

# Configurazione di Catalyst 9800 WLC iPSK con ISE

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Comprendere che cos'è iPSK e quali scenari si adattano](#)

[Configurazione 9800 WLC](#)

[Configurazione di ISE](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi relativi al WLC 9800](#)

[Risoluzione dei problemi ISE](#)

## Introduzione

In questo documento viene descritta la configurazione di una WLAN protetta con iPSK su un controller LAN wireless Cisco 9800 con Cisco ISE come server RADIUS.

## Prerequisiti

### Requisiti

In questo documento si presume che l'utente abbia già familiarità con la configurazione di base di una WLAN su 9800 e sia in grado di adattare la configurazione alla propria implementazione.

### Componenti usati

- Cisco 9800-CL WLC con 17.6.3
- Cisco ISE 3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

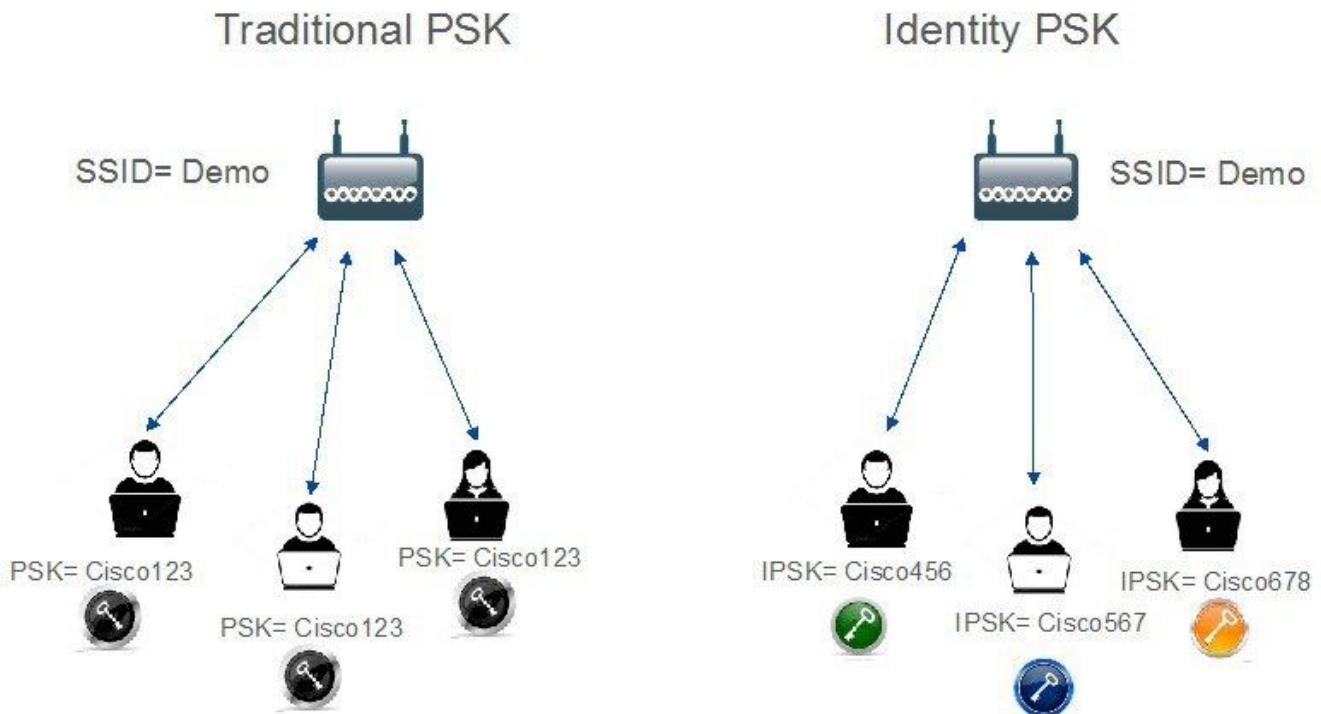
## Comprendere che cos'è iPSK e quali scenari si adattano

Le reti tradizionali protette con chiave precondivisa (PSK) utilizzano la stessa password per tutti i client connessi. In questo modo, la chiave condivisa con utenti non autorizzati può causare una violazione della sicurezza e l'accesso non autorizzato alla rete. Il rimedio più comune a questa violazione è la modifica della chiave primaria PSK, una modifica che interessa tutti gli utenti in quanto molti dispositivi terminali devono essere aggiornati con la nuova chiave per poter accedere

nuovamente alla rete.

Con Identity PSK (iPSK), vengono create chiavi univoche pre-condivise per singoli utenti o un gruppo di utenti sullo stesso SSID con l'aiuto di un server RADIUS. Questo tipo di configurazione è estremamente utile nelle reti in cui i dispositivi dei client finali non supportano l'autenticazione dot1x, ma è necessario uno schema di autenticazione più sicuro e granulare. Dal punto di vista del client, questa WLAN sembra identica alla rete PSK tradizionale. Nel caso in cui uno dei PSK sia compromesso, solo l'utente o il gruppo interessato deve aggiornare il PSK. ciò non influisce sugli altri dispositivi collegati alla WLAN.

## Traditional Vs Identity PSK



## Configurazione 9800 WLC

In **Configurazione > Sicurezza > AAA > Server/Gruppi > Server** aggiungere l'ISE come server RADIUS:

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

In **Configurazione > Sicurezza > AAA > Server/Gruppi > Gruppi di server**, creare un gruppo di server RADIUS e aggiungervi il server ISE creato in precedenza:

+ 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

Nella scheda **Elenco metodi AAA** creare un elenco di **autorizzazioni** con il tipo **"rete"** e il tipo di gruppo **"gruppo"** che punta al gruppo di server RADIUS creato in precedenza:

+ 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

L'impostazione dell'accounting è facoltativa, ma può essere eseguita configurando il tipo su **"identity"** e puntandolo allo stesso gruppo di server RADIUS:

+ 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

Questa operazione può essere eseguita anche dalla riga di comando utilizzando:

```
radius server
```

In **Configurazione > Tag e profili > WLAN**, creare una nuova WLAN. In Configurazione layer 2:

- Abilitare il filtro MAC e impostare l'elenco autorizzazioni su quello creato in precedenza
- In **Gestione chiavi di autenticazione** abilitare **PSK**
- Il campo chiave già condivisa può essere compilato con qualsiasi valore. Questa operazione viene eseguita solo per soddisfare i requisiti di progettazione dell'interfaccia Web. Nessun utente è in grado di eseguire l'autenticazione utilizzando questa chiave. In questo caso, la

chiave già condivisa è stata impostata su "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

È possibile effettuare la separazione degli utenti nella scheda **Avanzate**. Impostandolo su Consenti gruppo privato, gli utenti che utilizzano la stessa chiave PSK possono comunicare tra loro, mentre gli utenti che utilizzano una chiave PSK diversa sono bloccati:

General	Security	<b>Advanced</b>	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"/>
<b>P2P Blocking Action</b>	<input type="checkbox"/>	<b>Allow Private Group</b> ▼	Band Select <input type="checkbox"/>
Multicast Buffer	<input type="checkbox"/>	<input type="checkbox"/>	IP Source Guard <input type="checkbox"/>

In **Configurazione > Tag e profili > Criterio**, creare un nuovo Profilo criterio. Nella scheda **Access Policies** (Criteri di accesso), impostare il gruppo di VLAN o VLAN usato dalla WLAN:

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

Nella scheda **Avanzate**, abilitare la sostituzione AAA e aggiungere l'elenco Contabilità se creato in precedenza:

## 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

In Configurazione > Tag e profili > Tag > Criterio, verificare che la WLAN sia mappata al profilo di criterio creato:

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

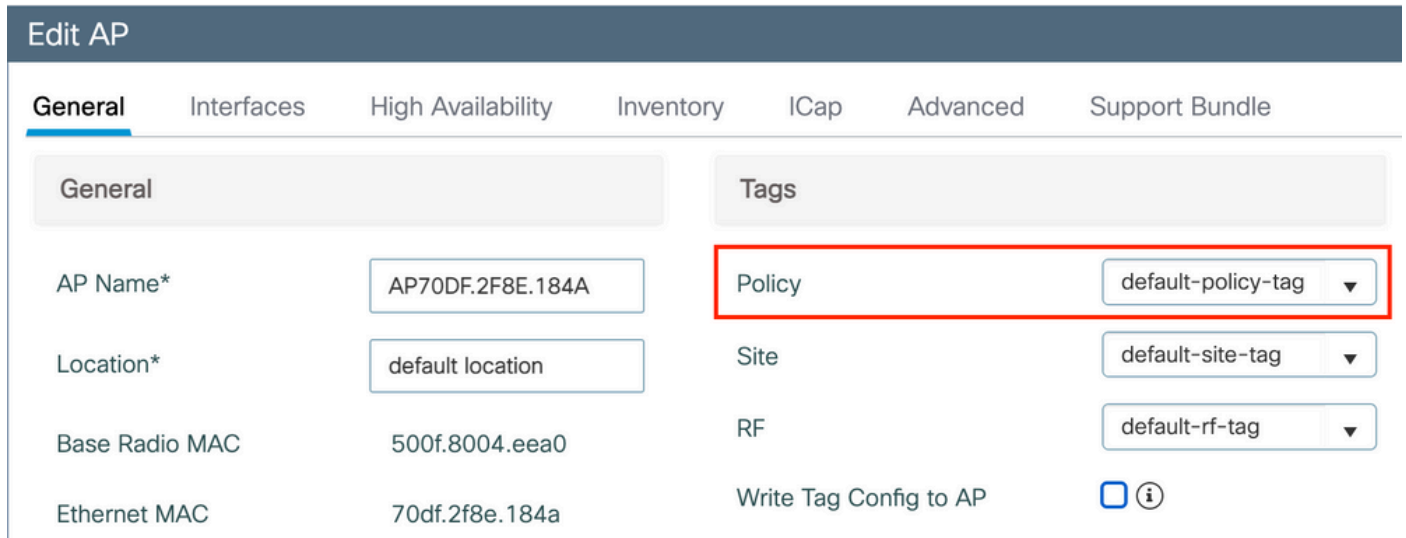
1 10 items per page

1 - 1 of 1 items

Questa operazione può essere eseguita anche dalla riga di comando utilizzando:

wlan

In **Configurazione > Wireless > Access Point** verificare che il tag sia stato applicato ai punti di accesso sui quali la WLAN deve essere trasmessa:



The screenshot shows the 'Edit AP' configuration page. The 'General' tab is selected. The 'Tags' section is highlighted with a red box. The 'Policy' dropdown menu is set to 'default-policy-tag'. Other fields include 'AP Name\*' (AP70DF.2F8E.184A), 'Location\*' (default location), 'Base Radio MAC' (500f.8004.eea0), 'Ethernet MAC' (70df.2f8e.184a), 'Site' (default-site-tag), 'RF' (default-rf-tag), and 'Write Tag Config to AP' (checkbox).

Field	Value
AP Name*	AP70DF.2F8E.184A
Location*	default location
Base Radio MAC	500f.8004.eea0
Ethernet MAC	70df.2f8e.184a
Policy	default-policy-tag
Site	default-site-tag
RF	default-rf-tag
Write Tag Config to AP	<input type="checkbox"/> ⓘ

## Configurazione di ISE

Questa guida alla configurazione descrive uno scenario in cui la chiave PSK del dispositivo viene determinata in base all'indirizzo MAC del client. In **Amministrazione > Risorse di rete > Dispositivi di rete**, aggiungere un nuovo dispositivo, specificare l'indirizzo IP, abilitare le impostazioni di autenticazione RADIUS e specificare un segreto condiviso RADIUS:

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](#)

In **Context Visibility > Endpoints > Authentication** (Visibilità contesto > Endpoint > Autenticazione), aggiungere gli indirizzi MAC di tutti i dispositivi (client) che si connettono alla rete iPSK:

Cisco ISE Context Visibility - Endpoints

Authentication

INACTIVE ENDPOINTS

AUTHENTICATION STATUS

AUTHENTIFICATIONS

Failure Reason Identity Store Identity Group

Location Type

Rows/Page 1 / 1 Total Rows

ANC Change Authorization Clear Threats & Vulnerabilities Export Import MDM Actions Release Rejected Revoke Certificate Filter

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_Authenticate.

In **Amministrazione > Gestione delle identità > Gruppi > Gruppi di identità degli endpoint**, creare uno o più gruppi e assegnarvi gli utenti. Ciascun gruppo può essere successivamente configurato per l'utilizzo di un PSK diverso per la connessione alla rete.



The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes "Cisco ISE" and "Administration · Identity Management". The main navigation menu has "Identities", "Groups", "External Identity Sources", "Identity Source Sequences", and "Settings". The "Groups" menu is expanded, showing "Endpoint Identity Groups" and "User Identity Groups". The "Endpoint Identity Groups" page displays a table with the following data:

Name	Description
<input type="checkbox"/> Android	Identity Group for Profile: Android
<input type="checkbox"/> Apple-iDevice	Identity Group for Profile: Apple-iDevice

The screenshot shows the "New Endpoint Group" form in the Cisco ISE Administration interface. The form is titled "Endpoint Identity Group" and has the following fields:

- \* Name: Identity\_Group\_IPSK
- Description: (empty text box)
- Parent Group: (dropdown menu)

At the bottom of the form, there are "Submit" and "Cancel" buttons.

Una volta creato il gruppo, è possibile assegnarvi degli utenti. Selezionare il gruppo creato e fare clic su "Modifica":

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes "Cisco ISE" and "Administration · Identity Management". The main navigation menu has "Identities", "Groups", "External Identity Sources", "Identity Source Sequences", and "Settings". The "Groups" menu is expanded, showing "Endpoint Identity Groups" and "User Identity Groups". The "Endpoint Identity Groups" page displays a table with the following data:

Name	Description
<input type="checkbox"/> Epson-Device	Identity Group for Profile: Epson-Device
<input type="checkbox"/> GuestEndpoints	Guest Endpoints Identity Group
<input checked="" type="checkbox"/> Identity_Group_IPSK	
<input type="checkbox"/> Iuniner-Device	Identity Group for Profile: Iuniner-Device

Nella configurazione di gruppo, aggiungere l'indirizzo MAC dei client che si desidera assegnare a questo gruppo facendo clic sul pulsante "Aggiungi":

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is "Endpoint Identity Group List > Identity\_Group\_IPSK". The main heading is "Endpoint Identity Group".

On the left sidebar, "Endpoint Identity Groups" is highlighted. The main form contains the following fields:

- \* Name: Identity\_Group\_IPSK
- Description: (empty text box)
- Parent Group: (empty dropdown)

Below the form are "Save" and "Reset" buttons. Underneath, there is a section for "Identity Group Endpoints" with "Selected 0 Total 1" and a refresh icon. There are "+ Add" and "Remove" buttons. Below this is a table with columns: "MAC Address", "Static Group Assignment", and "Endpoint Profile".

MAC Address	Static Group Assignment	Endpoint Profile
<input type="checkbox"/> 08:BE:AC:27:85:7E	true	Unknown

In Criterio > Elementi criterio > Risultati > Autorizzazione > Profili di autorizzazione, creare un nuovo profilo di autorizzazione. Imposta attributi come:

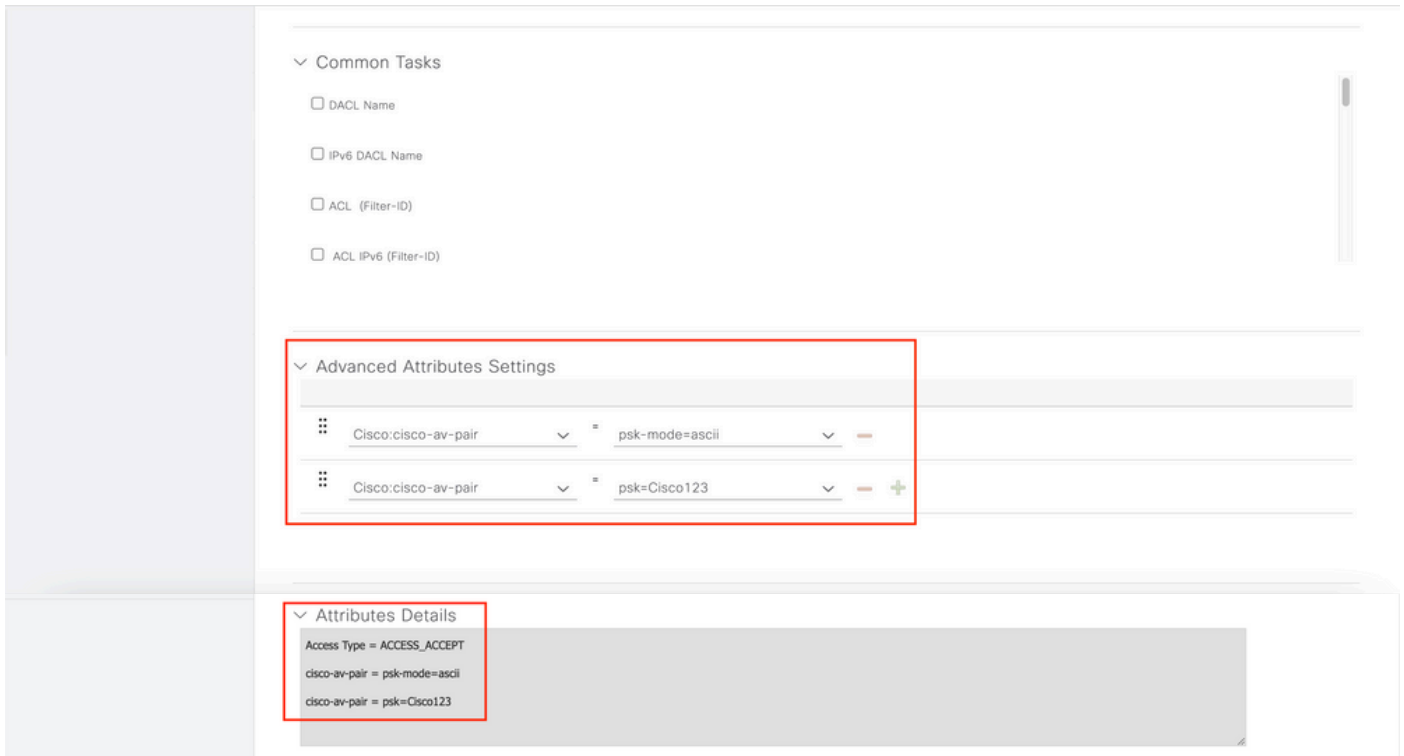
```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

Per ogni gruppo di utenti che deve utilizzare una chiave PSK diversa, creare un risultato aggiuntivo con una coppia av psk diversa. In questa finestra è possibile configurare anche parametri aggiuntivi come l'override di ACL e VLAN.

The screenshot shows the Cisco ISE Administration interface for Policy Elements. The breadcrumb trail is "Authorization Profiles > New Authorization Profile". The main heading is "Authorization Profile".

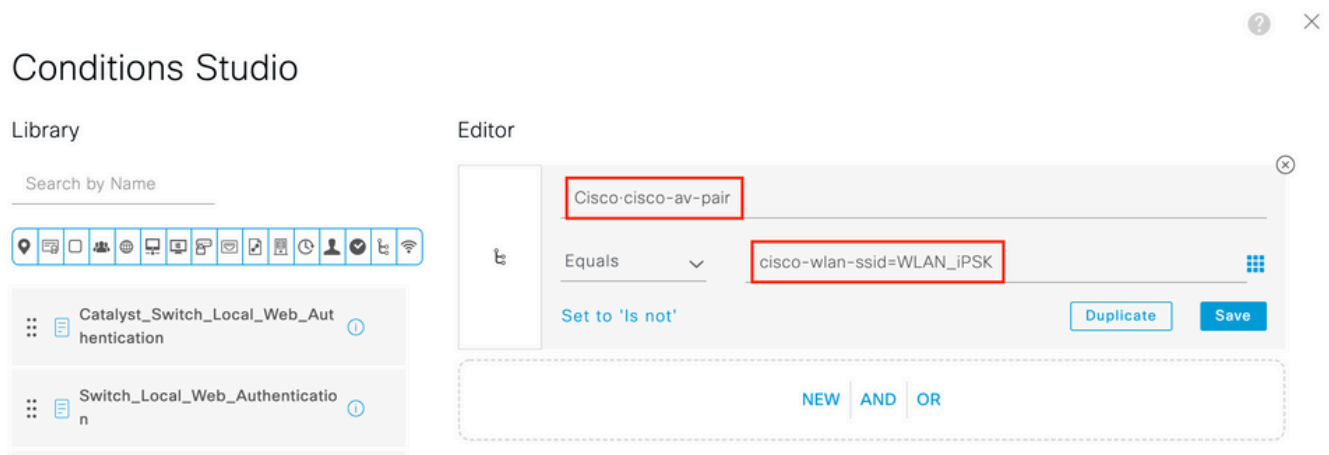
On the left sidebar, "Authorization Profiles" is highlighted. The main form contains the following fields:

- \* Name: Authz\_Profile\_IPSK
- Description: (empty text box)
- \* Access Type: ACCESS\_ACCEPT (dropdown menu)
- Network Device Profile: Cisco (dropdown menu)
- Service Template:
- Track Movement:  ⓘ
- Agentless Posture:  ⓘ
- Passive Identity Tracking:  ⓘ

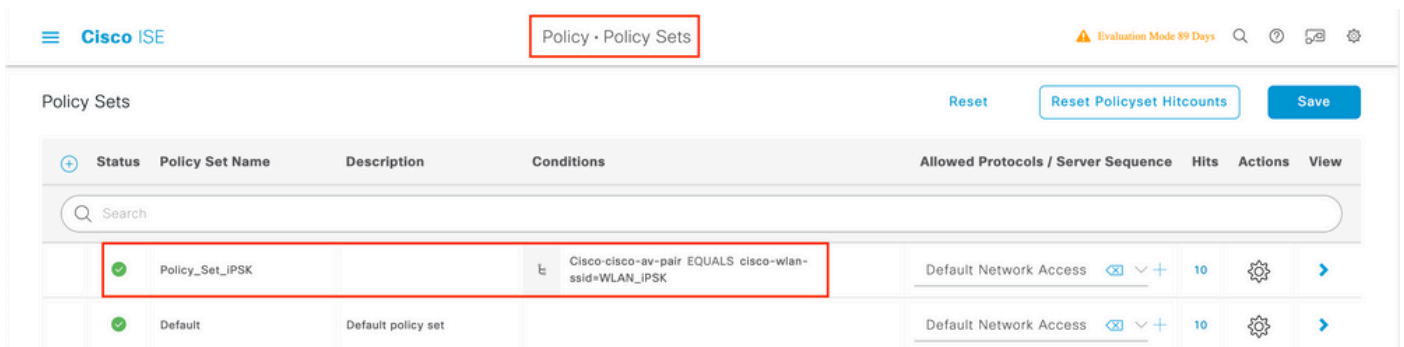


In **Criterio > Set di criteri**, crearne uno nuovo. Per assicurarsi che il client corrisponda al set di criteri, viene utilizzata la seguente condizione:

Cisco:cisco-av-pair **EQUALS** cisco-wlan-ssid=WLAN\_iPSK // "WLAN\_iPSK" is WLAN name



È possibile aggiungere ulteriori condizioni per rendere la corrispondenza dei criteri più sicura.



Passare alla configurazione del nuovo set di criteri iPSK facendo clic sulla freccia blu a destra della riga Set di criteri:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">✔</span>	Policy_Set_IPSK		Cisco-cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_IPSK	Default Network Access	77		

Verificare che il criterio di **autenticazione** sia impostato su "Endpoint interni":

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Policy Sets → Policy\_Set-IPSK Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
<span style="color: green;">✔</span>	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
<span style="color: green;">✔</span>	Default		Internal Endpoints	0	

In **Criteri di autorizzazione** creare una nuova regola per ogni gruppo di utenti. Come condizione, utilizzare:

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

in cui **Result** è il **profilo di autorizzazione** creato in precedenza. Verificare che la regola **predefinita** rimanga nella parte inferiore e punti a **DenyAccess**.

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
<span style="color: green;">✔</span>	Default		Internal Endpoints	0		
<p>&gt; Authorization Policy - Local Exceptions</p> <p>&gt; Authorization Policy - Global Exceptions</p> <p>Authorization Policy (1)</p>						
<span style="color: green;">✔</span>	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK	Select from list	0	
<span style="color: green;">✔</span>	Default		DenyAccess	Select from list	0	

Se a ogni utente viene assegnata una password diversa, anziché creare gruppi di endpoint e regole corrispondenti a tale gruppo di endpoint, è possibile creare una regola con la seguente condizione:

Radius-Calling-Station-ID **EQUALS** <client\_mac\_addr>

**Nota:** Il delimitatore di indirizzo MAC può essere configurato sul WLC in **AAA > AAA Advanced > Global Config > Advanced Settings**. Nell'esempio è stato utilizzato il carattere "-".

The screenshot shows the Cisco ISE interface for Policy Sets. The 'Authorization Policy (1)' section is expanded, showing a table of rules. The first rule, 'Authz\_Rule\_Single', is highlighted with a red box. Its condition is 'Radius-Calling-Station-ID EQUALS 08-BE-AC-27-85-7E'. The profile is 'Authz\_Profile\_IPSK' and the security group is 'Select from list'.

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	

Le regole relative ai criteri di autorizzazione consentono di utilizzare molti altri parametri per specificare la password utilizzata dall'utente. Di seguito sono riportate alcune delle regole più comunemente utilizzate.

### 1. Corrispondenza basata sulla posizione dell'utente

In questo scenario, il WLC deve inviare le informazioni sulla posizione dell'access point all'ISE. In questo modo gli utenti di un percorso potranno utilizzare una password, mentre gli utenti di un altro percorso ne utilizzeranno una diversa. È possibile configurare questa opzione in **Configurazione > Sicurezza > Policy AAA wireless**:

## 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. Corrispondenza basata sul profilo del dispositivo

In questo scenario, il WLC deve essere configurato per profilare i dispositivi a livello globale. Ciò consente a un amministratore di configurare password diverse per i dispositivi laptop e telefonici. La classificazione globale dei dispositivi può essere abilitata in **Configurazione > Wireless > Wireless globale**. Per la configurazione del profilo del dispositivo su ISE, consultare la [ISE Profiling Design Guide](#).

Oltre alla restituzione della chiave di crittografia, poiché l'autorizzazione avviene nella fase di associazione 802.11, è possibile restituire altri attributi AAA da ISE, ad esempio l'ACL o l'ID VLAN.

## Risoluzione dei problemi

### Risoluzione dei problemi relativi al WLC 9800

Sul WLC, raccogliere tracce radioattive deve essere più che sufficiente per identificare la maggior parte dei problemi. Questa operazione può essere eseguita nell'interfaccia Web del WLC in **Risoluzione dei problemi > Traccia radioattiva**. Aggiungere l'indirizzo MAC del client, premere **Start** e provare a riprodurre il problema. Fare clic su **Generate** (Genera) per creare il file e scaricarlo:

## 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	<b>Generate</b>

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

**Importante:** gli iPhone sugli smartphone IOS 14 e Android 10 usano un indirizzo mac casuale quando si associano alla rete. Questa funzionalità può interrompere completamente la configurazione di iPSK. Accertarsi che questa funzione sia disattivata.

Se le tracce radioattive non sono sufficienti per identificare il problema, le acquisizioni dei pacchetti possono essere raccolte direttamente sul WLC. In **Risoluzione dei problemi > Acquisizione pacchetto**, aggiungere un punto di acquisizione. Per impostazione predefinita, WLC utilizza l'interfaccia di gestione wireless per tutte le comunicazioni RADIUS AAA. Aumentare la dimensione del buffer a 100 MB se il WLC ha un numero elevato di client:

### 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

Selected (1)

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

- Vlan39 ←

Nella figura seguente è illustrata l'acquisizione di un pacchetto relativo a un tentativo di autenticazione e accounting riuscito. Utilizzare questo filtro Wireshark per filtrare tutti i pacchetti pertinenti per questo client:

ip.addr==

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

## Risoluzione dei problemi ISE

La tecnica principale di risoluzione dei problemi su Cisco ISE è la pagina **Live Logs**, in **Operations > RADIUS > Live Logs**. Possono essere filtrati inserendo l'indirizzo MAC del client nel campo ID endpoint. L'apertura di un report ISE completo offre maggiori dettagli sulla causa dell'errore. Verificare che il client stia violando la policy ISE corretta:

**Cisco ISE** Operations - RADIUS

**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

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	



## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).