

Securing Wireless Networks with Cisco Identity Services Engine and Access Manager

cisco Live !

Fletcher Joyce
Solutions Engineer
fjoyce@cisco.com

Cisco Webex App

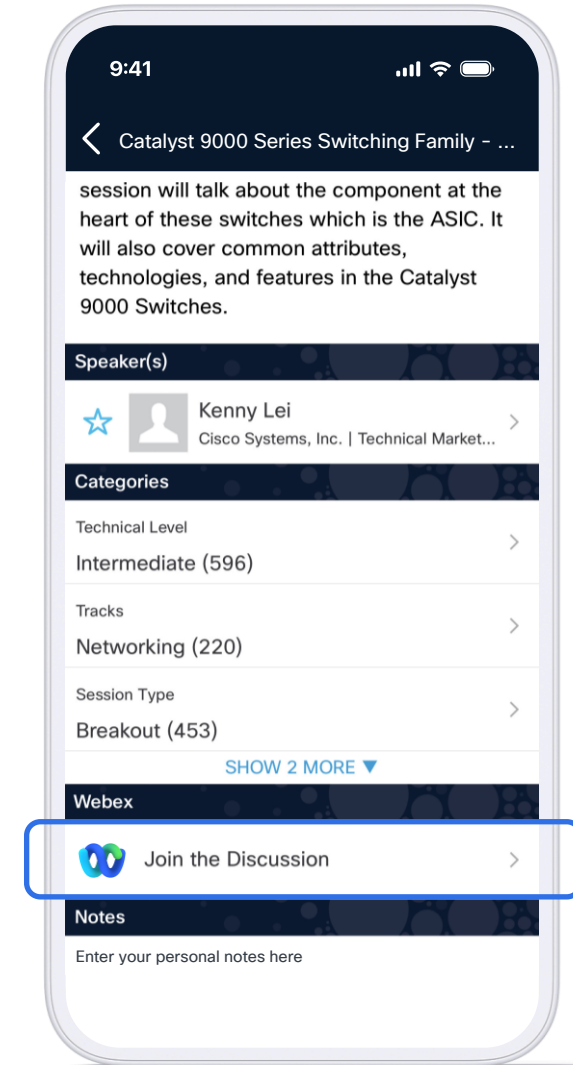
Questions?

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-2047>

Agenda

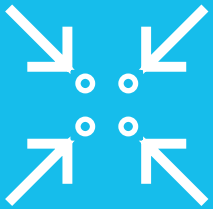
- 01 Introduction
- 02 Access Policy Fundamentals
- 03 Managing Wireless Access with Identity Services Engine
- 04 Wireless Access Control with Cisco Access Manager
- 05 Takeaways

About Me



Before we jump in...

A security policy framework should help



**minimize exposure in
an organization**



**provide multi-tenancy
in a secure way**



**maintain compliance
and pass security
audits**



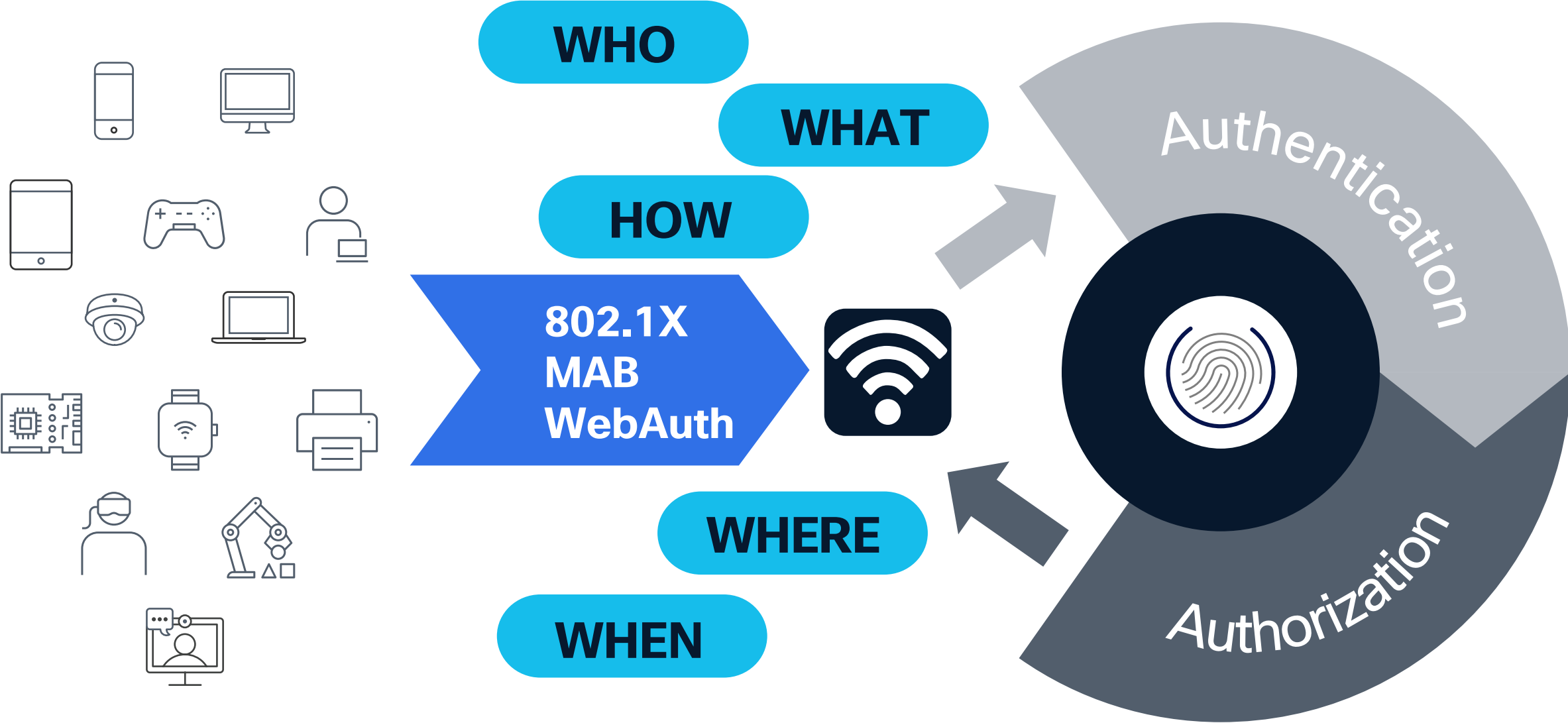
**quarantine malicious
or compromised
devices**



**implement a zero-
trust framework**

Access Policy Fundamentals

Access Policy







A9541
MUC-AOI

WED 03 FEB 2016

GATE

INTL

SEAT

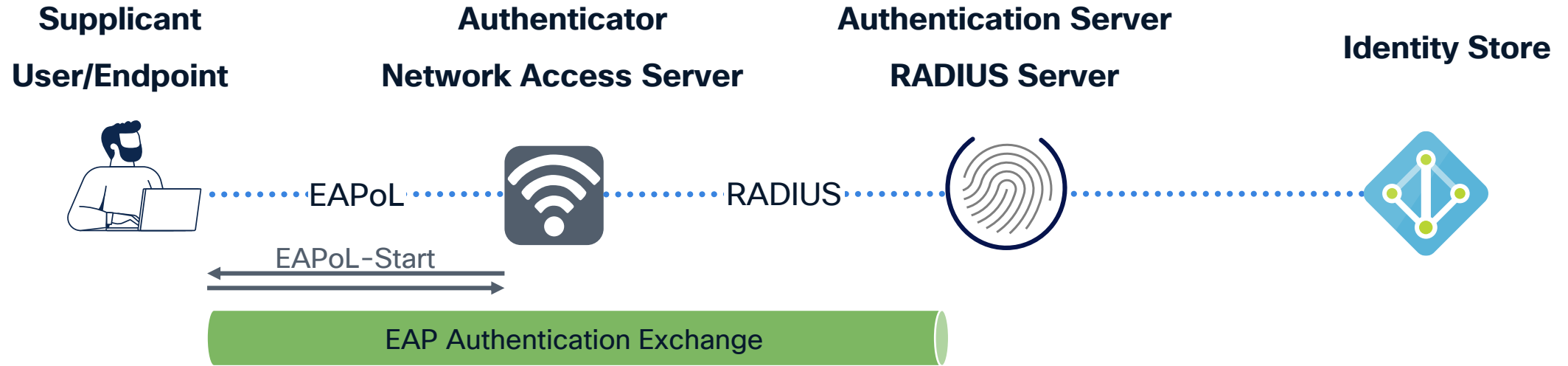
16A

PASSPORT

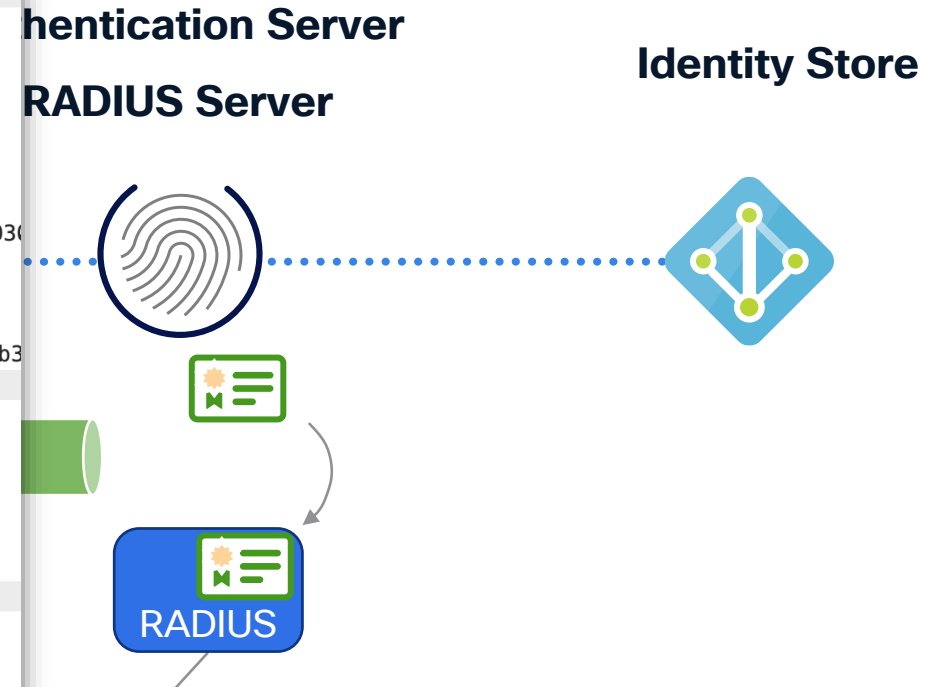




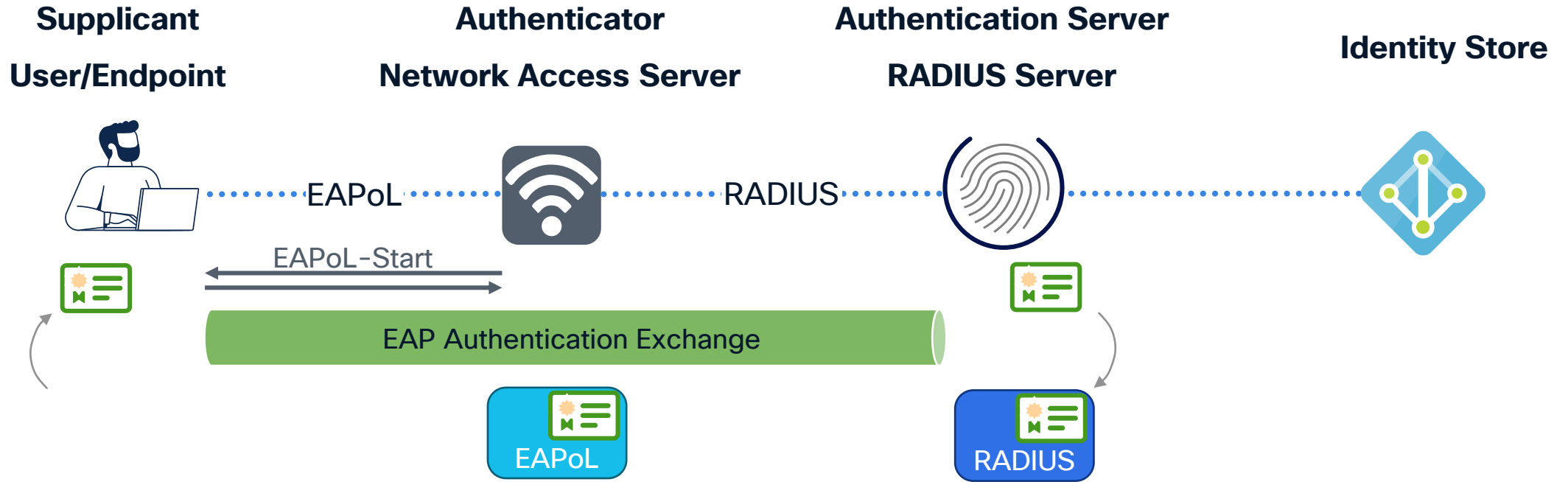
802.1X



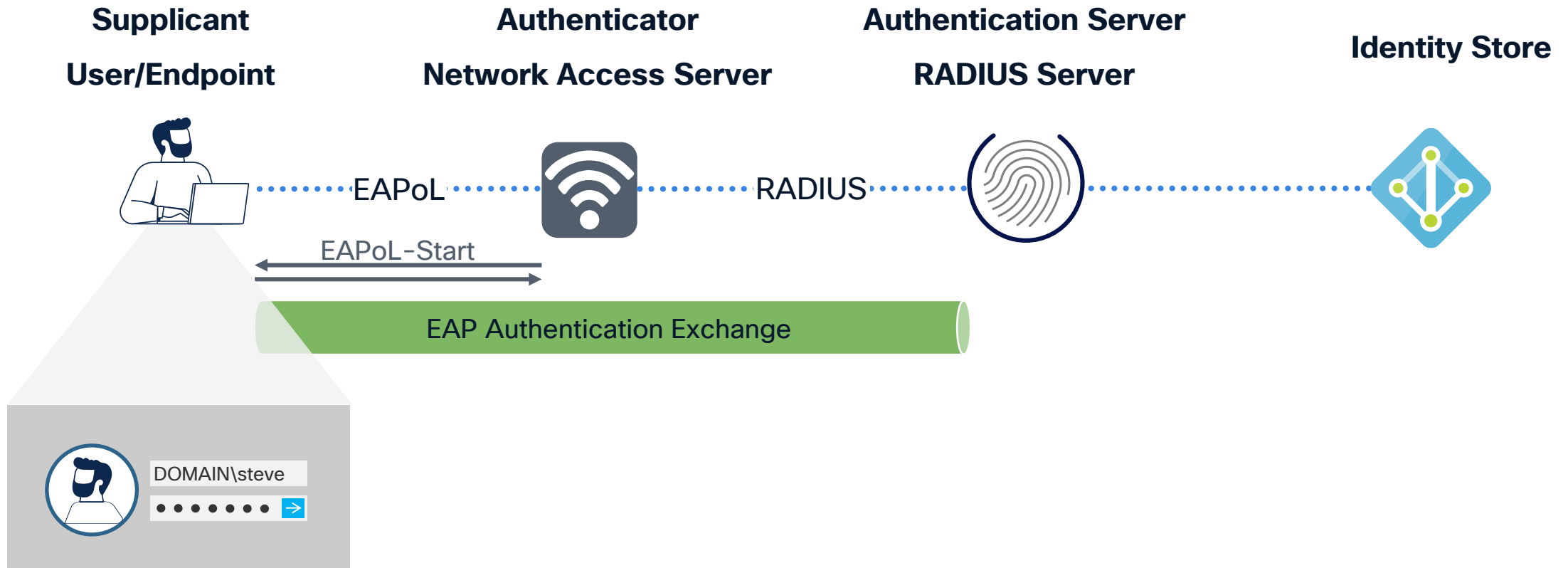
802.1X

[illegible]

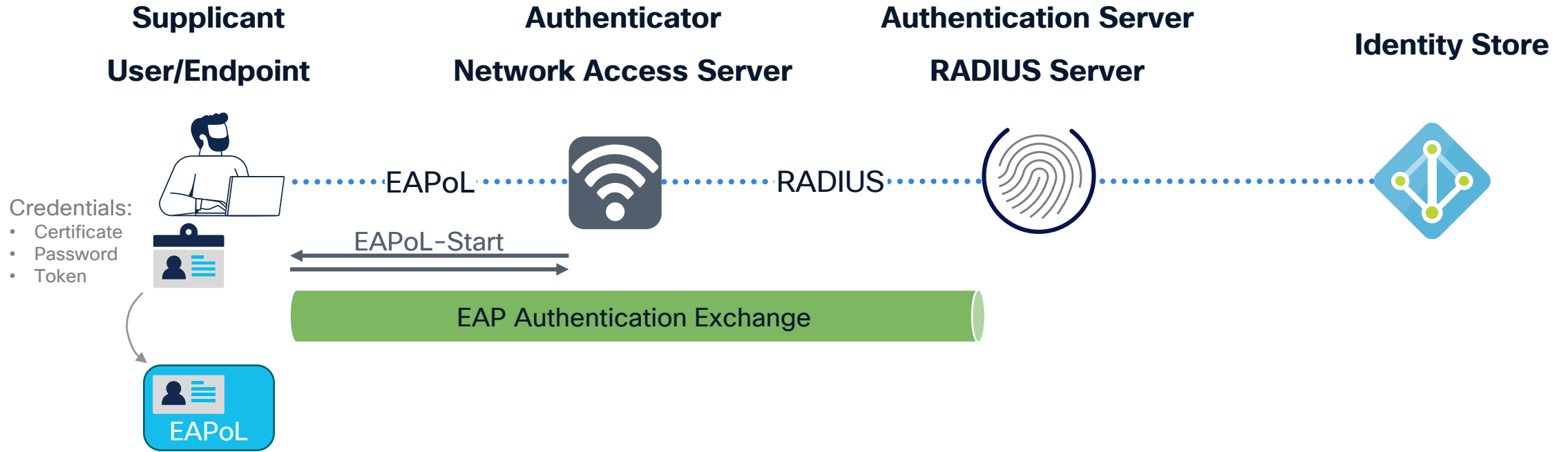
802.1X



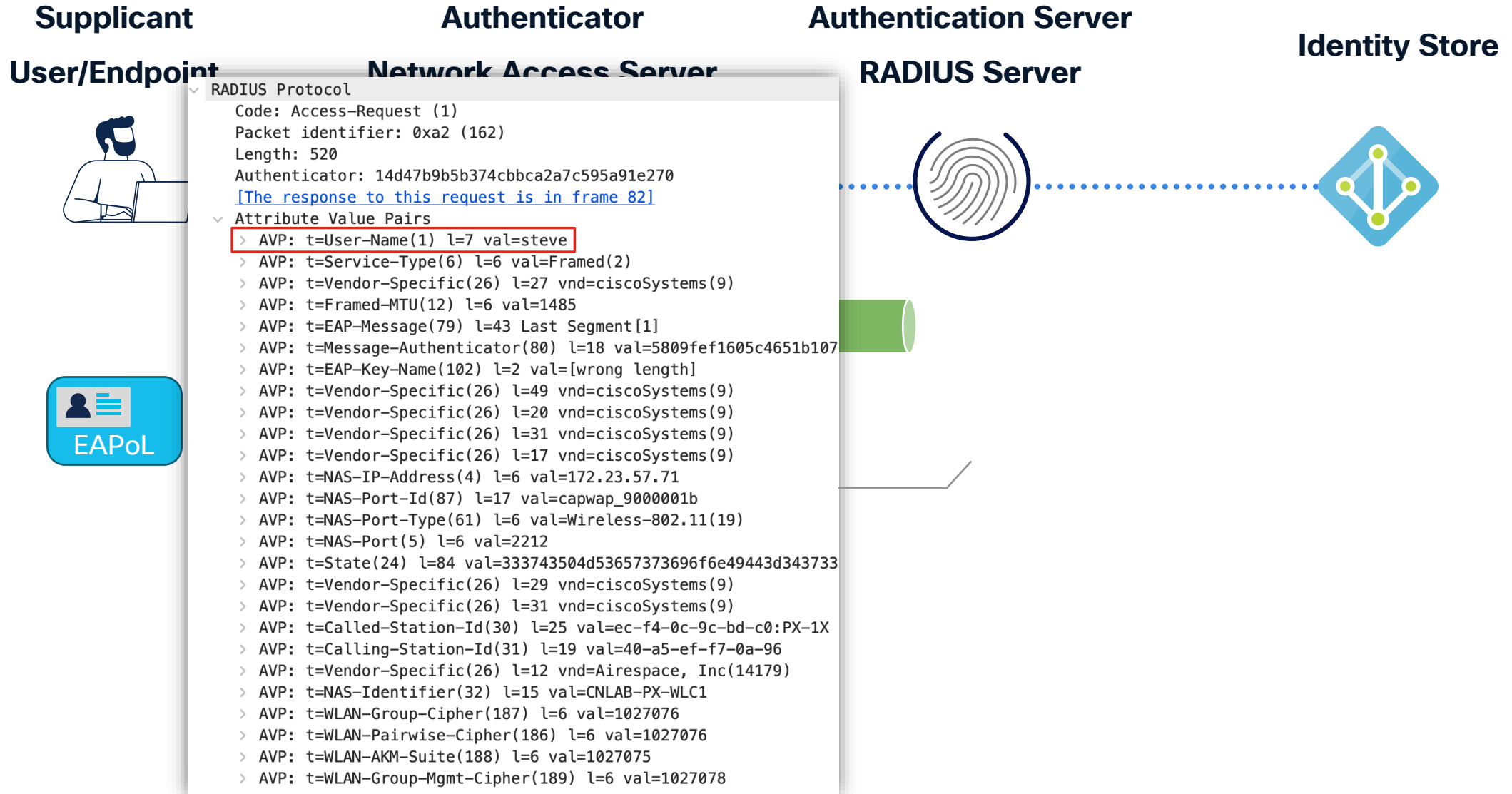
802.1X



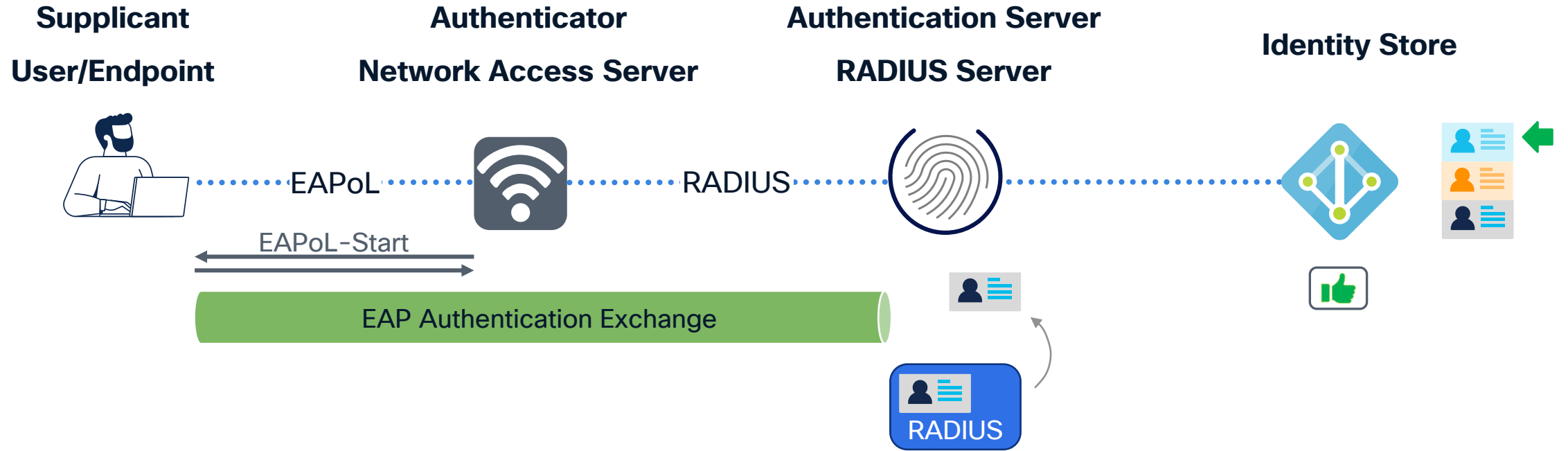
802.1X



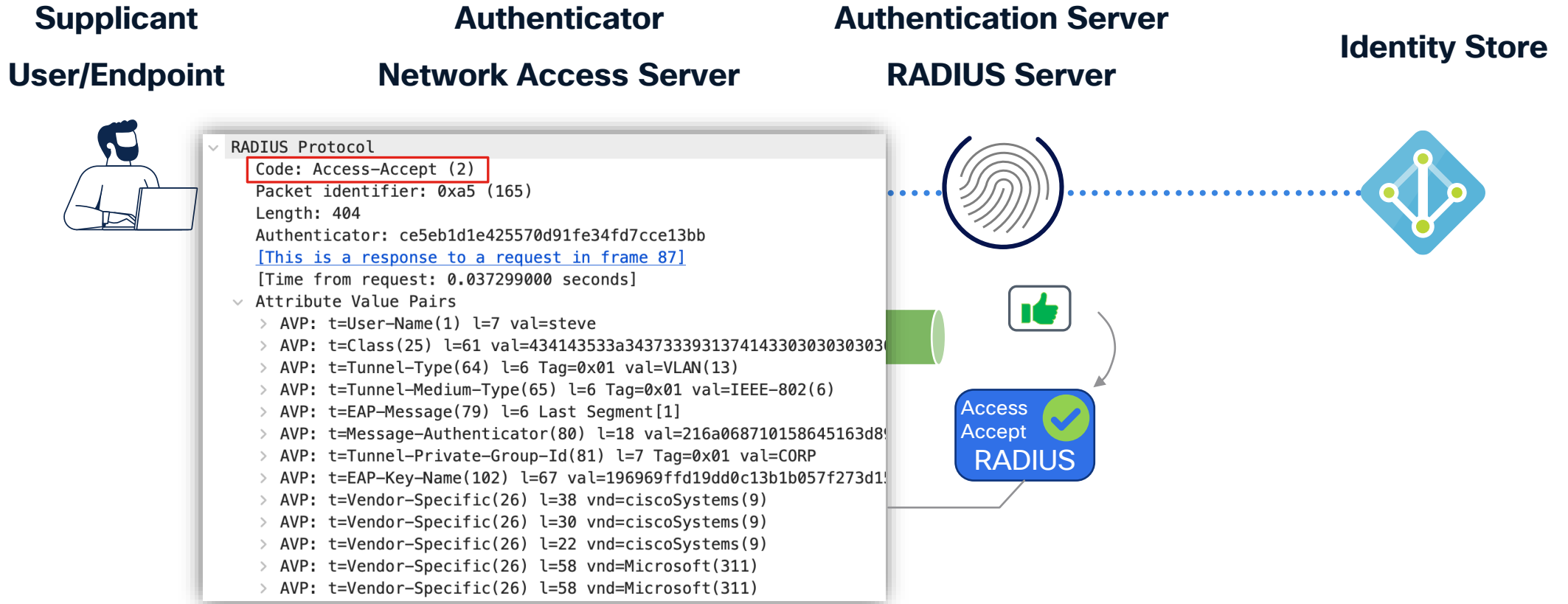
802.1X



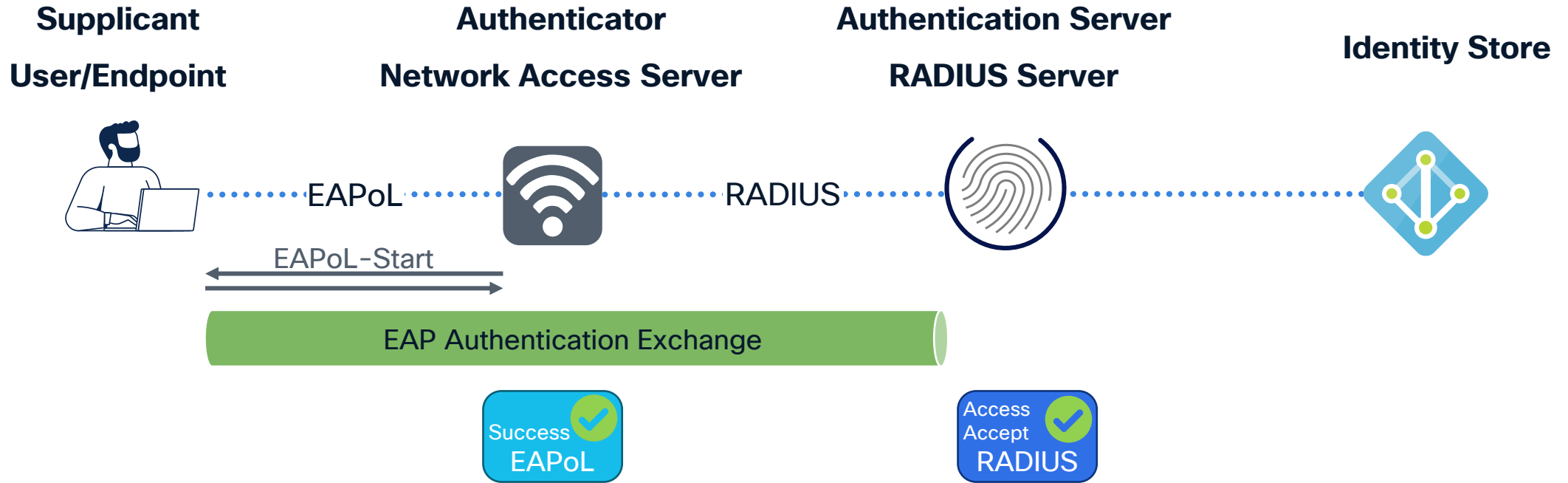
802.1X



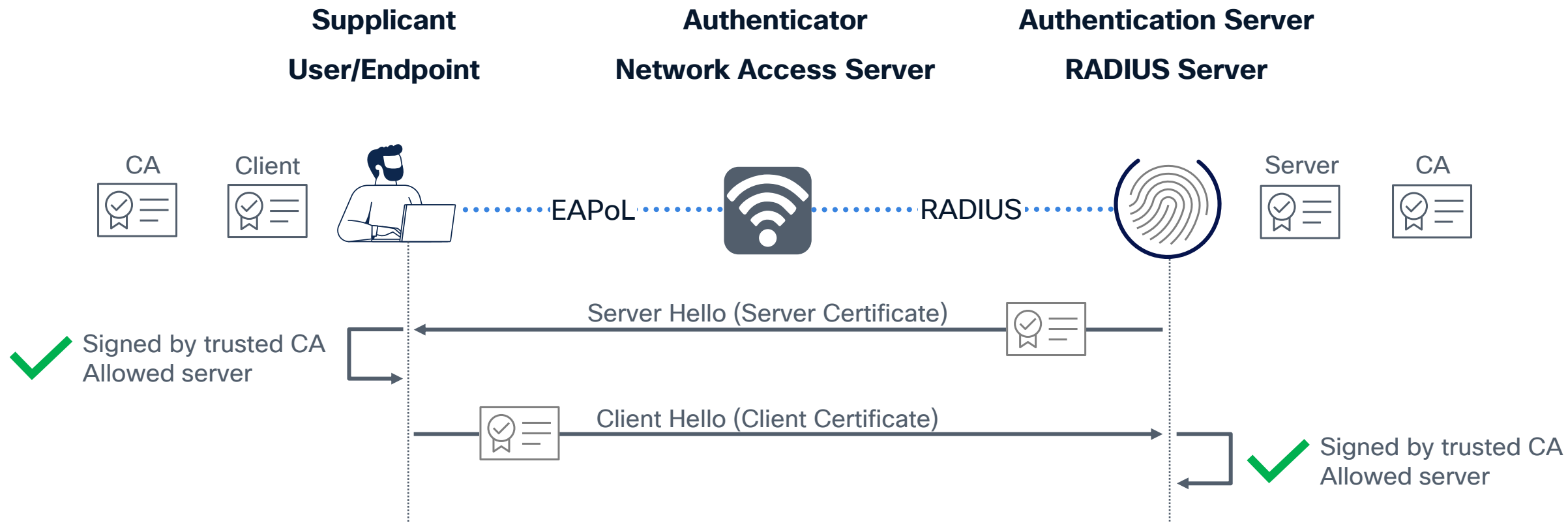
802.1X



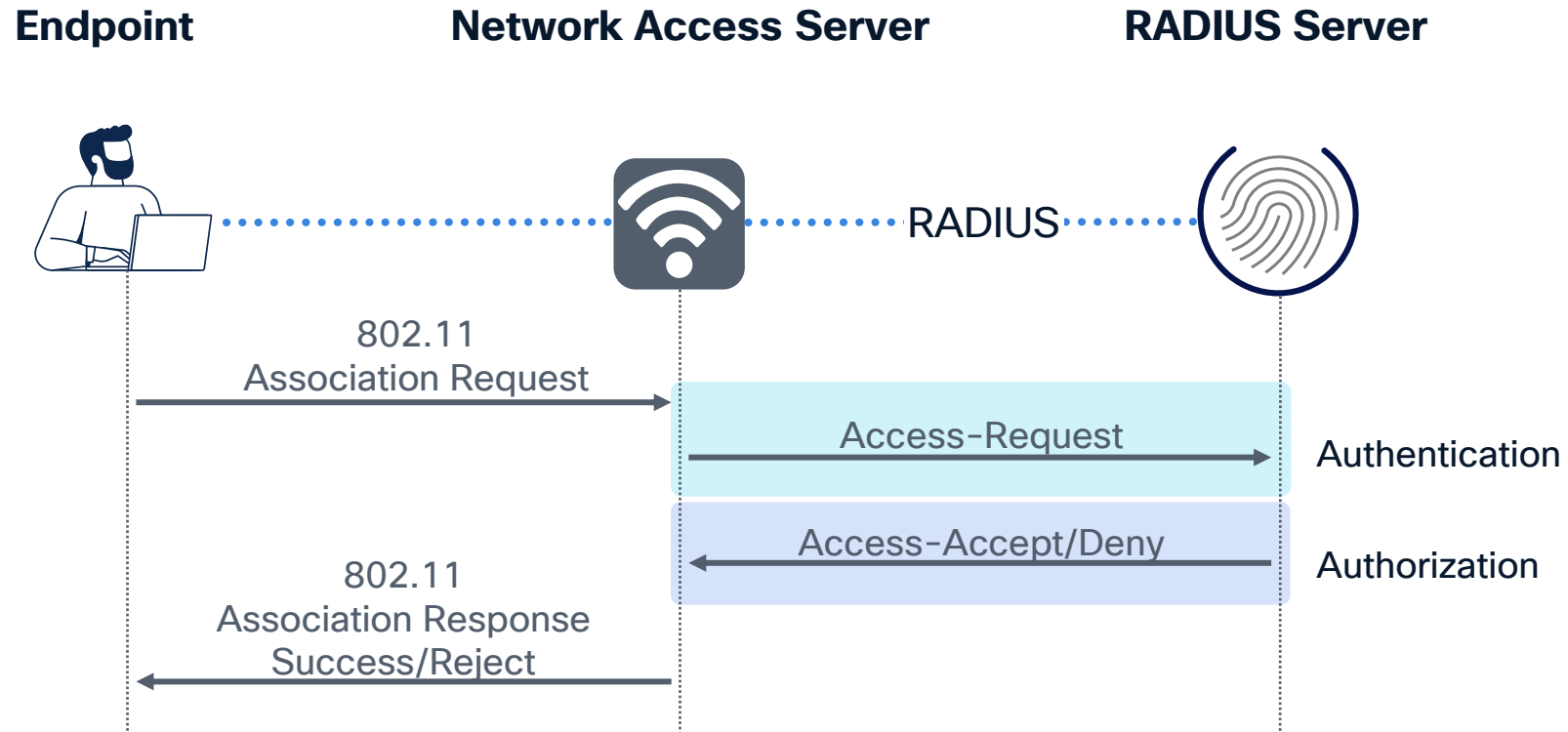
802.1X



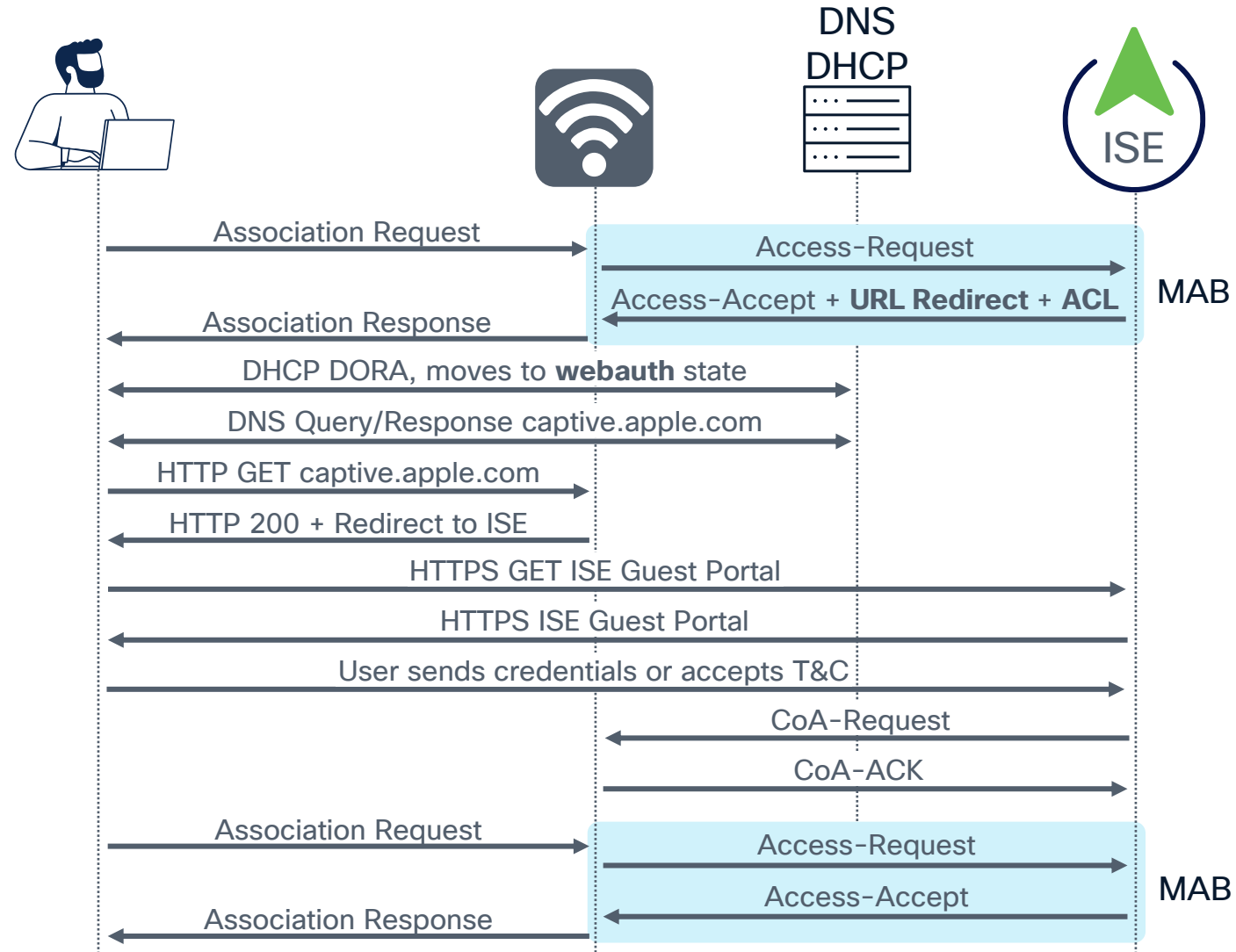
EAP-TLS



MAC Authentication



Central Web Authentication (CWA)



RADIUS Packet Format

Access-Request

```

RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0xa2 (162)
Length: 520
Authenticator: 14d47b9b5b374cbbca2a7c595a91e270
[The response to this request is in frame 82]
Attribute Value Pairs
> AVP: t=User-Name(1) l=7 val=steve
> 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=43 Last Segment[1]
> AVP: t=Message-Authenticator(80) l=18 val=5809fef1605c4651b107
> AVP: t=EAP-Key-Name(102) l=2 val=[wrong length]
> 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=31 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=17 vnd=ciscoSystems(9)
> AVP: t=NAS-IP-Address(4) l=6 val=172.23.57.71
> AVP: t=NAS-Port-Id(87) l=17 val=capwap_9000001b
> AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
> AVP: t=NAS-Port(5) l=6 val=2212
> AVP: t=State(24) l=84 val=333743504d5365737369666e49443d343733
> AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
> AVP: t=Called-Station-Id(30) l=25 val=ec-f4-0c-9c-bd-c0:PX-1X
> AVP: t=Calling-Station-Id(31) l=19 val=40-a5-ef-f7-0a-96
> AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
> AVP: t=NAS-Identifier(32) l=15 val=CNLAB-PX-WLC1
> AVP: t=WLAN-Group-Cipher(187) l=6 val=1027076
> AVP: t=WLAN-Pairwise-Cipher(186) l=6 val=1027076
> AVP: t=WLAN-AKM-Suite(188) l=6 val=1027075
> AVP: t=WLAN-Group-Mgmt-Cipher(189) l=6 val=1027078

```

Codes

Attributes
Vendor Specific

Access-Accept

```

RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0xa5 (165)
Length: 404
Authenticator: ce5eb1d1e425570d91fe34fd7cce13bb
[This is a response to a request in frame 87]
[Time from request: 0.037299000 seconds]
Attribute Value Pairs
> AVP: t=User-Name(1) l=7 val=steve
> AVP: t=Class(25) l=61 val=434143533a343733393137414330303030303
> AVP: t=Tunnel-Type(64) l=6 Tag=0x01 val=VLAN(13)
> AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x01 val=IEEE-802(6)
> AVP: t=EAP-Message(79) l=6 Last Segment[1]
> AVP: t=Message-Authenticator(80) l=18 val=216a068710158645163d8
> AVP: t=Tunnel-Private-Group-Id(81) l=7 Tag=0x01 val=CORP
> AVP: t=EAP-Key-Name(102) l=67 val=196969ffd19dd0c13b1b057f273d1
> AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=30 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
> AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)

```

Managing Wireless Access with Identity Services Engine

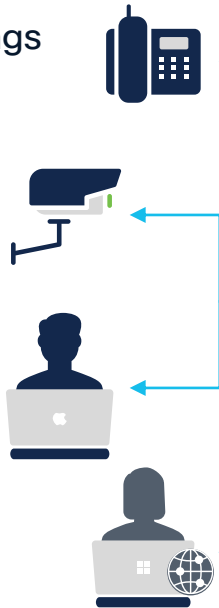
ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things



Network Devices

- Switches
- WLCs / APs
- VPN



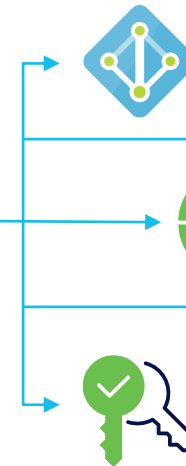
Cisco ISE

- 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

Integrating ISE with Cisco Wireless

	802.1X	MAB	VLAN	ACL	SGTs	URL Redirect	CoA	Profiling
Meraki	✓	✓	✓	✓ GPACL	✓ Adaptive Policy MR27.6 11ac W2+	✓	✓	Coming R31.2 11ax+
Catalyst	✓	✓	✓	✓ ACL dACL (17.10.1+)	✓	✓	✓	✓



Authorization Results

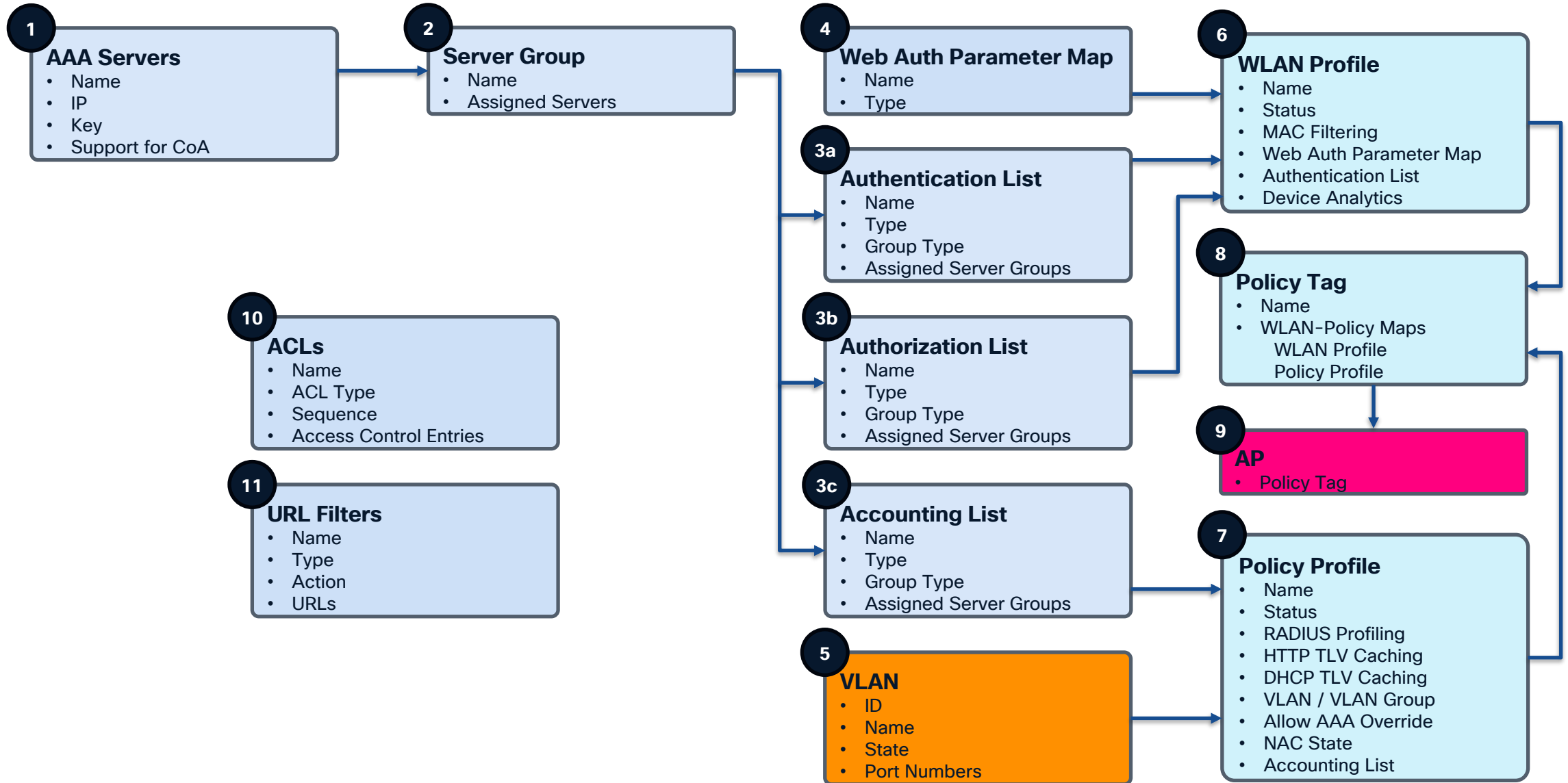
Identity and Context

Adding Wireless Network Devices to ISE

Wireless Infrastructure - Base Configuration for ISE

Catalyst 9800 Base Configuration for ISE

Catalyst 9800 Configuration for ISE



Configuration > Security > AAA

Create AAA Radius Server

General

RadSec

Name*	ISE1	Support for CoA ⓘ	ENABLED ☒
Server Address*	172.23.0.111	CoA Server Key Type	Clear Text ▼
PAC Key	☐	CoA Server Key ⓘ	
Key Type	Clear Text ▼	Confirm CoA Server Key	
Key* ⓘ		VRF	<input type="text"/> 
Confirm Key*		Automate Tester	☐
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	5		
Retry Count	3		

Cancel

Apply to Device

Configuration > Security > AAA

Create AAA Radius Server

GeneralRadSec

Name*

ISE1

Server Address*

172.23.0.111

PAC Key

☐

Key Type

Clear Text

Support for CoA ⓘ

ENABLED

CoA Server Key Type

Clear Text

CoA Server Key ⓘ

Confirm CoA Server Key

Acct Port

1813

Server Timeout (seconds)

5

Retry Count

3

Cancel

Apply to Device

Support for CoA ⓘ

ENABLED

Configuration > Security > AAA

Create AAA Radius Server Group

Name*	ISEgroup
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	5
Load Balance	☐ DISABLED
IPv4 Source Interface	Search or Select ⓘ
IPv4 VRF	Search or Select ⓘ
IPv6 Source Interface	Search or Select ⓘ
IPv6 VRF	Search or Select ⓘ

Available Servers

Assigned Servers

ISE1
ISE2

Assigned Servers

ISE1
ISE2

Configuration > Security > AAA

Quick Setup: AAA Authentication

Method List Name*

ISEauthCdot1X

Type*

dot1x



Group Type

group



Fallback to local



Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

ISEgroup



Assigned Server Groups

ISEgroup

 Cancel

Apply to Device

Configuration > Security > AAA

Quick Setup: AAA Authorization

Method List Name*

ISEauthZnetwork

Type*

network

Group Type

group

Fallback to local

☐

Authenticated

☐

Available Server Groups

radius

ldap

tacacs+

Assigned Server Groups

ISEgroup

>

<

>>

<<

ISEgroup

Cancel

Apply to Device

Assigned Server Groups

ISEgroup

Configuration > Security > AAA

Quick Setup: AAA Accounting

Method List Name*

ISEaccTidentity

Type*

identity



Available Server Groups

radius
ldap
tacacs+



Assigned Server Groups

ISEgroup

Assigned Server Groups

ISEgroup



Cancel



Apply to Device



Configuration > Tags & Profiles > WLANS

Add WLAN

General Security Advanced

Profile Name* SECURE

SSID* SECURE

WLAN ID* 1

Status ☐ DISABLED

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 ▼

Cancel Apply to Device



Configuration > Tags & Profiles > WLANS

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	☐	Beacon Protection	☒

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 (AKM)

FT + 802.1X	☒	802.1X-SHA256	☒
OWE	☐	SAE	☐
FT + SAE	☐	SAE-EXT-KEY	☐
FT + SAE-EXT-KEY	☐		



Configuration > Tags & Profiles > WLANS

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List ISEauthCdot1X ▼

Local EAP Authentication ☐

Static WEP ☐ None ☐

WPA Parameters

WPA Policy ☐	WPA2 Policy ☐
GTK Randomize ☐	WPA3 Policy ☒
Transition Protection ☐	Replay Protection ☐

Fast Transition

Status Enabled ▼

Over the DS ☐

PMF Required ▼

Association Comeback Timer* 1

SA Query Time* 200

FT + SAE ☐ SAE-EXT-KEY ☐

FT + SAE-EXT-KEY ☐

Cancel Apply to Device

Authentication List

ISEauthCdot1X ▼

Configuration > Tags & Profiles > WLANS

Add WLAN

GeneralSecurityAdvanced

Profile Name*

OPEN

SSID*

OPEN

WLAN ID*

1

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

DISABLED

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

Cancel

Apply to Device



Configuration > Tags & Profiles > WLANS

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

☐ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☒ None

MAC Filtering

☒

Authorization List*

ISEauth...

OWE Transition Mode

☐

Lobby Admin Access

☐

Fast Transition

Status

Disabled

Over the DS

☐

Reassociation Timeout *

20

Cancel

Apply to Device

Configuration > Tags & Profiles > WLANS

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

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

MAC Filtering ☒  Configuration List* ISEauth... ⓘ

OWE Transition Mode ☐

Lobby Admin Access ☐

Fast Transition ☐

Status Disabled

MAC Filtering ☒

Cancel Apply to Device

Configuration > Tags & Profiles > WLANS

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

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

MAC Filtering ☒ Authorization List* ISEauth... ⓘ

OWE Transition Mode ☐

Lobby Admin Access ☐

Fast Transition ☐

Status Disabled

Authorization List* ISEauth... ⓘ

Cancel Apply to Device

Configuration > Tags & Profiles > Policy

Add Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

USERSpolicy

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

Configuration > Tags & Profiles > Policy

Add Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

28800

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

☒60

Guest LAN Session Timeout

☐

DHCP

IPv4 DHCP Required

☐

DHCP Server IP Address

DHCP Server VRF

Search or Select

Show more >>>

AAA Policy

Allow AAA Override

☒

NAC State

☒

Fabric Profile

☐

Search or Select

Link-Local Bridging

☐

mDNS Service Policy

Search or Select

Hotspot Server

Search or Select

L3 Access

DISABLED

User Defined (Private) Network

Status

☐

Drop Unicast

☐

DNS Layer Security

DNS Layer Security Parameter Map

Not Configured

Flex DHCP Option for DNS

ENABLED

Flex DNS Traffic Redirect

IGNORE

WLAN Flex Policy

VLAN Central Switching

☐

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

BRKEWN-2047



Configuration > Tags & Profiles > Policy

Add Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

28800

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

☒ 60

Fabric Profile

☐

Search or Select

Link-Local Bridging

☐

mDNS Service Policy

Search or Select

Hotspot Server

Search or Select

L3 Access

DISABLED

User Defined (Private) Network

☒

DHCP Server VRF

Search or Select

Show more >>>

AAA Policy

Allow AAA Override

☒

NAC State

☒

DNS Layer Security Parameter Map

Not Configured

Flex DHCP Option for DNS

ENABLED

Flex DNS Traffic Redirect

IGNORE

WLAN Flex Policy

VLAN Central Switching

☐

Allow AAA Override ☒



Configuration > Tags & Profiles > Tags

Add Policy Tag

Name*ISEnabled

DescriptionEnter Description

WLAN-POLICY Maps : 0

+ Add

× Delete

WLAN Profile

SECURE

Policy Profile

USERSpolicy

Map WLAN and Policy

WLAN Profile*Search or Select

Policy Profile*Search or Select

×

✓

Cancel

Apply to Device

WLAN Profile

SECURE

Policy Profile

USERSpolicy

1

10

items per page

1 - 1 of 1 Items



Configuration > Wireless > Access Points

Edit AP

General Interfaces High Availability Inventory Geolocation ICap Advanced Support Bundle

General

AP Name*
AP6B8B4567-0001

Location*
default location

Base Radio MAC
0a0b.0c00.0100

Ethernet MAC
0a0b.0cf0.0001

MLD Base MAC ⓘ
0000.0000.0000

Admin Status
ENABLED ☒

AP Mode
Local ▾

Operation Status
Registered

Fabric Status
Disabled

LED Settings

LED State
ENABLED ☒

Brightness Level
8 ▾

Flash Settings

Flash State
DISABLED

⬇️ Apply

Tags

Policy
ISEenabled ▾

Site
default-site-tag ▾ ☒

RF
default-rf-tag ▾ ☒

Write Tag Config to AP
 ⓘ

Version

Primary Software Version
17.17.0.87

Predownloaded Status
N/A

Predownloaded Version
N/A

Next Retry Time
N/A

Boot Version
1.1.2.4

IOS Version
17.17.0.87

Mini IOS Version
0.0.0.0

IP Config

CAPWAP Preferred Mode
IPv4

DHCP IPv4 Address
172.23.57.197

Static IP (IPv4/IPv6)
☐

Time Statistics

Up Time
2 days 17 hrs 34 mins
34 secs

Controller Association Latency
2 secs

Policy

ISEenabled ▾

Meraki Wireless Base Configuration for ISE

Meraki Wireless Configuration for ISE

Wireless > Configure > Access Control

Security WPA3 Enterprise with 1 RADIUS server and 1 accounting server

- ☐ Open (no encryption)
Any user can associate
- ☐ Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption
- ☐ Password
Users must enter a passphrase to associate ⓘ

- ☐ MAC-based access control (no encryption)

my RADIUS server ▼

RADIUS server is queried at association time

MAB

- ☐ Enterprise with

my RADIUS server ▼

User credentials are validated with 802.1X at association time

802.1X

- ☐ Identity PSK with RADIUS

MAC-based Authentication ▼

RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

iPSK

Splash page Cisco ISE authentication

- ☒ Cisco Identity Services Engine (ISE) Authentication ⓘ
Users are redirected to the Cisco ISE web portal for device posturing and guest access

Web Auth

Meraki Wireless Configuration for ISE

Wireless > Configure > Access Control

RADIUS

1 RADIUS server, 1 accounting server

RADIUS servers

#	Host IP or FQDN	Auth port	Secret	RadSec ⓘ	Test	Actions
1	172.23.57.11	1812		☐	<div>Test</div>	...

Add server

 3 max.

RADIUS accounting servers

#	Host IP or FQDN	Acct port	Secret	RadSec ⓘ	Actions
1	172.23.57.11	1813		☐	...

Adding Wireless Network Devices to ISE

ISE Configuration for Wireless - NAD

Administration > Network Resources > Network Devices

Catalyst 9800

Name	WLC1		
Description			
	IP Address	* IP :	172.23.57.71 / 32

ISE Configuration for Wireless - NAD

Administration > Network Resources > Network Devices

Catalyst 9800 - Flexconnect Meraki

Name

MerakiAPs-Network1

Description

IP Address

⌵

* IP :

172.23.58.0

/

24

ISE Configuration for Wireless - NAD

Administration > Network Resources > Network Devices

☒ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

☐ Use Second Shared Secret 

Second Shared
Secret

[Show](#)

CoA Port [Set To Default](#)

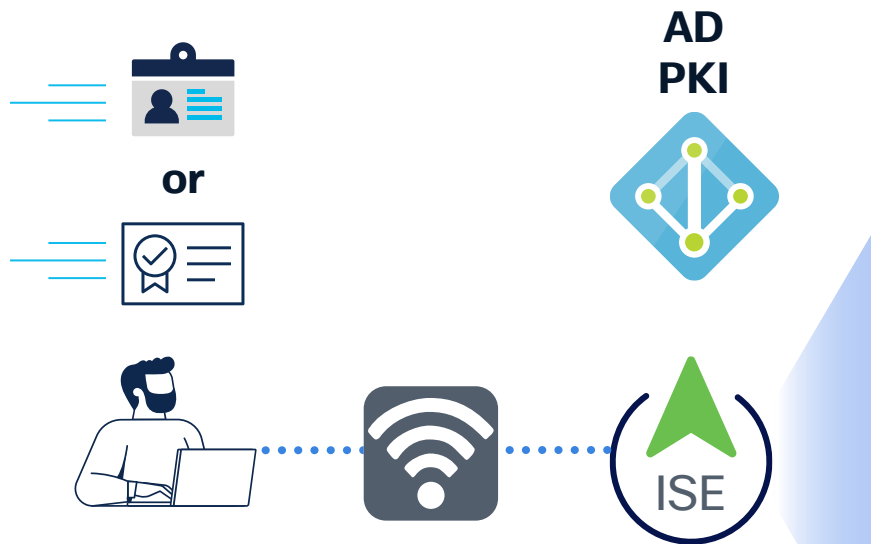
Identity and Context

Certificate Attributes



Dictionary	Attribute	ID	Info
CERTIFICATE	Binary Encoded		i
CERTIFICATE	Days to Expiry		i
CERTIFICATE	Extended Key Usage - Name		i
CERTIFICATE	Extended Key Usage - OID		i
CERTIFICATE	Is Expired		i
CERTIFICATE	Issuer		i
CERTIFICATE	Issuer - Common Name		i
CERTIFICATE	Issuer - Country		i
CERTIFICATE	Issuer - Domain Component		i
CERTIFICATE	Issuer - Email		i
CERTIFICATE	Issuer - Fingerprint SHA-256		i
CERTIFICATE	Issuer - Location		i

Active Directory Attributes



Dictionary	Attribute	ID	Info
AD	accountExpires		i
AD	adminCount		i
AD	badPasswordTime		i
AD	badPwdCount		i
AD	cn		i
AD	codePage		i
AD	countryCode		i
AD	dSCorePropagationData		i
AD	displayName		i
AD	distinguishedName		i
AD	givenName		i
AD	instanceType		i
AD	lastLogoff		i

Catalyst 9800 Advanced RADIUS Attributes

Configuration > Security > AAA

Radius Attributes

	Accounting	Authentication
Called-station-id	<div>macaddress ▼</div>	<div>ap-macaddress-s... ▼</div>
Called-station-id case	<div>lower ▼</div>	<div>lower ▼</div>
MAC-Delimiter	<div>hyphen ▼</div>	<div>hyphen ▼</div>
Username Case	<div>lower ▼</div>	
Username Delimiter	<div>hyphen ▼</div>	

Catalyst 9800 Advanced RADIUS Attributes

Configuration > Security > AAA

Radius Attributes

	Accounting	Authentication
Called-station-id	<div>macaddress ▼</div>	<div>ap-macaddress-s... ▼</div>
Called-station-id case	<div>lower ▼</div>	<div>lower ▼</div>
MAC-Delimiter	<div>hyphen ▼</div>	<div>hyphen ▼</div>
Username Case	<div>lower ▼</div>	
Username Delimiter	<div>hyphen ▼</div>	

- ap-location
- ap-macaddress
- ap-macaddress-ssid
- ap-macaddress-ssid-flexprofilename
- ap-macaddress-ssid-policytagname
- ap-macaddress-ssid-sitetagname
- ap-name
- ap-name-ssid
- flex-profile-name
- ipaddress
- macaddress
- policy-tag-name
- site-tag-name
- vlan-id

Catalyst 9800 Advanced RADIUS Attributes

Configuration > Security > Wireless AAA Policy

Configuration > Security > Wireless AAA Policy

+ Add

× Delete

Selected Rows : 0

☐	Policy Name
☐	default-aaa-policy
<div>⏪ ⏩ 1 ⏪ ⏩</div>	

Edit Wireless AAA Policy

Policy Name*

default-aaa-policy

NAS-ID Option 1

System Name ▼

NAS-ID Option 2

Not Configured ▼

NAS-ID Option 3

Not Configured ▼

↶ Cancel

💾

Update & Apply to Device

Catalyst 9800 Advanced RADIUS Attributes

Configuration > Security > Wireless AAA Policy

Configuration > Security > Wireless AAA Policy

+ Add

× Delete

Selected Rows : 0

☐	Policy Name
☐	default-aaa-policy
<div>⏪ ⏩ 1 ⏪ ⏩</div>	

Edit Wireless AAA Policy

Policy Name*

default-aaa-policy

NAS-ID Option 1

System Name ▼

NAS-ID Option 2

Not Configured ▼

NAS-ID Option 3

Not Configured ▼

↶ Cancel

💾 Update

AP ETH MAC Address

AP IP Address

AP Location

AP MAC Address

AP Name

AP Policy Tag

AP Site Tag

SSID

System IP Address

System MAC Address

System Name

Custom String

Meraki Advanced RADIUS Attributes

Wireless > Configure > Access Control

Advanced RADIUS settings

(NAS ID, Called-station-ID, RADIUS timeout, retry count, failover)

Called-station-ID

#

Category

1

AP MAC address

x

2

SSID name

x

Add identifier 4 max.

NAS ID

#

Category

1

AP MAC address

x

2

SSID number

x

Add identifier 4 max.

Attributes

AP MAC address

SSID name

SSID number

AP name

RF Profile

AP VLAN ID

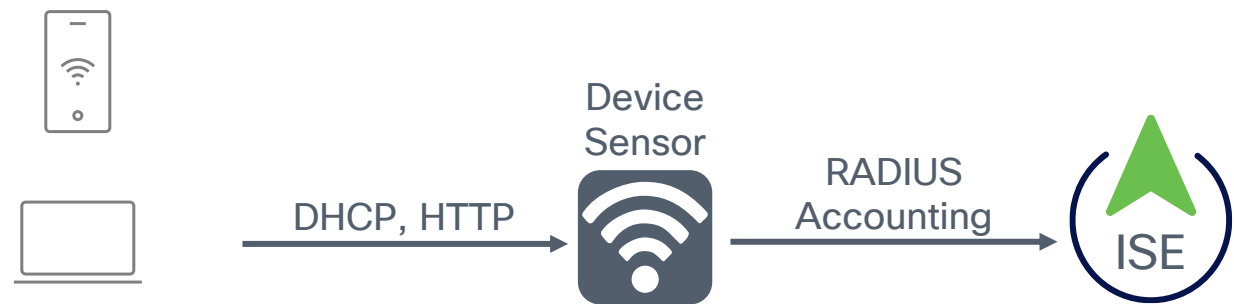
AP tags

AP LAN IP

AP Public IP

Custom

Device Sensor



Device Classification	
Device Name	cnlab-EPw301
Protocol Map	0x000029 (OUI, DHCP, HTTP)
Day Zero Classification	ASUSTEK COMPUTER INC.
Device Vendor	MSFT 5.0

```

RADIUS Protocol
Code: Accounting-Request (4)
Packet identifier: 0x3f (63)
Length: 656
Authenticator: f2c386e09460c1e6a43b19ce8f07aaff
[The response to this request is in frame 38]
Attribute Value Pairs
  AVP: t=Vendor-Specific(26) l=45 vnd=ciscoSystems(9)
    Type: 26
    Length: 45
    Vendor ID: ciscoSystems (9)
  VSA: t=Cisco-AVPair(1) l=39 val=dc-profile-name=Microsoft-Workstation
    Type: 1
    Length: 39
    Cisco-AVPair: dc-profile-name=Microsoft-Workstation
  AVP: t=Vendor-Specific(26) l=35 vnd=ciscoSystems(9)
    Type: 26
    Length: 35
    Vendor ID: ciscoSystems (9)
  VSA: t=Cisco-AVPair(1) l=29 val=dc-device-name=cnlab-EPw301
    Type: 1
    Length: 29
    Cisco-AVPair: dc-device-name=cnlab-EPw301
  AVP: t=Vendor-Specific(26) l=61 vnd=ciscoSystems(9)
    Type: 26
    Length: 61
    Vendor ID: ciscoSystems (9)
  VSA: t=Cisco-AVPair(1) l=55 val=dc-device-class-tag=Workstation:Microsoft-Workstation
    Type: 1
    Length: 55
    Cisco-AVPair: dc-device-class-tag=Workstation:Microsoft-Workstation

```

Intel, Apple, Samsung Analytics



	Device Type and Version	IOS-XE WLC	Meraki MR Firmware	ISE
Intel Connectivity Analytics	Intel 22.50.1 on AX200/201/210/211/411 or newer	17.6.1	MR29	3.3
Apple Analytics	iOS 11 on iPhone 7/iPad (5th Gen) or newer MacOS14 on Apple Silicon	16.12.1s	MR27	
Samsung Analytics	Android 9 on Galaxy S10 or newer	17.1.1	MR29	

*Accounting Reports coming MR31.2



Enabling Device Analytics - WLC

Configuration > Wireless > Wireless Global

Default Mobility Domain *

default

RF Group Name*

RF

Maximum Login Sessions Per User*

Management Via Wireless

☐

Device Classification

☒

Device Classification

Enabling Device Analytics - WLC

Configuration > Tags & Profiles > Policy

General

Access Policies

QOS and AVC

RADIUS Profiling



HTTP TLV Caching



DHCP TLV Caching



AAA Policy

Advanced

Allow AAA Override



NAC State



Policy Name

default-aaa-p...



Accounting List

AcctMethod



Interim Accounting

ENABLED



Enabling Device Analytics - WLC

Configuration > Tags & Profiles > WLANs

Device Analytics

Advertise Support



Advertise PC Analytics
Support ⓘ



Share Data with Client



11k Beacon Radio Measurement

Client Scan Report

On Association



On Roam



SAMSUNG

Enabling Device Analytics - WLC

Configuration > Tags & Profiles > WLANs

Device Analytics

Advertise Support ☒

Advertise PC Analytics Support ⓘ



Share Data with Client

intel®

Protected Management Frame

PMF

Optional

Association Comeback Timer*

Optional

Required

SA Query Time*

200

Enabling Device Analytics - WLC



Device Analytics Attributes – Authorization Policy

Policy > Policy Sets > Authorization Policy

Editor

Click to add an attribute

Equals ▾

Select attribute for condition

Dictionary	Attribute	ID	Info
Wifi_Device_Analytics ▾ ×	Attribute	ID	
Wifi_Device_Analytics	DEVICE_INFO_FIRMWARE_...		i
Wifi_Device_Analytics	DEVICE_INFO_HW_MODEL		i
Wifi_Device_Analytics	DEVICE_INFO_MANUFACT...		i
Wifi_Device_Analytics	DEVICE_INFO_MODEL_NA...		i
Wifi_Device_Analytics	DEVICE_INFO_MODEL_NUM		i
Wifi_Device_Analytics	DEVICE_INFO_OS_VERSION		i
Wifi_Device_Analytics	DEVICE_INFO_VENDOR_T...		i

Device Analytics Attributes – Profiler Policy

Policy > Profiling > Profiler Policy

☐ No, use existing Identity Group hierarchy

NONE

Global Settings

CoA Type

Conditions

Then

Certain

Condition Name	Expression

Select Attribute

Wifi_Device_Analytics

× wifi

<  

DEVICE_INFO_FIRMWARE_VERSION

DEVICE_INFO_HW_MODEL

DEVICE_INFO_MANUFACTURER_NAME

DEVICE_INFO_MODEL_NAME

DEVICE_INFO_MODEL_NUM

DEVICE_INFO_OS_VERSION

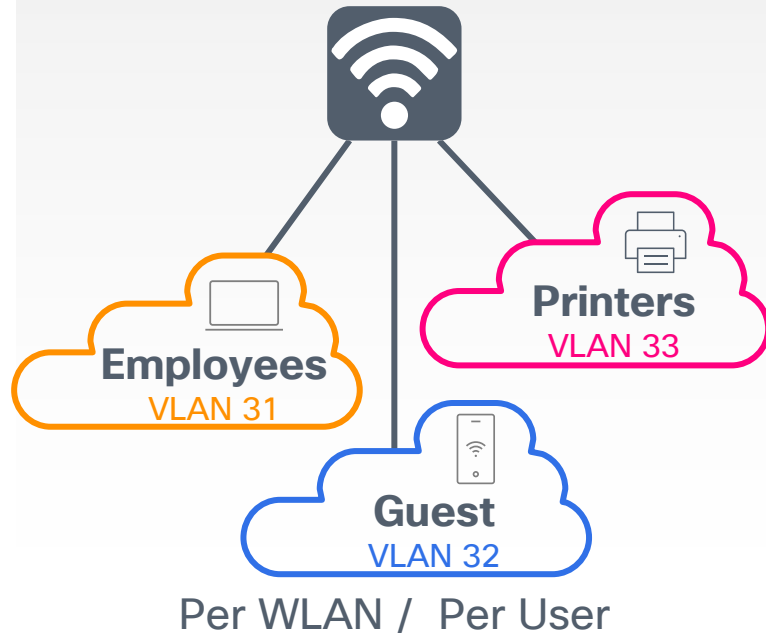
Authorization Results

ISE Segmentation Options

Beyond RADIUS Access-Accept / Access-Reject

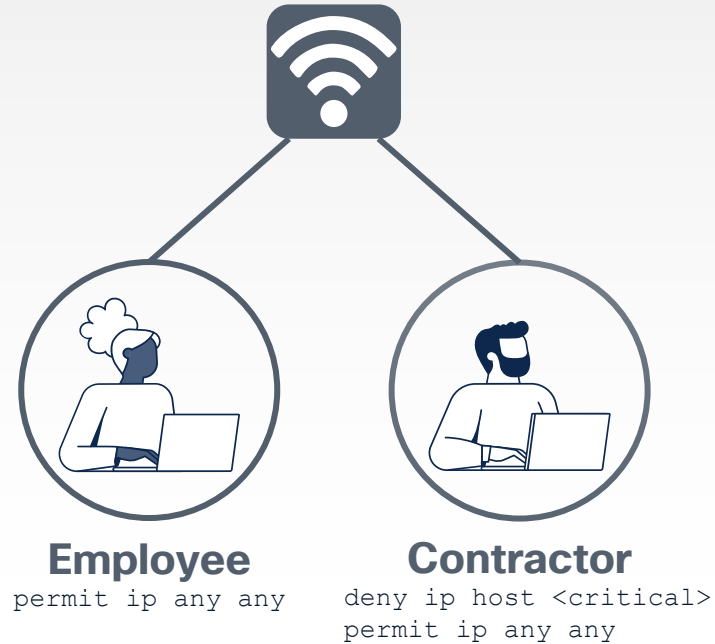
VLANs

Dynamic VLAN Assignments



ACLs

Downloadable ACLs
Named ACLs / Group Policy

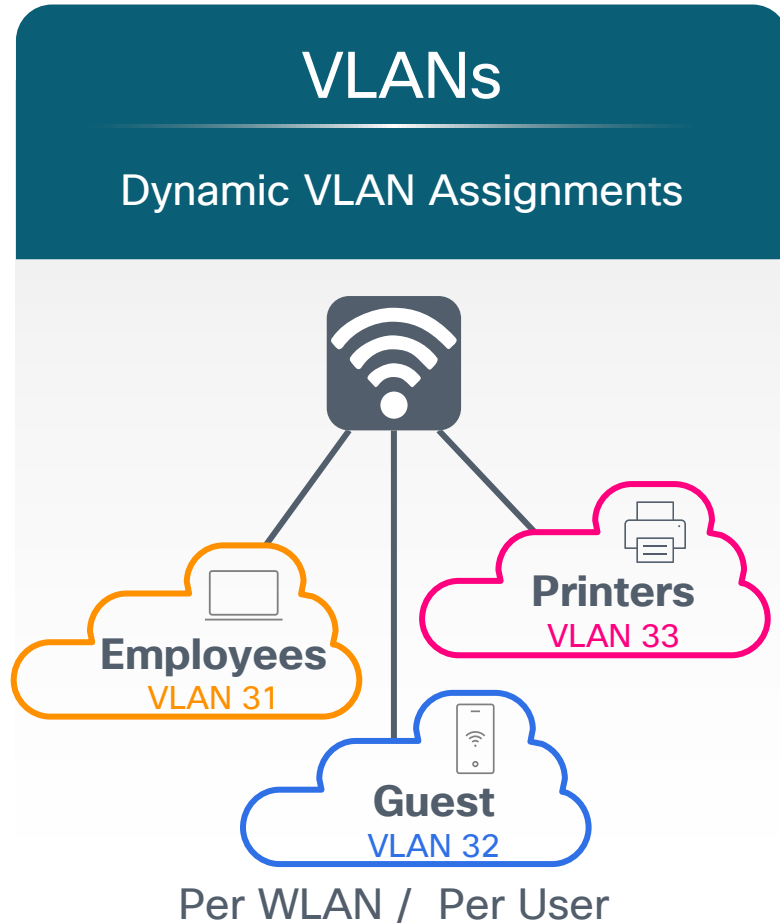


Security Group Tags

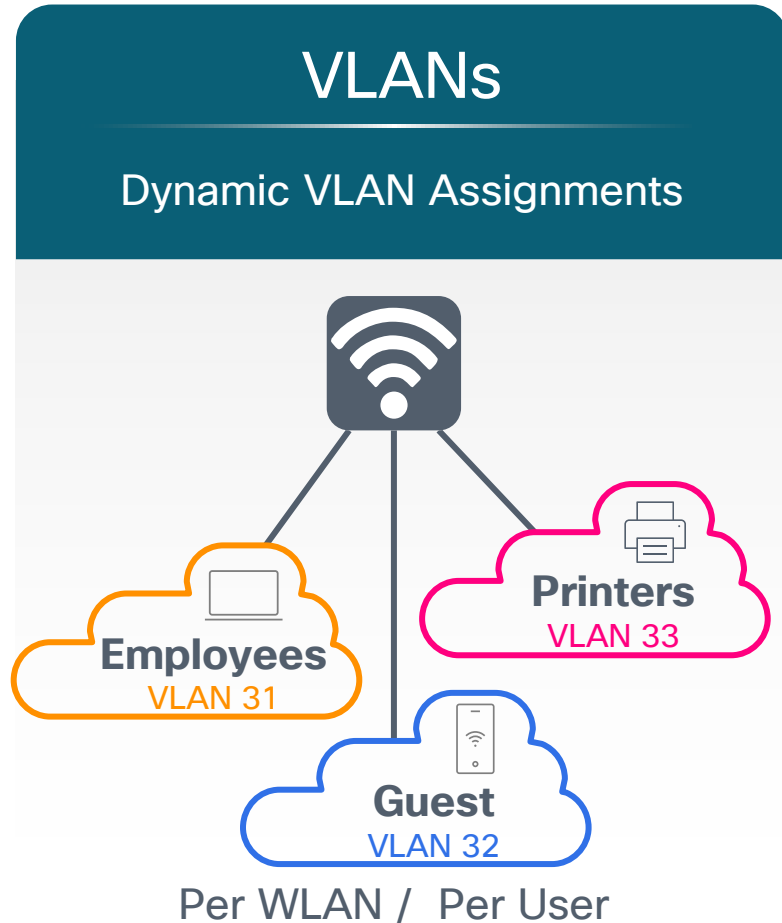
TrustSec
Adaptive Policy



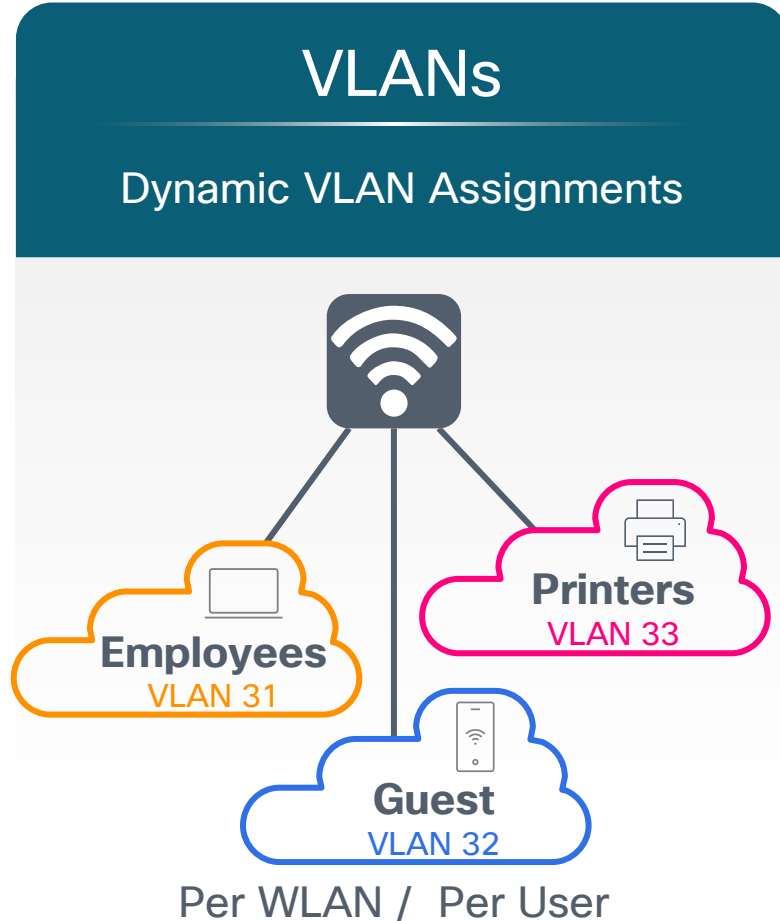
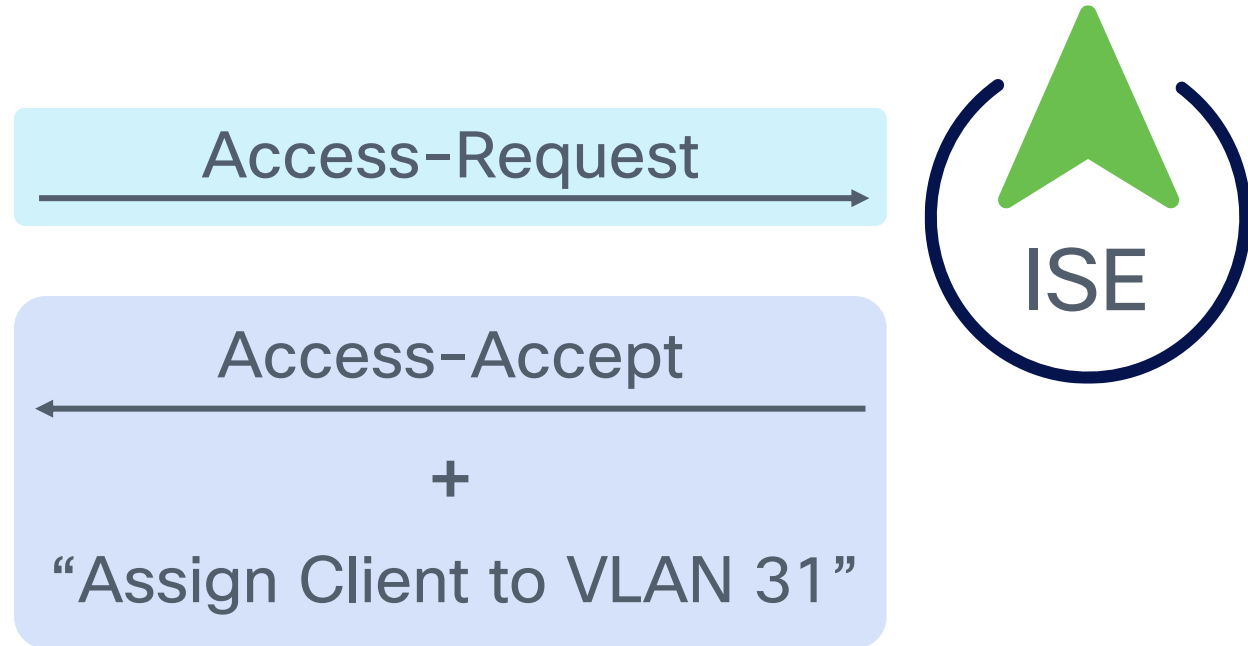
Dynamic VLAN Assignment



Dynamic VLAN Assignment



Dynamic VLAN Assignment



Dynamic VLAN – ISE

Policy > Policy Elements > Results > Authorization

Authorization Profiles > Employee_dACL

Authorization Profile

* Name Employee_VLAN

Description

* Access Type ACCESS_ACCEPT ▼

Network Device Profile  Cisco ▼ 

Service Template ☐

Track Movement ☐ ⓘ

Agentless Posture ☐ ⓘ

Passive Identity Tracking ☐ ⓘ

▼ Common Tasks

☒ VLAN Tag ID 1 [Edit Tag](#) ID/Name 31 ▼

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:31
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Dynamic VLAN – ISE

Policy > Policy Elements > Results > Authorization

Authorization Profiles > Employee_dACL

Authorization Profile

* Name Employee_VLAN

Description

* Access Type ACCESS_ACCEPT ▼

Passive Identity Tracking ☐ ⓘ

▼ Common Tasks

☒ VLAN Tag ID 1 31 ▼

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:31
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Dynamic VLAN – ISE

Policy > Policy Elements > Results > Authorization

Tunnel-Private-Group-ID = 1:31

Authorization Profiles > Employee_dACL

Authorization Profile

* Name Employee_VLAN

Description

* Access Type ACCESS_ACCEPT ▼

Passive Identity Tracking ☐ ⓘ

Common Tasks

☒ VLAN Tag ID 1 ID/Name 31 ▼

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:31
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Dynamic VLAN – ISE

Policy > Policy Elements > Results > Authorization

Authorization Profiles > Employee_dACL

Authorization Profile

* Name Employee_VLAN

Description

* Access Type ACCESS_ACCEPT ▼

Passive Identity Tracking ☐ ⓘ

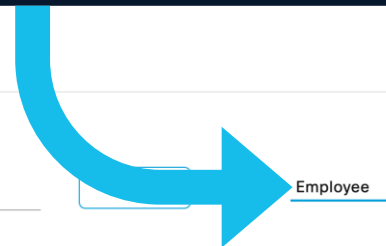
▼ Common Tasks

☒ VLAN Tag ID 1 Employee

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:Employee
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

ID/Name Employee ▼



Dynamic VLAN – ISE

Policy > Policy Elements > Results > Authorization

Tunnel-Private-Group-ID = 1:Employee

Authorization Profiles > Employee_dACL

Authorization Profile

* Name Employee_VLAN

Description

* Access Type ACCESS_ACCEPT ▼

Passive Identity Tracking ☐ ⓘ

Common Tasks

☒ VLAN Tag ID 1 [Edit Tag](#) ID/Name Employee

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:Employee
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Dynamic VLAN – Catalyst 9800

Configuration > Layer2 > VLAN

Configuration > Layer2 > VLAN

SVI **VLAN** VLAN Group

+ Add × Delete

☐	VLAN ID	Name	Status	Ports
☐	1	default	active	
☐	22	WM	active	
☐	31	Employee	active	
☐	32	Guest	active	
☐	33	IoT	active	
<div><div>1</div><div>10</div><div>1 - 5 of 5 items</div></div>				

Dynamic VLAN – Catalyst 9800

Configuration > Layer2 > VLAN

Configuration > Layer2 > VLAN

SVI VLAN VLAN

+ Add

× Delete

31

Employee

☐	VLAN ID	Name	Status	Ports
☐	1	default	active	
☐	22	WM	active	
☐	31	Employee	active	
☐	32	Guest	active	
☐	33	IoT	active	

1 - 5 of 5 items

Dynamic VLAN – Catalyst 9800

Configuration > Layer2 > VLAN

Configuration > Layer2 > VLAN

SVI VLAN VLAN

+ Add × Delete

☐	VLAN ID	Name	Status	Ports
☐	1	default	active	
☐	22	WM	active	
☐	31	Employee	active	
☐	32	Guest	active	
☐	33	IoT	active	

1 10 1 - 5 of 5 items

☐ 31 Employee

 VLANs must exist

Dynamic VLAN – Catalyst 9800

Configuration > Layer2 > VLAN

SVI

VLAN

VLAN Group

+ Add

× Delete



VLAN GROUP NAME



VLAN LIST



Employee_vGroup

40-50



10 ▼

1 - 1 of 1 items

Dynamic VLAN – Catalyst 9800

Configuration > Layer2 > VLAN

The screenshot shows the 'VLAN Group' configuration page in the Cisco ISE GUI. At the top, there are tabs for 'SVI', 'VLAN', and 'VLAN Group'. Below the tabs, there is a blue button with a '+' sign and the text 'Add'. The main table has two columns: 'VLAN GROUP NAME' and 'VLAN LIST'. The 'VLAN GROUP NAME' column contains a list of VLAN groups, with 'Employee_vGroup' highlighted by a blue box. A blue arrow points from the 'VLAN LIST' column to the 'Employee_vGroup' entry. The 'VLAN LIST' column contains the value '40-50'. At the bottom, there is a pagination bar showing '1' of 1 items, a '10' dropdown menu, and the text '1 - 1 of 1 items'.

Dynamic VLAN – Catalyst 9800

Configuration > Layer2 > VLAN

SVI

VLAN

VLAN Group

+ Add

×

40-50



VLAN GROUP NAME



VLAN LIST



Employee_vGroup

40-50



1



10



1 - 1 of 1 items

Dynamic VLAN – Catalyst 9800

Configuration > Tags & Profiles > Flex

Add Flex Profile

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

+ Add

× Delete

☐	VLAN Name ▼	ID ▼	Ingress ACL ▼	Egress ACL ▼
☐	Employee	31		
☐	Guest	32		
☐	IoT	33		

⏮

⏪

1

⏩

⏭



If using Flexconnect
VLANs need to be
added to Flex Profile

Dynamic VLAN – Meraki

Wireless > Configure > Access Control

Client IP and VLAN Bridge mode

☐ Meraki AP assigned (NAT mode)
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.

☒ External DHCP server assigned
Meraki devices operate transparently (do not perform NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, and wireless cameras.

Bridged

Tunneled

☐ Layer 3 roaming

RADIUS override ⓘ

Override VLAN tag

Ignore VLAN attribute

RADIUS guest VLAN ⓘ

Disabled

Bonjour forwarding
Bridge mode only

Enabled

Disabled

VLAN tagging ⓘ

VLAN ID

#	Access point tags	VLAN ID
	Default	22

+ Add VLAN ID

Assign group policies by device type

Enabled

Disabled

Dynamic VLAN – Meraki

Wireless > Configure > Access Control

Client IP and VLAN Bridge mode

RADIUS override ⓘ

Override VLAN tag

Ignore VLAN attribute

LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, and wireless cameras.

Bridged

Tunneled

☐ Layer 3 roaming

RADIUS override ⓘ

Override VLAN tag

Ignore VLAN attribute

RADIUS guest VLAN ⓘ

Disabled

Bonjour forwarding
Bridge mode only

Enabled

Disabled

VLAN tagging ⓘ

VLAN ID

#	Access point tags	VLAN ID
---	-------------------	---------

Default		22
---------	--	----

+ Add VLAN ID

Assign group policies by device type

Enabled

Disabled

Dynamic VLAN – Meraki VLAN Profiles

Network-Wide > VLAN Profiles

VLAN profiles

VLAN profiles Profile assignment Settings

Edit profile

Profile name

Default Profile

Iname

Default

Active VLANs

all

VLAN name

+ Add Named VLAN

#	VLAN name	VLAN ID	Actions
1	default	1	
2	Employee	31	
3	Guest	32	
4	IoT	33	

Group name

+ Add VLAN Group

#	Group Name	VLAN list	Actions
1	Employee_vGroup	40-50	

Save profile changes

Cancel

Dynamic VLAN – Meraki VLAN Profiles

Network-Wide > VLAN Profiles

#	VLAN name	VLAN ID	Actions
1	default	<input type="text" value="1"/>	
2	<input type="text" value="Employee"/>	<input type="text" value="31"/>	
3	<input type="text" value="Guest"/>	<input type="text" value="32"/>	

VLAN name

+ Add Named VLAN

#	VLAN name	VLAN ID	Actions
1	default	<input type="text" value="1"/>	
2	<input type="text" value="Employee"/>	<input type="text" value="31"/>	
3	<input type="text" value="Guest"/>	<input type="text" value="32"/>	
4	<input type="text" value="IoT"/>	<input type="text" value="33"/>	

Save profile changes

Cancel

Group name

+ Add VLAN Group

#	Group Name	VLAN list	Actions
1	Employee_vGroup	<input type="text" value="40-50"/>	

Dynamic VLAN – Meraki VLAN Profiles

Network-Wide > VLAN Profiles

VLAN profiles

VLAN profilesProfile assignmentSettings

6 Devices

Assign profile

☐	Device name	Type	Assigned profile
☐	CNLAB-PX-AP5	wireless	Default Profile
☐	CNLAB-PX-AP6	wireless	Default Profile
☐	CNLAB-PX-AP2	wireless	Default Profile
☐	CNLAB-PX-AP1	wireless	Default Profile
☐	CNLAB-PX-AP3	wireless	Default Profile
☐	CNLAB-PX-AP4	wireless	Default Profile

<

1

>

Dynamic VLAN – Meraki VLAN Profiles

Network-Wide > VLAN Profiles

VLAN profiles

VLAN profiles Profile assignment Settings

Named VLAN ☒ Enable Named VLANs for use with RADIUS ⓘ

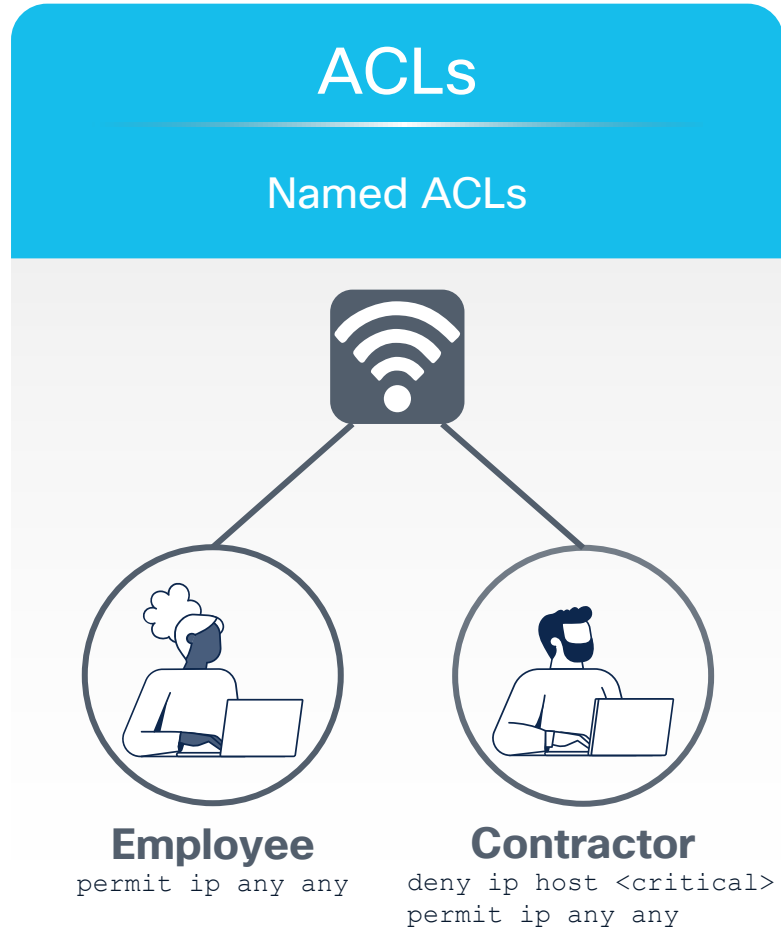
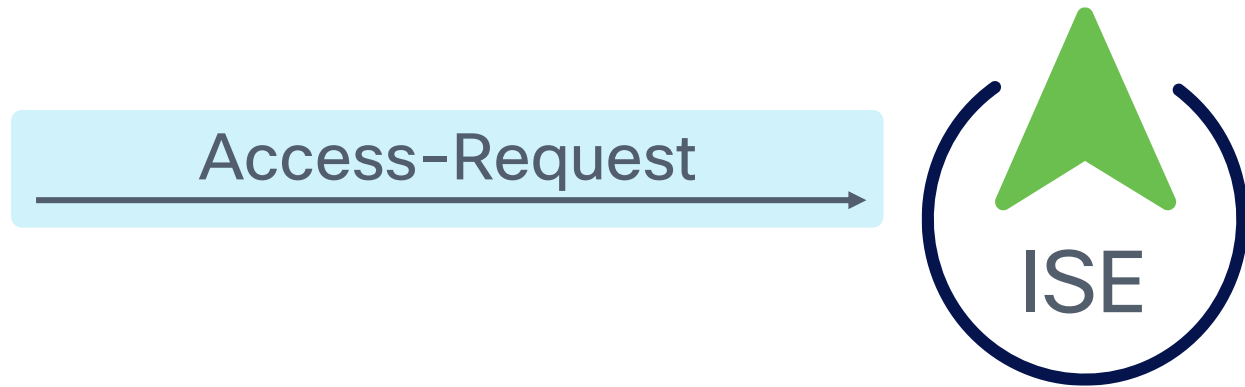


Must enable Named VLANs for use with RADIUS

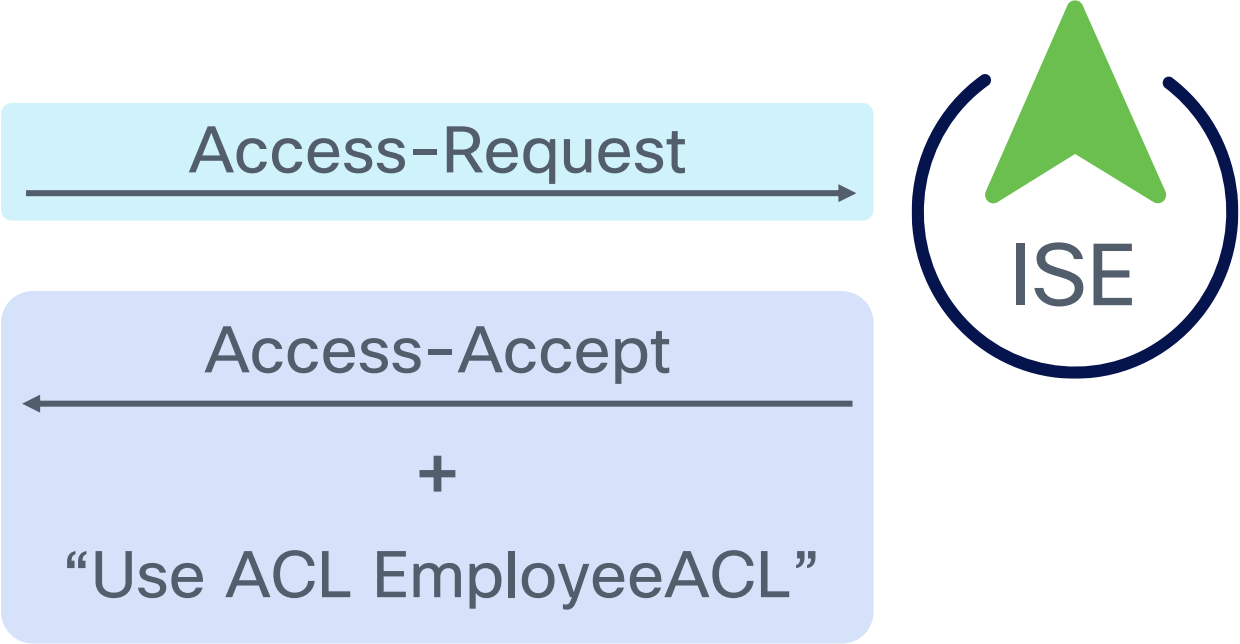
Named ACLs – ISE Configuration



Named ACLs – ISE Configuration



Named ACLs – ISE Configuration



Named ACLs – ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

* Name

Employee_ACL

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

Cisco

Service Template

☐

Track Movement

☐

Agentless Posture

☐

Passive Identity Tracking

☐

Common Tasks

☐ ACL (Filter-ID)

☐ Airespace ACL Name

Advanced Attributes Settings

Cisco:cisco-av-pair

=

bsn-acl-name=EmployeeACL

+

Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = bsn-acl-name=EmployeeACL

Named ACLs – ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

* Name Employee_ACL

Description

* Access

Network

Service

Track M

Agentle

Passive

Common Tasks

☐ ACL (Filter-ID)

☐ Airespace ACL Name

Advanced Attributes Settings

Cisco:cisco-av-pair = bsn-acl-name=EmployeeACL

Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = bsn-acl-name=EmployeeACL

Advanced Attributes Settings

Cisco:cisco-av-pair = bsn-acl-name=EmployeeACL

Catalyst 9800

Named ACLs – ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

Common Tasks

☐ ACL (Filter-ID)

☐ Airespace ACL Name

Advanced Settings

=

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = bsn-acl-name=EmployeeACL

Catalyst 9800

Common Tasks

☐ ACL (Filter-ID)

☐ Airespace ACL Name

Can be used for backwards compatibility with AireOS

Named ACLs – ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

Common Tasks

☐ ACL (Filter-ID)

☐ Airespace ACL Name

Advanced Settings

=

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = bsn-acl-name=EmployeeACL

Common Tasks

☐ ACL (Filter-ID)

☐ Airespace ACL Name

Meraki

Named ACLs – Catalyst 9800

Configuration > Security > ACL

Configuration > Security > ACL

+ Add

× Delete

✎ Associate Interfaces

ACL

0

Add ACL Setup

×

ACL Name*

EmployeeACL

ACL Type

IPv4 Extended

Rules

Sequence*

Action

permit

Source Type

any

Destination Type

any

Protocol

ahp

Log

☐

DSCP

None

+ Add

× Delete

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port
☐	10	permit	any		172.23.0.0	0.0.255.255	ip	None	None
☐	20	deny	any		172.16.0.0	0.15.255.255	ip	None	None
☐	30	permit	any		any		ip	None	None

1

10

1 - 3 of 3 items

↺ Cancel

📄 Apply to Device

Named ACLs – Catalyst 9800

Configuration > Security > ACL

Configuration > Security > ACL

+ Add

× Delete

✎ Associate Interfaces

ACL

0

Add ACL Setup

×

ACL Name*

EmployeeACL

Rules

Sequence*

Action

permit

ACL Name*

EmployeeACL

+ Add

× Delete

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port
☐	10	permit	any		172.23.0.0	0.0.255.255	ip	None	None
☐	20	deny	any		172.16.0.0	0.15.255.255	ip	None	None
☐	30	permit	any		any		ip	None	None

1

10

1 - 3 of 3 items

↺ Cancel

📄 Apply to Device

Named ACLs – Catalyst 9800

Configuration > Security > ACL

Configuration > Security > ACL

	Sequence ↑	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port
☐	10	permit	any		172.23.0.0	0.0.255.255	ip	None	None
☐	20	deny	any		172.16.0.0	0.15.255.255	ip	None	None
☐	30	permit	any		any		ip	None	None

Destination Type
any

Protocol
ahp

Log☐

DSCP
None

+ Add

× Delete

	Sequence ↑	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port
☐	10	permit	any		172.23.0.0	0.0.255.255	ip	None	None
☐	20	deny	any		172.16.0.0	0.15.255.255	ip	None	None
☐	30	permit	any		any		ip	None	None

1

10

1 - 3 of 3 items

Cancel

Apply to Device

Named ACLs – Catalyst 9800

Configuration > Tags & Profiles > Flex

Add Flex Profile

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

+ Add

× Delete

☐	ACL Name	Central Web Auth	URL Filter
☐	EmployeeACL	Disabled	
◀ 1 ▶▶			



If using Flexconnect
ACLs need to be
added to Flex Profile

Catalyst 9800 dACL



Authentication

Authorization

Access-Accept
dACL name
Method-List

Access-Request
dACL name

Access-Accept
dACL

```

RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0xb7 (183)
Length: 144
Authenticator: dc0633f0d1b4d01b7b5b95875ed585a8
[The response to this request is in frame 85]
Attribute Value Pairs
  > AVP: t=NAS-IP-Address(4) l=6 val=172.23.57.71
  > AVP: t=User-Name(1) l=38 val=#ACSACL#-IP-USERS_dACL_IPV4-68003539
  > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    Type: 26
    Length: 32
    Vendor ID: ciscoSystems (9)
    > VSA: t=Cisco-AVPair(1) l=26 val=aaa:service=ip_admission
      Type: 1
      Length: 26
      Cisco-AVPair: aaa:service=ip_admission
    > AVP: t=Vendor-Specific(26) l=30 vnd=ciscoSystems(9)
      Type: 26
      Length: 30
      Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=24 val=aaa:event=acl-download
        Type: 1
        Length: 24
        Cisco-AVPair: aaa:event=acl-download
      > AVP: t=Message-Authenticator(80) l=18 val=19b13cb7bc8df22354a5348644c6b32d

```

```

RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0xb7 (183)
Length: 309
Authenticator: 7b92c3806e04228f3f50105925640ea6
[This is a response to a request in frame 84]
[Time from request: 0.001437000 seconds]
Attribute Value Pairs
  > AVP: t=User-Name(1) l=38 val=#ACSACL#-IP-USERS_dACL_IPV4-68003539
  > AVP: t=Class(25) l=88 val=434143533a61633137333930625448335345504144526f563650756d
  > AVP: t=Message-Authenticator(80) l=18 val=5840a54710943c11dd1f8f8a9fd3e687
  > AVP: t=Vendor-Specific(26) l=55 vnd=ciscoSystems(9)
    Type: 26
    Length: 55
    Vendor ID: ciscoSystems (9)
    > VSA: t=Cisco-AVPair(1) l=49 val=ip:inac1#1=permit ip any 172.23.0.0 0.0.255.255
      Type: 1
      Length: 49
      Cisco-AVPair: ip:inac1#1=permit ip any 172.23.0.0 0.0.255.255
    > AVP: t=Vendor-Specific(26) l=54 vnd=ciscoSystems(9)
      Type: 26
      Length: 54
      Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=48 val=ip:inac1#2=deny ip any 172.16.0.0 0.15.255.255
        Type: 1
        Length: 48
        Cisco-AVPair: ip:inac1#2=deny ip any 172.16.0.0 0.15.255.255
      > AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
        Type: 26
        Length: 36
        Vendor ID: ciscoSystems (9)
        > VSA: t=Cisco-AVPair(1) l=30 val=ip:inac1#3=permit ip any any
          Type: 1
          Length: 30
          Cisco-AVPair: ip:inac1#3=permit ip any any

```

Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization

[Downloadable ACL List](#) > USERS_dACL_IPV4

Downloadable ACL

* Name

USERS_dACL_IPV4

Description

Deny all ipv4 traffic

IP version

☒ IPv4 ☐ IPv6 ☐ Agnostic [i](#)

* DACL Content

1

2

3

4

5

6

7

8

9

10

11

permit ip any 172.23.0.0 0.0.255.255

deny ip any 172.16.0.0 0.15.255.255

permit ip any any

Check DACL Syntax

Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization

[Downloadable ACL List](#) > USERS_dACL_IPV4

Downloadable ACL

* Name

Description

IP version ☒ IPv4 ☐ IPv6 ☐ Agnostic ⓘ

* Name

✓ Check DACL Syntax

Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization

```
permit ip any 172.23.0.0 0.0.0.255  
deny ip any 17.16.0.0 0.15.255.255  
permit ip any any
```

IP version ☒ IPv4 ☐ IPv6 ☐ Agnostic ⓘ

* DACL
Content

1	permit ip any 172.23.0.0 0.0.255.255
2	deny ip any 172.16.0.0 0.15.255.255
3	permit ip any any
4	
5	
6	
7	
8	
9	
10	

✓ Check DACL Syntax

Catalyst 9800 dACL - ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

* Name Employee_dACL

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

Common Tasks

☒ DACL Name USERS_dACL_IPV4

Advanced Attributes Settings

Cisco:cisco-av-pair = Method-List=ISEauthZnet...

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = USERS_dACL_IPV4
cisco-av-pair = Method-List=ISEauthZnetwork

Catalyst 9800 dACL - ISE Configuration

Policy > Policy Elements > Results > Authorization

☒ DACL Name ⓘ

USERS_dACL_IPV4



DACL Name MUST Match

Authorization Profile

Network Device Profile Cisco ⓘ

Service Template ☐

Track Movement ☐ ⓘ

Agentless Posture ☐ ⓘ

Passive Identity Tracking ☐ ⓘ

Common Tasks

☒ DACL Name ⓘ

USERS_dACL_IPV4

Advanced Attributes Settings

Cisco:cisco-av-pair

Method-List=ISEauthZnet...

Attributes Details

Access Type = ACCESS_ACCEPT

DACL = USERS_dACL_IPV4

cisco-av-pair = Method-List=ISEauthZnetwork

Catalyst 9800 dACL - ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

Advanced Attributes Settings

Cisco:cisco-av-pair = Method-List=ISEauthZnet...

Common Tasks

☒ DACL Name ⓘ USERS_dACL_IPV4

Advanced Attributes Settings

Cisco:cisco-av-pair = Method-List=ISEauthZnet...

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = USERS_dACL_IPV4
cisco-av-pair = Method-List=ISEauthZnetwork



Catalyst 9800 dACL - ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

Access Type = ACCESS_ACCEPT

DACL = USERS_dACL_IPV4

Cisco-av-pair = Method-List=ISEauthZnetwork



Include AAA AuthZ
method list if not using
default method on WLC

Common Tasks

☒ DACL Name ⓘ USERS_dACL_IPV4

Advanced Attributes Settings

⋮ Cisco:cisco-av-pair = Method-List=ISEauthZnetwork

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = USERS_dACL_IPV4
cisco-av-pair = Method-List=ISEauthZnetwork

Catalyst 9800 dACL – Scale and Caveats

Controllers	Scale
Small/Medium	128 ACLs with 128 ACEs each
Large	256 ACLs with 256 ACEs each

Notes:

- **Flexconnect local switching is not supported**
- **Attributes sent are:**
 - cisco-av-pair = ACS:CiscoSecure-Defined-ACL
 - cisco-av-pair = Method-List

Catalyst 9800 dACL – Monitoring from ISE

Operations > RADIUS > Live Logs

Apr 17, 2025 09:17:20.9...



steve

CC:28:AA:6C:CD:B9

Result

User-Name	steve
Class	CACS:473917AC0000058F46ABEB70:CNLAB-PX-ISE1/532650495/93798
EAP-Key-Name	19:e3:8f:eb:97:a5:ae:94:0b:d6:f6:53:02:23:7e:39:79:82:90:e2:17:4f:96:b6:f6:0d:ed:d5:ff:eb:1e:7b:e2:ac:d2:0a:ed:1f:d0:96:09:67:a6:b2:2b:f6:15:d0:06:ff:3d:99:cf:2c:cb:da:36:2f:ff:b8:e8:8f:b4:db:2b
cisco-av-pair	Method-List=ISEauthZnetwork
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-USERS_dACL_IPV4-6801b533
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Essential license consumed.

Catalyst 9800 dACL – Monitoring from ISE

Operations > RADIUS > Live Logs

cisco-av-pair

Method-List=ISEauthZnetwork

AAA Method List

cisco-av-pair

ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-
USERS_dACL_IPV4-6801b533

ACL to Download

EAP-Key-Name

19:e3:8f:eb:97:a5:ae:94:0b:d6:16:53:02:23:7e:39:79:82:90:e2:
17:4f:96:b6:f6:0d:ed:d5:ff:eb:1e:7b:e2:ac:d2:0a:ed:1f:d0:96:0
9:67:a6:b2:2b:f6:15:d0:06:ff:3d:99:cf:2c:cb:da:36:2f:ff:b8:e8:8
f:b4:db:2b

cisco-av-pair

Method-List=ISEauthZnetwork

cisco-av-pair

ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-
USERS_dACL_IPV4-6801b533

MS-MPPE-Send-Key

MS-MPPE-Recv-Key

LicenseTypes

Essential license consumed.

Catalyst 9800 dACL – Monitoring from ISE

Operations > RADIUS > Live Logs

Apr 17, 2025 09:17:20.9...



#ACSACL#-IP-USERS_dACL_IPV4-6801b533

Result

Class	CACS:ac17390bziML77ZJGvJWjAuCNFTDinCnbPJnlsEAcG9ov R5_ywg:CNLAB-PX-ISE1/532650495/93819
cisco-av-pair	ip:inacl#1=permit ip any 172.23.0.0 0.0.255.255
cisco-av-pair	ip:inacl#2=permit ip 172.23.0.0 0.0.255.255 any
cisco-av-pair	ip:inacl#3=deny ip any 172.16.0.0 0.15.255.255
cisco-av-pair	ip:inacl#4=permit ip any any

Catalyst 9800 dACL – Monitoring from 9800 Controller

Configuration > Security > ACL

Configuration > Security > ACL

+ Add

× Delete

 Associate Interfaces

	ACL Name	ACL Type	ACE Count	Downloaded ACL ⓘ
☐	xACSACLx-IP-USERS_dACL_IPV4-6801b893	IPv4 Extended	3	Yes

⏪

⏩

1

⏪

⏩

10 ▼

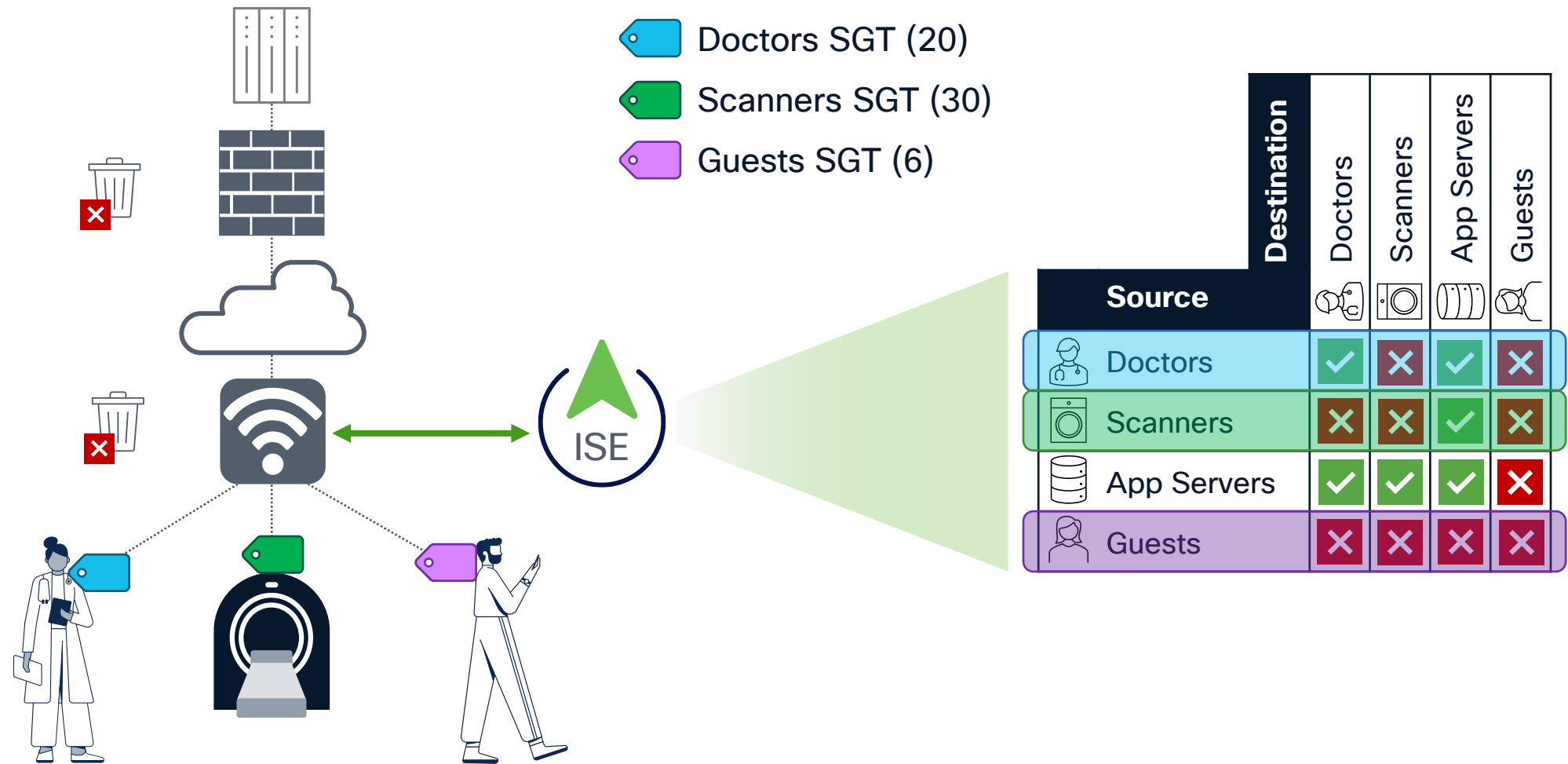
1 - 1 of 1 items

What's the Business Intent Here?

```
access-list 102 permit udp 126.183.90.85 0.0.0.255 eq 3256 114.53.254.245 255.255.255.255 lt 1780
access-list 102 deny icmp 203.36.110.37 255.255.255.255 lt 999 229.216.9.232 0.0.0.127 gt 3611
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
```

Group Based Policy with Security Group Tags (SGT)

TrustSec / Adaptive Policy



What's the Business Intent Here?

```
CNLAB-PX-SW3#show cts role-based permissions
```

```
IPv4 Role-based permissions default:
```

```
    Permit IP-00
```

```
IPv4 Role-based permissions from group 30:Scanners to group 40:App_Servers:
```

```
    Permit IP-00
```

```
IPv4 Role-based permissions from group 6:Guests to group 40:App_Servers:
```

```
    Deny IP-00
```

```
IPv4 Role-based permissions from group 20:Doctors to group 40:App_Servers:
```

```
    AllowWeb-00
```

```
CNLAB-PX-SW3#show cts role-based permissions from 20 to 40 details
```

```
IPv4 Role-based permissions from group 20:Doctors to group 40:App_Servers:
```

```
    AllowWeb-00
```

```
Details:
```

```
Role-based IP access list AllowWeb-00 (downloaded)
```

```
10 permit tcp dst eq www
```

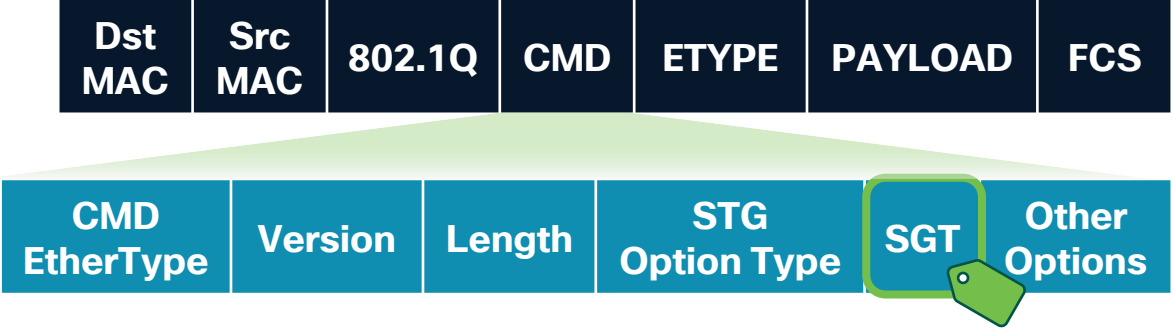
```
20 permit tcp dst eq 443
```

```
30 permit udp dst eq 443
```

```
40 deny ip
```

Security Group Tags (SGT)

INLINE



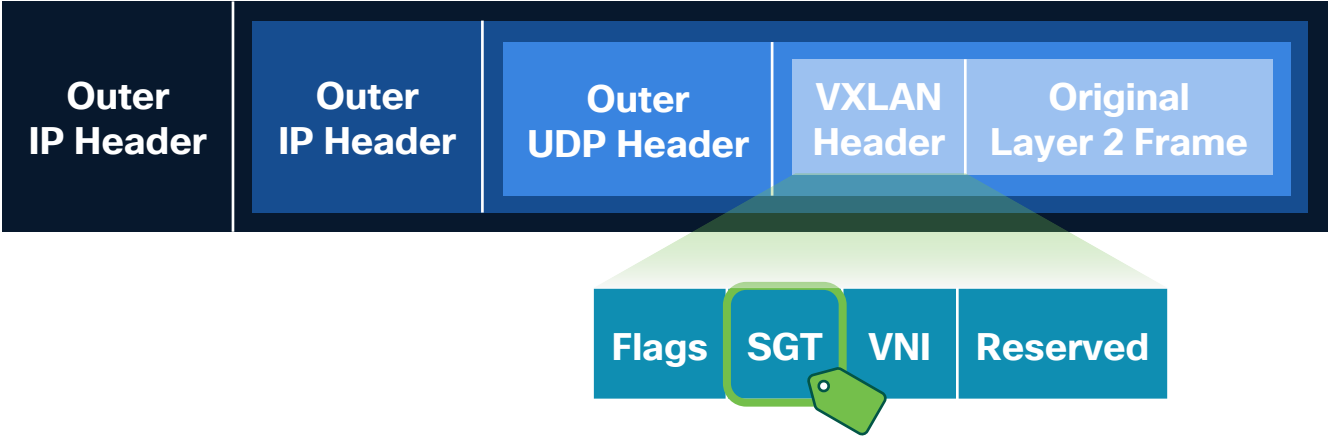
Catalyst

- Local
- Flexconnect

Meraki



TUNNELED
VXLAN FABRIC



Catalyst

- Fabric Enabled Wireless

ISE - TrustSec

Work Centers > TrustSec > Overview

The screenshot displays the ISE TrustSec Overview page. The top navigation bar includes tabs for Overview, Components, TrustSec Policy, Policy Sets, SXP, Integrations, Troubleshoot, Reports, and Settings. The left sidebar shows 'Introduction' and 'Dashboard' under the 'Overview' tab. The main content area is titled 'TrustSec Overview' and is divided into three columns representing a three-step process:

- 1. Prepare**
 - Plan Security Groups**
Identify resources that require different levels of protection
 - Classify the users or clients that will access those resources
 - Objective is to identify the minimum required number of Security Groups, as this will simplify management of the matrix
 - Preliminary Setup**
Set up the **TrustSec AAA server**.
 - Set up TrustSec **network devices**
 - Check default TrustSec **settings** to make sure they are acceptable.
 - If relevant, set up **TrustSec-ACI** policy group exchange to enable consistent policy across your network.
 - Consider activating the **workflow process** to prepare staging policy with an approval process.
- 2. Define**
 - Create Components**
Create **security groups** for resources, user groups and Network Devices as defined in the preparation phase. Also, examine if default SGTs can be used to match the roles defined.
 - Define the **network device authorization policy** by assigning SGTs to network devices.
 - Policy**
Define **SGACLs** to specify egress policy.
 - Assign SGACLs to cells within the **matrix** to enforce security.
 - Exchange Policy**
Configure **SXP** to allow distribution of IP to SGT mappings directly to TrustSec enforcement devices.
- 3. Go Live & Monitor**
 - Push Policy**
Push the **matrix** policy live.
 - Push the **SGTs, SGACLs** and the **matrix** to the network devices ⓘ
 - Real-time Monitoring**
Check **dashboards** to monitor current access.
 - Auditing**
Examine **reports** to check access and authorization is as intended.

ISE - TrustSec Policy

Work Centers > TrustSec > TrustSec Policy

TrustSec Policy

Policy Sets

SXP

Integrations

Troubleshoot

More

Production Matrix

Populated cells:13

+ Create Policy

👁 Monitor All Disabled

▶ Deploy

🛡 Verify Deploy

Default Policy:

Destination (5)

Doctors
20/0014
Scanners
30/001E
App_Servers
40/0028
Guests
6/0006
TrustSec_Devi...
2/0002

Source (5)

Doctors		✓	✓	✓	
20/0014					
Scanners	✓	✓		✓	
30/001E					
App_Servers	✓			✓	
40/0028					
Guests	✓	✓	✓	✓	
6/0006					
TrustSec_Devi...					
2/0002					

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

BRKEWN-2047

ISE - Assign SGTs

Policy > Policy Elements > Results > Authorization Profile

Authorization Profile

* Name

Scanners

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

 Cisco

Service Template

☐

Track Movement

☐ ⓘ

Agentless Posture

☐ ⓘ

Passive Identity Tracking

☐ ⓘ

Common Tasks

☒ Security Group ⓘ

Scanners

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = cts:security-group-tag=0014-4
cisco-av-pair = cts:sgt-name=Scanners

ISE - Assign SGTs via Authorization Profile

Policy > Policy Elements > Results > Authorization Profile

The screenshot shows the 'Authorization Profile' configuration page for the 'Scanners' profile. A blue callout box highlights the 'Security Group' selection. A large blue arrow points from the 'Security Group' dropdown in the callout box to the 'Security Group' dropdown in the 'Common Tasks' section.

Authorization Profile

* Name: Scanners

Description:

☒ Security Group ⓘ Scanners ▼

Track Movement ☐ ⓘ

Agentless Posture ☐ ⓘ

Passive Identity Tracking ☐ ⓘ

▼ Common Tasks

☒ Security Group ⓘ Scanners ▼

▼ Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = cts:security-group-tag=0014-4

cisco-av-pair = cts:sgt-name=Scanners

ISE - Assign SGTs via Authorization Policy

Policy > Policy Sets > Authorization Policy

Security Groups

Scanners

Authorization Policy				Result
	Status	Rule Name	Conditions	Profiles
	+			
	✓	Scanners	AND <div><div>Radius-Called-Station-ID ENDS_WITH PX-PSK</div><div>IdentityGroup-Name EQUALS Endpoint Identity Groups:Scanners</div></div>	PermitAccess
				Security Groups
				Scanners

Integration of ISE with Meraki



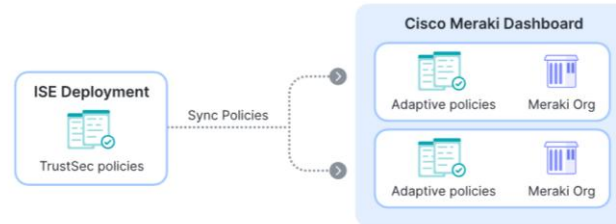
Integration of ISE with Meraki

Work Centers > TrustSec > Integrations

TrustSec Policy Policy Sets SXP **Integrations** Troubleshoot Reports Settings

Overview

You have carefully segmented your Cisco network by defining Cisco TrustSec policies and propagating them across the network using ISE. Now, you can easily extend these policies into the Meraki domain by using this Integration. Specify a set of policies that you want to replicate to one or more Meraki organizations, and the Integration will sync them automatically to Meraki Dashboard. From there, the policies will be propagated to your Meraki network devices.



1. Prepare

Identify the TrustSec policies currently configured in ISE that you wish to sync to Meraki

Identify the Meraki Organizations that you want to sync to. You must have access to each of these Organizations from your Meraki Dashboard account.

In Meraki Dashboard, enable access to the Meraki Dashboard API, and generate an API key for your account.

[Meraki Dashboard Authentication](#)

2. Define

Perform the setup workflow by pressing the Connect Meraki button.

Connect Meraki

In the workflow you will:

- Create a Meraki Dashboard connection.
- Select the Organizations to sync to.
- Specify the sync interval, i.e, how frequently the policy sync should be performed.
- Select ISE TrustSec policies to be synced.
- Select any additional SGACLs and Security Groups to be synced.

3. Go Live & Monitor

When setup workflow is completed, each selected policy will be synced to each of the selected Organizations.

Thereafter, any policy changes made in ISE will be detected at the next sync interval, and the corresponding policies in your Meraki Organizations will be updated to match.

At any time, you can change policy selections on the Sync Selections page, and Organization selections on the Connections page. These changes will be picked up at the next sync interval.

You can view the results of the latest sync operations on the Sync Status page.

Integration of ISE with Meraki

Work Centers > TrustSec > Integrations

The screenshot shows the 'Integrations' tab in the Cisco ISE TrustSec Policy configuration interface. A blue button labeled 'Connect Meraki' is highlighted with a rounded rectangle and a large blue arrow pointing to it from the right. The page content is organized into three columns: 1. Prepare, 2. Define, and 3. Go & Monitor.

TrustSec Policy | Policy Sets | SXP | **Integrations** | Troubleshoot | Reports | Settings

Overview

You have carefully segmented your network by defining Cisco TrustSec policies and propagating them across the network. Now, you can easily extend the protection of the Meraki domain by using this integration. Specify a set of policies that you want to replicate to one or more Meraki Organizations, and the Integration will sync them to Meraki Dashboard. From there, the policies will be propagated to your Meraki network devices.

1. Prepare

Identify the TrustSec policies currently configured in ISE that you wish to sync to Meraki.

Identify the Meraki Organizations that you want to sync to. You must have access to each of these Organizations from your Meraki Dashboard account.

In Meraki Dashboard, enable access to the Meraki Dashboard API, and generate an API key for your account.

[Meraki Dashboard Authentication](#)

2. Define

Perform the setup workflow by pressing the **Connect Meraki** button.

Connect Meraki

In the workflow you will:

- Create a Meraki Dashboard connection.
- Select the Organizations to sync to.
- Specify the sync interval, i.e., how frequently the policy sync should be performed.
- Select ISE TrustSec policies to be synced.
- Select any additional SGACLs and Security Groups to be synced.

3. Go & Monitor

When the setup workflow is completed, the selected policy will be synced to the Meraki Dashboard of the selected Organizations.

Thereafter, any policy changes made in ISE will be detected at the next sync interval, and the corresponding policies in your Meraki Organizations will be updated to match.

At any time, you can change policy selections on the Sync Selections page, and Organization selections on the Connections page. These changes will be picked up at the next sync interval.

You can view the results of the latest sync operations on the Sync Status page.

Integration of ISE with Meraki

Work Centers > TrustSec > Integrations

TrustSec Policy Policy Sets SXP **Integrations** Troubleshoot Reports Settings

Overview

You have carefully segmented your Cisco network by defining Cisco TrustSec policies and propagating them across the network using ISE. Now, you can easily extend these policies into the Meraki domain by using this Integration. Specify a set of policies that you want to replicate to one or more Meraki organizations, and the Integration will sync them automatically to Meraki Dashboard. From there, the policies will be propagated to your Meraki network devices.



1. Prepare

Identify the TrustSec policies currently configured in ISE that you wish to sync to Meraki

Identify the Meraki Organizations that you want to sync to. You must have access to each of these Organizations from your Meraki Dashboard account.

In Meraki Dashboard, enable access to the Meraki Dashboard API, and generate an API key for your account.

[Meraki Dashboard Authentication](#)

2. Define

Perform the setup workflow by pressing the Connect Meraki button.

Connect Meraki

In the workflow you will:

- Create a Meraki Dashboard connection.
- Select the Organizations to sync to.
- Specify the sync interval, i.e, how frequently the policy sync should be performed.
- Select ISE TrustSec policies to be synced.
- Select any additional SGACLs and Security Groups to be synced.

3. Go Live & Monitor

When setup workflow is completed, each selected policy will be synced to each of the selected Organizations.

Thereafter, any policy changes made in ISE will be detected at the next sync interval, and the corresponding policies in your Meraki Organizations will be updated to match.

At any time, you can change policy selections on the Sync Selections page, and Organization selections on the Connections page. These changes will be picked up at the next sync interval.

You can view the results of the latest sync operations on the Sync Status page.

The recommended maximum limits for TrustSec objects that Cisco ISE can share with Cisco Meraki dashboards:

- 625 policies, 7 ACLs per policy
- 95 ACLs, 16 rules per ACL
- 40 SGTs

Meraki Adaptive Policy

Organization > Configure > Adaptive Policy

Adaptive policy

[Policies](#)[Groups](#)[Custom ACLs](#)[Networks](#)

▼

Search...

26 networks, 1 selected

1 network selected

Enable

Disable

 Networks	Status ▼	
☒ WirelessNetwork	● Adaptive policy enabled	
☐ CNLab-PX	● Adaptive policy enabled	

20

▼ results per page

<

1

>

Meraki Group Policies

Network-wide > Configure > Group Policies

Name

Employee

Schedule ⓘ

Scheduling disabled ▾

Bandwidth ⓘ

Use custom bandwidth limit ▾

100 Mbps

[details](#)

Firewall and traffic shaping ⓘ

Custom SSID firewall & shaping rules ▾

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Allow ▾	Any ▾	172.23.0.0/16	Any		⛶ ✕
2	Deny ▾	Any ▾	172.16.0.0/12	Any		⛶ ✕
	Allow	Any	Any	Any	Default rule	

[Add a firewall rule](#)

Layer 7 firewall

#	Policy	Application		Actions
1	Deny	Video & music ▾	All Video & music ▾	⛶ ✕
2	Deny	Social web & photo sharing ▾	All Social web & photo sharing ▾	⛶ ✕

[Add a layer 7 firewall rule](#)

DNS layer protection (Cisco Umbrella)

Enable Umbrella protection

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

You have umbrella integration enabled on your MX. Click [here](#) to learn about using umbrella integration for MR with wireless advance license.

Traffic shaping

[Add a new shaping rule](#)

VLAN

Tag VLAN ▾

22

Adaptive Policy SGT

Assign SGT ▾

4: Employees ▾

Meraki Group Policies

Network-wide > Configure > Group Policies

Name

Employee

Schedule ⓘ

Scheduling disabled ▾

Bandwidth ⓘ

Use custom bandwidth limit ▾

100 Mbps

[details](#)

Firewall and traffic shaping ⓘ

Custom SSID firewall & shaping rules ▾

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Allow ▾	Any ▾	172.23.0.0/16	Any		⬆ ⬆ ✕
2	Deny ▾	Any ▾	172.16.0.0/12	Any		⬆ ⬆ ✕
	Allow	Any	Any	Any	Default rule	

[Add a firewall rule](#)

Layer 7 firewall

#	Policy	Application	Actions
---	--------	-------------	---------



Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Allow ▾	Any ▾	172.23.0.0/16	Any		⬆ ⬆ ✕
2	Deny ▾	Any ▾	172.16.0.0/12	Any		⬆ ⬆ ✕
	Allow	Any	Any	Any	Default rule	

Meraki Group Policies

Network-wide > Configure > Group Policies

Name

Employee

Schedule ⓘ

Scheduling disabled ▾

Bandwidth ⓘ

Use custom bandwidth limit ▾

100 Mbps

[details](#)

Firewall and traffic shaping ⓘ

Custom SSID firewall & shaping rules ▾

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Allow ▾	Any ▾	172.23.0.0/16	Any		<div>⊕</div> <div>×</div>

Layer 7 firewall

Tag VLAN ▾

22

DNS layer protection (Cisco Umbrella)

Enable Umbrella protection

You have umbrella integration enabled on your MX. Click [here](#) to learn about using umbrella integration for MR with wireless advance license.

Traffic shaping

[Add a new shaping rule](#)

VLAN

Tag VLAN ▾

22

Adaptive Policy SGT

Assign SGT ▾

4: Employees ▾

Meraki Group Policies

Network-wide > Configure > Group Policies

NameEmployee

Schedule ⓘScheduling disabled ▾

Bandwidth ⓘUse custom bandwidth limit ▾100 Mbps ▬details

Firewall and traffic shaping ⓘCustom SSID firewall & shaping rules ▾

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
---	--------	----------	-------------	------	---------	---------

Assign SGT ▾

4: Employees ▾

DNS layer protection (Cisco Umbrella)

Enable Umbrella protection

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

You have umbrella integration enabled on your MX. Click [here](#) to learn more about using umbrella integration for MR with wireless advance license.

Traffic shaping

Add a new shaping rule

VLAN

Tag VLAN ▾22

Adaptive Policy SGT

Assign SGT ▾4: Employees ▾

Meraki Group Policies – RADIUS Attribute

Wireless > Configure > Access Control

RADIUS

1 RADIUS server, 1 accounting server

RADIUS servers

#	Host IP or FQDN	Auth port	Secret	RadSec ⓘ	Test	Actions
1	172.23.0.111	1812		☐	<button>Test</button>	...

Add server 3 max.

RADIUS accounting servers

#	Host IP or FQDN	Acct port	Secret	RadSec ⓘ	Actions
1	172.23.0.111	1813		☐	...

Add server 3 max.

Accounting interim interval

10 minutes

☐ RADIUS testing ⓘ

☐ RADIUS CoA support ⓘ

☐ Dashboard RADIUS proxy ⓘ

RADIUS attribute specifying group policy name ⓘ

Filter-Id ▾

Meraki Group Policies – RADIUS Attribute

Wireless > Configure > Access Control

RADIUS attribute
specifying group policy
name



Filter-Id
Reply-Message
Airespace-ACL-Name
Aruba-User-Rule

- ☐ RADIUS testing ⓘ
- ☐ RADIUS CoA support ⓘ
- ☐ Dashboard RADIUS proxy ⓘ

RADIUS attribute ⓘ
specifying group policy
name

Filter-Id ▼



Meraki Group Policies – RADIUS Attribute

Policy > Policy Elements > Results > Authorization

Filter-Id

Reply-Message

Airespace-ACL-Name

Aruba-User-Rule

Common Tasks

☒ ACL (Filter-ID)

Employee

Attributes Details

Access Type = ACCESS_ACCEPT

Filter-ID = Employee

Meraki Group Policies – RADIUS Attribute

Policy > Policy Elements > Results > Authorization

Filter-Id

Reply-Message

Airespace-ACL-Name

Aruba-User-Rule

Common Tasks



Airespace ACL Name

Employee

Attributes Details

Access Type = ACCESS_ACCEPT

Airespace-ACL-Name = Employee

Meraki Group Policies – RADIUS Attribute

Policy > Policy Elements > Results > Authorization

Filter-Id

Reply-Message

Airespace-ACL-Name

Aruba-User-Role

Advanced Attributes Settings



Aruba:Aruba-User-Role



=

Employee

Attributes Details

Access Type = ACCESS_ACCEPT

Aruba-User-Role = Employee

Authorization Options with ISE



iPSK

Assigns unique pre-shared keys for endpoints on the same SSID

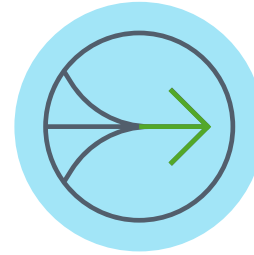
cisco-av-pair = **psk-mode=ascii**
cisco-av-pair = **psk**
Meraki Tunnel-Password



UDN

Enables users to create a private segment to add their devices

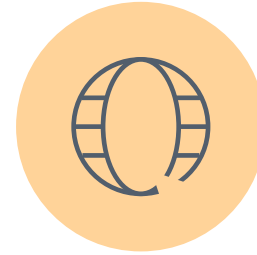
cisco-av-pair = **private-group-id**
cisco-av-pair = **private-group-name**
cisco-av-pair = **private-group-owner**



URL Redirect

Facilitates conditional web redirection when traffic is blocked

cisco-av-pair = **url-redirect-acl**
cisco-av-pair = **url-redirect**



URL Filter

Controls which FQDNs the endpoint can reach or not

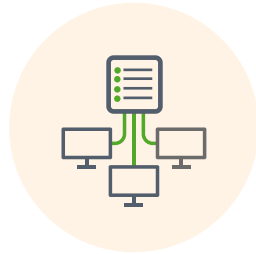
cisco-av-pair = **url-filter-preauth**
cisco-av-pair = **url-filter-postauth**



QoS

Permits prioritizing and managing per endpoint network traffic based on different criteria

cisco-av-pair = **ip:sub-qos-policy-in**
cisco-av-pair = **ip:sub-qos-policy-out**



mDNS Profile

Attaches mDNS profiles to broker mDNS advertisements

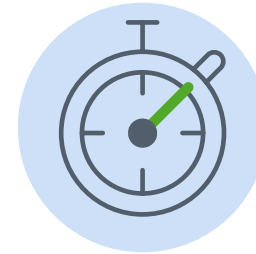
cisco-av-pair = **mDNS-profile-name**



Roles

Allocates a role that includes multiple attributes: VLAN, Session Timeout, ACL, QoS, mDNS

cisco-av-pair = **role**

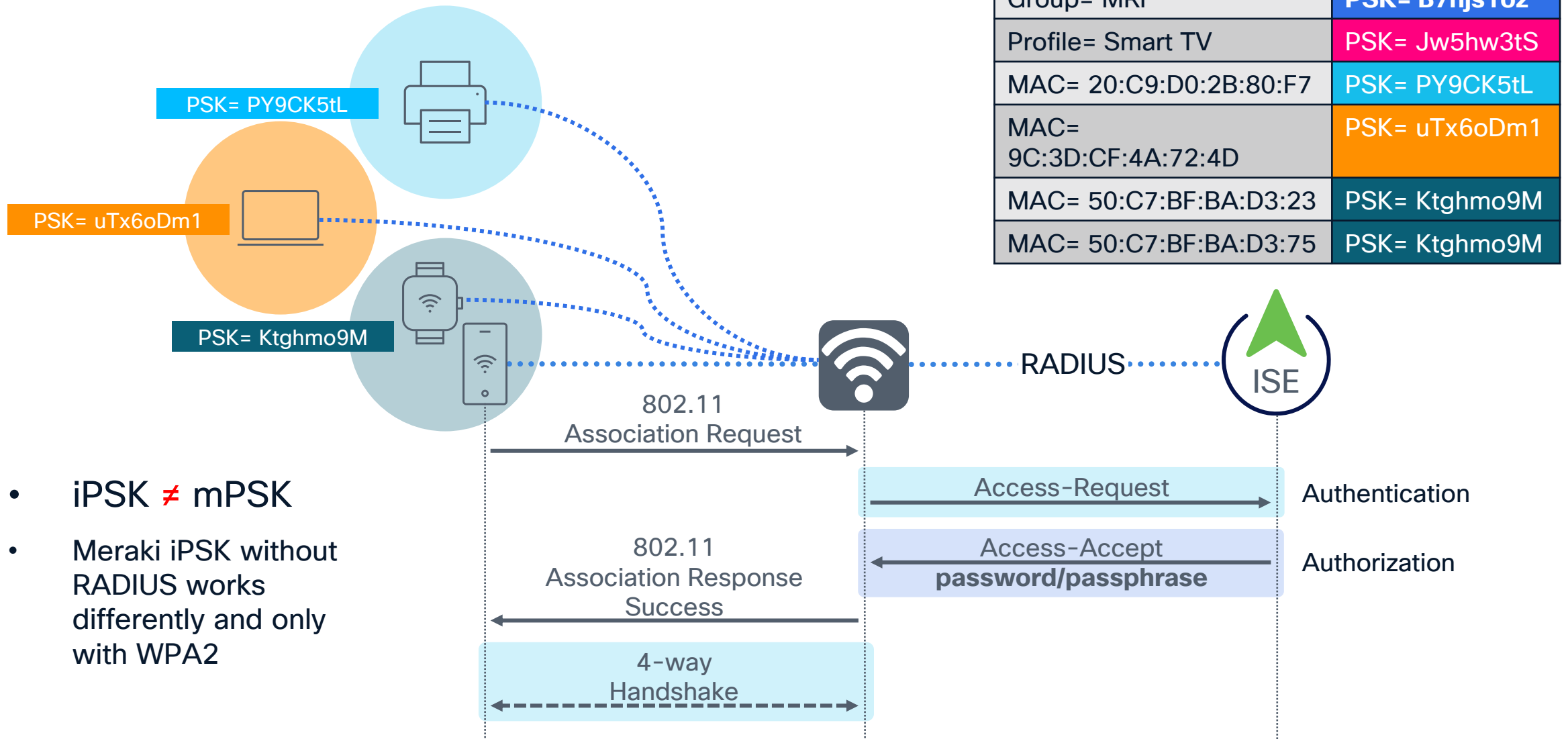


Timers

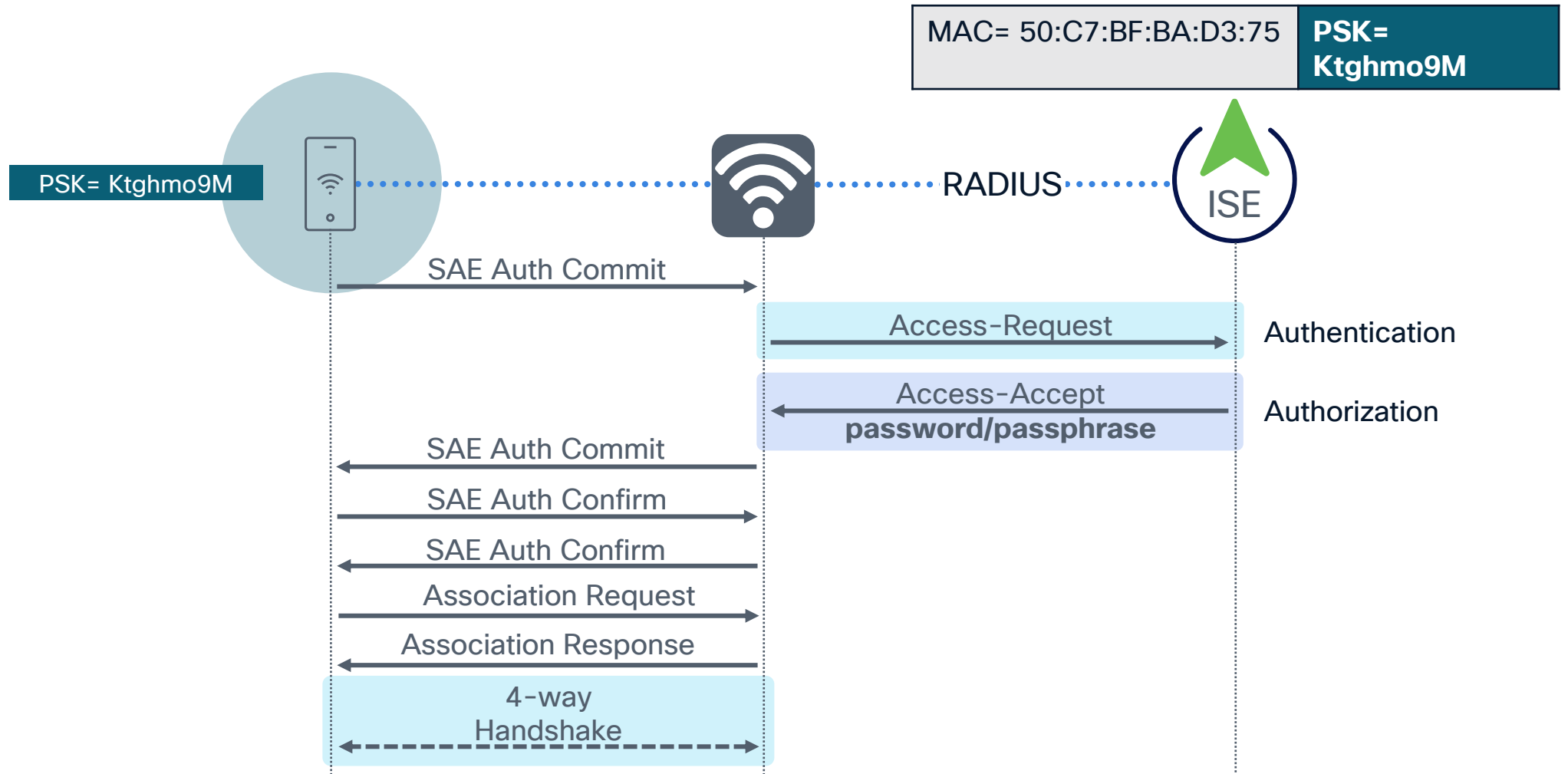
Sets the maximum duration of a user's session

Session-Timeout
Idle-Timeout

Identity PSK



Identity PSK – WPA3 SAE



Identity PSK – ISE Configuration

Policy > Policy Elements > Results > Authorization

Authorization Profile

* Name

authZprofile_iPSK1

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

Cisco

Service Template

☐

Track Movement

☐

Agentless Posture

☐

Passive Identity Tracking

☐

Advanced Attributes Settings

Cisco:cisco-av-pair

psk-mode=ascii

psk=CiscoiPSK1

Cisco:cisco-av-pair

=

psk-mode=ascii

Cisco:cisco-av-pair

=

psk=CiscoiPSK1

Identity PSK – ISE Configuration

Policy > Policy Sets > Authorization Policy

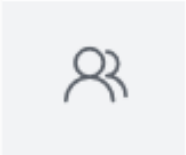
Status	Rule Name	Conditions	Results
			Profiles
✓	Group.1 Devices	 IdentityGroup-Name EQUALS Endpoint Identity Groups:Grp iP	authZprofile_iPSK1

authZprofile_iPSK1

Identity PSK – ISE Configuration

Policy > Policy Sets > Authorization Policy

Status	Rule Name	Conditions	Results
			Profiles
✓	Group.1 Devices	 IdentityGroup·Name EQUALS Endpoint Identity Groups:Grp_iPSK1 ↗	authZprofile_iPSK1

 IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Grp_iPSK1

Identity PSK – WLC Configuration

Configuration > Tags & Policy > Policy

General Security **Advanced** Add To Policy Tags

Coverage Hole Detection ☒

Aironet IE ☐

Advertise AP Name ☐

P2P Blocking Action ☐

Multicast Buffer

Media Stream Multicast-direct

Allow Private Gro... ▼

Disabled

Drop

Forward-UpStream

Allow Private Group

Allow Private Gro... ▼

Disabled

Drop

Forward-UpStream

Allow Private Group

Identity PSK – ISE Configuration (Option)

Administration > Identity Management > Settings > Endpoint Custom Attributes

Endpoint Custom Attributes

Attribute Name	Type		
Variable_iPSK	String		

Identity PSK – ISE Configuration (Option)

Context Visibility > Endpoints

Edit Endpoint

General Attributes

Mac Address*

78:A7:C7:52:9E:A6

Description

☐ Static Assignment

☒ Static Group Assignment

Policy Assignment

Apple-iPhone

Identity Group Assignment

Grp_iPSK1

Custom Attributes

Filter

Attribute String	Attribute Value	
<div><div>X</div><div>Attribute String</div></div>	<div>Attribute Value</div>	
Variable_iPSK	psk=CiscoiPSK1	<div><div></div><div></div></div>

Identity PSK – ISE Configuration (Option)

Context Visibility > Endpoints

Edit Endpoint

General Attributes

Mac Address*

78

Attribute String	Attribute Value
✕ Attribute String	Attribute Value
Variable_iPSK	psk=CiscoiPSK1

Attribute String	Attribute Value
✕ Attribute String	Attribute Value
Variable_iPSK	psk=CiscoiPSK1

Identity PSK – ISE Configuration (Option)

Policy > Policy Elements > Results > Authorization

Authorization Profile

* Name

authZprofile_iPSK1

Description

Cisco:cisco-av-pair

=

EndPoints:Variable_iPSK

Passive Identity Tracking

☐

Advanced Attributes Settings

Cisco:cisco-av-pair

=

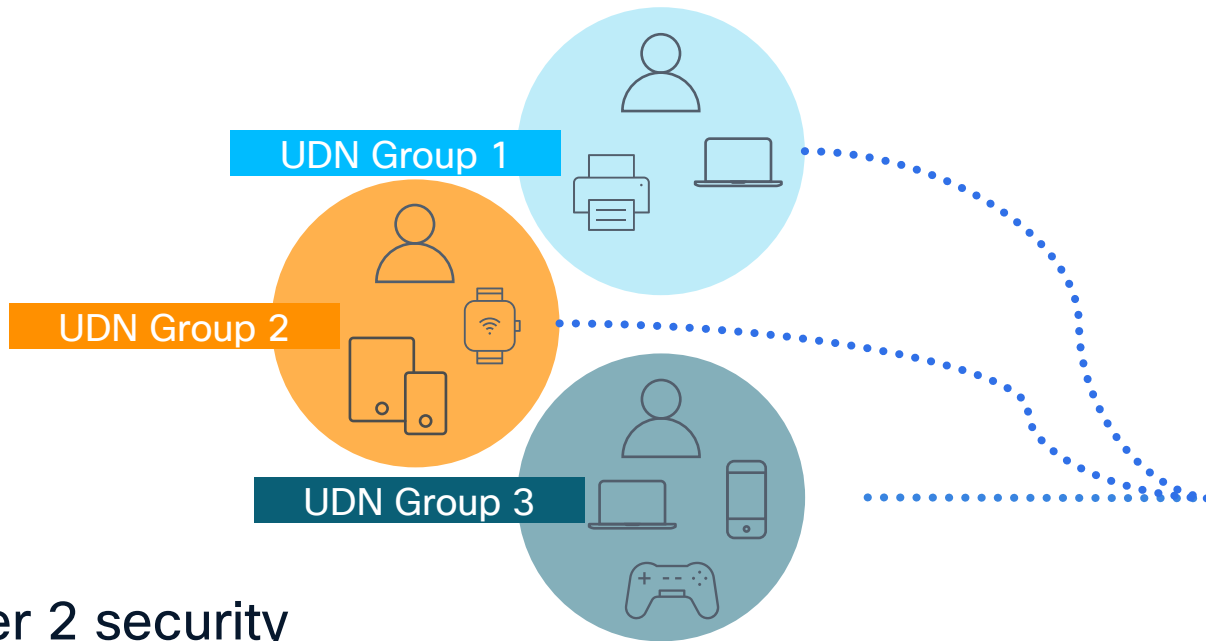
psk-mode=ascii

Cisco:cisco-av-pair

=

EndPoints:Variable_iPSK

User Defined Network (UDN)



Layer 2 security

- Open SSID + MAC filtering
- PSK + MAC filtering
- IPSK
- 802.1X

All the devices get their UDN ID, and devices with the same UDN ID are part of a private network.

Devices in the private network can see the multicast DNS (mDNS) and link-local advertisements only inside the private network.

Optionally, unicast traffic also can be restricted inside the private network and gateway.

UDN- ISE Configuration

Policy > Policy Elements > Results > Authorization

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

Common Tasks

☒ UDN Lookup

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = UDN:Private-group-id
cisco-av-pair = UDN:Private-group-name
cisco-av-pair = UDN:Private-group-owner

cisco-av-pair = UDN:Private-group-id
cisco-av-pair = UDN:Private-group-name
cisco-av-pair = UDN:Private-group-owner

UDN- WLC Configuration

Configuration > Tags & Profiles > Policy

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

28800



Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)



60

Guest LAN Session Timeout



DHCP

Fabric Profile



Search or Select



Link-Local Bridging



mDNS Service Policy

default-mdns-ser...



[Clear](#)

Hotspot Server

Search or Select



User Defined (Private) Network

Status



Drop Unicast



UDN- WLC Configuration

Configuration > Tags & Profiles > Policy

GeneralAccess PoliciesQOS and AVCMobilityAdvanced

User Defined (Private) Network

Status☒

Drop Unicast☐

Client Exclusion Timeout (sec)☒60

Guest LAN Session Timeout☐

DHCP

Fabric Profile☐

Link-Local Bridging☐

NS Service Policydefault-mdns-ser...[Clear](#)

Not Server☐

User Defined (Private) Network

Status☒

Drop Unicast☐

UDN– Meraki WPN

Wireless > Configure > Access Control

Wi-Fi Personal Network (WPN) ⓘ

Enabled

Disabled

WPN Supported Networks

802.1X

iPSK with RADIUS

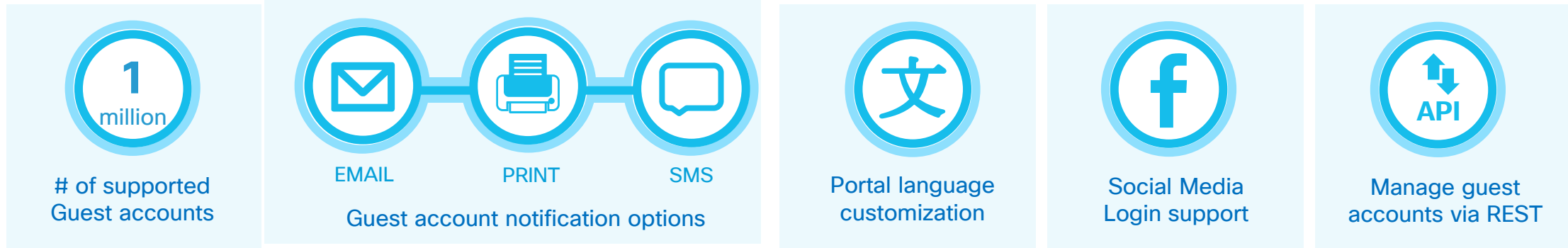
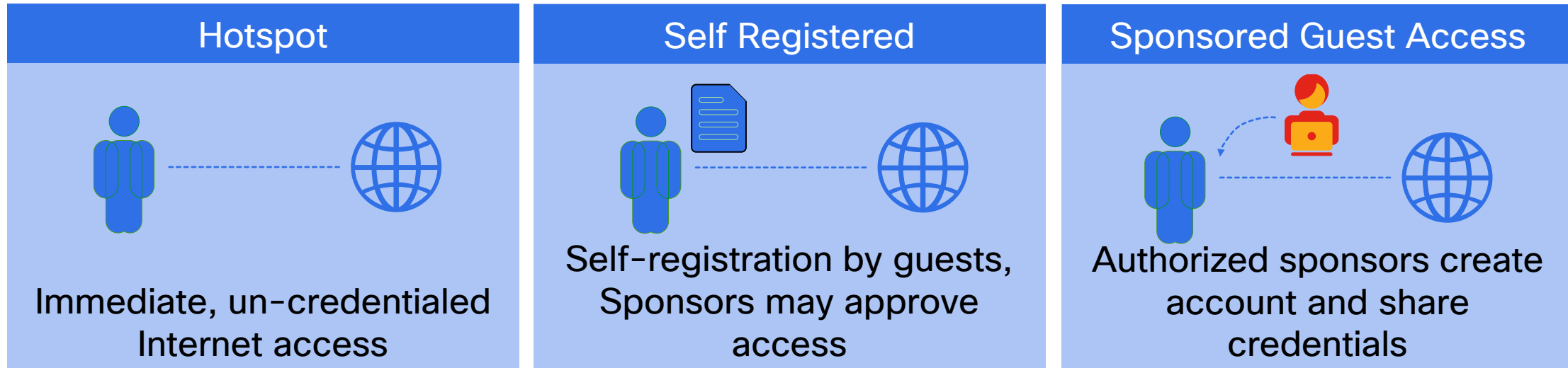
MAC Auth

iPSK without RADIUS



Not Interoperable with
UDN on Catalyst

ISE Guest Features



← The 3 types of guest access →

Authentication and Authorization Policies

ISE - Authentication Policy

Policy > Policy Sets > Authentication Policy

Authentication Policy(3)							
	Status	Rule Name	Conditions	Use	Hits	Actions	
	✓	MAB	OR <div>Wired_MAB</div> <div>Wireless_MAB</div>	Internal Endpoints <div>Options ⓘ</div> <div>If Auth fail REJECT</div> <div>If User not found CONTINUE</div> <div>If Process fail DROP</div>	108292	⚙️	
	✓	Dot1X	OR <div>Wired_802.1X</div> <div>Wireless_802.1X</div>	All_User_ID_Stores <div>Options</div>	1701	⚙️	
	✓	Default		All_User_ID_Stores <div>Options</div>	74	⚙️	

ISE - Authorization Policy

Policy > Policy Sets > Authentication Policy

Authorization Policy(10)

				Results					
+	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions		
	✓	SMLabGuestPortal_GuestAccessPolicy	AND Wireless_MAB Guest_Flow	SMLab_Guest_Access	SMLab_Guest	0			
	✓	SMLab Cameras	SMLab IOT Cameras	SMLab-Camera-IPSK	SMLab_IoT	0			
	✓	SMLab Admins	SMLab Admins	SMLab Jumphost	SMLab_Admin	0			
	✓	Sales	SMLab Sales Users	SMLab_Sales_Enterprise...	SMLab_Sales	0			
	✓	Marketing	SMLab Marketing Users	SMLab_Marketing_Enterpri...	SMLab_Marketing	0			
	✓	Finance	SMLab Finance Users	SMLab_Finance_Enterprise...	SMLab_Finance	0			
⋮	✓	Employees	SMLab Employees	SMLab_Employee_Enterpri...	SMLab_Employee	0			
	✓	Domain Computers	SMLab Domain Computers	SMLab_Employee_Enterpri...	SMLab_Domain_Computer	0			
	✓	Default		SMLabGuestPortal_Profile...	SMLab_Guest	0			

Wireless Access Control with Cisco Access Manager

Cisco Access Manager

Cloud-delivered access control services to enforce identity and context-based access to the users and devices

Multi-tenant SaaS for High Availability and Scale globally

Secure RADIUS transport over encrypted TLS tunnels to the Meraki Dashboard

Simplified and rapid Zero-Trust adoption using identity-based micro-segmentation

Flexible Authentication Options for wired and wireless users, computers, and I/OT

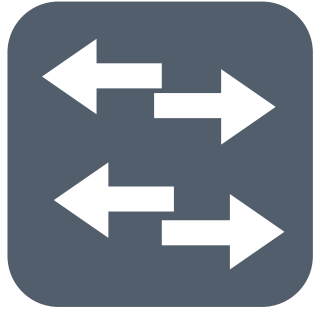


Cisco Access Manager – Solution Components

Users
+
Endpoints



Cloud-Managed
Networks



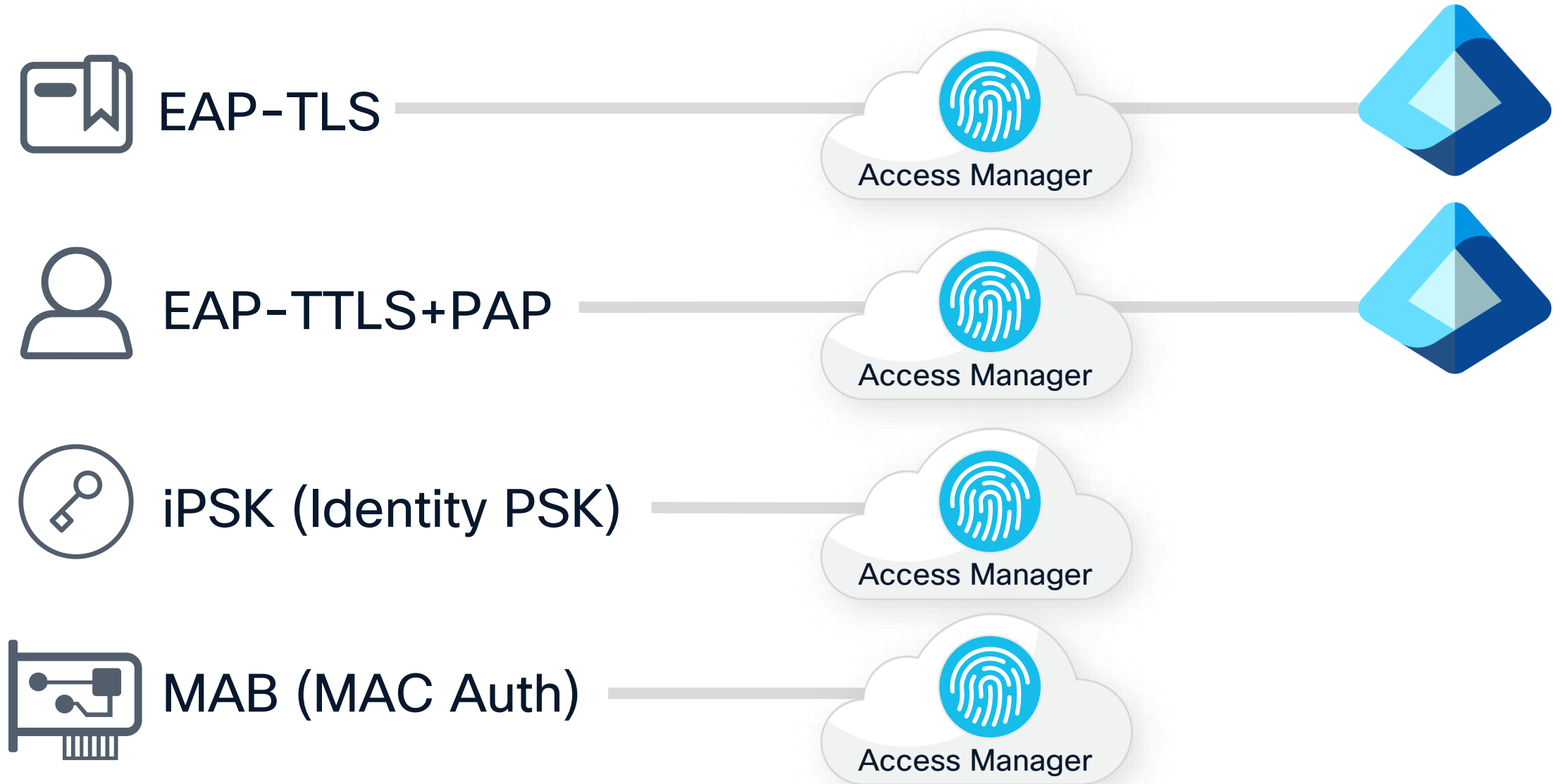
Meraki Dashboard



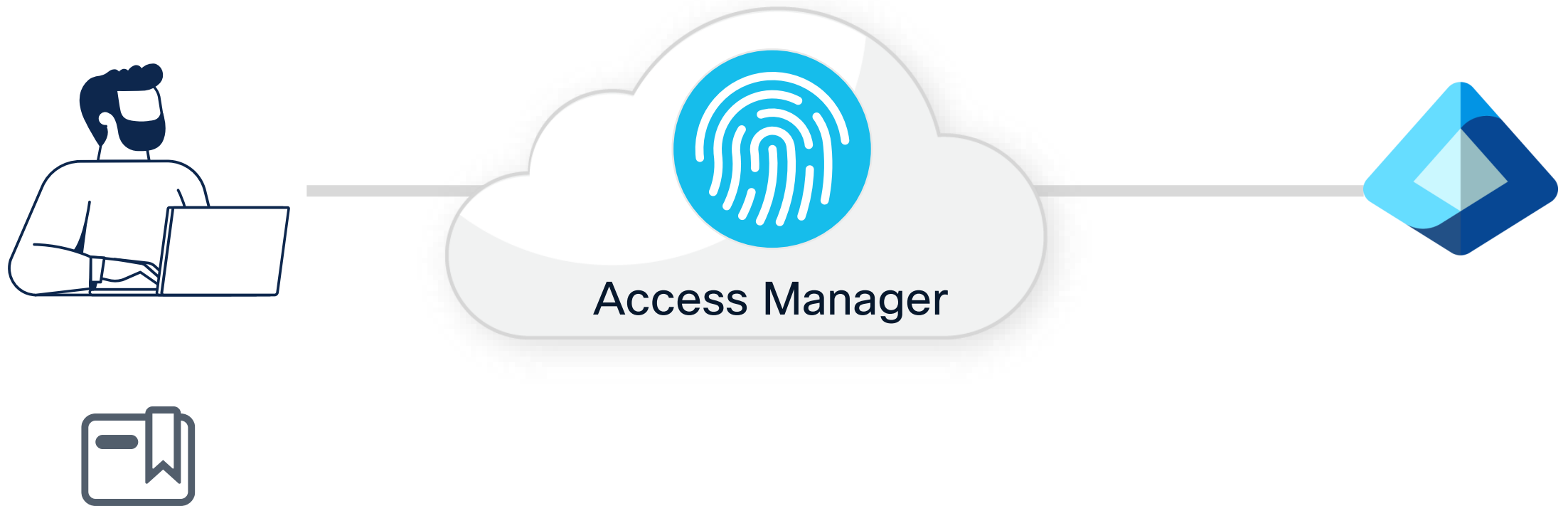
Identity Providers



Cisco Access Manager – Identify Users and Endpoints



Cisco Access Manager – EAP-TLS Authentication



Cisco Access Manager – EAP-TLS Authentication



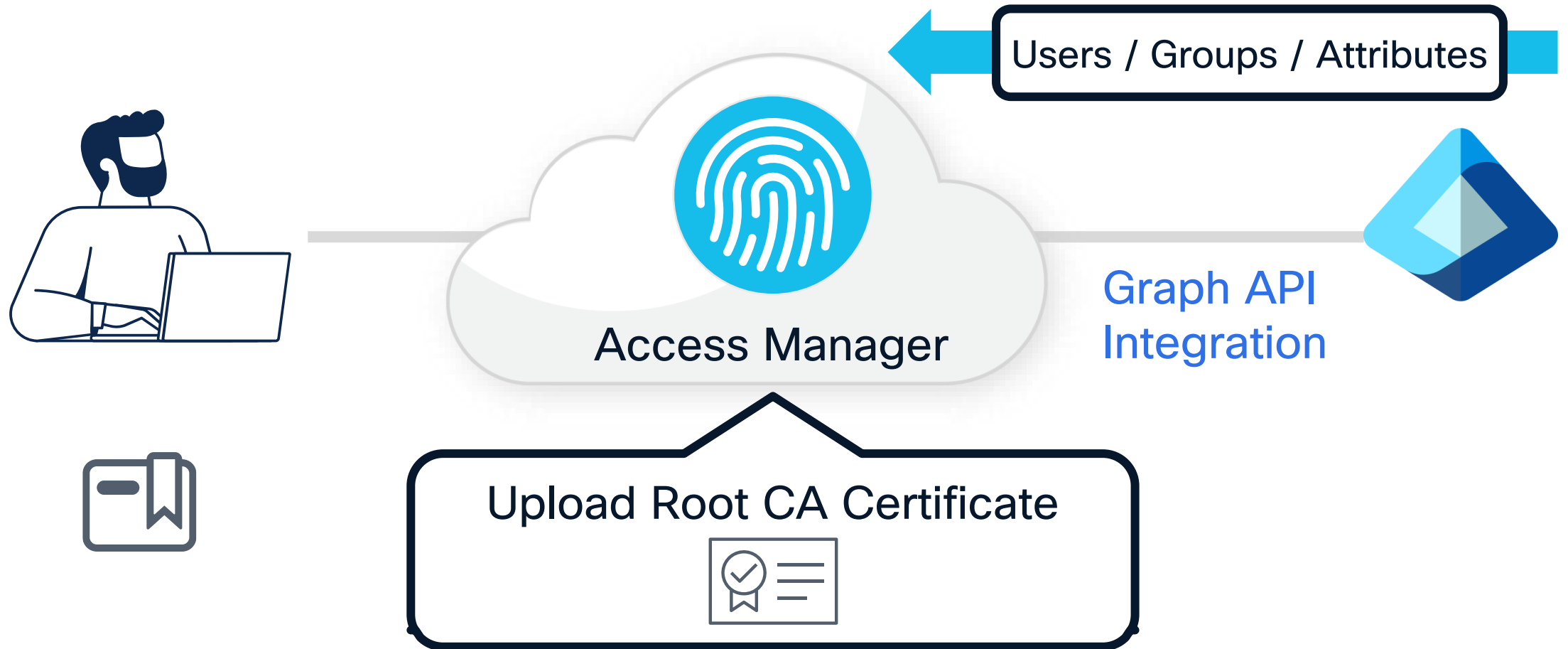
Max **150K** Microsoft Entra ID Users per Org
Max **100K** Microsoft Entra ID Groups per Org

Cisco Access Manager – EAP-TLS Authentication



***Sync Every 6 Hours**

Cisco Access Manager – EAP-TLS Authentication



Cisco Access Manager – EAP-TLS Authentication



Cisco Access Manager – EAP-TLS Authentication



What's matched

Attribute source 1

EntraID-AM

Group or Attribute

Group

Match a...

2

☒ Employee

☐ Employees

☒ Engineering



Cisco Access Manager – EAP-TLS Authentication



What's matched



Attribute source 1

Endpoint certificate

Group or Attribute

Issuer - Organizational Unit

Contains

APJC

Cisco Access Manager – EAP-TLS Authentication



What's matched

M

Attribute source 1

Network Access

Group or Attribute

SSID

1

☒ isedtea

Cisco Access Manager – EAP-TLS Authentication



What's matched

M

Attribute source 1

Network Access

Group or Attribute

Connection Method

1

☐ Wired

☒ Wireless

Cisco Access Manager – EAP-TLS Authentication



What's matched



Attribute source 1

RADIUS

Radius



Group or Attribute

NAS-Identifier



Equals



0:1A:2B:3C:4D:5E

Cisco Access Manager – EAP-TLS Authentication



Authorization

Access permission

Allow restricted access



VLAN ID / name

30

Cisco Access Manager – EAP-TLS Authentication



Authorization

Access permission

Allow restricted access



Adaptive policy

Infrastructure



Cisco Access Manager – EAP-TLS Authentication



Authorization

Access permission

Allow restricted access



Identity PSK

CiscoLiveRocks

Hide

Cisco Access Manager – EAP-TLS Authentication



Authorization

Access permission

Allow restricted access

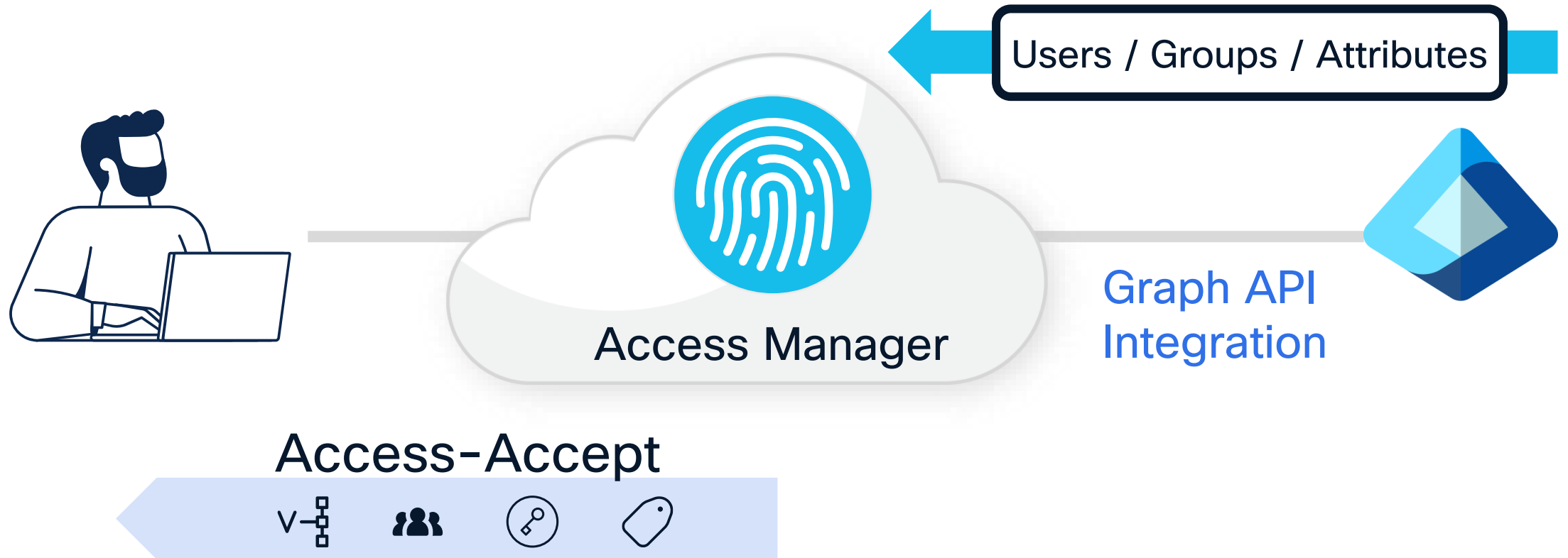


Group policy

Employee



Cisco Access Manager – EAP-TLS Authentication



Cisco Access Manager – EAP-TTLS Authentication



Cisco Access Manager – EAP-TTLS Authentication



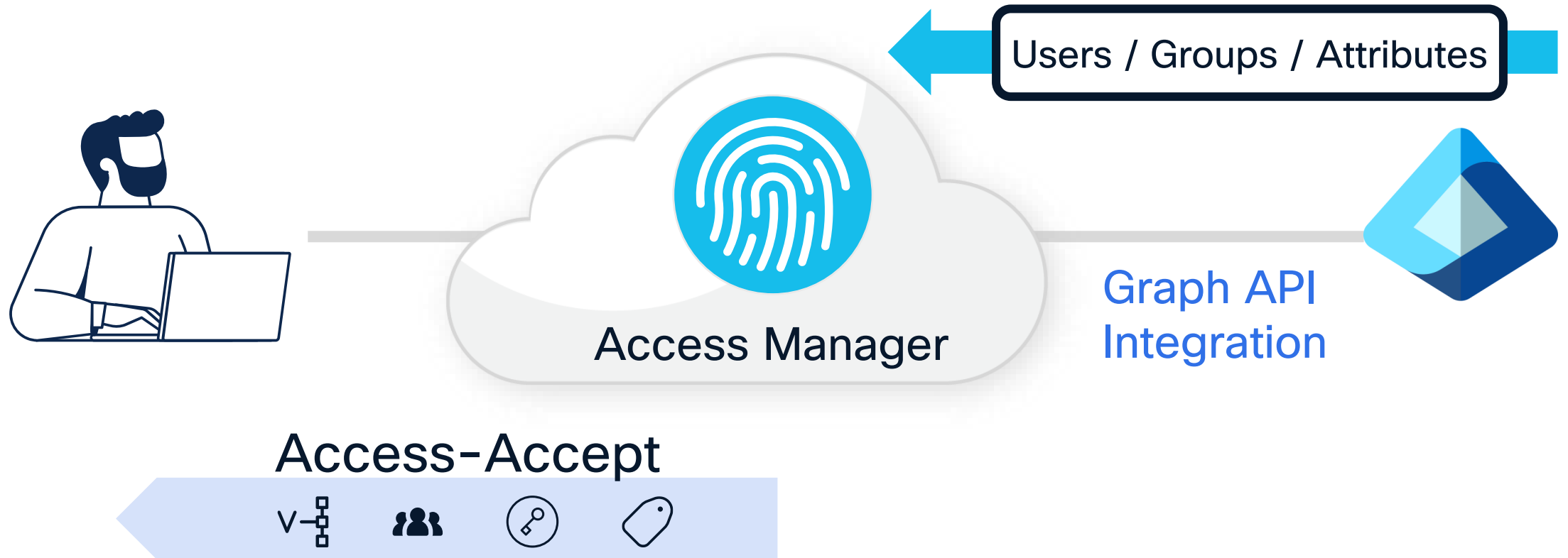
Cisco Access Manager – EAP-TTLS Authentication



Cisco Access Manager – EAP-TTLS Authentication



Cisco Access Manager – EAP-TTLS Authentication



Cisco Access Manager – iPSK/MAB Authentication



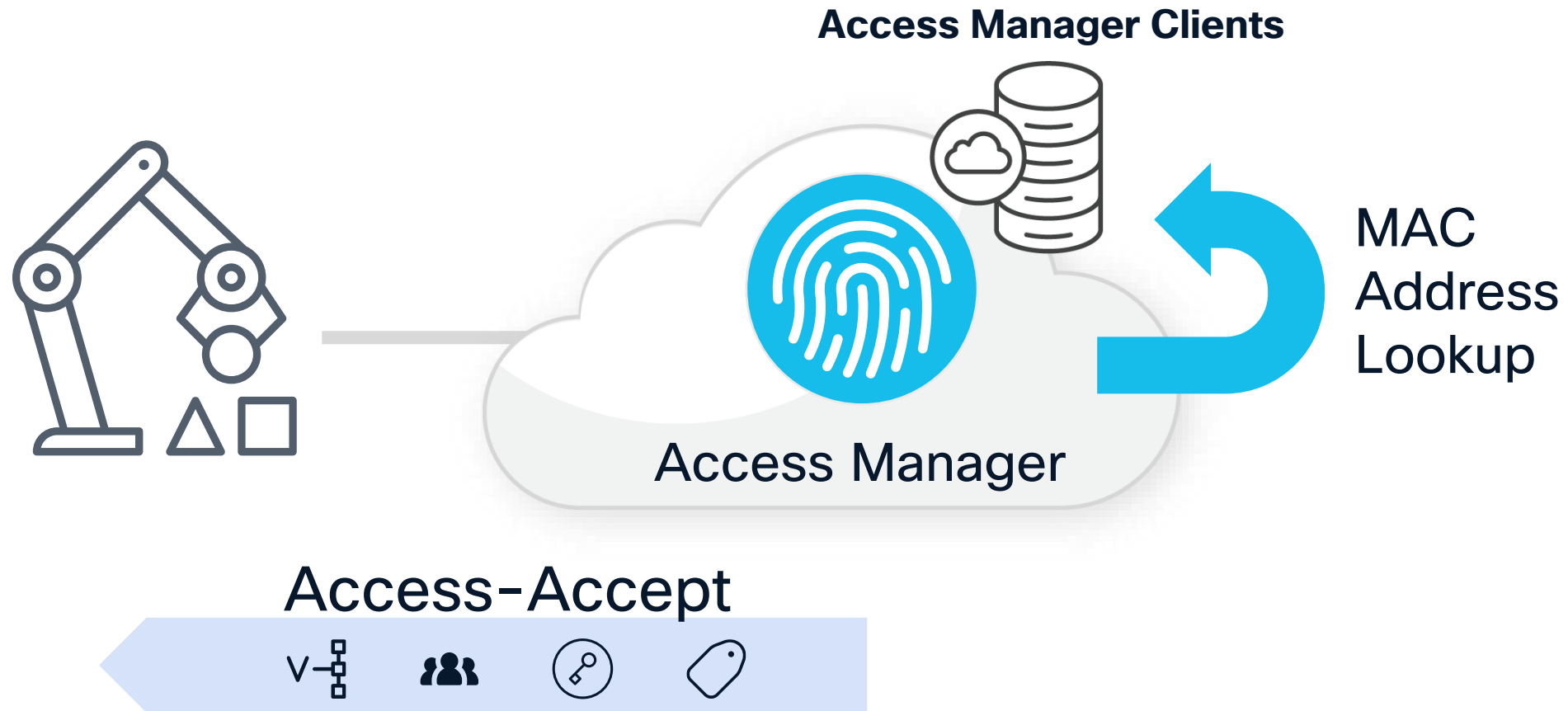
Cisco Access Manager – iPSK/MAB Authentication



Cisco Access Manager – iPSK/MAB Authentication



Cisco Access Manager – iPSK/MAB Authentication



Cisco Access Manager – Feature Summary



Authentication Methods

Authenticate users and device using



EAP-TLS (certificate)



EAP-TTLS (user/pwd)



MAB (MAC Authentication)



Identity & Context

Match identity & context attributes



Certificate Attributes



RADIUS Attributes



Entra ID Attributes



Network Access



Endpoint Attributes



Authorization Results

Apply authorization



Adaptive Policy Group



Group Policy



VLAN



iPSK

Wireless Configuration for Access Manager

Wireless > Configure > Access Control

☐ MAC-based access control (no encryption)

Access Manager ▼

RADIUS server is queried at association time

MAB

☐ Enterprise with

Access Manager ▼

User credentials are validated with 802.1X at association time

802.1X

☐ Identity PSK with RADIUS

Access Manager ▼

RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

iPSK

Access Rules

Access Manager > Policies > Access Rules

Type ⓘ	Status	Name	What's matched ⓘ	Authorization ⓘ
Rule group	✓	Default rule group	Any	
⋮ └ Rule	✓	Entra-ID-Group-Sales	MerakiNation-EntralID: Group = SALES [And] LAUNCHPAD	VLAN = 10 Adaptive policy = employees-sales ...
⋮ └ Rule	✓	EAP-TLS-certificate-SEs	Endpoint certificate: Issuer - Organization [Contains] Meraki, Subject - Common Name = MaryAnderson	VLAN = 10 Adaptive policy = employees-SEs ...
⋮ └ Rule	✓	IoT-client-SGT900	Endpoints: Client group = IoT-group	VLAN = 10 Adaptive policy = IoT ...
└ Rule	✓	Default rule	Any	Deny access ...

 Max 50 Rules

Session Log

Access Manager > Monitor > Session Log

Session Log ⓘ

1 All networks ⓘ

Last 30 days ▾

Q Search

Filters 94 matching results

↺

Time (UTC)	Status ⓘ	Details	Username	Endpoint MAC address	Authentication Protocol	SSID	Repeat counts ⓘ
Sep 05 15:06:12	⚠ Rejected	The matched rule has an AC...	12debe975b85	12:de:be:97:5b:85	MAB	DEMO - MAB-IPSK	0
Sep 05 15:06:06	⚠ Rejected	The matched rule has an AC...	12debe975b85	12:de:be:97:5b:85	MAB	DEMO - MAB-IPSK	0
Sep 04 21:32:51	✅ Success	IoT Cameras - IPSK/MAB	faf93ce4c2ed	fa:f9:3c:e4:c2:ed	MAB	DEMO - MAB-IPSK	1
Sep 04 21:32:17	✅ Success	IoT Cameras - IPSK/MAB	faf93ce4c2ed	fa:f9:3c:e4:c2:ed	MAB	DEMO - MAB-IPSK	1
Sep 04 18:46:12	✅ Success	IoT Cameras - IPSK/MAB	faf93ce4c2ed	fa:f9:3c:e4:c2:ed	MAB	DEMO - MAB-IPSK	1
Sep 03 13:18:36	❌ Failed	Supplicant stopped respond...		1e:11:f1:ac:0b:ad	EAP	CISCO-CORP	0
Sep 02 23:02:26	✅ Success	Engineering	Feynman@physicz.us	1e:11:f1:ac:0b:ad	EAP-TLS	CISCO-CORP	1
Aug 29 23:42:30	✅ Success	IoT Cameras - Wired	6cdea9000ac3	6c:de:a9:00:0a:c3	MAB		1
Aug 29 23:07:30	✅ Success	IoT Cameras - Wired	6cdea9000ac3	6c:de:a9:00:0a:c3	MAB		1
Aug 29 22:22:30	✅ Success	IoT Cameras - Wired	6cdea9000ac3	6c:de:a9:00:0a:c3	MAB		1

Session Log

Access Manager > Monitor > Session Log

Session Log ⓘ

1 All networks ⓘ

Last 30 days ▾

Q Search

Filters 94 matching results

Time (UTC)	Status ⓘ	Details	Username	Endpoint
Sep 05 15:06:12	⚠ Rejected	The matched rule has an AC...	12debe975b85	12:de:b...
Sep 05 15:06:06	⚠ Rejected	The matched rule has an AC...	12debe975b85	12:de:b...
Sep 04 21:32:51	✓ Success	IoT Cameras - iPSK/MAB	faf93ce4c2ed	fa:f9:3...
Sep 04 21:32:17	✓ Success	IoT Cameras - iPSK/MAB	faf93ce4c2	fa:f9:3...
Sep 04 18:46:12	✓ Success	IoT Cameras - iPSK/MAB	faf93ce4c	fa:f9:3...
Sep 03 13:18:36	❌ Failed	Supplicant stopped respond...		1e:11:f...
Sep 02 23:02:26	✓ Success	Engineering	Feynman@physicz.us	1e:11:f...
Aug 29 23:42:30	✓ Success	IoT Cameras - Wired	6cdea9000ac3	6c:de:a...
Aug 29 23:07:30	✓ Success	IoT Cameras - Wired	6cdea9000ac3	6c:de:a...
Aug 29 22:22:30	✓ Success	IoT Cameras - Wired	6cdea9000ac3	6c:de:a...

User

Username

Feynman@physicz.us

Endpoint

Endpoint MAC address

1e:11:f1:ac:0b:ad

Endpoint IP address

192.168.250.16

Authentication

Authentication method

EAP

Authentication protocol

EAP-TLS

Authorization

Authorization rule

Engineering

Authorization result

Adaptive policy = 42

Takeaways

Takeaways

No One-Size-Fits-All Solution

Every network is unique, evaluate your specific use cases focusing on security, scalability, and the diversity of devices in your environment.

Leverage ISE and Access Manager

Use these tools to enforce context-aware policies, simplify wireless access control, and align with both modern security and operational needs.

Adopt Best Practices

Follow key recommendations like top-down rule evaluation, Zero-Trust principles, and granular access policies to minimize interruptions and maintain security.

Simplify and Scale

With a cloud-native approach, simplify management today while ensuring effortless scalability for future growth.

Embrace Zero-Trust Principles

Design your strategy around identity-based micro-segmentation to ensure least-privilege access and prevent lateral movement.

Call to Action

Take the first step-evaluate your current challenges and explore how ISE and Access Manager can transform your wireless access strategy.

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.

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

Contact me at: caalcant@cisco.com

Thank you

CISCO Live !

