a seamless client authentication and standby monitoring.

Avoiding Inter-WNCD Roaming

What Are WNCd's



What Are WNCd's



WNCd : controller process managing AP and client session

- Capwap : AP discovery
- Dot11 : Client dot11
- SANET/AAA: Client authentication
- EPM : Client policies
- SISF : client IP learning
- Client Orchestrator : Client State Transitions
- LISP-agent : L2 Lisp handling for Fabric deployment

Avoiding Inter-WNCD Roaming

- How Many WNCd's do I have?

```
show processes cpu platform sorted  |  count wncd
```

```
show platform software system all
```

← Specific for 9800-CL

Platform	WNCd Instances
EWC (on AP and Catalyst 9k switches)	1
C9800-L	1
C9800-CL (small)	1
C9800-CL (medium)	3
C9800-40	5
C9800-CL (large)	7
C9800-80	8

Avoiding Inter-WNCD Roaming

What's key here is, having all AP's from a single roaming domain be part of the same WNCD by having them within the same site tag

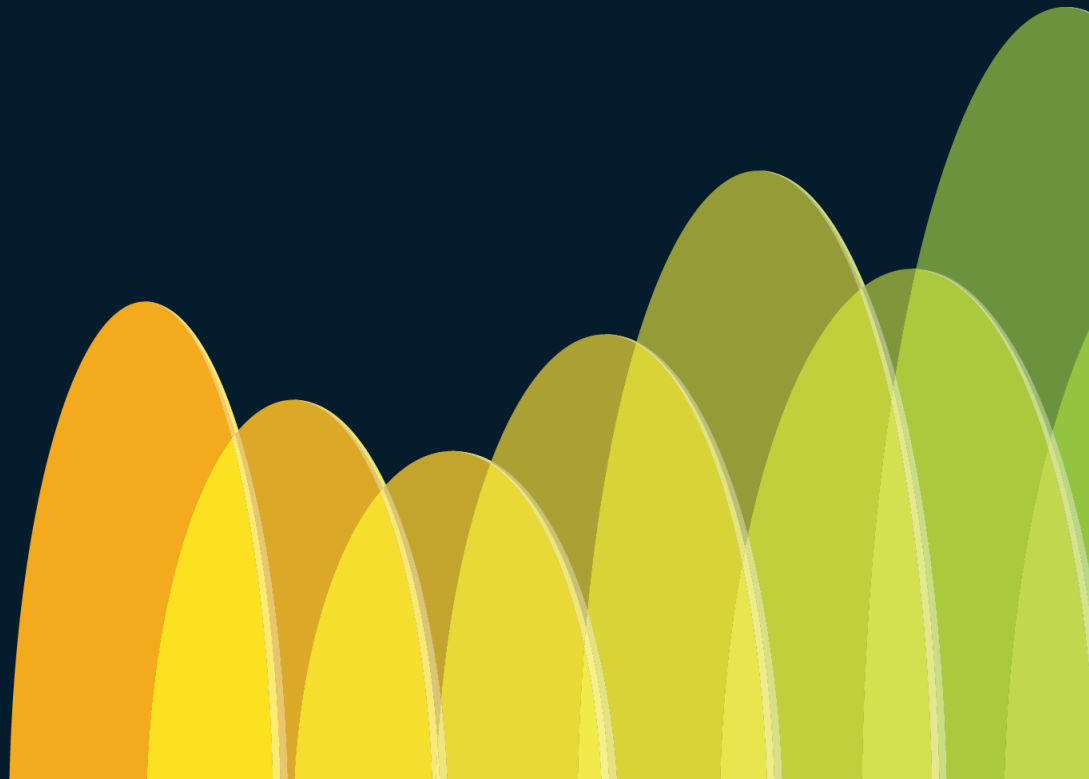
For example, if you have a 9800-40, handling one main office, plus 5 branch offices, with different AP counts, the configuration could look like this:

```
wireless tag site office-main
 load 120

wireless tag site branch-1
 load 10

wireless tag site branch-2
 load 12

wireless tag site branch-3
 load 45

wireless tag site branch-4
 load 80

wireless tag site branch-5
 load 5
```

The load command is a expected size hint, it does not have to match exactly the AP count, but it is normally set to the expected APs that might join.

As the 9800-40 has 5 WNCD's we would want to prevent the main office sharing its WNCD with any other branch, hence its the one with the highest load value.

Network Segmentations and Security Group Tags



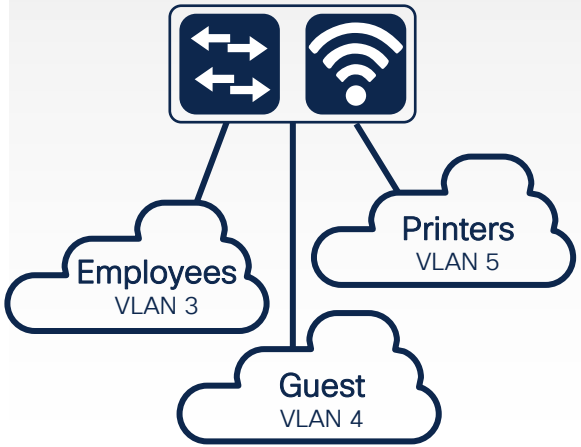
cisco Live!

ISE Segmentation Options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

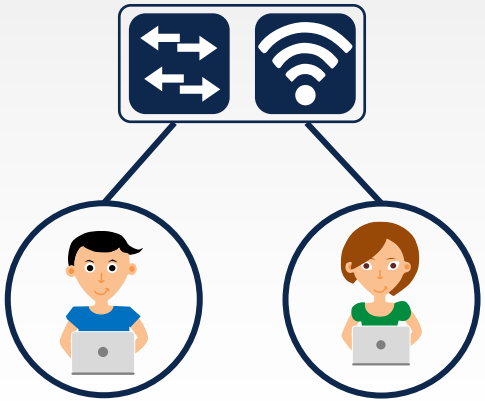
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)



Employee
`permit ip any any`

Contractor
`deny ip host <critical>`
`permit ip any any`

Security Group Tags

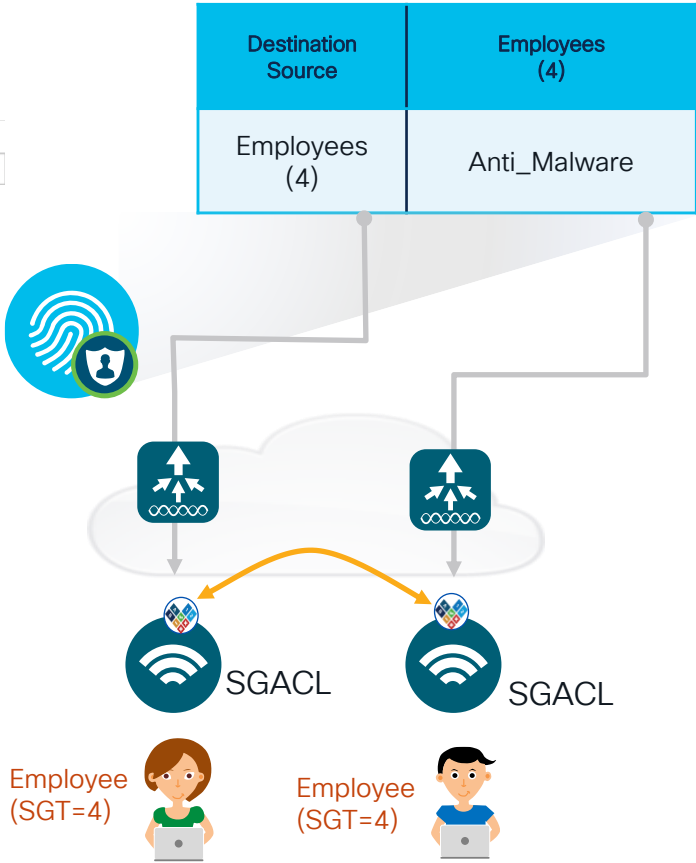
Cisco Group-Based Policy

16-bit SGT assignment and
SGT based Access Control

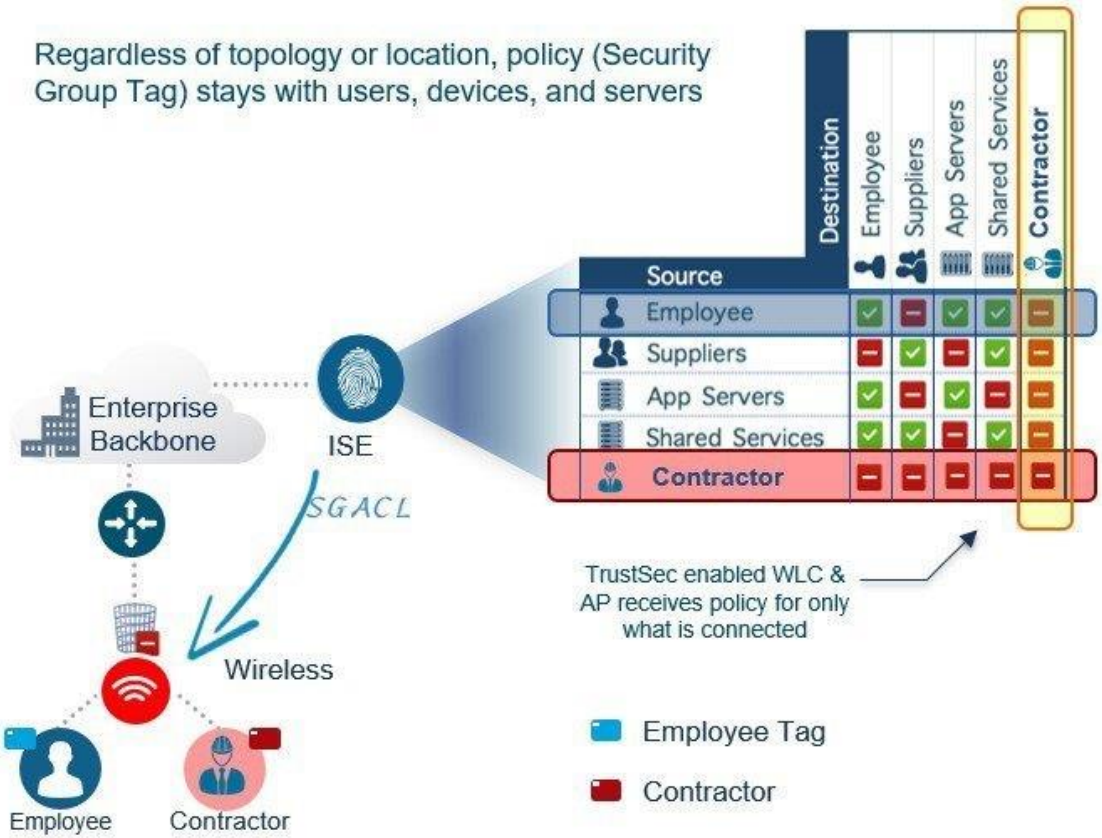
Dynamic Segmentation

Features	C9105/C9115/C9117	C9120/C9124/ C9130	C9136	CW9162/CW9164/CW9166	CW9163
TrustSec SXP, SGT	No for 9105	Yes	Yes	Yes	Yes

System Component	Platform	License	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement Services
Tier I Cisco Catalyst 9800 Series	Cisco Catalyst 9800 Series	No license for the 9800 itself. Each AP joined is licensed through global setting of either Essentials or Advantage	Support for v4/v6: Dynamic, IP to SGT, Subnet to SGT, Policy Profile to SGT	Speaker, Listener V4 V5 from 17.9.1	SGT over Ethernet SGT over VXLAN	SGACL V4, V6 (Note 17), Monitor mode, Logging. *SGT NetFlow v9*



ISE Policy Download



Summary

- There is no common authentication method that is optimal for all use cases, deployments or client types.
- ISE and Cisco Wireless enables us to easily manage and maintain a various set of authentication methods for various use cases.
- Follow the best practices prescribed to avoid interruptions and inconveniences in the network
- This will **simplify** managing the setup and **scaling** it up.
- Follow the lab guide that will be provided and practice implementation.

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

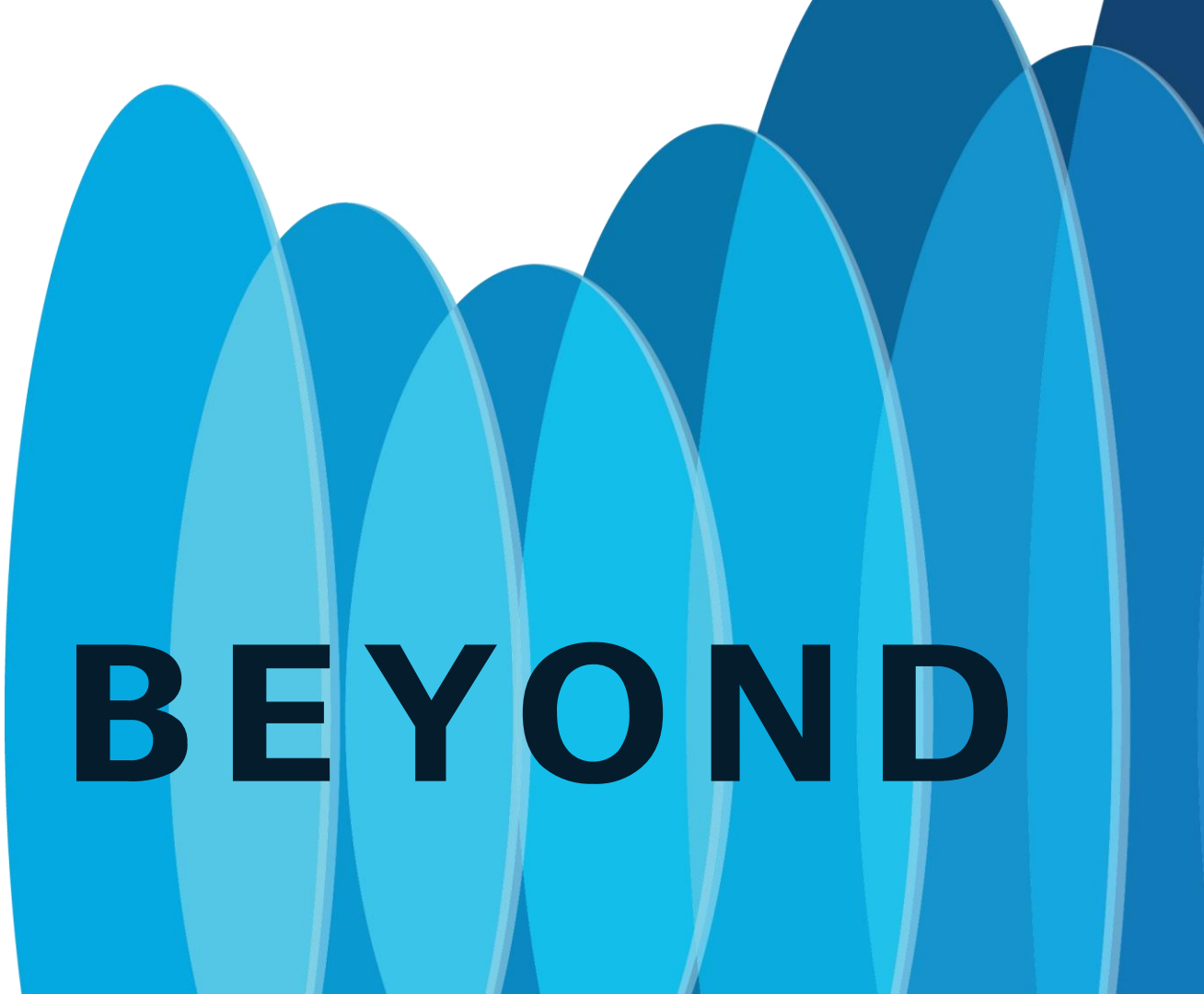
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: surendrr@cisco.com , rahamdan@cisco.com


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND