

Configurar o iPSK do Catalyst 9800 WLC com ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Entender o que é o iPSK e em quais cenários ele se encaixa](#)

[Configurar a WLC 9800](#)

[Configuração do ISE](#)

[Troubleshoot](#)

[Solução de problemas no 9800 WLC](#)

[Solução de problemas do ISE](#)

Introduction

Este documento descreve a configuração de uma WLAN segura iPSK em um Cisco 9800 Wireless LAN Controller com o Cisco ISE como um servidor RADIUS.

Prerequisites

Requirements

Este documento pressupõe que você já esteja familiarizado com a configuração básica de uma WLAN no 9800 e seja capaz de adaptar a configuração à sua implementação.

Componentes Utilizados

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

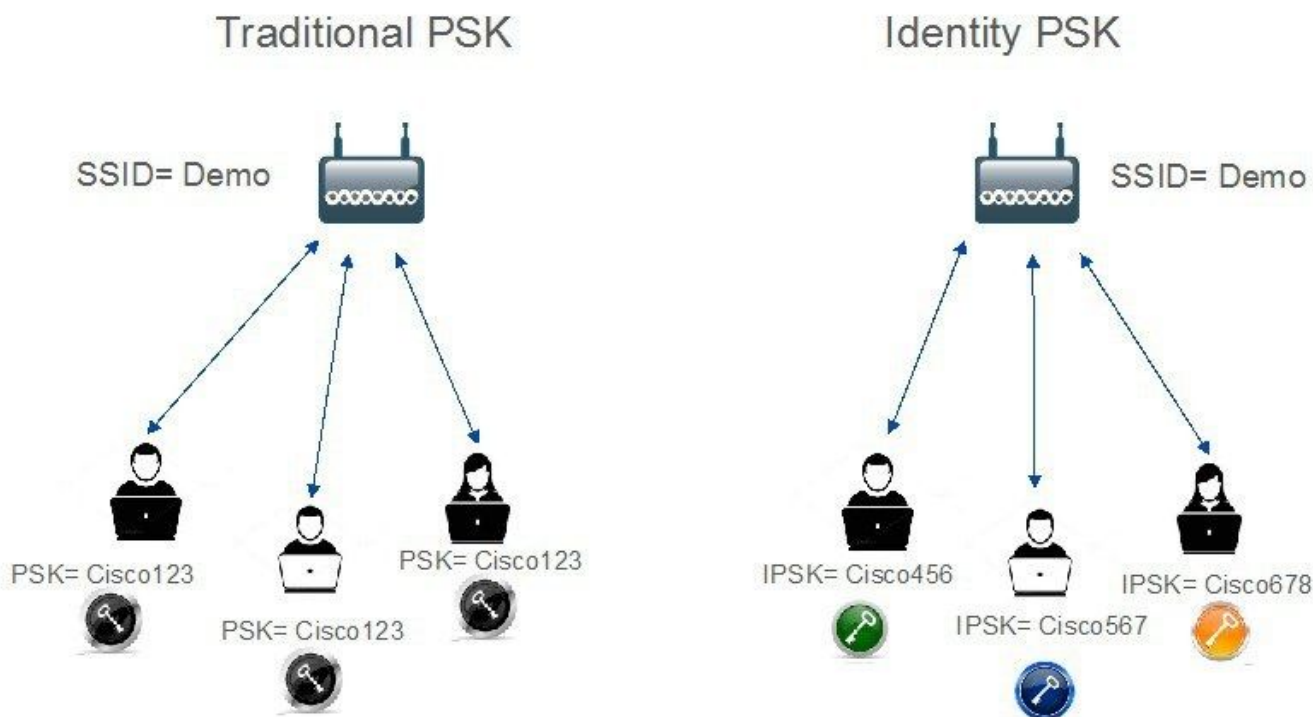
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Entender o que é o iPSK e em quais cenários ele se encaixa

As redes protegidas tradicionais por chave pré-compartilhada (PSK) usam a mesma senha para todos os clientes conectados. Isso pode fazer com que a chave compartilhada com usuários não autorizados cause uma violação de segurança e acesso não autorizado à rede. A mitigação mais comum dessa violação é a alteração da PSK em si, uma alteração que afeta todos os usuários, já que muitos dispositivos finais precisam ser atualizados com a nova chave para acessar a rede novamente.

Com o Identity PSK (iPSK), chaves pré-compartilhadas exclusivas são criadas para indivíduos ou um grupo de usuários no mesmo SSID com a ajuda de um servidor RADIUS. Esse tipo de configuração é extremamente útil em redes onde os dispositivos de cliente final não suportam autenticação dot1x, mas é necessário um esquema de autenticação mais seguro e granular. Da perspectiva do cliente, essa WLAN parece idêntica à rede PSK tradicional. Caso uma das PSKs seja comprometida, somente o indivíduo ou grupo afetado precisará ter sua PSK atualizada. O restante dos dispositivos conectados à WLAN não são afetados.

Traditional Vs Identity PSK



Configurar a WLC 9800

Em **Configuration > Security > AAA > Servers/Groups > Servers**, adicione o 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

1 10 items per page 1 - 1 of 1 items

Em **Configuration > Security > AAA > Servers/Groups > Server Groups**, crie um grupo de servidores RADIUS e adicione o servidor ISE criado anteriormente a ele:

+ 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

Na guia **AAA Method List**, crie uma lista **Authorization** com o tipo "network" e o tipo de grupo "group", apontando para o grupo de servidores RADIUS criado anteriormente:

+ 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

A configuração da Contabilidade é opcional, mas pode ser feita configurando o Tipo como "identity" e apontando-o para o mesmo 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

Isso também pode ser feito por meio da linha de comando usando:

```
radius server
```

Em **Configuration > Tags & Profiles > WLANs**, crie uma nova WLAN. Na configuração da camada 2:

- Habilite a filtragem de endereços MAC e defina a lista de autorização como a criada anteriormente
- Em **Auth Key Mgmt**, habilite a **PSK**
- O campo de chave pré-compartilhada pode ser preenchido com qualquer valor. Isso é feito

apenas para satisfazer o requisito do projeto de interface da Web. Nenhum usuário pode se autenticar usando esta chave. Nesse caso, a chave pré-compartilhada foi definida como "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:

A segregação de usuários pode ser obtida na guia **Advanced**. Defini-la como Permitir grupo privado permite que os usuários que usam a mesma PSK se comuniquem entre si, enquanto os

usuários que usam uma PSK diferente são bloqueados:

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

Em **Configuration > Tags & Profiles > Policy**, crie um novo Policy Profile. Na guia **Access Policies**, defina a VLAN ou o grupo de VLAN que esta WLAN está usando:

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"/>			WLAN ACL
HTTP TLV Caching	<input type="checkbox"/>			IPv4 ACL <input type="text" value="Search or Select"/>
DHCP TLV Caching	<input type="checkbox"/>			IPv6 ACL <input type="text" value="Search or Select"/>
WLAN Local Profiling				URL Filters
Global State of Device Classification	<input type="checkbox"/>			Pre Auth <input type="text" value="Search or Select"/>
Local Subscriber Policy Name	<input type="text" value="Search or Select"/>			Post Auth <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"/>			

Na guia **Advanced**, habilite AAA Override e adicione a lista Accounting se tiver sido criada 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 IGNORE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Em **Configuration > Tags & Profiles > Tags > Policy**, certifique-se de que a WLAN esteja mapeada para o perfil de política que você criou:

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

WLAN_iPSK Policy_Profile_iPSK

1 10 Items per page

1 - 1 of 1 items

Isso também pode ser feito por meio da linha de comando usando:

wlan

Em **Configuration > Wireless > Access Points**, certifique-se de que esta etiqueta tenha sido aplicada nos access points nos quais a WLAN deve ser transmitida:

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"/>	i		

Configuração do ISE

Este guia de configuração cobre um cenário em que a PSK do dispositivo é determinada com base no endereço MAC do cliente. Em **Administração > Recursos de rede > Dispositivos de rede**, adicione um novo dispositivo, especifique o endereço IP, habilite as Configurações de autenticação RADIUS e especifique um Segredo compartilhado 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](#)

Em **Context Visibility > Endpoints > Authentication**, adicione os endereços MAC de todos os dispositivos (clientes) que estão se conectando à rede 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.

Em **Administration > Identity Management > Groups > Endpoint Identity Groups**, crie um ou mais grupos e atribua usuários a eles. Cada grupo pode ser configurado posteriormente para usar uma PSK diferente para se conectar à rede.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes "Cisco ISE", "Administration · Identity Management", and "Evaluation Mode 89 Days". 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 fields are:

- Name: Identity_Group_IPSK
- Description: (empty)
- Parent Group: (dropdown menu)

Buttons for "Submit" and "Cancel" are visible at the bottom right.

Depois que o grupo for criado, você poderá atribuir usuários a eles. Selecione o grupo criado e clique em "Editar":

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes "Cisco ISE", "Administration · Identity Management", and "Evaluation Mode 89 Days". 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"/> Iusiner-Device	Identity Group for Profile: Iusiner-Device

Na configuração do grupo, adicione o endereço MAC do(s) cliente(s) que você deseja atribuir a este grupo clicando no botão "Adicionar":

Administration - Identity Management

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

Endpoint Identity Group List > Identity_Group_IPSK

Endpoint Identity Group

* Name Identity_Group_IPSK

Description

Parent Group

Save Reset

Selected 0 Total 1

+ Add Remove

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

Em Policy > Policy Elements > **Results** > Authorization > Authorization Profiles, crie um novo perfil de autorização. Definir atributos como:

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

Para cada grupo de usuários que deve estar usando uma PSK diferente, crie um resultado adicional com uma psk av-pair diferente. Parâmetros adicionais como ACL e substituição de VLAN também podem ser configurados aqui.

Policy - Policy Elements

Dictionary Conditions **Results**

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name Authz_Profile_IPSK

Description

* Access Type ACCESS_ACCEPT

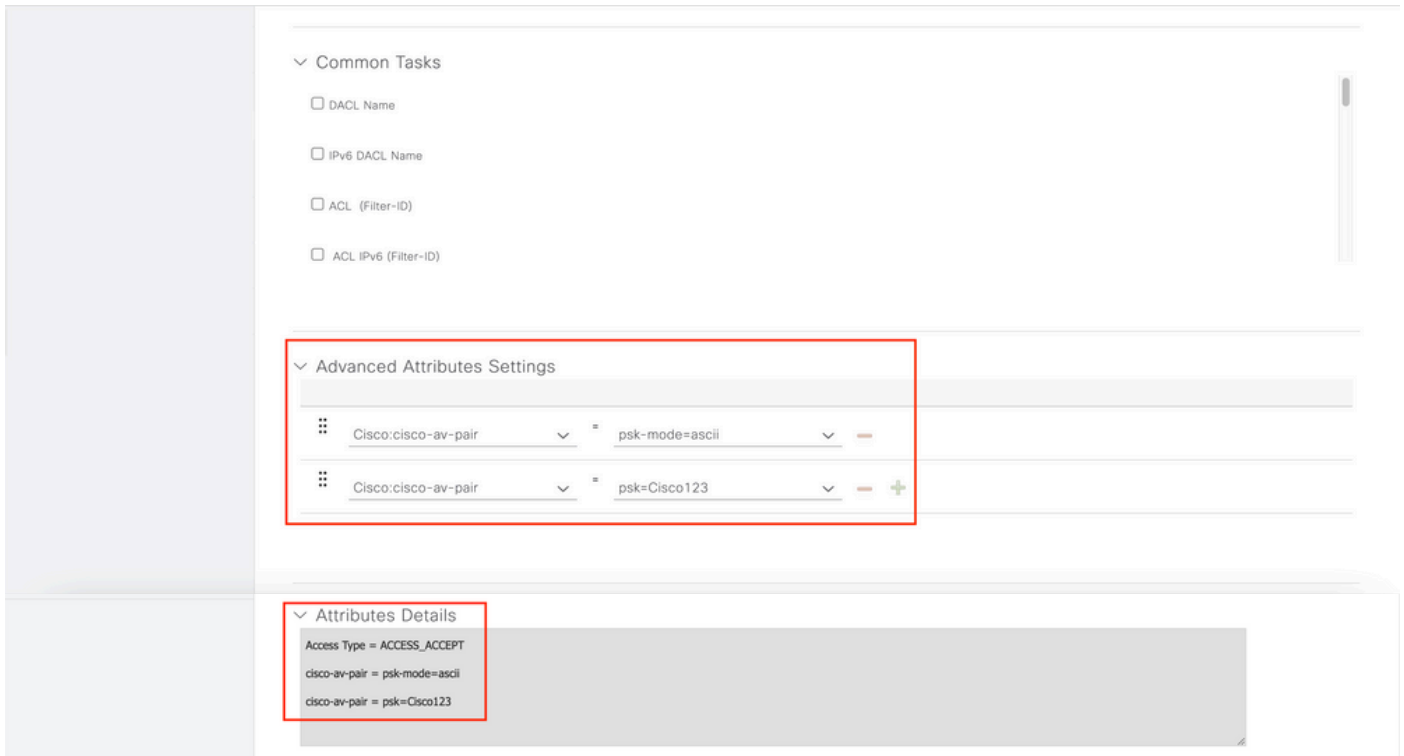
Network Device Profile Cisco

Service Template

Track Movement

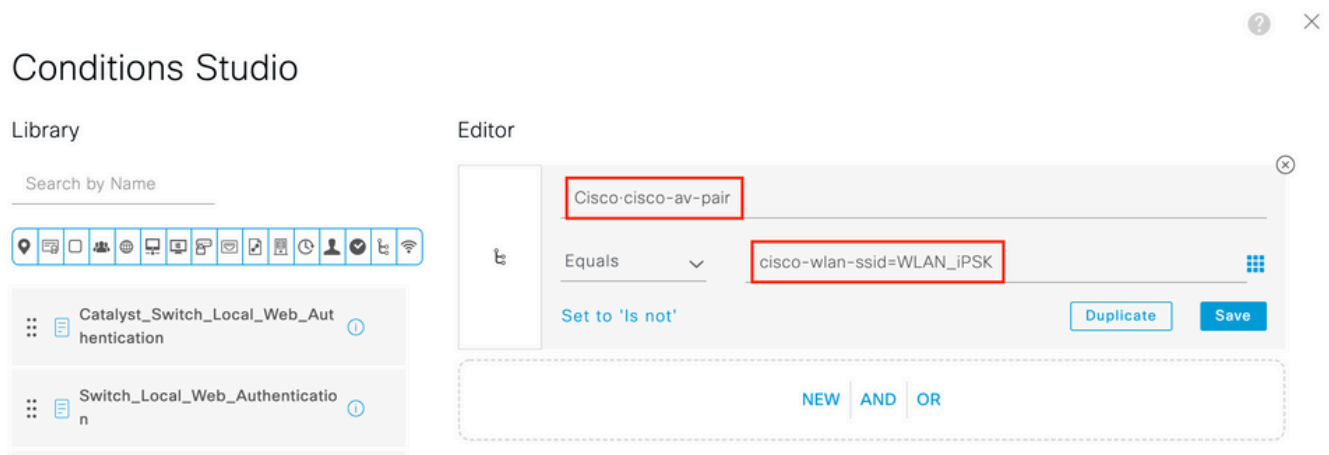
Agentless Posture

Passive Identity Tracking

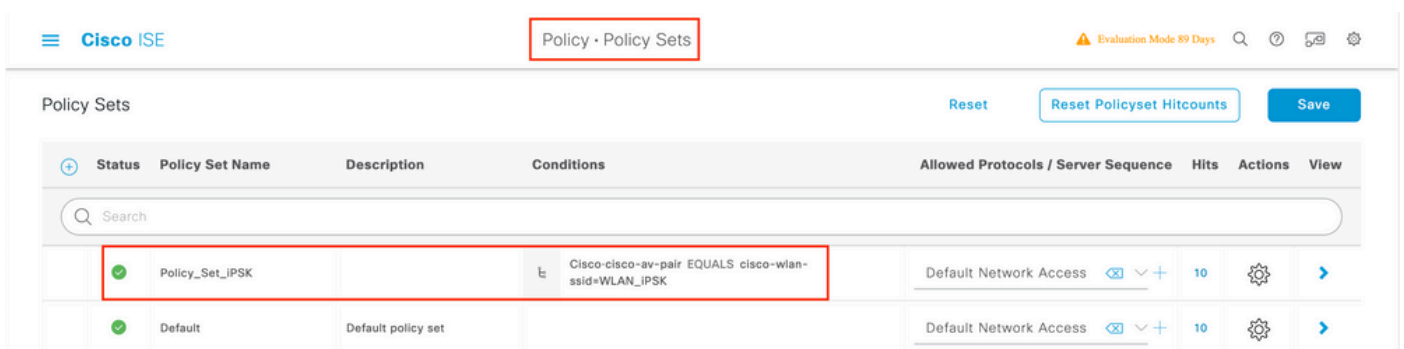


Em **Policy > Policy Sets**, crie um novo. Para garantir que o cliente corresponda ao conjunto de políticas, esta condição é usada:

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



Condições adicionais podem ser adicionadas para tornar a correspondência de políticas mais segura.



Acesse a configuração recém-criada do conjunto de políticas iPSK clicando na seta azul à direita

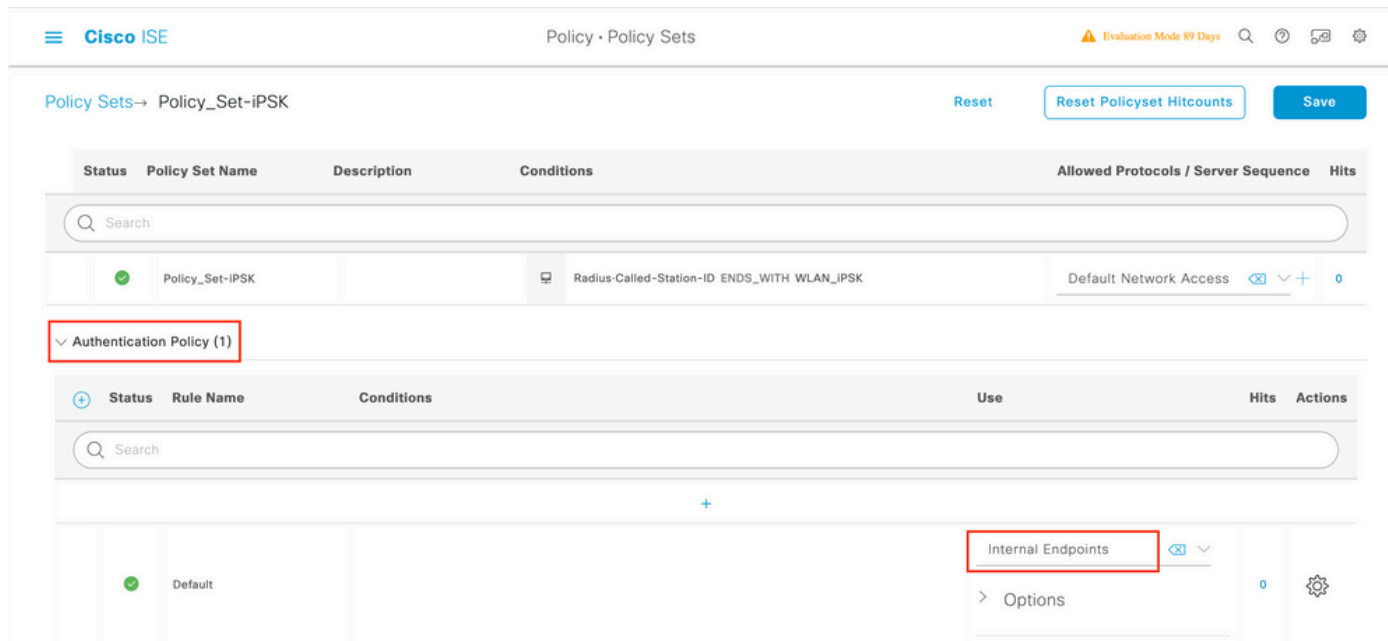
da linha do conjunto de políticas:



The screenshot shows the 'Policy Sets' page in Cisco ISE. At the top right, there are buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. Below is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. A search bar is present. One row is visible with a green status icon, 'Policy_Set_IPSK' name, and a condition 'Cisco-cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_IPSK'. The 'Allowed Protocols / Server Sequence' is 'Default Network Access', 'Hits' is '77', and there is a gear icon and a blue arrow icon in a red box.

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	⚙️	➡️

Certifique-se de que **Authentication Policy** esteja definida como "Internal Endpoints":



The screenshot shows the configuration page for 'Policy_Set-iPSK' in Cisco ISE. It includes a breadcrumb 'Policy Sets → Policy_Set-iPSK' and buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. The main table has columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A search bar is present. One row is visible with a green status icon, 'Policy_Set-iPSK' name, and a condition 'Radius-Called-Station-ID ENDS_WITH WLAN_IPSK'. The 'Allowed Protocols / Server Sequence' is 'Default Network Access', 'Hits' is '0', and there is a gear icon. Below this table, there is a section 'Authentication Policy (1)' with a red box around the header. Underneath is another table with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. A search bar is present. One row is visible with a green status icon, 'Default' name, and 'Internal Endpoints' in the 'Use' column, which is highlighted with a red box. There is also an 'Options' link and a gear icon.

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	⚙️

Em **Authorization Policy**, crie uma nova regra para cada um dos grupos de usuários. Como condição, use:

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

com o **Resultado** sendo o **Perfil de Autorização** que foi criado anteriormente. Certifique-se de que a regra **Default** fique na parte inferior e aponte para **DenyAccess**.

The screenshot shows the Cisco ISE Policy Sets configuration page. At the top, there is a search bar and navigation tabs for 'Internal Endpoints' and 'Options'. Below this, there are sections for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (1)'. The main table displays the following data:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	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	

Se cada usuário tiver uma senha diferente, em vez de criar grupos de endpoint e regras correspondentes a esse grupo de endpoint, uma regra com esta condição poderá ser feita:

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

Note: O delimitador de endereço MAC pode ser configurado na WLC em **AAA >AAA Advanced > Global Config > Advanced Settings**. Neste exemplo, o caractere "-" foi usado.

The screenshot shows the Cisco ISE Policy Sets configuration page with a different rule. The main table displays the following data:

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	

As regras da política de autorização permitem que muitos outros parâmetros sejam usados para especificar a senha que o usuário está utilizando. Algumas das regras mais comumente usadas seriam:

1. Correspondência com base no local do usuário

Neste cenário, a WLC precisa enviar informações de localização do AP para o ISE. Isso

permite que os usuários em um local usem uma senha, enquanto os usuários em outro local usam uma senha diferente. Isso pode ser configurado em **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. Correspondência baseada no perfil do dispositivo

Neste cenário, a WLC precisa ser configurada para criar o perfil dos dispositivos globalmente. Isso permite que um administrador configure uma senha diferente para dispositivos de laptop e telefone. A classificação global de dispositivos pode ser ativada em **Configuration > Wireless > Wireless Global**. Para obter a configuração de criação de perfil do dispositivo no ISE, consulte o [Guia de design de criação de perfil do ISE](#).

Além do retorno da chave de criptografia, como essa autorização acontece na fase de associação 802.11, é inteiramente possível retornar outros atributos AAA do ISE, como ACL ou ID de VLAN.

Troubleshoot

Solução de problemas no 9800 WLC

Na WLC, a coleta de rastreamentos radioativos deve ser mais do que suficiente para identificar a maioria dos problemas. Isso pode ser feito na interface da Web da WLC em **Troubleshooting > Radioactive Trace**. Adicione o endereço MAC do cliente, pressione **Start** e tente reproduzir o problema. Clique em **Gerar** para criar o arquivo e baixá-lo:

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: iPhones em smartphones IOS 14 e Android 10 usam endereços mac aleatórios ao se associarem à rede. Essa funcionalidade pode quebrar completamente a configuração do iPSK. Verifique se esse recurso está desativado!

Se os rastreamentos radioativos não forem suficientes para identificar o problema, as capturas de pacotes poderão ser coletadas diretamente no WLC. Em **Troubleshooting > Captura de Pacotes**, adicione um ponto de captura. Por padrão, a WLC usa a interface de gerenciamento sem fio para todas as comunicações RADIUS AAA. Aumente o tamanho do buffer para 100 MB se a WLC tiver um número alto de clientes:

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 ←

Uma captura de pacote de uma tentativa de autenticação e contabilização bem-sucedida é mostrada na figura abaixo. Use este filtro do Wireshark para filtrar todos os pacotes 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

Solução de problemas do ISE

A principal técnica de solução de problemas no Cisco ISE é a página **Live Logs**, encontrada em **Operations > RADIUS > Live Logs**. Eles podem ser filtrados colocando o endereço MAC do cliente no campo ID do endpoint. Abrir um relatório completo do ISE fornece mais detalhes sobre o motivo da falha. Verifique se o cliente está atingindo a política correta do ISE:

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	

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.