

Configuración de Catalyst 9800 WLC iPSK con ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Comprender qué es iPSK y en qué situaciones encaja](#)

[Configuración del WLC 9800](#)

[Configuración de ISE](#)

[Troubleshoot](#)

[Resolución de problemas en el 9800 WLC](#)

[Troubleshooting de ISE](#)

Introducción

Este documento describe la configuración de una WLAN segura iPSK en un Cisco 9800 Wireless LAN Controller con Cisco ISE como servidor RADIUS.

Prerequisites

Requirements

Este documento asume que ya está familiarizado con la configuración básica de una WLAN en 9800 y que puede adaptar la configuración a su implementación.

Componentes Utilizados

- Cisco 9800-CL WLC que ejecuta 17.6.3
- Cisco ISE 3.0

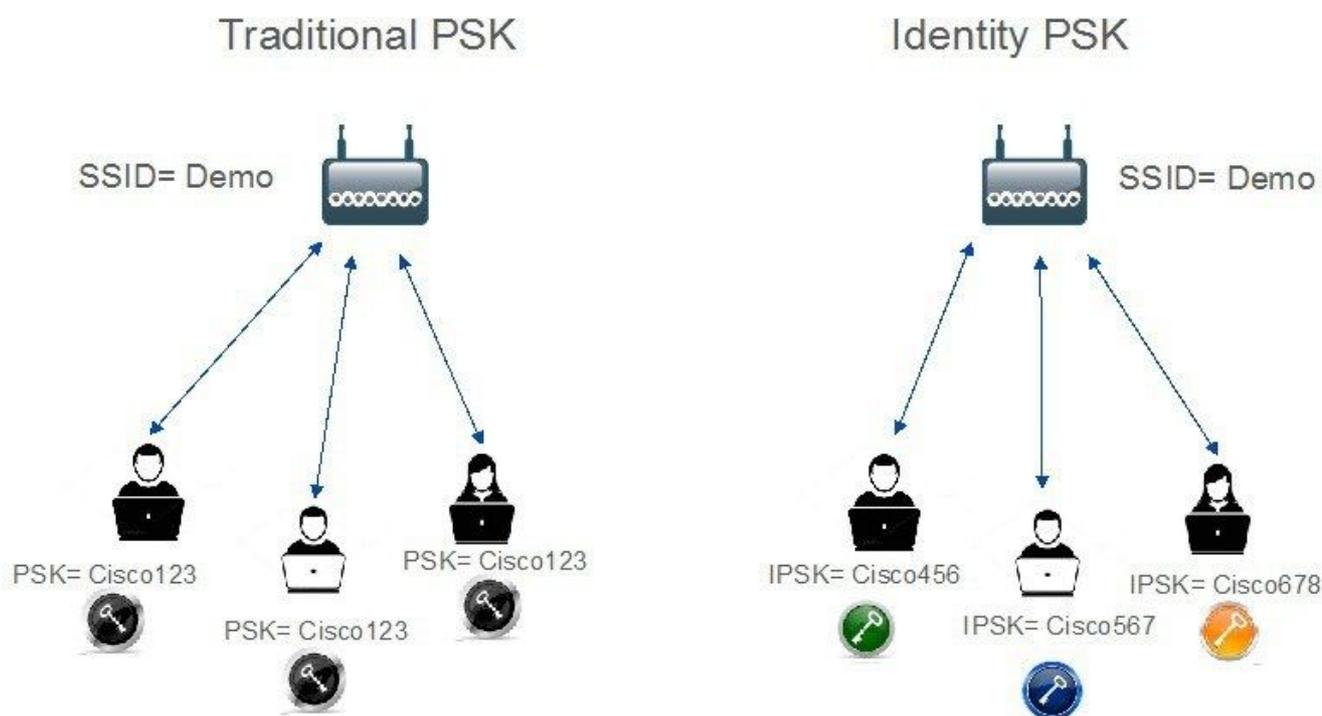
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Comprender qué es iPSK y en qué situaciones encaja

Las redes seguras con clave precompartida (PSK) tradicionales utilizan la misma contraseña para todos los clientes conectados. Esto puede dar lugar a que la clave compartida con usuarios no autorizados provoque una brecha en la seguridad y un acceso no autorizado a la red. La mitigación más habitual de esta brecha es el cambio de la propia PSK, un cambio que afecta a todos los usuarios, ya que muchos dispositivos finales deben actualizarse con la nueva clave para poder acceder de nuevo a la red.

Con Identity PSK (iPSK), se crean claves previamente compartidas únicas para usuarios individuales o de un grupo de usuarios en el mismo SSID con la ayuda de un servidor RADIUS. Este tipo de configuración es extremadamente útil en redes donde los dispositivos de cliente final no admiten la autenticación dot1x, pero se necesita un esquema de autenticación más seguro y granular. Desde la perspectiva de un cliente, esta WLAN parece idéntica a la red PSK tradicional. En caso de que una de las PSK se vea comprometida, solo la persona o el grupo afectado necesita que se actualice su PSK. El resto de los dispositivos conectados a la WLAN no se ven afectados.

Traditional Vs Identity PSK



Configuración del WLC 9800

En **Configuration > Security > AAA > Servers/Groups > Servers**, agregue ISE como servidor 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

En **Configuration > Security > AAA > Servers/Groups > Server Groups**, cree un grupo de servidores RADIUS y agréguele el servidor ISE creado anteriormente:

+ 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

En la pestaña **Lista de Métodos AAA** cree una lista de **Autorización** con el Tipo "red" y el Tipo de Grupo "grupo" señalando al grupo de servidores RADIUS previamente creado:

+ 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

La configuración de la Contabilización es opcional, pero se puede hacer configurando el Tipo a "identidad" y apuntándolo al mismo grupo de servidores 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

Esto también se puede realizar a través de la línea de comandos mediante:

```
radius server
```

En **Configuration > Tags & Profiles > WLANs**, cree una nueva WLAN. En Configuración de capa 2:

- Active el filtrado de MAC y establezca la lista de autorización en la creada anteriormente
- En **Auth Key Mgmt**, habilite **PSK**
- El campo de clave previamente compartida se puede rellenar con cualquier valor. Esto se hace solamente para satisfacer el requisito del diseño de la interfaz web. Ningún usuario

puede autenticarse con esta clave. En este caso, la clave previamente compartida se estableció en "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

La separación de usuarios se puede lograr en la pestaña **Advanced**. Si se establece en Permitir grupo privado, los usuarios que utilicen la misma PSK podrán comunicarse entre sí, mientras que los usuarios que utilicen una PSK diferente se bloquearán:

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"/>	IP Source Guard <input type="checkbox"/>

En **Configuration > Tags & Profiles > Policy**, cree un nuevo perfil de política. En la pestaña **Access Policies**, configure la VLAN o el grupo VLAN que esta WLAN está utilizando:

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	<input type="checkbox"/>			
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"/>		

En la pestaña **Advanced**, habilite AAA Override y agregue la lista de cuentas si se creó anteriormente:

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

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

En **Configuration > Tags & Profiles > Tags > Policy**, asegúrese de que la WLAN esté asignada al perfil de política que creó:

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

Esto también se puede realizar a través de la línea de comandos mediante:

wlan

En **Configuration > Wireless > Access Points**, asegúrese de que esta etiqueta se haya aplicado en los puntos de acceso en los que se debe transmitir la WLAN:

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"/> ⓘ

Configuración de ISE

Esta guía de configuración cubre un escenario en el que la PSK del dispositivo se determina en función de la dirección MAC del cliente. Bajo **Administration > Network Resources > Network Devices**, agregue un nuevo dispositivo, especifique la dirección IP, habilite la configuración de autenticación RADIUS y especifique un secreto compartido 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]

En **Context Visibility > Endpoints > Authentication**, agregue las direcciones MAC de todos los dispositivos (clientes) que se conectan a la red iPSK:

Cisco ISE Context Visibility - Endpoints

Authentication

INACTIVE ENDPOINTS

AUTHENTICATION STATUS

AUTHENTIFICATIONS

NETWORK DEVICES

Rows/Page: 1 / 1 Total Rows

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.

En **Administration > Identity Management > Groups > Endpoint Identity Groups**, cree uno o más grupos y asígneles usuarios. Posteriormente, cada grupo se puede configurar para utilizar una PSK diferente para conectarse a la red.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is "Administration > Identity Management". The "Groups" tab is selected. In the left sidebar, "Endpoint Identity Groups" is highlighted. The main content area is titled "Endpoint Identity Groups" and shows a table with two entries:

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

Buttons for "Edit", "+ Add", and "Delete" are visible above the table. The "Add" button is highlighted with a red box.

The screenshot shows the "New Endpoint Group" form. The breadcrumb navigation is "Administration > Identity Management > Endpoint Identity Group List > New Endpoint Group". The form title is "Endpoint Identity Group". The "Name" field contains "Identity_Group_IPSK" and is highlighted with a red box. There are fields for "Description" and "Parent Group". "Submit" and "Cancel" buttons are at the bottom.

Una vez creado el grupo, puede asignarles usuarios. Seleccione el grupo que ha creado y haga clic en "Editar":

The screenshot shows the "Endpoint Identity Groups" list. The breadcrumb navigation is "Administration > Identity Management". The "Groups" tab is selected. In the left sidebar, "Endpoint Identity Groups" is highlighted. The main content area shows a table with three entries:

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

The "Identity_Group_IPSK" row is highlighted in blue. The "Edit" button above the table is highlighted with a red box.

En la configuración del grupo, agregue la dirección MAC de los clientes que desea asignar a este grupo haciendo clic en el botón "Agregar":

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".

Fields and controls include:

- * Name: Identity_Group_IPSK
- Description: (empty text box)
- Parent Group: (empty text box)
- Buttons: Save, Reset
- Identity Group Endpoints: Selected 0 Total 1
- Buttons: + Add, Remove (with dropdown arrow)
- Filter: All (with dropdown arrow)

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

En Directiva > Elementos de directiva > Resultados > Autorización > Perfiles de autorización, cree un nuevo perfil de autorización. Establezca los atributos en:

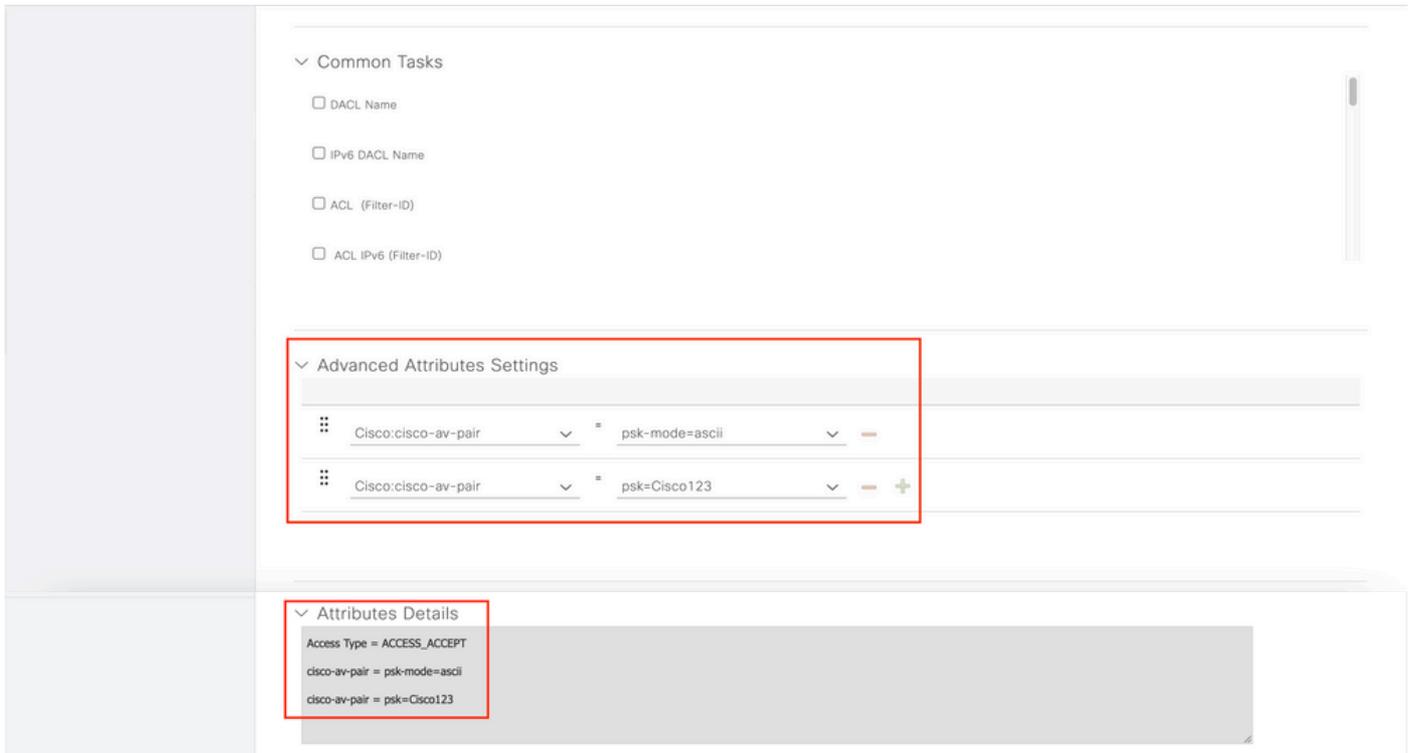
```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

Para cada grupo de usuarios que debe utilizar una PSK diferente, cree un resultado adicional con un par av psk diferente. Aquí también se pueden configurar parámetros adicionales como la anulación de ACL y VLAN.

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

Fields and controls include:

- * 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: ⓘ



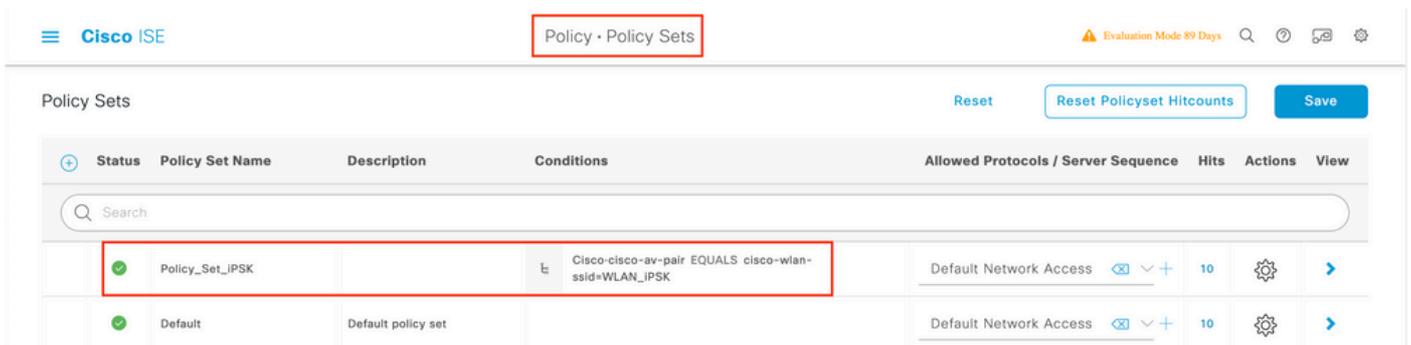
En **Policy > Policy Sets**, cree uno nuevo. Para asegurarse de que el cliente coincide con el conjunto de directivas, se utiliza esta condición:

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

Conditions Studio



Se pueden agregar condiciones adicionales para que la coincidencia de políticas sea más segura.



Vaya a la configuración del conjunto de políticas iPSK recién creado haciendo clic en la flecha azul a la derecha de la línea del conjunto de políticas:

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		

Asegúrese de que **Authentication Policy** esté configurado en "Internal Endpoints":

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
✔	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	

En **Directiva de autorización**, cree una nueva regla para cada uno de los grupos de usuarios. Como condición, utilice:

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

con el **Resultado** siendo el **Perfil de autorización** que se creó previamente. Asegúrese de que la regla **predeterminada** permanece en la parte inferior y señala a **DenyAccess**.

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

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

Si cada usuario va a tener una contraseña diferente, en lugar de crear grupos de terminales y reglas que coincidan con ese grupo de terminales, se puede crear una regla con esta condición:

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

Nota: El delimitador de dirección MAC se puede configurar en el WLC en **AAA >AAA Advanced > Global Config > Advanced Settings**. En este ejemplo, se utilizó el carácter "-".

The screenshot shows the Cisco ISE interface for configuring Policy Sets. The main table lists the following rules:

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	Select from list		
✓	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK	Select from list		
✓	Default		DenyAccess	Select from list	0	

Las reglas de la política de autorización permiten utilizar muchos otros parámetros para especificar la contraseña que el usuario está utilizando. Algunas de las reglas más utilizadas serían:

1. Coincidencia basada en la ubicación del usuario

En este escenario, el WLC necesita enviar la información de la ubicación del AP al ISE. Esto permite a los usuarios de una ubicación utilizar una contraseña, mientras que los usuarios de otra ubicación utilizan una contraseña diferente. Esto se puede configurar en **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. Coincidencia basada en el perfil del dispositivo

En este escenario, el WLC necesita ser configurado para perfilar los dispositivos globalmente. Esto permite al administrador configurar una contraseña diferente para los dispositivos de teléfono y portátil. La clasificación de dispositivos globales se puede habilitar en **Configuration > Wireless > Wireless Global**. Para la configuración de perfiles de dispositivos en ISE, consulte la [Guía de diseño de perfiles de ISE](#).

Además de devolver la clave de cifrado, dado que esta autorización se produce en la fase de asociación 802.11, es totalmente posible devolver otros atributos AAA desde ISE, como ACL o ID de VLAN.

Troubleshoot

Resolución de problemas en el 9800 WLC

En el WLC, recolectar rastros radiactivos debe ser más que suficiente para identificar la mayoría de los problemas. Esto se puede hacer en la interfaz web del WLC bajo **Troubleshooting > Radioactive Trace**. Agregue la dirección MAC del cliente, presione **Start** e intente reproducir el problema. Haga clic en **Generate** para crear el archivo y descargarlo:

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

Importante: Los iPhones de los smartphones IOS 14 y Android 10 utilizan direcciones MAC aleatorias al asociarse a la red. Esta funcionalidad puede interrumpir completamente la configuración de iPSK. Asegúrese de que esta función está desactivada.

Si los rastros radiactivos no son suficientes para identificar el problema, las capturas del paquete se pueden recolectar directamente en el WLC. En **Troubleshooting > Captura de paquetes**, agregue un punto de captura. De forma predeterminada, el WLC utiliza la interfaz de administración inalámbrica para todas las comunicaciones RADIUS AAA. Aumente el tamaño del buffer a 100 MB si el WLC tiene un número alto de clientes:

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 ←

En la imagen siguiente se muestra una captura de paquetes de un intento de autenticación y contabilización exitoso. Utilice este filtro de Wireshark para filtrar todos los paquetes relevantes para este cliente:

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

Troubleshooting de ISE

La principal técnica de solución de problemas de Cisco ISE es la página **Live Logs**, que se encuentra en **Operations > RADIUS > Live Logs**. Se pueden filtrar colocando la dirección MAC del cliente en el campo Endpoint ID. La apertura de un informe completo de ISE proporciona más detalles sobre el motivo del fallo. Asegúrese de que el cliente está aplicando la política de ISE correcta:

The screenshot shows the Cisco ISE interface for 'Operations - RADIUS'. The 'Live Logs' tab is active. Summary statistics are displayed: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (1). The table below shows a log entry for a failed authentication attempt on August 19, 2022, at 08:04:20.5... The 'Identity' is '08:BE:AC:27:8...', 'Endpoint ID' is '08:BE:AC:27:85:7E', and 'Authorization Profile' is 'Authz_Profile_IPSK'. The status is 'Failed' (red circle with exclamation mark).

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).