

Configure Catalyst 9800 WLC iPSK with ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Understand what iPSK is and which scenarios it fits](#)

[Configure 9800 WLC](#)

[ISE Configuration](#)

[Troubleshoot](#)

[Troubleshoot on the 9800 WLC](#)

[Troubleshoot ISE](#)

Introduction

This document describes the configuration of an iPSK secured WLAN on a Cisco 9800 Wireless LAN Controller with Cisco ISE as a RADIUS server.

Prerequisites

Requirements

- Familiarity with the basic configuration of a WLAN on 9800
- Ability to adapt the configuration to your deployment

Components Used

- Cisco 9800-CL WLC that runs 17.6.3
- Cisco ISE 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

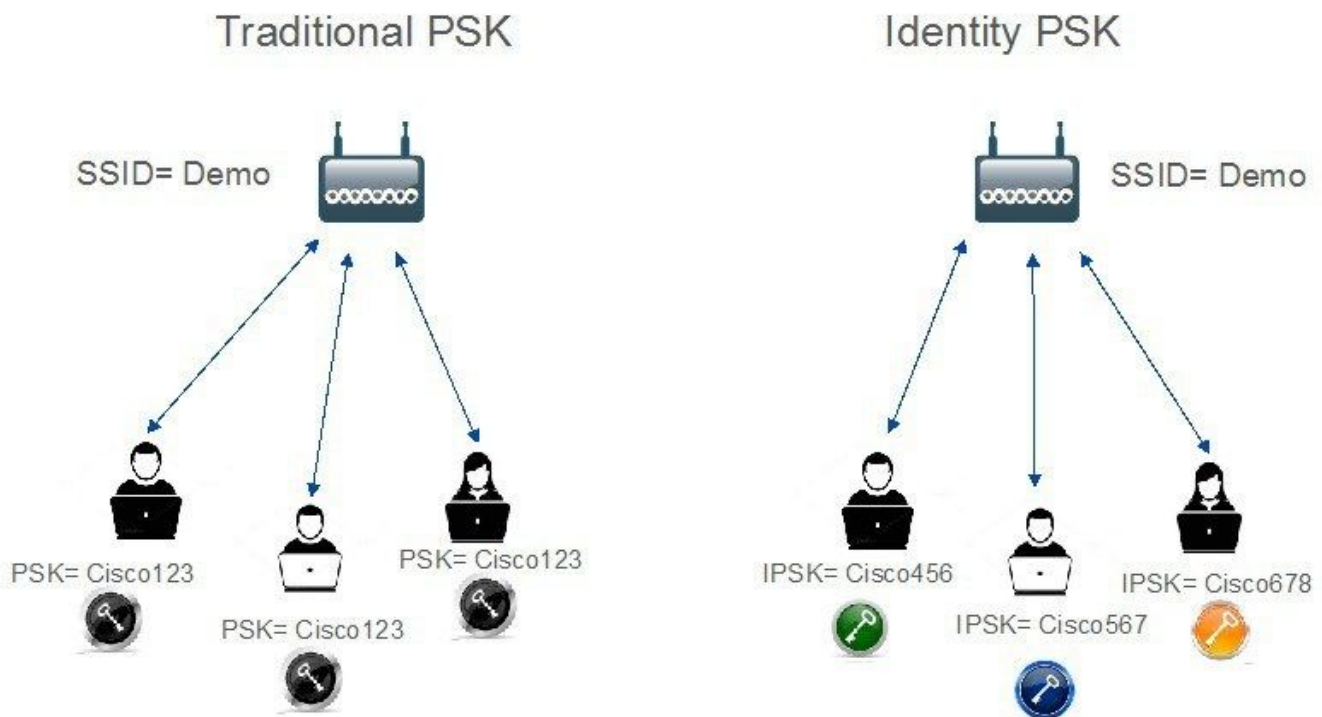
Understand what iPSK is and which scenarios it fits

Traditional Pre-Shared Key (PSK) secured networks use the same password for all the connected clients. This can result in the key shared with unauthorized users causing a security breach and unauthorized access to the network. The most common mitigation of this breach is the change of the PSK itself. This impacts all users because many end devices need to be updated with the new key in order to access the network again.

With Identity PSK (iPSK), unique pre-shared keys are created for individuals or a group of users on the same SSID with the help of a RADIUS server. This kind of setup is extremely useful in networks where end-client devices do not support dot1x authentication, but a more secure and granular authentication scheme is needed. From a client perspective, this WLAN looks identical to the traditional PSK network. In

the event of one of the PSKs is compromised, only the affected individual or group need to have their PSK updated. The rest of the devices connected to the WLAN are unaffected.

Traditional Vs Identity PSK



Configure 9800 WLC

Under **Configuration > Security > AAA > Servers/Groups > Servers**, add the ISE as RADIUS server:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Address	Auth Port	Acct Port
ISE_IPSK	10.48.39.126	1812	1813

1 - 1 of 1 items

Under **Configuration > Security > AAA > Servers/Groups > Server Groups**, create a RADIUS server group and add the previously created ISE server to it:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Server 1	Server 2	Server 3
<input type="checkbox"/> ISE_IPSK_Group	ISE_IPSK	N/A	N/A

10 items per page 1 - 1 of 1 items

In the **AAA Method List** tab, create an **Authorization** list with Type “**network**” and the Group Type “**group**” pointing to the previously made RADIUS server group:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Authz_List_IPSK	network	group	ISE_IPSK_Group	N/A	N/A	N/A

10 items per page 1 - 1 of 1 items

Setting up Accounting is optional, but can be done by configuring the Type to “**identity**” and pointing it to the same RADIUS server group:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name	Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Acc_List_IPSK	identity	ISE_IPSK_Group	N/A	N/A	N/A

10 items per page 1 - 1 of 1 items

This can also be performed through the command line using:

```
radius server <server_name>  
address ipv4 <ip_addr> auth-port 1812 acct-port 1813  
key 0 <shared_secret_key>
```

```
aaa group server radius <server_group_name>  
server name <server_name>
```

```
aaa authorization network <authz_method_name> group <server_group_name>
```

```
aaa accounting identity <acct_method_name> start-stop group <server_group_name>
```

Under **Configuration > Tags & Profiles > WLANs**, create a new WLAN. Under Layer 2 configuration:

- Enable MAC filtering and set the Authorization List to the one previously created
- Under **Auth Key Mgmt** enable **PSK**
- The pre-shared key field can be filled with any value. This is done only to satisfy the requirement of the web interface design. No user is able to authenticate using this key. In this case the pre-shared key was set to “12345678”.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Authorization List* Authz_List... ▼ ⓘ

Protected Management Frame

PMF Disabled ▼

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 Easy-PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

PSK Format ASCII ▼

PSK Type Unencrypted ▼

Pre-Shared Key*| 🔒

Lobby Admin Access

Fast Transition Adaptive Enabled▼

Over the DS

Reassociation Timeout 20

MPSK Configuration

MPSK

User segregation can be achieved under the **Advanced** tab. Setting it to Allow Private Group allows the users using the same PSK to communicate between each other, while the users using a different PSK are blocked off:

General	Security	Advanced	Add To Policy Tags
Coverage Hole Detection	<input checked="" type="checkbox"/>		Universal Admin <input type="checkbox"/>
Aironet IE ⓘ	<input type="checkbox"/>		OKC <input checked="" type="checkbox"/>
Advertise AP Name	<input type="checkbox"/>		Load Balance <input type="checkbox"/>
P2P Blocking Action	Allow Private Group ▼		Band Select <input type="checkbox"/>
Multicast Buffer	<input type="checkbox"/> DISABLED		IP Source Guard <input type="checkbox"/>

Under **Configuration** > **Tags & Profiles** > **Policy**, create a new Policy Profile. In the **Access Policies** tab, set the VLAN or VLAN group this WLAN is using:

Add Policy Profile ✕

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
WLAN Local Profiling				
Global State of Device Classification ⓘ				
Local Subscriber Policy Name	Search or Select ▼			
VLAN				
VLAN/VLAN Group	VLAN0039 ▼			
Multicast VLAN	Enter Multicast VLAN			
				WLAN ACL IPv4 ACL Search or Select ▼ IPv6 ACL Search or Select ▼ URL Filters Pre Auth Search or Select ▼ Post Auth Search or Select ▼

In the **Advanced** tab, enable AAA Override and add Accounting list if previously created:

Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List ⓘ ✕

Fabric Profile

Link-Local Bridging

mDNS Service Policy

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS ENABLED

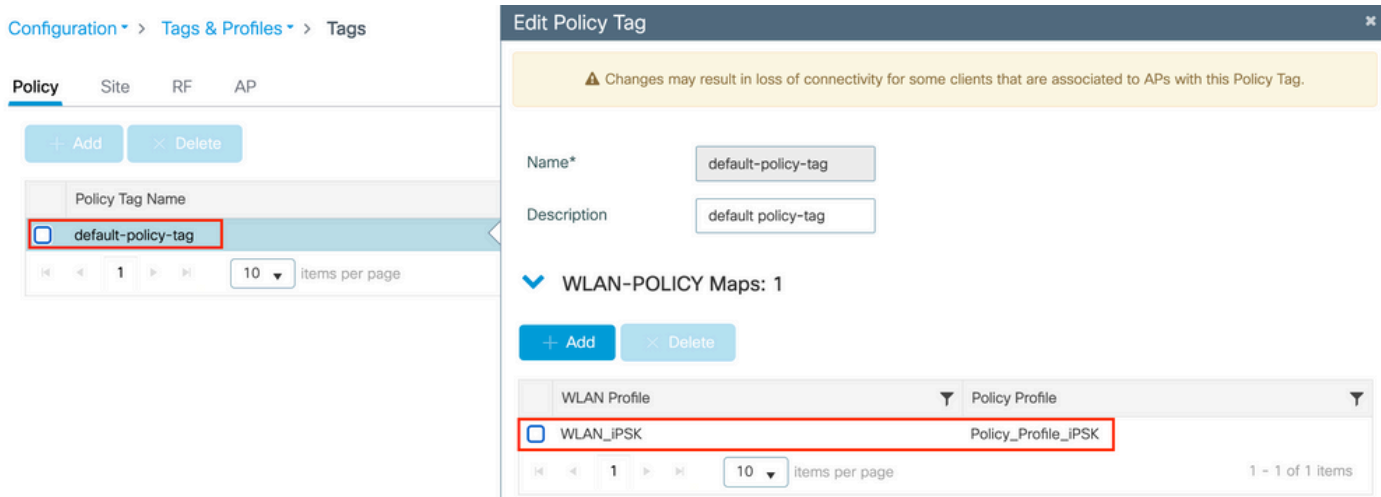
Flex DNS Traffic Redirect IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Under **Configuration > Tags & Profiles > Tags > Policy**, make sure that the WLAN is mapped to the Policy profile you created:



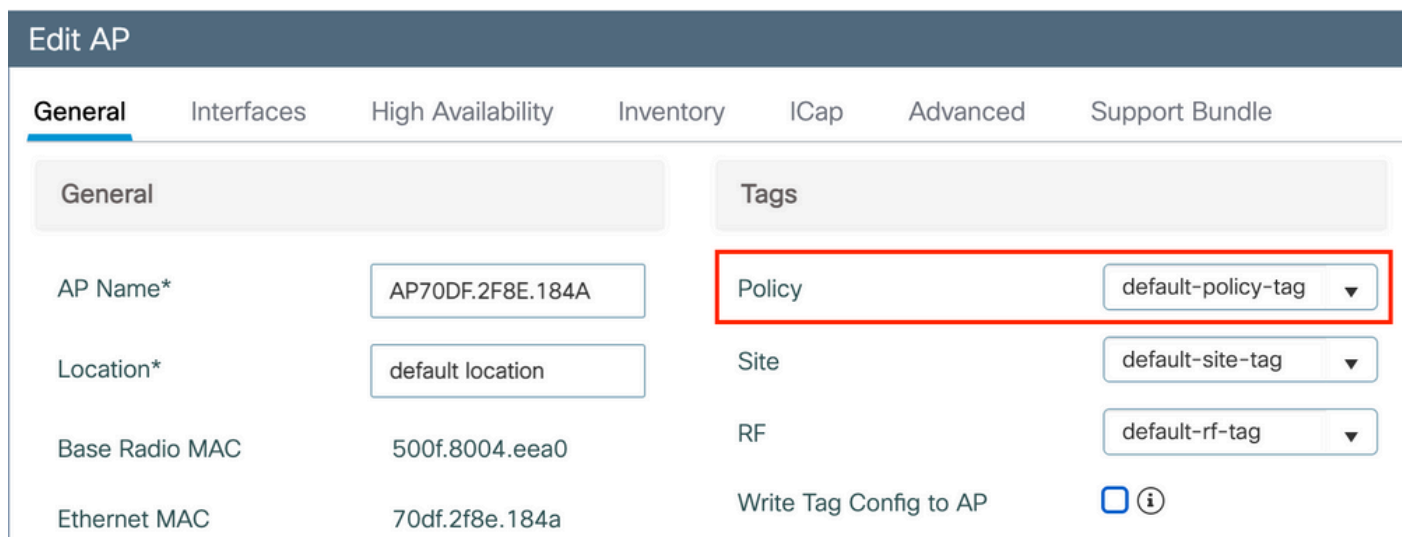
This can also be performed through the command line using:

```
wlan <wlan_name> <wlan_ID> <ssid_name>
mac-filtering <authz_method_name>
security wpa psk set-key ascii 0 <default_psk>
no security wpa akm dot1x
security wpa akm psk
peer-blocking allow-private-group
no shutdown
```

```
wireless profile policy <policy_name>
aaa-override
accounting-list <acct_method_name>
vlan <vlan_name>
no shutdown
```

```
wireless tag policy <policy_tag_name>
wlan <wlan_name> policy <policy_name>
```

Under **Configuration > Wireless > Access Points**, make sure that this tag has been applied on the Access Points on which the WLAN has to be broadcasted:



ISE Configuration

This config guide covers a scenario where the PSK of the device is determined based on the client MAC address. Under **Administration > Network Resources > Network Devices**, add a new device, specify the IP address, enable the RADIUS Authentication Settings and specify a RADIUS Shared Secret:

The screenshot displays the Cisco ISE Administration interface for configuring a new Network Device. The breadcrumb navigation is **Administration > Network Resources > Network Devices**. The left sidebar shows the **Network Devices** menu. The main content area is titled **Network Devices** and shows the configuration for a new device named **9800-WLC**. The **IP Address** is set to **10.48.38.86 / 32**. The **Device Profile** is set to **Cisco**. The **Network Device Group** is set to **All Locations**. The **Location** is set to **All Locations**. The **IPSEC** is set to **Is IPSEC Device**. The **Device Type** is set to **All Device Types**. The **RADIUS Authentication Settings** are enabled, and the **Protocol** is set to **RADIUS**. The **Shared Secret** is masked with dots and a **Show** button is visible.

Administration · Network Resources

Network Devices

Network Devices List > New Network Device

Network Devices

* Name 9800-WLC

Description

IP Address * IP: 10.48.38.86 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location All Locations Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret Show

Under **Context Visibility > Endpoints > Authentication**, add the MAC addresses of all the devices (clients) that are connecting to the iPSK network:

Cisco ISE Context Visibility - Endpoints

Authentication BYOD Compliance Compromised Endpoints Endpoint Classification Guest Vulnerable Endpoints Hardware

INACTIVE ENDPOINTS AUTHENTICATION STATUS AUTHENTIFICATIONS NETWORK DE

No data available. No data available.

Rows/Page 1 / 1 Total Rows

MAC Address Status IP Address Username Hostname Location Endpoint Profile Authentication Failure Re... Authentication ... Authorization P..

MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Reason	Authentication Policy	Authorization Policy
08-BE-AC:27:85:7E	*		08beac278...		Location...	Unknown	-	MAB	Basic_Authenticat...

Under **Administration > Identity Management > Groups > Endpoint Identity Groups**, create one or more groups and assign users to them. Each group can later be configured to use a different PSK to connect to the network.

Cisco ISE Administration - Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Endpoint Identity Groups

Selected 0 Total 18

Edit Add Delete

Name	Description
Android	Identity Group for Profile: Android
Apple-iDevice	Identity Group for Profile: Apple-iDevice

Cisco ISE Administration - Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Endpoint Identity Group List > New Endpoint Group

Endpoint Identity Group

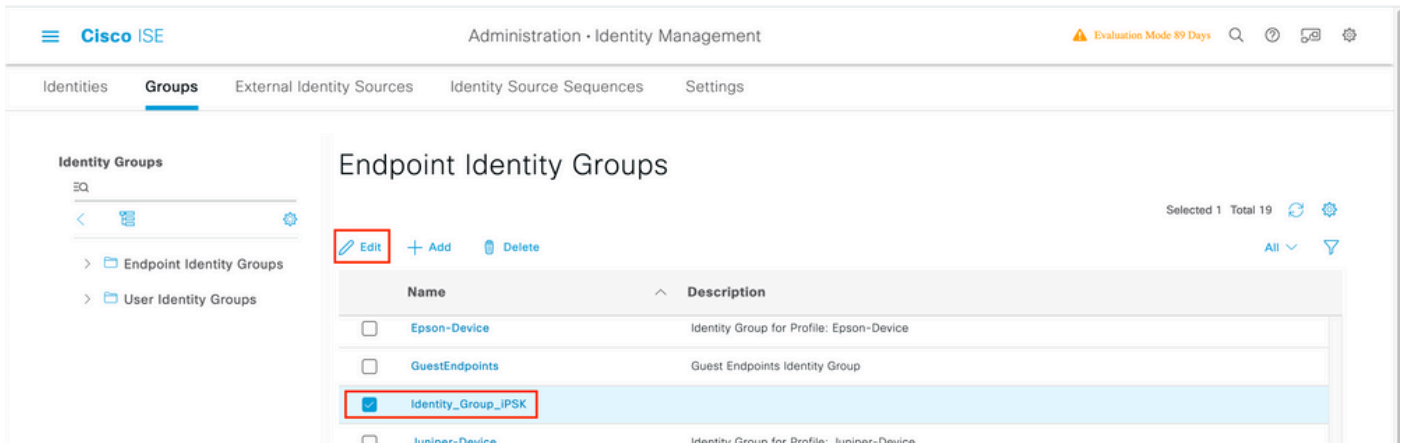
* Name Identity_Group_IPSK

Description

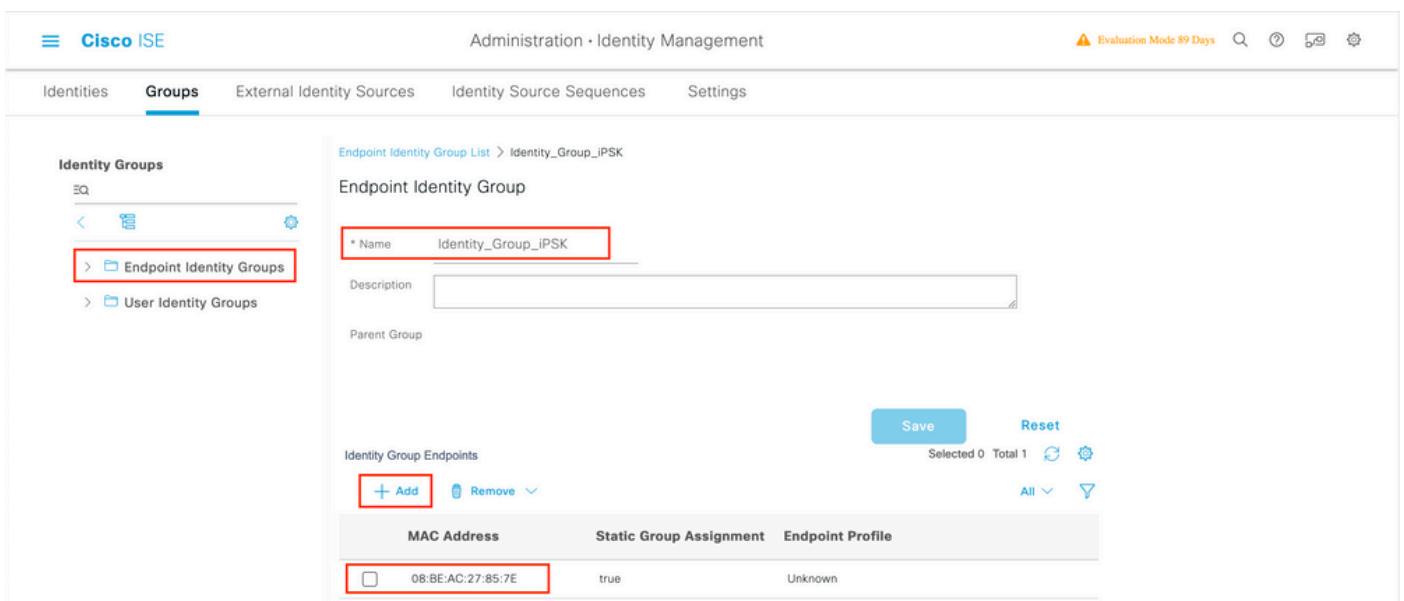
Parent Group

Submit Cancel

Once the group is created, you can now assign users to them. Select the group you created, and click **Edit**:



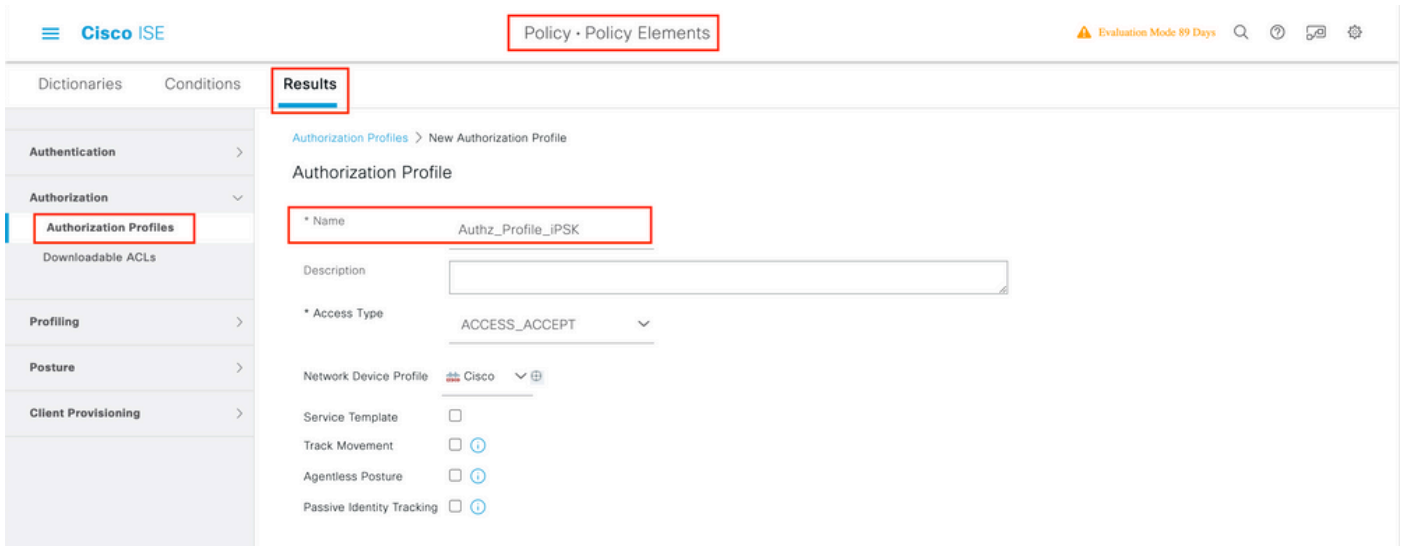
In the group configuration, add the MAC address of the client(s) you want to assign to this group by clicking the "Add" button:



Under **Policy > Policy Elements > Results > Authorization > Authorization Profiles**, create a new authorization profile. Set attributes to be:

```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=<PSK to be used> // This is the psk that the user group is using
```

For each user group that must be using a different PSK, create an additional result with a different psk av-pair. Additional parameters like ACL and VLAN override can also be configured here.



Under **Policy > Policy Sets**, create a new one. To make sure that the client matches the policy set, this condition is used:

```
<#root>
```

```
Cisco:cisco-av-pair
```

```
EQUALS
```

```
cisco-wlan-ssid=WLAN_iPSK // "WLAN_iPSK" is WLAN name
```

Conditions Studio

Library

Search by Name

Library of conditions including:

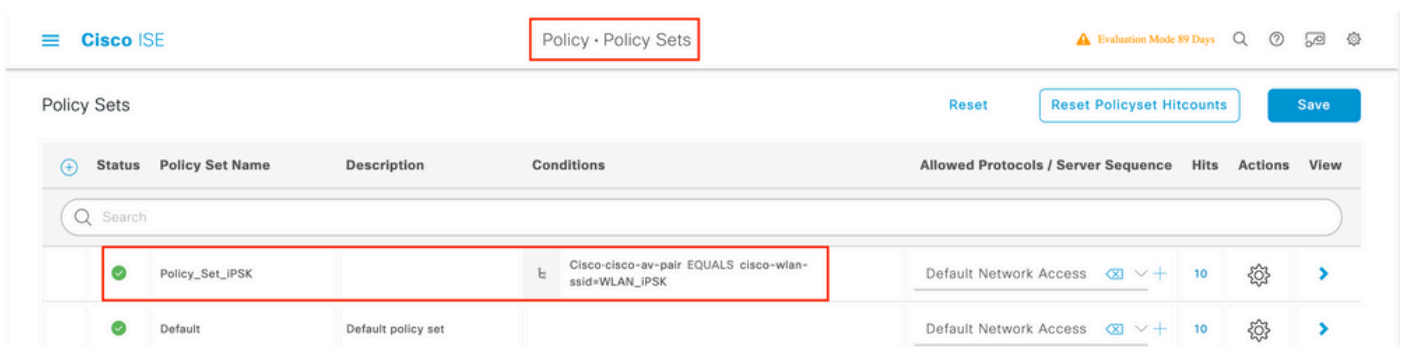
- Catalyst_Switch_Local_Web_Authentication
- Switch_Local_Web_Authentication

Editor

Editor interface showing the configuration of a condition:

- Object: Cisco:cisco-av-pair
- Operator: Equals
- Value: cisco-wlan-ssid=WLAN_iPSK
- Buttons: Duplicate, Save
- Logic: NEW AND OR

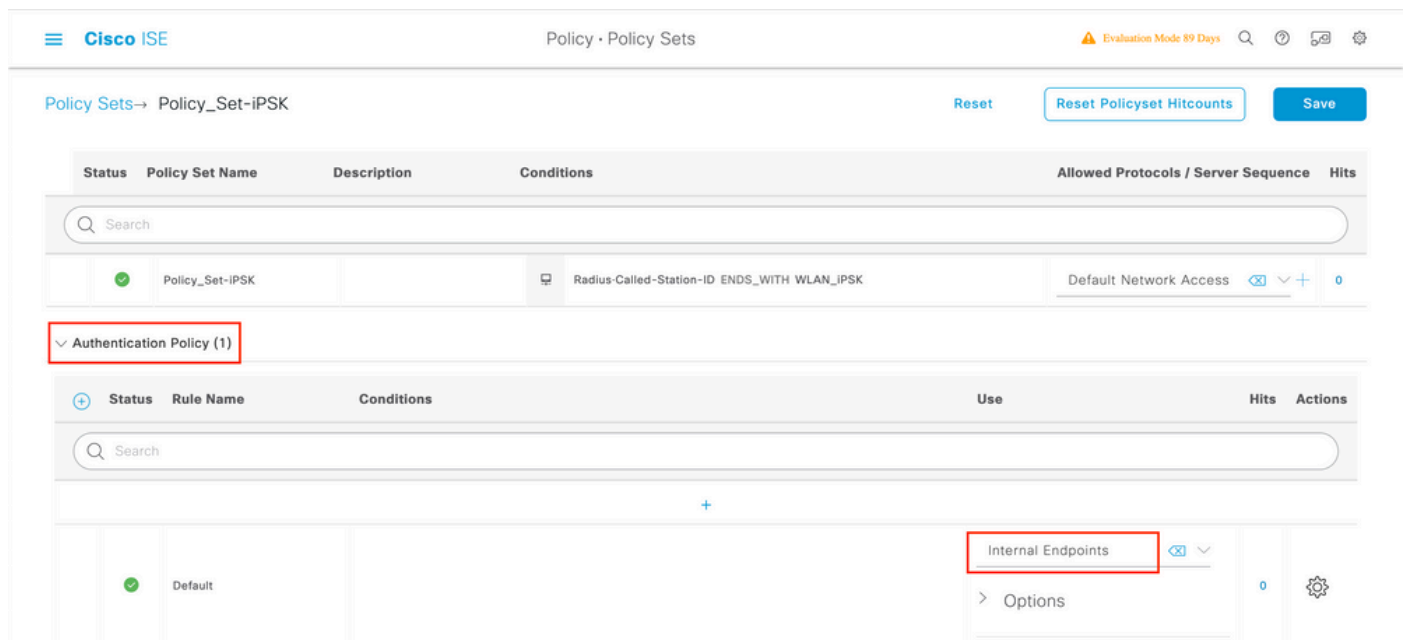
Additional conditions can be added to make policy matching more secure.



Go to the newly created iPSK Policy Set configuration by clicking the blue arrow on the right of the Policy Set line:



Make sure that **Authentication Policy** is set to "Internal Endpoints":



Under **Authorization Policy**, create a new rule for each of the user groups. As a condition, use:

```
<#root>
```

```
IdentityGroup-Name
```

```
EQUALS
```

```
Endpoint Identity Group:Identity_Group_iPSK // "Identity_Group_iPSK" is name of the created endpo
```

with the **Result** being the **Authorization Profile** that was previously created. Make sure that the **Default** Rule stays at the bottom and points to **DenyAccess**.

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Search

Internal Endpoints Options

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK	Select from list		
✓	Default		DenyAccess	Select from list	0	


If every user is going to have a different password, instead of creating Endpoint groups and rules matching that endpoint group, a rule with this condition can be made:

<#root>

Radius-Calling-Station-ID

EQUALS

<client_mac_addr>

 **Note:** MAC address delimiter can be configured on the WLC under **AAA >AAA Advanced > Global Config > Advanced Settings**. In this example, the character "-" was used.

Cisco ISE Policy - Policy Sets Evaluation Mode 89 Days

Search

Internal Endpoints Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Authz_Rule_Single	Radius-Calling-Station-ID EQUALS 08-BE-AC-27-85-7E	Authz_Profile_IPSK x	Select from list		
✓	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK x	Select from list		
✓	Default		DenyAccess x	Select from list	0	

Rules on the authorization policy allow many other parameters to be used in order to specify the password the user is utilizing.

Some of the most commonly used rules are:

1. Matching based on the user location

In this scenario, the WLC needs to send AP Location information to the ISE. This allows users in one location to use one password, while the users on another location is using a different one. This can be configured under the **Configuration > Security > Wireless AAA Policy**:

Edit Wireless AAA Policy

Policy Name* default-aaa-policy

NAS-ID Option 1 System Name

NAS-ID Option 2 AP Location

NAS-ID Option 3 Not Configured

2. Matching based on the device profiling

In this scenario, the WLC needs to be configured to profile devices globally. This allows an administrator to configure different password for laptop and phone devices. Global device classification can be enabled under **Configuration > Wireless > Wireless Global**. For device profiling configuration on ISE, consult the [ISE Profiling Design Guide](#).

On top of returning the encryption key, since this authorization happens at the 802.11 association phase, it is entirely possible to return other AAA attributes from ISE such as ACL or VLAN id.

Troubleshoot

Troubleshoot on the 9800 WLC

On the WLC, collecting radioactive traces must be more than enough to identify a majority of issues. This can be done in the WLC web interface under **Troubleshooting > Radioactive Trace**. Add the client MAC address, press **Start** and try to reproduce the issue. Click on **Generate** to create the file and download it:

Troubleshooting > Radioactive Trace


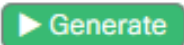
Conditional Debug Global State: **Stopped**


+ Add

× Delete

✓ Start

■ Stop

	MAC/IP Address	Trace file	
<input type="checkbox"/>	74da.38f6.76f0	debugTrace_74da.38f6.76f0.txt 	
◀ 1 ▶		20 items per page	1 - 1 of 1 items

 **Important:** iPhones on IOS 14 and Android 10 smartphones use randomised mac address when associating to the network. This functionality can completely break the iPSK configuration. Make sure that this feature is disabled!

If Radioactive Traces are not enough to identify the problem, packet captures can be collected directly on the WLC. Under **Troubleshooting > Packet Capture**, add a capture point. By default, WLC uses Wireless Management interface for all RADIUS AAA communication. Increase the buffer size to 100 MB if the WLC has high number of clients:

Edit Packet Capture

Capture Name*

Filter*

Monitor Control Plane

Buffer Size (MB)*

Limit by* secs ~ 1.00 hour

Available (4)

- GigabitEthernet1
- GigabitEthernet2
- GigabitEthernet3
- Vlan1

Selected (1)

- Vlan39

A packet capture of a successful authentication and accounting attempt is shown in the picture below. Use this Wireshark filter to filter out all the relevant packets for this client:

```
ip.addr==<ISE_IP_ADDR> || eapol || bootp
```

wlc pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.48.39.134 || eapol || bootp

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.48.39.212	10.48.39.134	RADIUS	430	56240	1812	Access-Request id=123
2	0.014007	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123
3	0.000000	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123, Duplicate Response
4	5.944995	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	203	5247	5253	Key (Message 1 of 4)
5	0.005004	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	213	5253	5247	Key (Message 2 of 4)
6	0.001007	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	237	5247	5253	Key (Message 3 of 4)
7	0.004990	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	191	5253	5247	Key (Message 4 of 4)
8	4.318043	10.48.39.212	10.48.39.134	RADIUS	569	56240	1813	Accounting-Request id=124
9	0.013992	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124
10	0.000000	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124, Duplicate Response

Troubleshoot ISE

The main troubleshooting technique on Cisco ISE is the **Live Logs** page, found under **Operations > RADIUS > Live Logs**. They can be filtered by putting the MAC address of the client in the Endpoint ID field. Opening a full ISE report gives more details about the failure reason. Make sure that the client is hitting the correct ISE policy:

Live Logs

Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 1

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Refresh | Reset Repeat Counts | Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentic...	Authoriz...	Authorization Pro...	IP Address
Aug 19, 2022 08:04:20.5...			1	08:BE:AC:27:8...	08:BE:AC:27:85:7E	Unknown	Policy_Set...	Policy_Set...	Authz_Profile_IPSK	fe80::e864:b6
Aug 19, 2022 08:04:13.3...				08:BE:AC:27:8...	08:BE:AC:27:85:7E	Unknown	Policy_Set...	Policy_Set...	Authz_Profile_IPSK	