Securing Wireless Networks with Cisco Identity Services Engine and Access Manager

Fletcher Joyce
Solutions Engineer
fjoyce@cisco.com

Session ID: BRKEWN-2047

Cisco Webex App

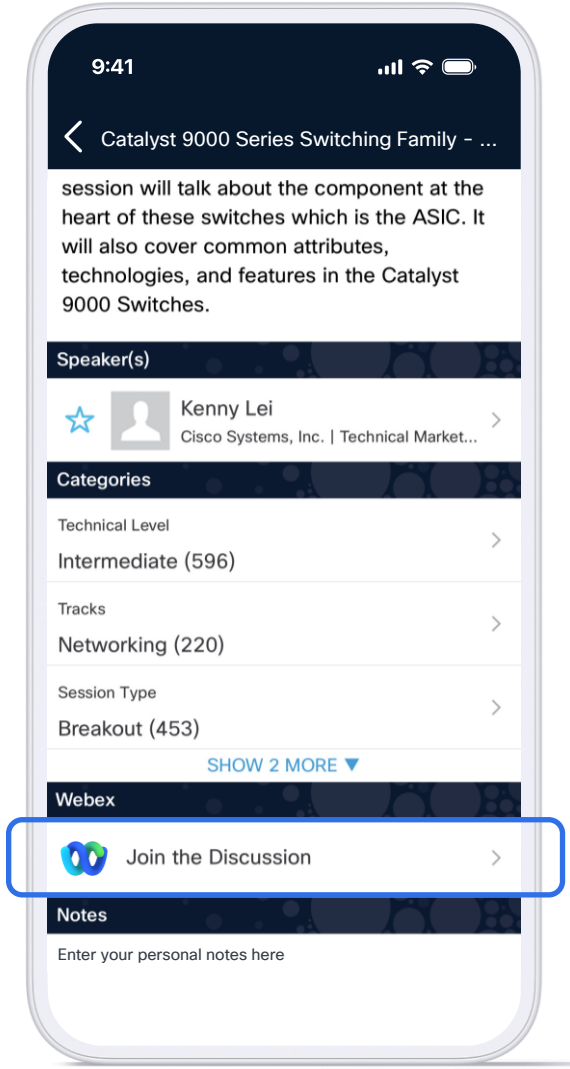
Questions?

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**

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

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

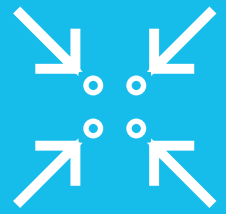
© 2025 Cisco and/or its affiliates. All rights reserved.

About Me

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

Before we jump in...

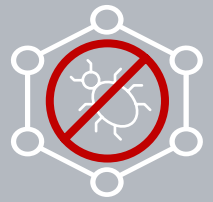
A security policy framework should help



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

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

Access Policy Fundamentals

Access Policy

WHO

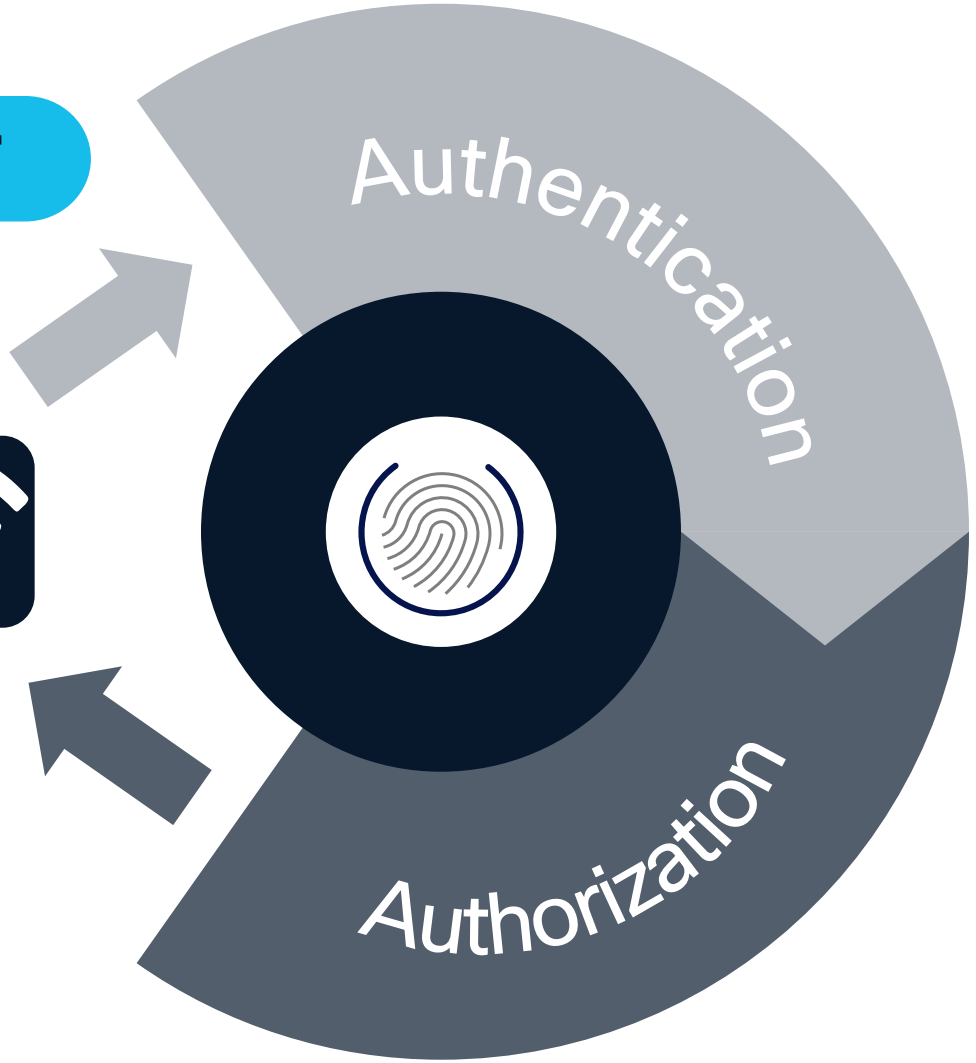
WHAT

HOW

802.1X
MAB
WebAuth

WHERE

WHEN



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

cisco

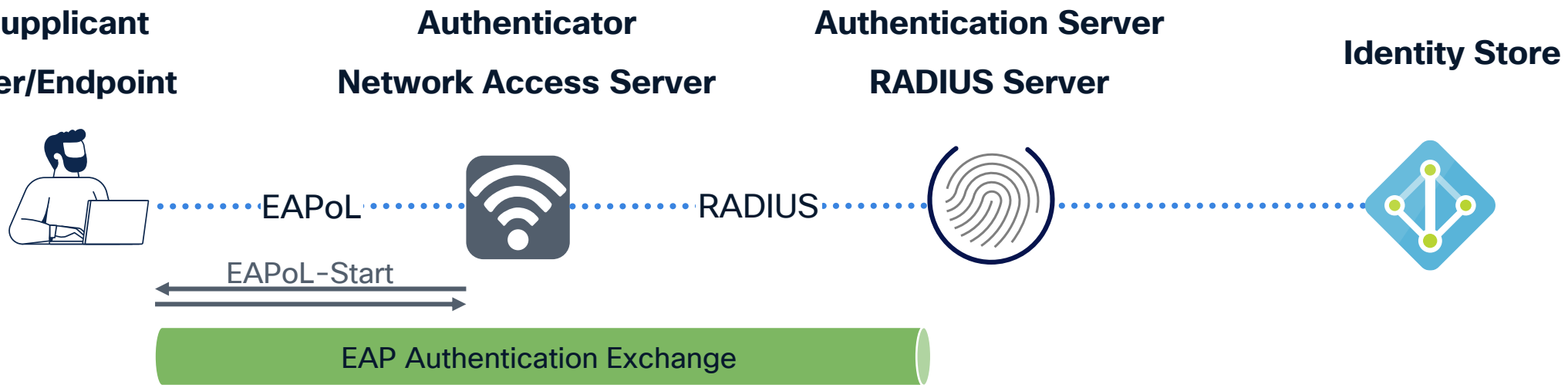
© 2025 Cisco and/or its affiliates. All rights reserved.

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

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

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

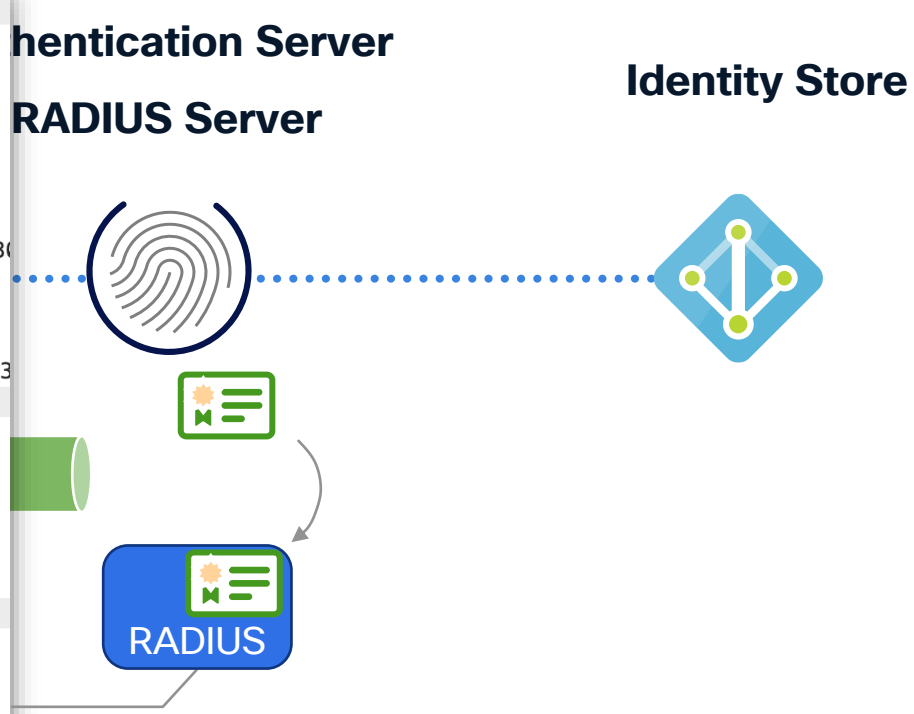
802.1X



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

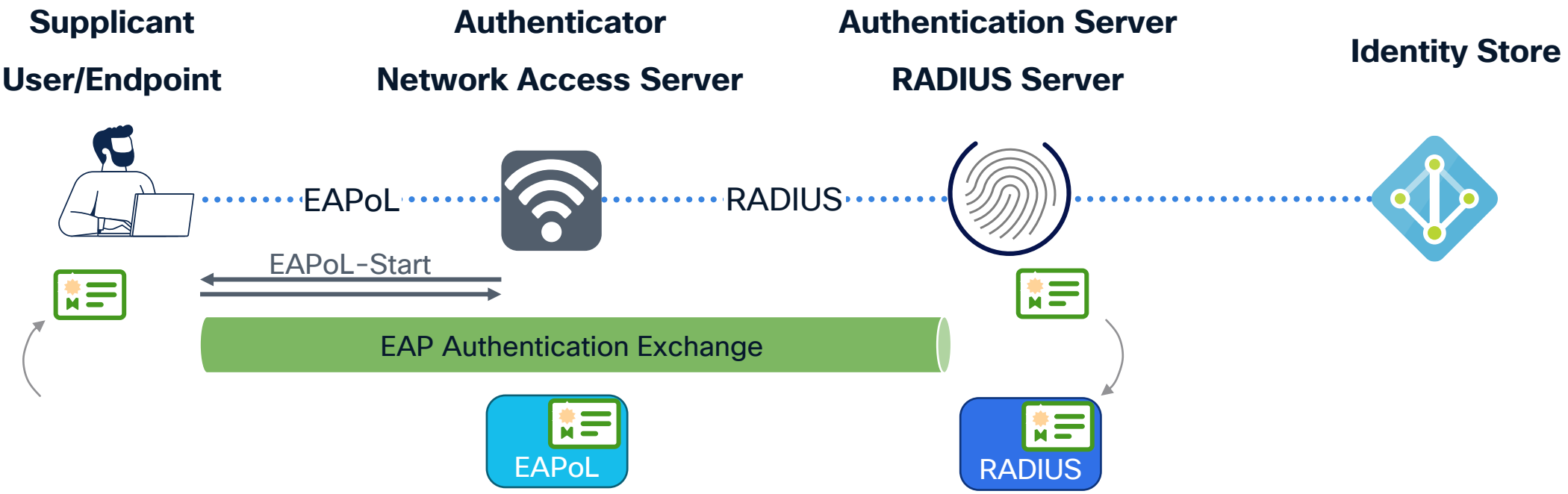
802.1X

```
RADIUS Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x9f (159)
    Length: 212
    Authenticator: d6a2602d5ceaf0efdee9c75856baf260
    [This is a response to a request in frame 75]
    [Time from request: 0.000623000 seconds]
  Attribute Value Pairs
    > AVP: t=State(24) l=84 val=333743504d53657373696f6e49443d343733393137414330303030303(
    AVP: t=EAP-Message(79) l=90 Last Segment[1]
        Type: 79
        Length: 90
        EAP fragment: 019200581900e0dae44d3c3a5fcc8f02108ea90b60960bc0f7a7cc94048908cdcb3
      Extensible Authentication Protocol
          Code: Request (1)
          Id: 146
          Length: 88
          Type: Protected EAP (EAP-PEAP) (25)
        > EAP-TLS Flags: 0x00
        > [4 EAP-TLS Fragments (3088 bytes): #70(1002), #72(1002), #74(1002), #76(82)]
        Transport Layer Security
          > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
          TLSv1.2 Record Layer: Handshake Protocol: Certificate
              Content Type: Handshake (22)
              Version: TLS 1.2 (0x0303)
              Length: 2350
            Handshake Protocol: Certificate
                Handshake Type: Certificate (11)
                Length: 2346
                Certificates Length: 2343
              Certificates (2343 bytes)
                  Certificate Length: 1404
                > Certificate […]: 3082057830820460a003020102021312000017795 1b4c349eb4
                  Certificate Length: 933
                > Certificate […]: 308203a130820289a003020102021063673 7fc160a5a98420a8
          > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
          > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
    > AVP: t=Message-Authenticator(80) l=18 val=3b28cab9939f5dfb72fd911ec578a9ae
```



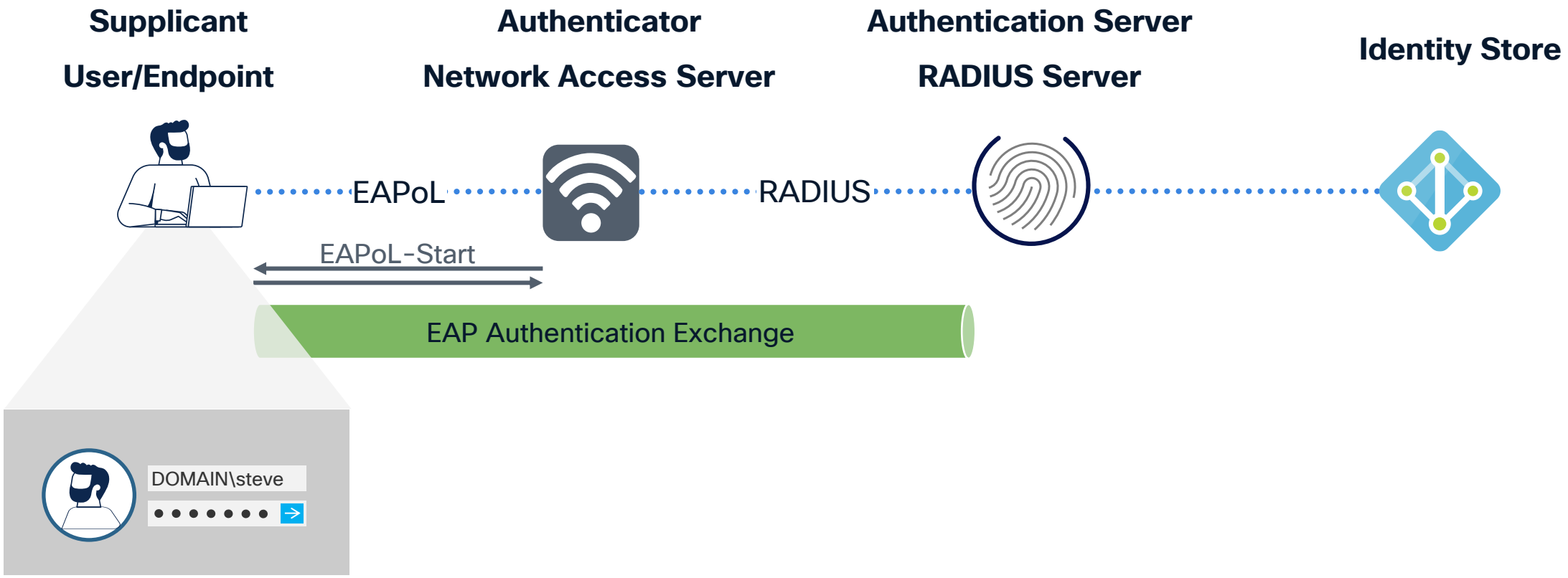
© 2025 Cisco and/or its affiliates. All rights reserved.

802.1X



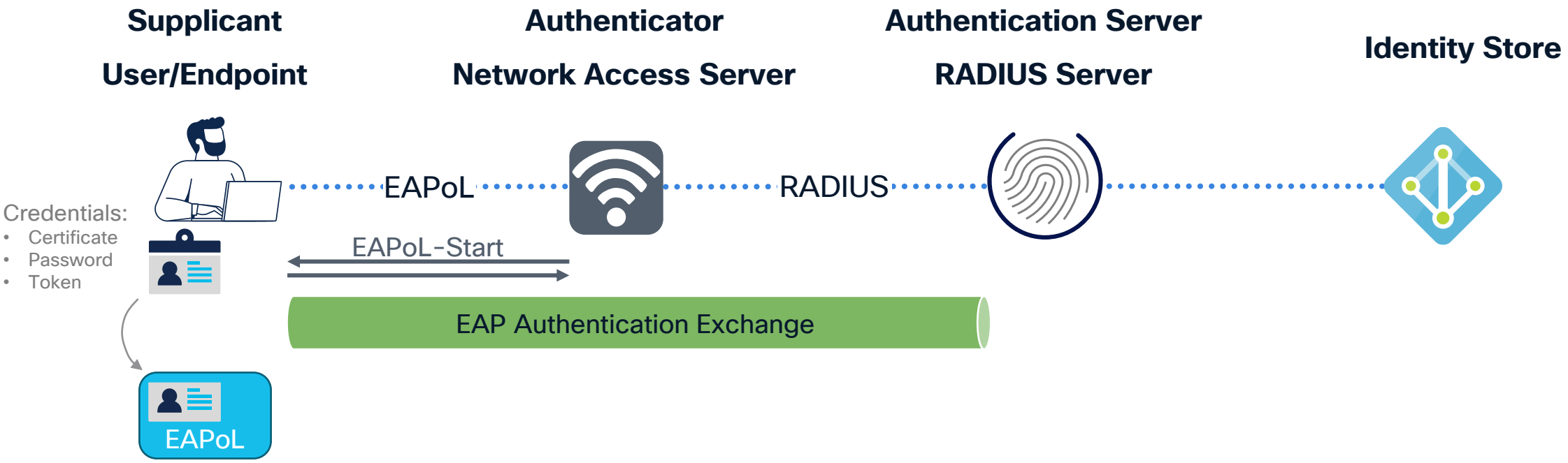
© 2025 Cisco and/or its affiliates. All rights reserved.

802.1X



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

802.1X



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

802.1X

Supplicant

User/Endpoint

Authenticator

Network Access Server

Authentication Server

RADIUS Server

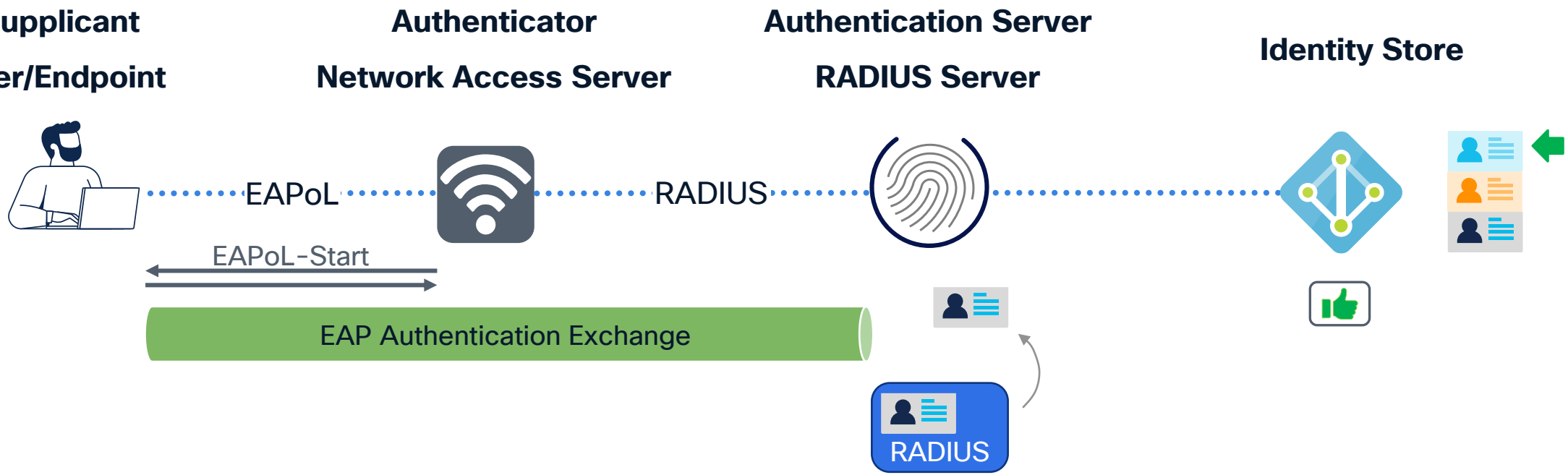
Identity Store

```
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=333743504d53657373696f6e49443d343733
    > 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
```

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

cisco

802.1X



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

802.1X

Supplicant

User/Endpoint

Authenticator

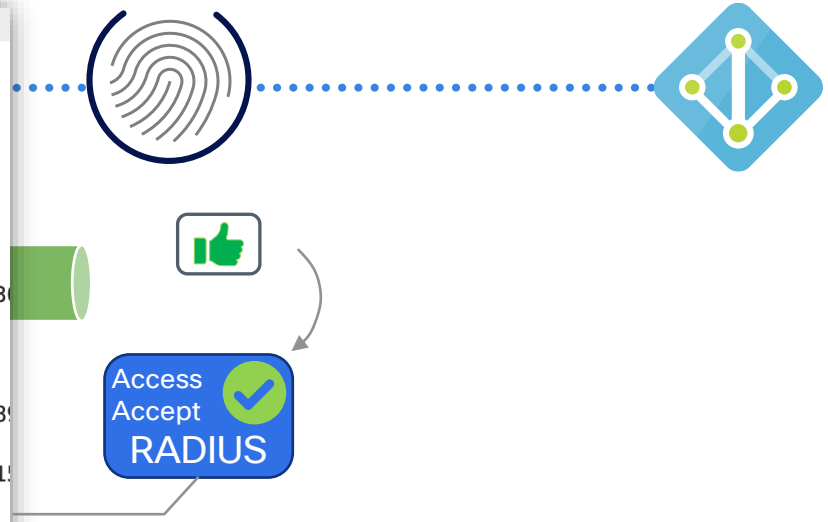
Network Access Server

Authentication Server

RADIUS Server

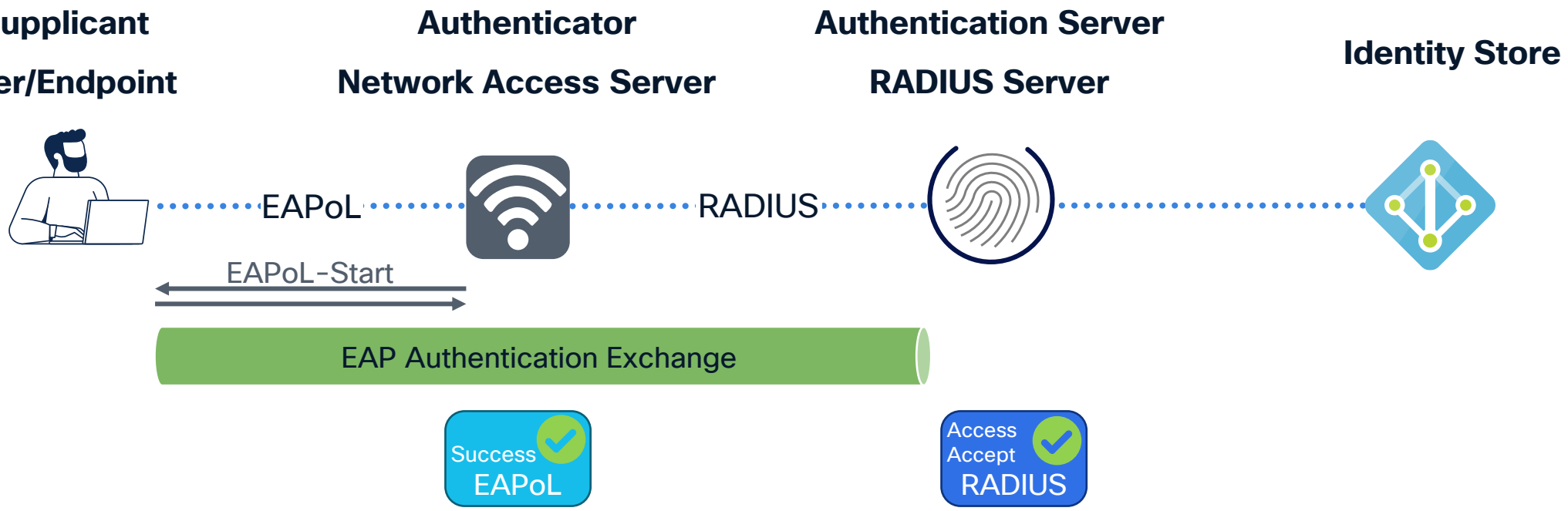
Identity Store

```
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)
```



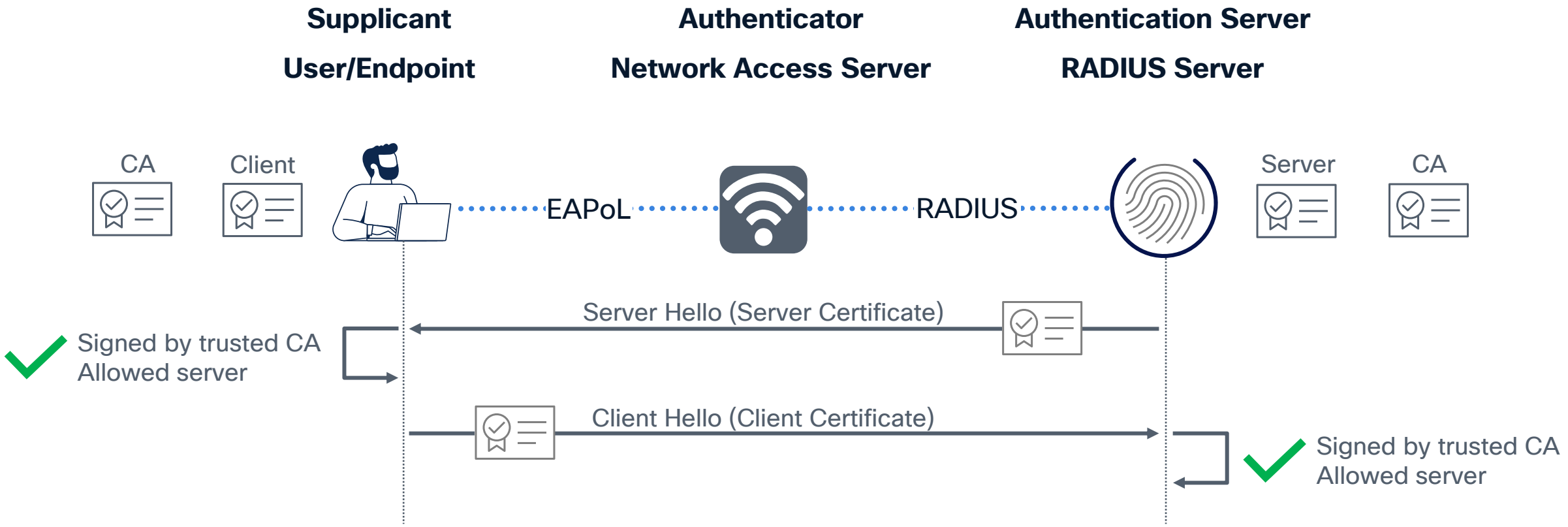
© 2025 Cisco and/or its affiliates. All rights reserved.

802.1X



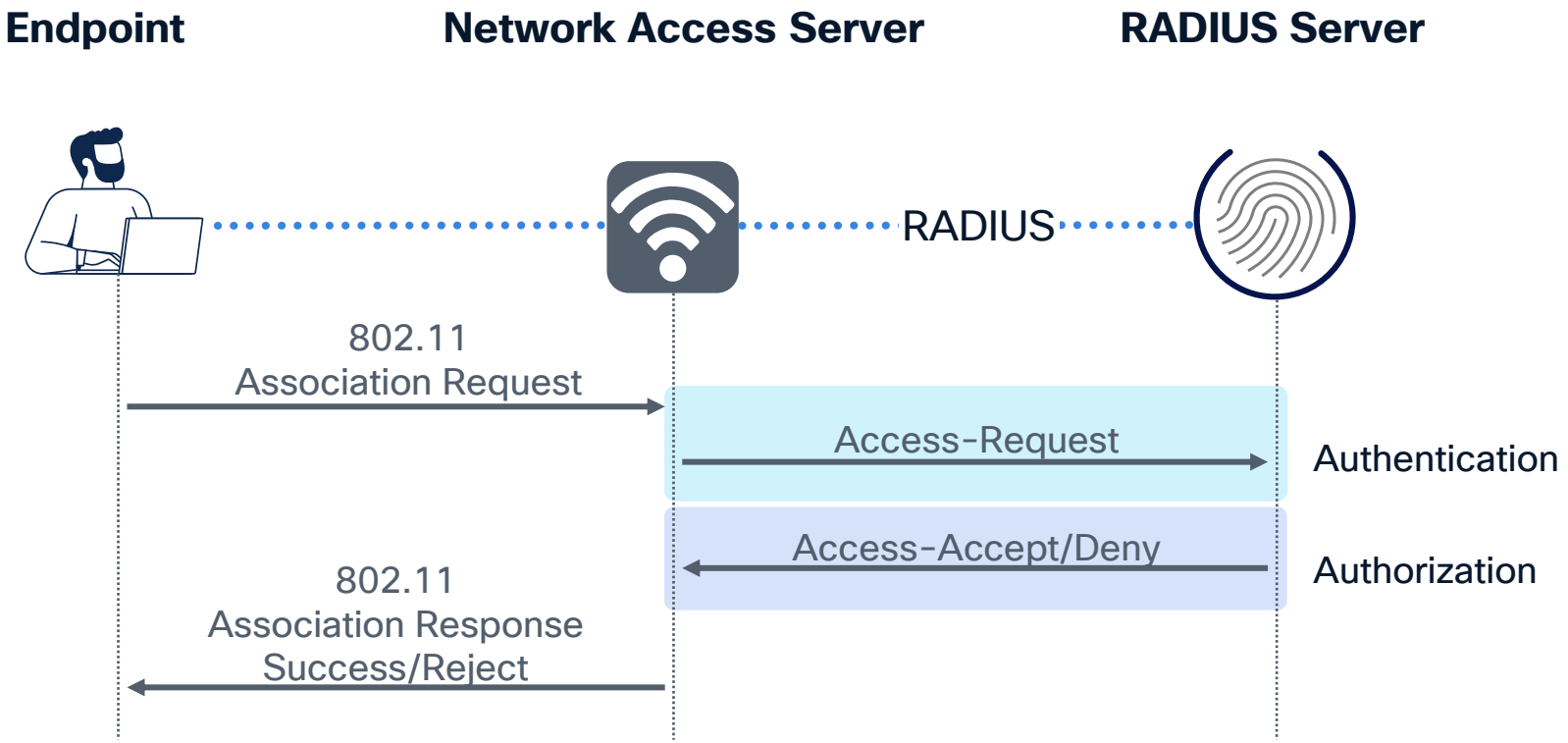
© 2025 Cisco and/or its affiliates. All rights reserved.

EAP-TLS



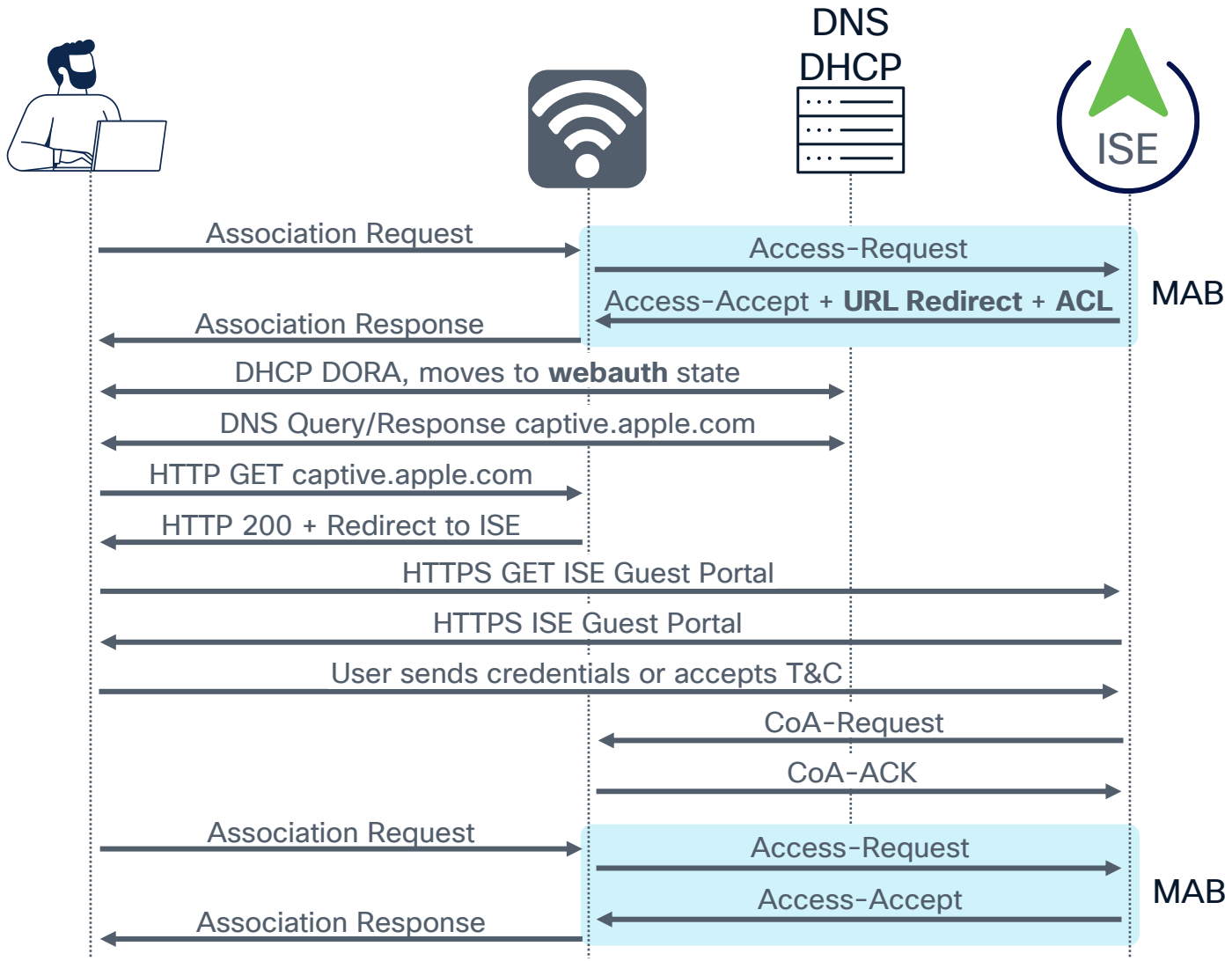
© 2025 Cisco and/or its affiliates. All rights reserved.

MAC Authentication



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

Central Web Authentication (CWA)



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

RADIUS Packet Format

RFC 2865 RADIUS

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=333743504d53657373696f6e49443d343733
      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)
```

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

cisco

Managing Wireless Access with Identity Services Engine

CISCO Live !

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

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

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+)	✅	✅	✅	✅

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

cisco

Authorization Results

Identity and Context

Adding Wireless Network Devices to ISE

Wireless Infrastructure - Base Configuration for ISE

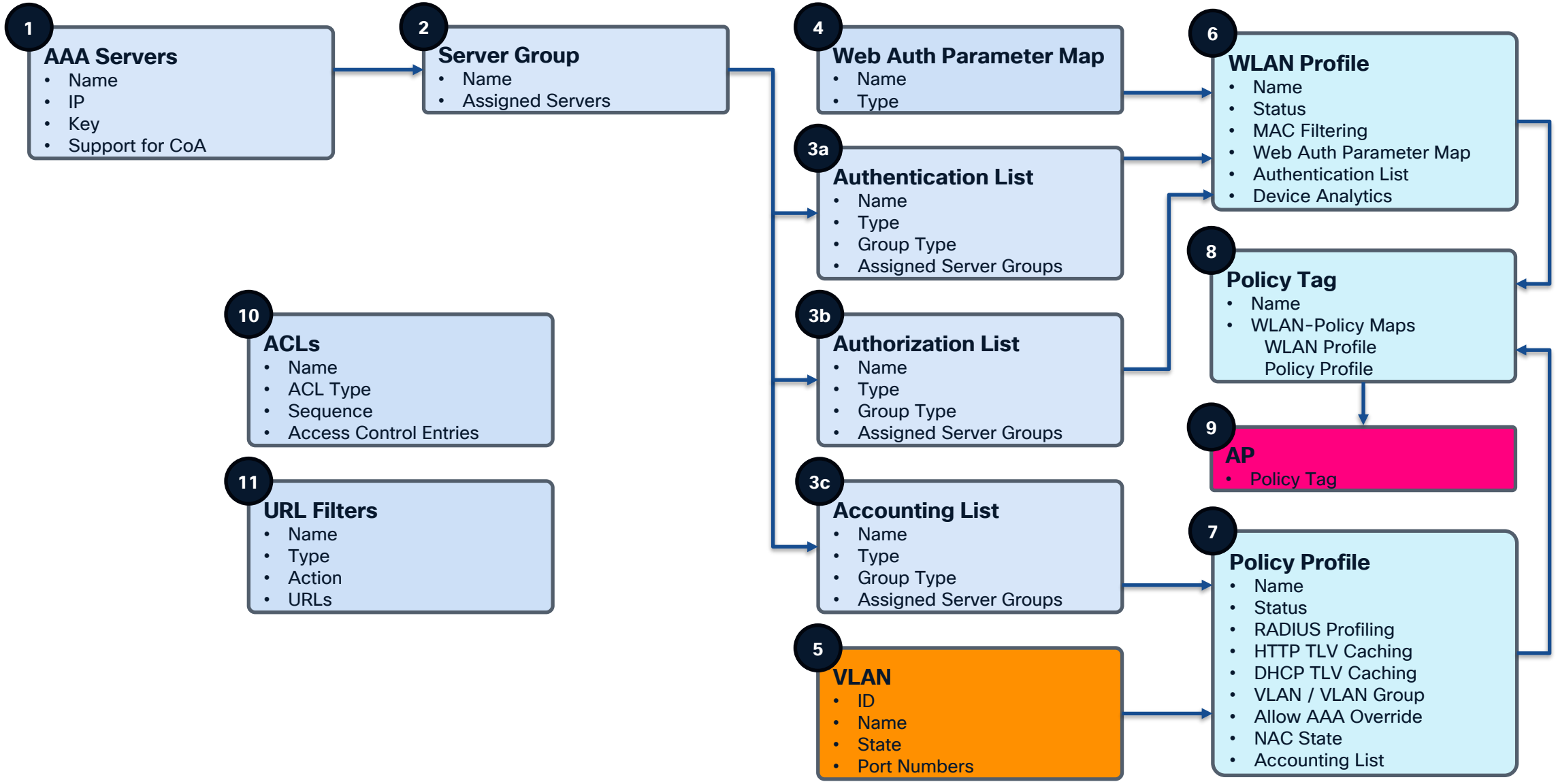
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Catalyst 9800
Base Configuration for ISE

cisco Live !

Catalyst 9800 Configuration for ISE



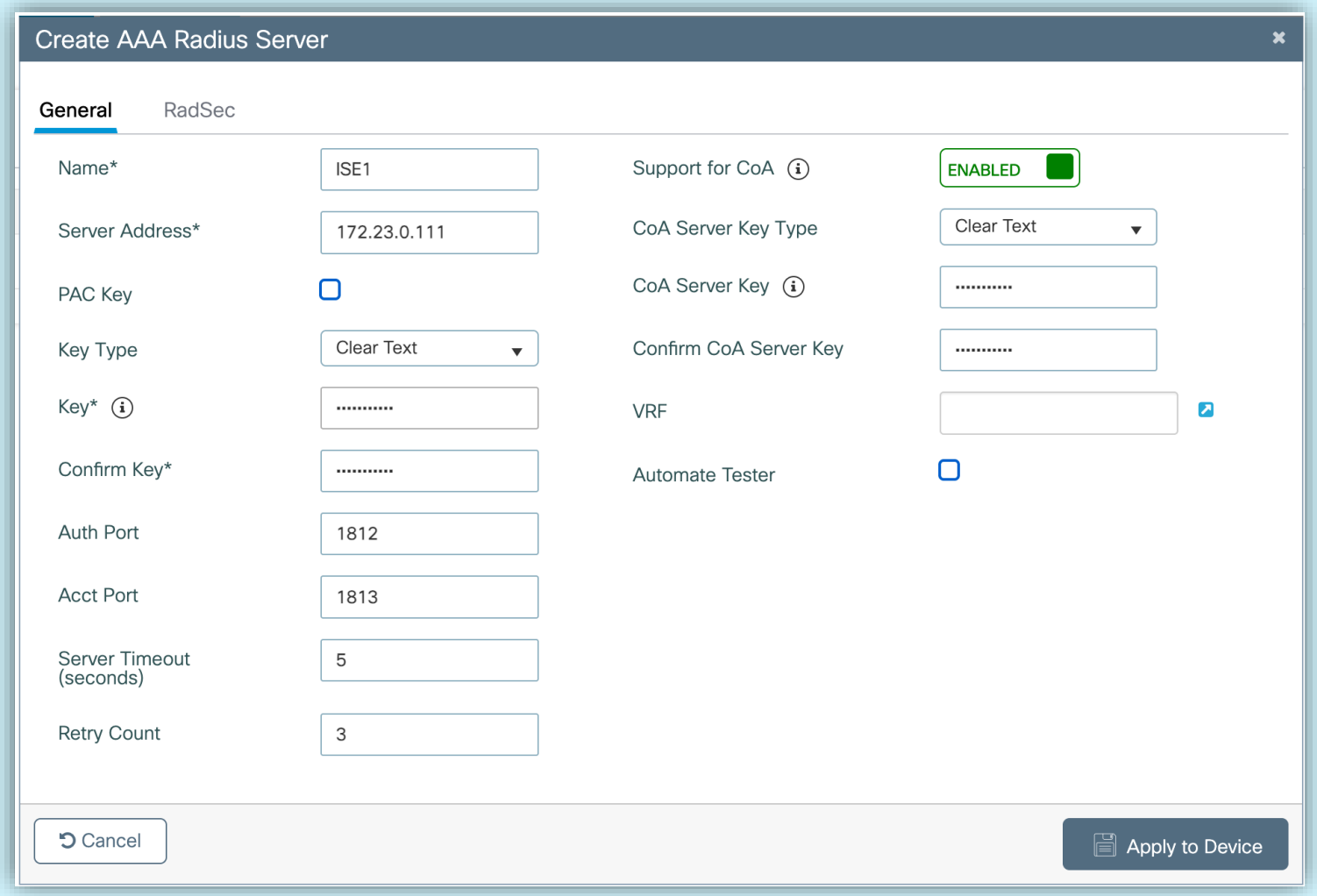
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

1 AAA Servers

Reference

Configuration > Security > AAA

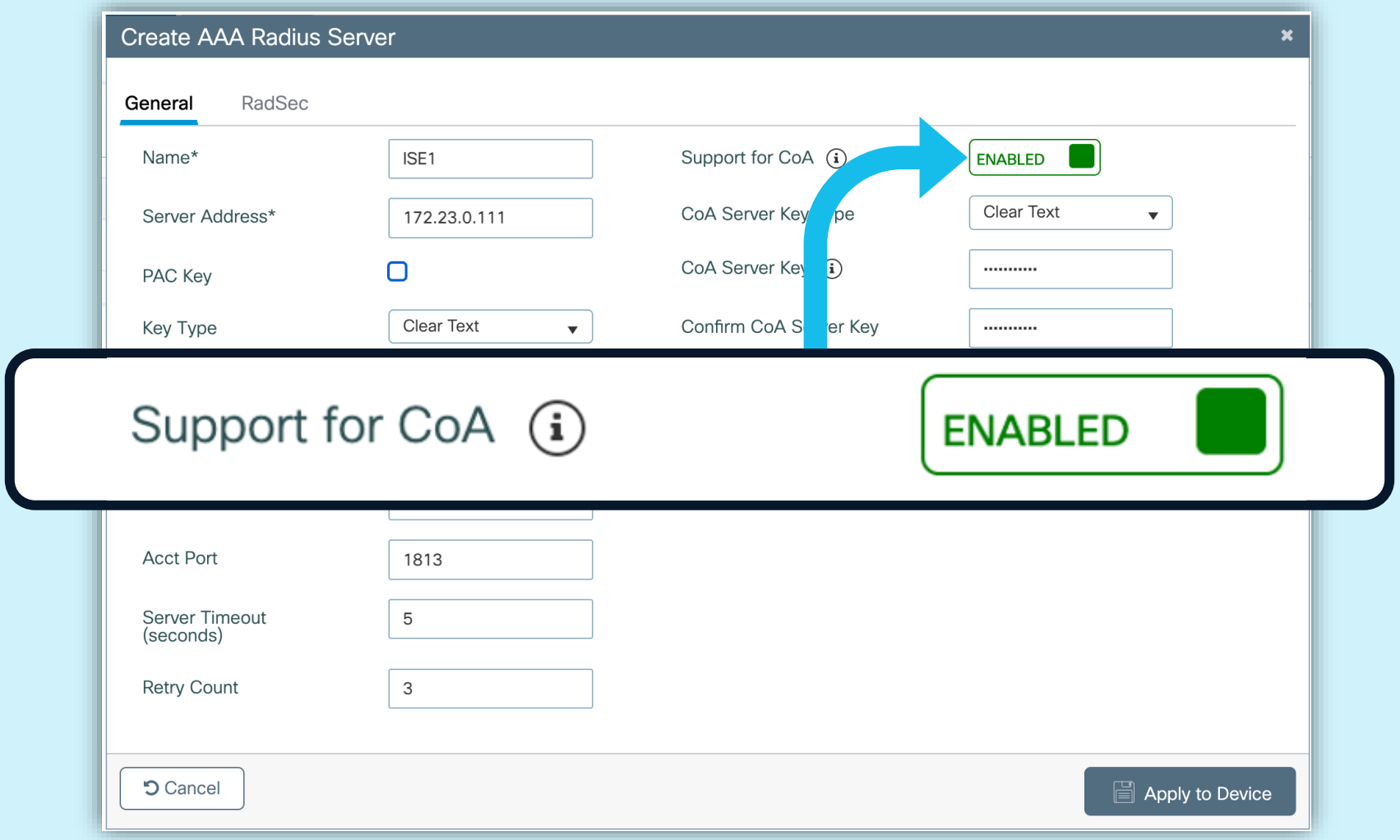


© 2025 Cisco and/or its affiliates. All rights reserved.

1 AAA Servers

Reference

Configuration > Security > AAA

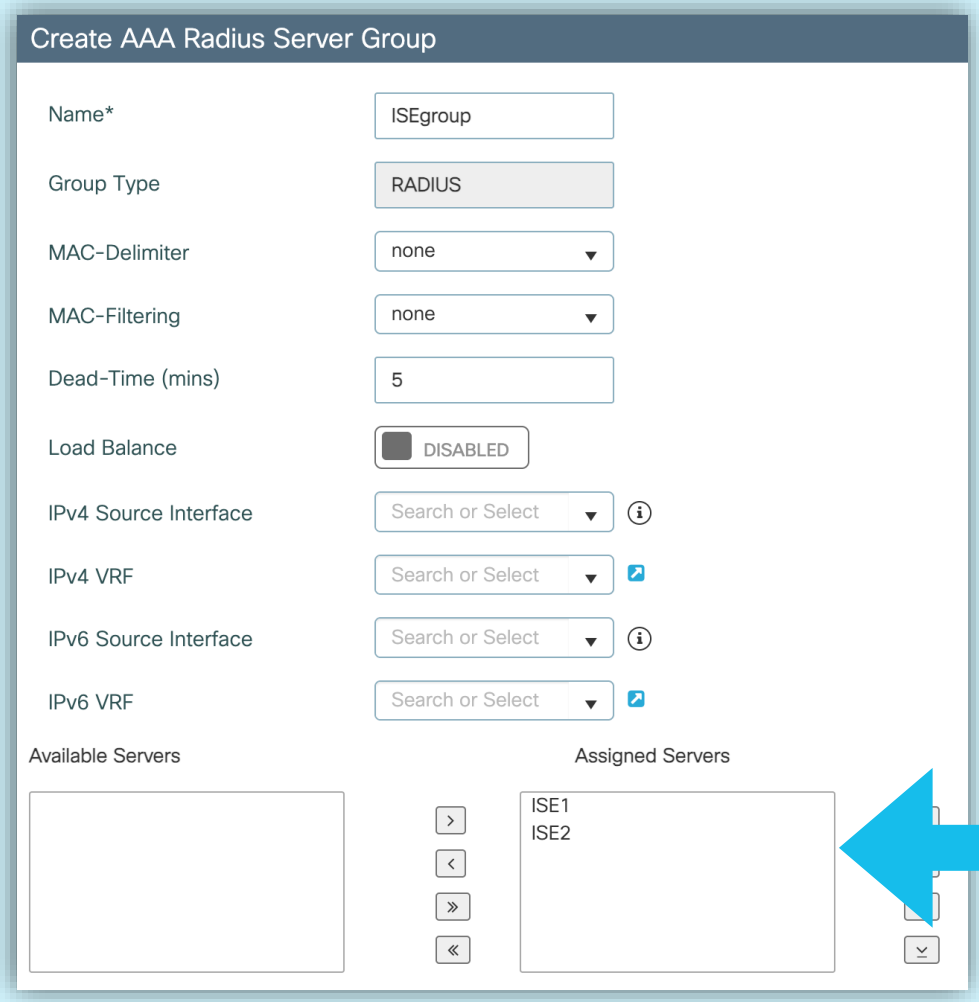


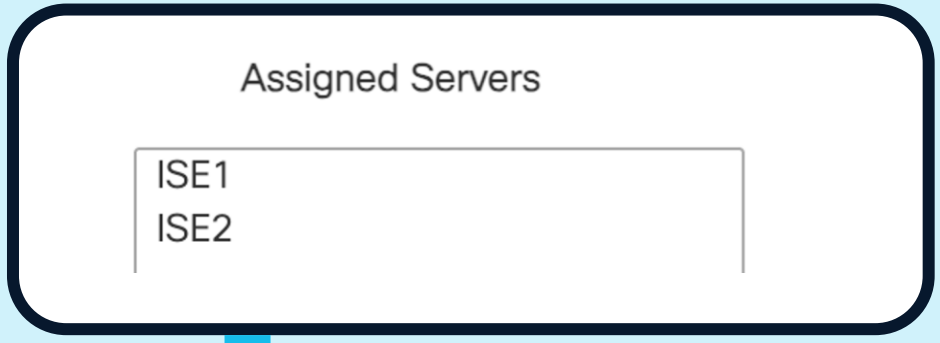
© 2025 Cisco and/or its affiliates. All rights reserved.

2 Server Group

Reference

Configuration > Security > AAA



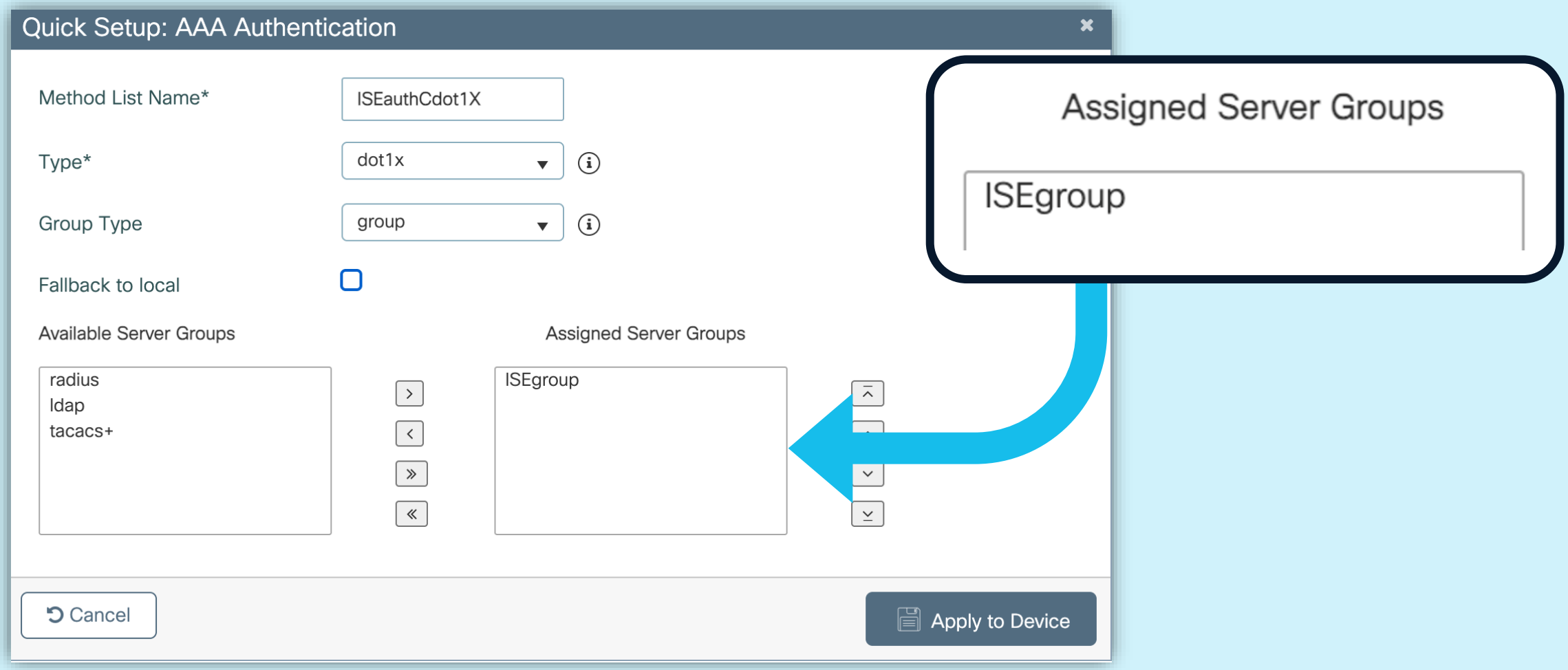


© 2025 Cisco and/or its affiliates. All rights reserved.

3a Authentication List

Reference

Configuration > Security > AAA

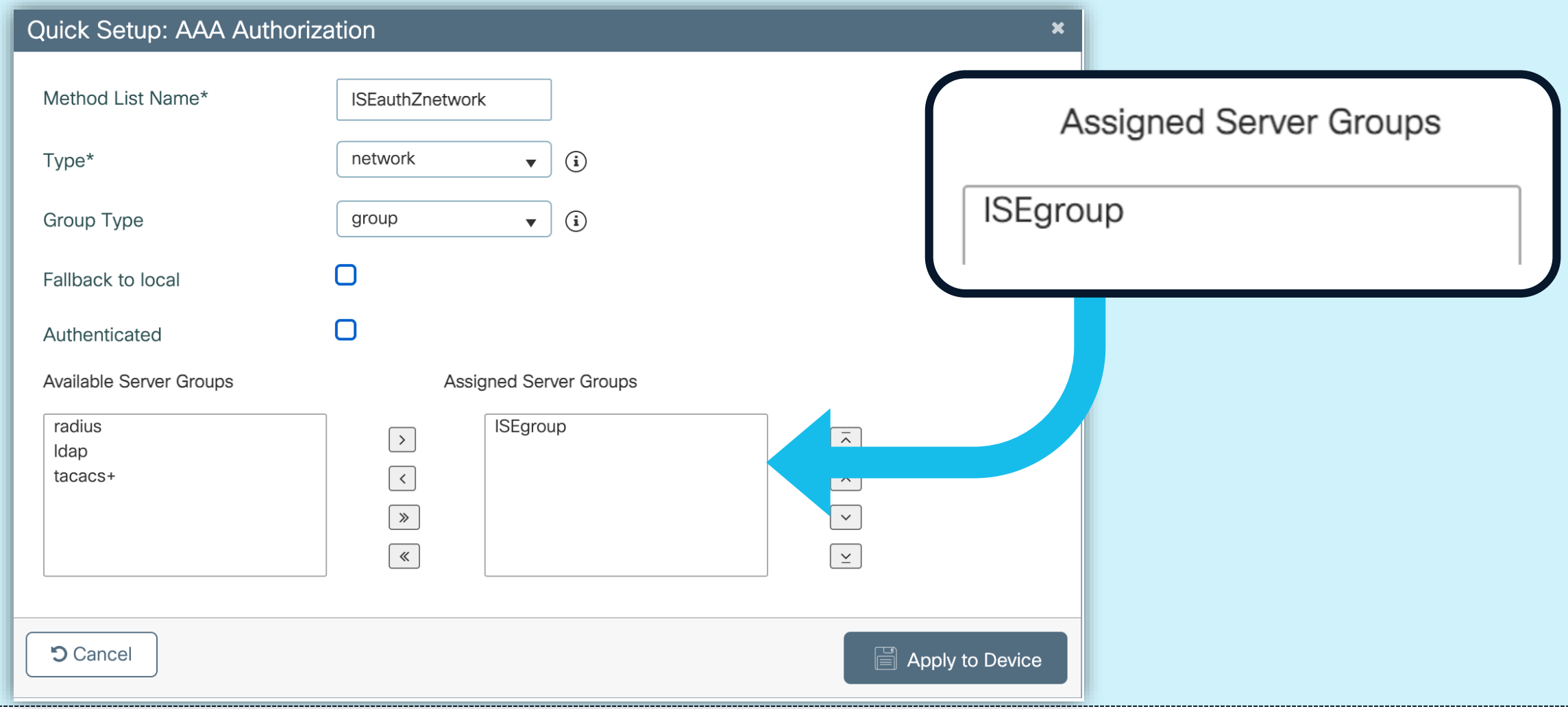


© 2025 Cisco and/or its affiliates. All rights reserved.

3b Authorization List

Reference

Configuration > Security > AAA

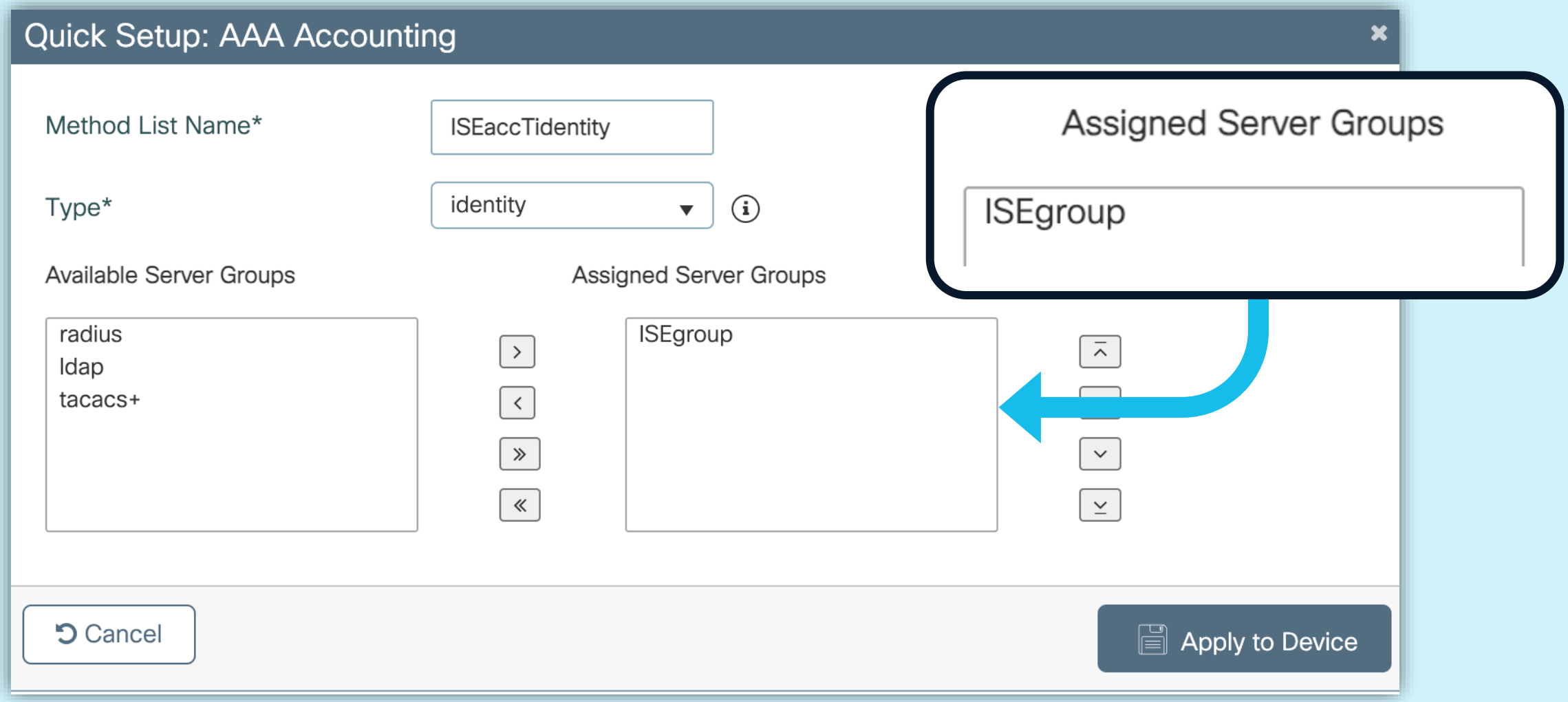


© 2025 Cisco and/or its affiliates. All rights reserved.

3c Accounting List

Reference

Configuration > Security > AAA

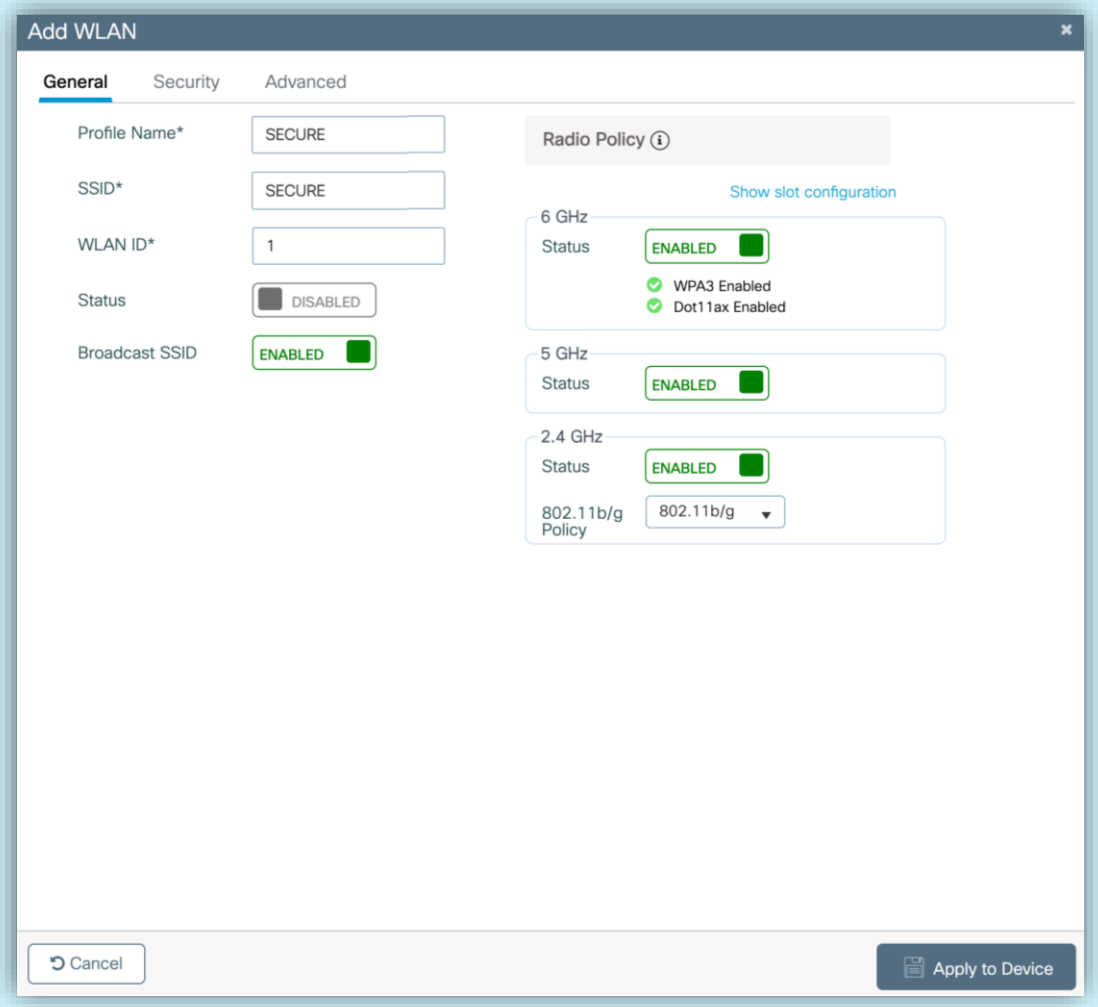


© 2025 Cisco and/or its affiliates. All rights reserved.

6 WLAN Profile – 802.1X

Reference

Configuration > Tags & Profiles > WLANS

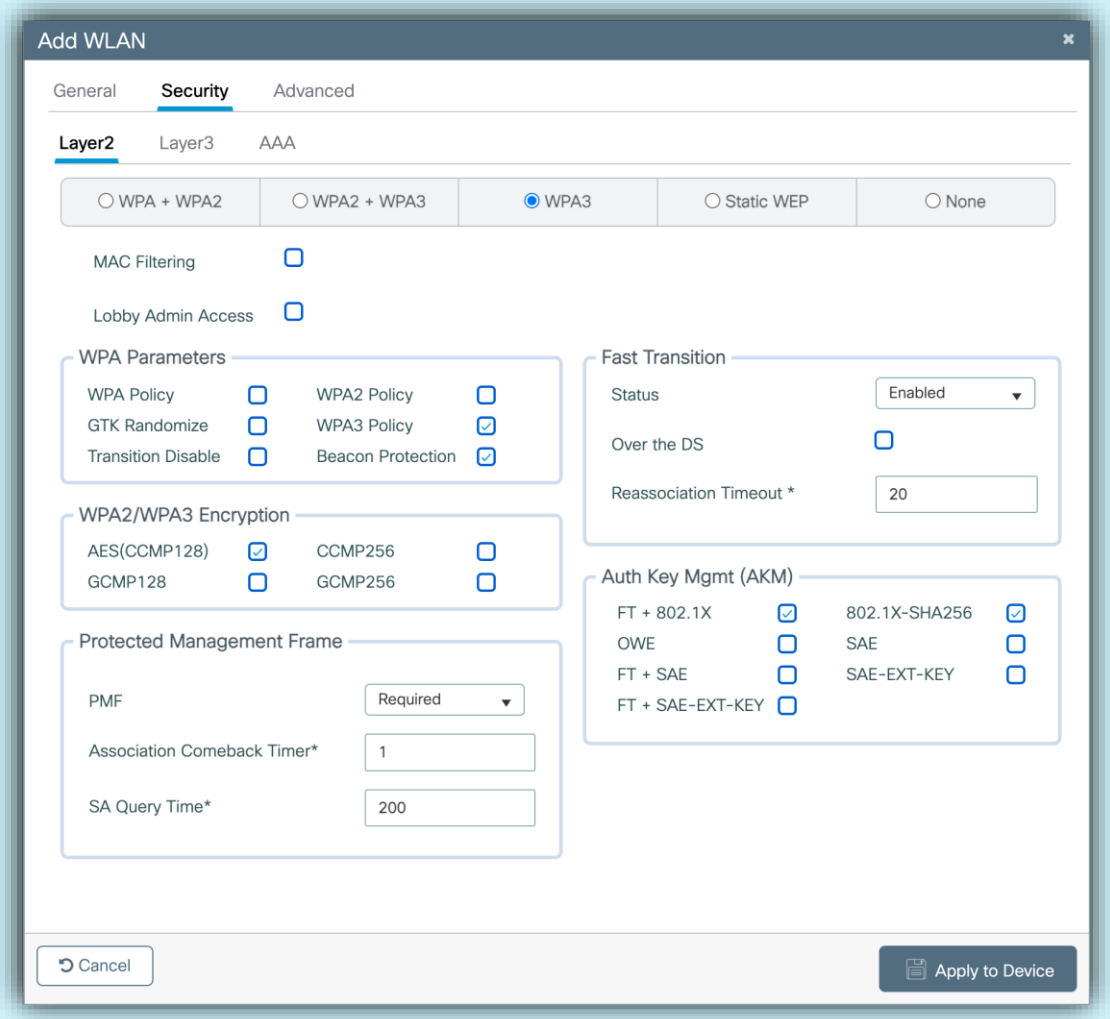


© 2025 Cisco and/or its affiliates. All rights reserved.

6 WLAN Profile – 802.1X

Reference

Configuration > Tags & Profiles > WLANS

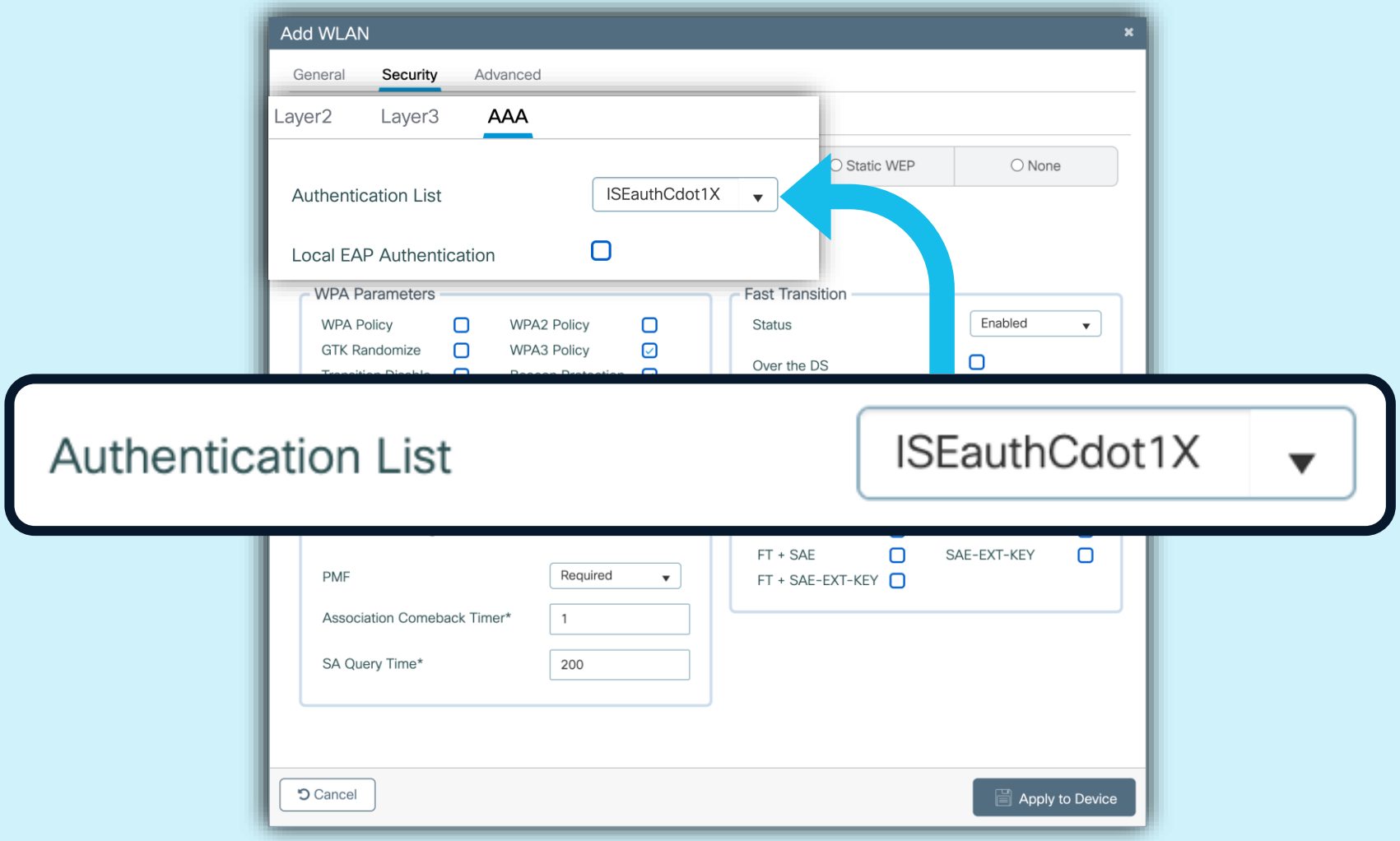


© 2025 Cisco and/or its affiliates. All rights reserved.

6 WLAN Profile – 802.1X

Reference

Configuration > Tags & Profiles > WLANS



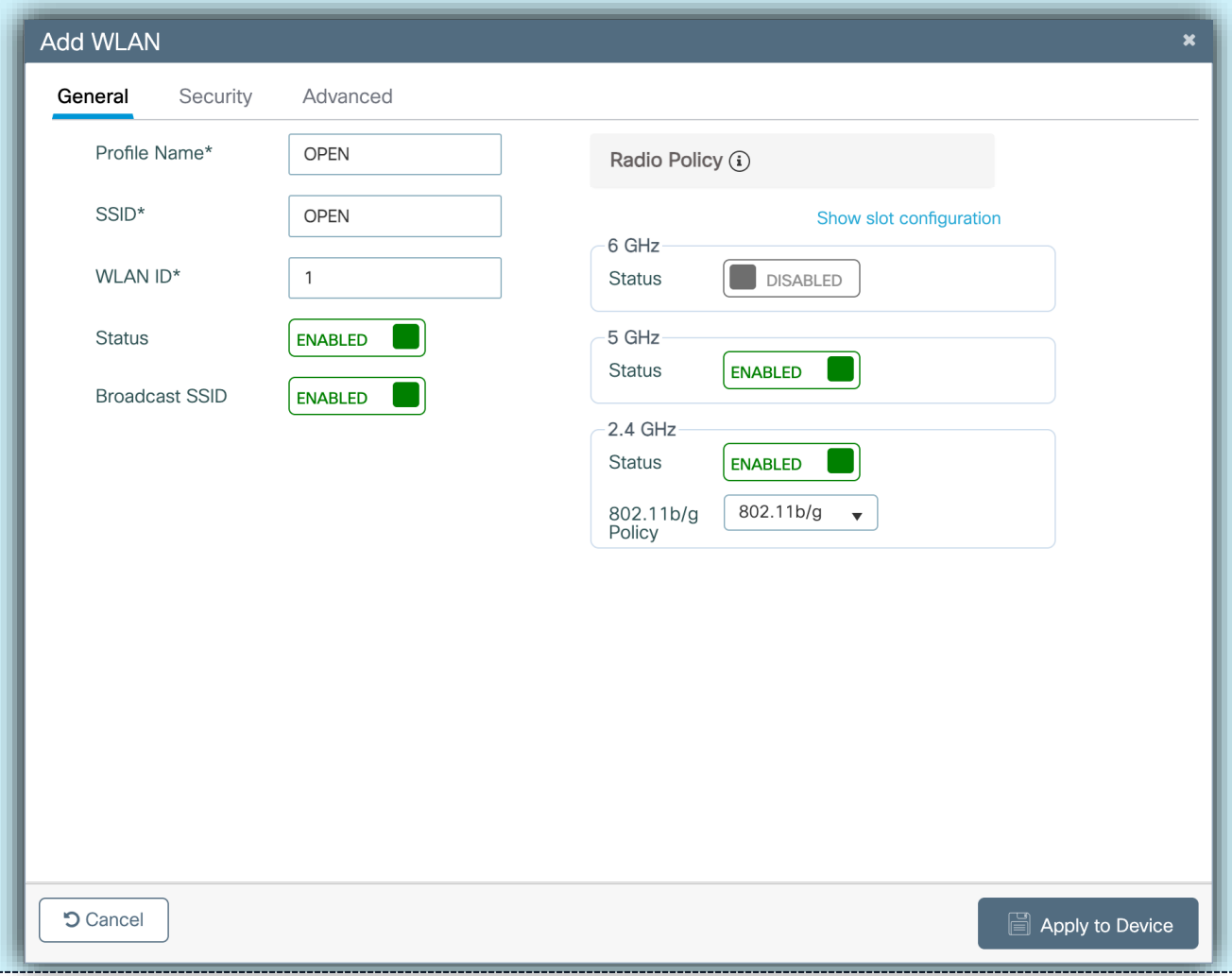
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

6 WLAN Profile – MAC Auth

Reference

Configuration > Tags & Profiles > WLANS

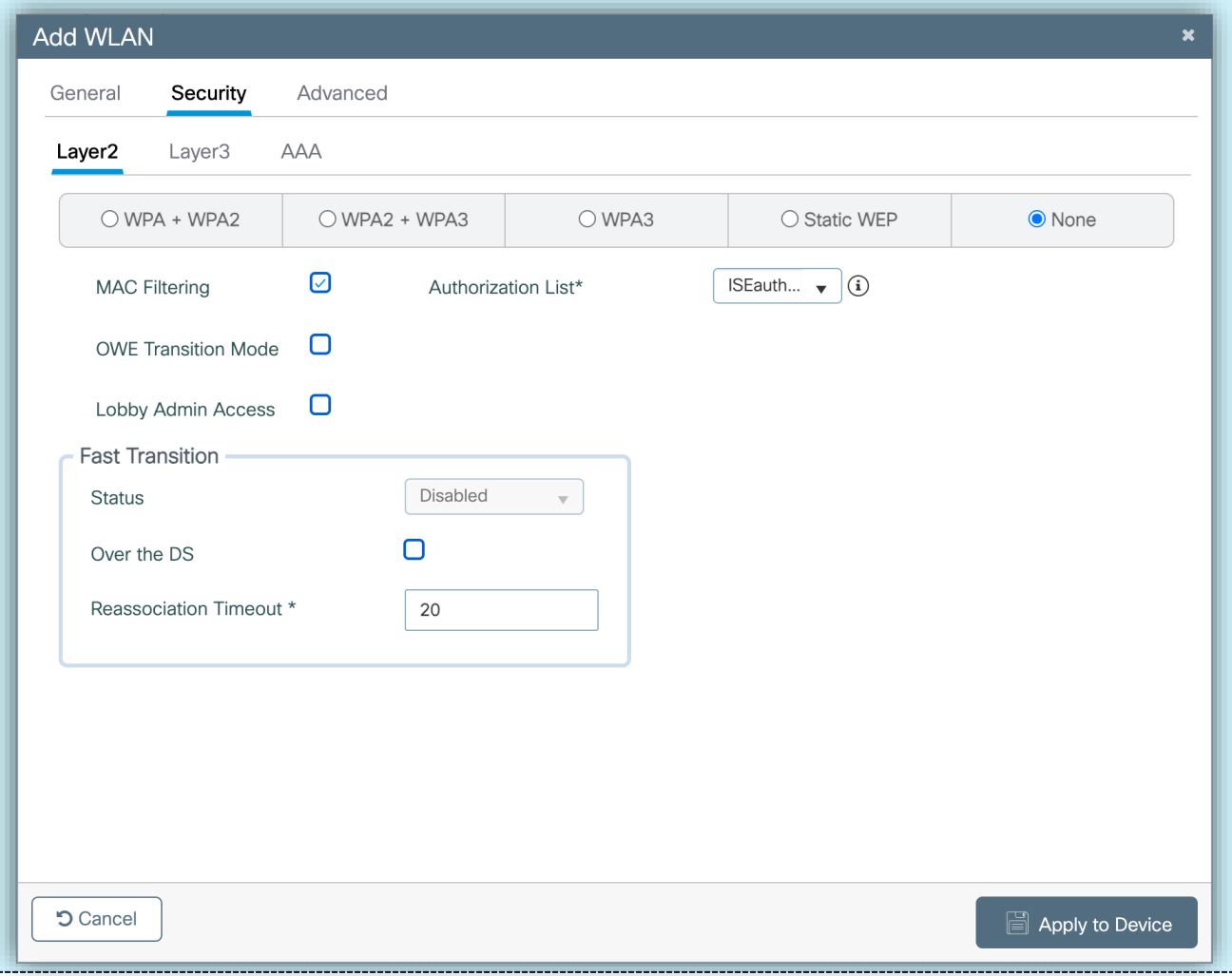


© 2025 Cisco and/or its affiliates. All rights reserved.

6 WLAN Profile – MAC Auth

Reference

Configuration > Tags & Profiles > WLANS



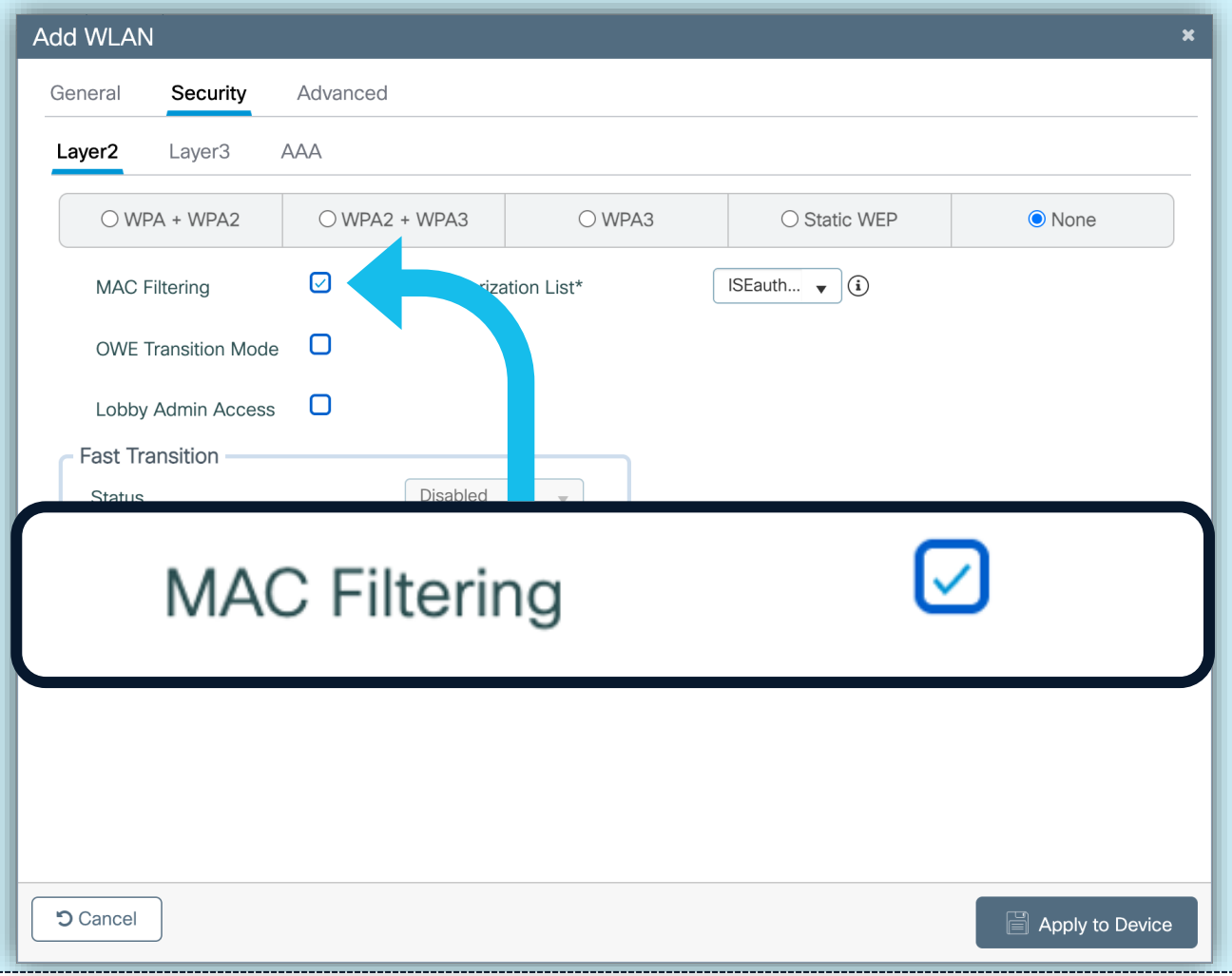
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

6 WLAN Profile – MAC Auth

Reference

Configuration > Tags & Profiles > WLANS



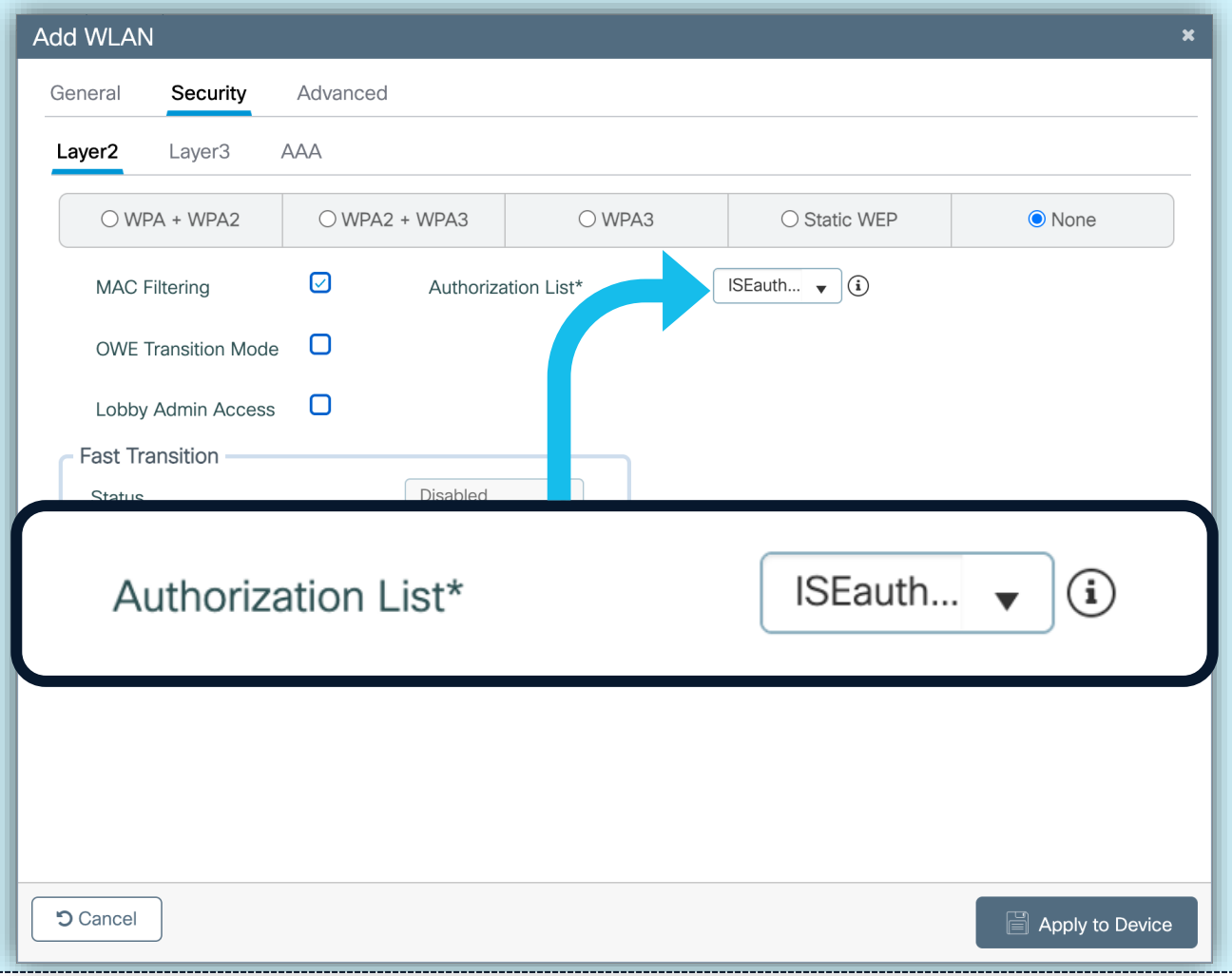
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

6 WLAN Profile – MAC Auth

Reference

Configuration > Tags & Profiles > WLANS

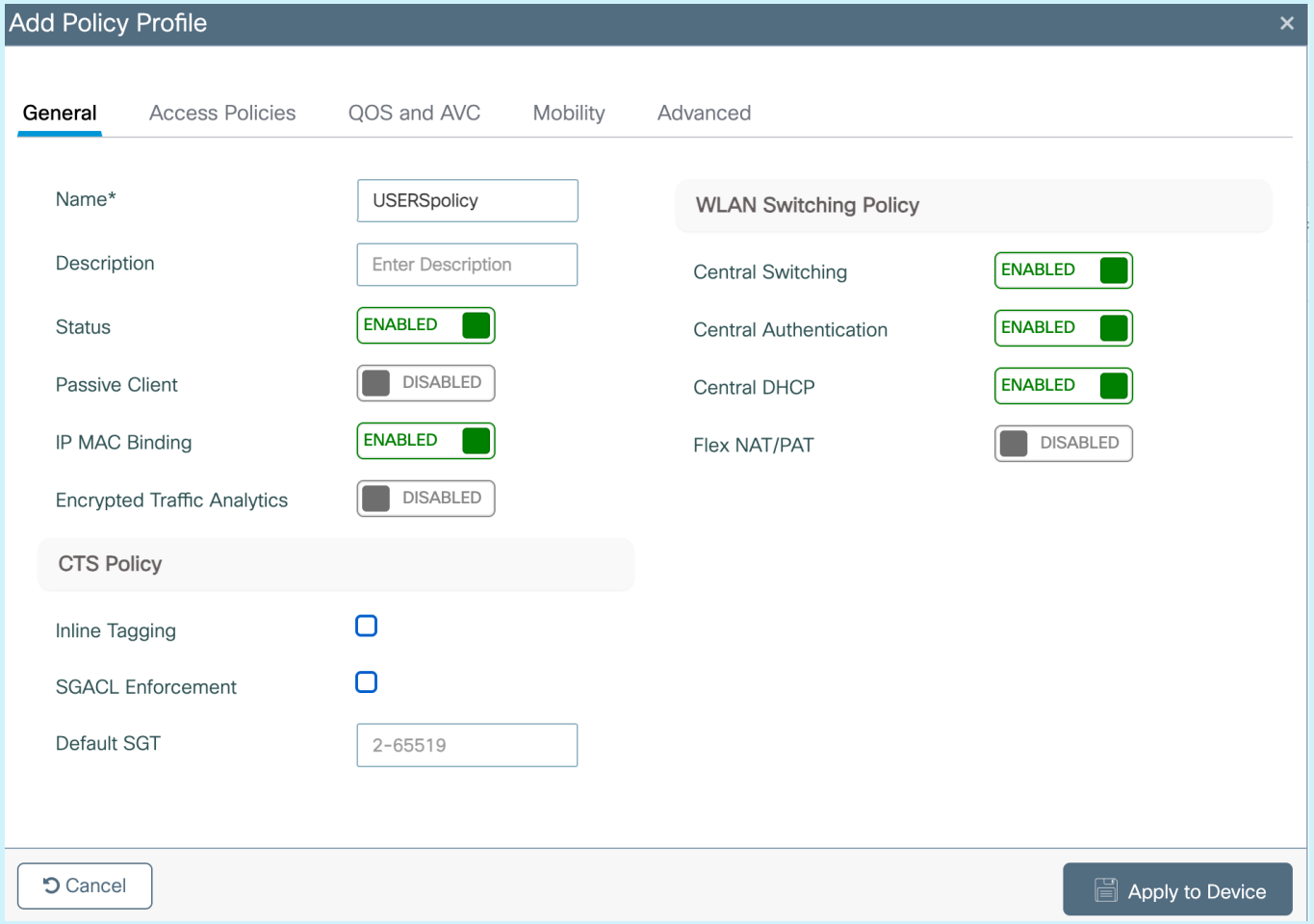


© 2025 Cisco and/or its affiliates. All rights reserved.

7 Policy Profile

Reference

Configuration > Tags & Profiles > Policy

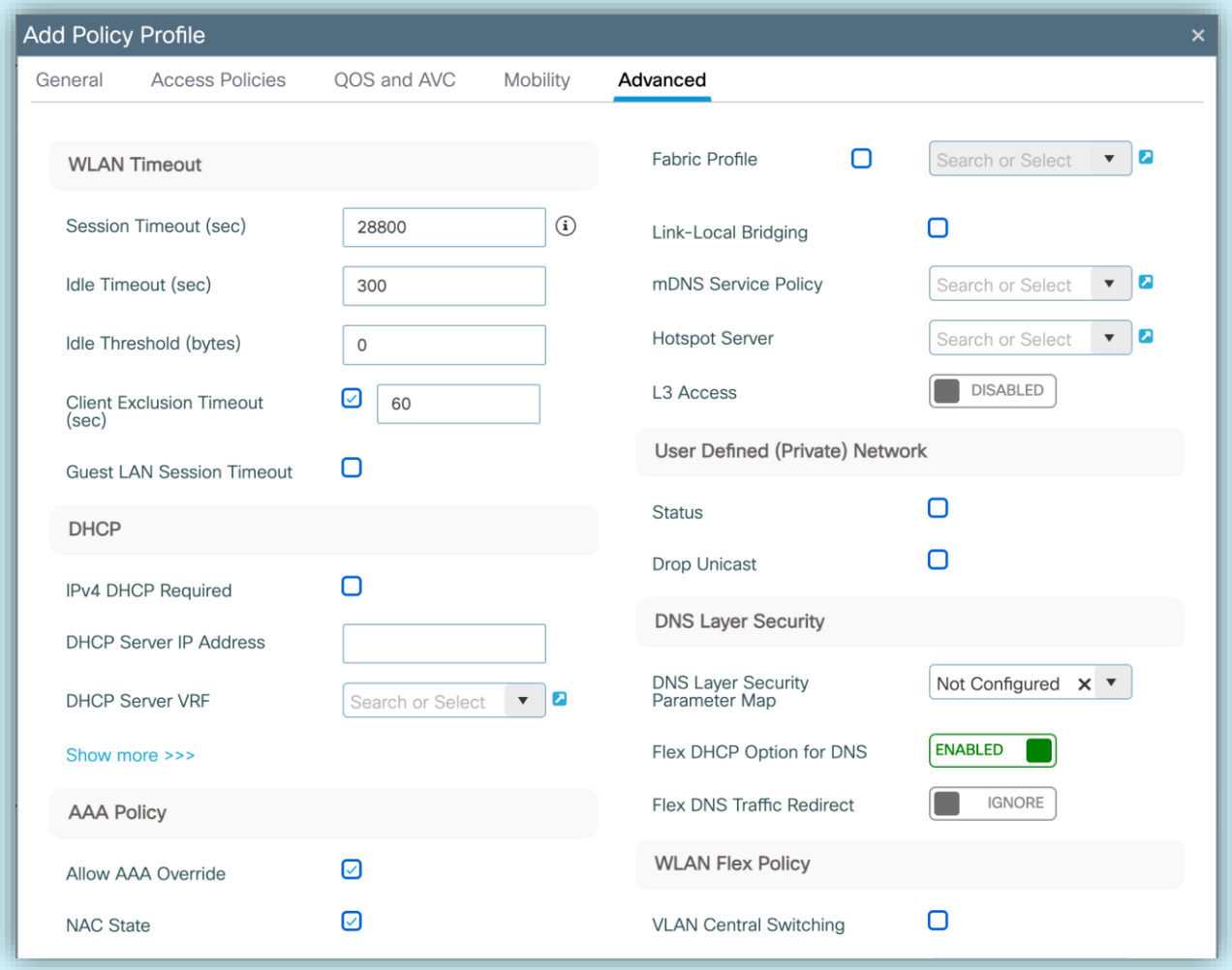


© 2025 Cisco and/or its affiliates. All rights reserved.

7 Policy Profile

Reference

Configuration > Tags & Profiles > Policy



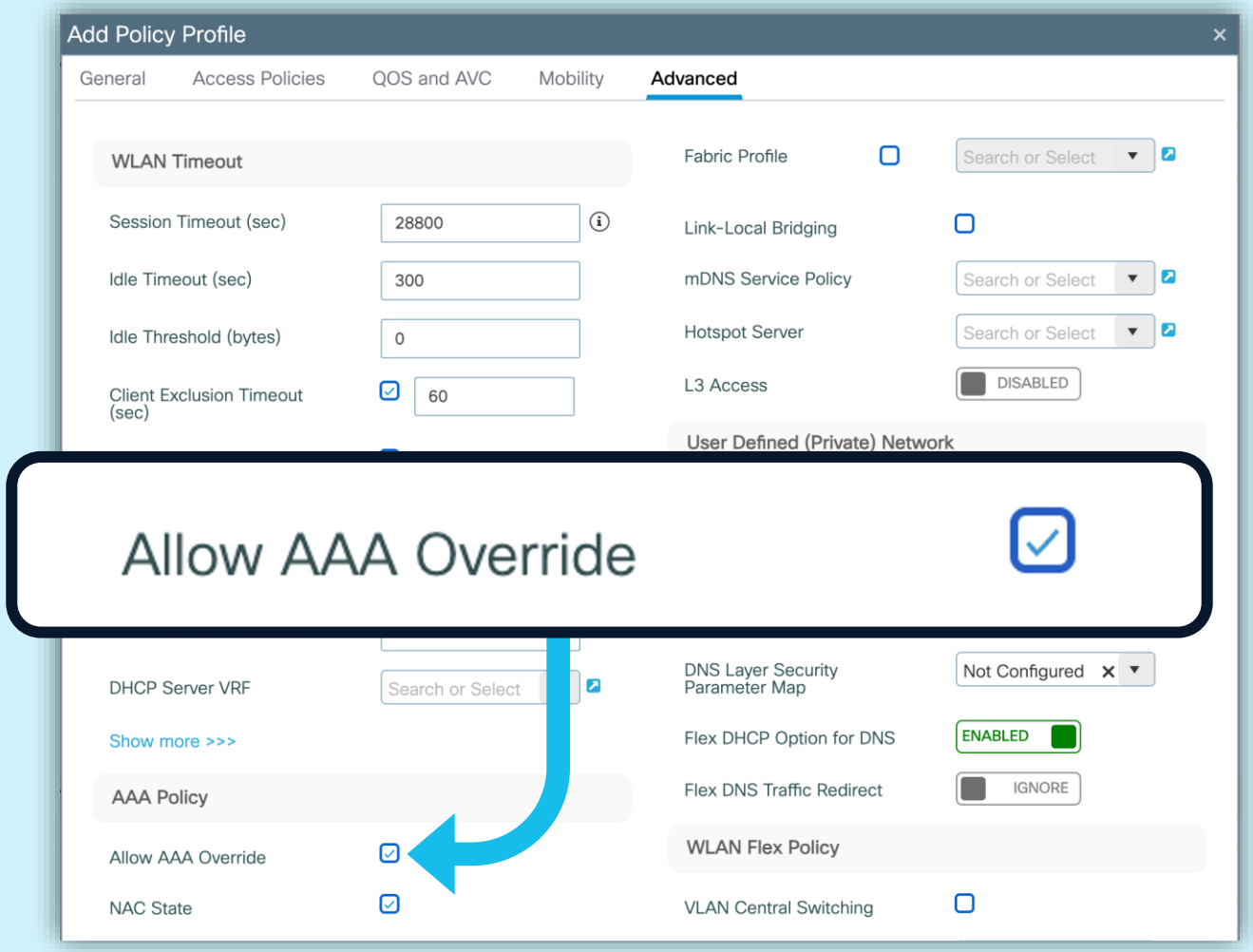
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

7 Policy Profile

Reference

Configuration > Tags & Profiles > Policy

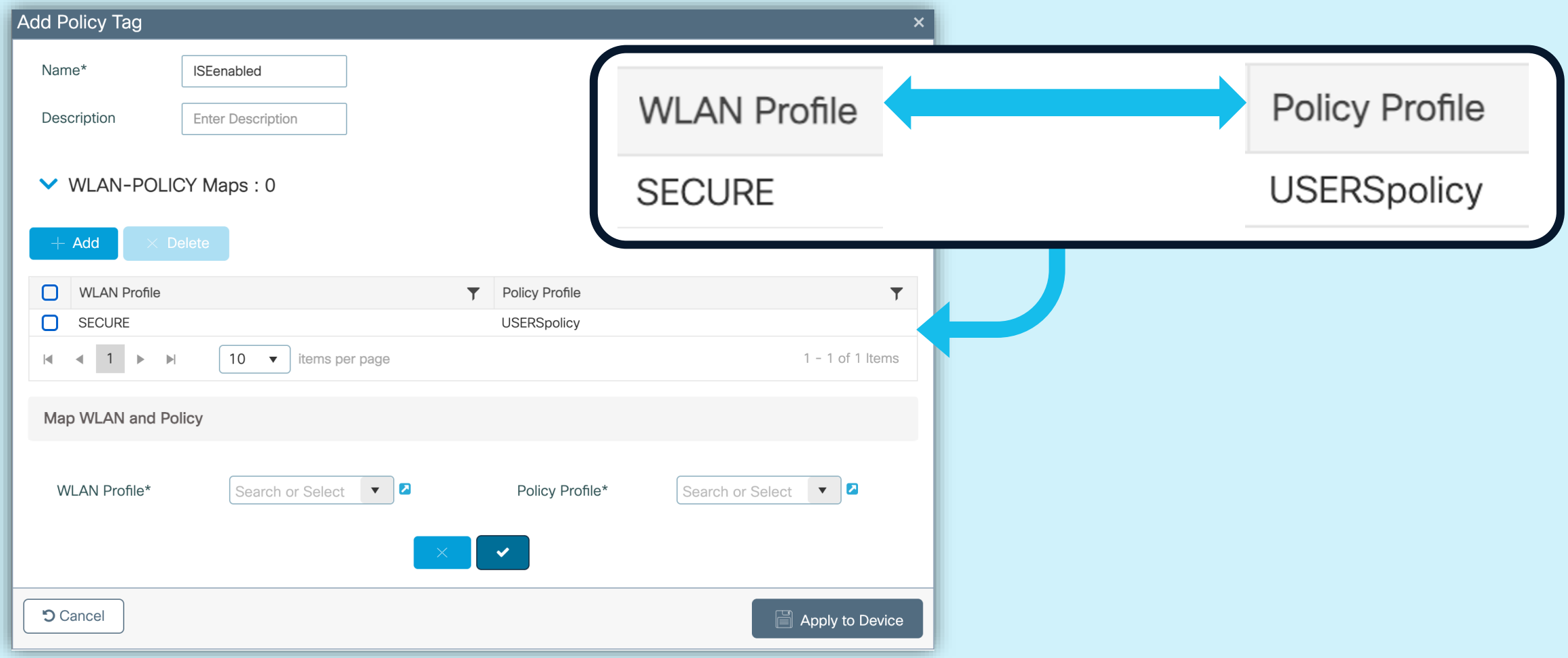


© 2025 Cisco and/or its affiliates. All rights reserved.

8 Policy Tag

Reference

Configuration > Tags & Profiles > Tags

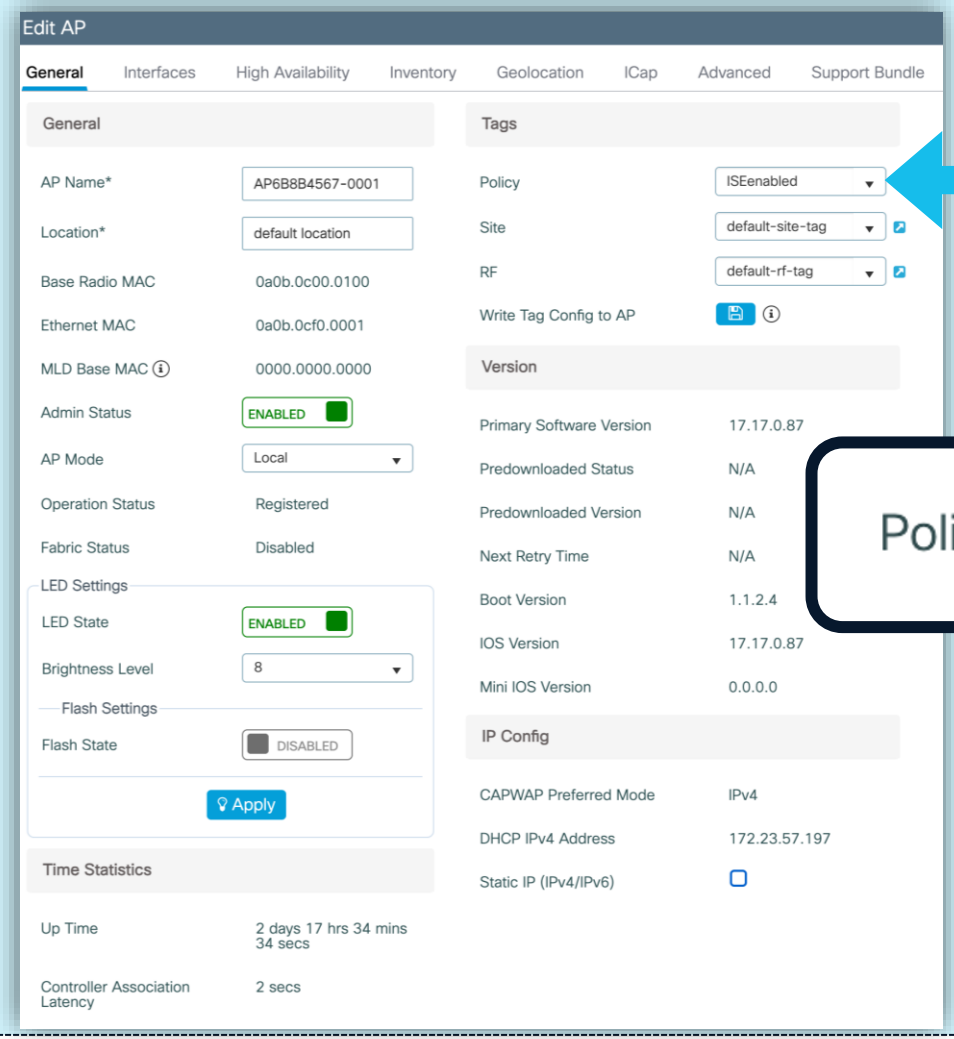


© 2025 Cisco and/or its affiliates. All rights reserved.

9 AP

Reference

Configuration > Wireless > Access Points



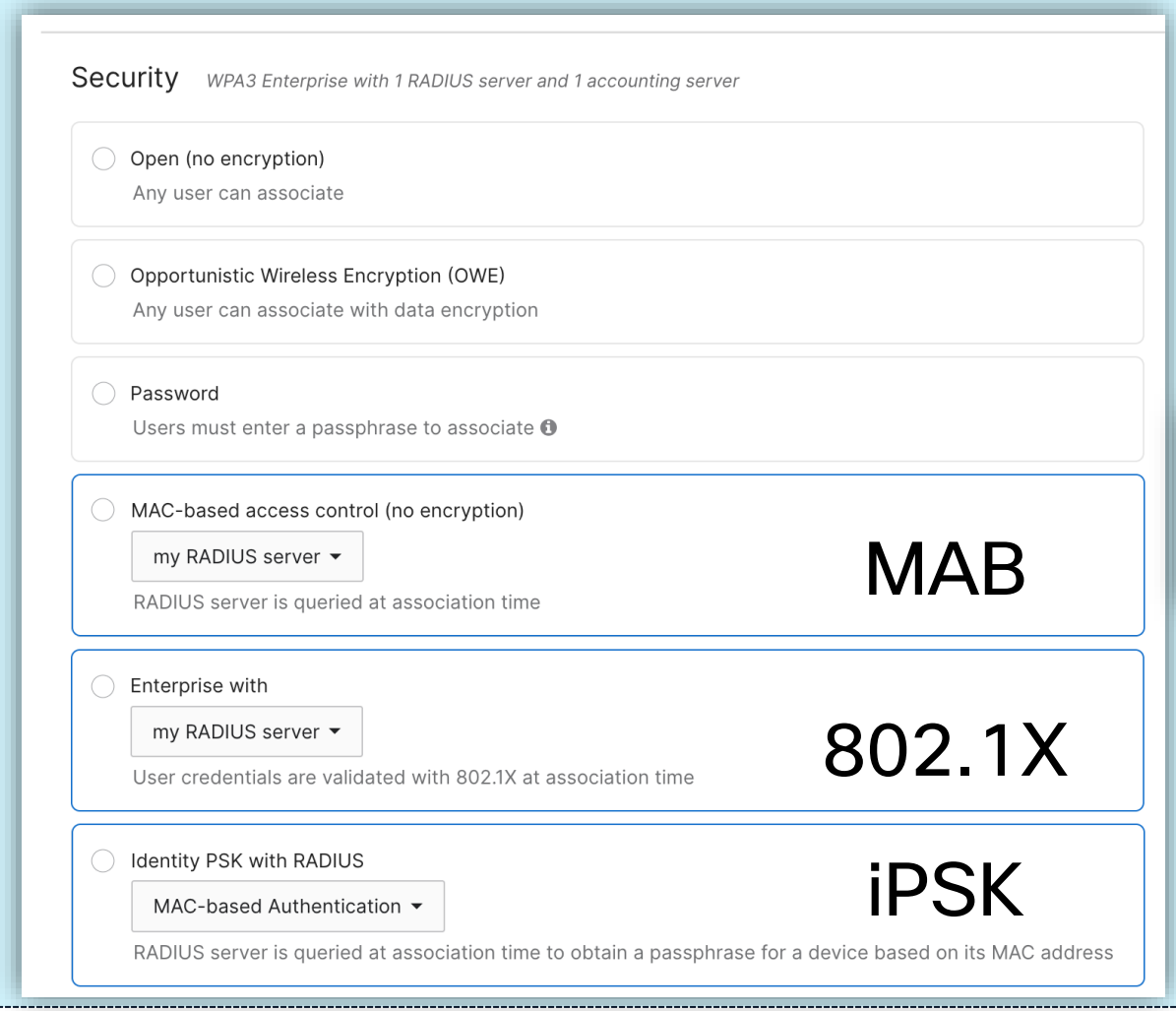
© 2025 Cisco and/or its affiliates. All rights reserved.

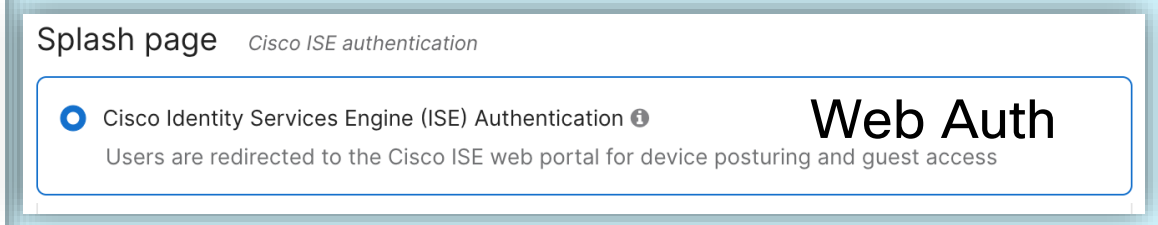
Meraki Wireless Base Configuration for ISE

cisco Live !

Meraki Wireless Configuration for ISE

Wireless > Configure > Access Control

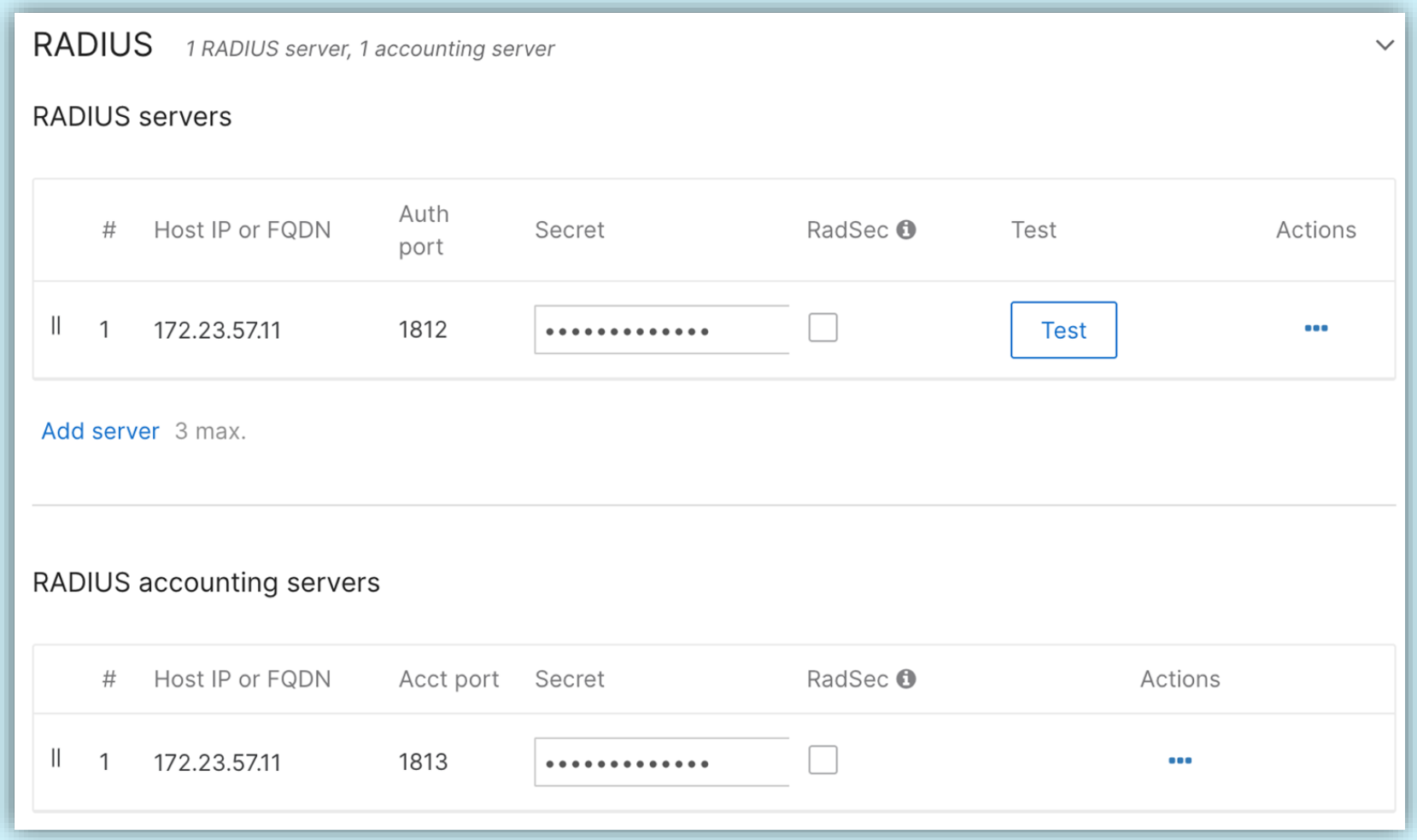




© 2025 Cisco and/or its affiliates. All rights reserved.

Meraki Wireless Configuration for ISE

Wireless > Configure > Access Control



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

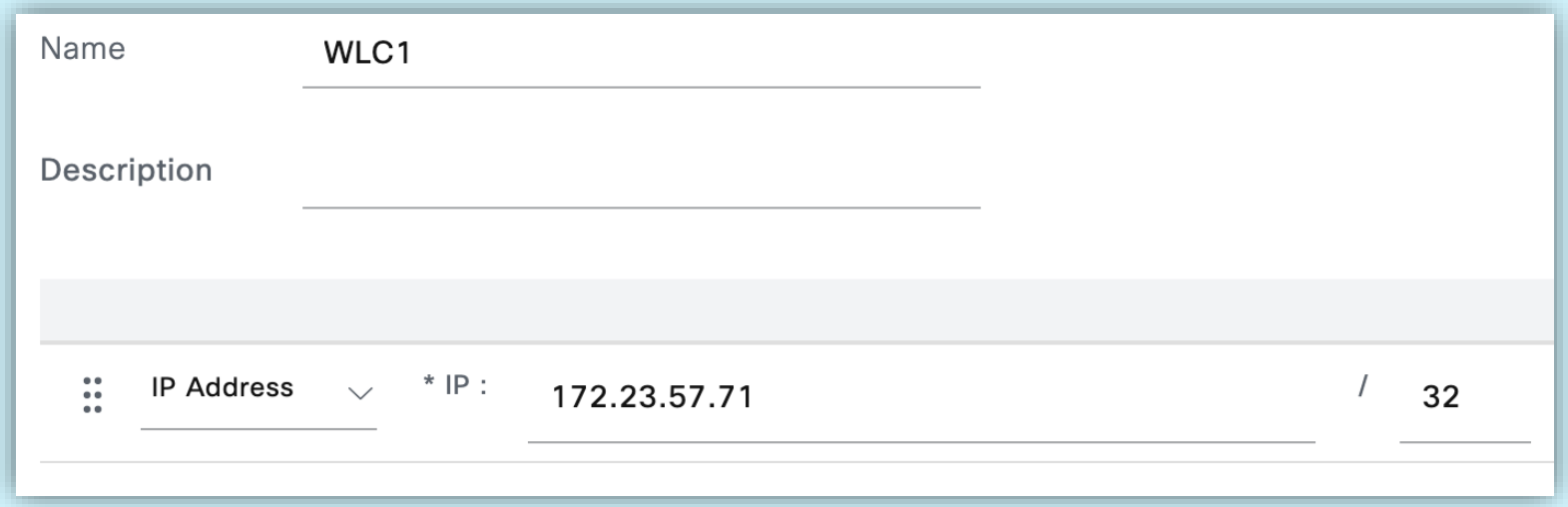
Adding Wireless Network Devices to ISE

cisco Live !

ISE Configuration for Wireless - NAD

Administration > Network Resources > Network Devices

Catalyst 9800



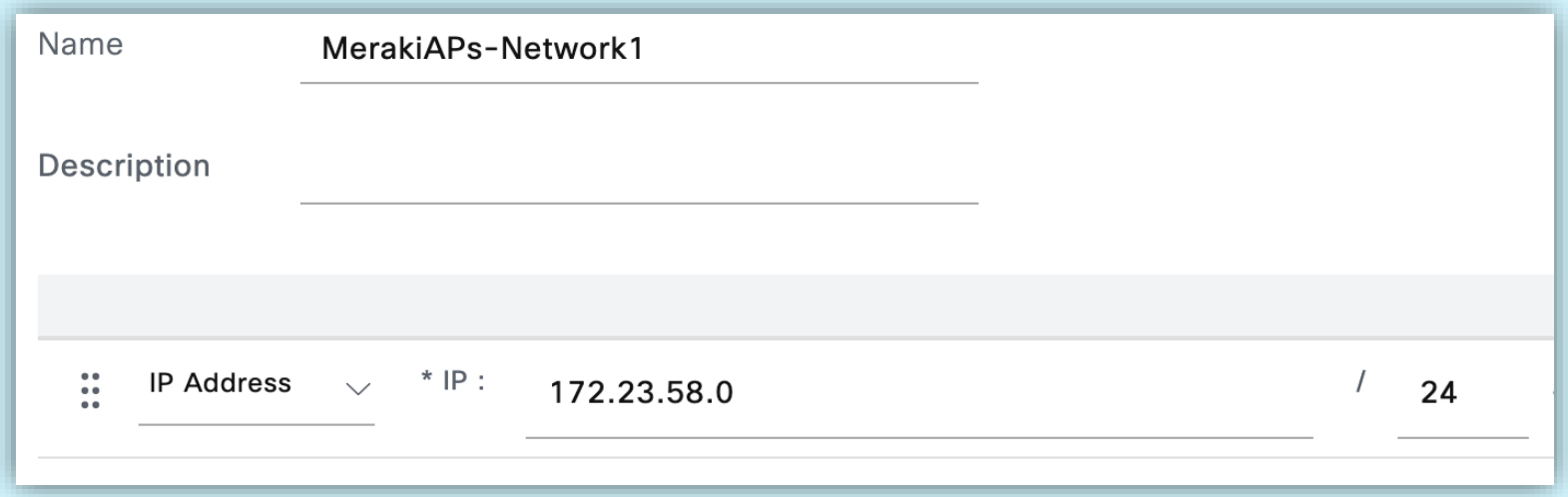
© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Configuration for Wireless - NAD

Administration > Network Resources > Network Devices

Catalyst 9800 - Flexconnect

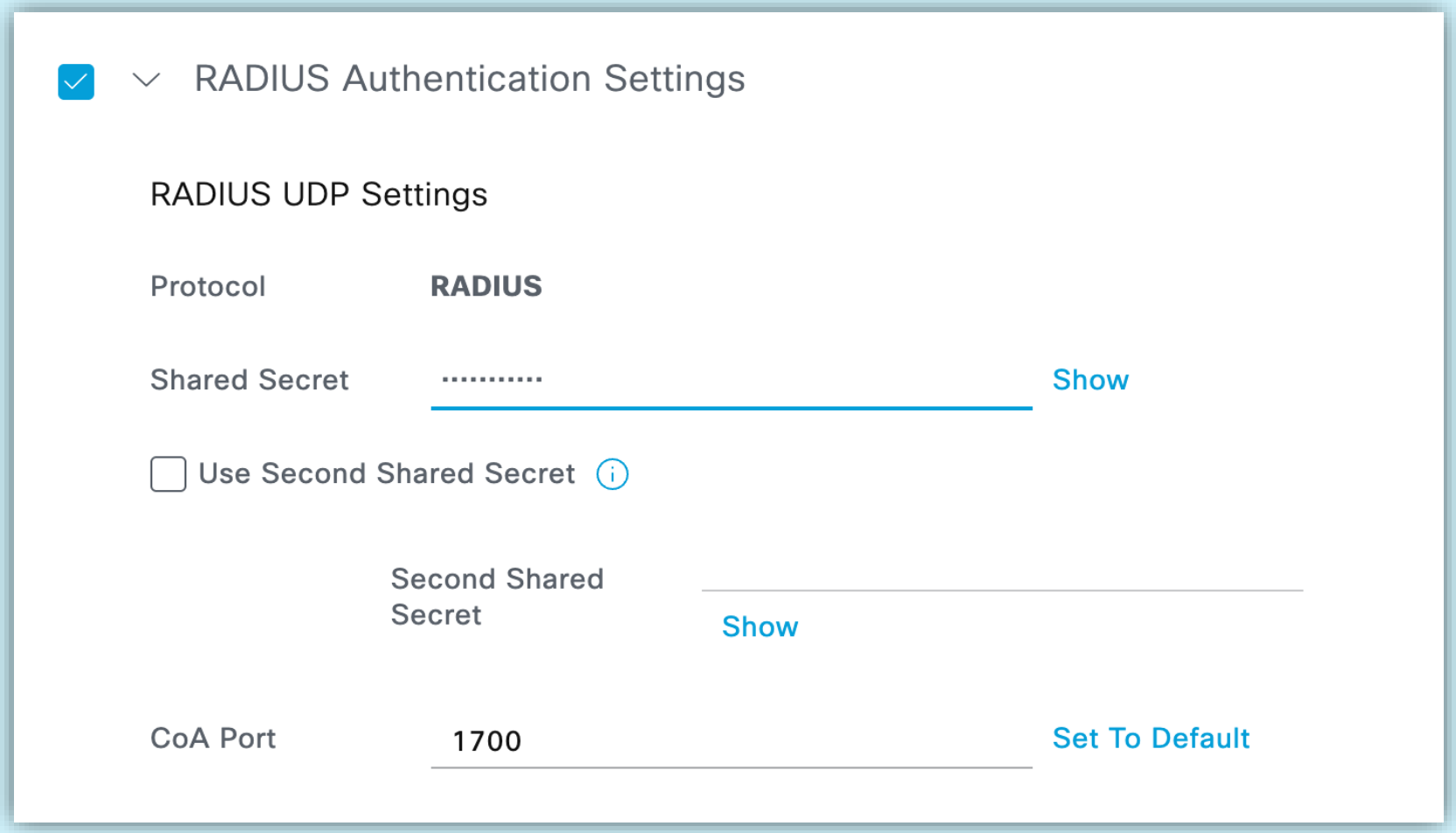
Meraki



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

ISE Configuration for Wireless - NAD

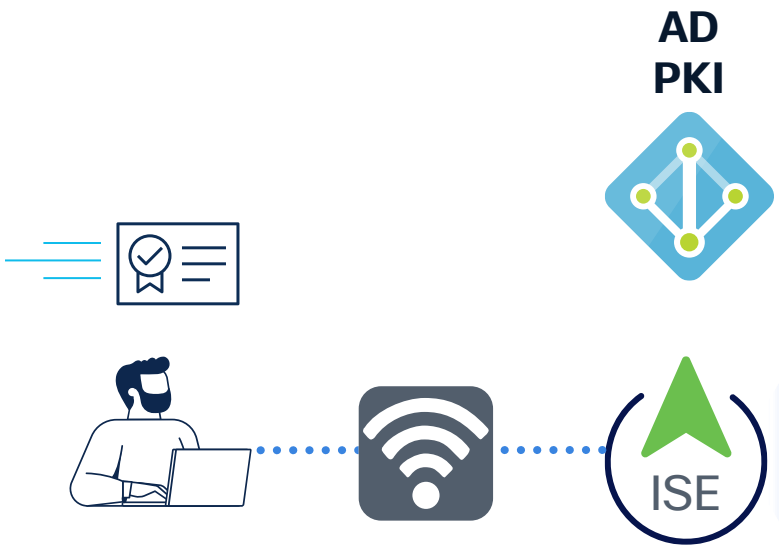
Administration > Network Resources > Network Devices



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

Identity and Context

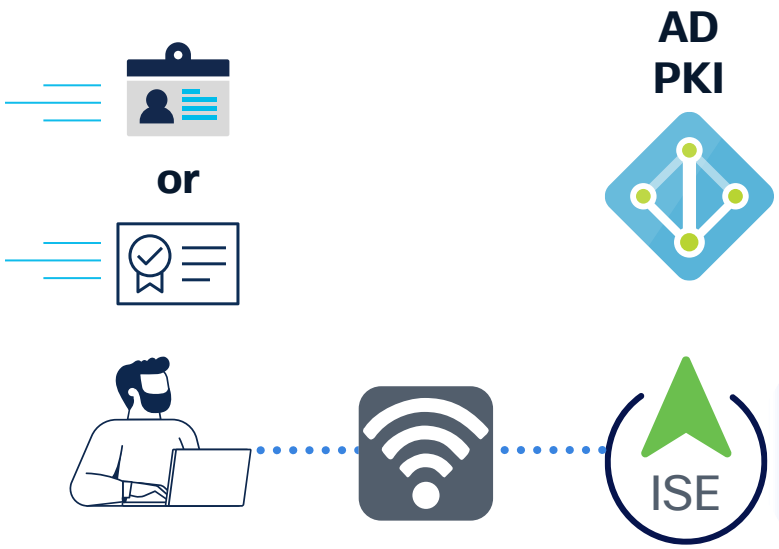
Certificate Attributes



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

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

Active Directory Attributes

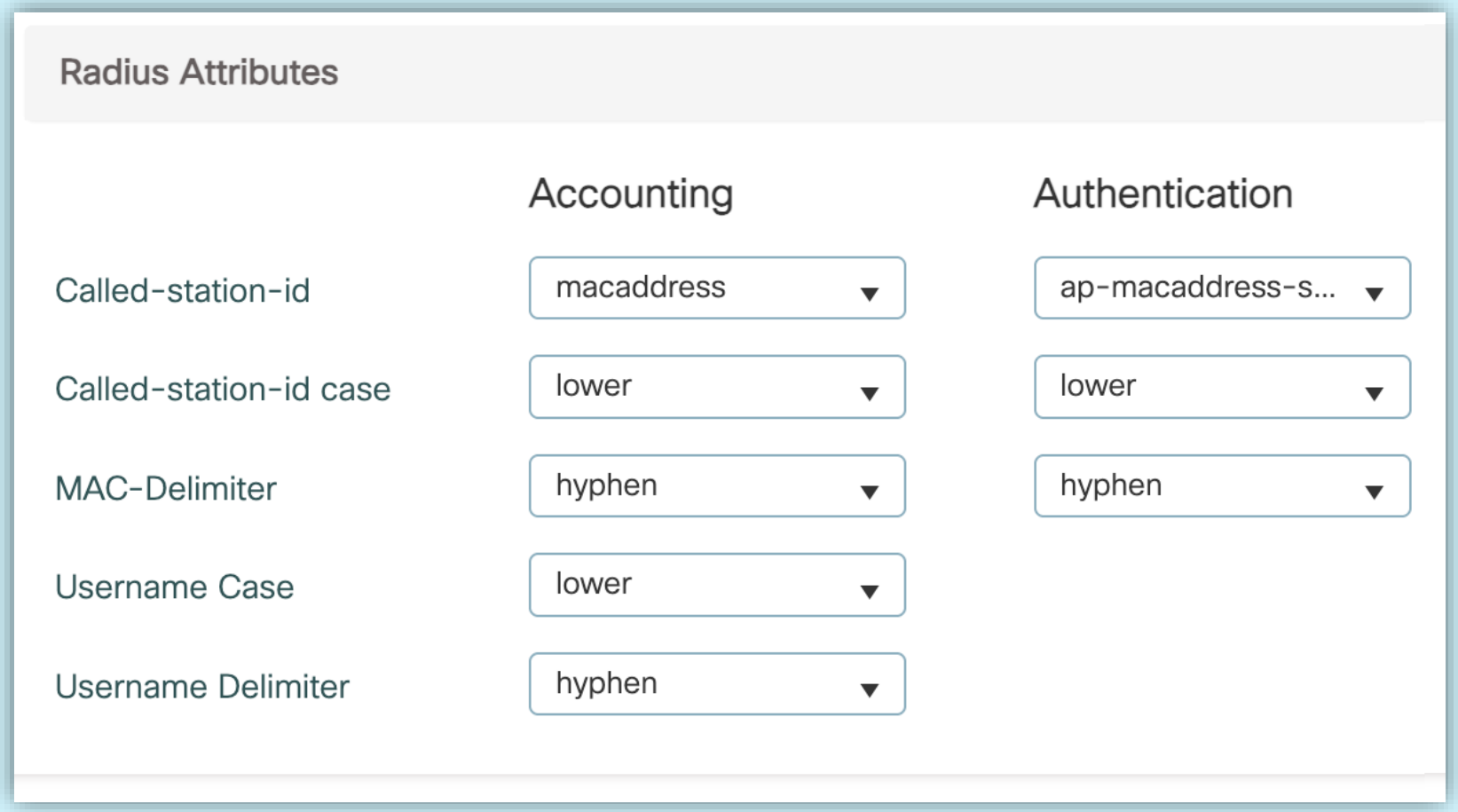


Dictionary	Attribute	ID	Info
AD	accountExpires		
AD	adminCount		
AD	badPasswordTime		
AD	badPwdCount		
AD	cn		
AD	codePage		
AD	countryCode		
AD	dSCorePropagationData		
AD	displayName		
AD	distinguishedName		
AD	givenName		
AD	instanceType		
AD	lastLogoff		

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

Catalyst 9800 Advanced RADIUS Attributes

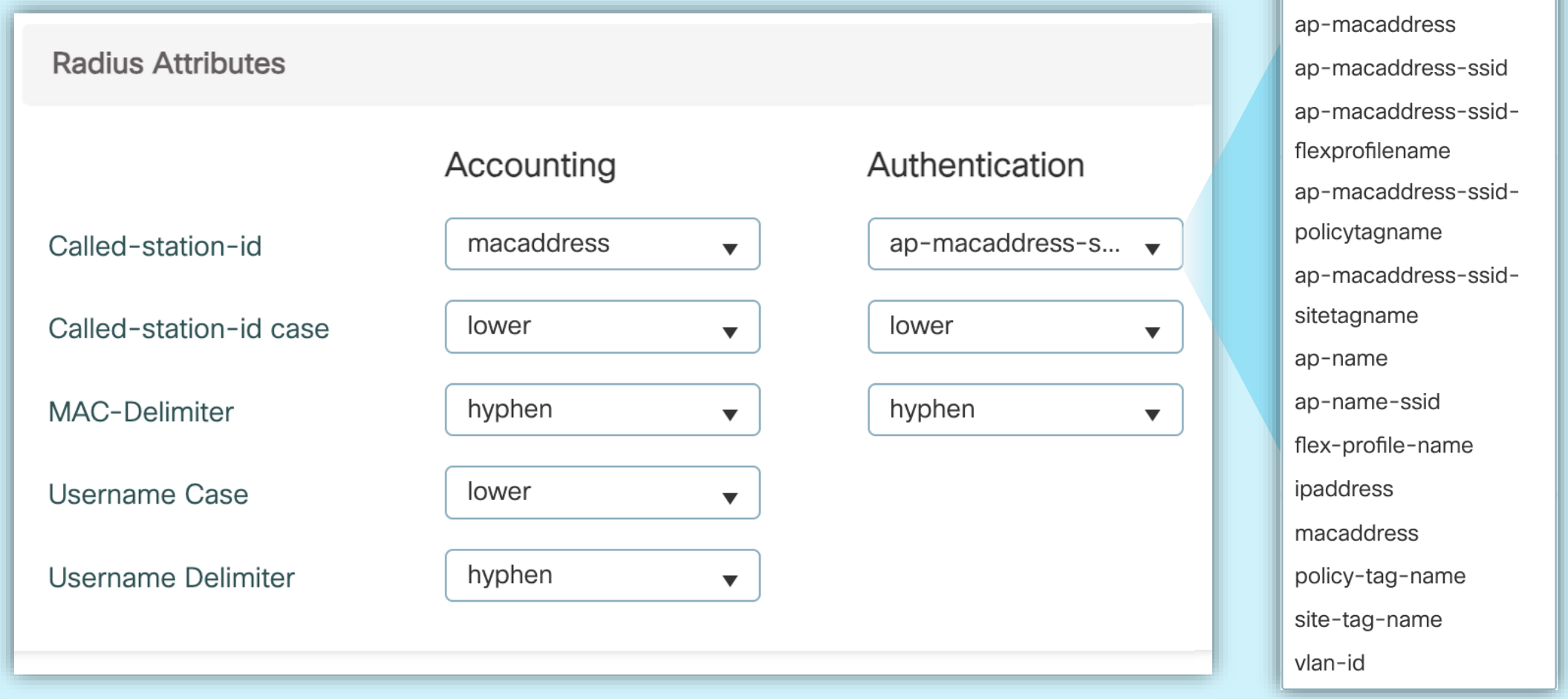
Configuration > Security > AAA



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

Catalyst 9800 Advanced RADIUS Attributes

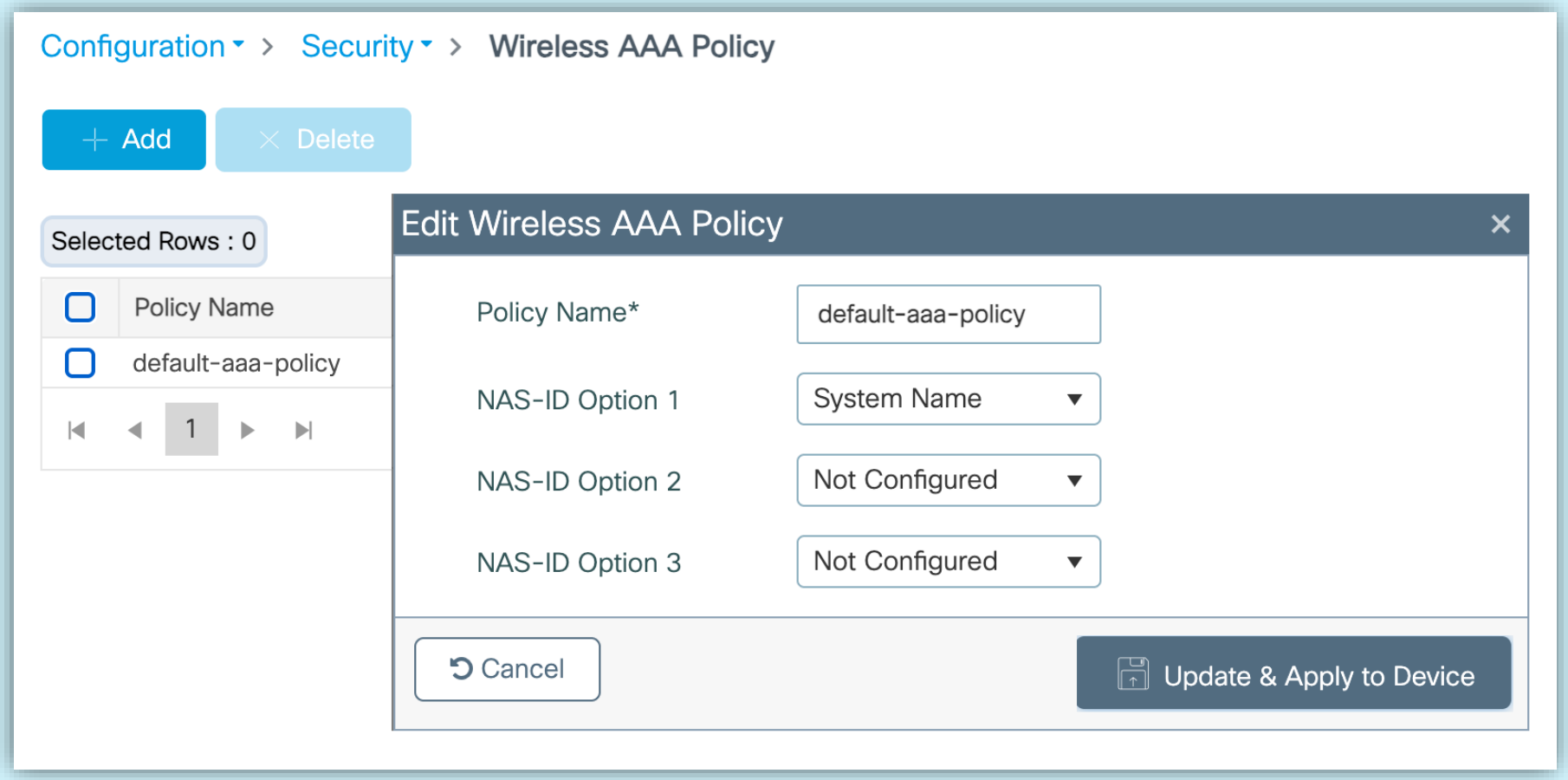
Configuration > Security > AAA



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

Catalyst 9800 Advanced RADIUS Attributes

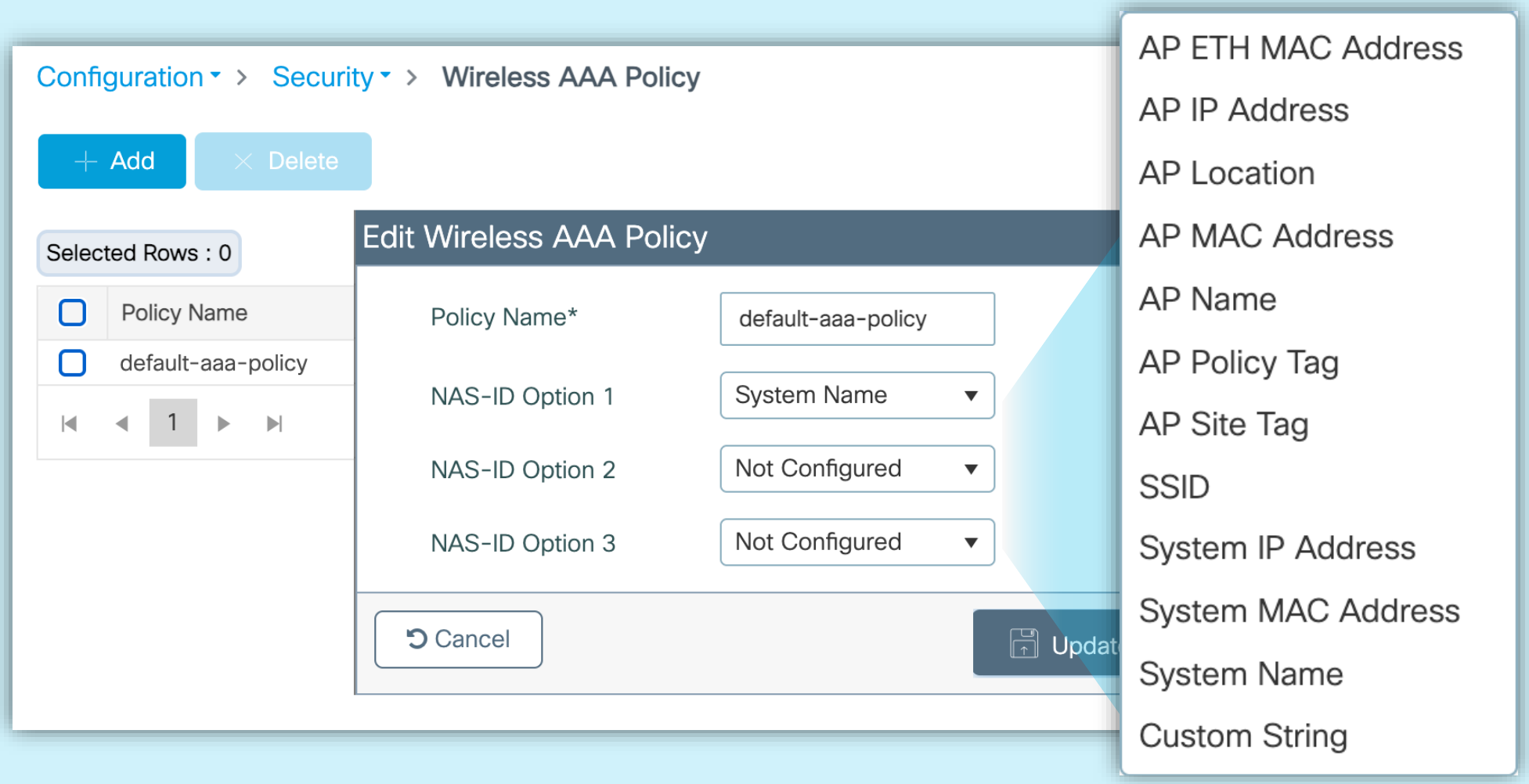
Configuration > Security > Wireless AAA Policy



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

Catalyst 9800 Advanced RADIUS Attributes

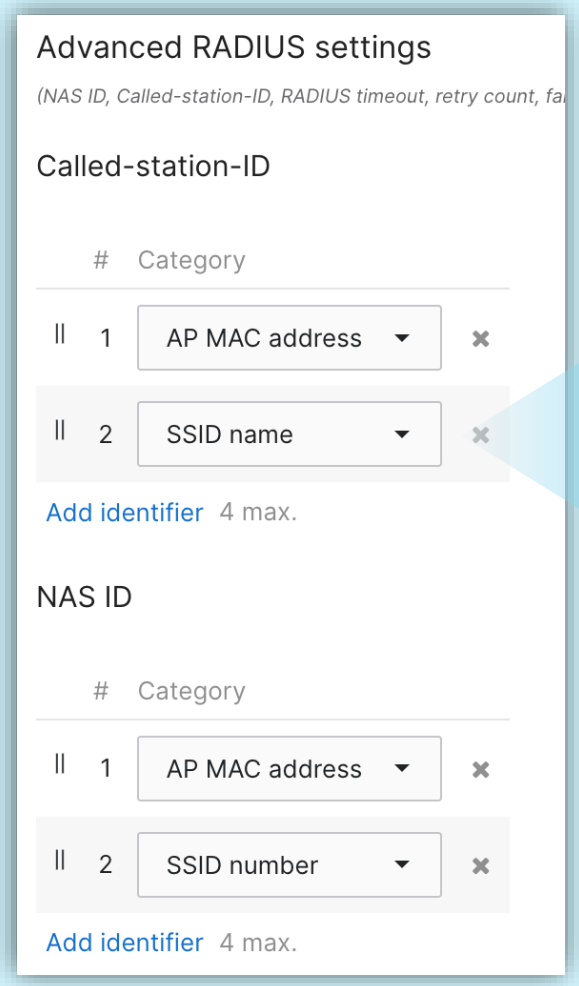
Configuration > Security > Wireless AAA Policy



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

Meraki Advanced RADIUS Attributes

Wireless > Configure > Access Control

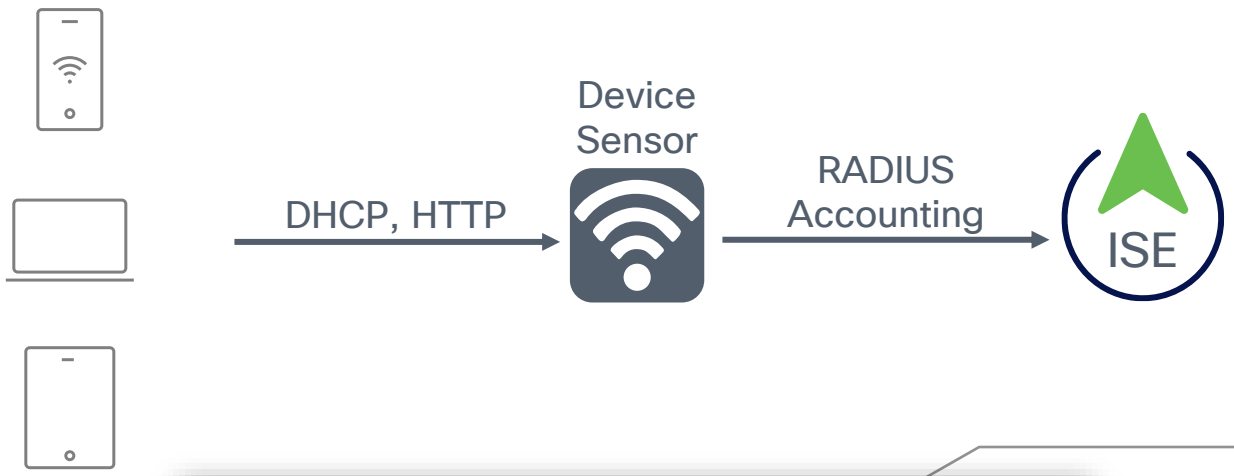


Attributes

AP MAC address	AP VLAN ID
SSID name	AP tags
SSID number	AP LAN IP
AP name	AP Public IP
RF Profile	Custom

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

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
```

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

Intel, Apple, Samsung Analytics

Reference

	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	

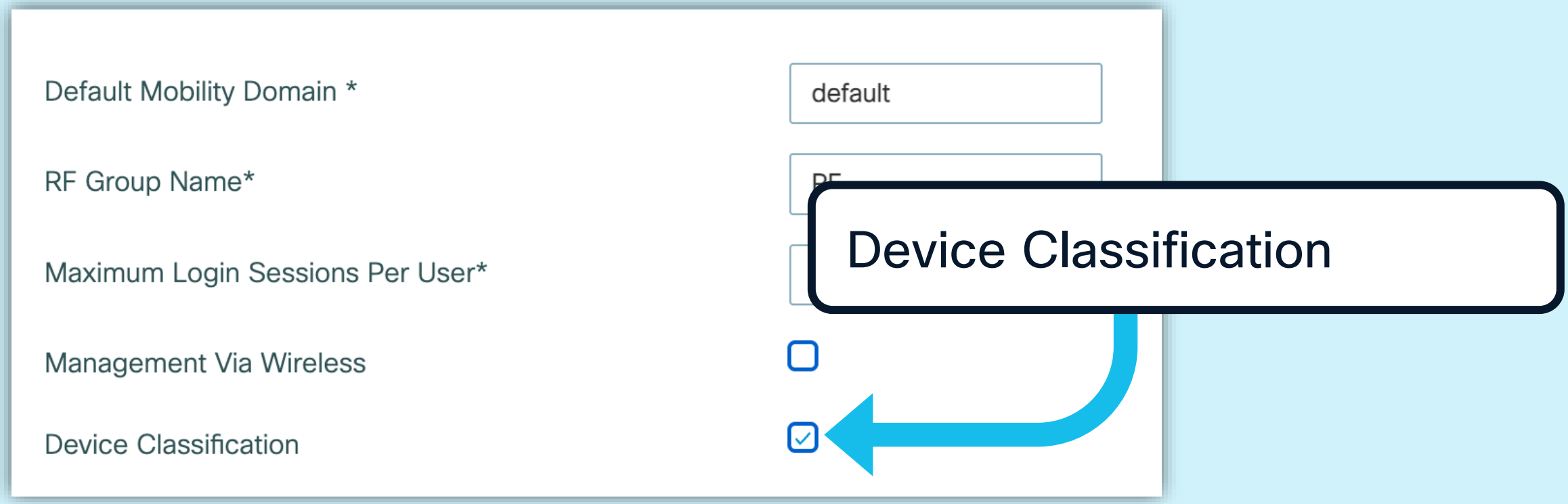
*Accounting Reports coming MR31.2

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

cisco

Enabling Device Analytics - WLC

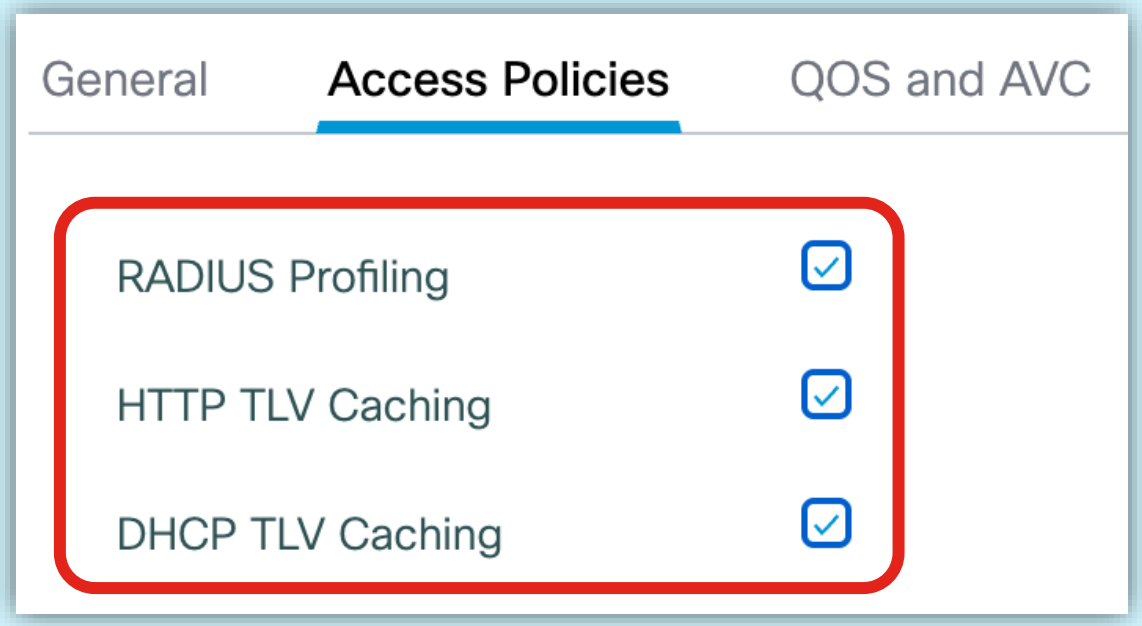
Configuration > Wireless > Wireless Global

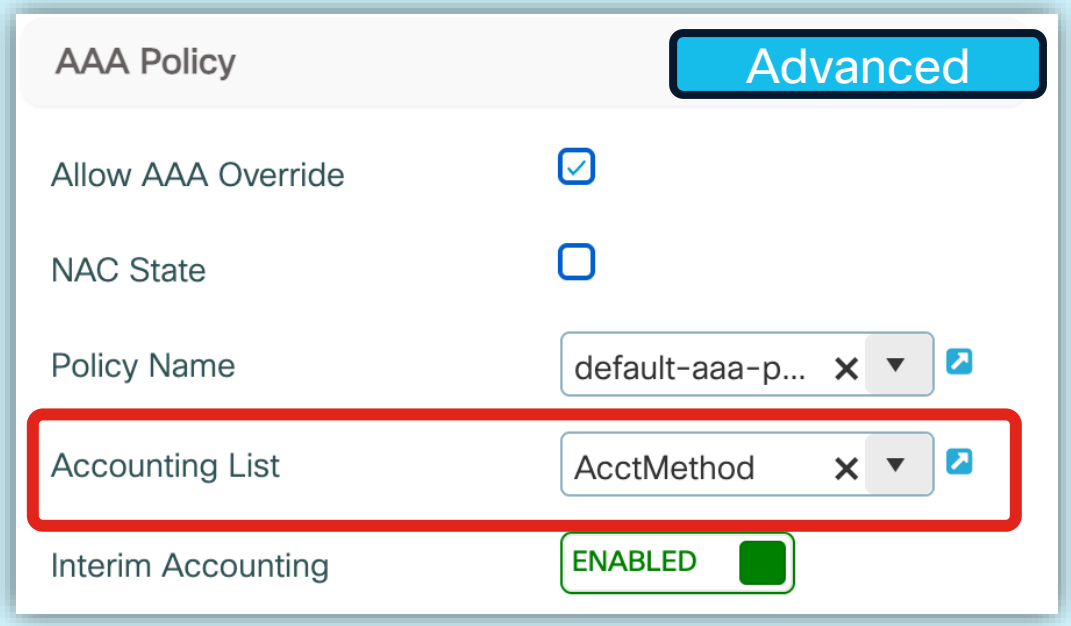


© 2025 Cisco and/or its affiliates. All rights reserved.

Enabling Device Analytics - WLC

Configuration > Tags & Profiles > Policy

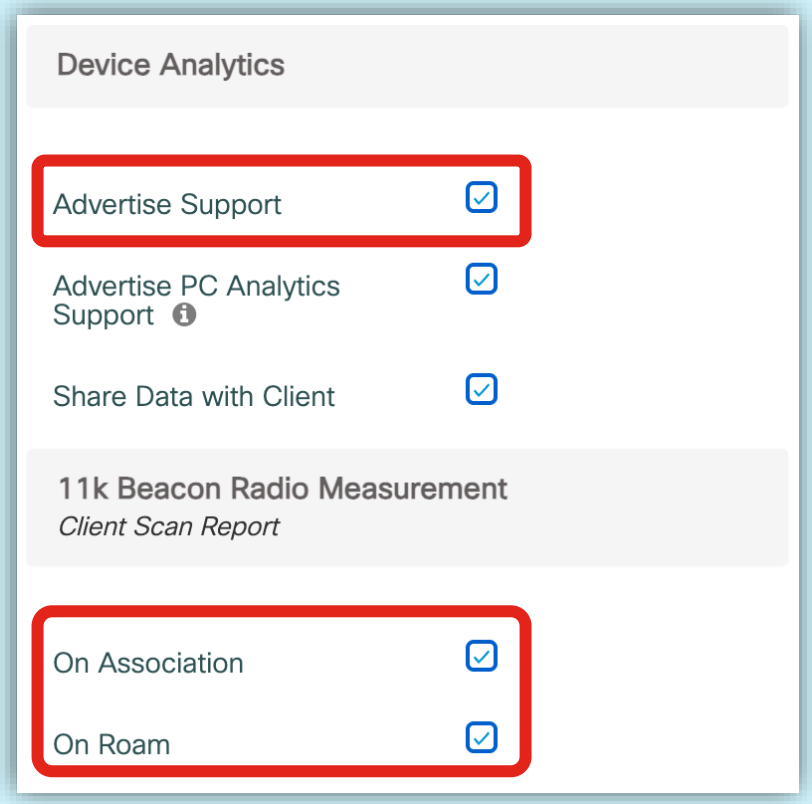




© 2025 Cisco and/or its affiliates. All rights reserved.

Enabling Device Analytics - WLC

Configuration > Tags & Profiles > WLANs

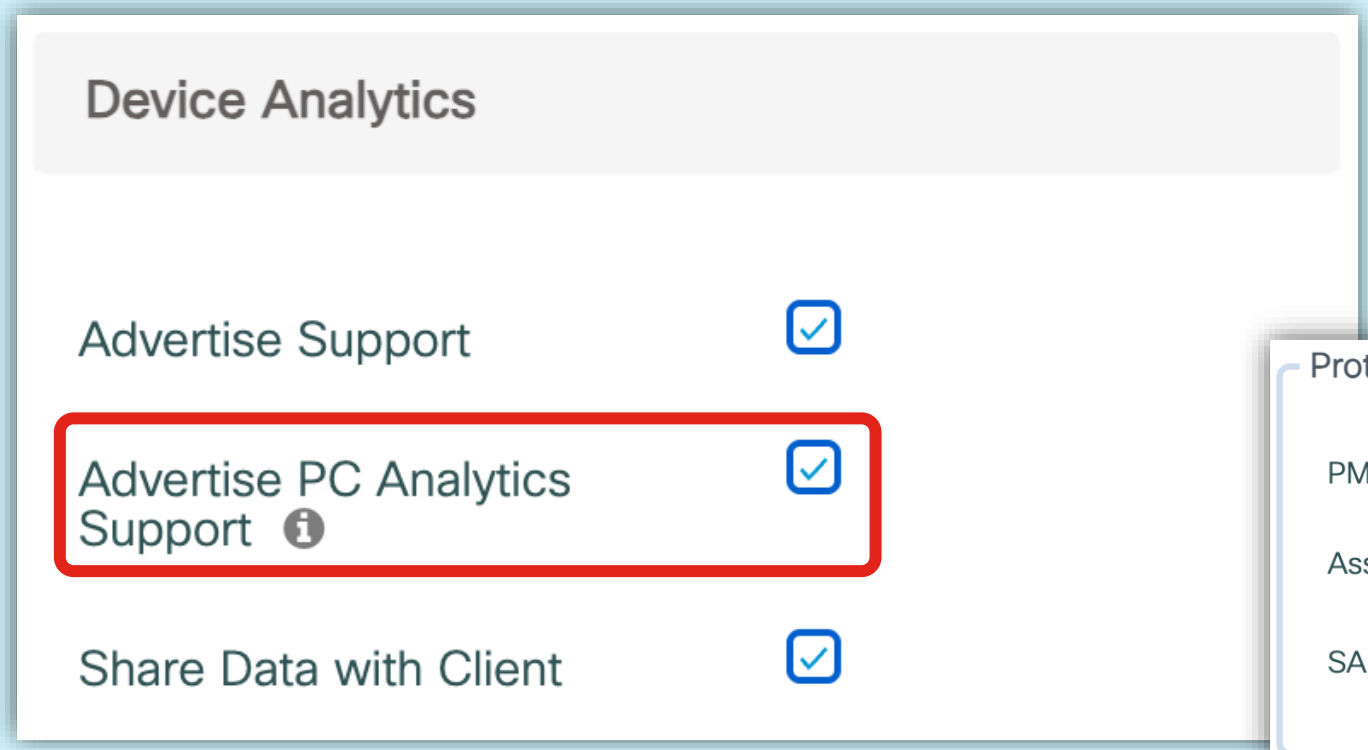


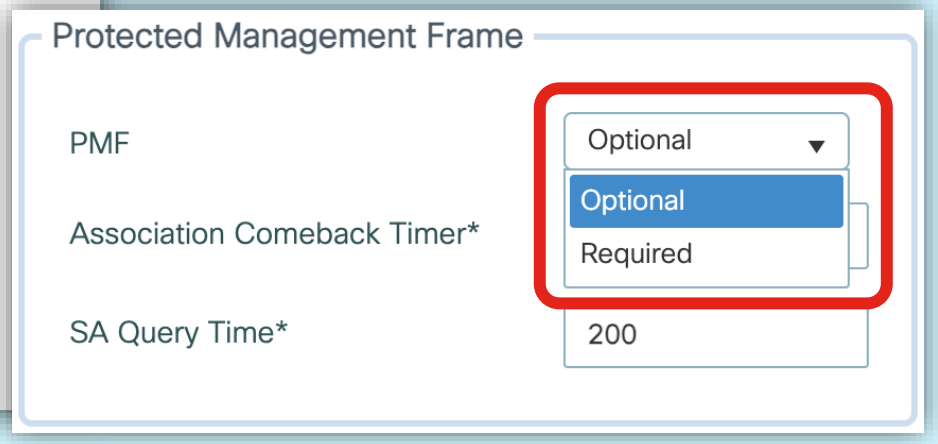
SAMSUNG

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

Enabling Device Analytics - WLC

Configuration > Tags & Profiles > WLANs





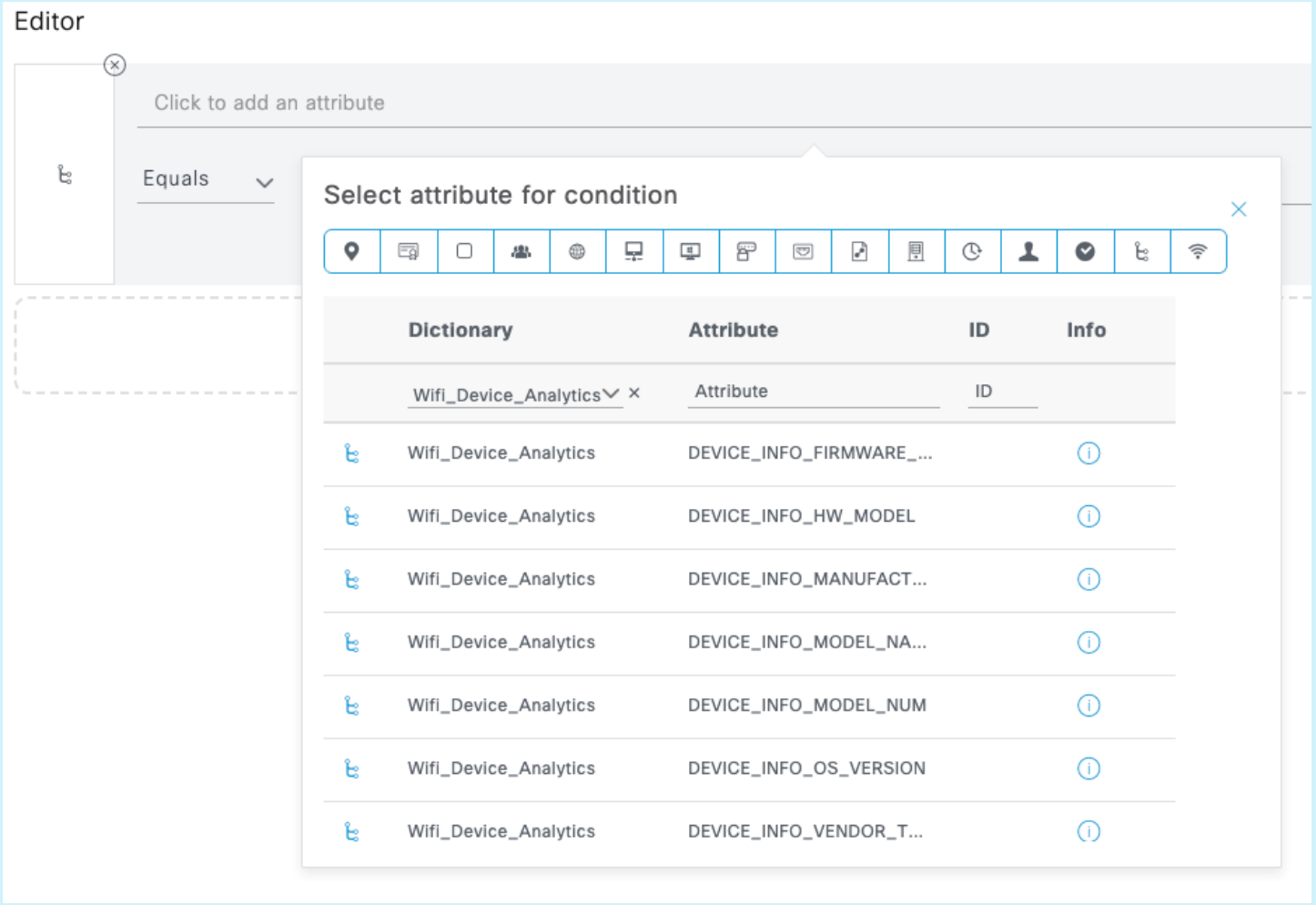
© 2025 Cisco and/or its affiliates. All rights reserved.

Enabling Device Analytics - WLC

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

Device Analytics Attributes – Authorization Policy

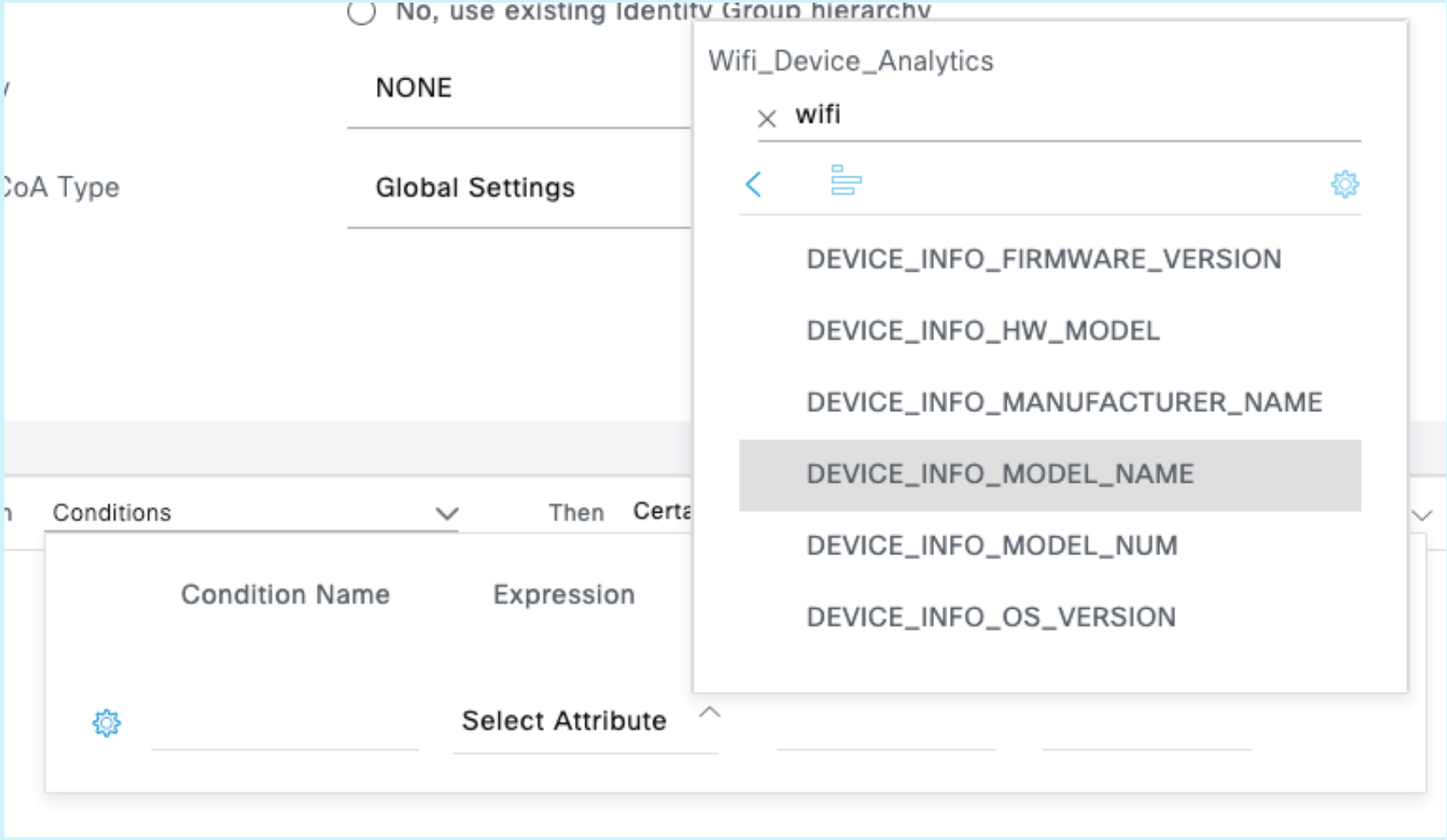
Policy > Policy Sets > Authorization Policy



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

Device Analytics Attributes – Profiler Policy

Policy > Profiling > Profiler Policy



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

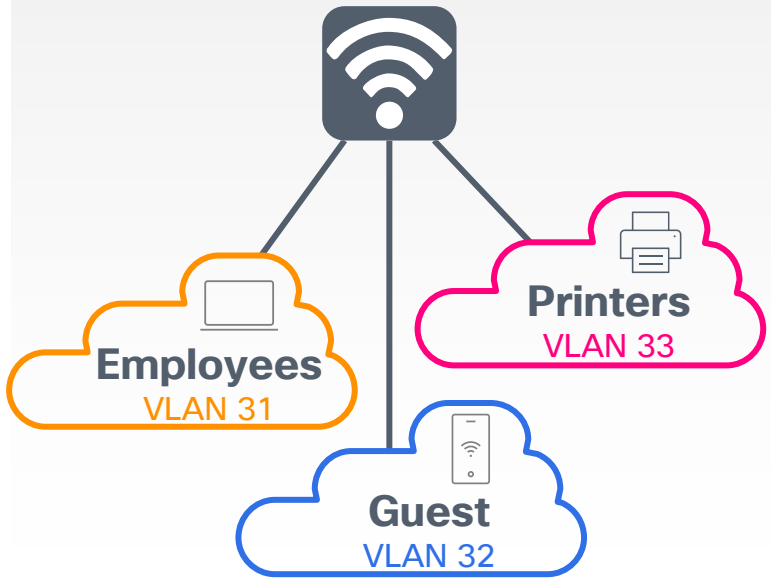
Authorization Results

ISE Segmentation Options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

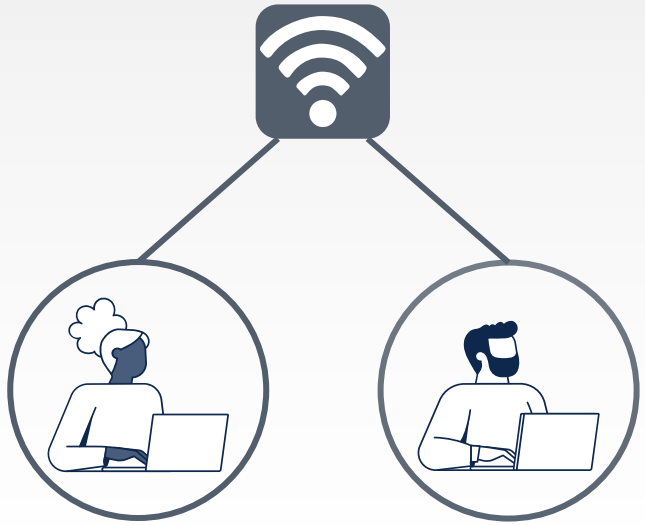
Dynamic VLAN Assignments



Per WLAN / Per User

ACLs

Downloadable ACLs
Named ACLs / Group Policy



Employee

```
permit ip any any
```

Contractor

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

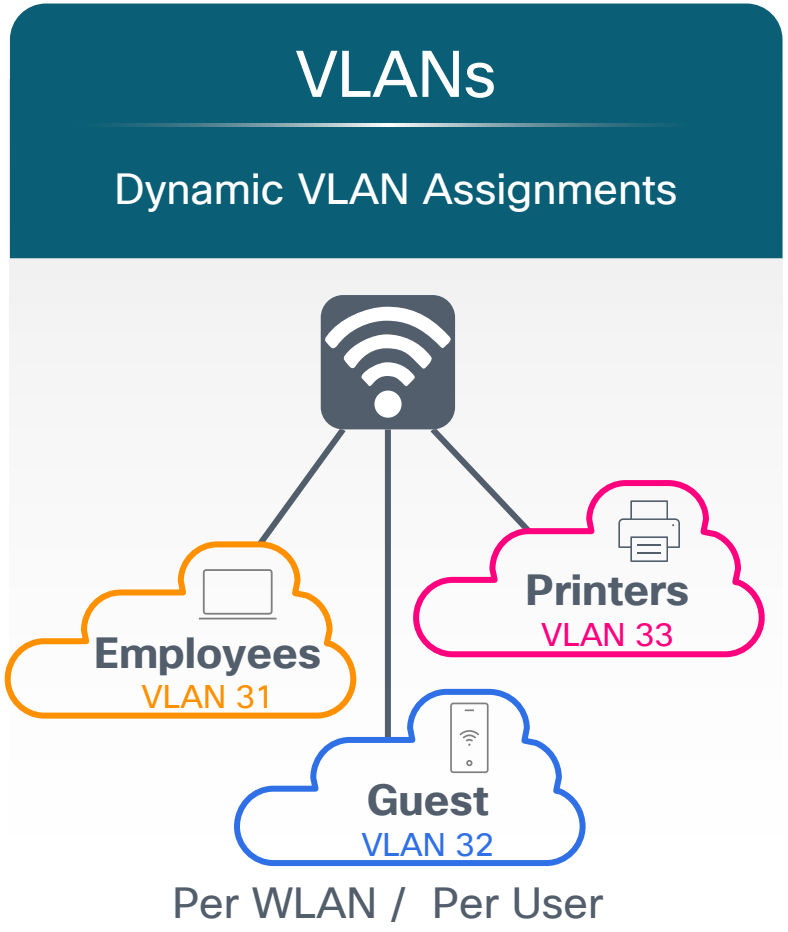
Security Group Tags

TrustSec
Adaptive Policy

16-bit SGT
SGT based Access Control

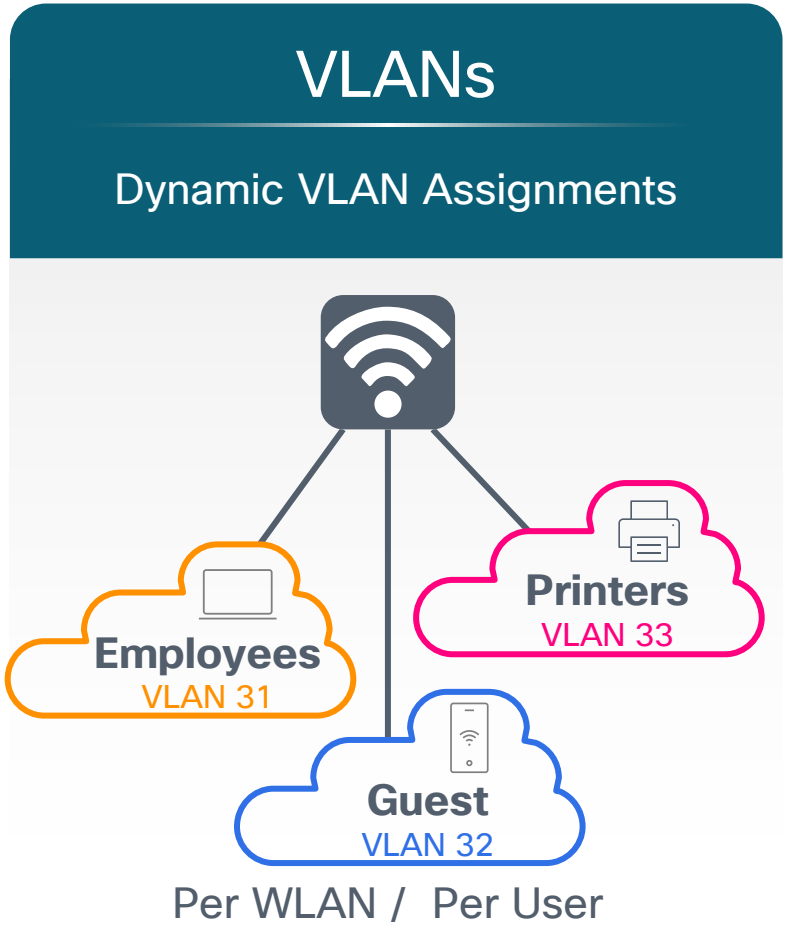
© 2025 Cisco and/or its affiliates. All rights reserved.

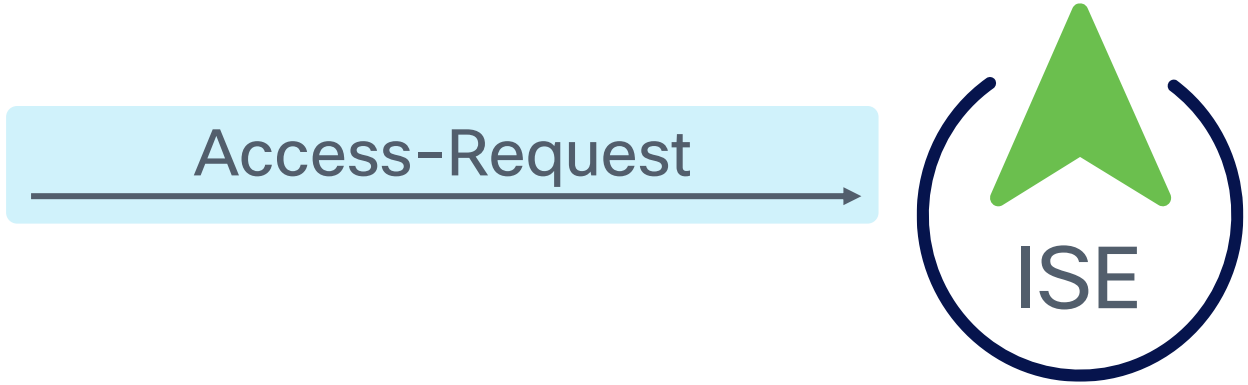
Dynamic VLAN Assignment



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

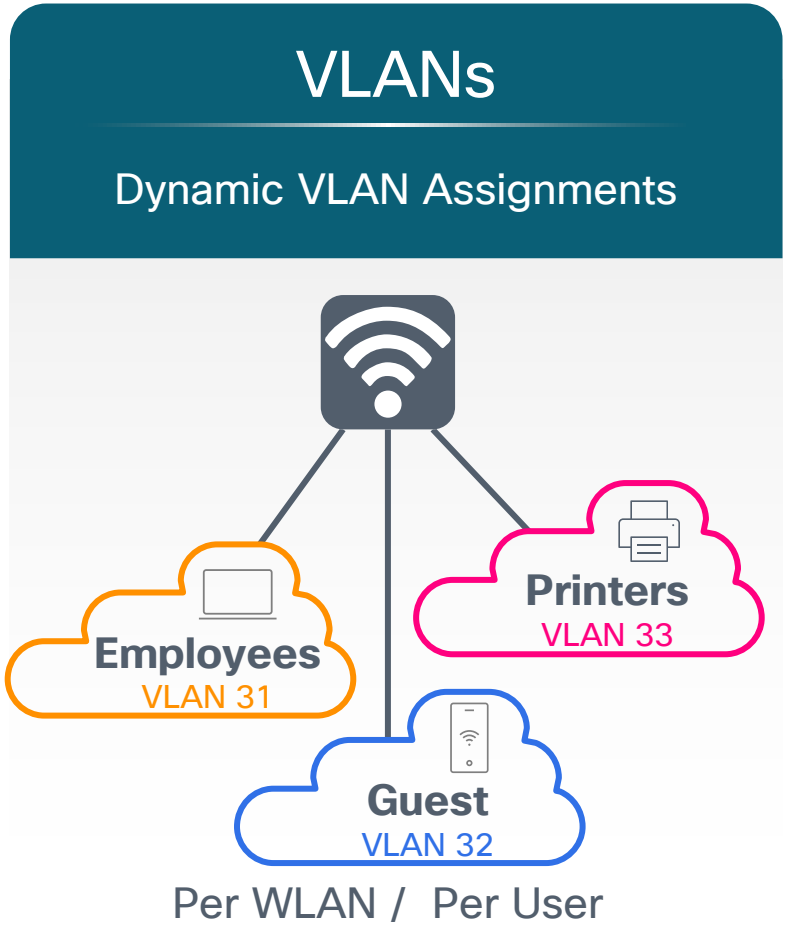
Dynamic VLAN Assignment





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

Dynamic VLAN Assignment



Access-Request

Access-Accept

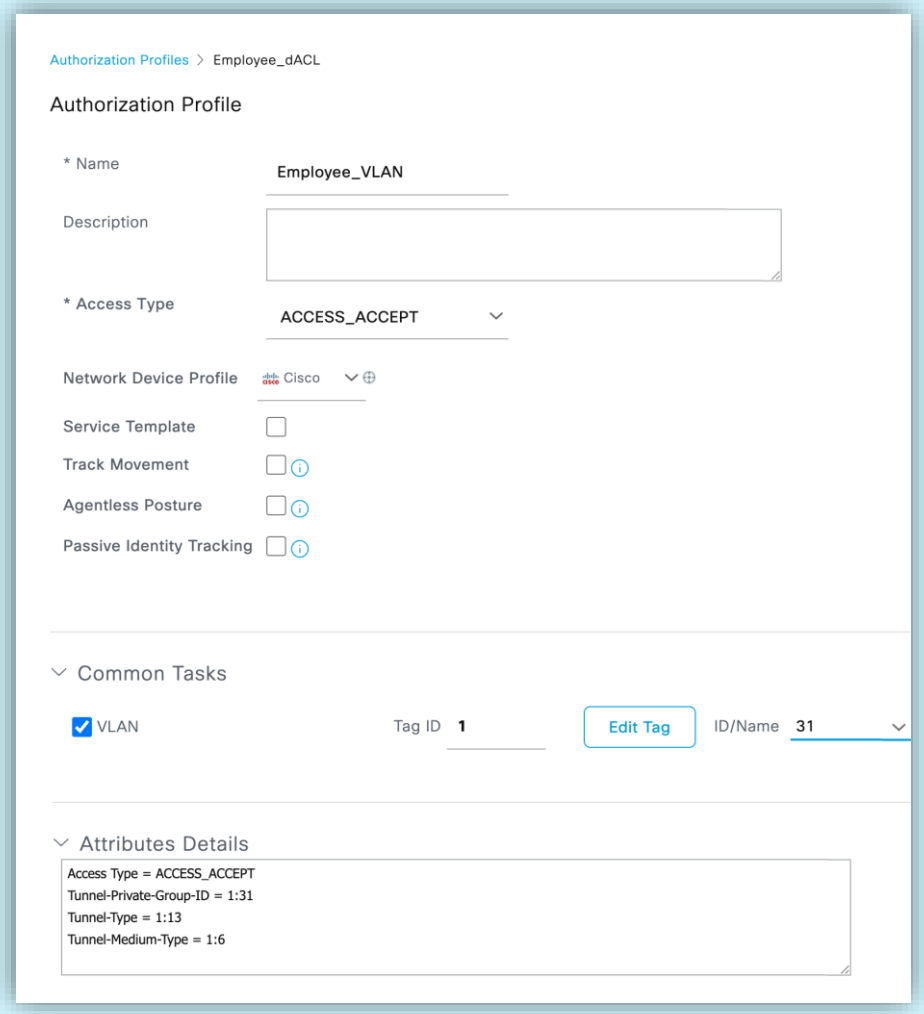
+

“Assign Client to VLAN 31”

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

Dynamic VLAN – ISE

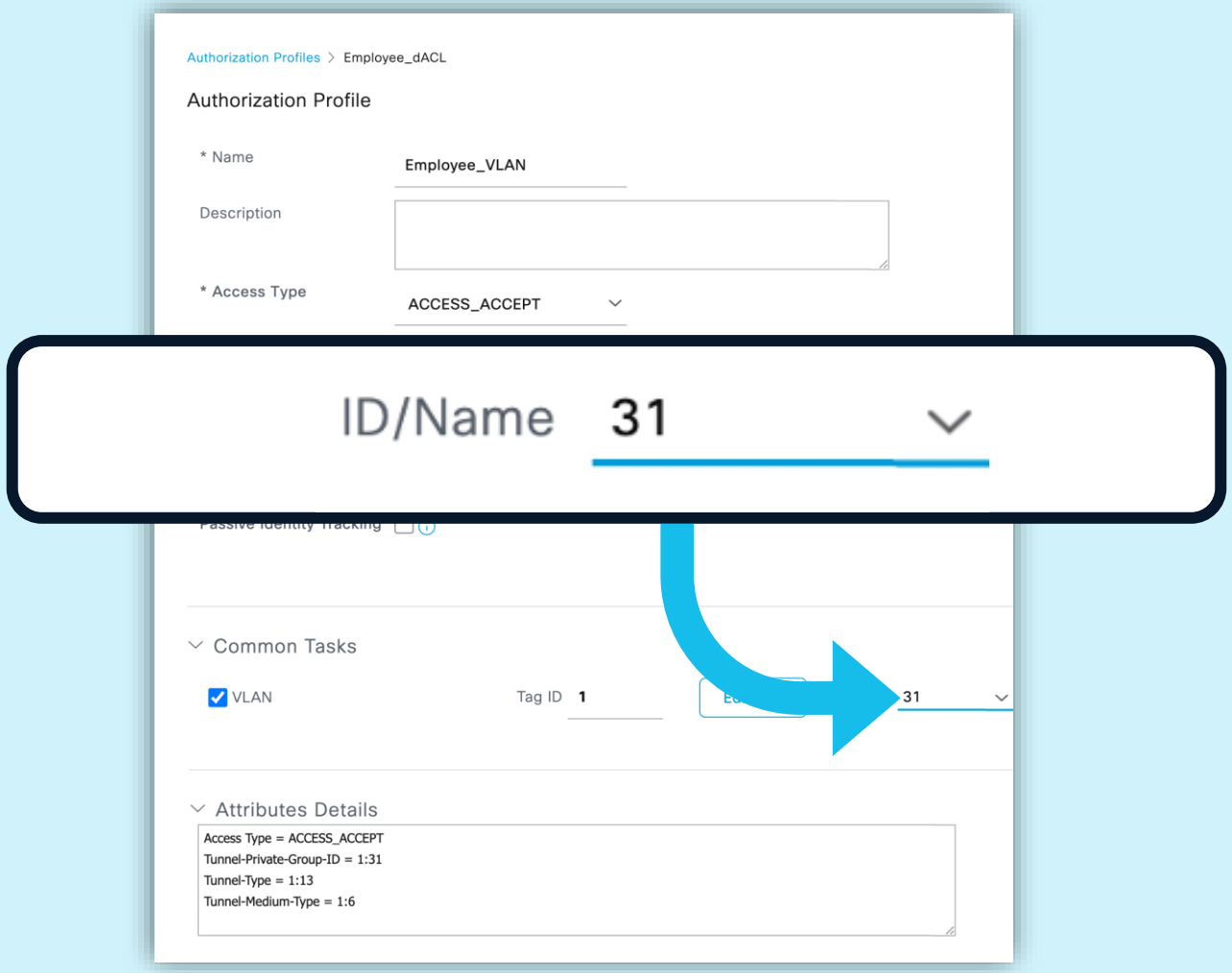
Policy > Policy Elements > Results > Authorization



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

Dynamic VLAN – ISE

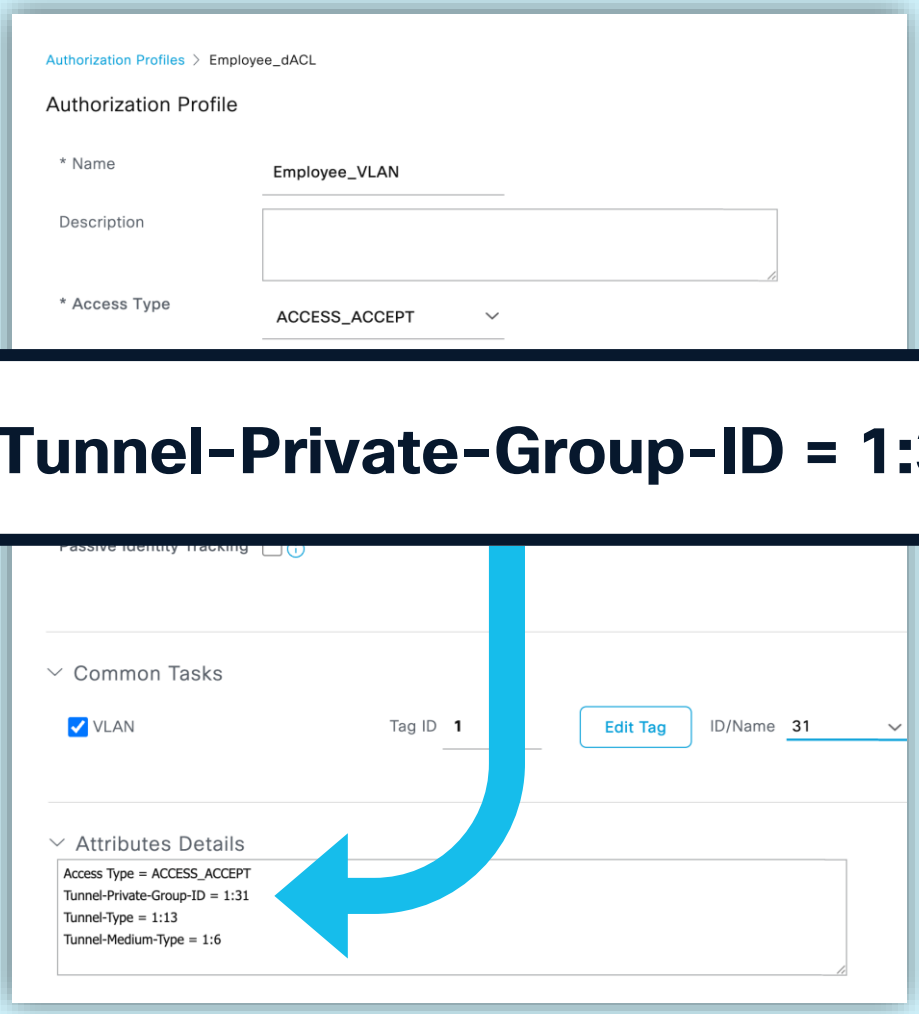
Policy > Policy Elements > Results > Authorization



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

Dynamic VLAN – ISE

Policy > Policy Elements > Results > Authorization

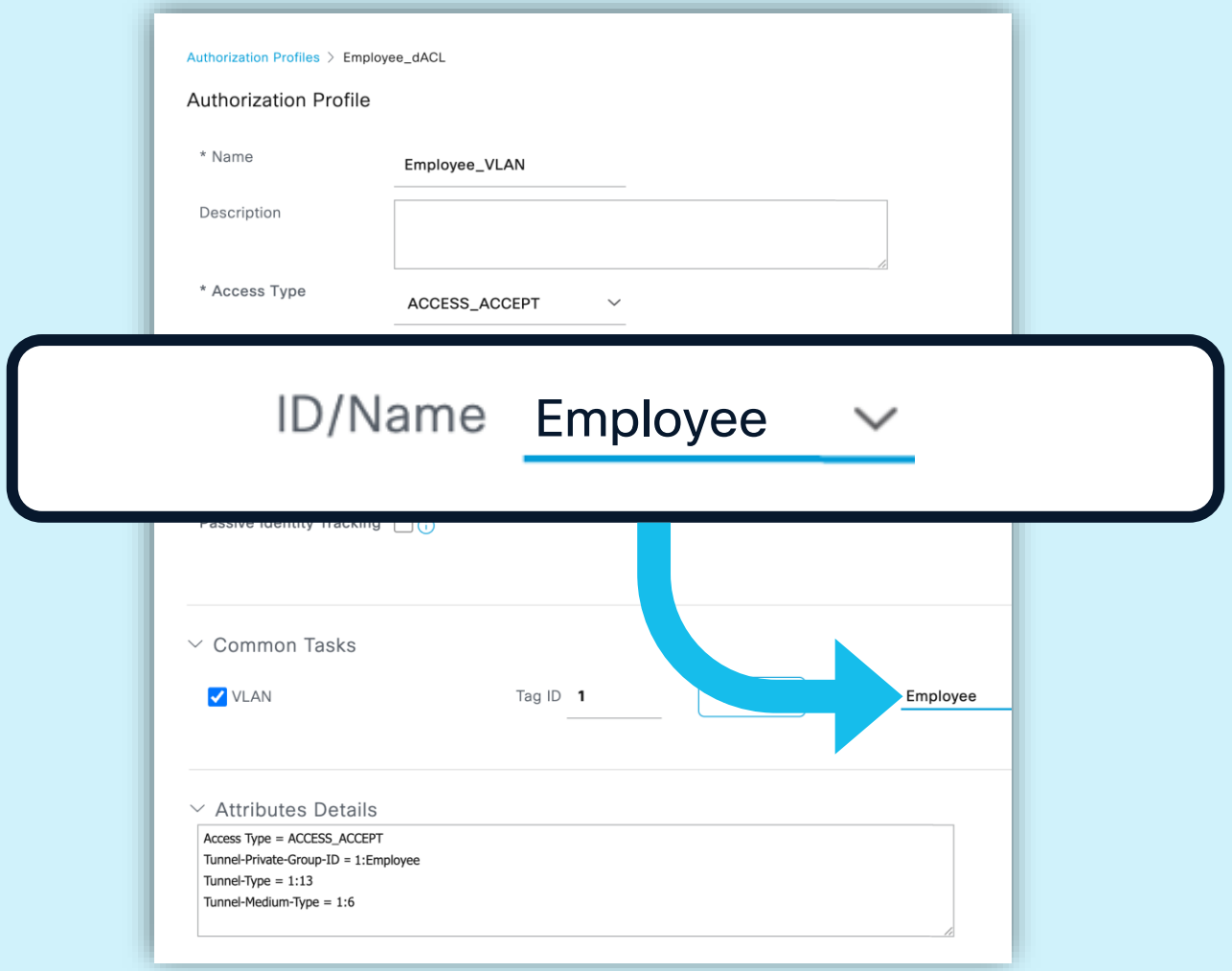


Tunnel-Private-Group-ID = 1:31

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

Dynamic VLAN – ISE

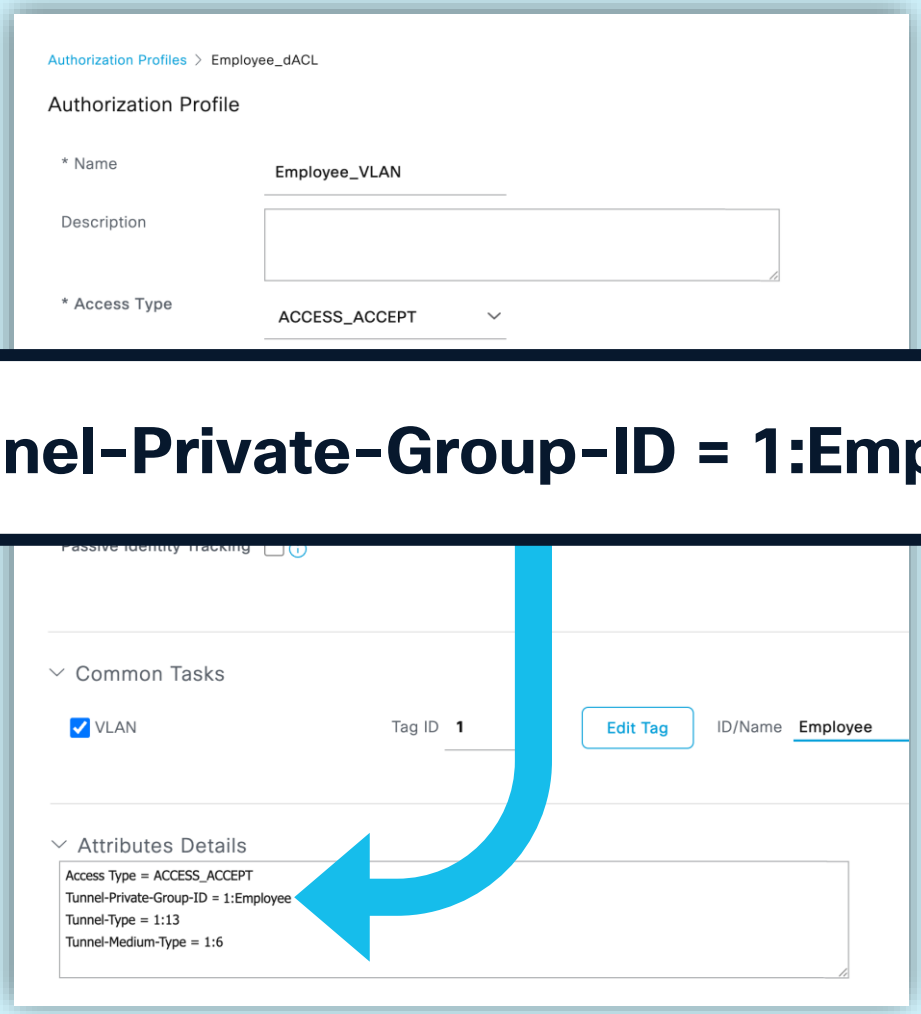
Policy > Policy Elements > Results > Authorization



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

Dynamic VLAN – ISE

Policy > Policy Elements > Results > Authorization

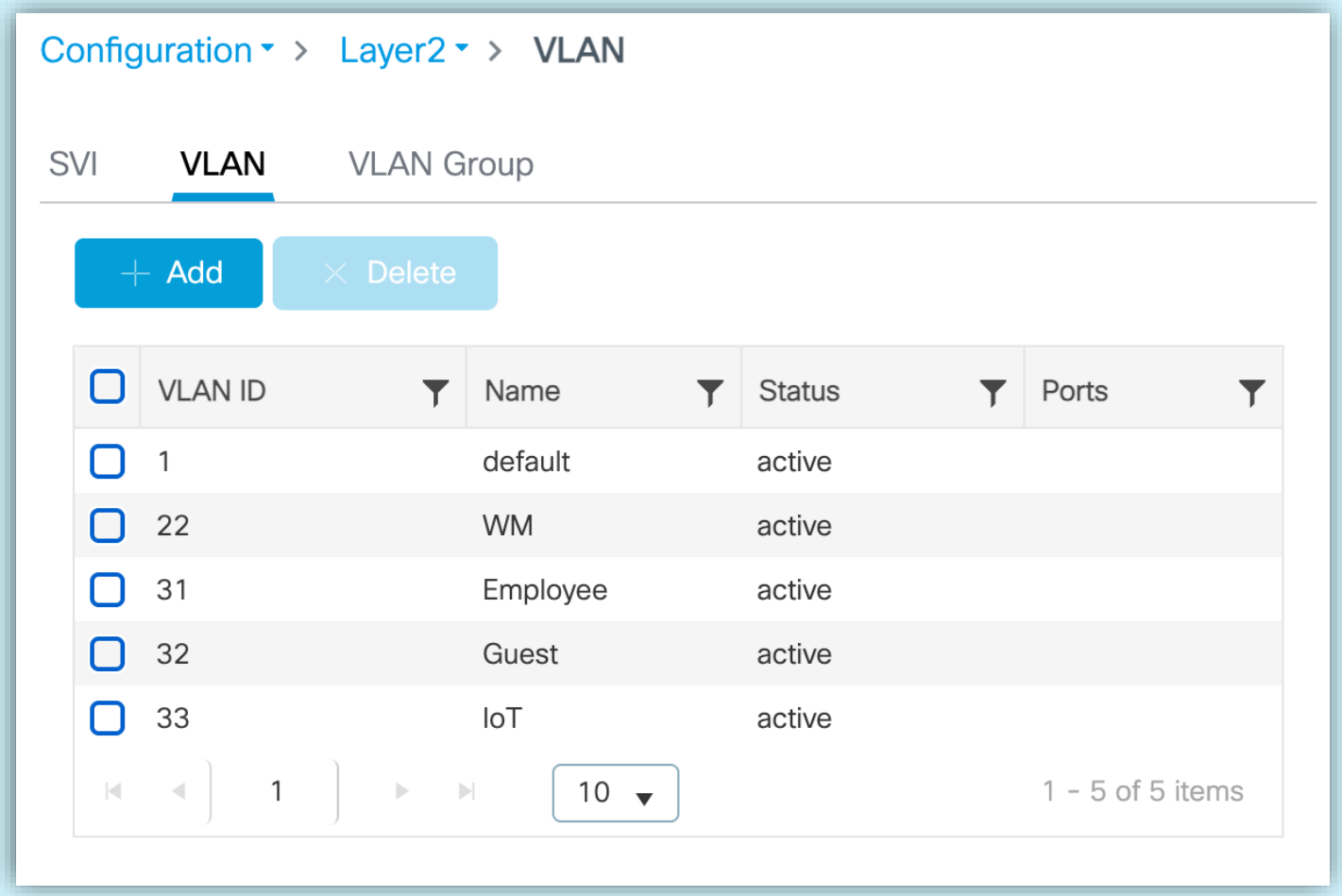


Tunnel-Private-Group-ID = 1:Employee

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

Dynamic VLAN – Catalyst 9800

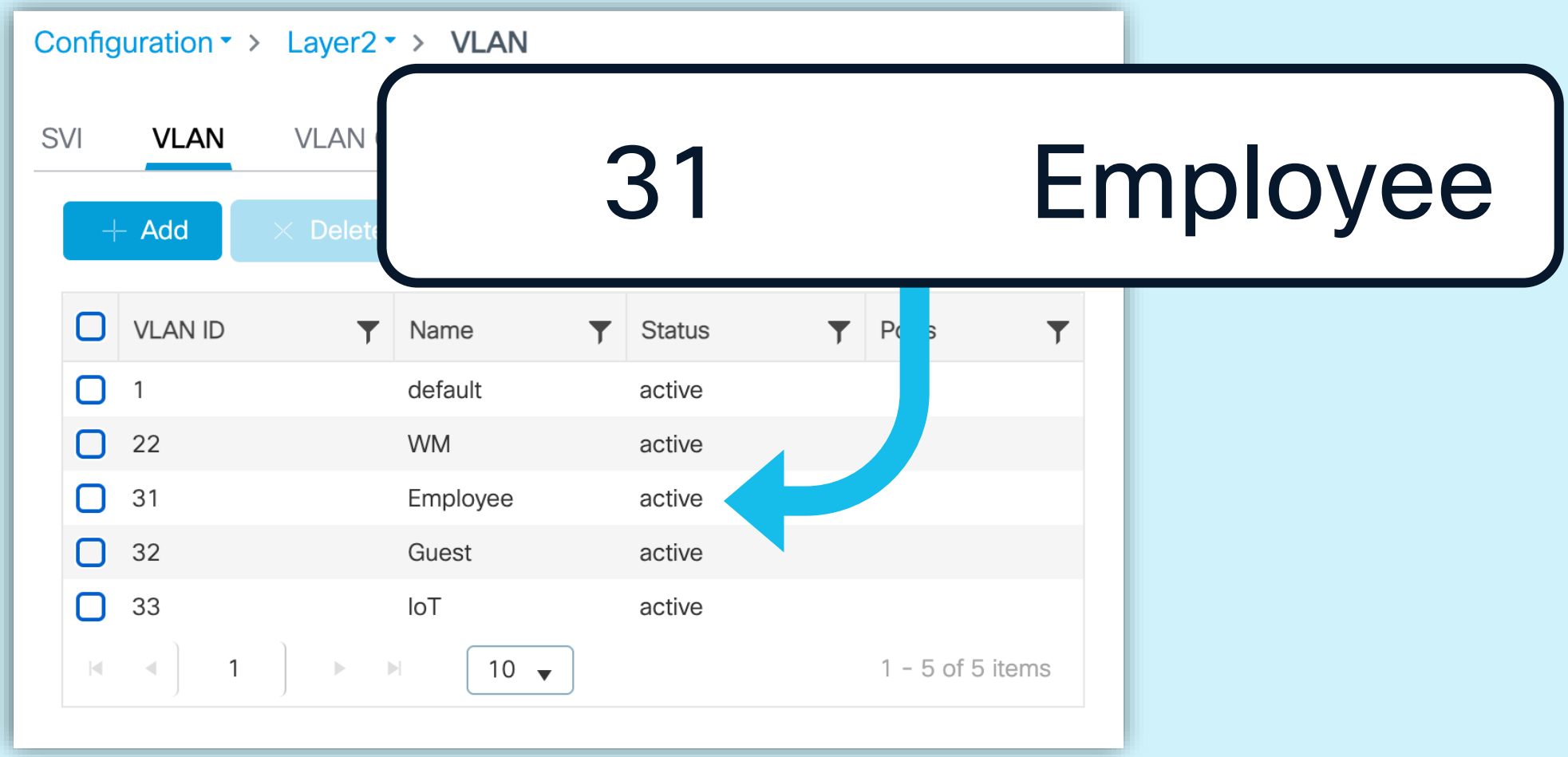
Configuration > Layer2 > VLAN



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

Dynamic VLAN – Catalyst 9800

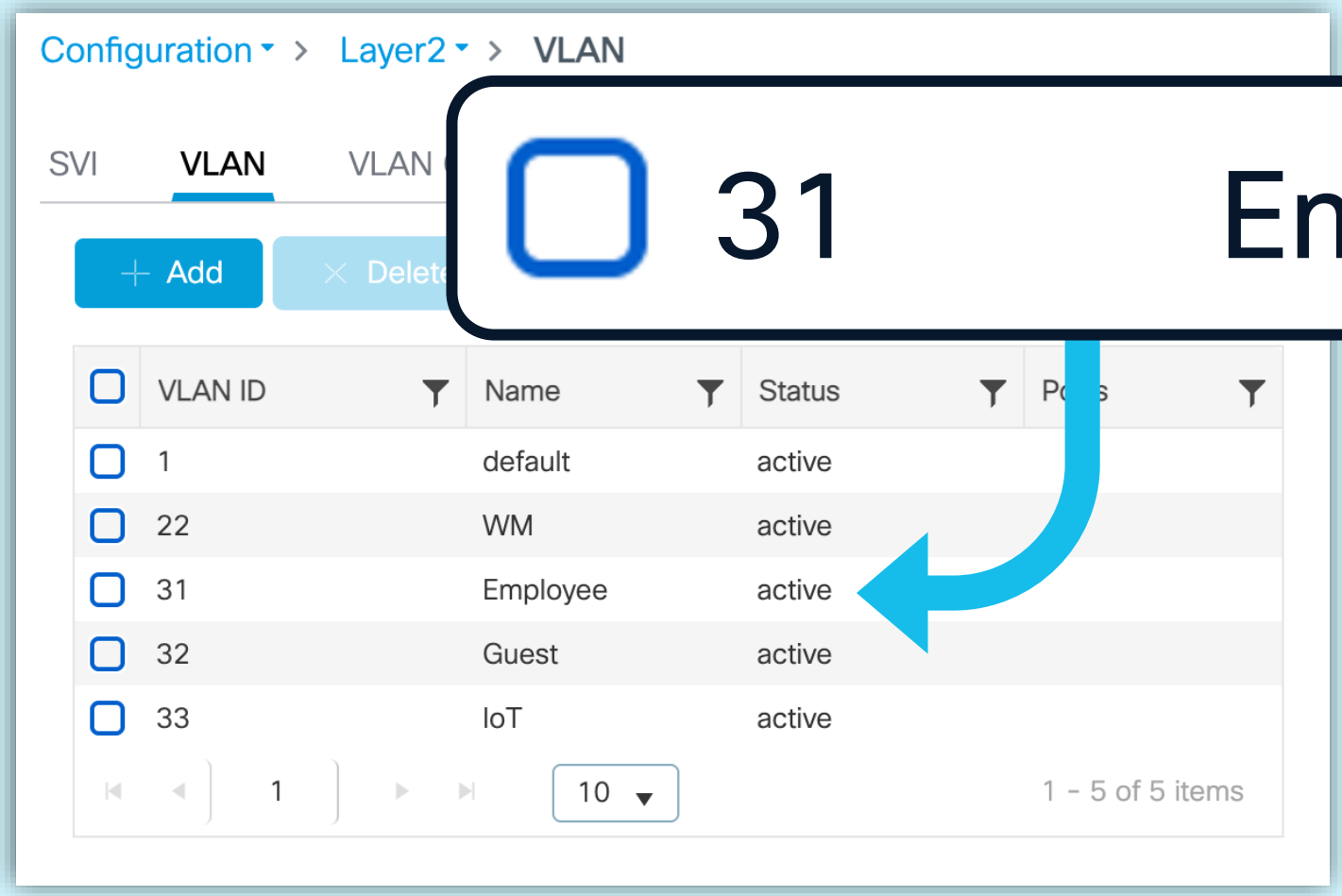
Configuration > Layer2 > VLAN



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

Dynamic VLAN – Catalyst 9800

Configuration > Layer2 > VLAN



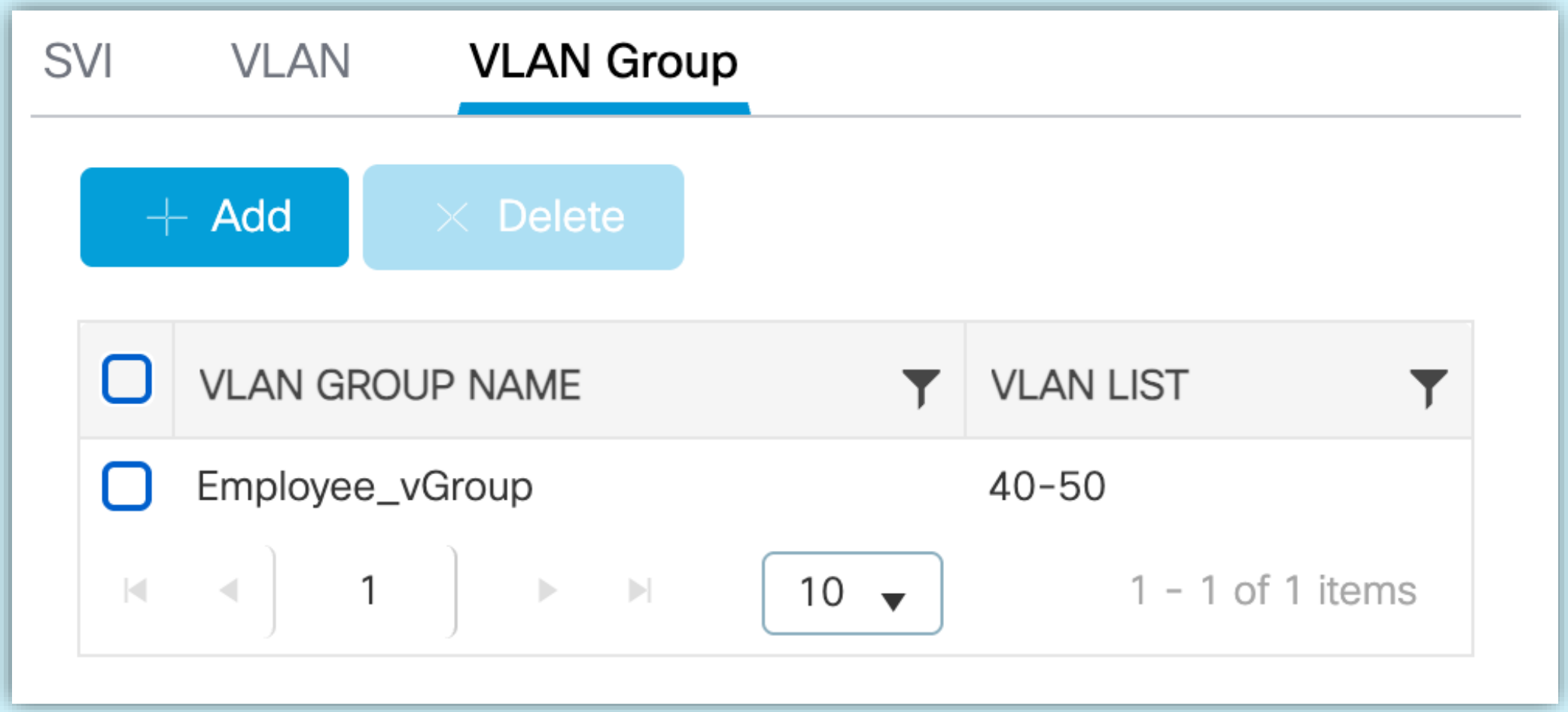
31 Employee

VLANs must exist

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

Dynamic VLAN – Catalyst 9800

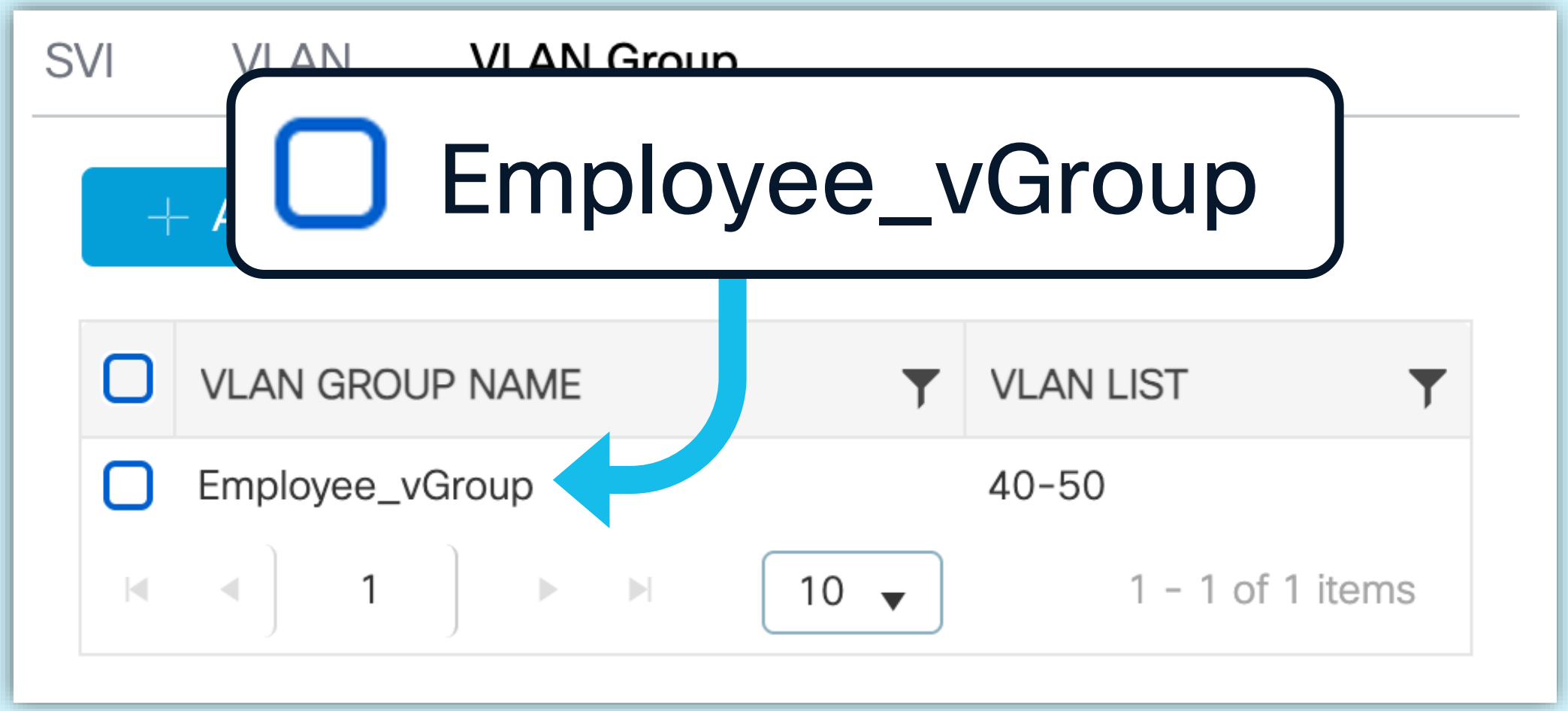
Configuration > Layer2 > VLAN



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

Dynamic VLAN – Catalyst 9800

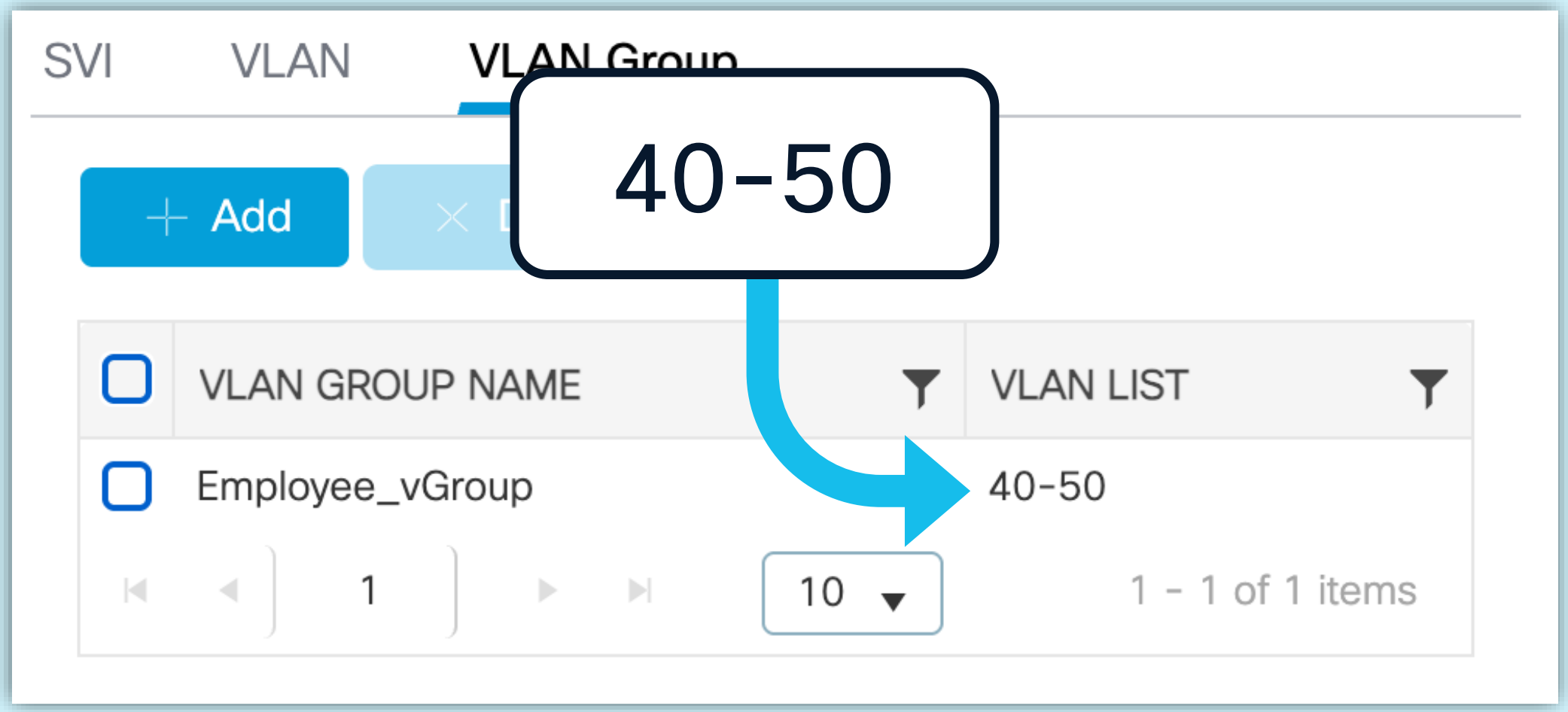
Configuration > Layer2 > VLAN



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

Dynamic VLAN – Catalyst 9800

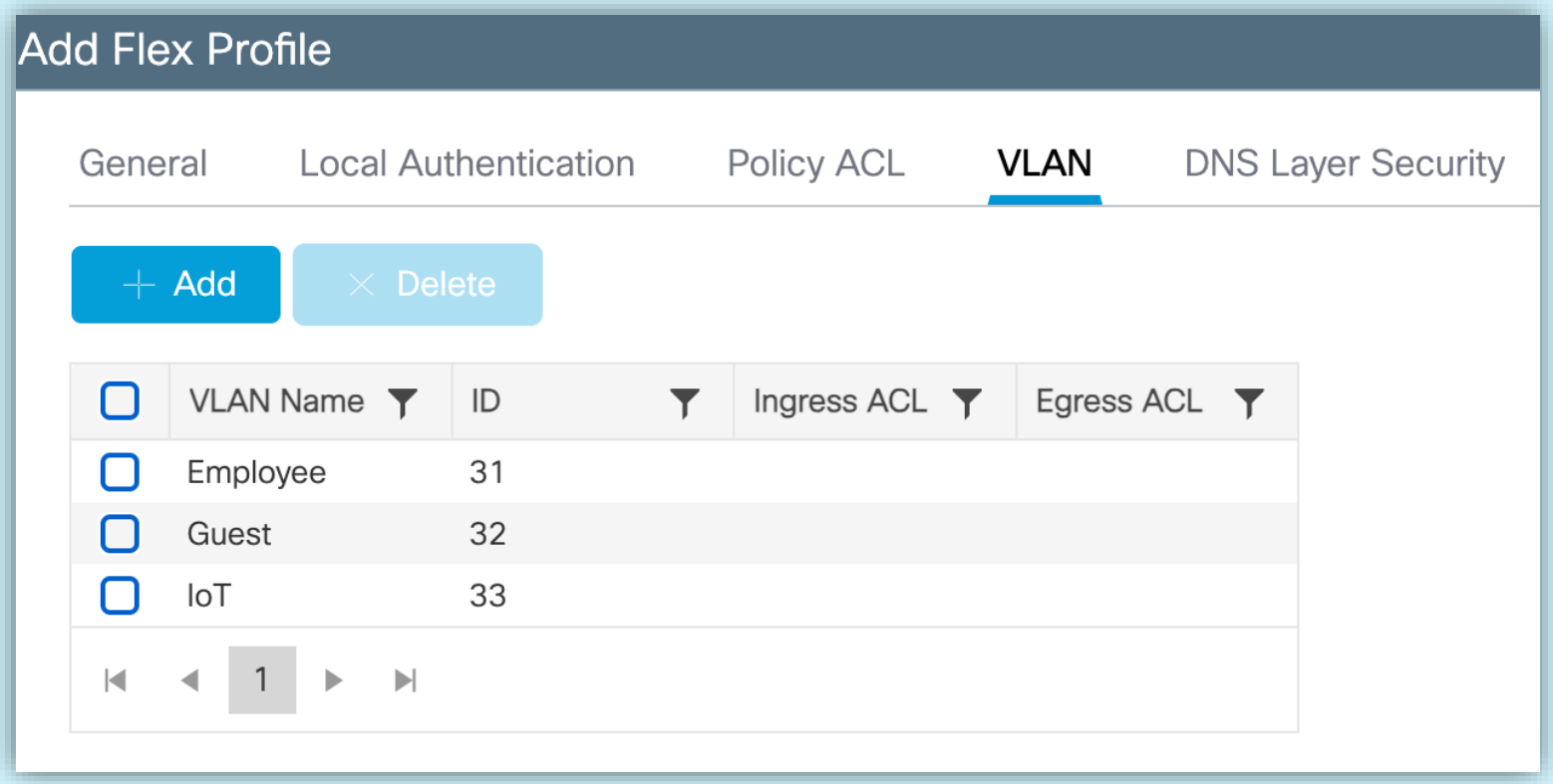
Configuration > Layer2 > VLAN



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

Dynamic VLAN – Catalyst 9800

Configuration > Tags & Profiles > Flex

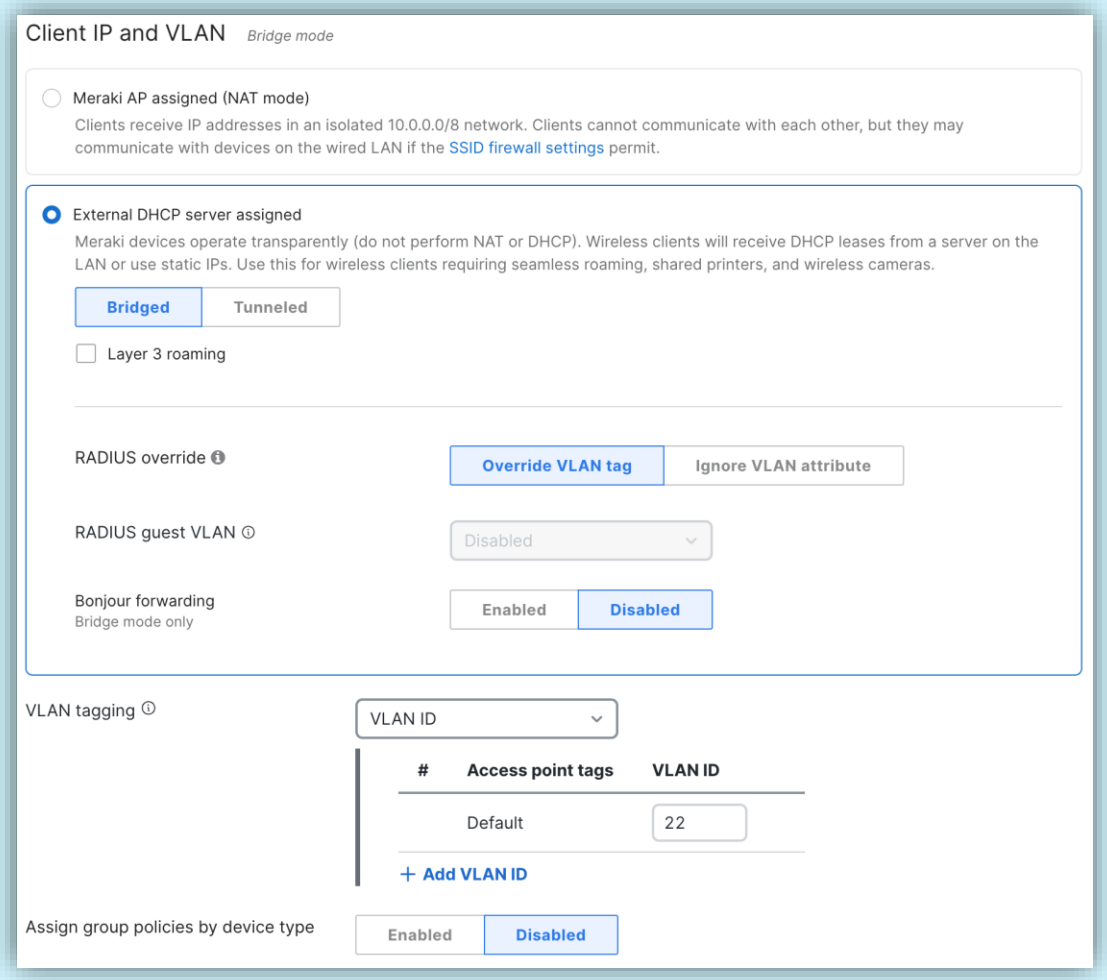


If using Flexconnect VLANs need to be added to Flex Profile

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

Dynamic VLAN – Meraki

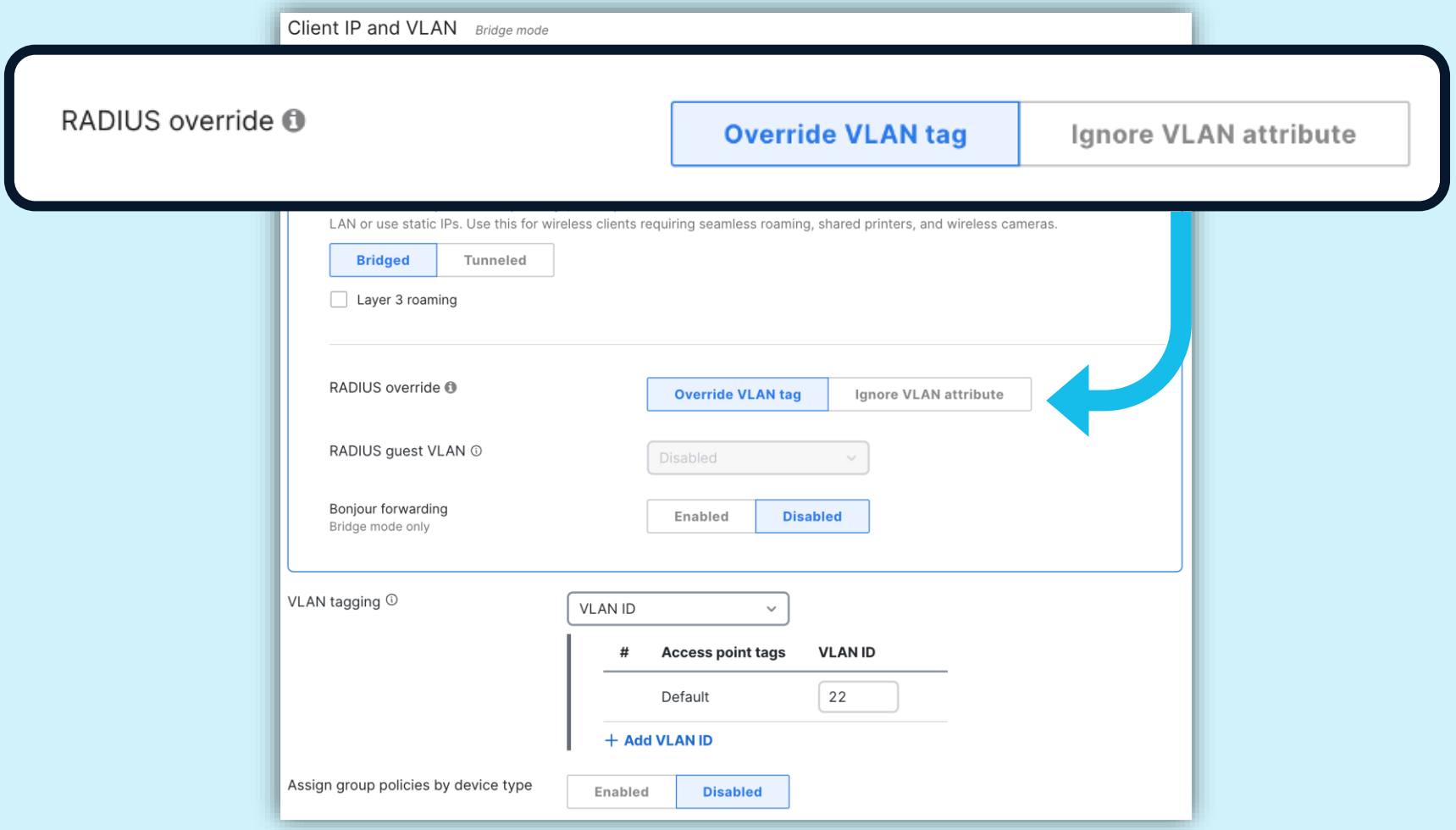
Wireless > Configure > Access Control



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

Dynamic VLAN – Meraki

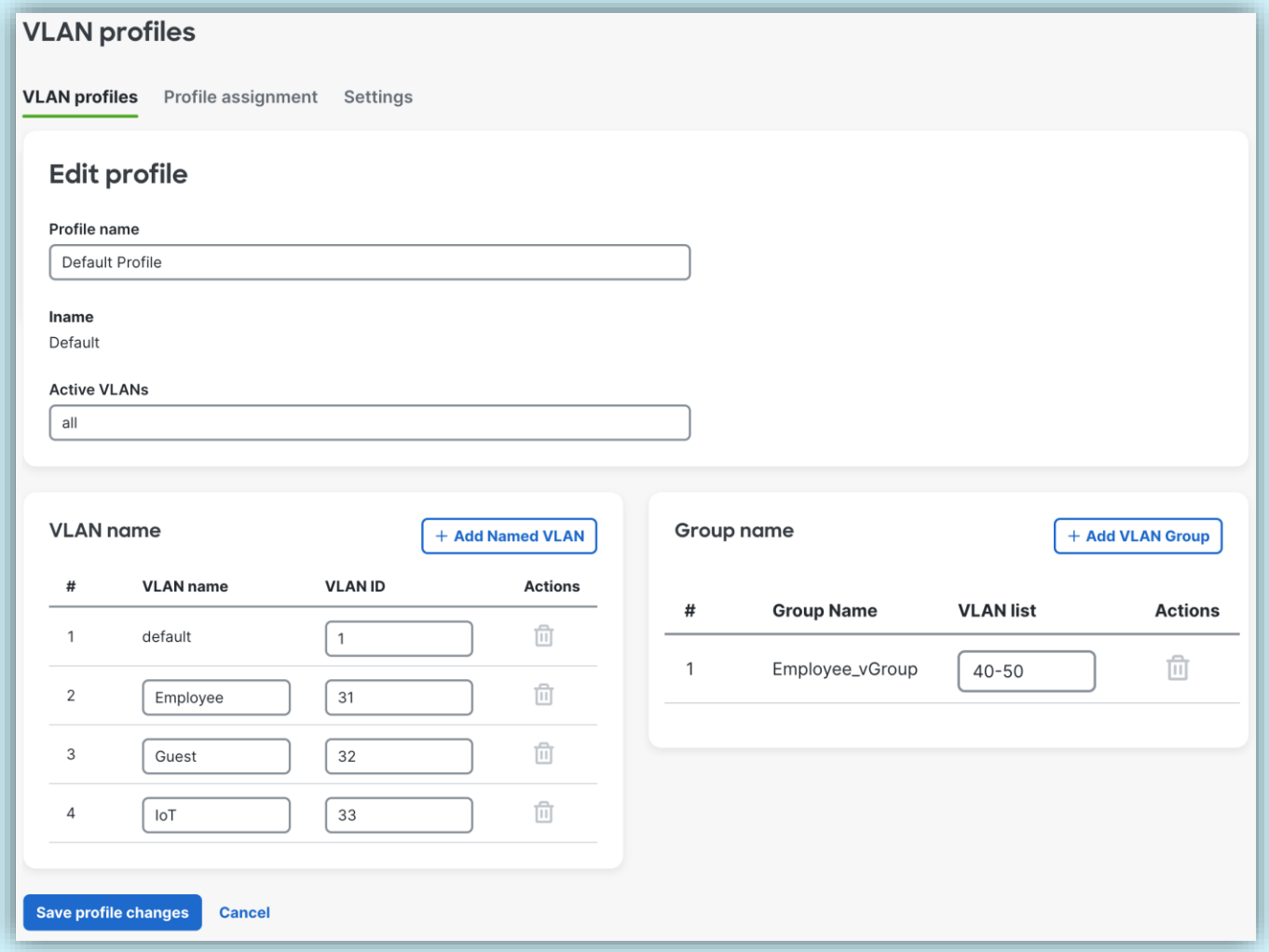
Wireless > Configure > Access Control



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

Dynamic VLAN – Meraki VLAN Profiles

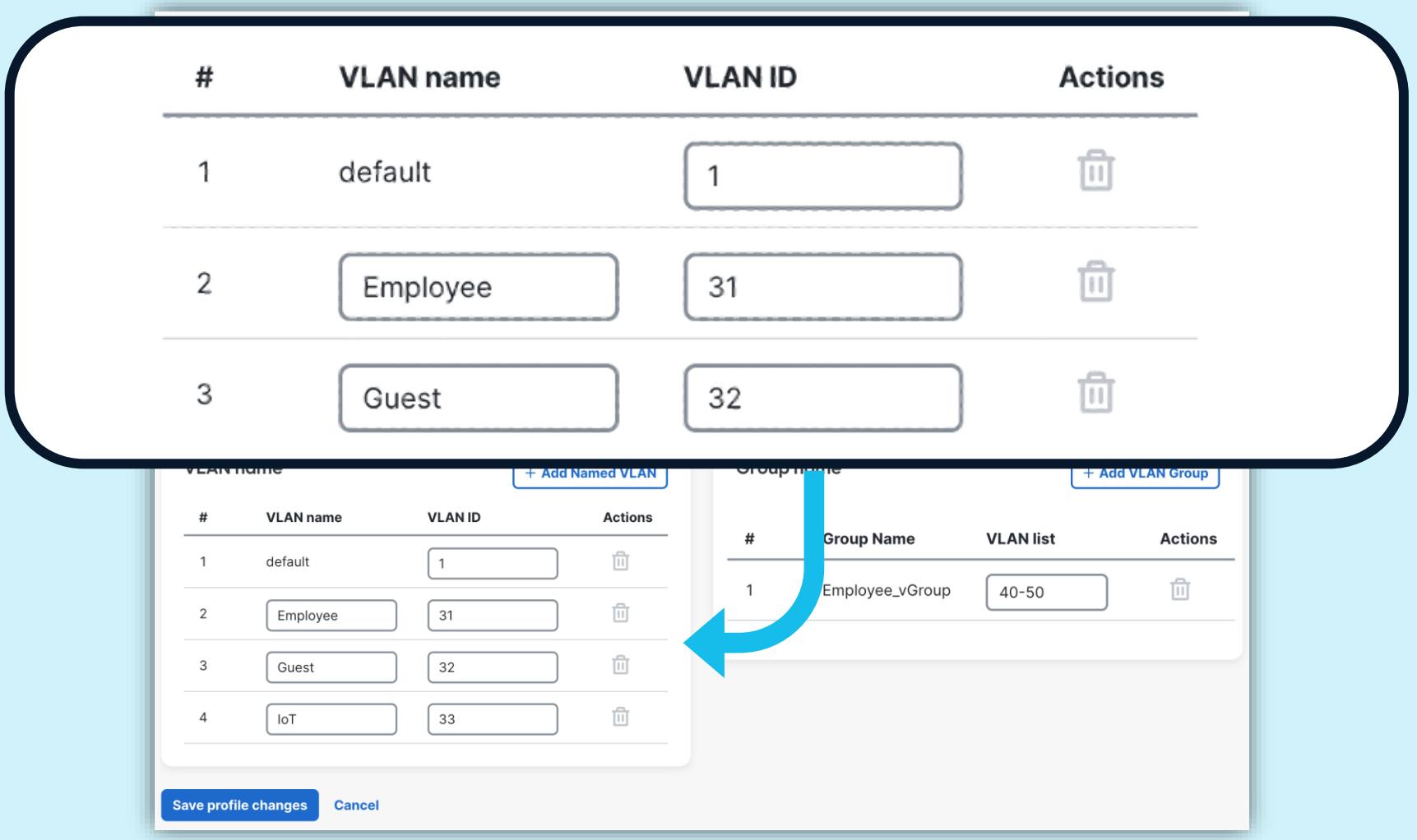
Network-Wide > VLAN Profiles



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

Dynamic VLAN – Meraki VLAN Profiles

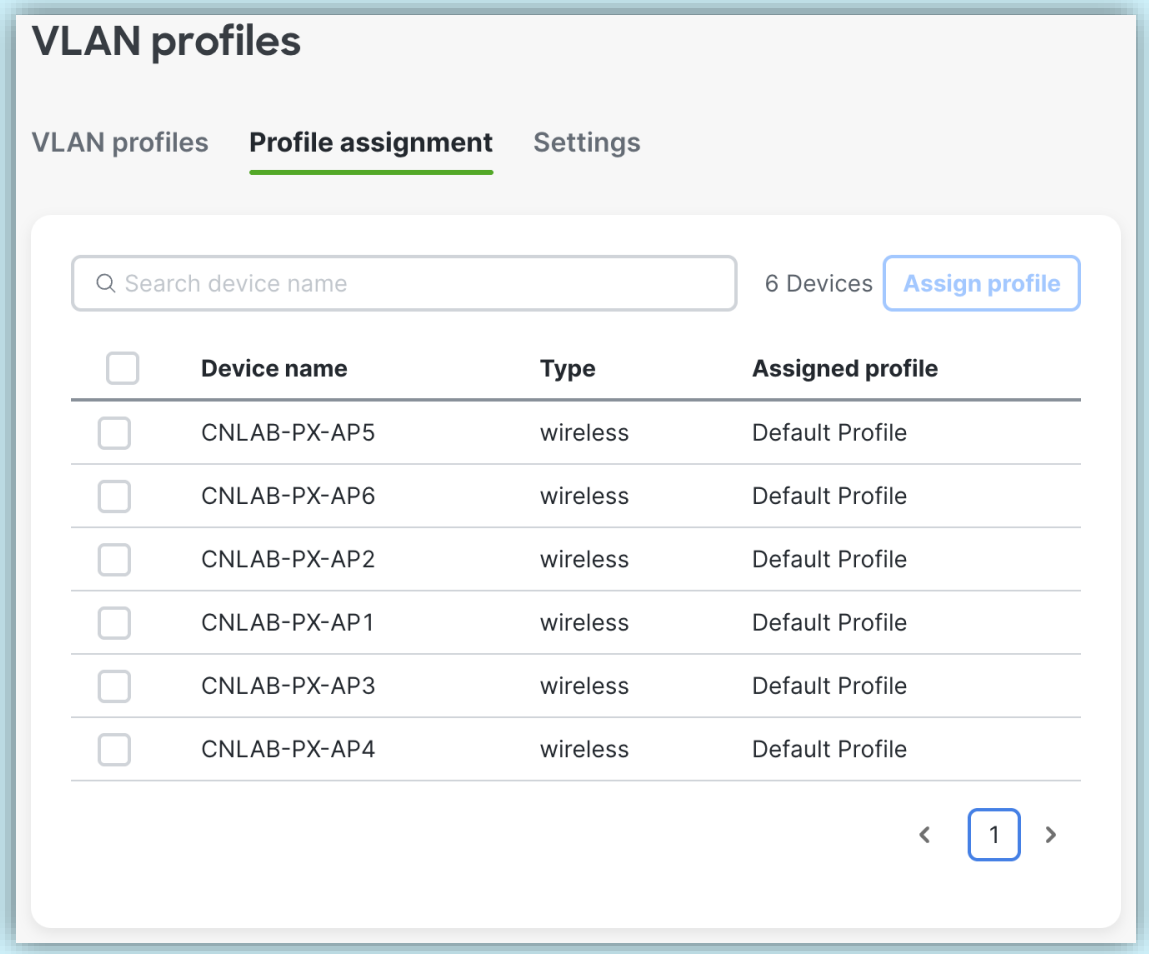
Network-Wide > VLAN Profiles



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

Dynamic VLAN – Meraki VLAN Profiles

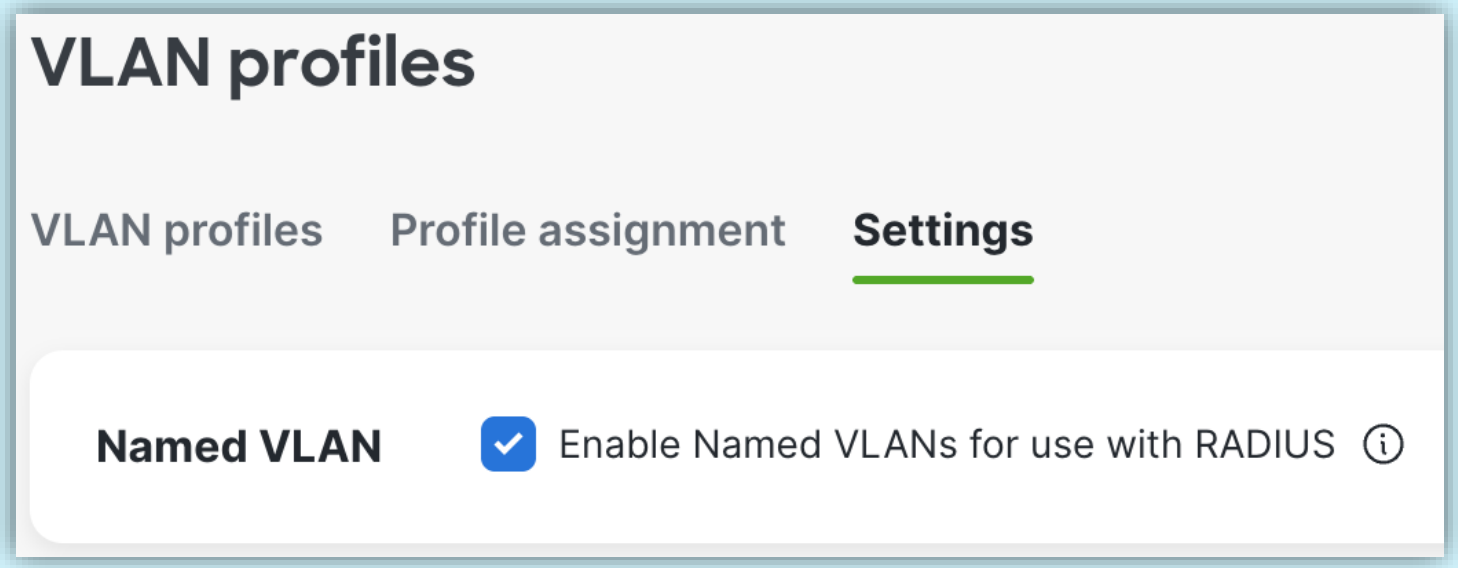
Network-Wide > VLAN Profiles



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

Dynamic VLAN – Meraki VLAN Profiles

Network-Wide > VLAN Profiles



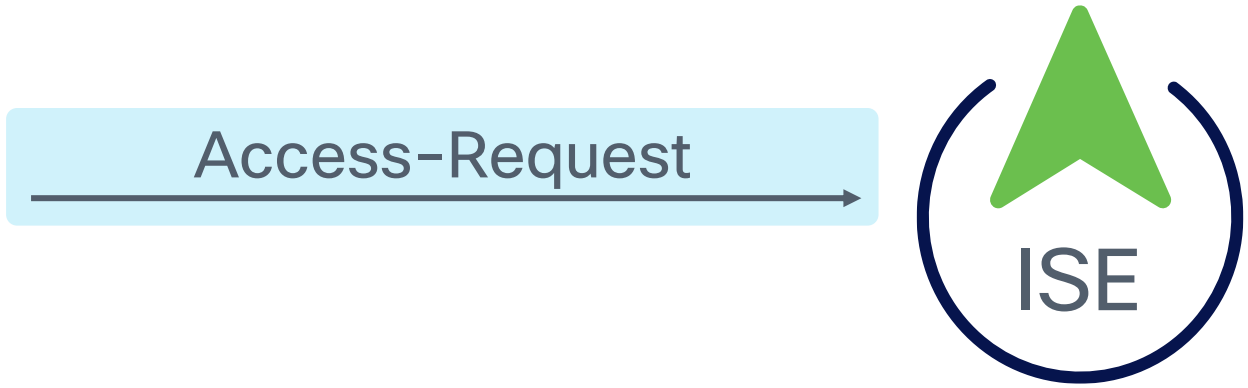
⚠ Must enable Named VLANs for use with RADIUS

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

Named ACLs – ISE Configuration

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

Named ACLs – ISE Configuration



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

Named ACLs – ISE Configuration

Access-Request

Access-Accept

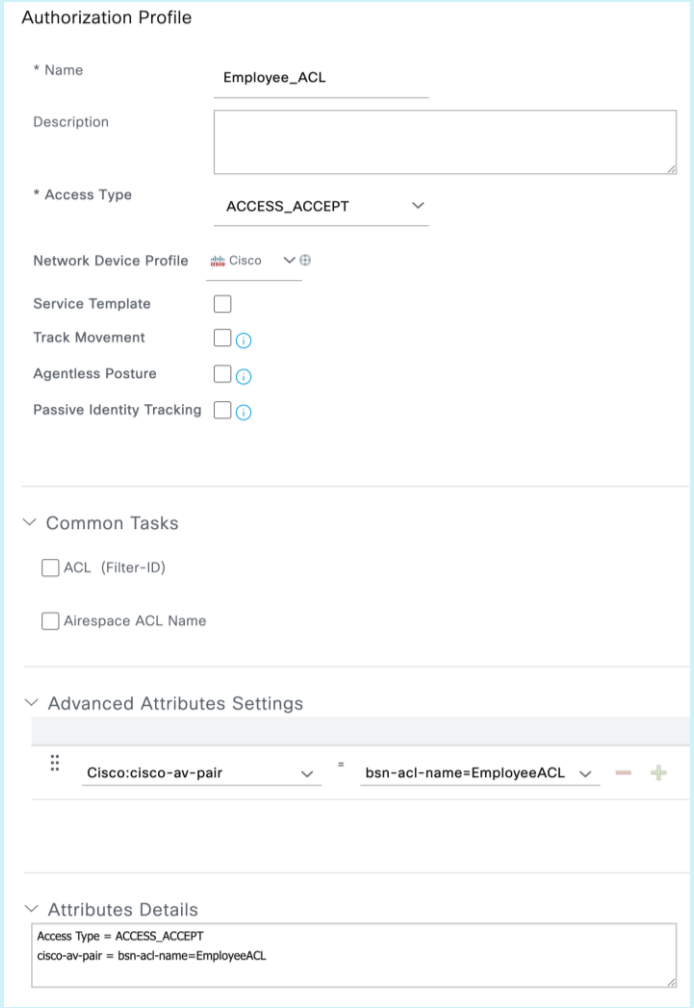
+

“Use ACL EmployeeACL”

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

Named ACLs – ISE Configuration

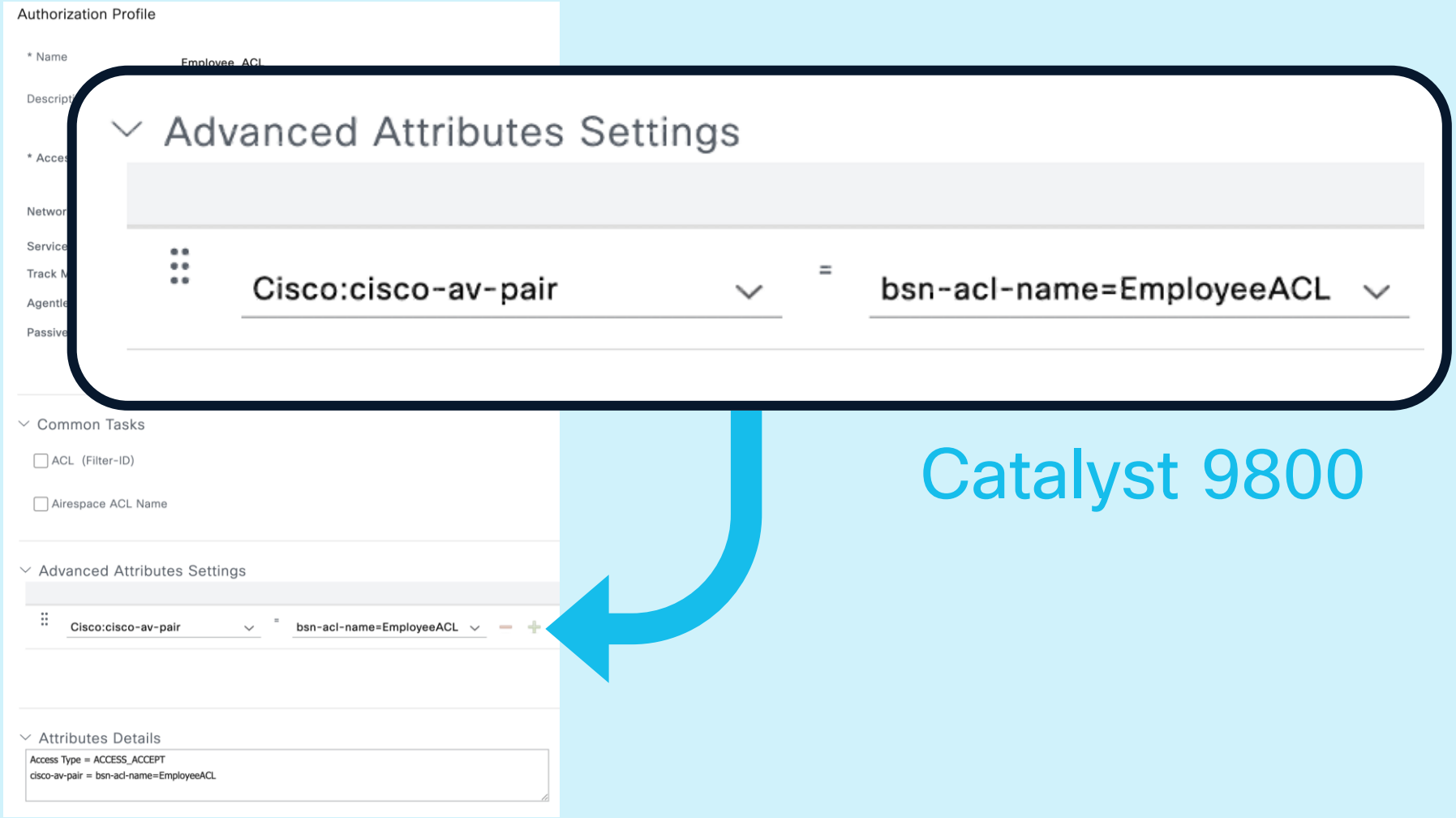
Policy > Policy Elements > Results > Authorization



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

Named ACLs – ISE Configuration

Policy > Policy Elements > Results > Authorization

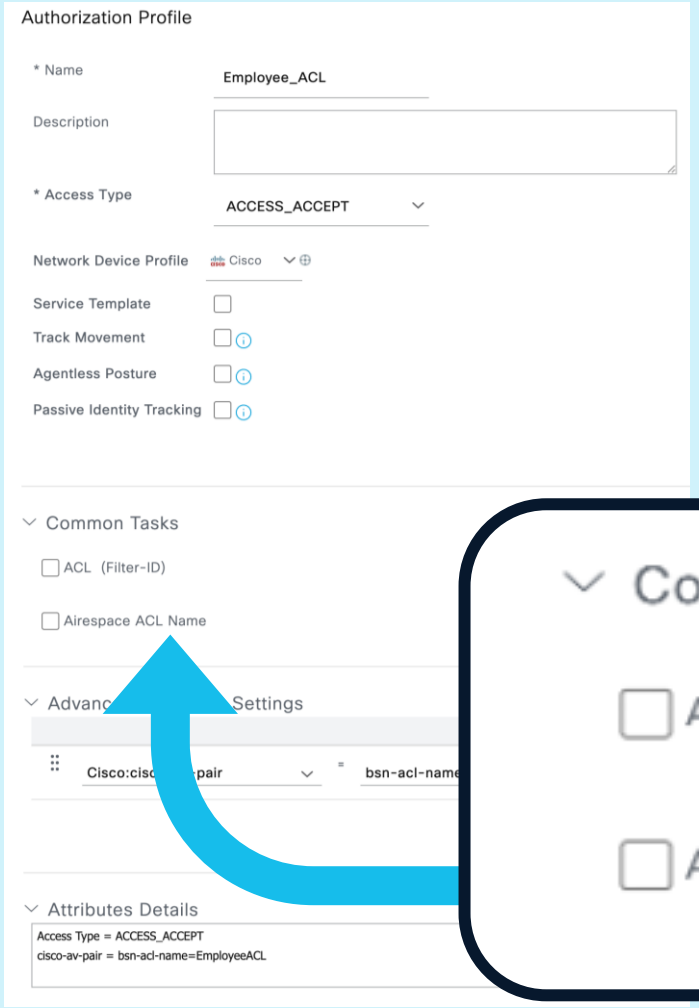


Catalyst 9800

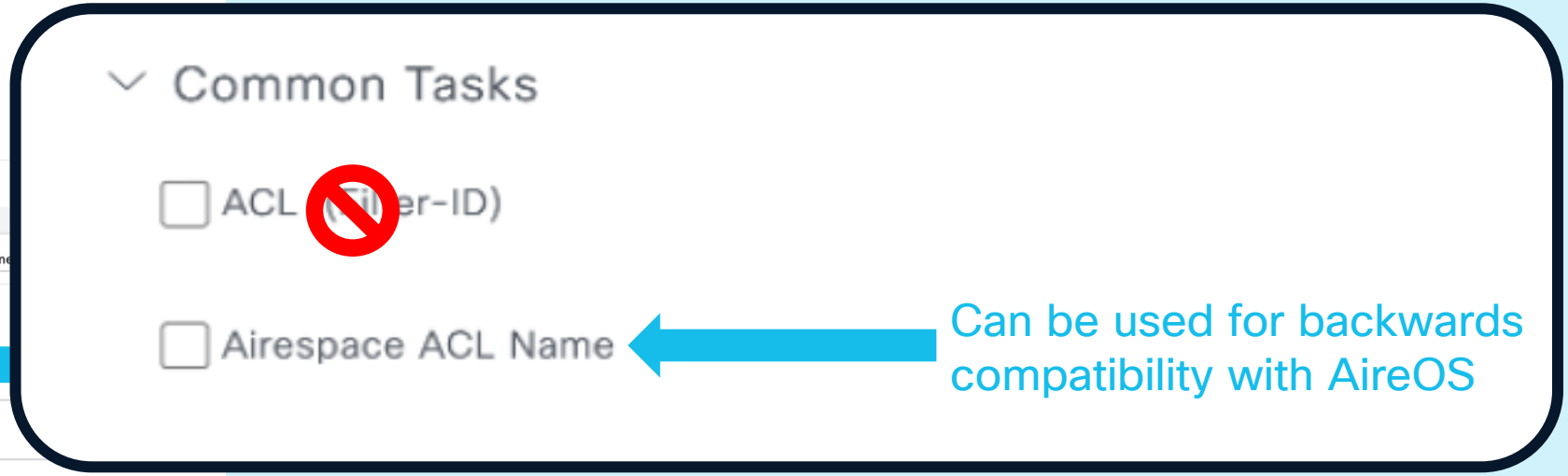
© 2025 Cisco and/or its affiliates. All rights reserved.

Named ACLs – ISE Configuration

Policy > Policy Elements > Results > Authorization



Catalyst 9800

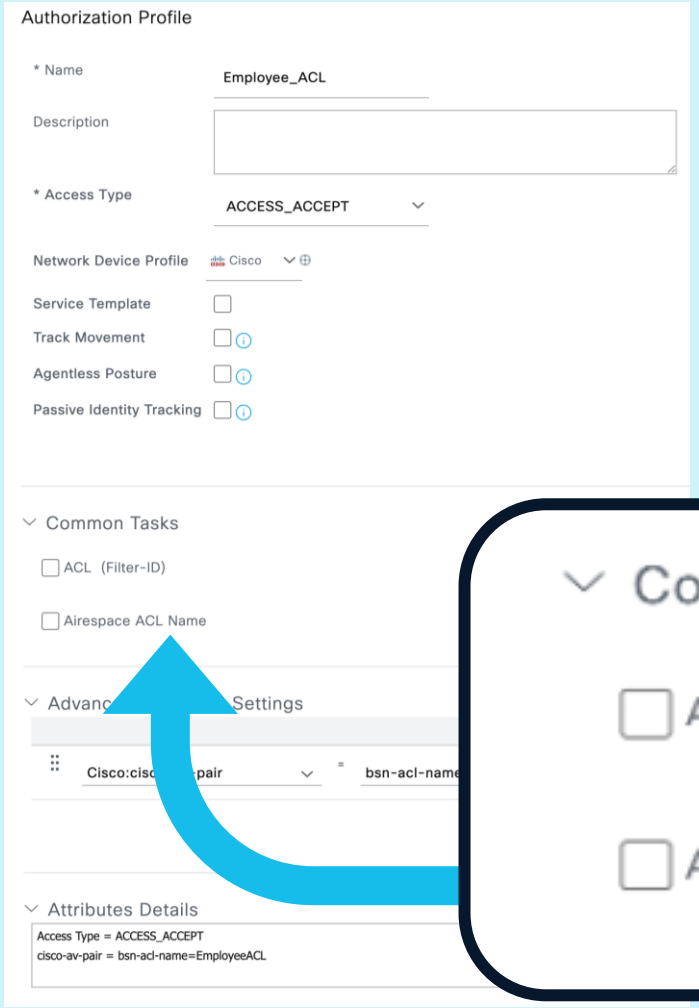


Can be used for backwards compatibility with AireOS

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

Named ACLs – ISE Configuration

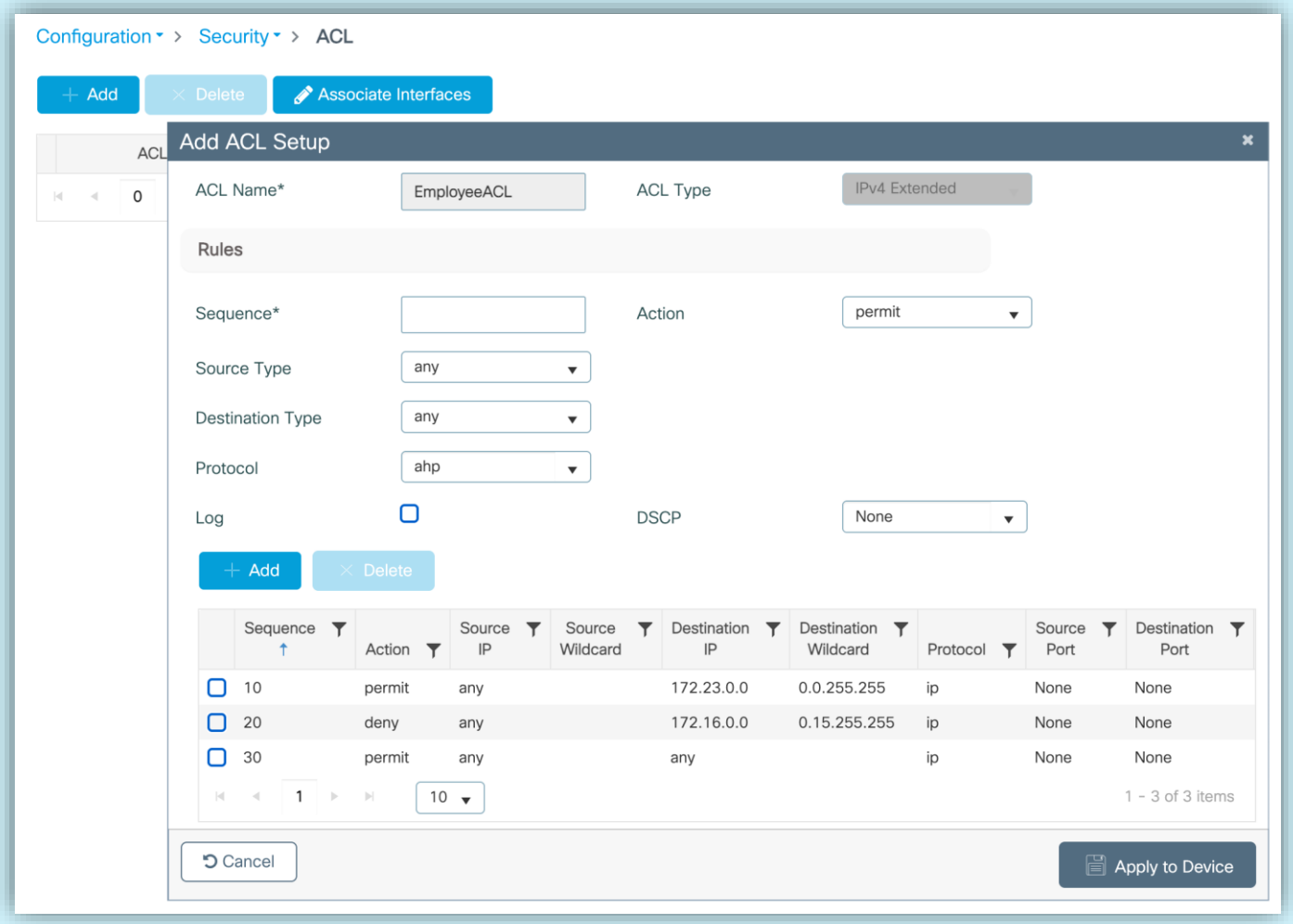
Policy > Policy Elements > Results > Authorization



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

Named ACLs – Catalyst 9800

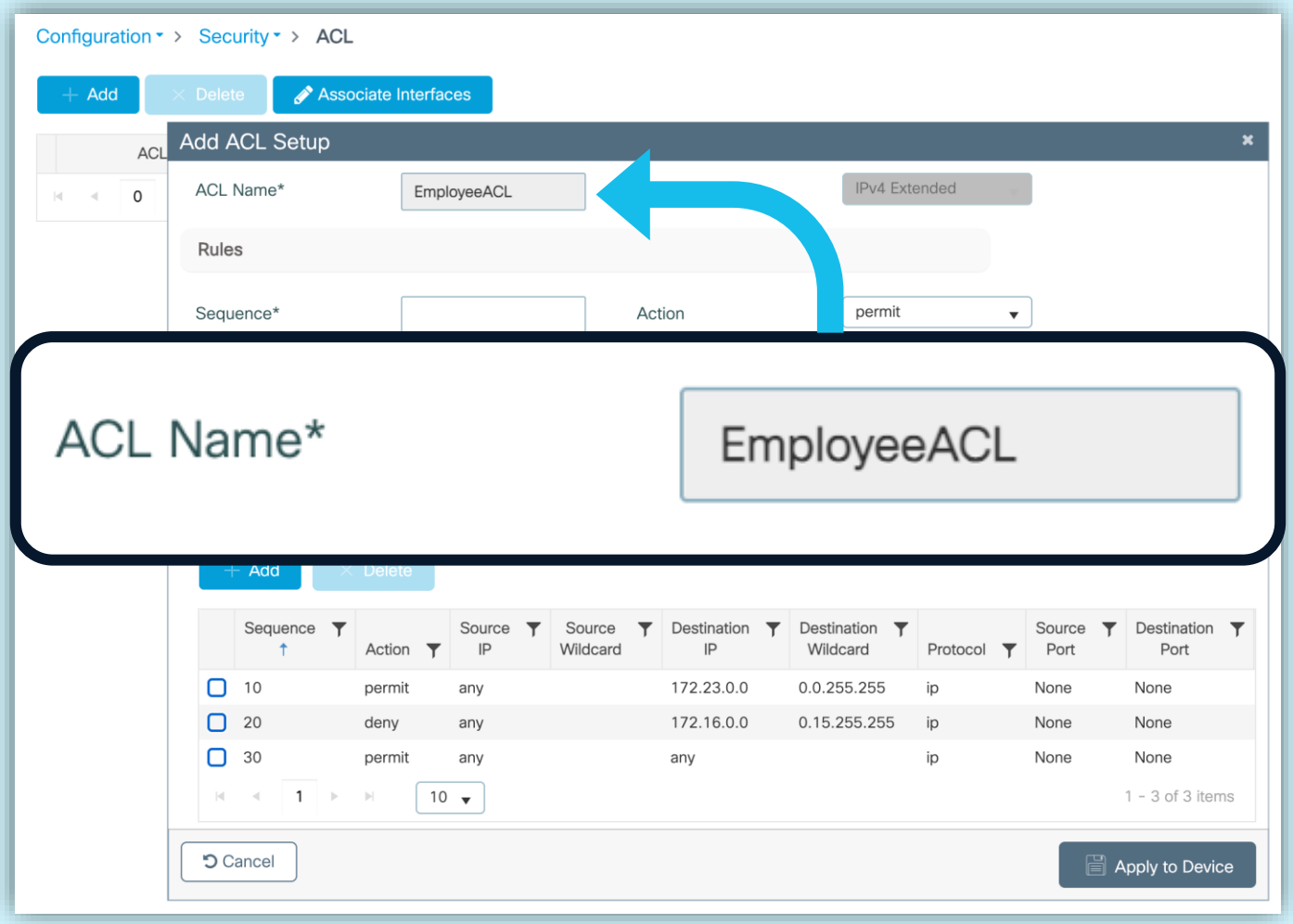
Configuration > Security > ACL



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

Named ACLs – Catalyst 9800

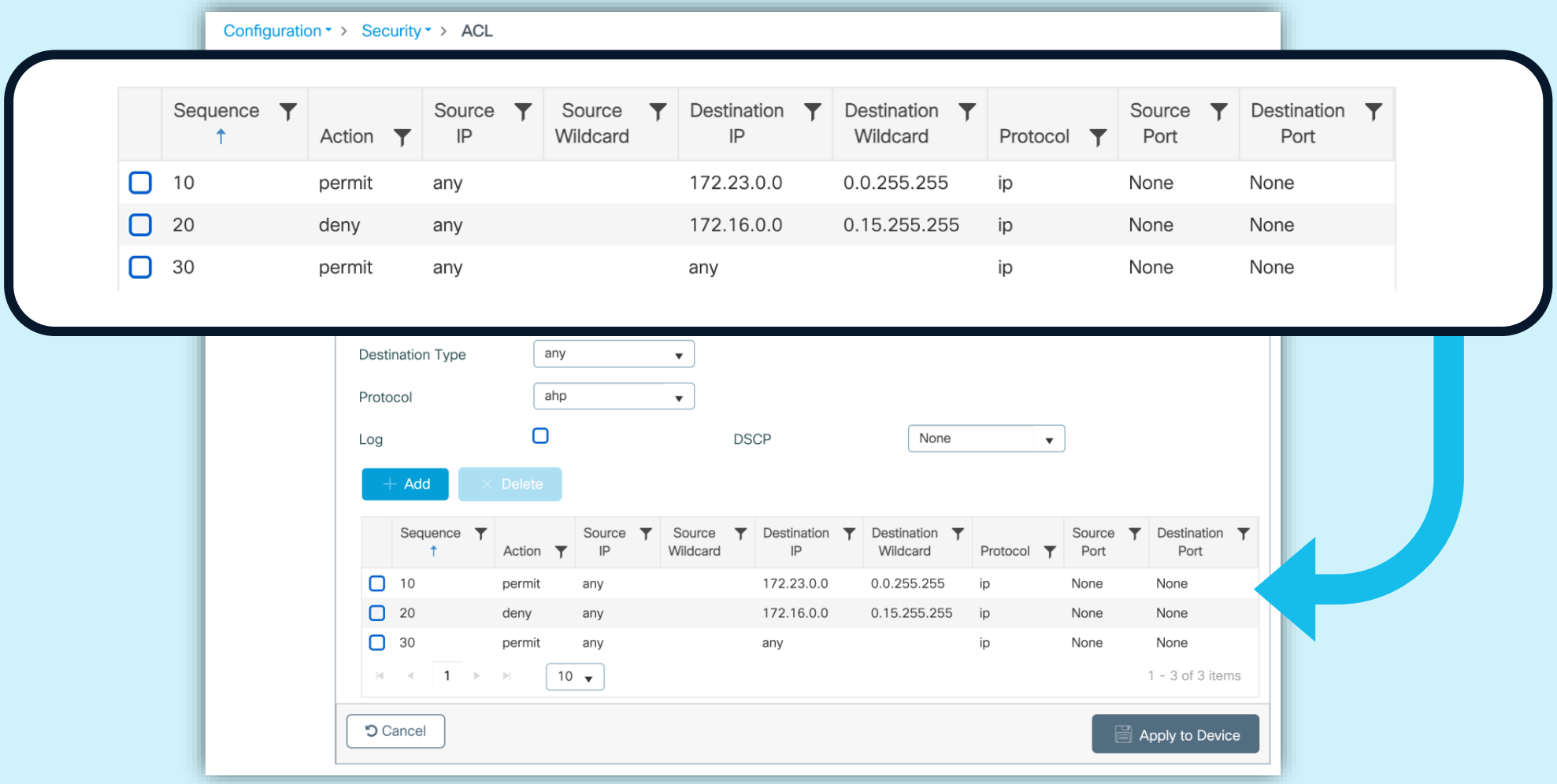
Configuration > Security > ACL



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

Named ACLs – Catalyst 9800

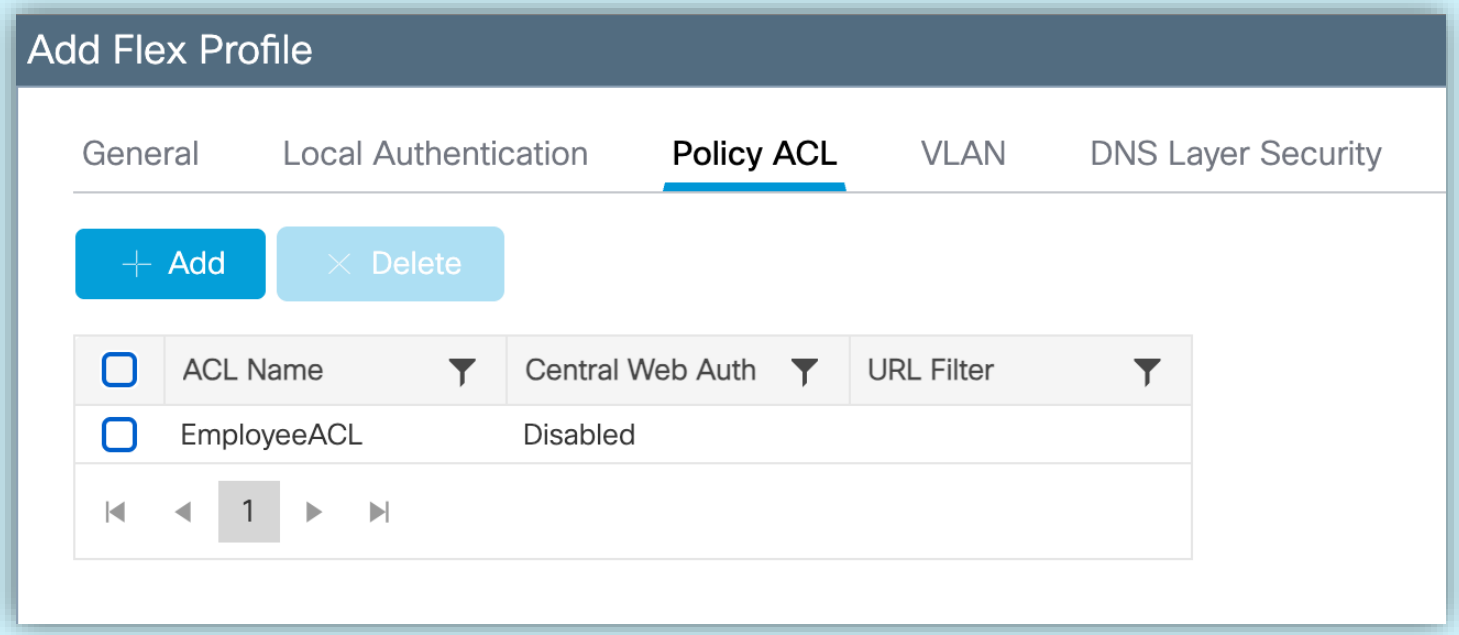
Configuration > Security > ACL



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

Named ACLs – Catalyst 9800

Configuration > Tags & Profiles > Flex



If using Flexconnect ACLs need to be added to Flex Profile

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

Catalyst 9800 dACL

Authentication

Authorization

Access-Accept
dACL name
Method-List

Access-Request
dACL name

Access-Accept
dACL

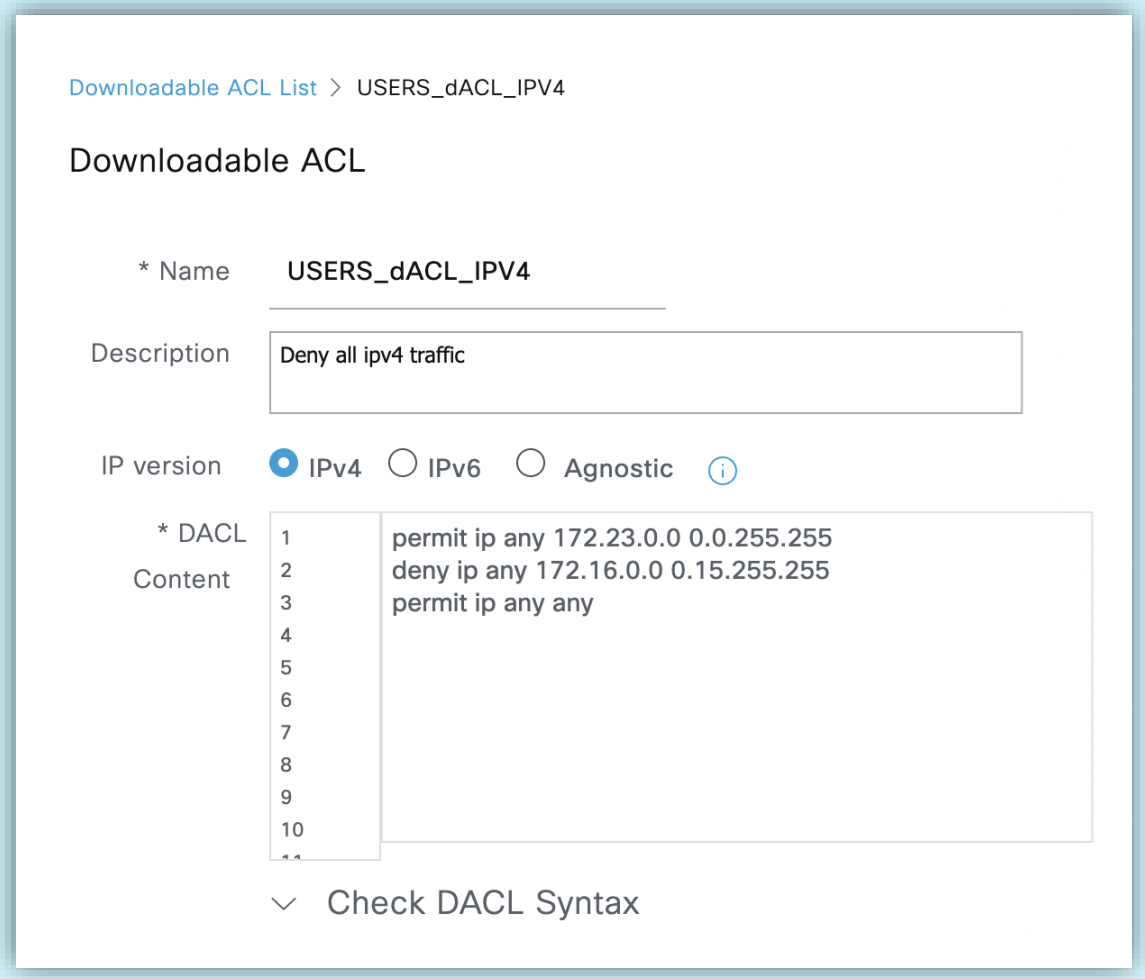
```
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xb7 (183)
    Length: 144
    Authenticator: dc0633f0d1b4d01b7b5b95875ed585a8
    [The response to this request is in frame 85]
  Attribute Value Pairs
    AVP: t=NAS-IP-Address(4) l=6 val=172.23.57.71
    AVP: t=User-Name(1) l=38 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=434143533a6163313733393062544833534550414452 6f563650756d
    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:inacl#1=permit ip any 172.23.0.0 0.0.255.255
        Type: 1
        Length: 49
        Cisco-AVPair: ip:inacl#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:inacl#2=deny ip any 172.16.0.0 0.15.255.255
        Type: 1
        Length: 48
        Cisco-AVPair: ip:inacl#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:inacl#3=permit ip any any
        Type: 1
        Length: 30
        Cisco-AVPair: ip:inacl#3=permit ip any any
```

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

Catalyst 9800 dACL – ISE Configuration

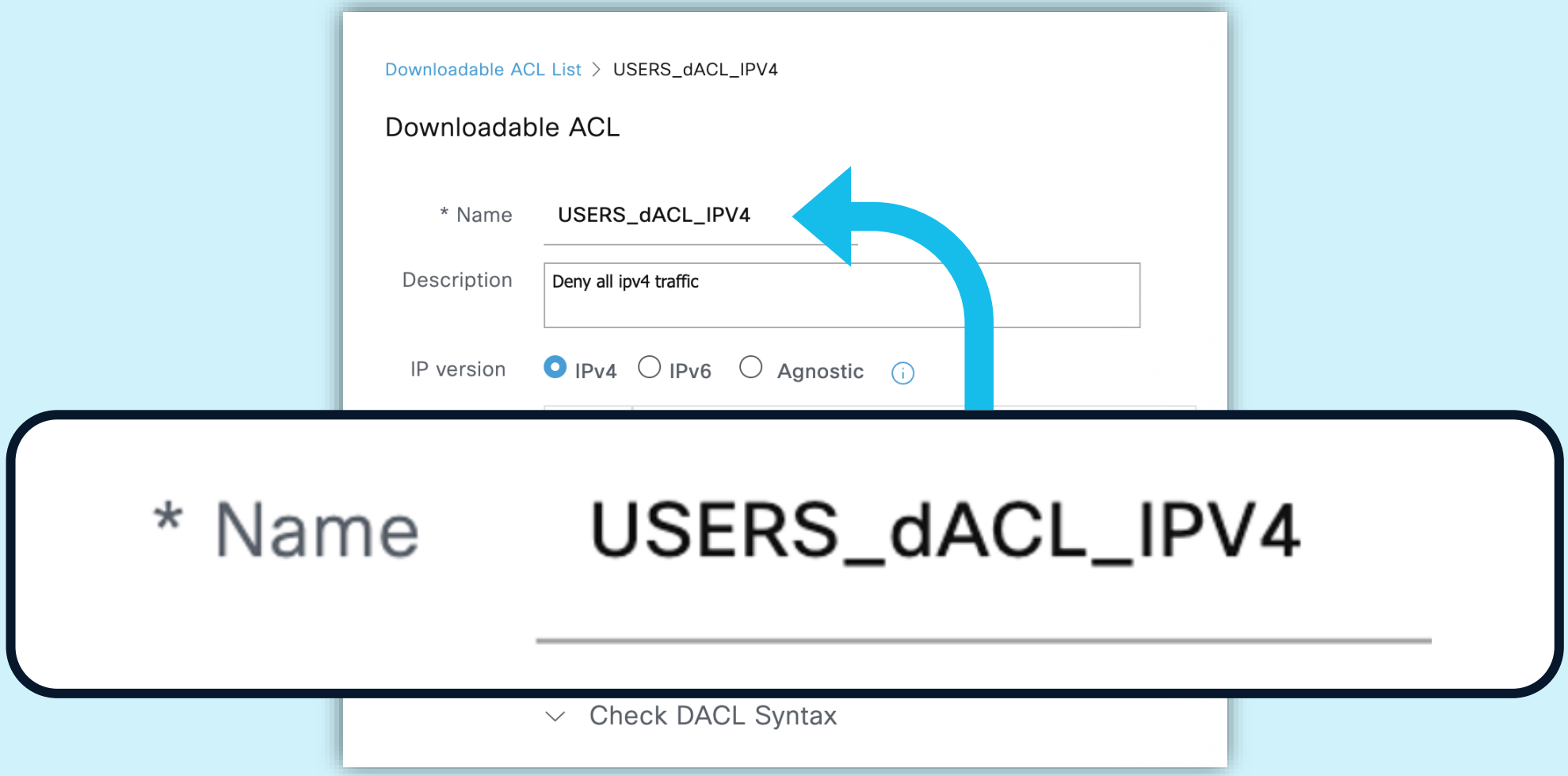
Policy > Policy Elements > Results > Authorization



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

Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization

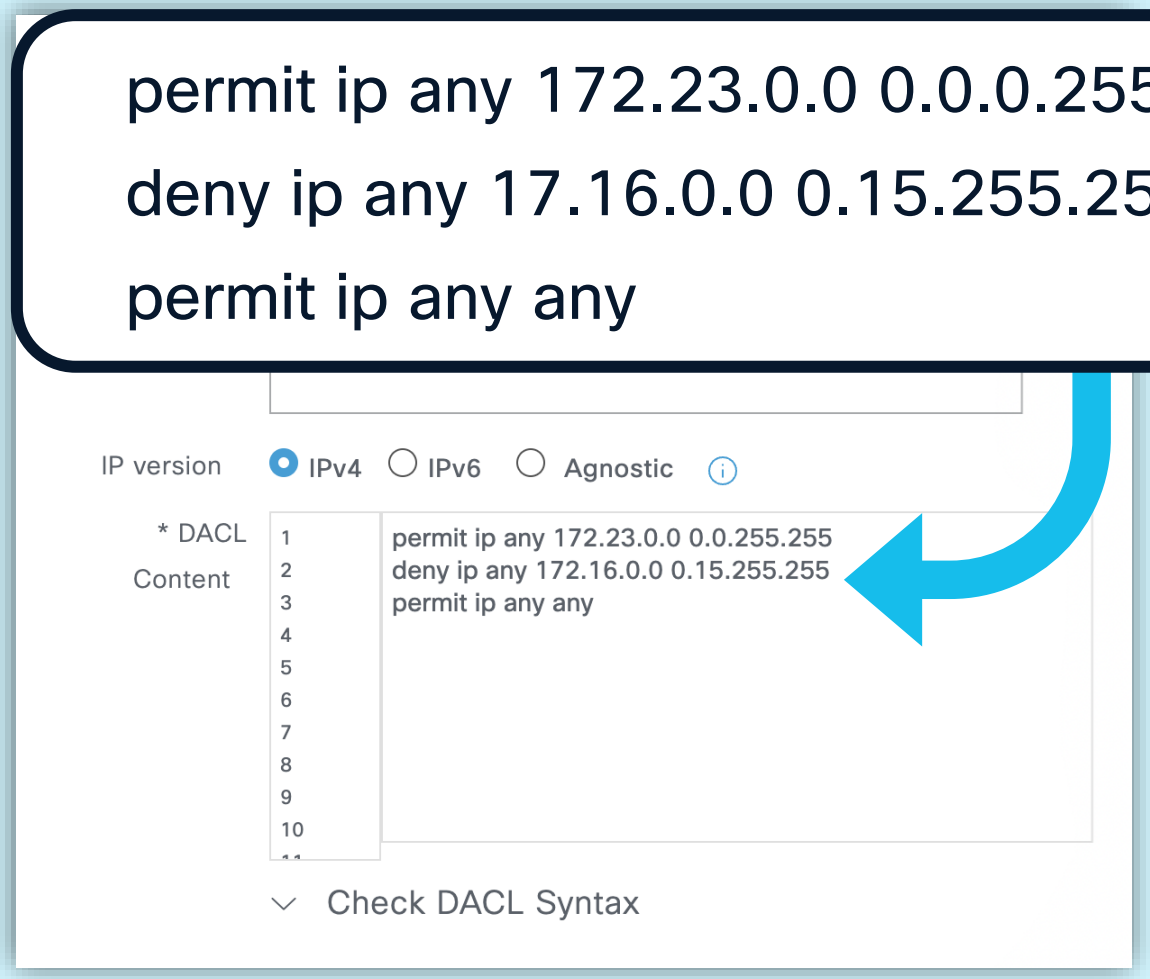


© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization

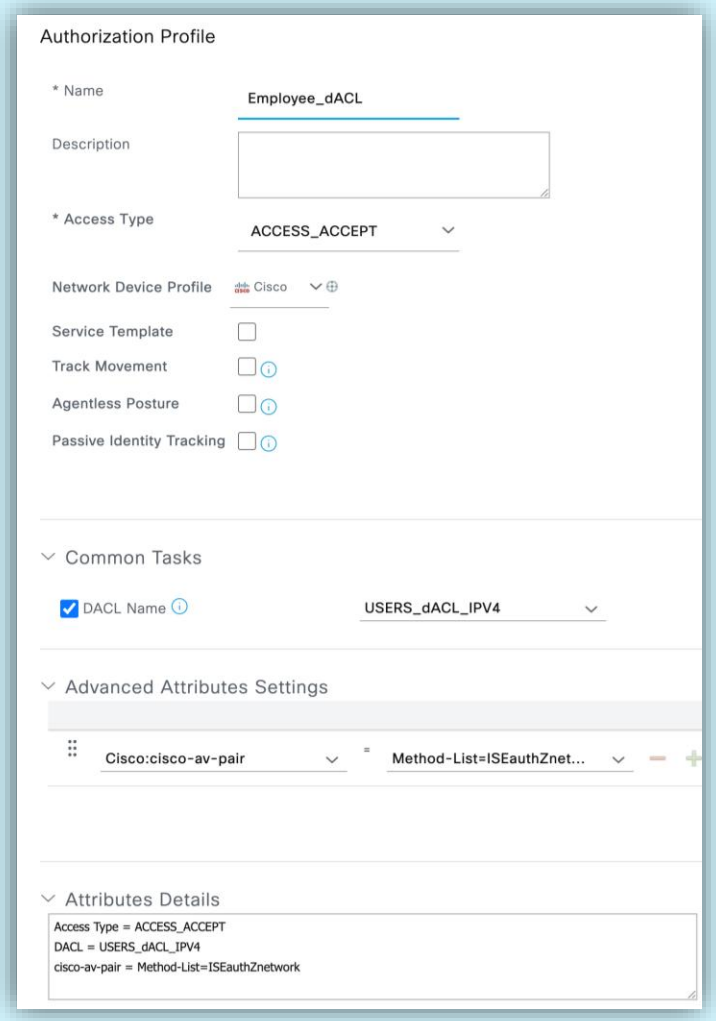
permit ip any 172.23.0.0 0.0.0.255
deny ip any 17.16.0.0 0.15.255.255
permit ip any any



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

Catalyst 9800 dACL – ISE Configuration

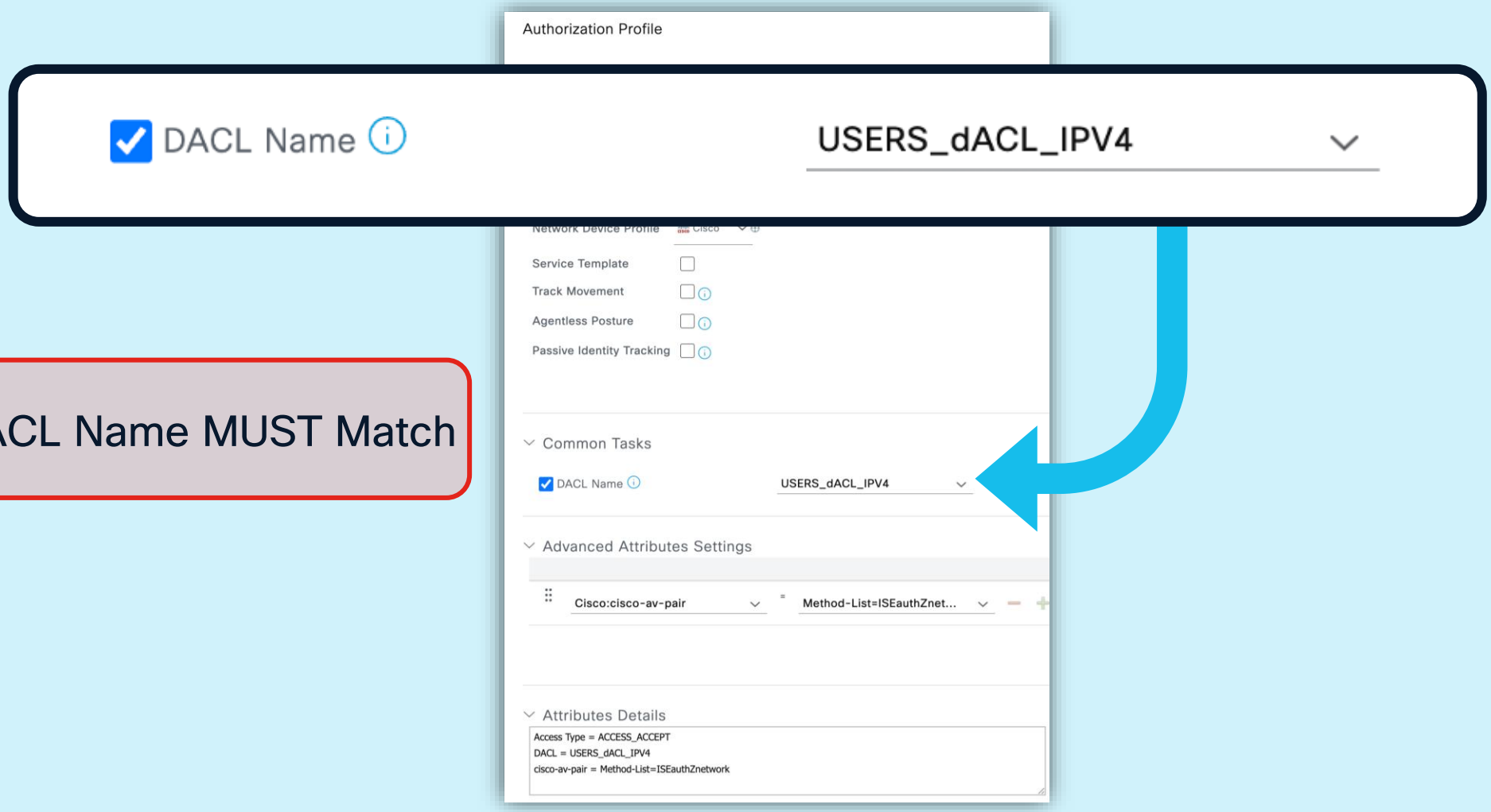
Policy > Policy Elements > Results > Authorization



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

Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization

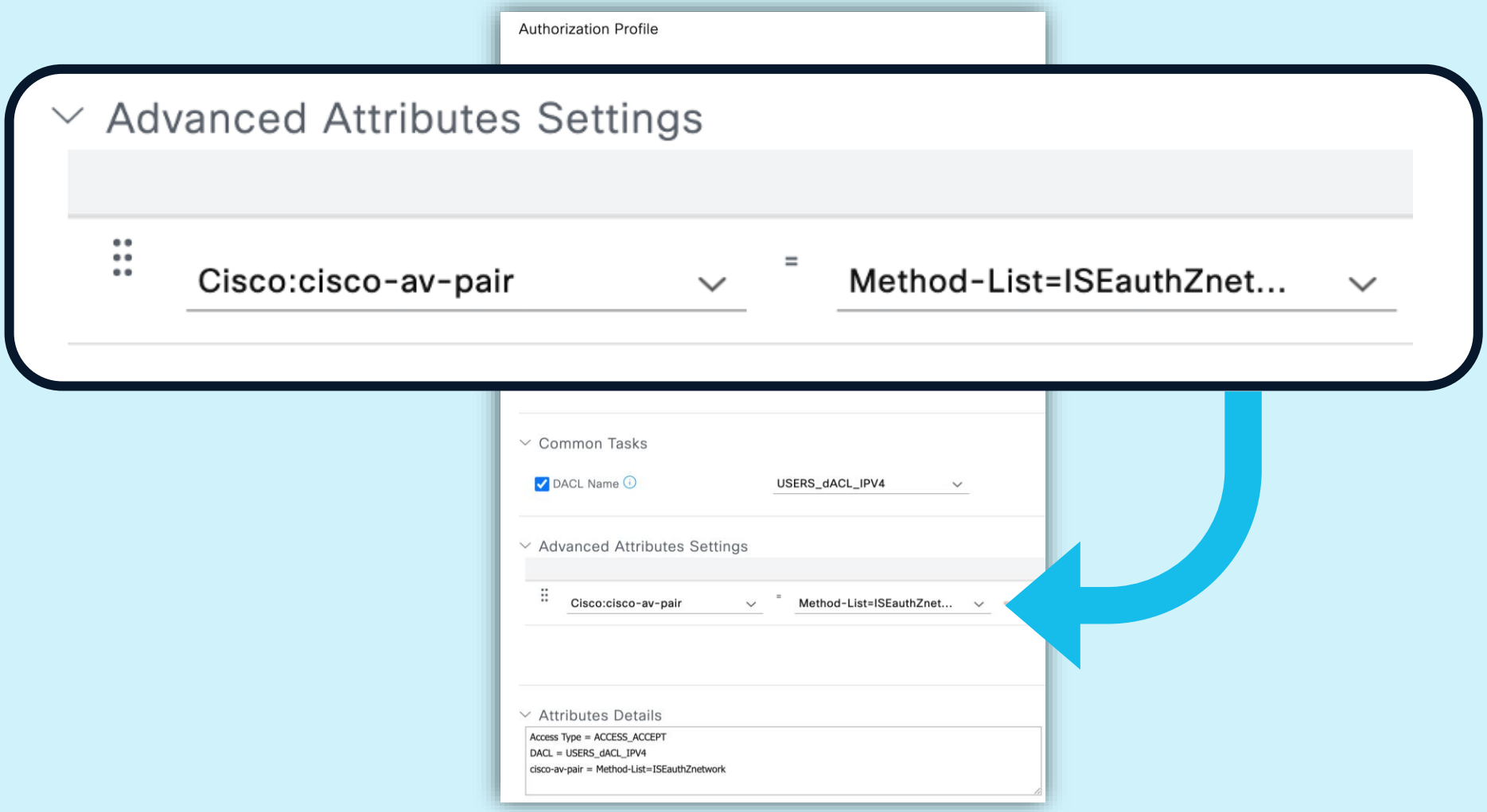


DACL Name MUST Match

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

Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization



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

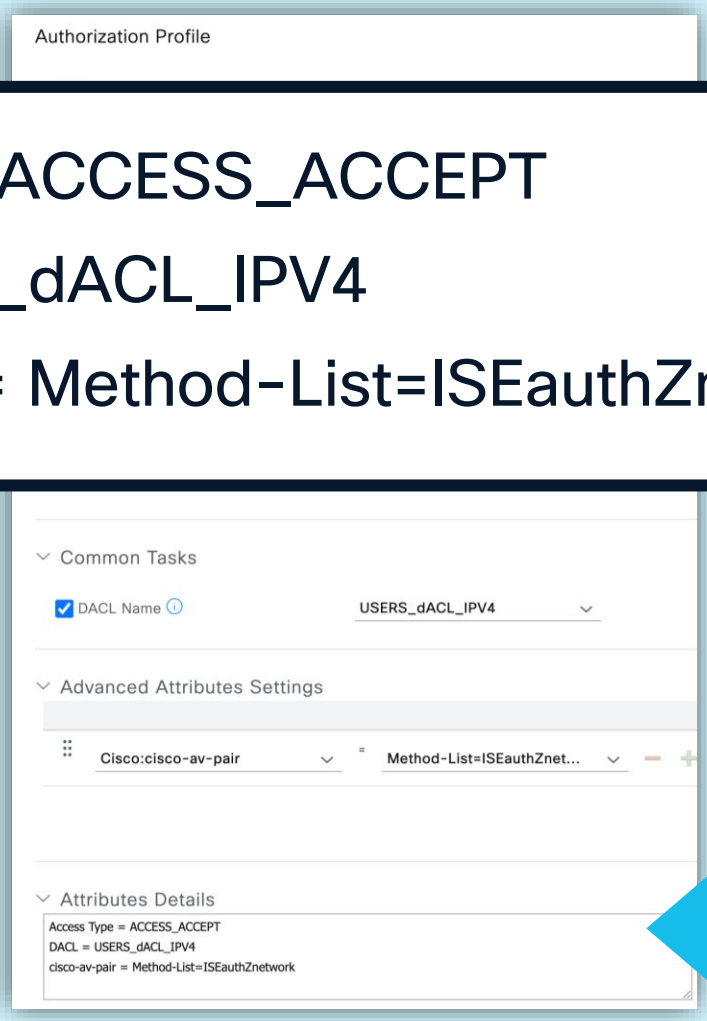
Catalyst 9800 dACL – ISE Configuration

Policy > Policy Elements > Results > Authorization

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

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

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

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

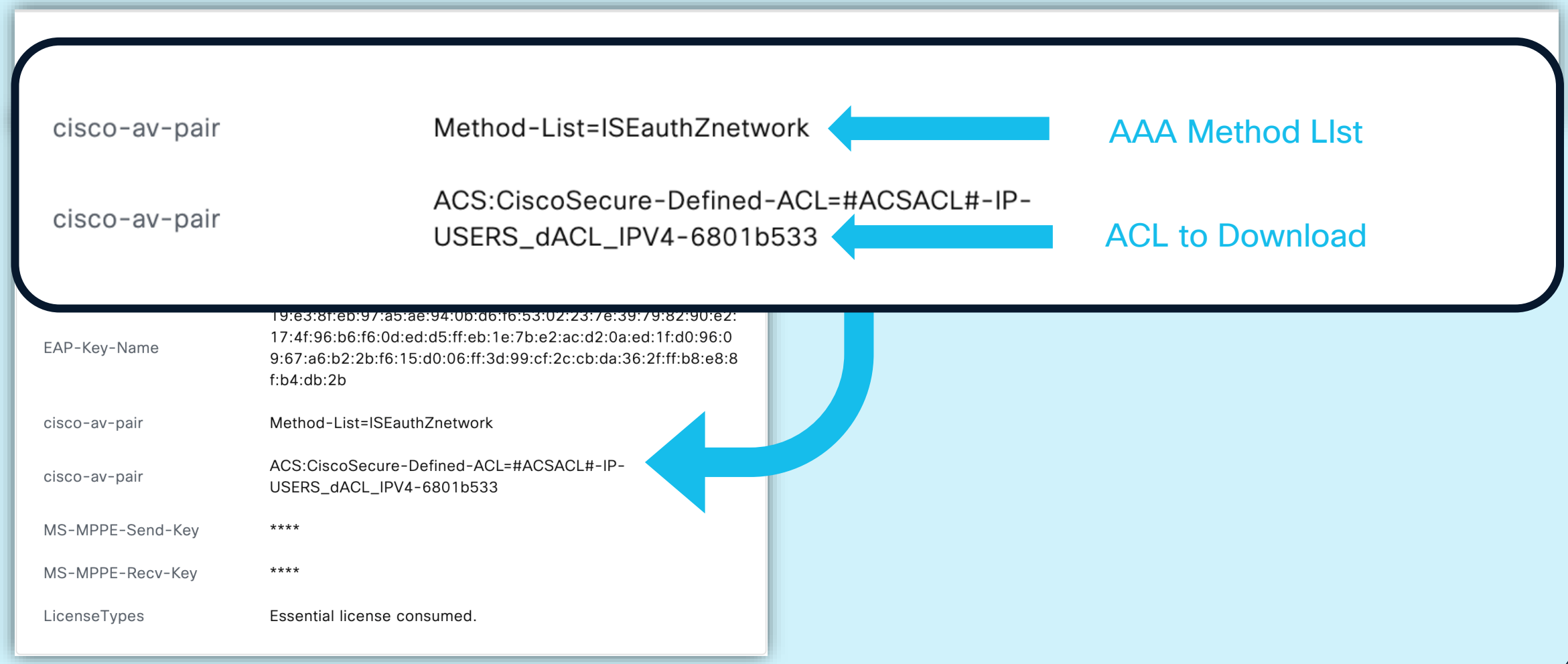
Catalyst 9800 dACL – Monitoring from ISE

Operations > RADIUS > Live Logs

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

Catalyst 9800 dACL – Monitoring from ISE

Operations > RADIUS > Live Logs



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

Catalyst 9800 dACL – Monitoring from ISE

Operations > RADIUS > Live Logs

Apr 17, 2025 09:17:20.9... #ACSACL#-IP-USERS_dACL_IPV4-6801b533

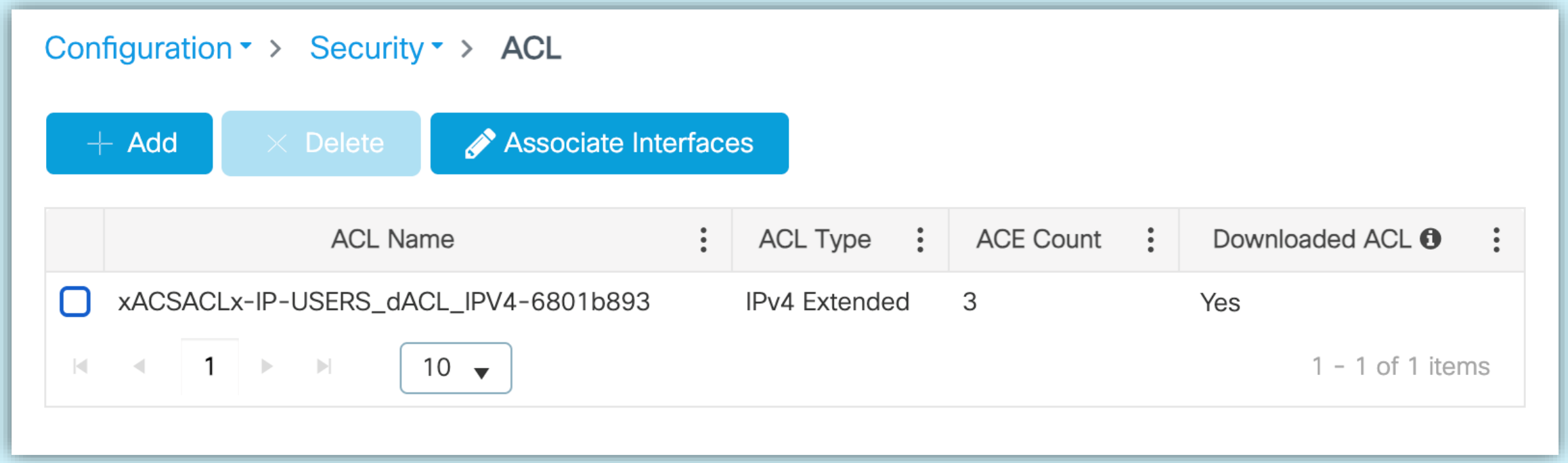
Result

Class	CACS:ac17390bziML77ZJGvJWjAuCNFTDinCnbPJnlsEAcG9ovR5_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

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

Catalyst 9800 dACL – Monitoring from 9800 Controller

Configuration > Security > ACL



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

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
```

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

cisco

Group Based Policy with Security Group Tags (SGT)

TrustSec / Adaptive Policy

Doctors SGT (20)

Scanners SGT (30)

Guests SGT (6)

Source \ Destination	Doctors	Scanners	App Servers	Guests
Doctors	✓	✗	✓	✗
Scanners	✗	✗	✓	✗
App Servers	✓	✓	✓	✗
Guests	✗	✗	✗	✗

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

What's the Business Intent Here?

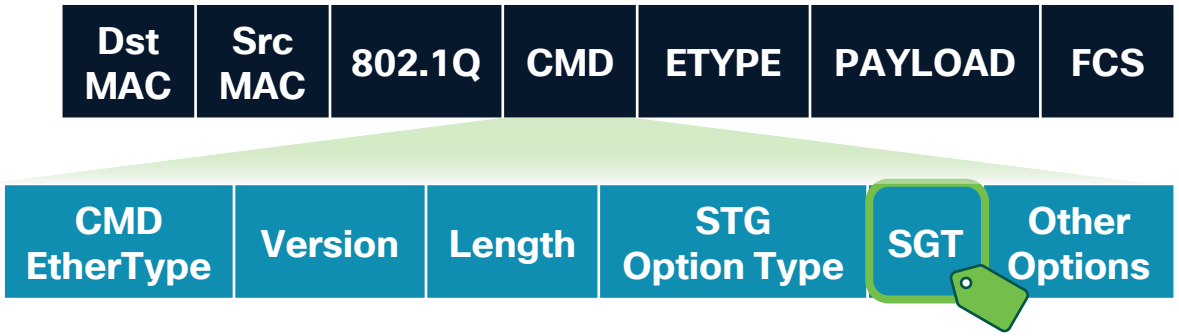
```
CNLAB-PX-SW3#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 30:Scanners to group 40:App_Servers:
        Permit IP-00
IPv4 Role-based permissions from group 6:Guests to group 40:App_Servers:
        Deny IP-00
IPv4 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
```

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

Security Group Tags (SGT)

INLINE

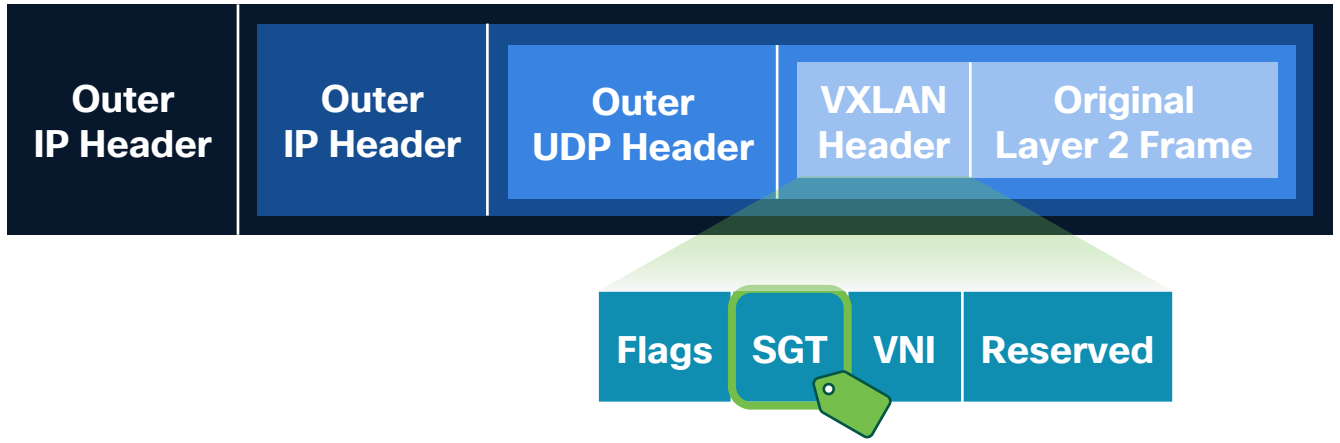


Catalyst
- Local
- Flexconnect

Meraki

TUNNELED

VXLAN FABRIC



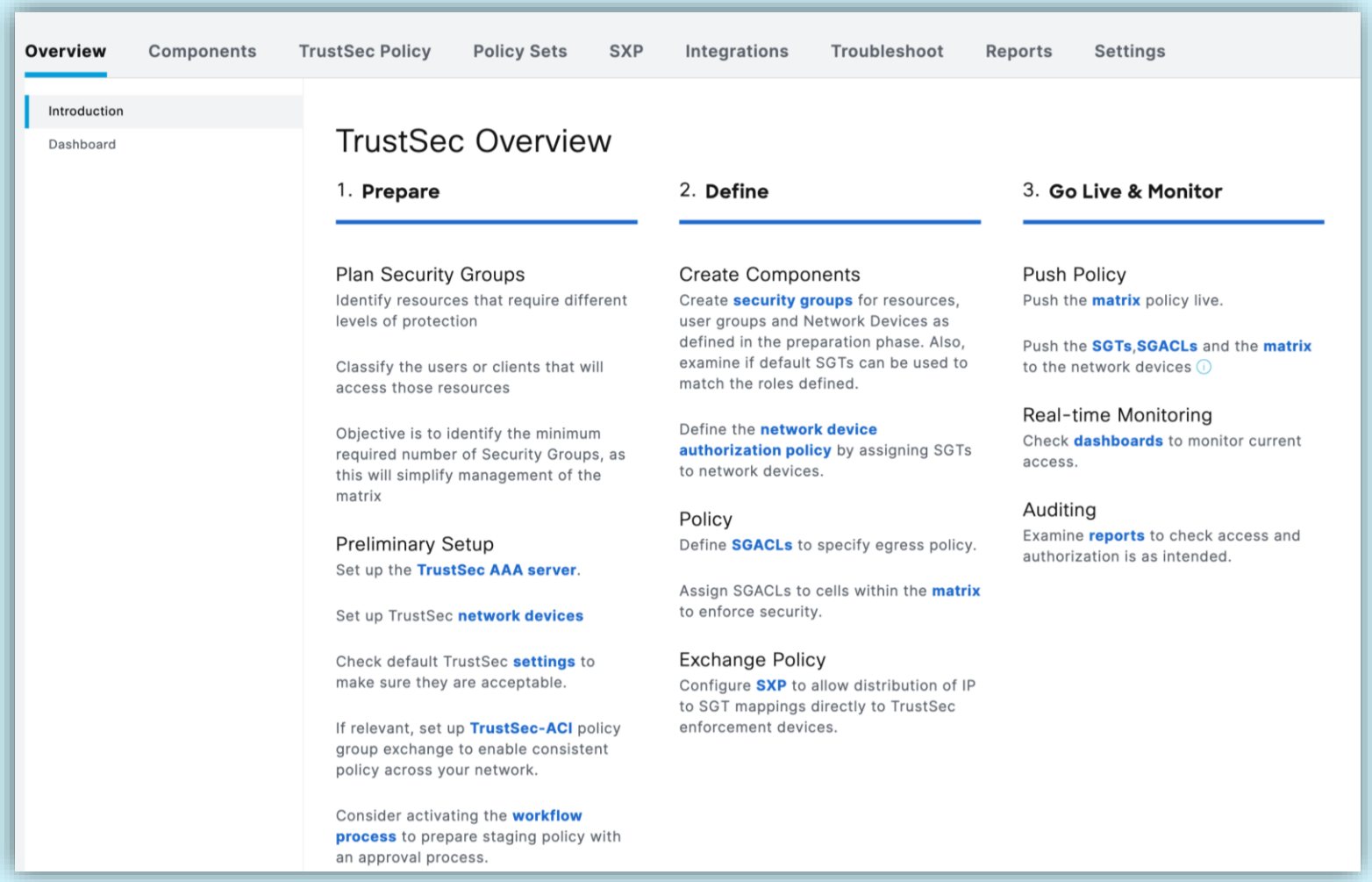
Catalyst
- Fabric Enabled Wireless

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

cisco

ISE - TrustSec

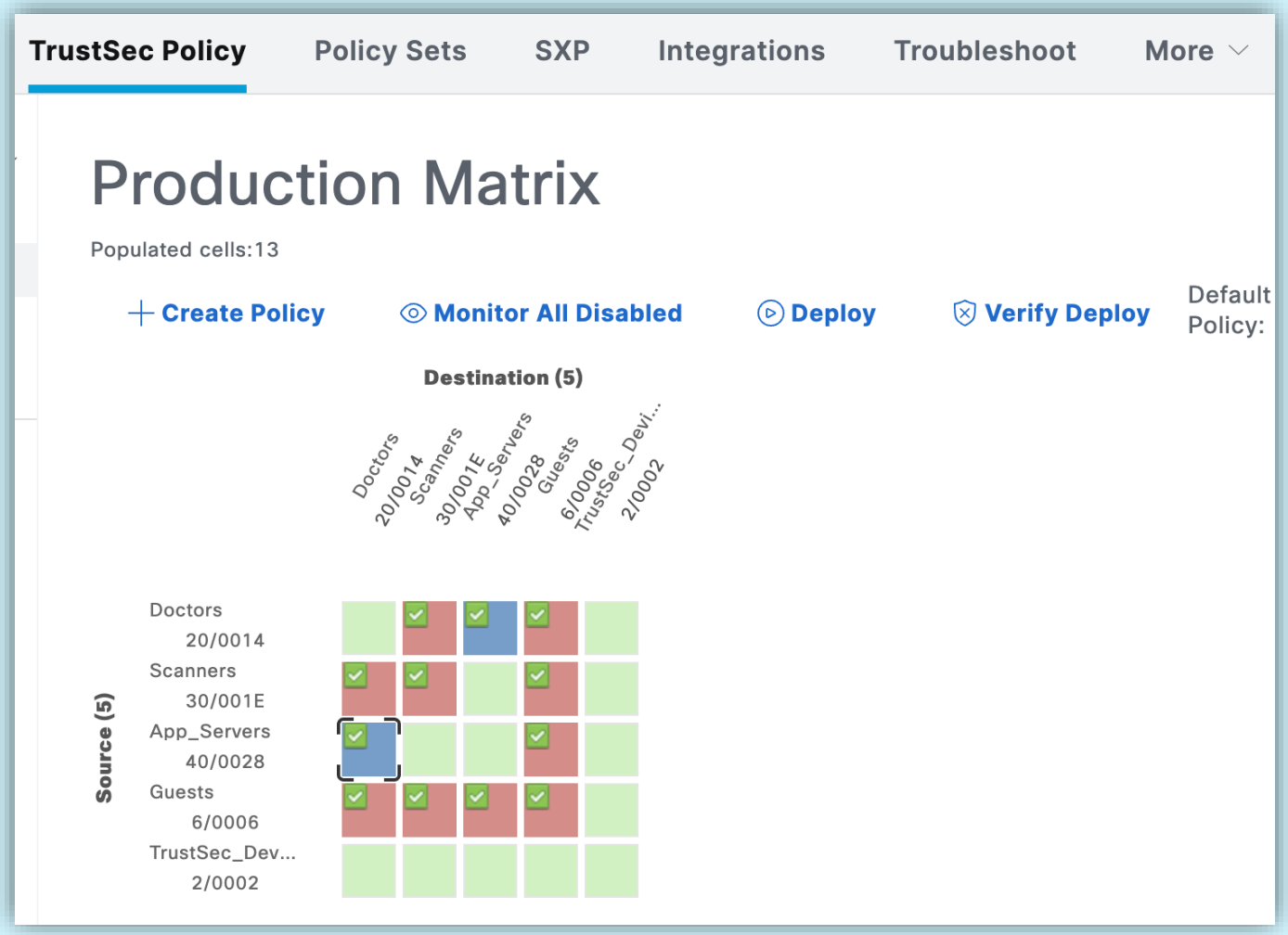
Work Centers > TrustSec > Overview



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

ISE - TrustSec Policy

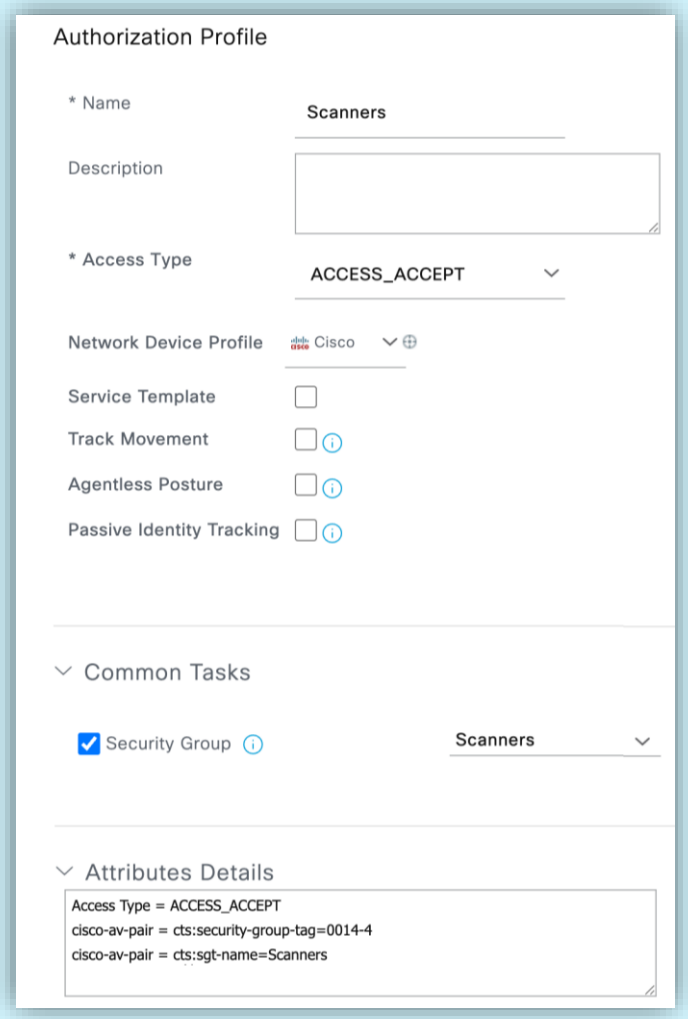
Work Centers > TrustSec > TrustSec Policy



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

ISE - Assign SGTs

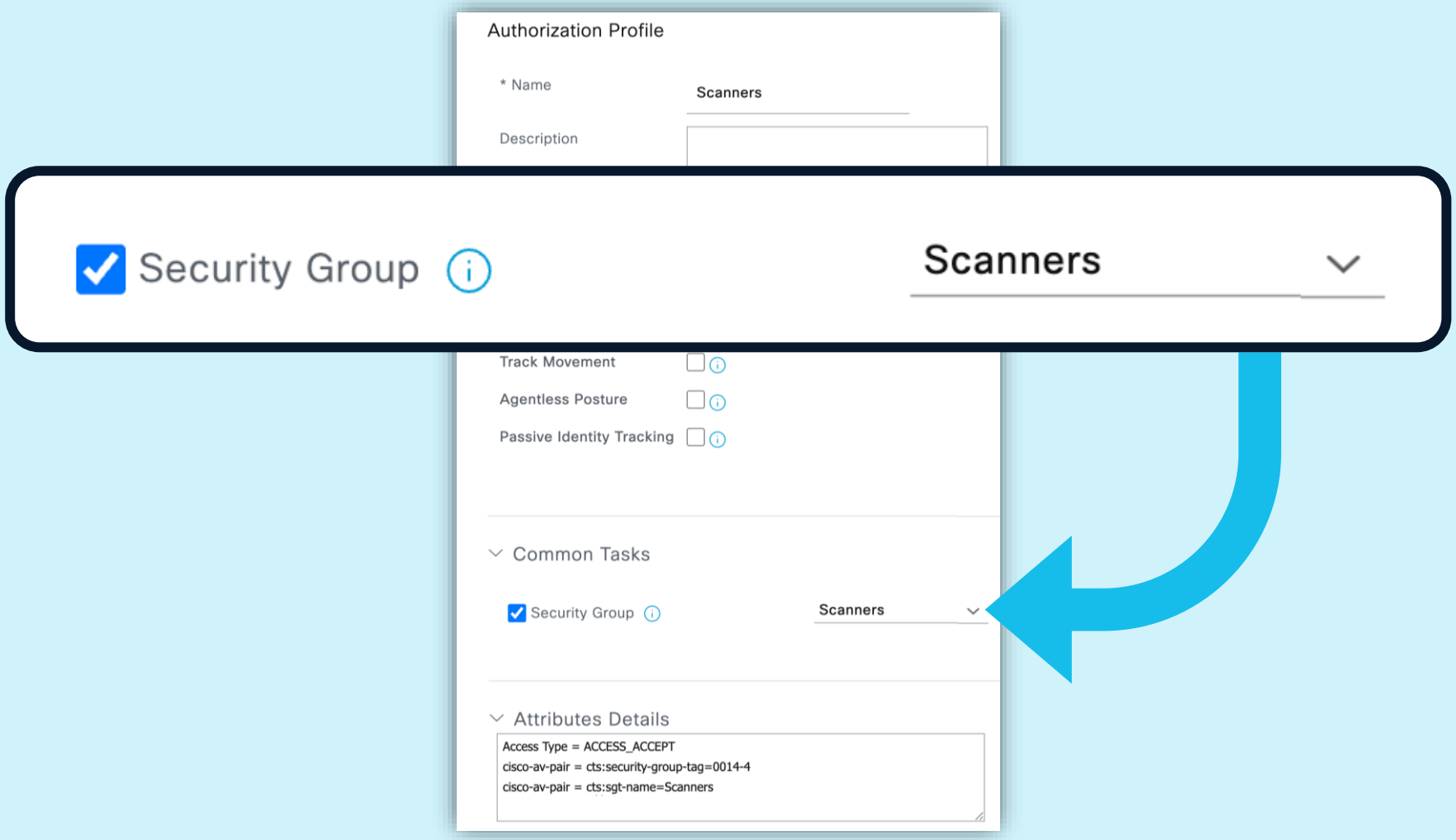
Policy > Policy Elements > Results > Authorization Profile



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

ISE - Assign SGTs via Authorization Profile

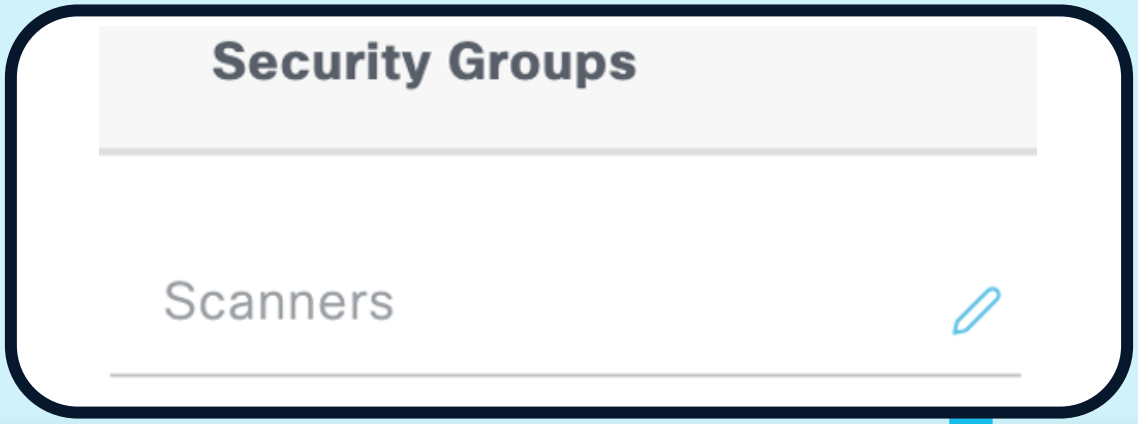
Policy > Policy Elements > Results > Authorization Profile



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

ISE - Assign SGTs via Authorization Policy

Policy > Policy Sets > Authorization Policy



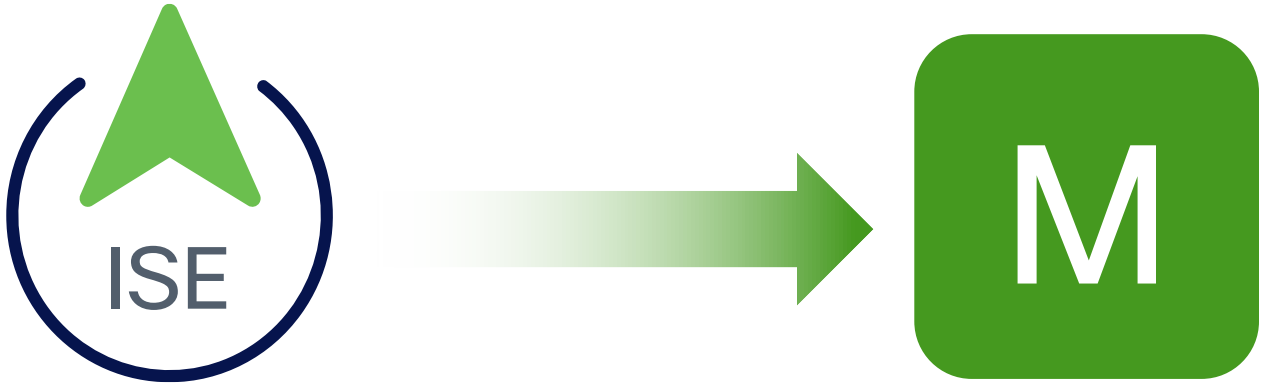
Authorization Policy

	Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups
	✓	Scanners	AND Radius·Called-Station-ID **ENDS_WITH** PX-PSK IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Scanners	PermitAccess	Scanners

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

cisco

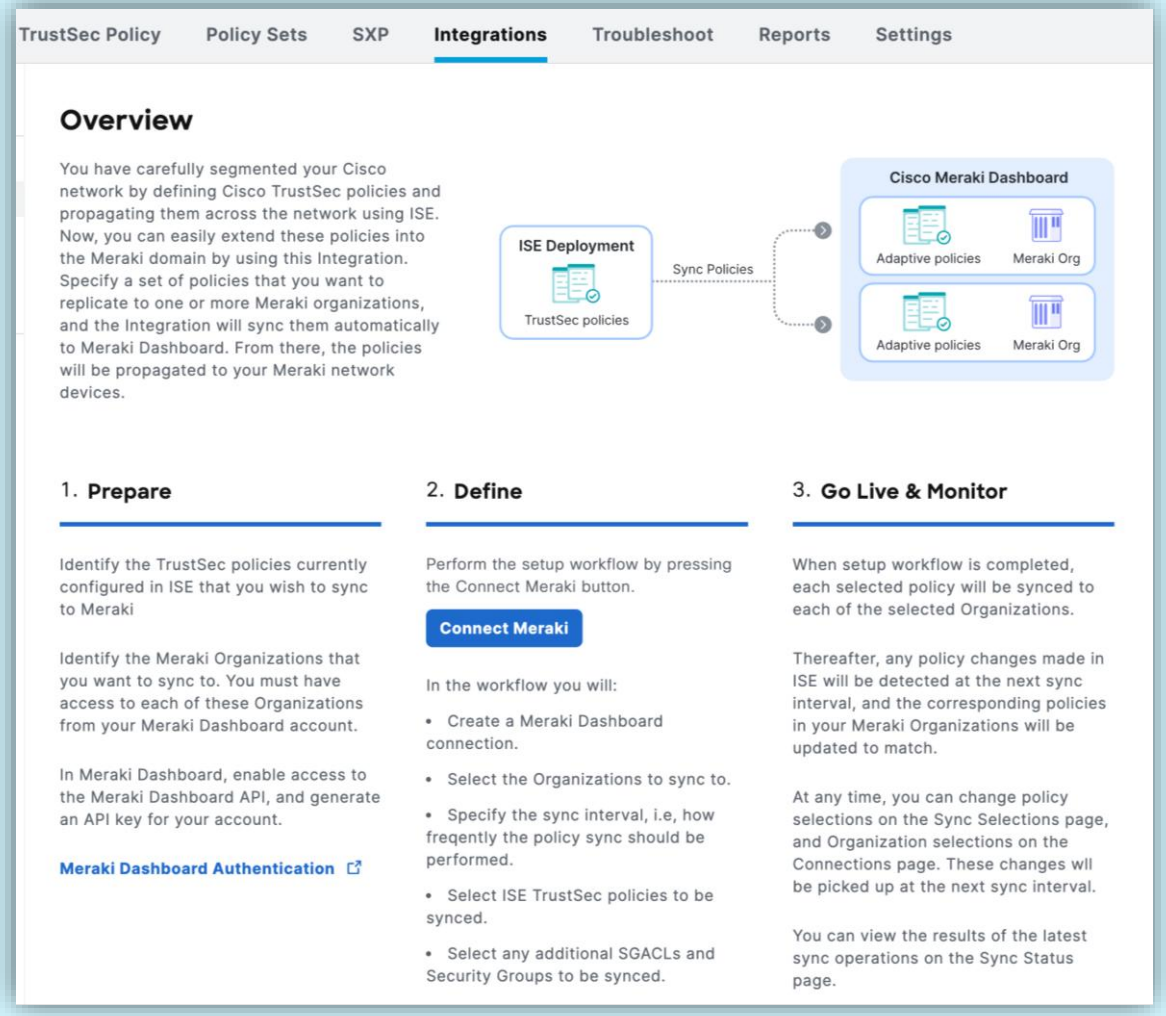
Integration of ISE with Meraki



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

Integration of ISE with Meraki

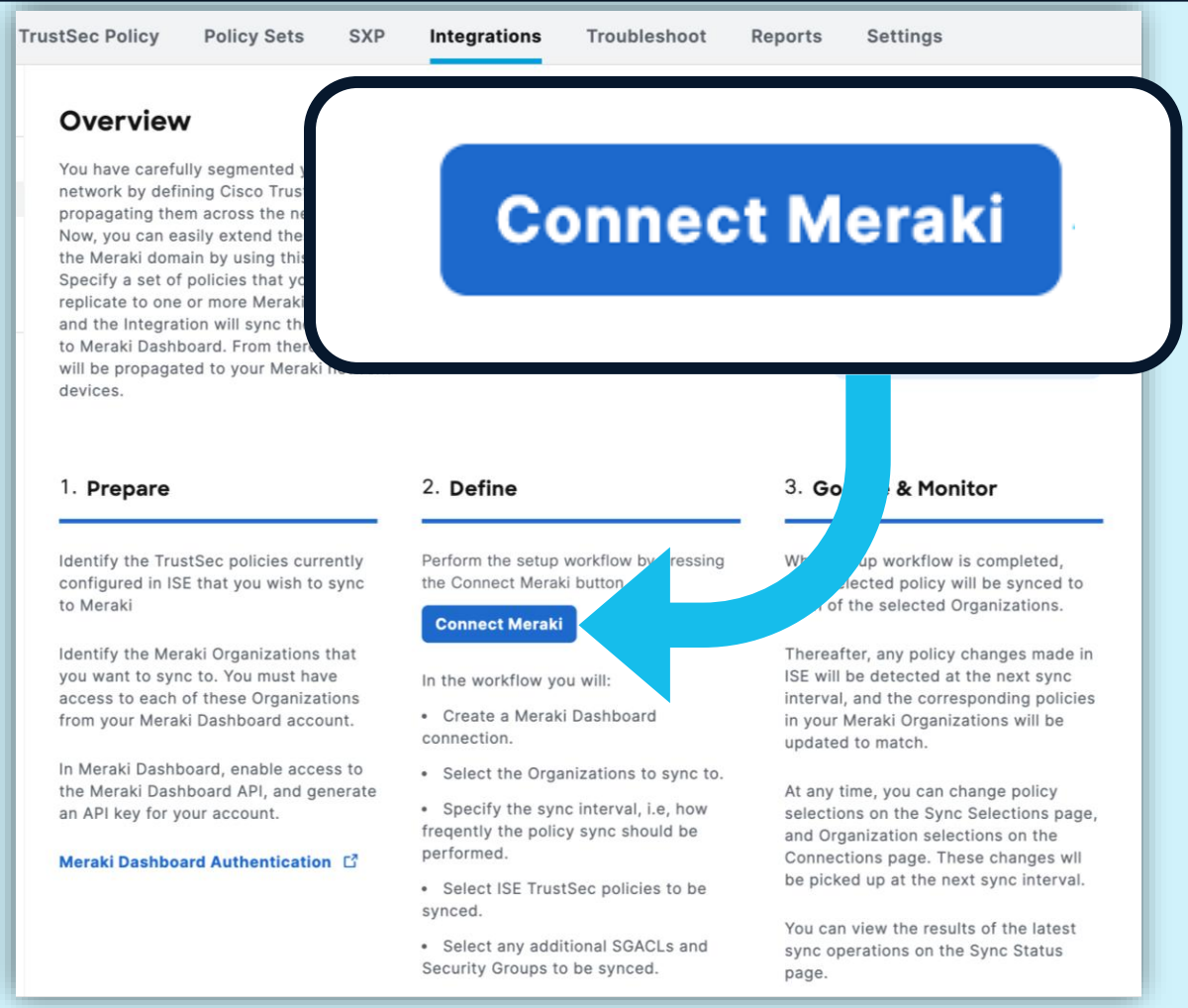
Work Centers > TrustSec > Integrations



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

Integration of ISE with Meraki

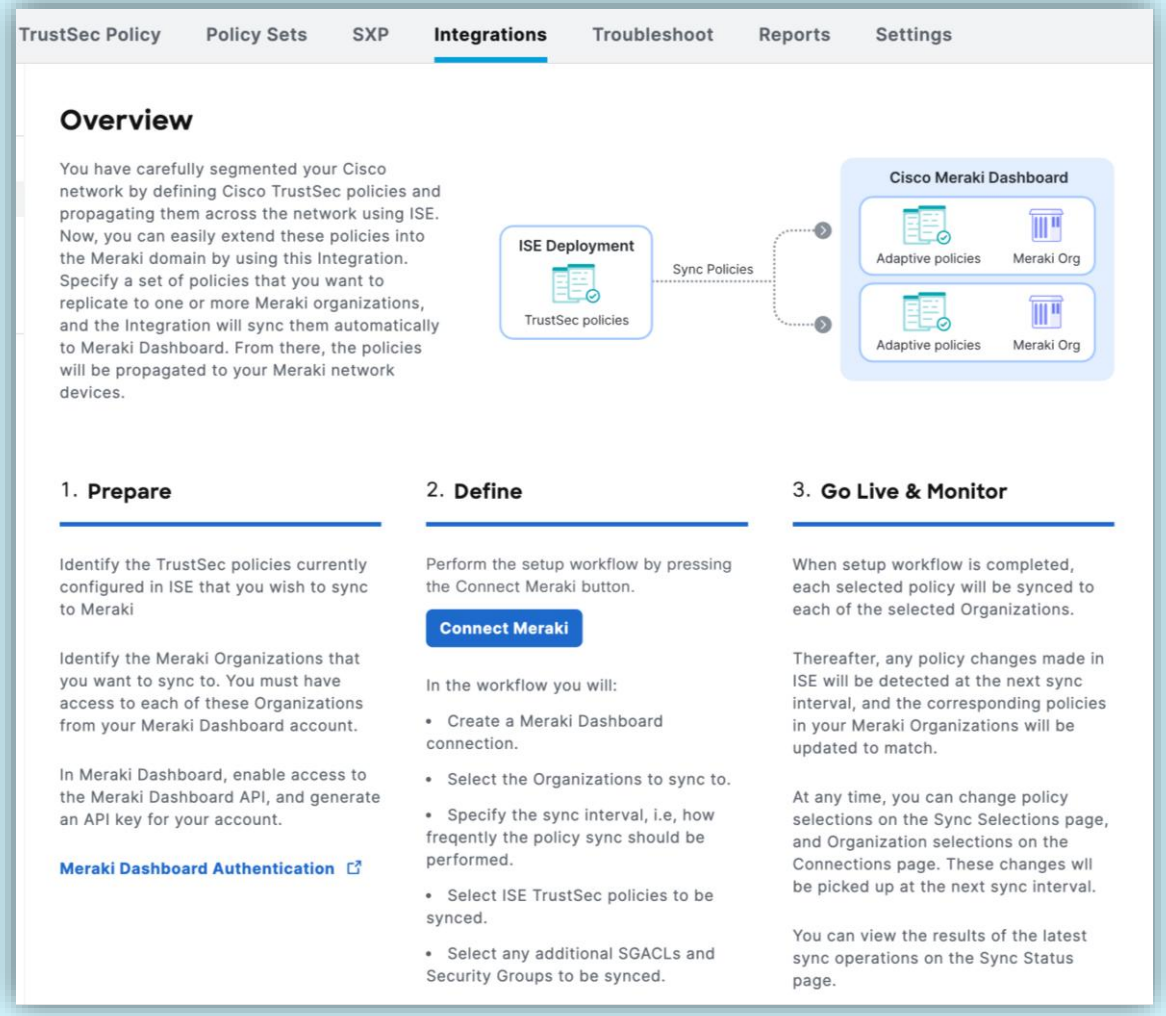
Work Centers > TrustSec > Integrations



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

Integration of ISE with Meraki

Work Centers > TrustSec > Integrations



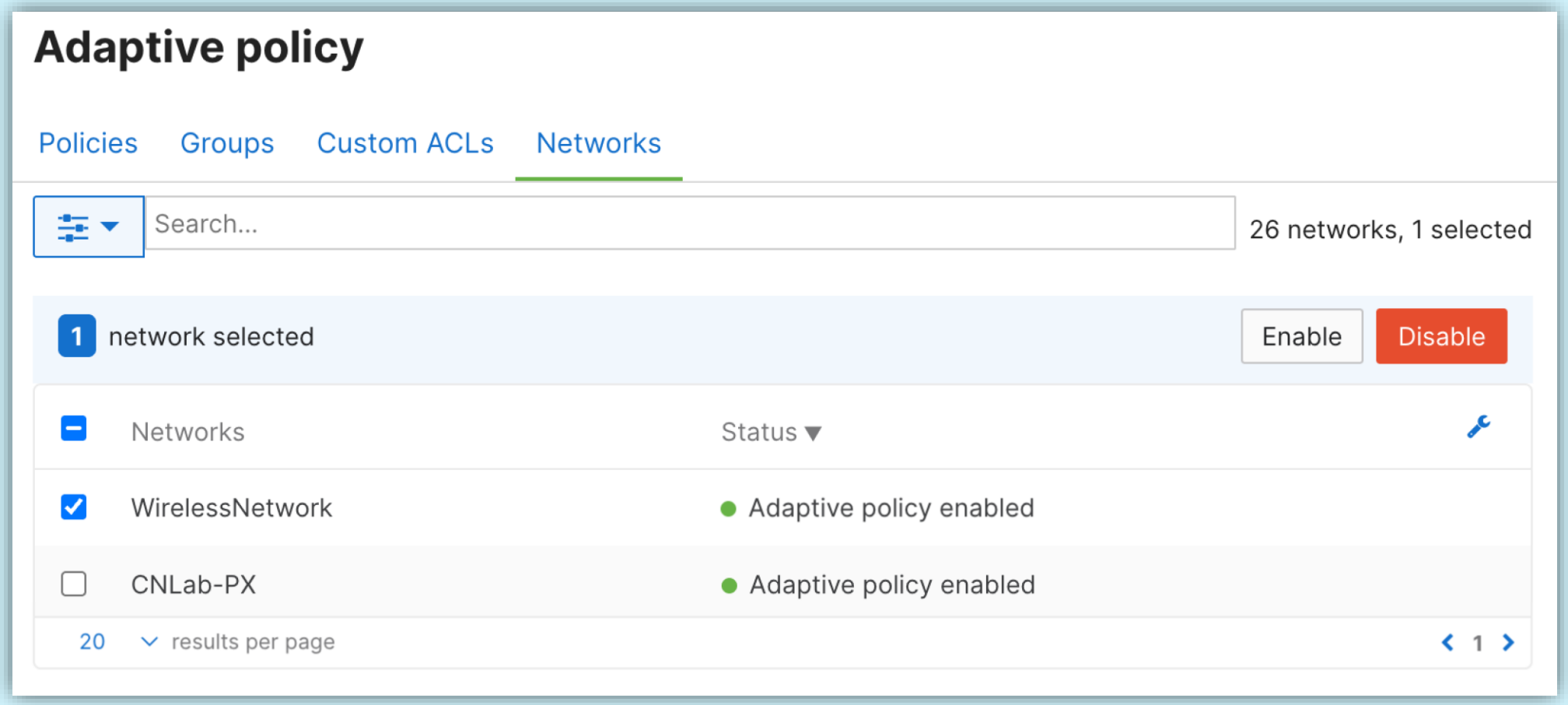
The recommended maximum limits for TrustSec objects that Cisco ISE can share with Cisco Meraki dashboards:

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

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

Meraki Adaptive Policy

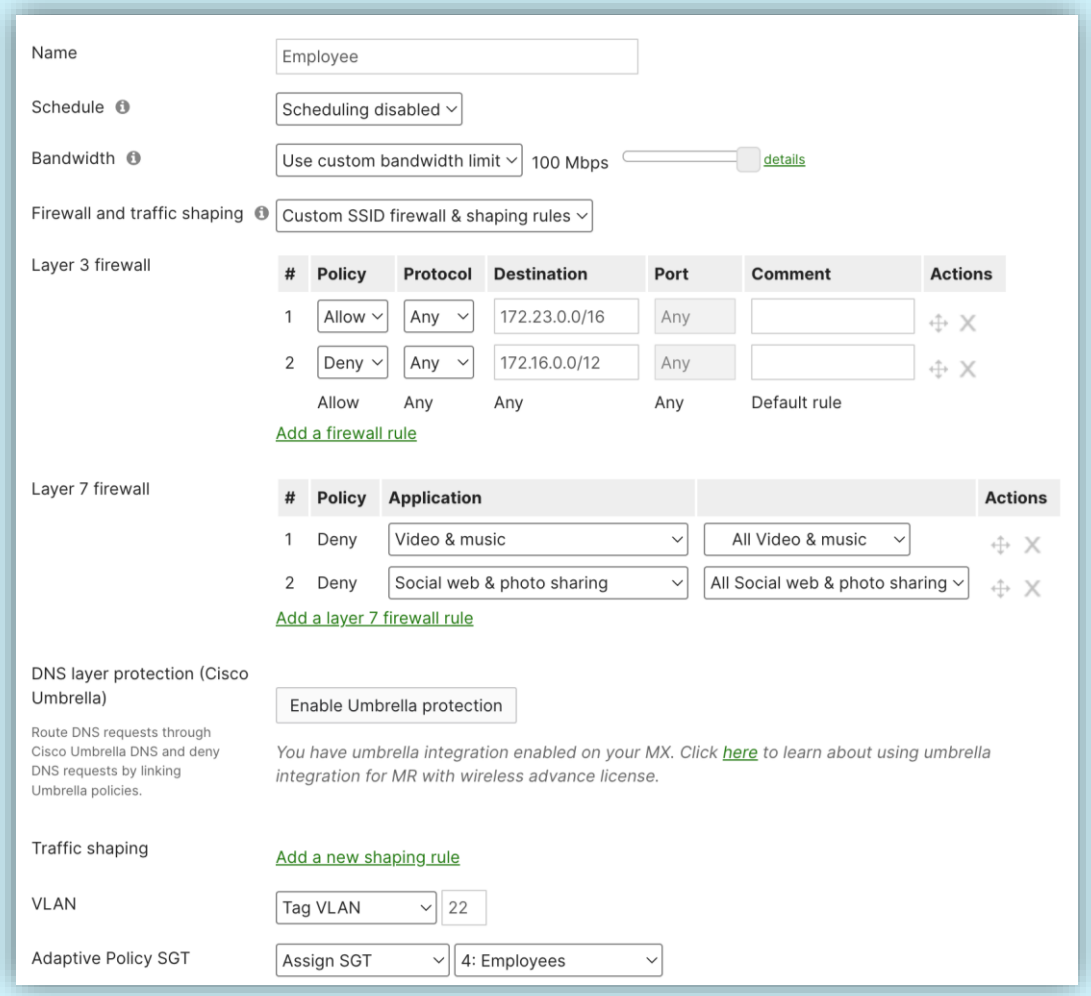
Organization > Configure > Adaptive Policy



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

Meraki Group Policies

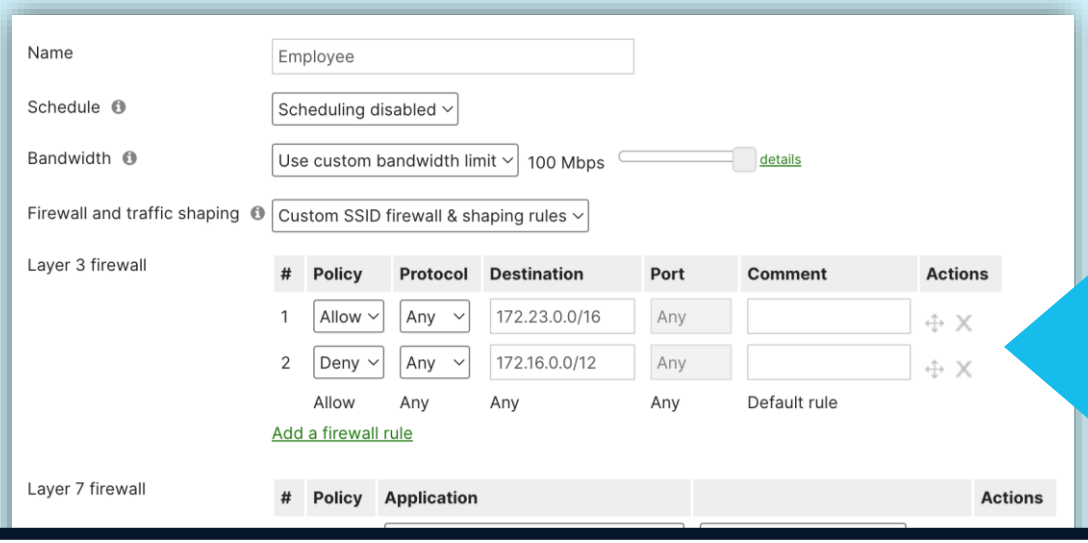
Network-wide > Configure > Group Policies



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

Meraki Group Policies

Network-wide > Configure > Group Policies



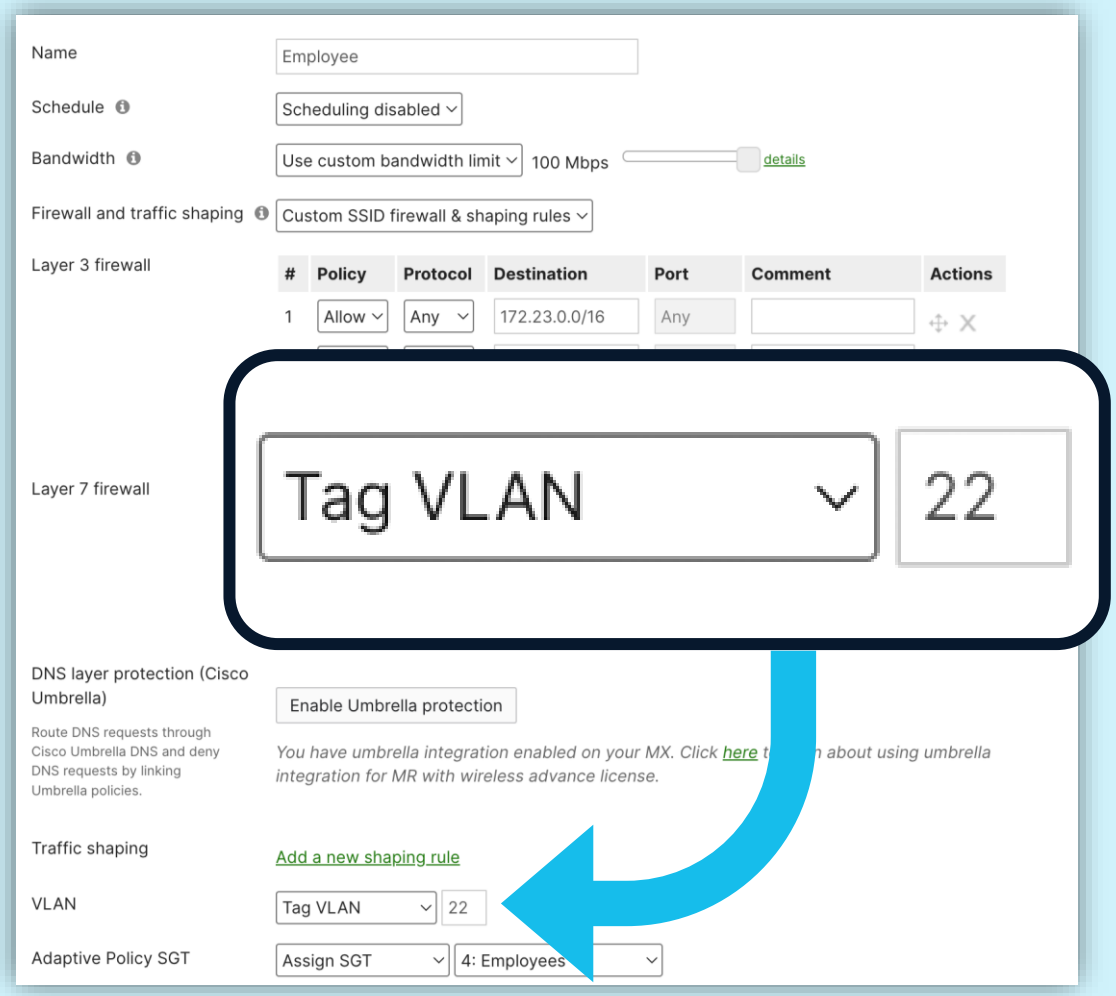
Layer 3 firewall

#	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	

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

Meraki Group Policies

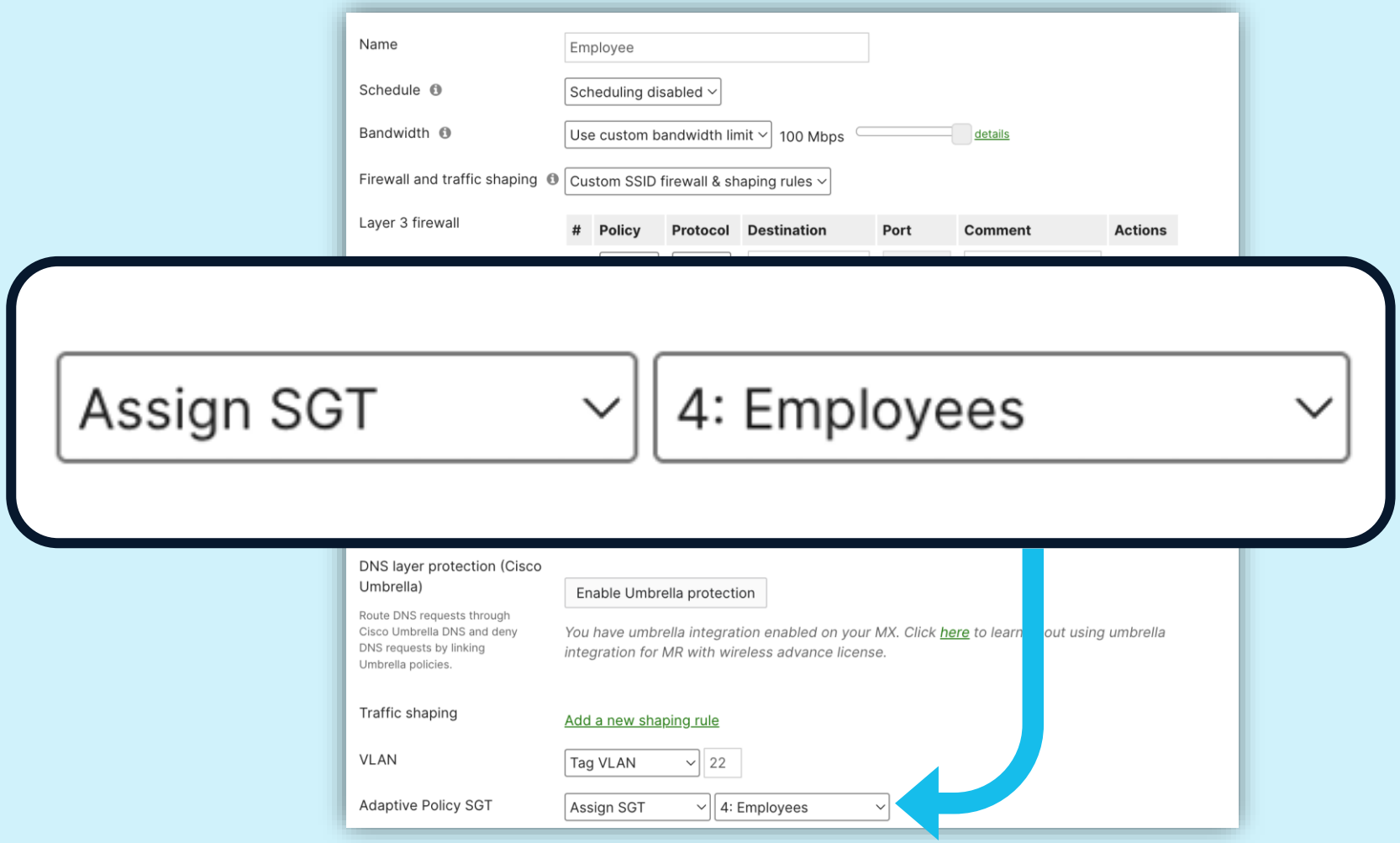
Network-wide > Configure > Group Policies



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

Meraki Group Policies

Network-wide > Configure > Group Policies

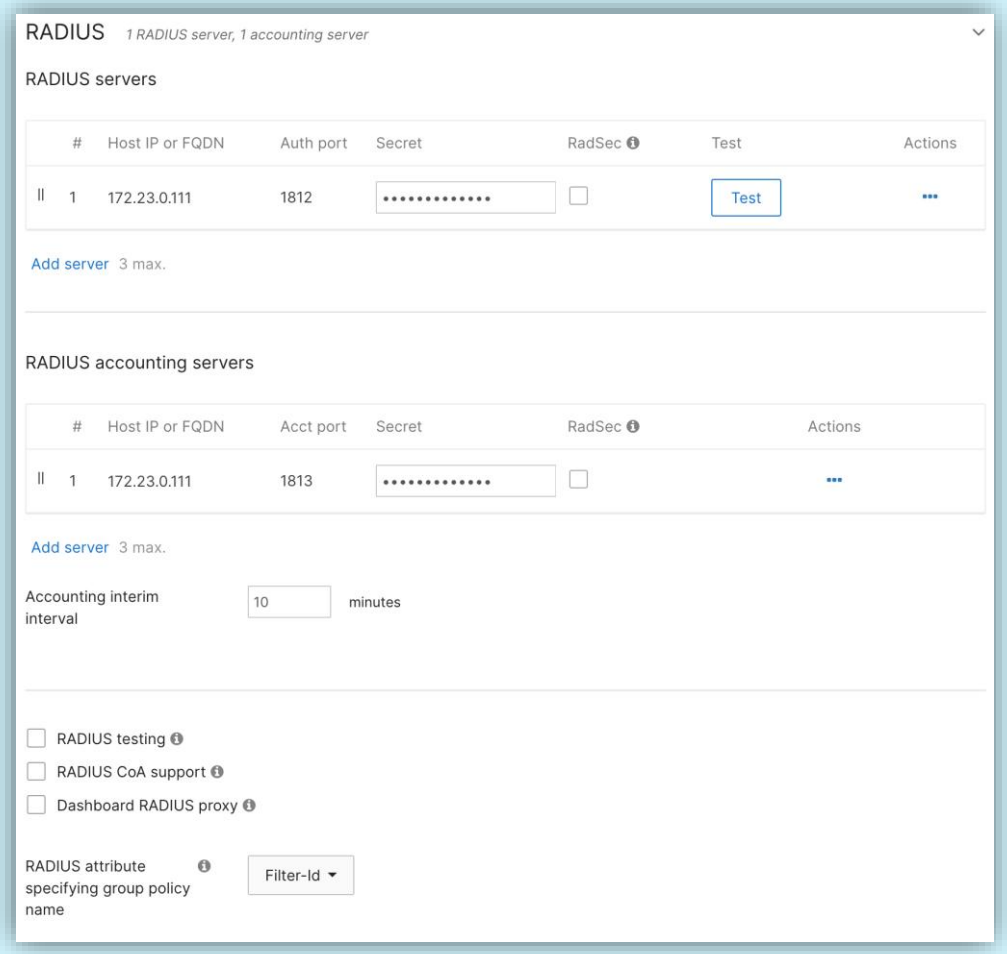


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Meraki Group Policies – RADIUS Attribute

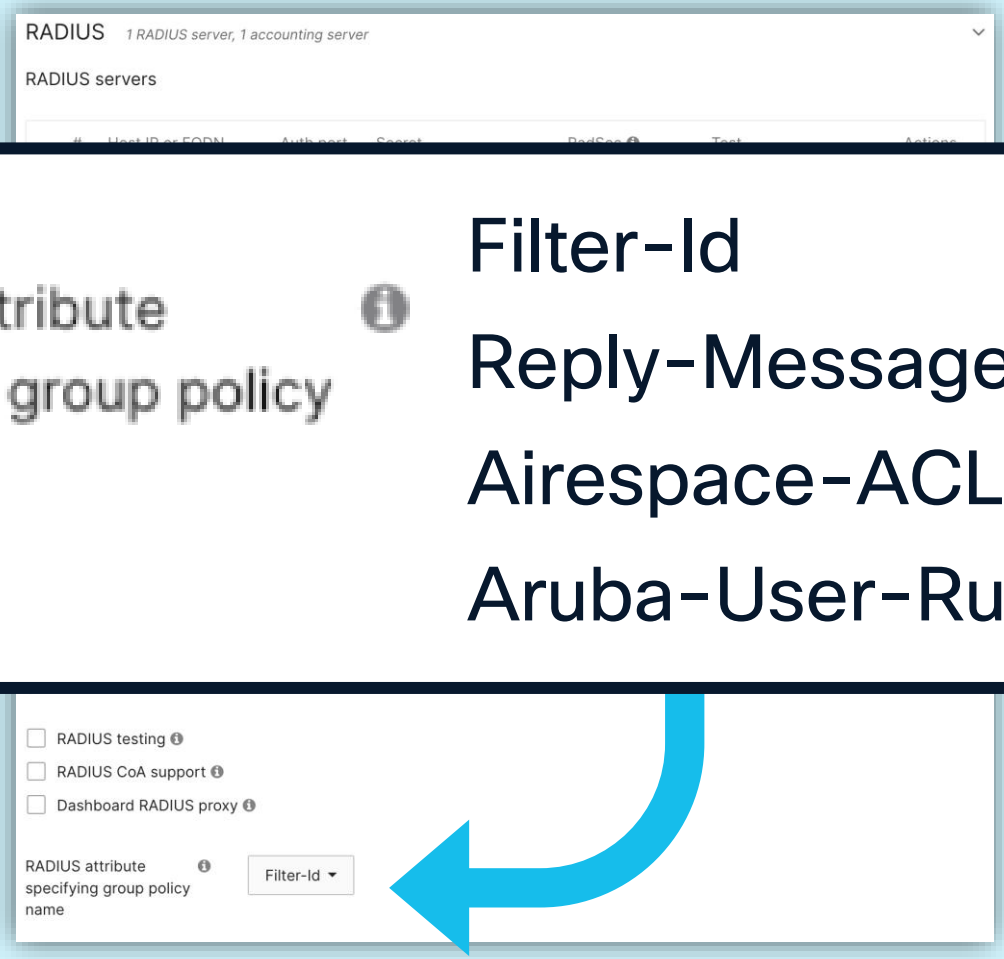
Wireless > Configure > Access Control



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

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

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

Meraki Group Policies – RADIUS Attribute

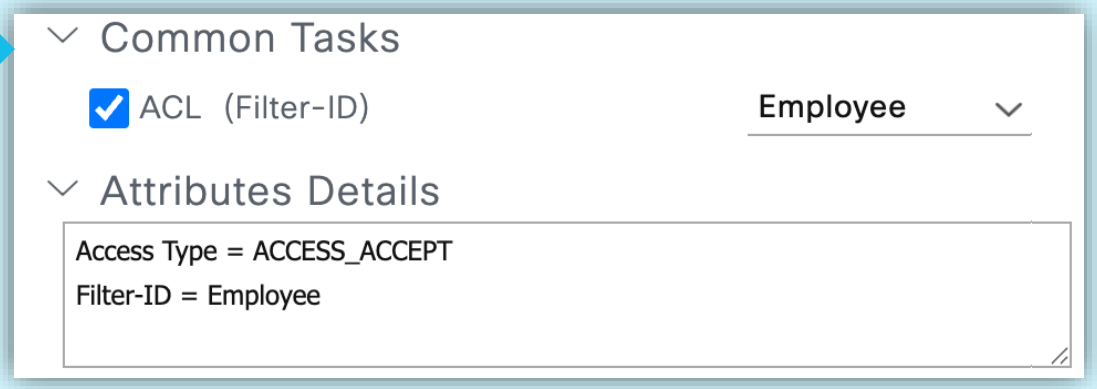
Policy > Policy Elements > Results > Authorization

Filter-Id

Reply-Message

Airespace-ACL-Name

Aruba-User-Rule



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

Meraki Group Policies – RADIUS Attribute

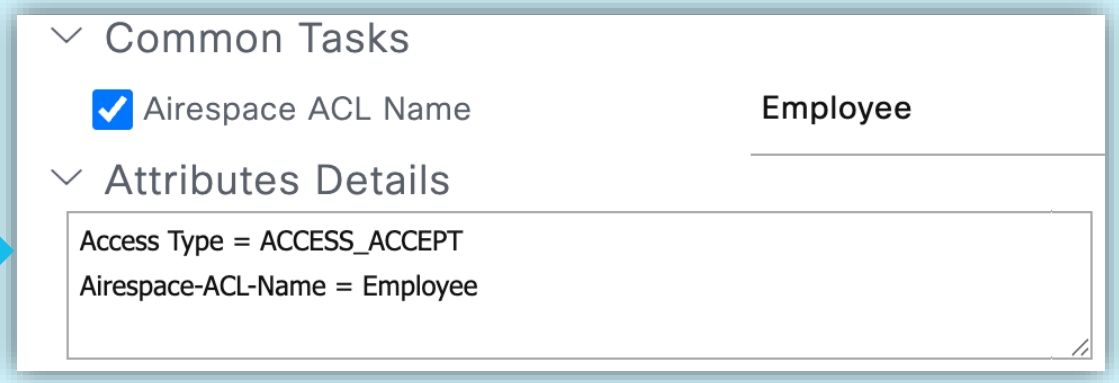
Policy > Policy Elements > Results > Authorization

Filter-Id

Reply-Message

Airespace-ACL-Name

Aruba-User-Rule



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

Meraki Group Policies – RADIUS Attribute

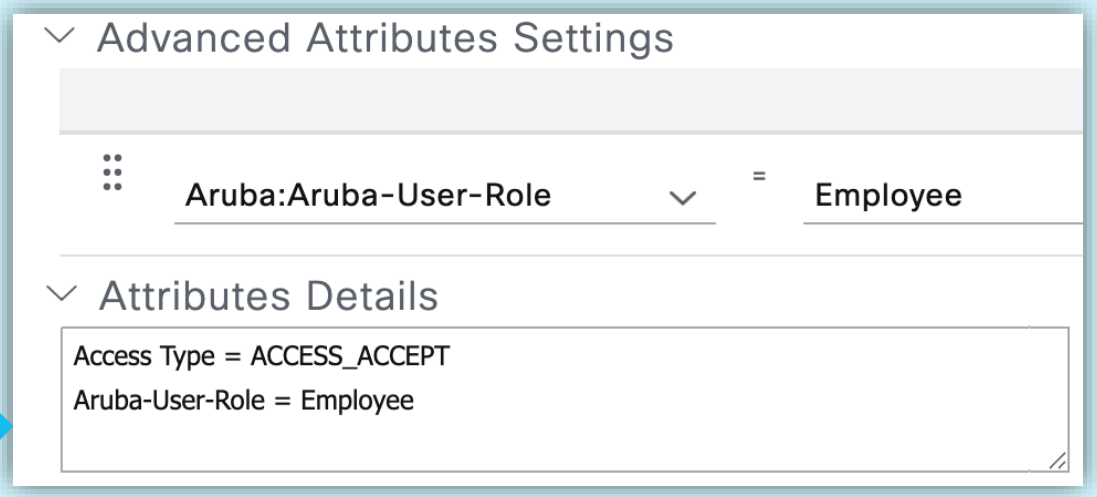
Policy > Policy Elements > Results > Authorization

Filter-Id

Reply-Message

Airespace-ACL-Name

Aruba-User-Rule



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

Authorization Options with ISE

iPSK

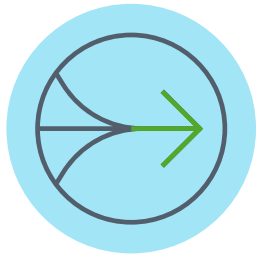
Assigns unique pre-shared keys for endpoints on the same SSID

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

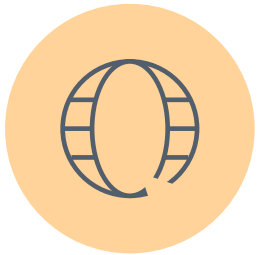
cisco-av-pair = **private-group-id**
cisco-av-pair = **private-group-name**
cisco-av-pair = **private-group-owner**



URL Redirect

Facilitates conditional web redirection when traffic is blocked

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



URL Filter

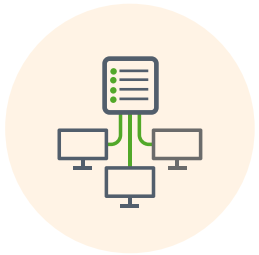
Controls which FQDNs the endpoint can reach or not

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

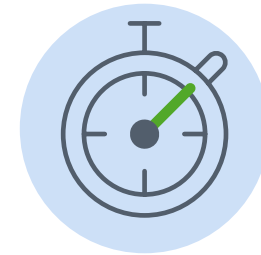
Attaches mDNS profiles to broker mDNS advertisements

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

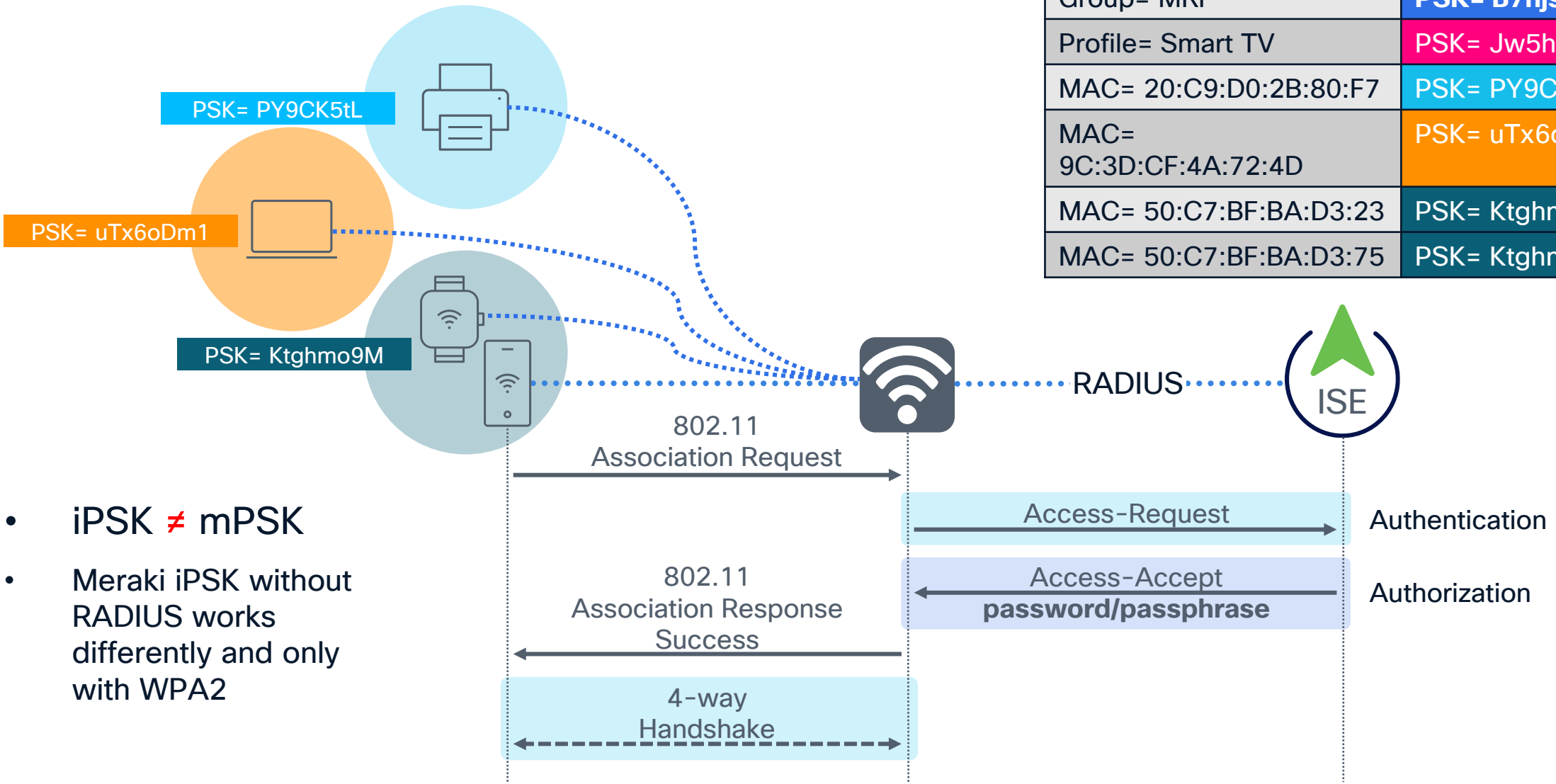
Sets the maximum duration of a user's session

Session-Timeout
Idle-Timeout

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

Identity PSK

Group= MRI	**PSK= B7hjs1oz**
Profile= Smart TV	PSK= Jw5hw3tS
MAC= 20:C9:D0:2B:80:F7	PSK= PY9CK5tL
MAC= 9C:3D:CF:4A:72:4D	PSK= uTx6oDm1
MAC= 50:C7:BF:BA:D3:23	PSK= Ktghmo9M
MAC= 50:C7:BF:BA:D3:75	PSK= Ktghmo9M



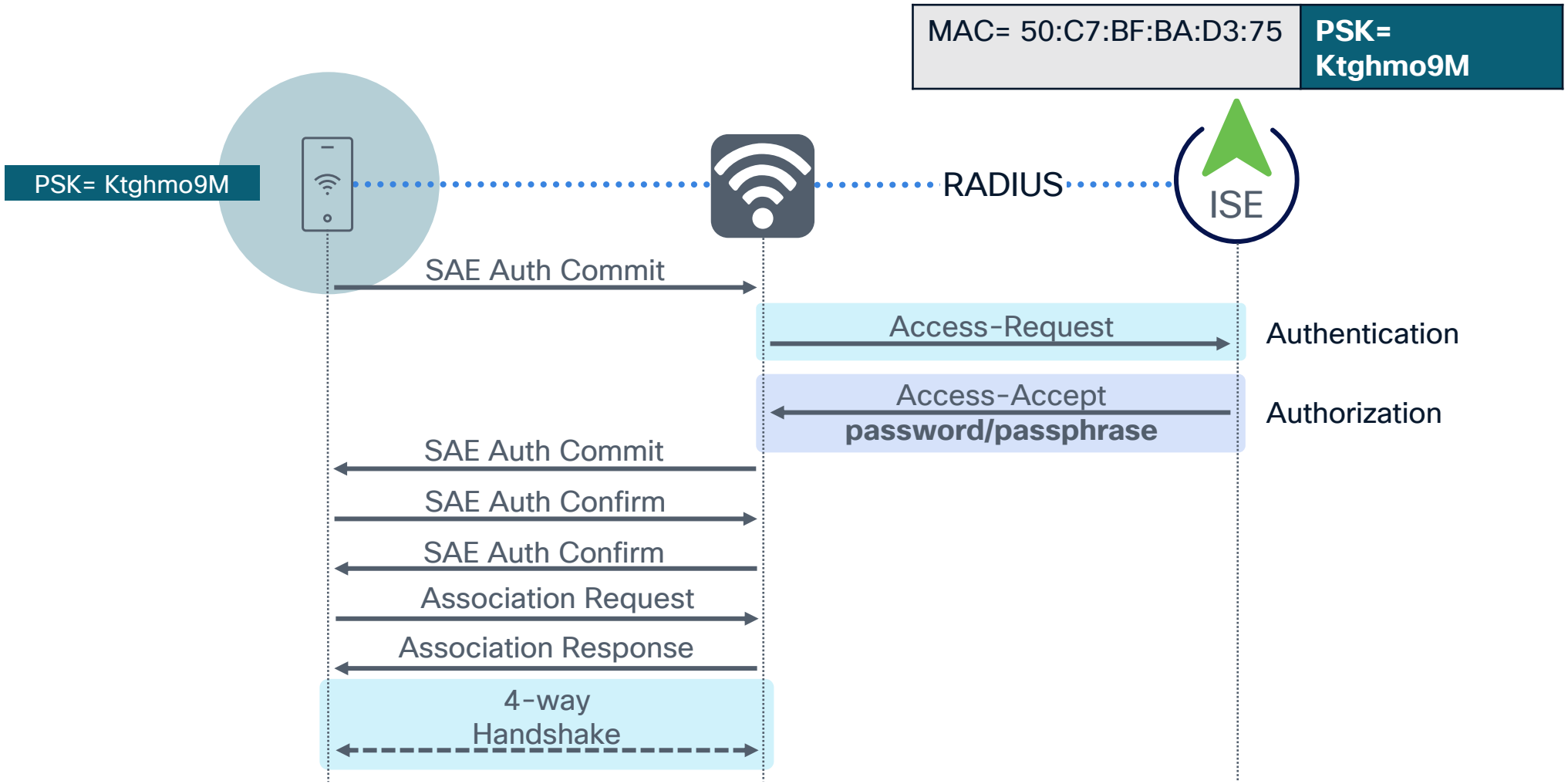
- iPSK ≠ mPSK
- Meraki iPSK without RADIUS works differently and only with WPA2

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

Identity PSK – WPA3 SAE

Catalyst 9800 IOS-XE 17.9.2

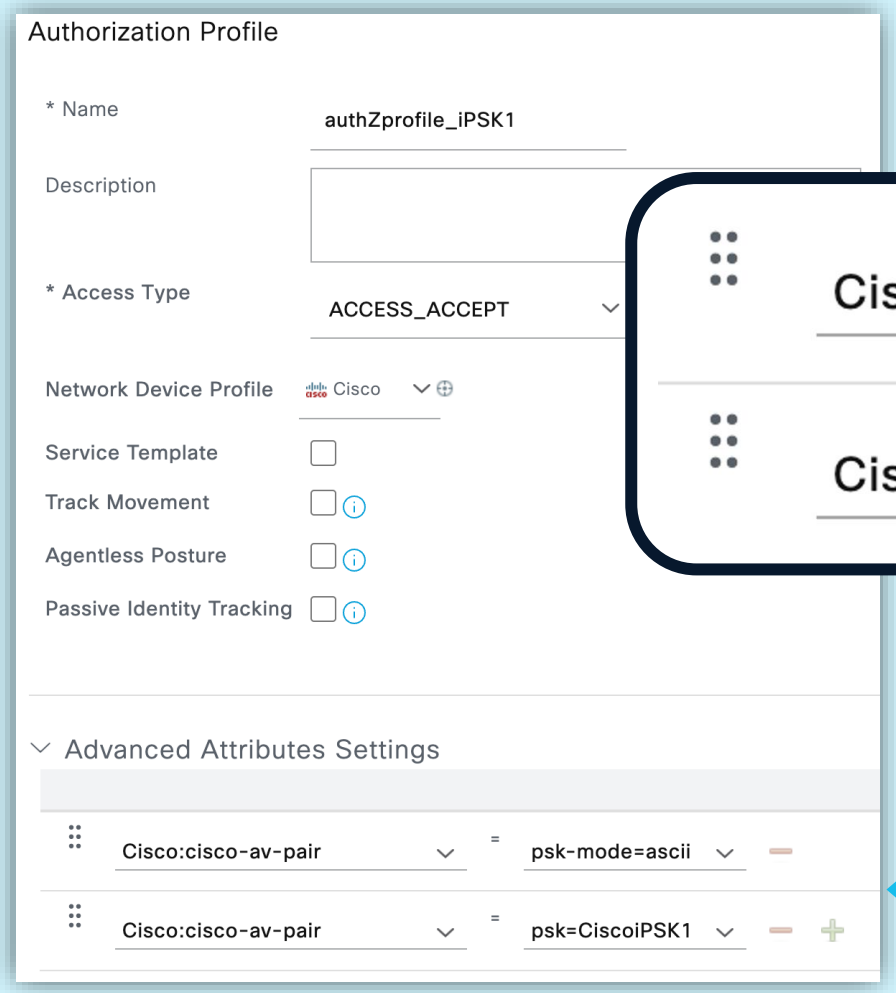
* Roadmap for Meraki



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

Identity PSK – ISE Configuration

Policy > Policy Elements > Results > Authorization

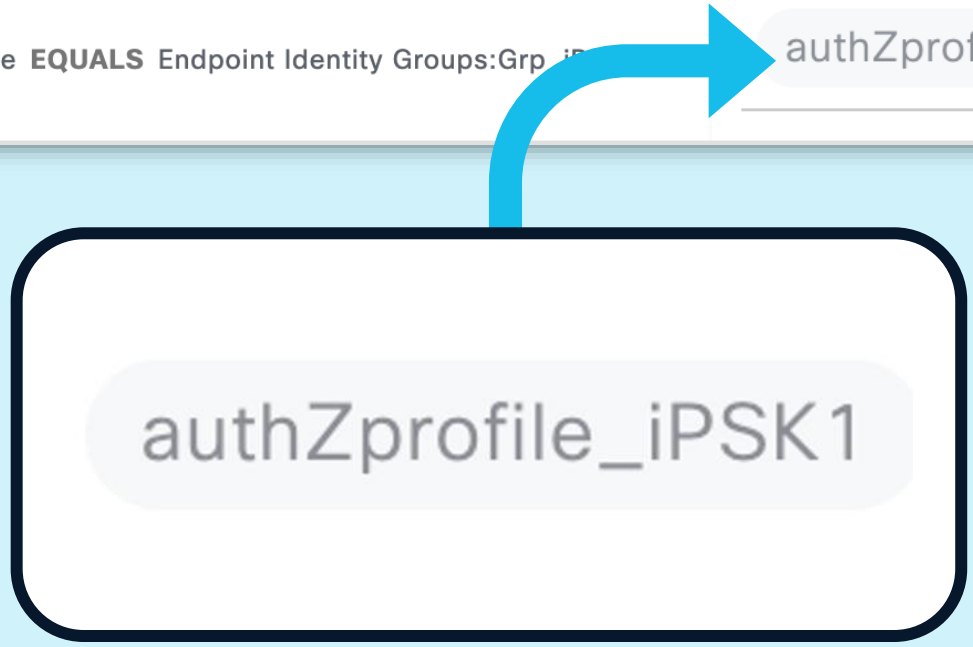


© 2025 Cisco and/or its affiliates. All rights reserved.

Identity PSK – ISE Configuration

Policy > Policy Sets > Authorization Policy

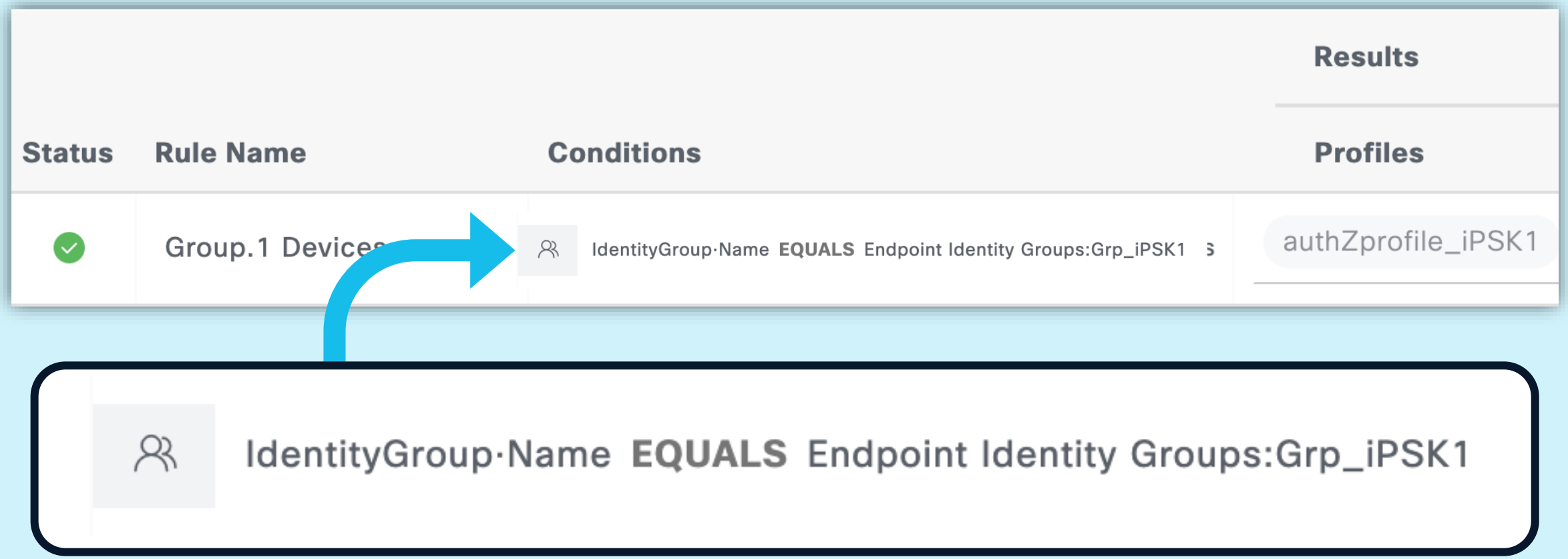
Status	Rule Name	Conditions	Results Profiles
✓	Group.1 Devices	IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Grp_iP	authZprofile_iPSK1



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

Identity PSK – ISE Configuration

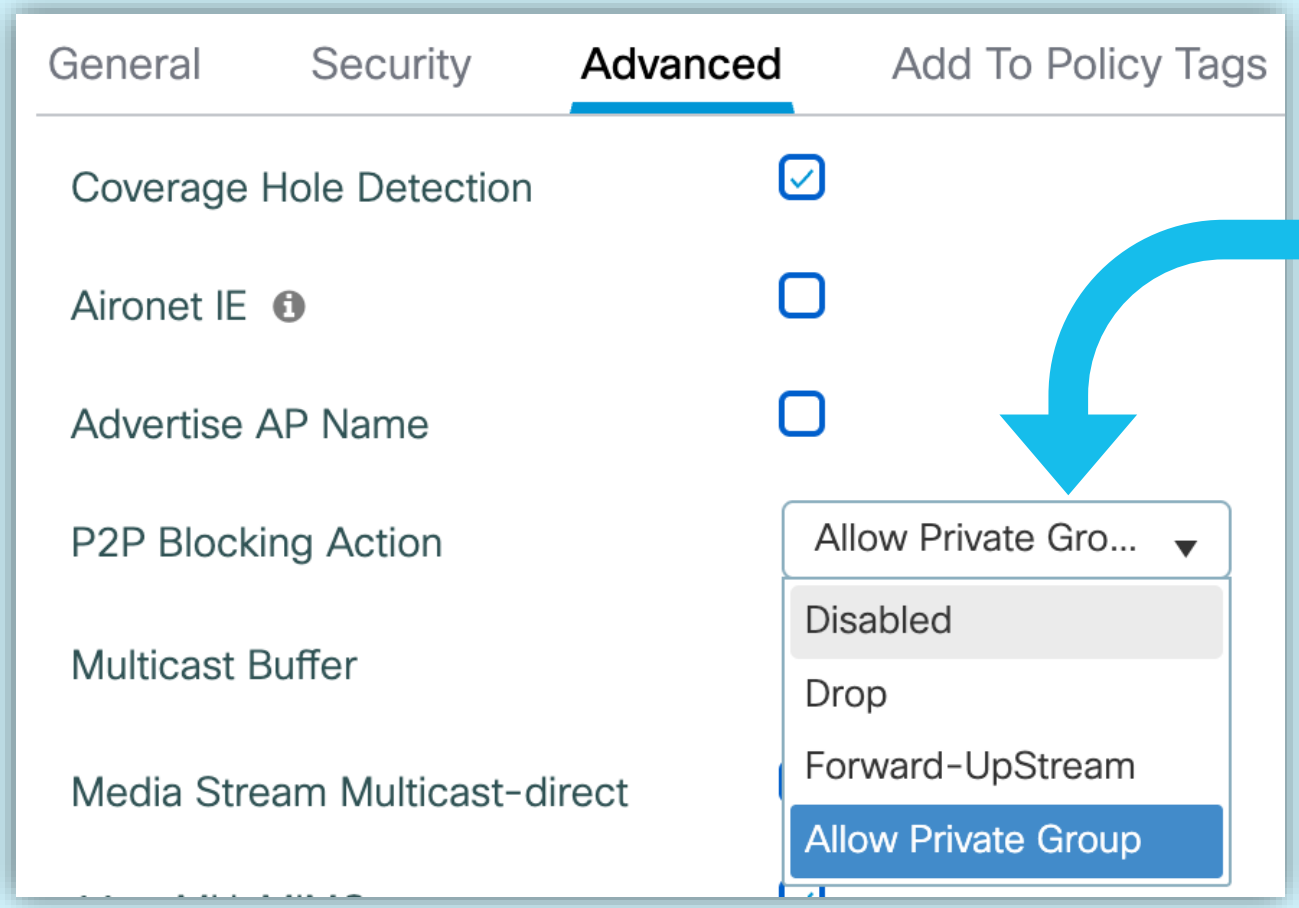
Policy > Policy Sets > Authorization Policy



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

Identity PSK – WLC Configuration

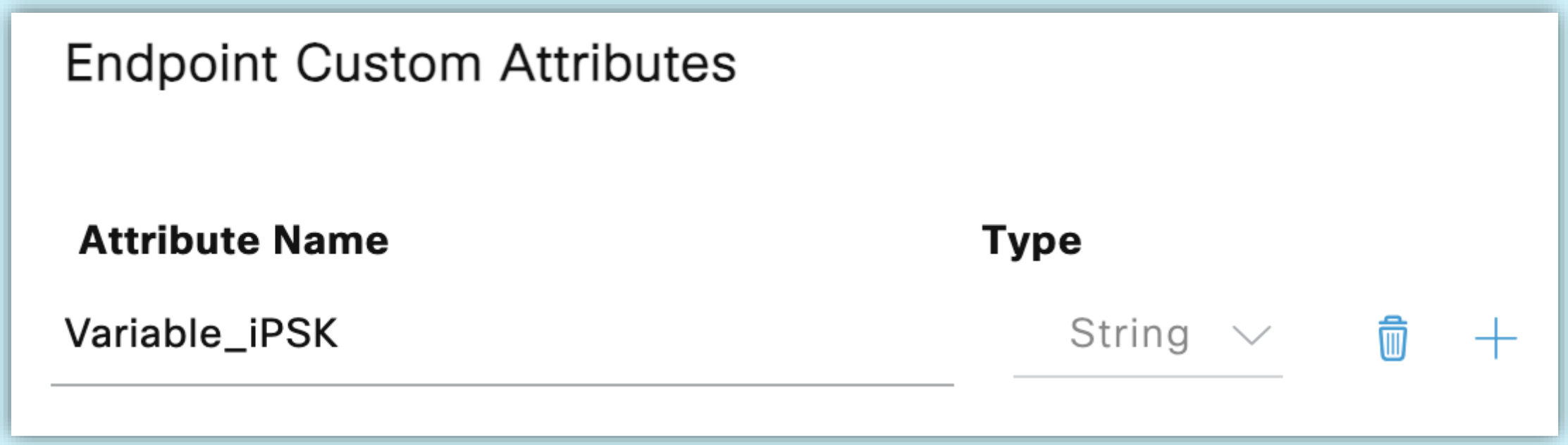
Configuration > Tags & Policy > Policy



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

Identity PSK – ISE Configuration (Option)

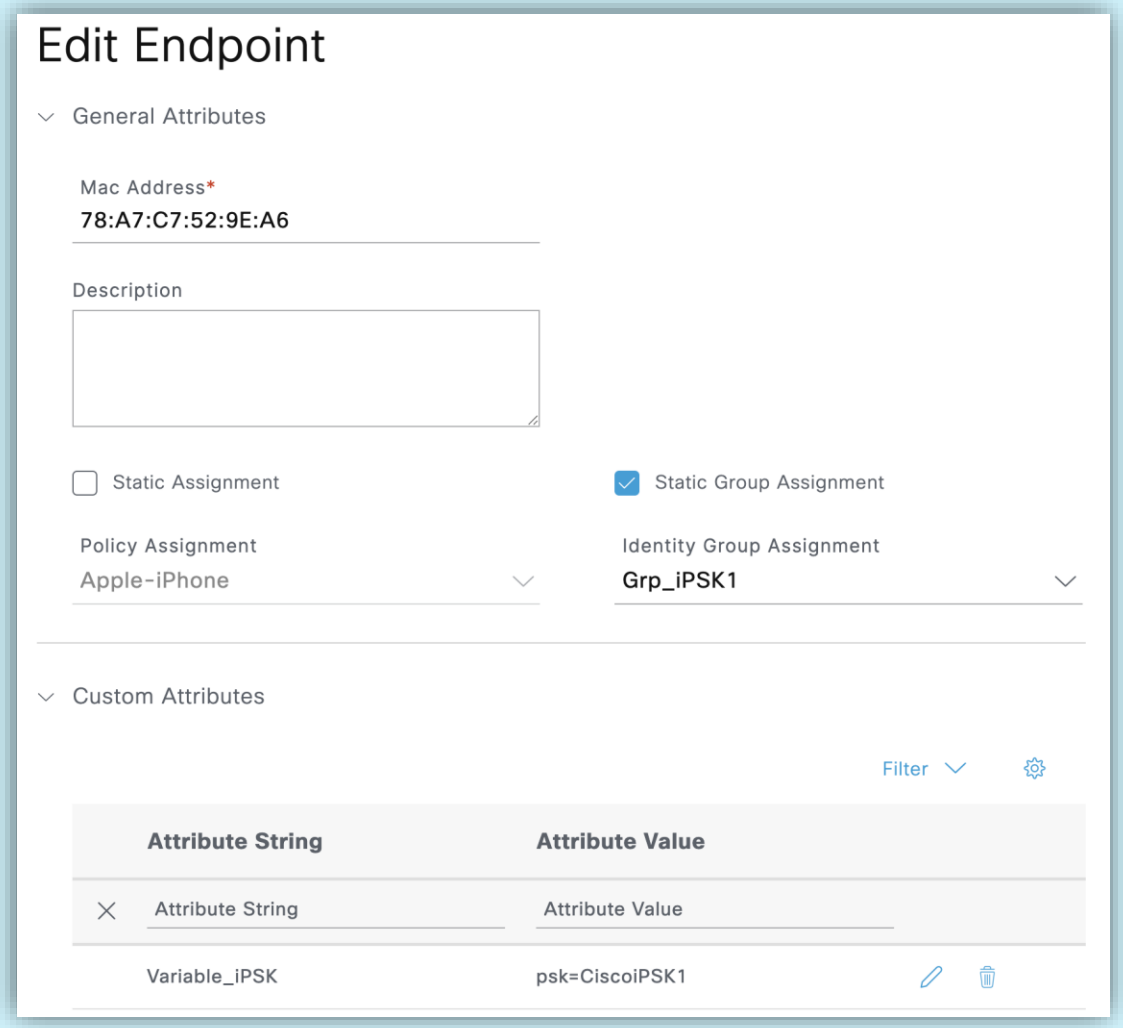
Administration > Identity Management > Settings > Endpoint Custom Attributes



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

Identity PSK – ISE Configuration (Option)

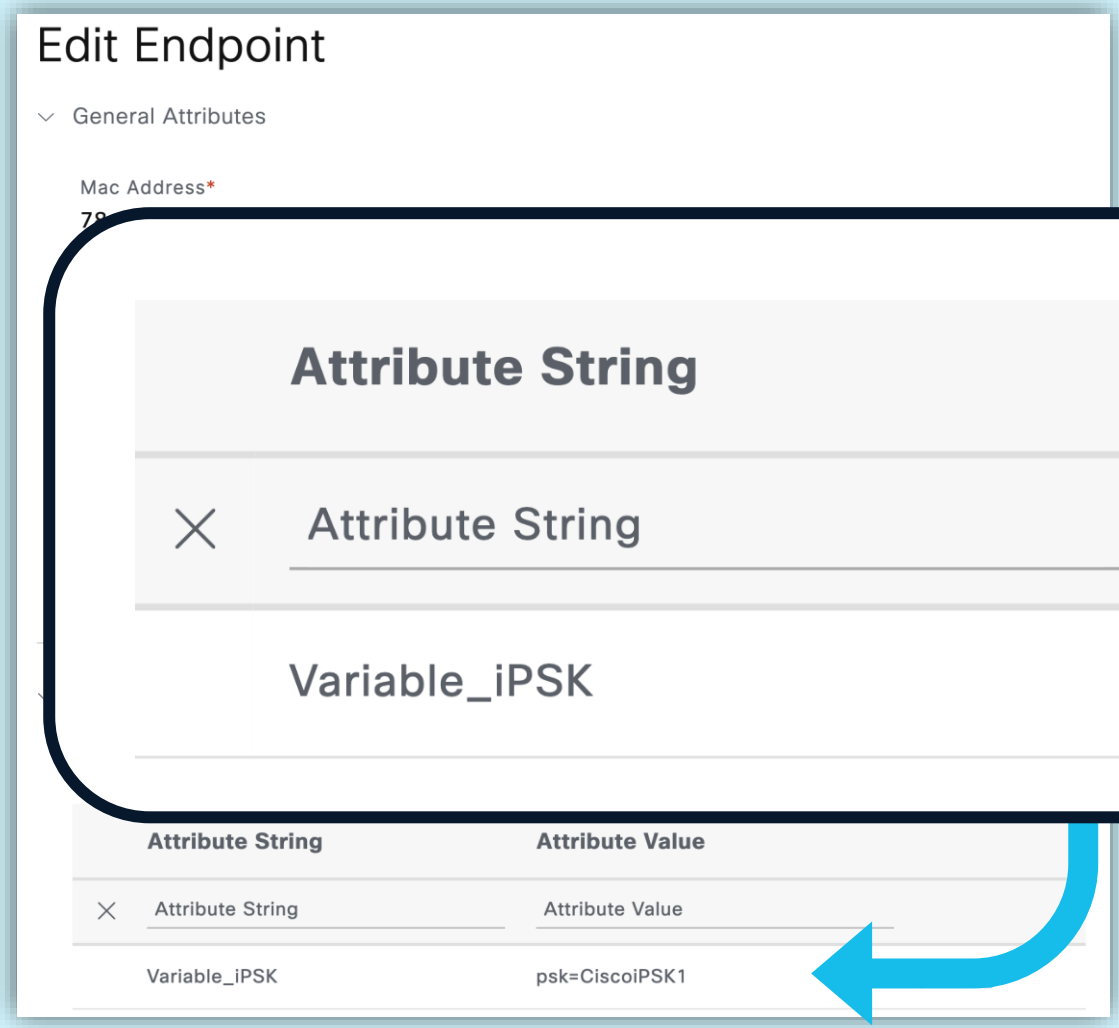
Context Visibility > Endpoints



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

Identity PSK – ISE Configuration (Option)

Context Visibility > Endpoints



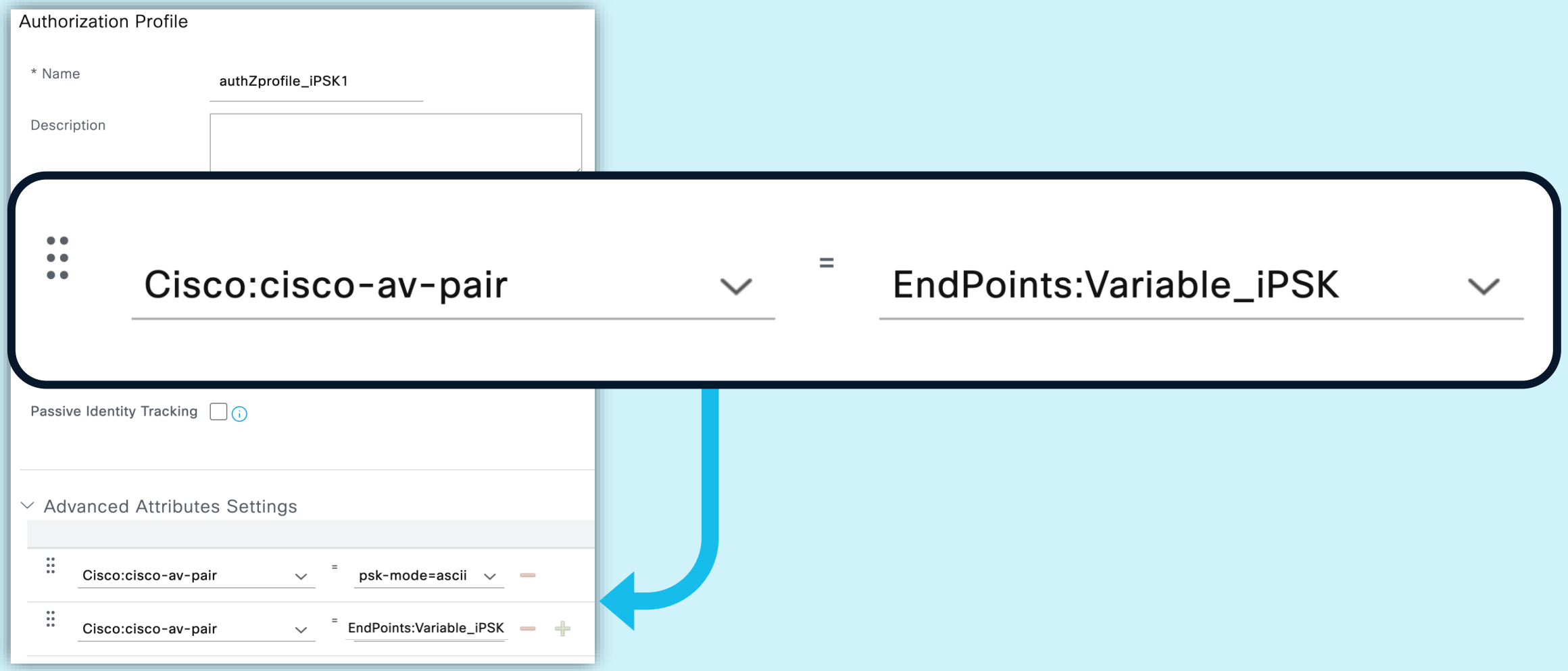
Attribute String | Attribute Value
Attribute String | Attribute Value
Variable_iPSK | psk=CiscoiPSK1

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

cisco

Identity PSK – ISE Configuration (Option)

Policy > Policy Elements > Results > Authorization



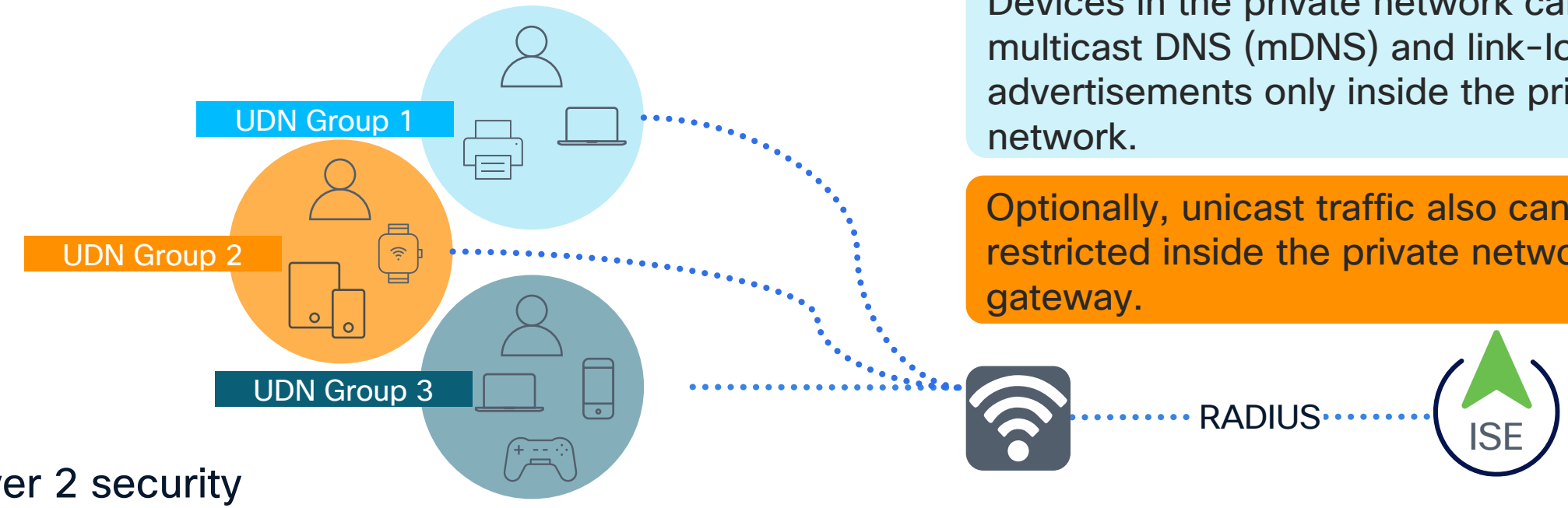
© 2025 Cisco and/or its affiliates. All rights reserved.

User Defined Network (UDN)

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.



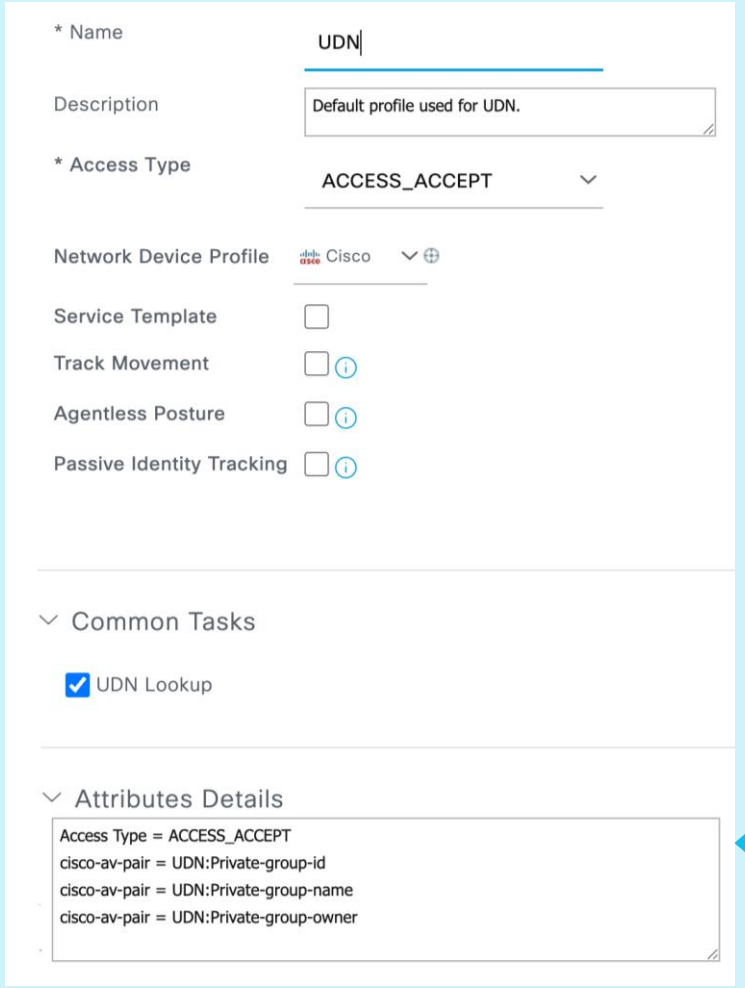
Layer 2 security

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

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

UDN- ISE Configuration

Policy > Policy Elements > Results > Authorization



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

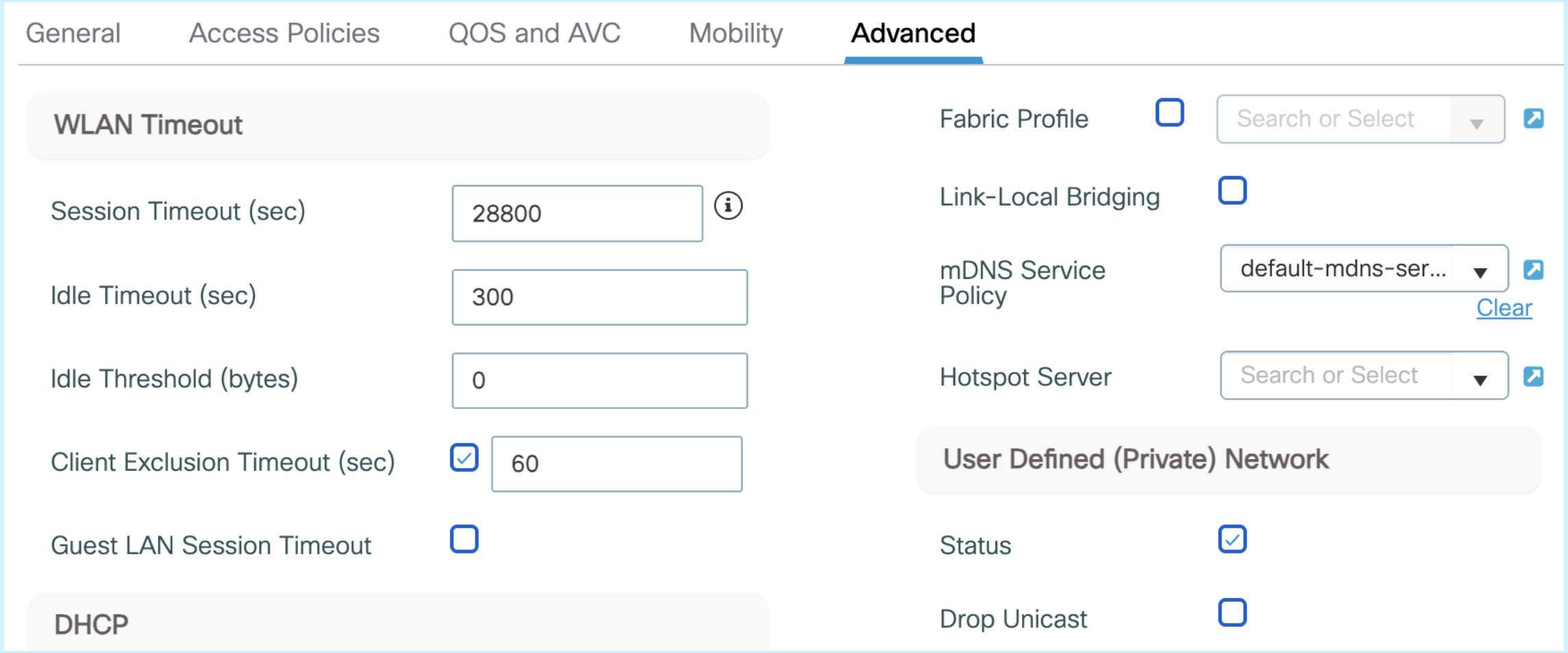
cisco-av-pair = UDN:Private-group-name

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

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

UDN- WLC Configuration

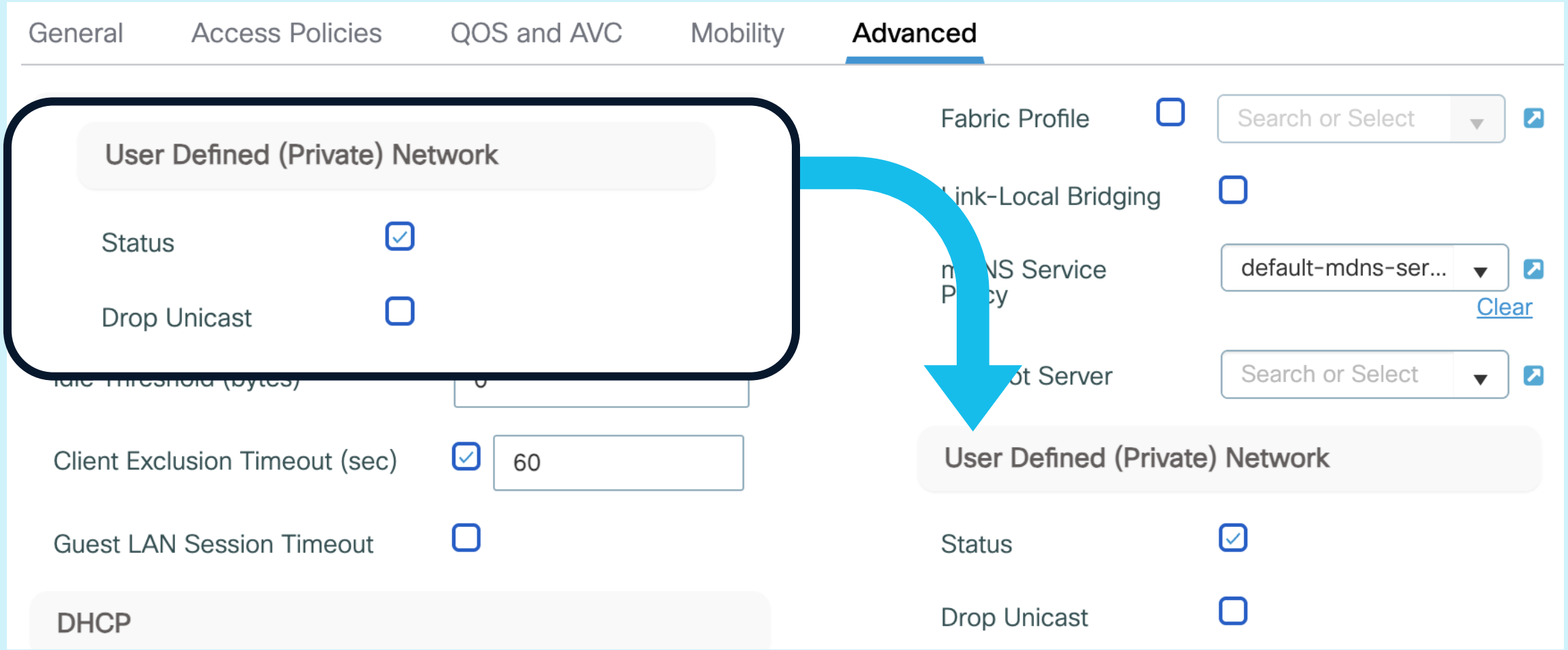
Configuration > Tags & Profiles > Policy



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

UDN- WLC Configuration

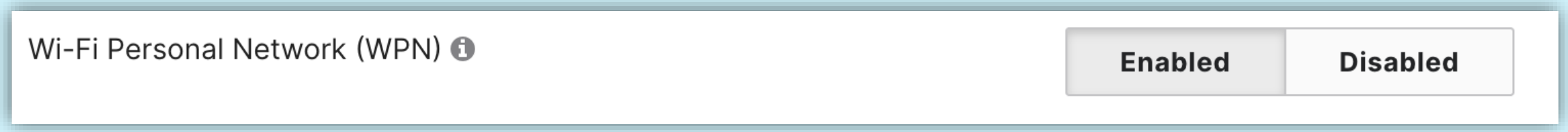
Configuration > Tags & Profiles > Policy



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

UDN– Meraki WPN

Wireless > Configure > Access Control



WPN Supported Networks

802.1X

MAC Auth

iPSK with RADIUS

iPSK without RADIUS

Not Interoperable with UDN on Catalyst

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

ISE Guest Features

1 million

# of supported Guest accounts

EMAIL PRINT SMS

Guest account notification options

Portal language customization

Social Media Login support

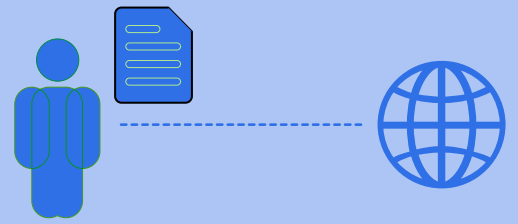
API

Manage guest accounts via REST

Hotspot

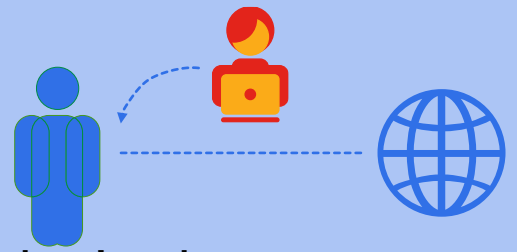
Immediate, un-credentialed Internet access

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

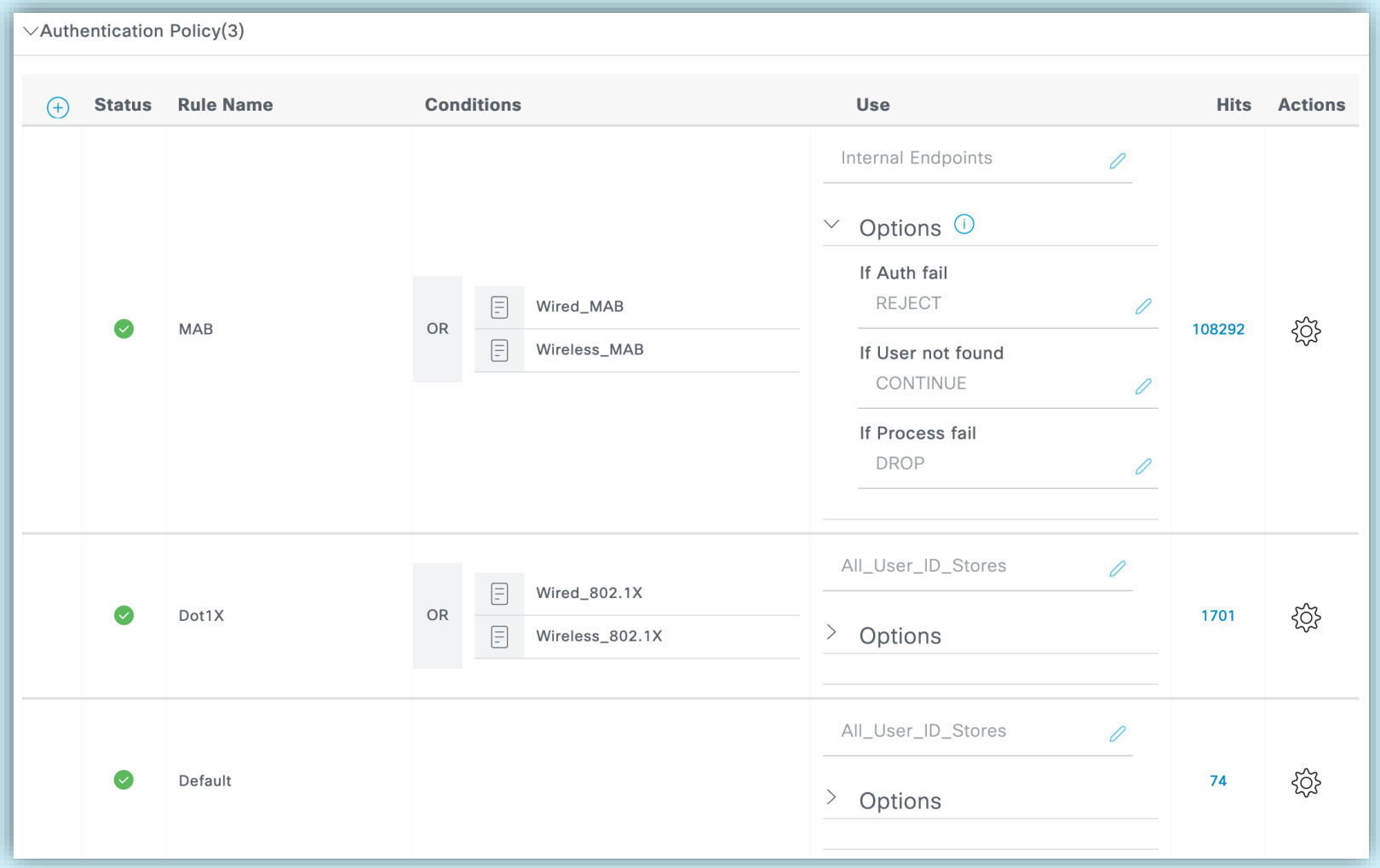
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Authentication and Authorization Policies

ISE - Authentication Policy

Policy > Policy Sets > Authentication Policy



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

ISE - Authorization Policy

Policy > Policy Sets > Authentication Policy

Authorization Policy(10)

	Status	Rule Name	Conditions		Results: Profiles	Results: 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_Admins	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	⚙

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

Wireless Access Control with Cisco Access Manager

cisco Live !

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

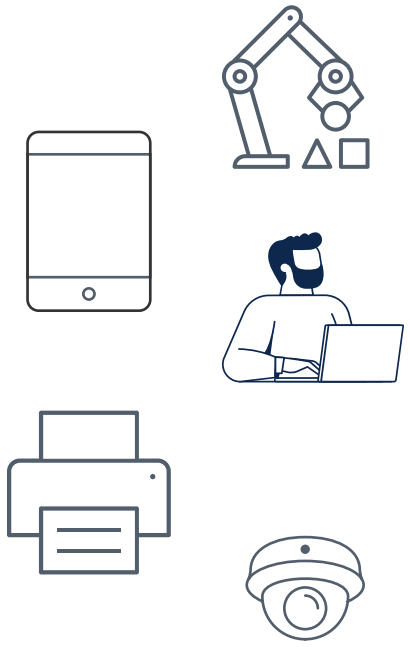
Simplified and rapid Zero-Trust adoption using identity-based micro-segmentation

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

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

Cisco Access Manager – Solution Components

Users
+
Endpoints



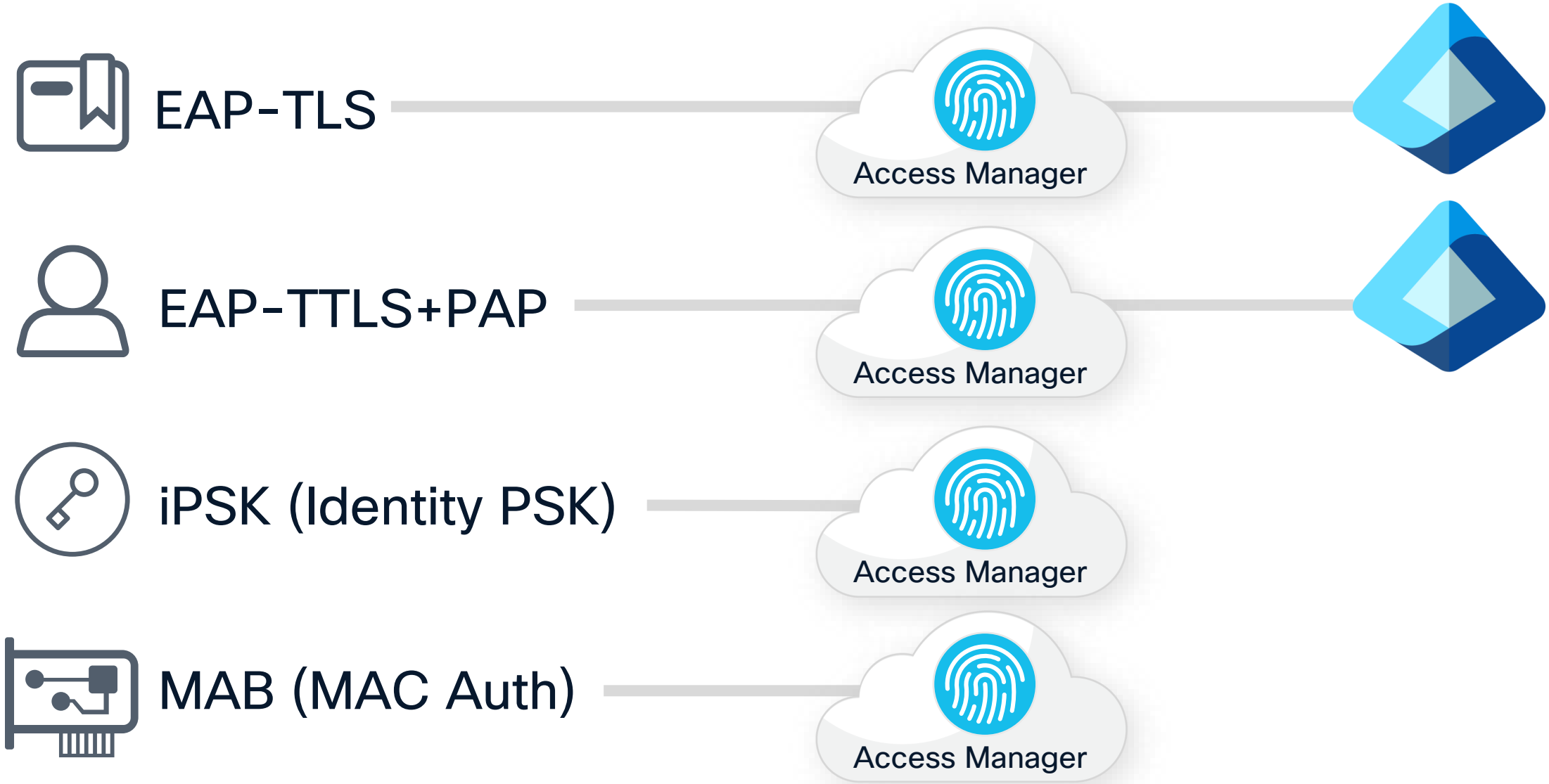
Cloud-Managed
Networks

Meraki Dashboard

Identity Providers

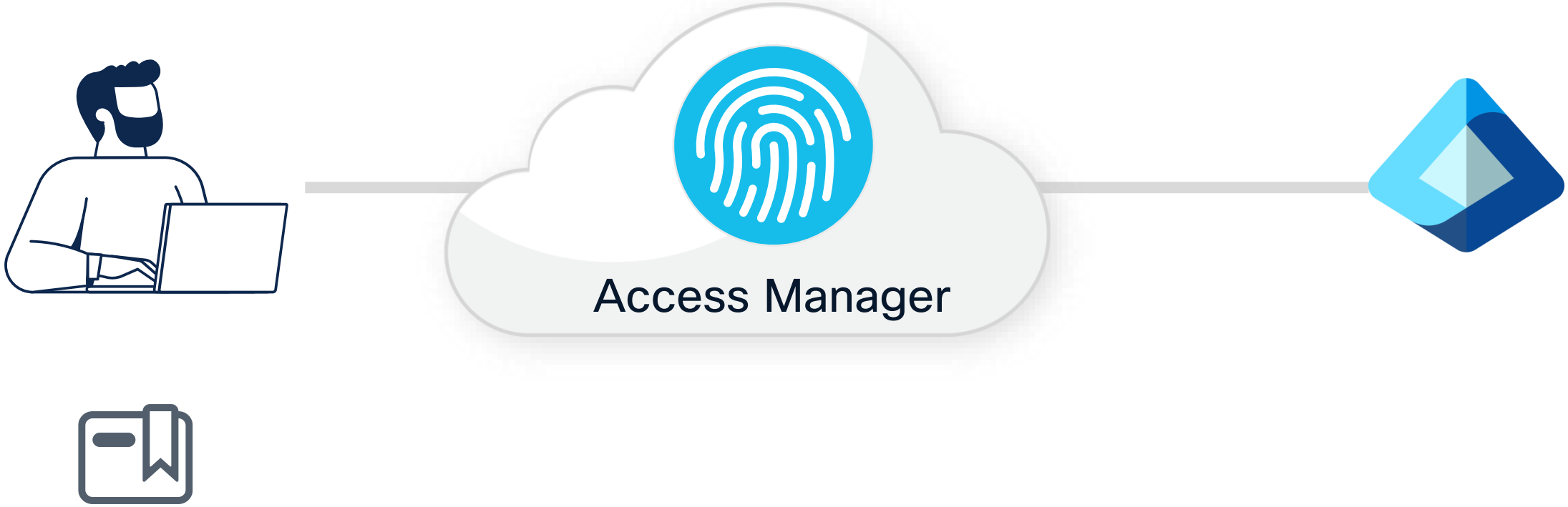
© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Access Manager – Identify Users and Endpoints



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

Cisco Access Manager – EAP-TLS Authentication



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

Cisco Access Manager – EAP-TLS Authentication

Access Manager

Graph API Integration

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

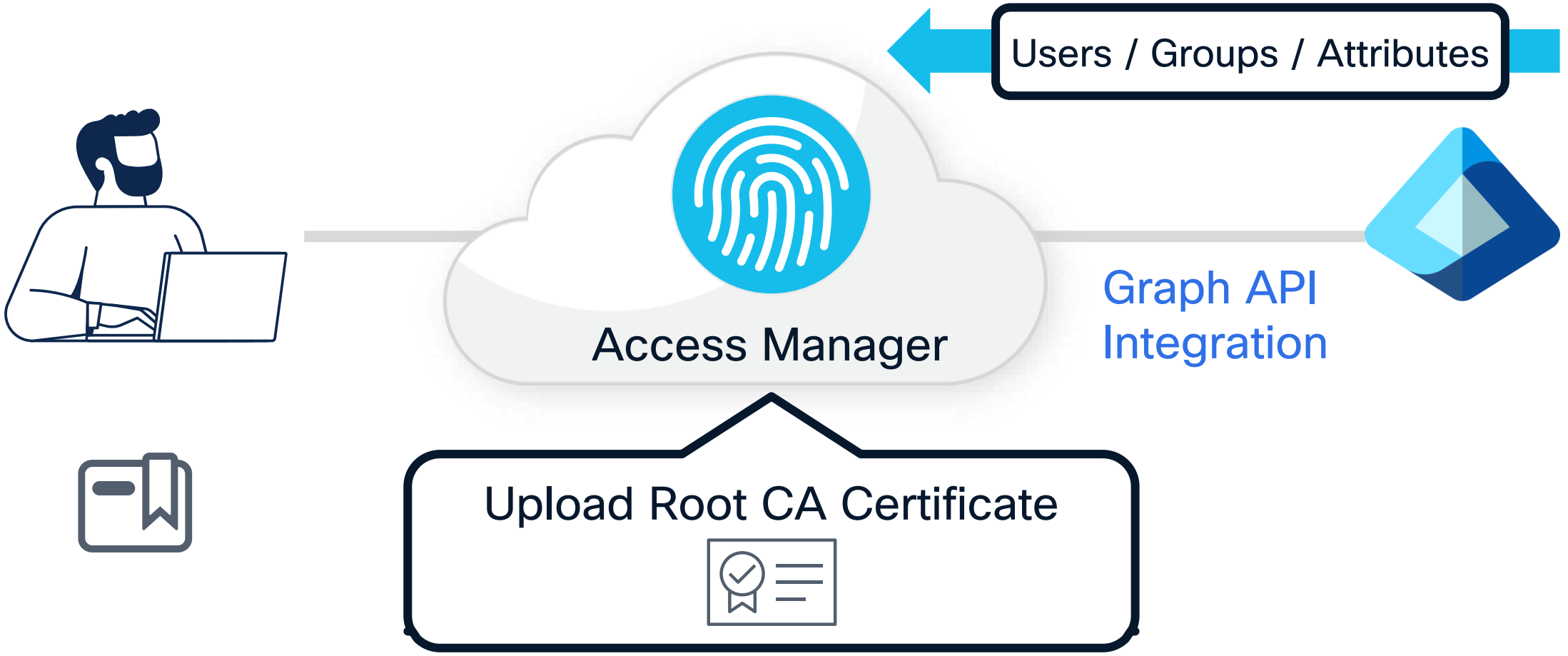
© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Access Manager – EAP-TLS Authentication

*Sync Every 6 Hours

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

Cisco Access Manager – EAP-TLS Authentication

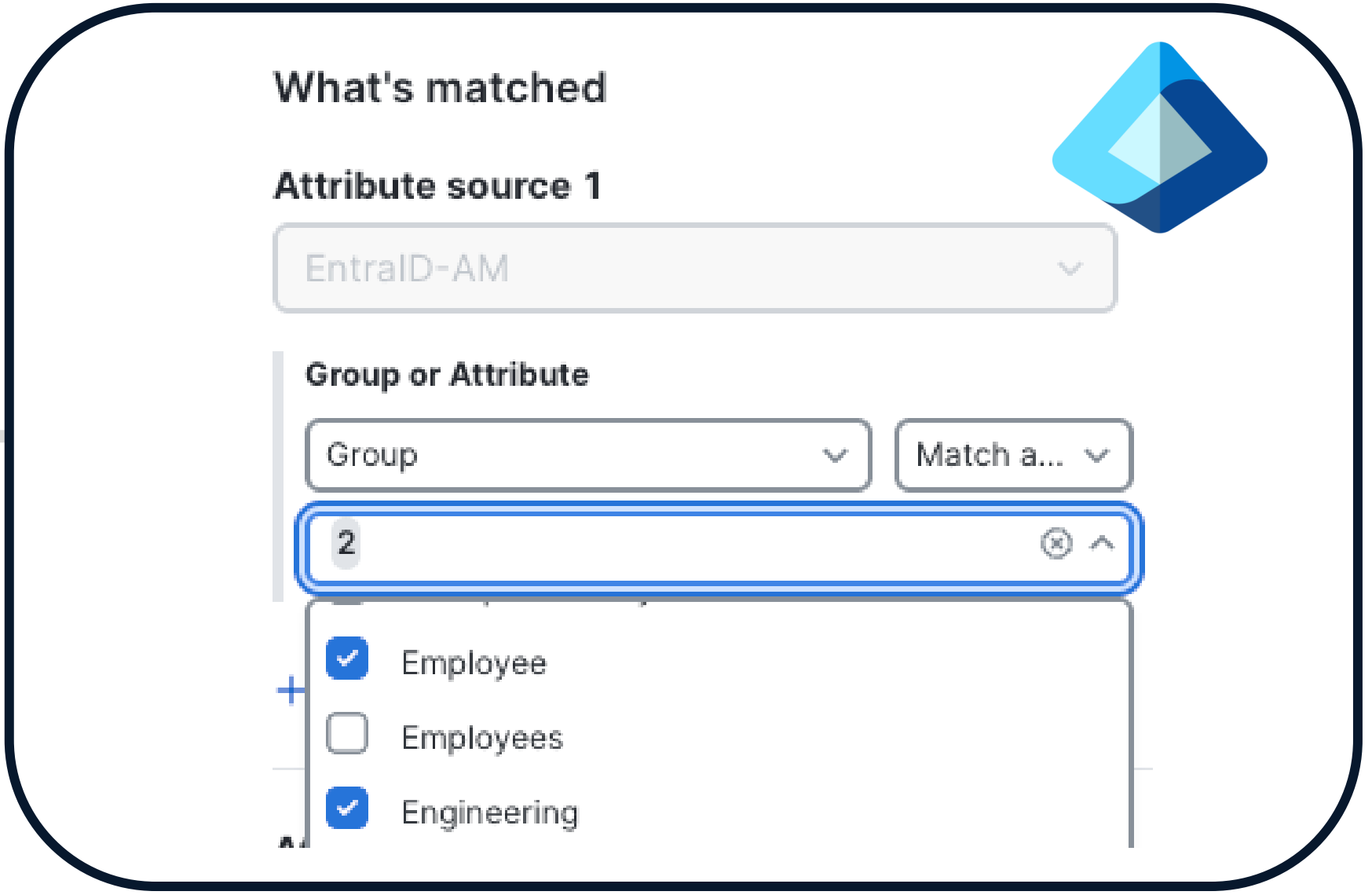


© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Access Manager – EAP-TLS Authentication

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

Cisco Access Manager – EAP-TLS Authentication



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

Cisco Access Manager – EAP-TLS Authentication

What's matched

Attribute source 1

Endpoint certificate

Group or Attribute

Issuer - Organizational Unit | Contains

APJC

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

Cisco Access Manager – EAP-TLS Authentication

What's matched

Attribute source 1

Network Access

Group or Attribute

SSID

1

isedtea

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

Cisco Access Manager – EAP-TLS Authentication

What's matched

Attribute source 1

Network Access

Group or Attribute

Connection Method

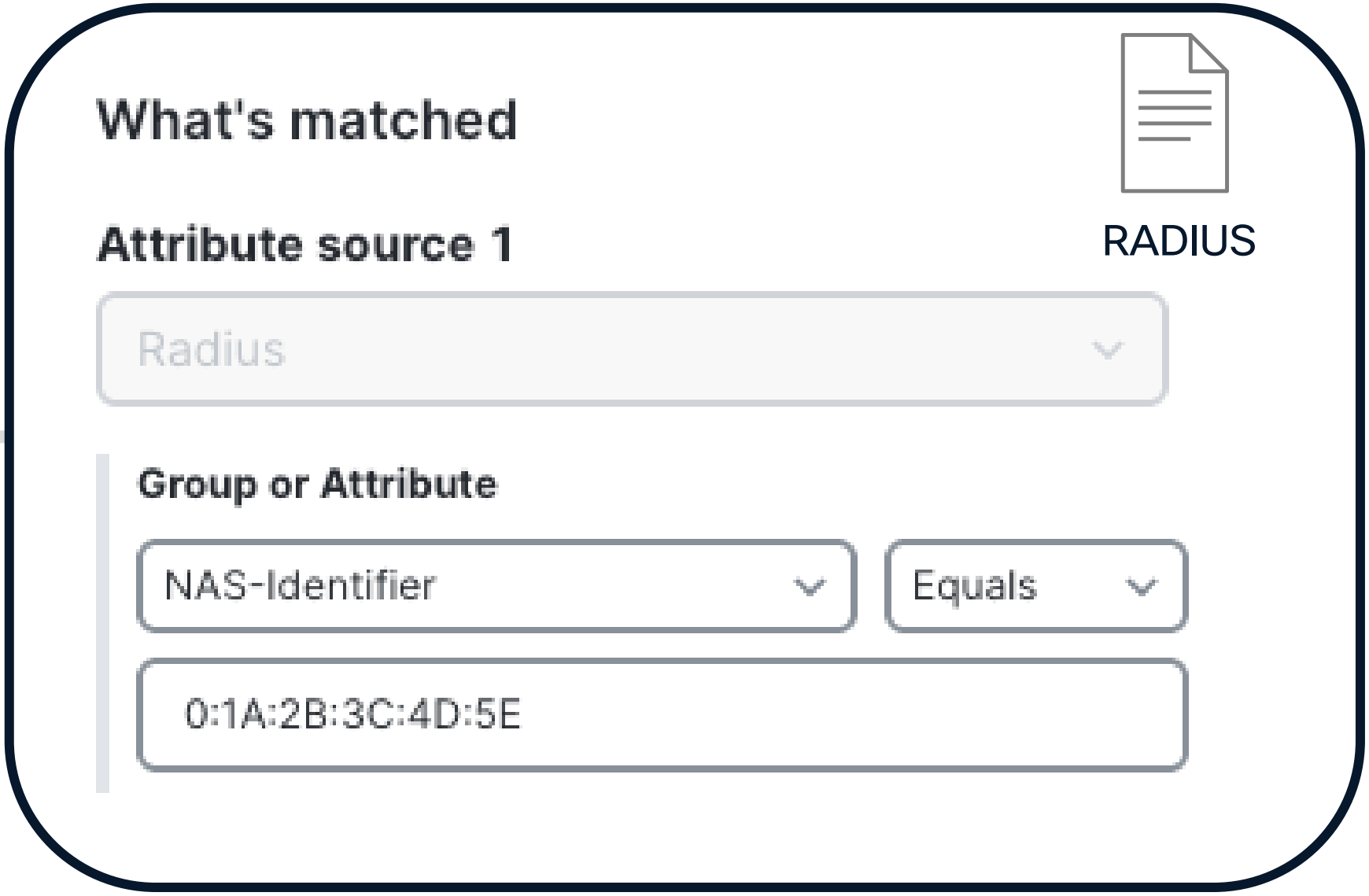
1

Wired

Wireless

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

Cisco Access Manager – EAP-TLS Authentication



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

Cisco Access Manager – EAP-TLS Authentication

Authorization

Access permission

Allow restricted access

VLAN ID / name

30

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

Cisco Access Manager – EAP-TLS Authentication

Authorization

Access permission

Allow restricted access

Adaptive policy

Infrastructure

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

Cisco Access Manager – EAP-TLS Authentication

Authorization

Access permission

Allow restricted access

Identity PSK

CiscoLiveRocks Hide

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

Cisco Access Manager – EAP-TLS Authentication

Authorization

Access permission

Allow restricted access

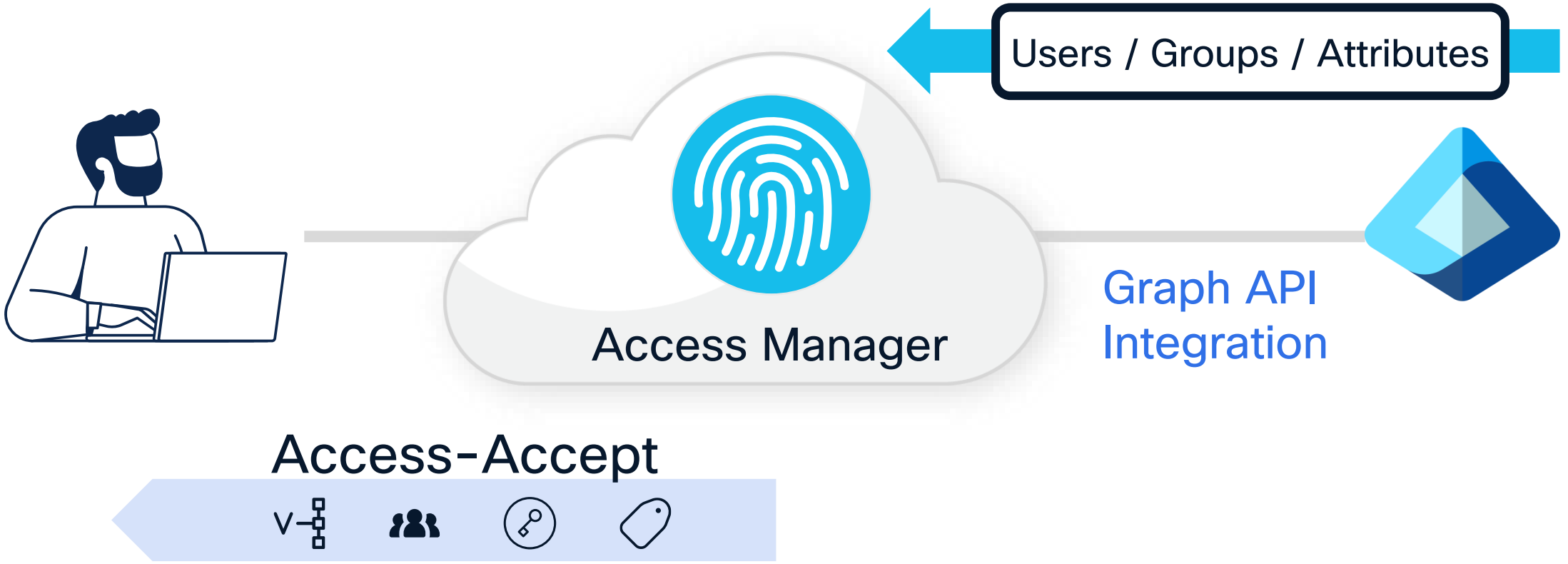
Group policy

Employee

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

cisco

Cisco Access Manager – EAP-TLS Authentication



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

Cisco Access Manager – EAP-TTLS Authentication

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

Cisco Access Manager – EAP-TTLS Authentication

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

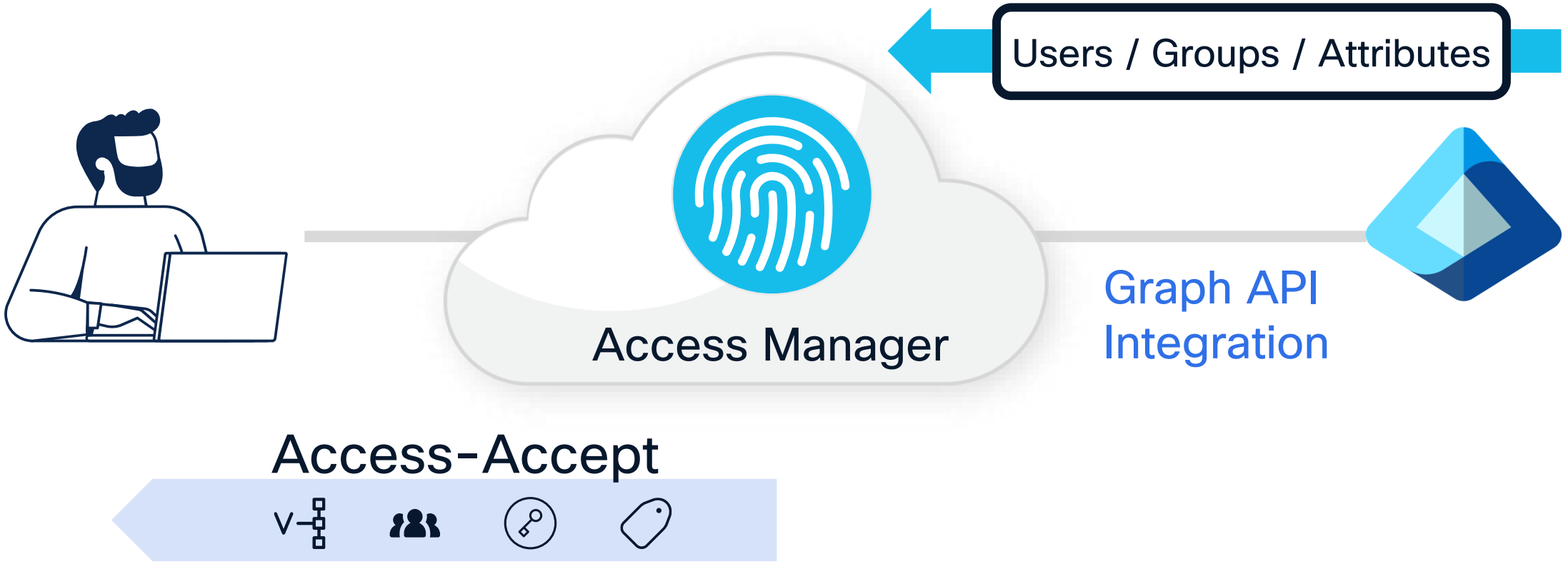
Cisco Access Manager – EAP-TTLS Authentication

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

Cisco Access Manager – EAP-TTLS Authentication

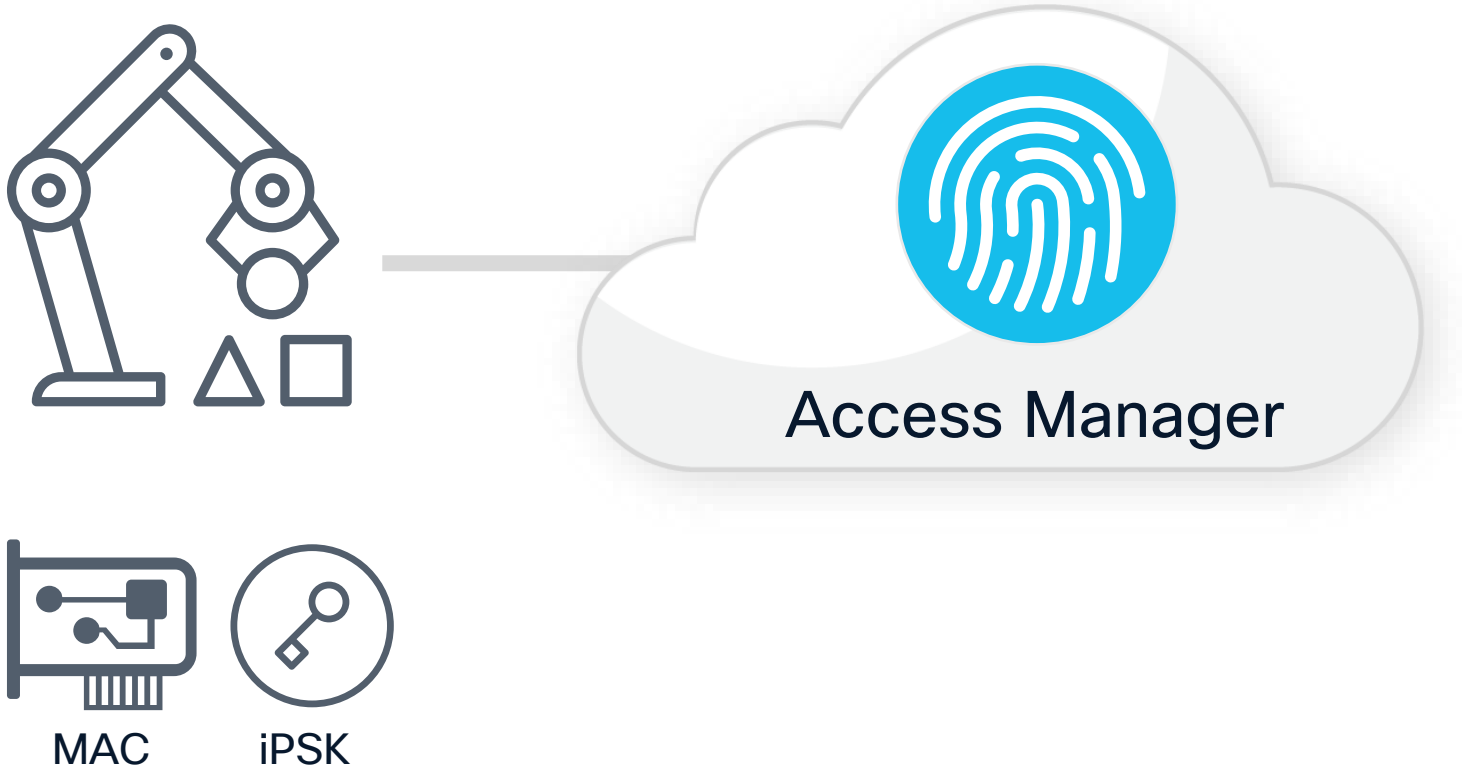
© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Access Manager – EAP-TTLS Authentication



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

Cisco Access Manager – iPSK/MAB Authentication



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

Cisco Access Manager – iPSK/MAB Authentication

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

Cisco Access Manager – iPSK/MAB Authentication

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

Cisco Access Manager – iPSK/MAB Authentication

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

Cisco Access Manager – Feature Summary

Reference

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

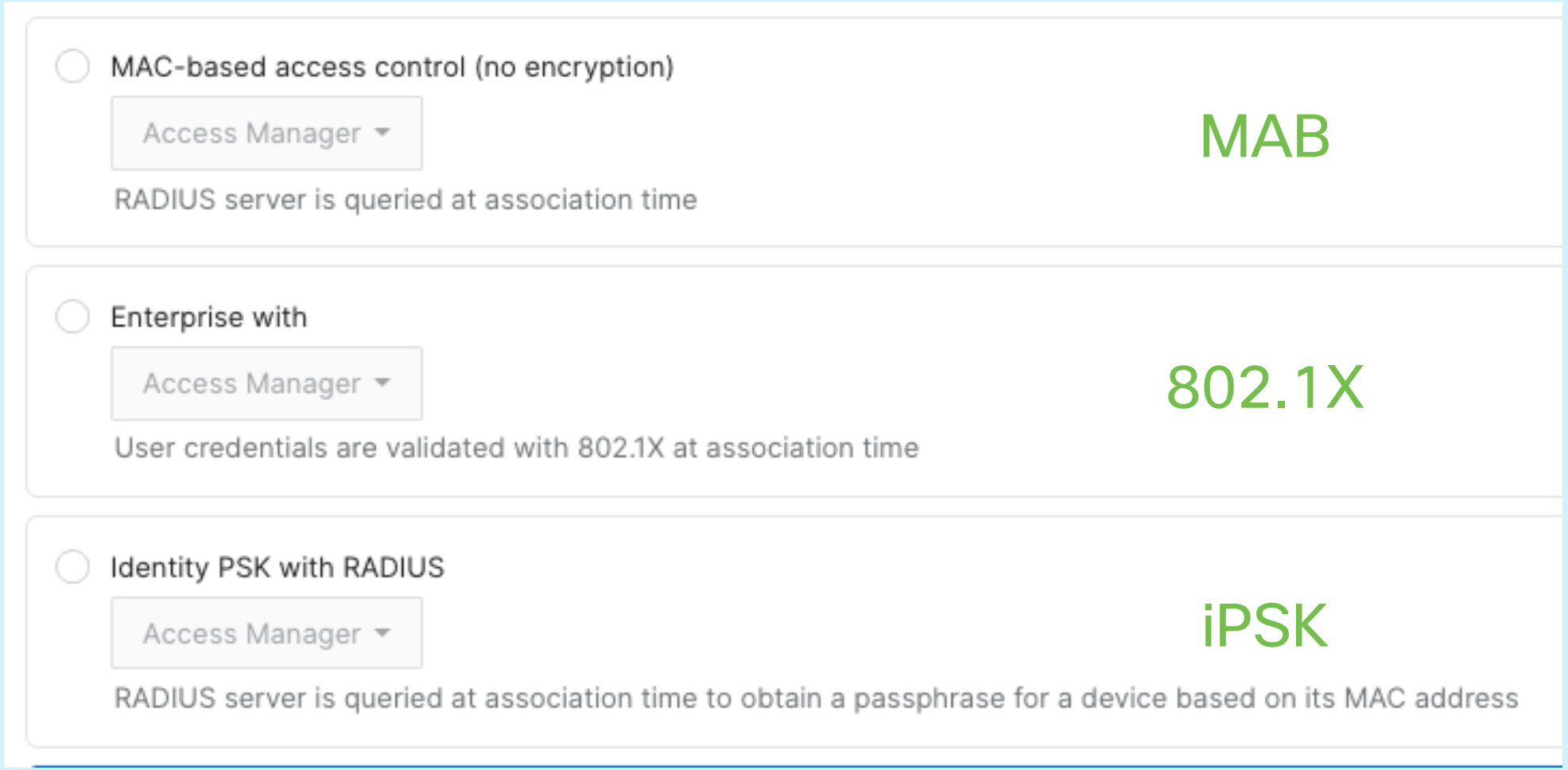
- Adaptive Policy Group
- Group Policy
- VLAN
- iPSK

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

cisco

Wireless Configuration for Access Manager

Wireless > Configure > Access Control



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

cisco

Access Rules

Access Manager > Policies > Access Rules

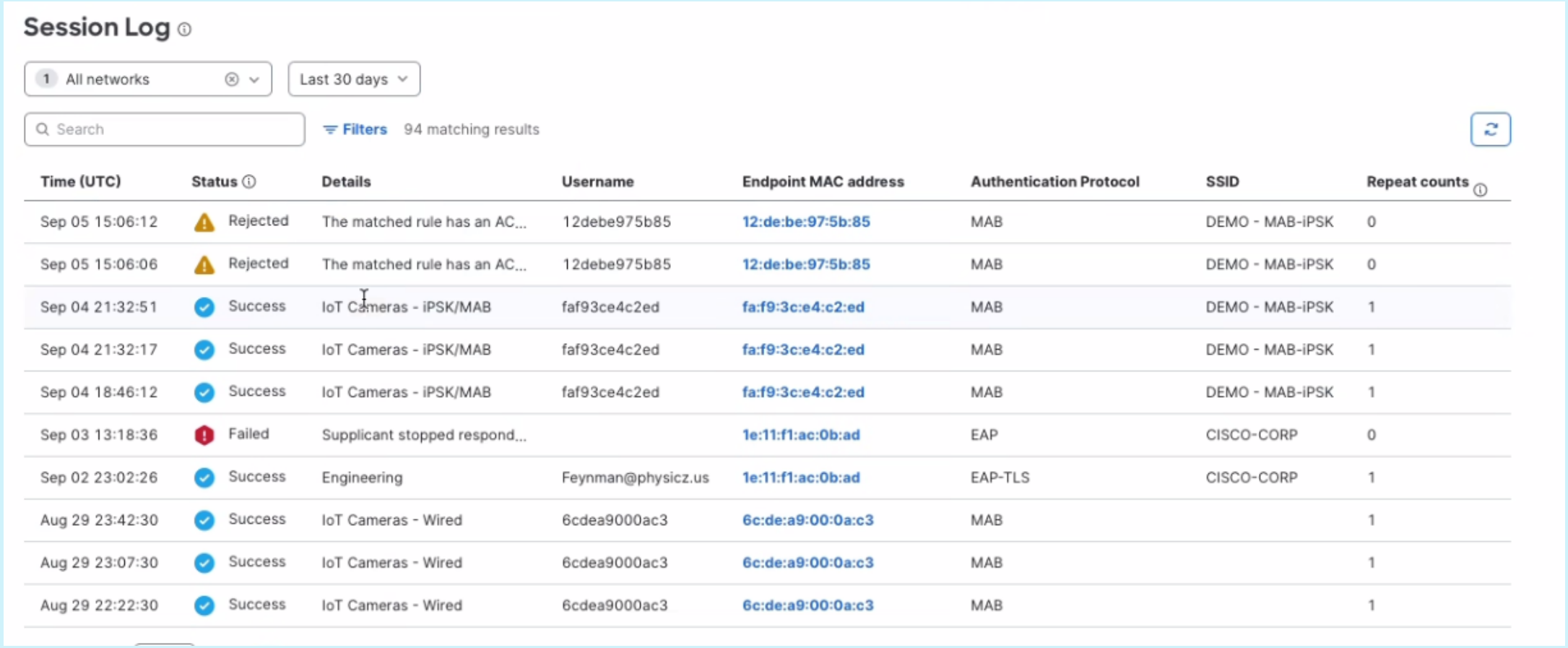
	Type	Status	Name	What's matched	Authorization	
	Rule group	✓	Default rule group	Any		
⠿	└ Rule	✓	Entra-ID-Group-Sales	MerakiNation-EntraID: Group = SALES [And] LAUNCHPAD	VLAN = 10 Adaptive policy = employees-sales	···
⠿	└ Rule	✓	EAP-TLS-certificate-SEs	Endpoint certificate: Issuer - Organization [Contains] 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

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

Session Log

Access Manager > Monitor > Session Log



Session Log

1 All networks | Last 30 days

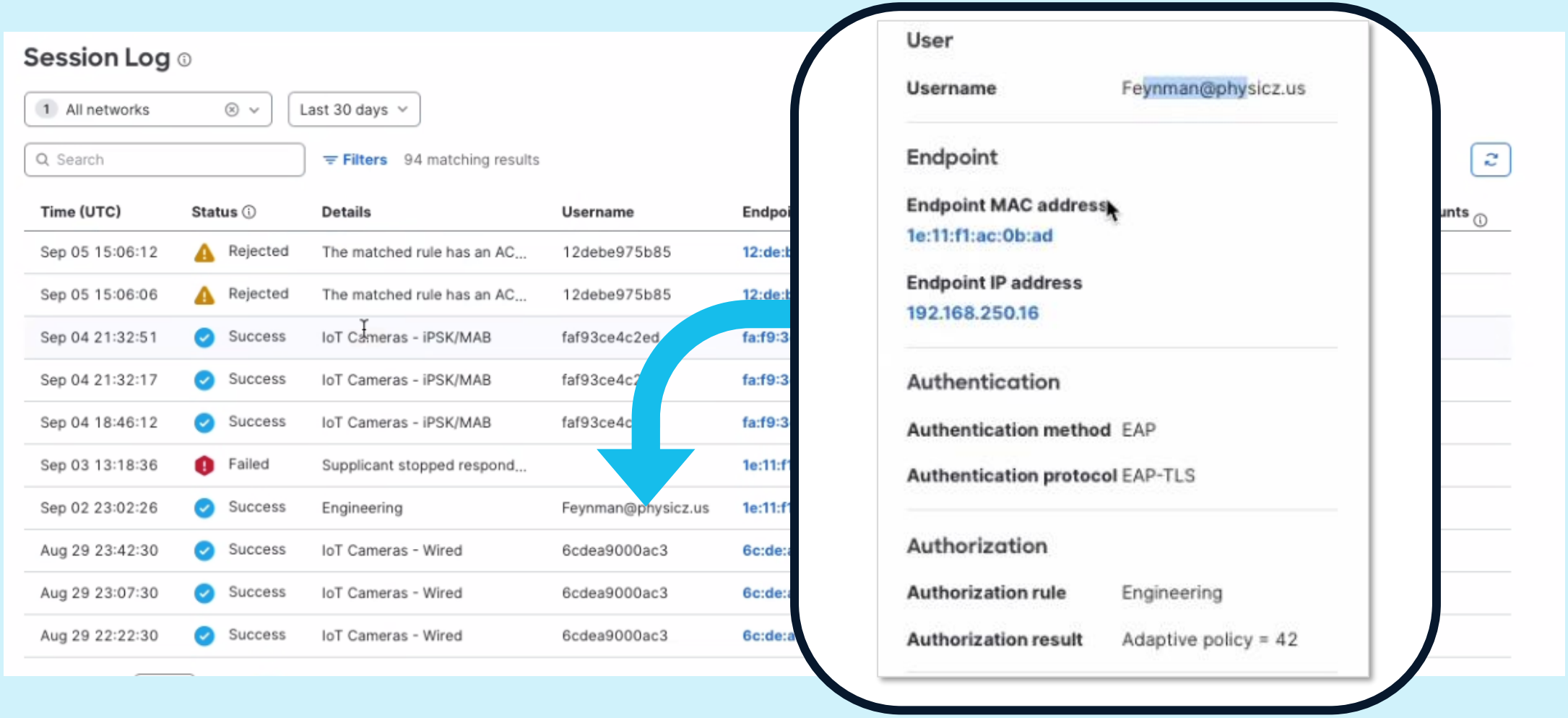
Search | Filters | 94 matching results

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

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

Session Log

Access Manager > Monitor > Session Log



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

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.

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

Complete your session evaluations

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

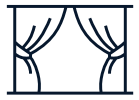
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

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

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

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

Thank you

cisco Live !

CISCO