

ISE를 사용하여 Catalyst 9800 WLC iPSK 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[iPSK가 무엇이며 어떤 시나리오에 적합한지 이해](#)

[9800 WLC 구성](#)

[ISE 구성](#)

[문제 해결](#)

[9800 WLC에서 문제 해결](#)

[ISE 문제 해결](#)

소개

이 문서에서는 Cisco ISE를 RADIUS 서버로 사용하는 Cisco 9800 Wireless LAN Controller에서 iPSK 보안 WLAN의 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 9800의 WLAN의 기본 컨피그레이션에 대해 이미 잘 알고 있으며 컨피그레이션을 구축에 맞게 조정할 수 있다고 가정합니다.

사용되는 구성 요소

- 17.6.3을 실행하는 Cisco 9800-CL WLC
- Cisco ISE 3.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

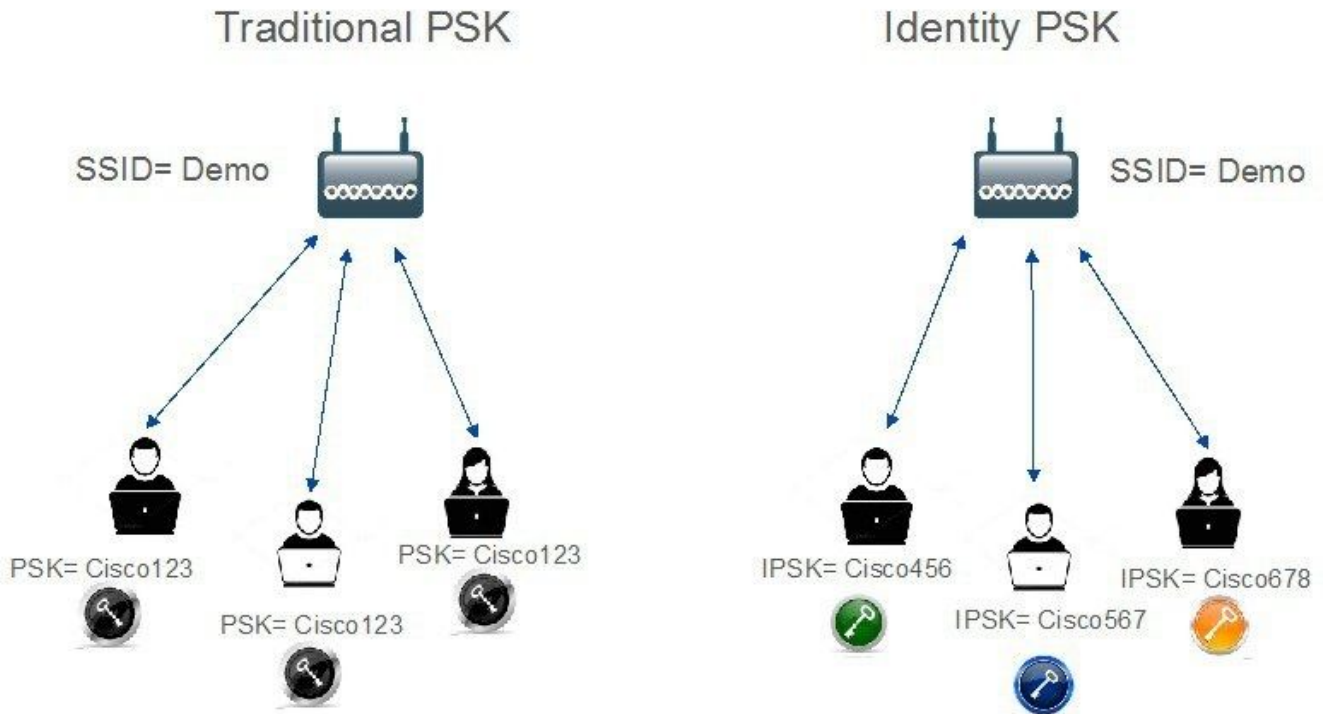
iPSK가 무엇이며 어떤 시나리오에 적합한지 이해

기존의 PSK(Pre-Shared Key) 보안 네트워크는 연결된 모든 클라이언트에 동일한 비밀번호를 사용합니다. 따라서 권한이 없는 사용자와 키를 공유하여 보안 침해를 일으키고 네트워크에 대한 무단 액세스를 초래할 수 있습니다. 이러한 보안 침해의 가장 일반적인 완화 방법은 PSK 자체를 변경하는 것입니다. 이는 네트워크에 다시 액세스하려면 새로운 키로 다수의 최종 장치를 업데이트해야 하기 때문에 모든 사용자에게 영향을 줍니다.

ID PSK(iPSK)를 사용하면 RADIUS 서버의 도움을 받아 동일한 SSID의 개인 또는 사용자 그룹에 대해 고유한 사전 공유 키가 생성됩니다. 이러한 종류의 설정은 최종 클라이언트 장치가 dot1x 인증

을 지원하지 않지만 더 안전하고 세부적인 인증 체계가 필요한 네트워크에서 매우 유용합니다. 클라이언트 관점에서 보면 이 WLAN은 기존 PSK 네트워크와 동일하게 보입니다. PSK 중 하나가 손상된 경우 영향을 받는 개인 또는 그룹만 PSK를 업데이트해야 합니다. WLAN에 연결된 나머지 디바이스는 영향을 받지 않습니다.

Traditional Vs Identity PSK



9800 WLC 구성

Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > Servers(서버)
아래에서 ISE를 RADIUS 서버로 추가합니다.

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
<input type="checkbox"/> ISE_IPSK	10.48.39.126	1812	1813

10 items per page 1 - 1 of 1 items

Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > Server Groups(서버 그룹)에서 RADIUS 서버 그룹을 생성하고 이전에 생성한 ISE 서버를 추가합니다.

+ 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

1 - 1 of 1 items

AAA Method List(AAA 방법 목록) 탭에서 Type(유형) "network" 및 Group Type(그룹 유형) "group"이 이전에 만든 RADIUS 서버 그룹을 가리키는 권한 부여 목록을 생성합니다.

+ 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

1 - 1 of 1 items

어카운팅 설정은 선택 사항이지만, Type(유형)을 "ID"로 구성하고 동일한 RADIUS 서버 그룹을 가리키면 설정할 수 있습니다.

+ 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

1 - 1 of 1 items

이 작업은 명령줄을 통해 다음을 사용하여 수행할 수도 있습니다.

radius server

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)에서 새 WLAN을 생성합니다. Layer 2 컨피그레이션에서

- MAC 필터링을 활성화하고 Authorization List(권한 부여 목록)를 이전에 생성한 목록으로 설정합니다
- 인증 키 관리에서 PSK를 활성화합니다.
- 사전 공유 키 필드는 임의의 값으로 채울 수 있다. 이는 웹 인터페이스 설계의 요구 사항을 충족

하기 위해서만 수행됩니다. 이 키를 사용하여 인증할 수 있는 사용자가 없습니다. 이 경우 사전 공유 키가 "12345678"로 설정되었습니다.

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

Advanced(고급) 탭에서 사용자 분리가 가능합니다. Allow Private Group(개인 그룹 허용)으로 설정하면 동일한 PSK를 사용하는 사용자가 서로 통신하면서 다른 PSK를 사용하는 사용자는 차단됩니다.

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	<input type="checkbox"/>	Allow Private Group ▾	Band Select <input type="checkbox"/>
Multicast Buffer	<input type="checkbox"/>	<input type="checkbox"/> DISABLED	IP Source Guard <input type="checkbox"/>

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)에서 새 정책 프로필을 생성합니다. Access Policies(액세스 정책) 탭에서 이 WLAN에서 사용 중인 VLAN 또는 VLAN 그룹을 설정합니다.

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	<input type="text" value="Search or Select"/>			
VLAN				
VLAN/VLAN Group	<input type="text" value="VLAN0039"/>			
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>			
			WLAN ACL	
			IPv4 ACL	<input type="text" value="Search or Select"/>
			IPv6 ACL	<input type="text" value="Search or Select"/>
			URL Filters	
			Pre Auth	<input type="text" value="Search or Select"/>
			Post Auth	<input type="text" value="Search or Select"/>

Advanced(고급) 탭에서 AAA Override(AAA 재정의)를 활성화하고 이전에 생성한 경우 Accounting(어카운트 관리) 목록을 추가합니다.

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

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Policy(정책)에서 WLAN이 생성한 정책 프로필에 매핑되었는지 확인합니다.

Configuration > Tags & Profiles > Tags

Policy

Site

RF

AP

+ Add

× Delete

Policy Tag Name

default-policy-tag

1 10 Items per page

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Description

WLAN-POLICY Maps: 1

+ Add × Delete

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WLAN_iPSK	Policy_Profile_iPSK

1 10 Items per page

1 - 1 of 1 items

이 작업은 명령줄을 통해 다음을 사용하여 수행할 수도 있습니다.

wlan

Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)에서 이 태그가 WLAN을 브로드캐스트해야 하는 액세스 포인트에 적용되었는지 확인합니다.

Edit AP						
General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle
General		Tags				
AP Name*	AP70DF.2F8E.184A	Policy	default-policy-tag ▼			
Location*	default location	Site	default-site-tag ▼			
Base Radio MAC	500f.8004.eea0	RF	default-rf-tag ▼			
Ethernet MAC	70df.2f8e.184a	Write Tag Config to AP	<input type="checkbox"/> ⓘ			

ISE 구성

이 컨피그레이션 가이드에서는 디바이스의 PSK가 클라이언트 MAC 주소를 기반으로 결정되는 시나리오를 다룹니다. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)에서 새 디바이스를 추가하고, IP 주소를 지정하고, RADIUS Authentication Settings(RADIUS 인증 설정)를 활성화하고, RADIUS Shared Secret(RADIUS 공유 암호)를 지정합니다.

Cisco ISE 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]

Context Visibility > Endpoints > Authentication에서 iPSK 네트워크에 연결하는 모든 디바이스(클라이언트)의 MAC 주소를 추가합니다.

Cisco ISE Context Visibility - Endpoints

Authentication

INACTIVE ENDPOINTS

AUTHENTICATION STATUS

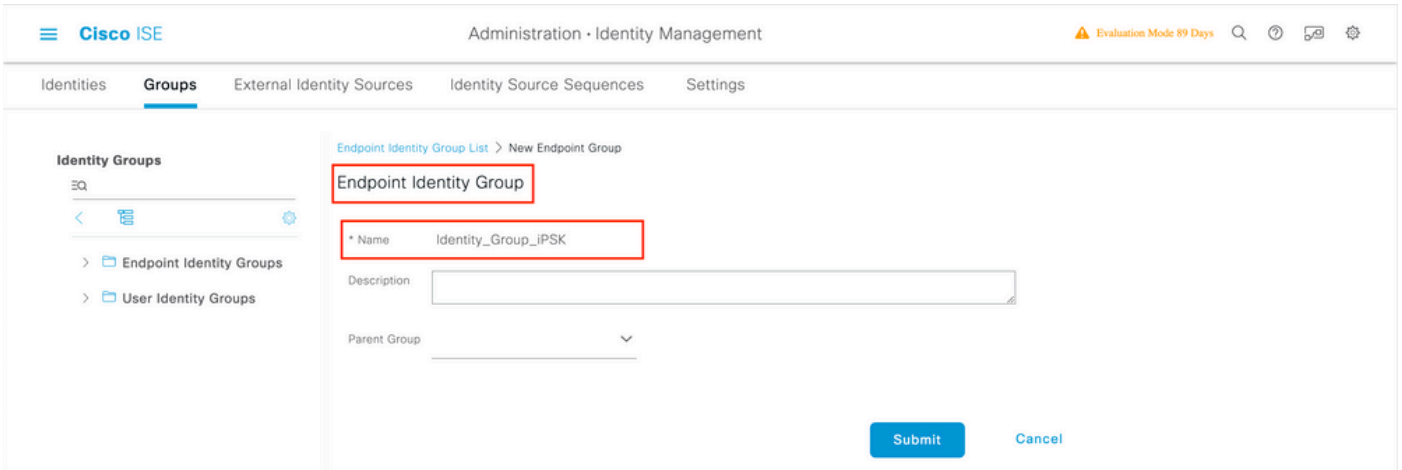
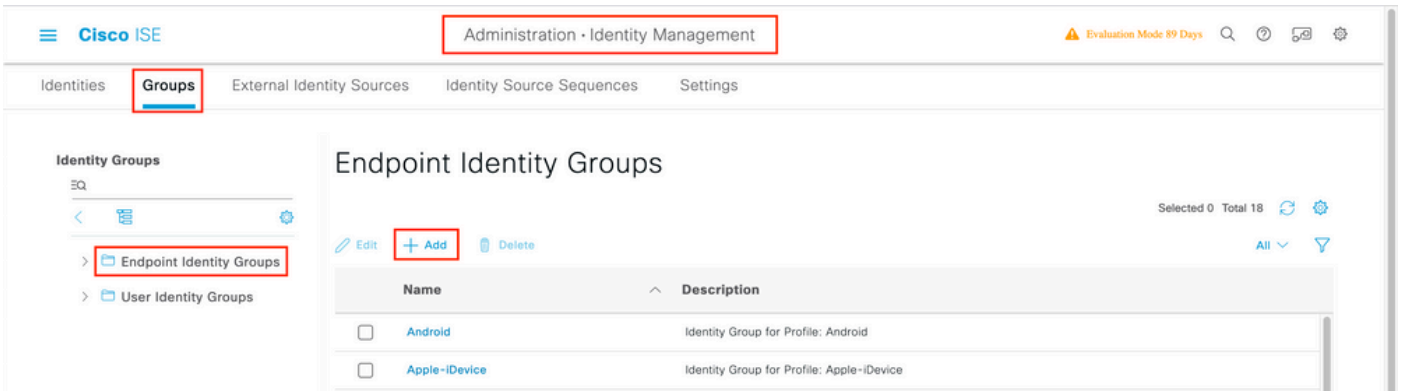
AUTHENTIFICATIONS

NETWORK DE

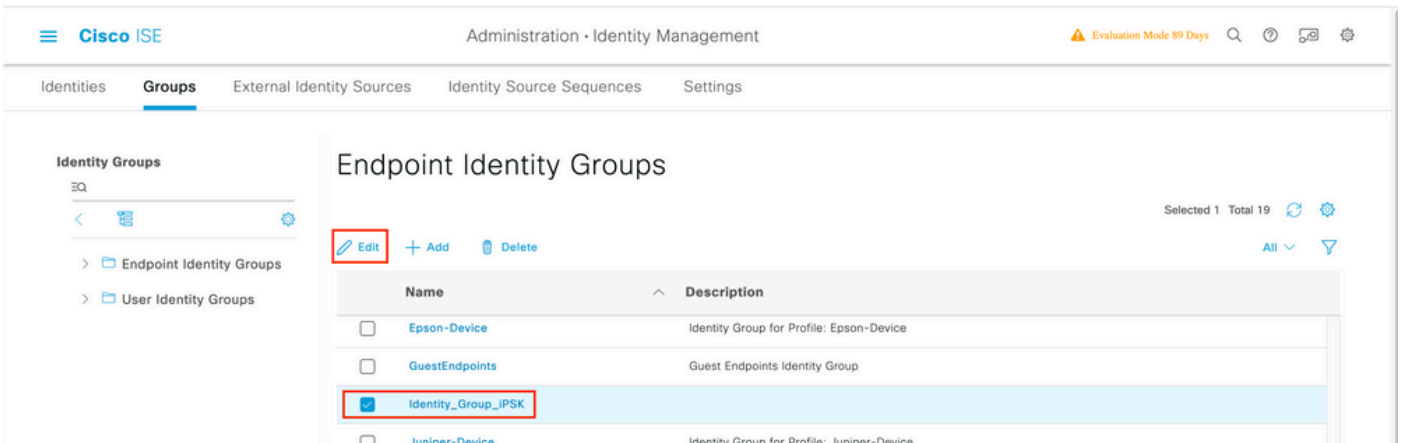
Rows/Page: 1 / 1 Total Rows

MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Re...	Authentication ...	Authorization P..
08-BE-AC-27-85-7E	*		08beac278...		Location...	Unknown	-	MAB	Basic_Authenticate.

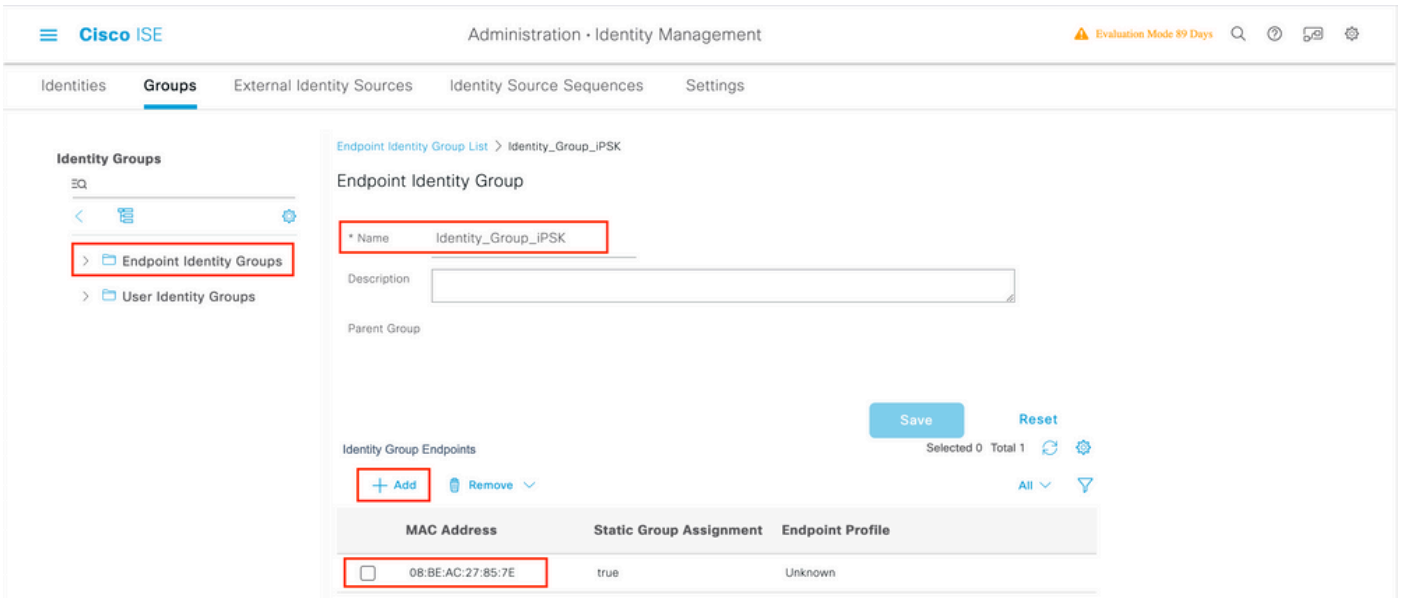
Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > Endpoint Identity Groups(엔드포인트 ID 그룹)에서 하나 이상의 그룹을 생성하고 사용자를 할당합니다. 각 그룹은 나중에 다른 PSK를 사용하여 네트워크에 연결하도록 구성할 수 있습니다.



그룹이 생성되면 사용자에게 사용자를 할당할 수 있습니다. 만든 그룹을 선택하고 "편집"을 클릭합니다.



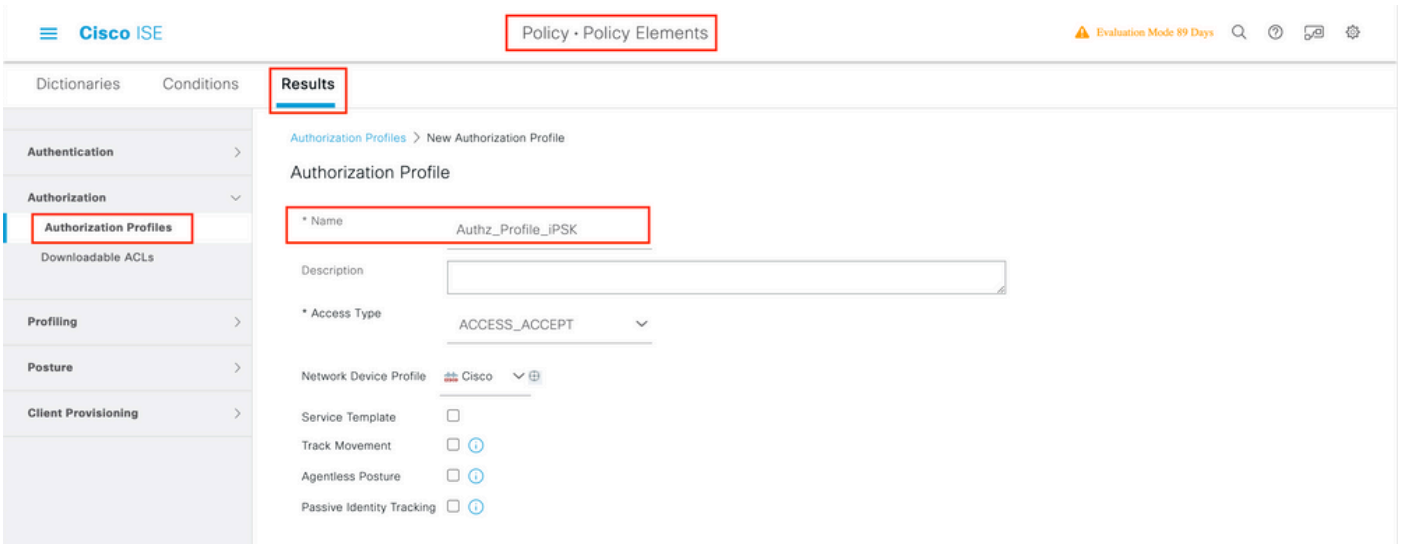
그룹 컨피그레이션에서 "Add(추가)" 버튼을 클릭하여 이 그룹에 할당할 클라이언트의 MAC 주소를 추가합니다.

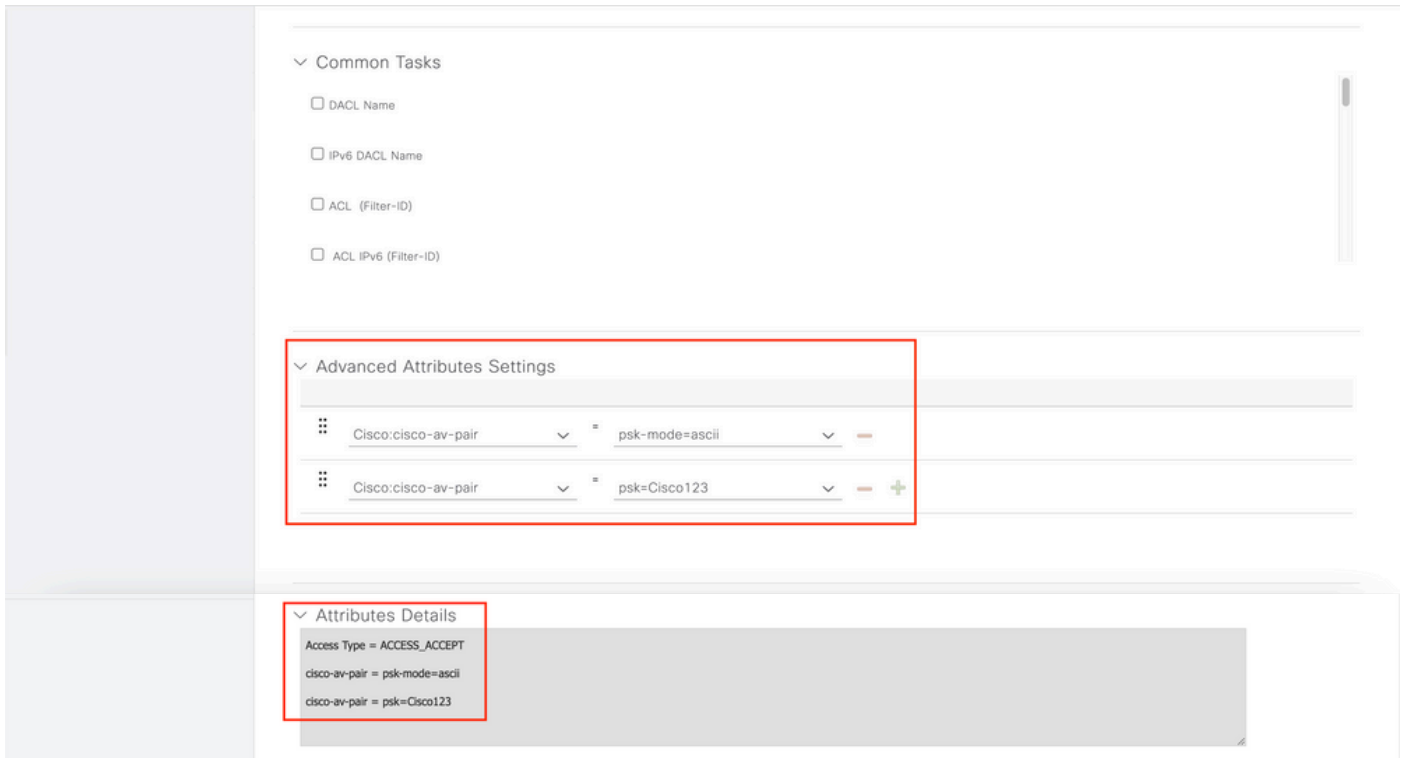


Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)에서 새 권한 부여 프로파일을 생성합니다. 다음과 같이 속성을 설정합니다.

```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

서로 다른 PSK를 사용해야 하는 각 사용자 그룹에 대해 서로 다른 psk av 쌍으로 추가 결과를 생성합니다. ACL 및 VLAN 재정의와 같은 추가 매개변수도 여기에서 구성할 수 있습니다.

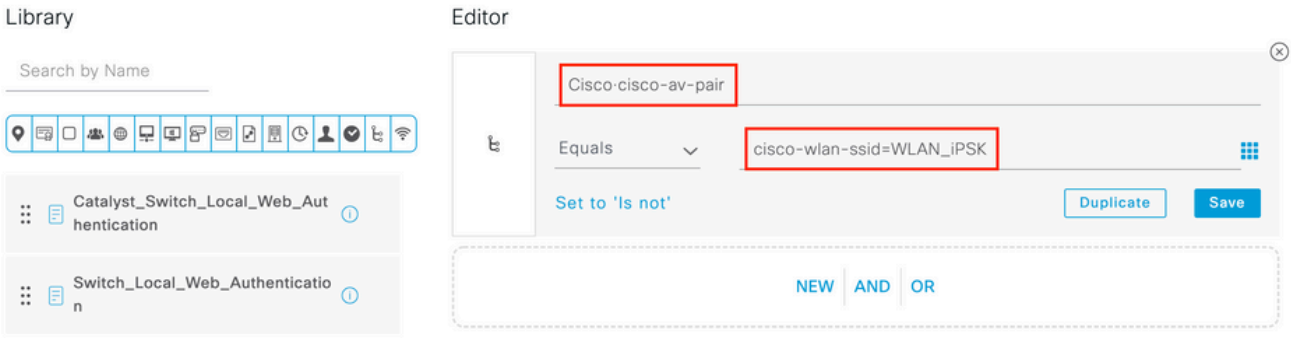




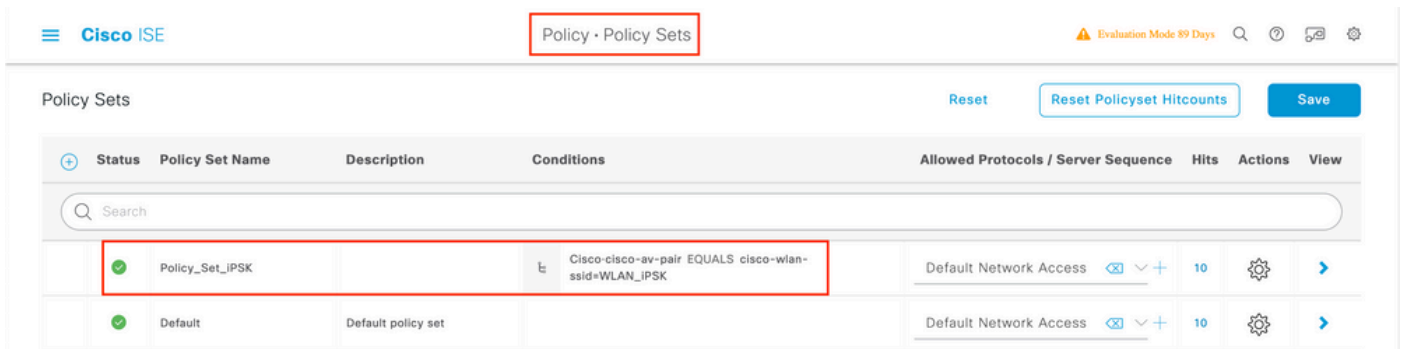
Policy(정책) > Policy Sets(정책 세트)에서 새 정책을 생성합니다. 클라이언트가 정책 집합과 일치하는지 확인하려면 다음 조건을 사용합니다.

```
Cisco:cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_iPSK // "WLAN_iPSK" is WLAN name
```

Conditions Studio



정책 일치를 더 안전하게 하기 위해 조건을 추가할 수 있습니다.



Policy Set(정책 설정) 라인 오른쪽에 있는 파란색 화살표를 클릭하여 새로 생성된 iPSK Policy Set(iPSK 정책 설정) 컨피그레이션으로 이동합니다.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Policy_Set_iPSK		Cisco-cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_iPSK	Default Network Access	77		

인증 정책이 "내부 엔드포인트"로 설정되었는지 확인합니다.

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Policy Sets → Policy_Set-iPSK

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
+	Policy_Set-iPSK		Radius-Called-Station-ID ENDS_WITH WLAN_iPSK	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
+	Default		Internal Endpoints	0	

Authorization Policy(권한 부여 정책)에서 각 사용자 그룹에 대한 새 규칙을 생성합니다. 조건으로 다음을 사용합니다.

```
IdentityGroup-Name EQUALS Endpoint Identity Group:Identity_Group_iPSK //
"Identity_Group_iPSK" is name of the created endpoint group
```

이전에 생성한 인증 프로파일이 결과(Result)인 경우 Default Rule이 아래쪽에 남아 있고 DenyAccess를 가리키는지 확인합니다.

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+	Default		Internal Endpoints	0		

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

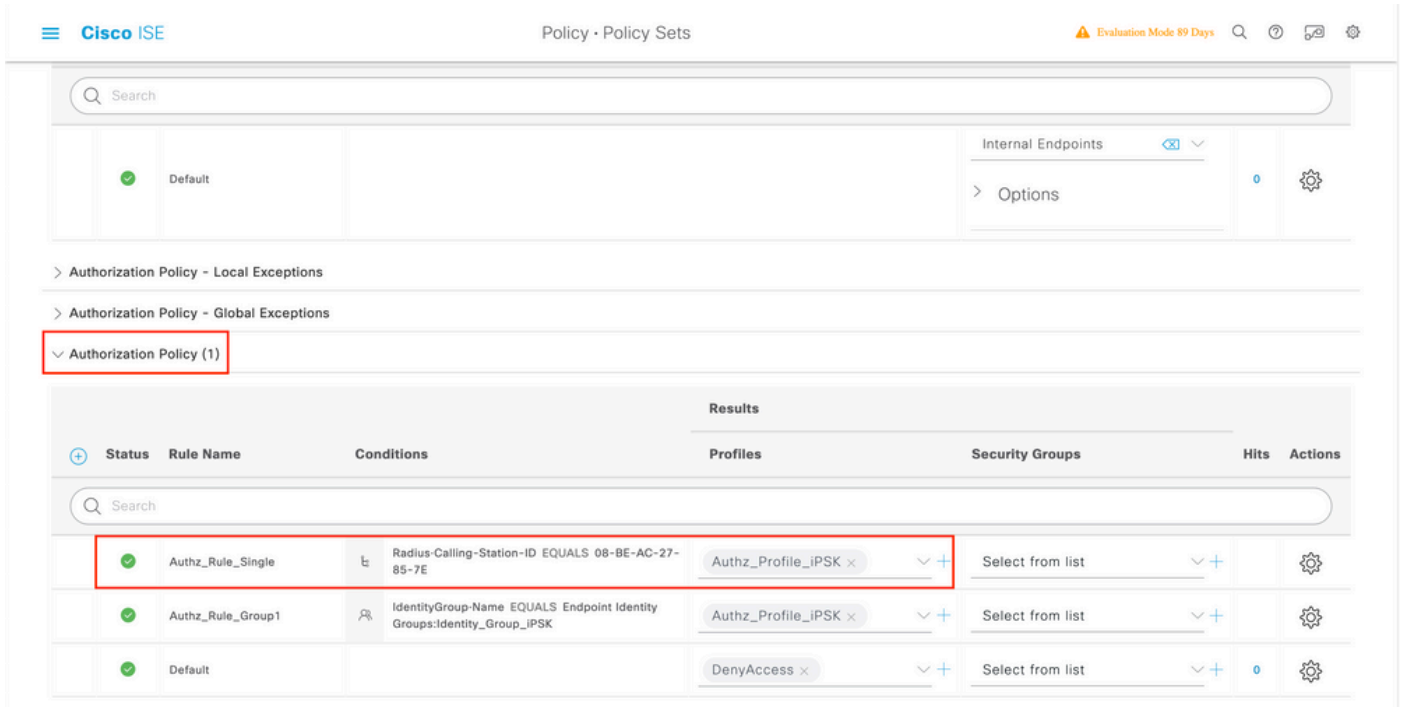
Authorization Policy (1)

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	0	
+	Default		DenyAccess	Select from list	0	

모든 사용자가 다른 비밀번호를 갖게 될 경우 엔드포인트 그룹과 해당 엔드포인트 그룹과 일치하는 규칙을 생성하는 대신 다음 조건을 가진 규칙을 생성할 수 있습니다.

Radius-Calling-Station-ID **EQUALS** <client_mac_addr>

참고: MAC 주소 구분 기호는 WLC의 AAA > AAA Advanced > Global Config > Advanced Settings 아래에서 구성할 수 있습니다. 이 예에서는 문자 "-"가 사용되었습니다.



권한 부여 정책에 대한 규칙을 사용하면 사용자가 사용 중인 비밀번호를 지정하기 위해 다른 여러 매개변수를 사용할 수 있습니다. 가장 일반적으로 사용되는 몇 가지 규칙은 다음과 같습니다.

1. 사용자 위치에 따라 일치

이 시나리오에서 WLC는 AP 위치 정보를 ISE에 전송해야 합니다. 이렇게 하면 한 위치의 사용자는 한 비밀번호를 사용하고 다른 위치의 사용자는 다른 비밀번호를 사용할 수 있습니다. 이는 Configuration(컨피그레이션) > Security(보안) > Wireless AAA Policy(무선 AAA 정책)에서 구성할 수 있습니다.

Edit Wireless AAA Policy

Policy Name*	<input type="text" value="default-aaa-policy"/>
NAS-ID Option 1	<input type="text" value="System Name"/>
NAS-ID Option 2	<input style="border: 2px solid red;" type="text" value="AP Location"/>
NAS-ID Option 3	<input type="text" value="Not Configured"/>

2. 디바이스 프로파일링을 기반으로 매칭

이 시나리오에서는 디바이스를 전역으로 프로파일링하도록 WLC를 구성해야 합니다. 이를 통해 관리자는 랩톱 및 전화 디바이스에 대해 서로 다른 비밀번호를 구성할 수 있습니다.

Configuration(컨피그레이션) > Wireless(무선) > **Wireless Global(무선 전역)**에서 전역 디바이스 분류를 활성화할 수 있습니다. ISE의 디바이스 프로파일링 컨피그레이션에 대해서는 ISE 프로파일링 [설계 가이드를 참조하십시오](#).

암호화 키를 반환하는 것 외에도 802.11 연결 단계에서 권한 부여가 이루어지므로 ISE에서 ACL 또는 VLAN ID와 같은 다른 AAA 특성을 반환할 수 있습니다.

문제 해결

9800 WLC에서 문제 해결

WLC에서, 방사능 흔적을 수집하는 것은 대부분의 문제를 식별하기에 충분치 않아야 한다. 이 작업은 WLC 웹 인터페이스의 Troubleshooting(문제 해결) > Radioactive Trace(**방사능 추적**)에서 수행할 수 있습니다. 클라이언트 MAC 주소를 추가하고 Start(**시작**)를 누른 다음 문제를 재현해 보십시오. Generate(**생성**)를 클릭하여 파일을 만들고 다운로드합니다.

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	▶ Generate

◀ 1 ▶ 20 items per page 1 - 1 of 1 items

중요: IOS 14 및 Android 10 스마트폰에서 iPhone은 네트워크에 연결할 때 무작위 맥 주소를 사용합니다. 이 기능은 iPSK 컨피그레이션을 완전히 중단할 수 있습니다. 이 기능이 비활성화되어 있는지 확인하십시오.

방사성 추적이 문제를 식별하기에 충분하지 않으면 패킷 캡처를 WLC에서 직접 수집할 수 있습니다. Troubleshooting(트러블슈팅) > Packet Capture(패킷 캡처)에서 캡처 포인트를 추가합니다. 기본적으로 WLC는 모든 RADIUS AAA 통신에 무선 관리 인터페이스를 사용합니다. WLC에 클라이언트 수가 많은 경우 버퍼 크기를 100MB로 늘립니다.

Edit Packet Capture

Capture Name*

iPSK

Filter*

any

Monitor Control Plane



Buffer Size (MB)*

100

Limit by*

Duration

3600

secs ~ 1.00 hour

Available (4)

Search



- GigabitEthernet1 →
- GigabitEthernet2 →
- GigabitEthernet3 →
- Vlan1 →

Selected (1)

Vlan39 ←

성공적인 인증 및 어카운팅 시도의 패킷 캡처가 아래 그림에 나와 있습니다. 이 Wireshark 필터를 사용하여 이 클라이언트에 대한 모든 관련 패킷을 필터링할 수 있습니다.

ip.addr==

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

ISE 문제 해결

Cisco ISE의 주요 문제 해결 방법은 **라이브 로그 페이지, 운영 > RADIUS > 라이브 로그**에 있습니다. 클라이언트의 MAC 주소를 Endpoint ID 필드에 입력하여 필터링할 수 있습니다. 전체 ISE 보고서를 열면 실패 사유에 대한 자세한 정보가 제공됩니다. 클라이언트가 올바른 ISE 정책에 도달했는지 확인합니다.

Cisco ISE Operations - RADIUS Evaluation Mode 89 Days

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:bf
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	

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.