

# Configuration de Catalyst 9800 WLC iPSK avec ISE

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Comprendre ce qu'est l'iPSK et les scénarios qu'il convient](#)

[Configuration du WLC 9800](#)

[Configuration ISE](#)

[Dépannage](#)

[Dépannage du WLC 9800](#)

[Dépanner ISE](#)

## Introduction

Ce document décrit la configuration d'un WLAN sécurisé iPSK sur un contrôleur LAN sans fil Cisco 9800 avec Cisco ISE comme serveur RADIUS.

## Conditions préalables

### Conditions requises

Ce document suppose que vous êtes déjà familiarisé avec la configuration de base d'un WLAN sur le 9800 et que vous êtes capable d'adapter la configuration à votre déploiement.

### Components Used

- WLC Cisco 9800-CL qui exécute 17.6.3
- Cisco ISE 3.0

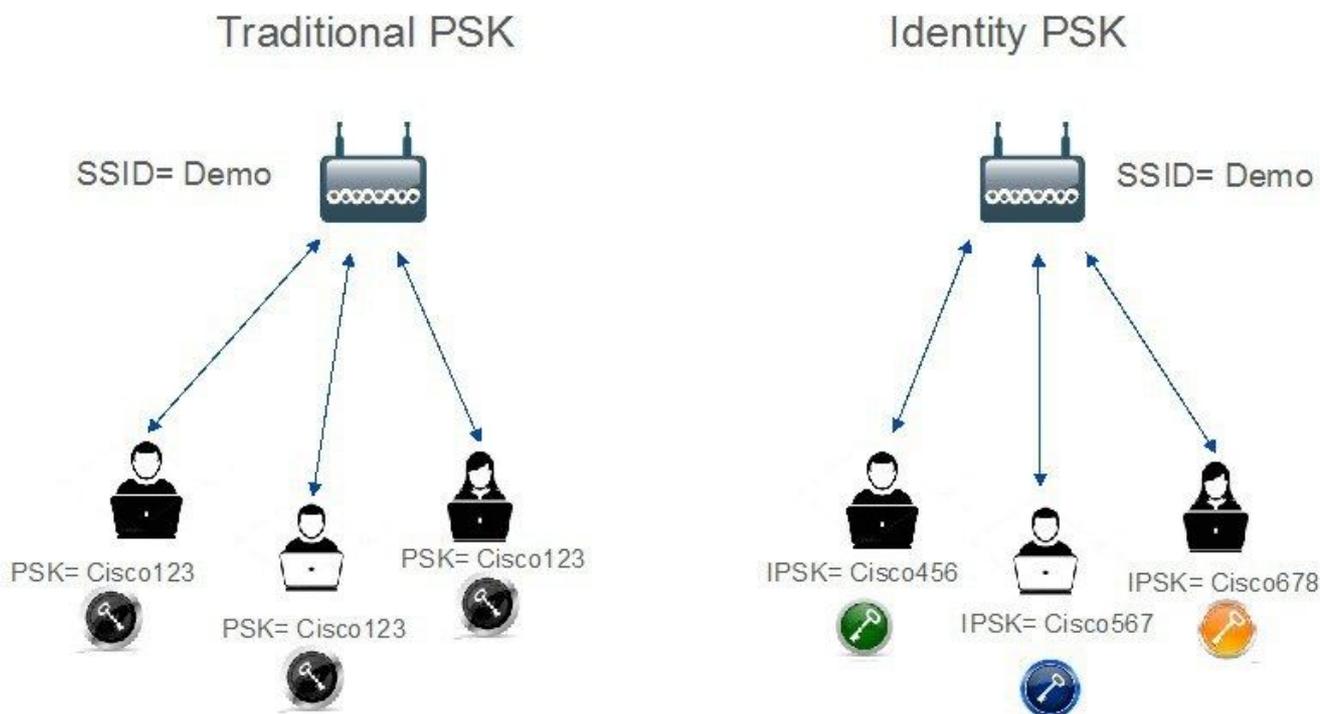
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Comprendre ce qu'est l'iPSK et les scénarios qu'il convient

Les réseaux sécurisés à clé prépartagée (PSK) traditionnelle utilisent le même mot de passe pour tous les clients connectés. La clé peut ainsi être partagée avec des utilisateurs non autorisés, ce qui peut entraîner une faille de sécurité et un accès non autorisé au réseau. L'atténuation la plus courante de cette faille est la modification de la clé PSK elle-même, une modification qui affecte tous les utilisateurs puisque de nombreux périphériques finaux doivent être mis à jour avec la nouvelle clé afin d'accéder à nouveau au réseau.

Avec Identity PSK (iPSK), des clés pré-partagées uniques sont créées pour des individus ou un groupe d'utilisateurs sur le même SSID à l'aide d'un serveur RADIUS. Ce type de configuration est extrêmement utile dans les réseaux où les périphériques clients finaux ne prennent pas en charge l'authentification dot1x, mais où un schéma d'authentification plus sécurisé et granulaire est nécessaire. Du point de vue du client, ce WLAN est identique au réseau PSK traditionnel. Dans le cas où l'une des clés PSK est compromise, seule la personne ou le groupe touché doit avoir sa clé PSK mise à jour. Les autres périphériques connectés au WLAN ne sont pas affectés.

## Traditional Vs Identity PSK



## Configuration du WLC 9800

Sous **Configuration > Security > AAA > Servers/Groups > Servers**, ajoutez l'ISE en tant que serveur 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 - 1 of 1 items

Sous **Configuration > Security > AAA > Servers/Groups > Server Groups**, créez un groupe de serveurs RADIUS et ajoutez-y le serveur ISE précédemment créé :

+ AAA Wizard

Servers / Groups    AAA Method List    AAA Advanced

+ Add    × Delete

**RADIUS**

TACACS+

LDAP

Servers    **Server Groups**

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

10 items per page    1 - 1 of 1 items

Dans l'onglet **AAA Method List**, créez une liste d'autorisation avec le type «**network**» et le type de groupe «**group**» pointant vers le groupe de serveurs RADIUS précédemment créé :

+ AAA Wizard

Servers / Groups    **AAA Method List**    AAA Advanced

Authentication

**Authorization**

Accounting

+ Add    × Delete

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

10 items per page    1 - 1 of 1 items

La configuration de la gestion des comptes est facultative, mais elle peut être effectuée en configurant le type sur «**identité**» et en le pointant vers le même groupe de serveurs 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

10 items per page    1 - 1 of 1 items

Cette opération peut également être effectuée via la ligne de commande à l'aide de :

radius server

Sous **Configuration > Tags & Profiles > WLANs**, créez un nouveau WLAN. Sous la configuration de couche 2 :

- Activez le filtrage MAC et définissez la liste d'autorisations sur celle créée précédemment
- Sous **Auth Key Mgmt** enable **PSK**
- Le champ de clé pré-partagée peut être rempli avec n'importe quelle valeur. Cette opération est effectuée uniquement pour répondre aux exigences de la conception de l'interface Web.

Aucun utilisateur ne peut s'authentifier à l'aide de cette clé. Dans ce cas, la clé pré-partagée a été définie sur « 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 séparation des utilisateurs peut être réalisée sous l'onglet **Advanced**. Sa définition sur Allow Private Group permet aux utilisateurs utilisant la même clé prépartagée de communiquer entre eux, tandis que les utilisateurs utilisant une autre clé prépartagée sont bloqués :

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"/>

Sous **Configuration > Tags & Profiles > Policy**, créez un nouveau profil de stratégie. Dans l'onglet **Access Policies**, définissez le VLAN ou le groupe de VLAN que ce WLAN utilise :

**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"/>			

Dans l'onglet **Advanced**, activez AAA Override et ajoutez la liste Accounting si elle a été créée précédemment :

## 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

Sous **Configuration > Tags & Profiles > Tags > Policy**, vérifiez que le WLAN est mappé au profil de stratégie que vous avez créé :

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

Cette opération peut également être effectuée via la ligne de commande à l'aide de :

wlan

Sous **Configuration > Wireless > Access Points**, vérifiez que cette balise a été appliquée aux points d'accès sur lesquels le WLAN doit être diffusé :

**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"/> ⓘ

## Configuration ISE

Ce guide de configuration couvre un scénario dans lequel la clé PSK du périphérique est déterminée en fonction de l'adresse MAC du client. Sous **Administration > Network Resources > Network Devices**, ajoutez un nouveau périphérique, spécifiez l'adresse IP, activez les paramètres d'authentification RADIUS et spécifiez un secret partagé 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](#)

Sous **Context Visibility > Endpoints > Authentication**, ajoutez les adresses MAC de tous les périphériques (clients) qui se connectent au réseau iPSK :

Cisco ISE Context Visibility - Endpoints

Authentication

INACTIVE ENDPOINTS

AUTHENTICATION STATUS

AUTHENTIFICATIONS

NETWORK DE

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 Re...	Authentication ...	Authorization P..
08:BE:AC:27:85:7E	*		08beac278...		Location...	Unknown	-	MAB	Basic_Authenticate.

Sous **Administration > Identity Management > Groups > Endpoint Identity Groups**, créez un ou plusieurs groupes et attribuez-leur des utilisateurs. Chaque groupe peut être configuré ultérieurement pour utiliser une clé prépartagée différente pour se connecter au réseau.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail 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 in the Cisco ISE Administration interface. The breadcrumb trail 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 also fields for "Description" and "Parent Group". "Submit" and "Cancel" buttons are at the bottom.

Une fois le groupe créé, vous pouvez lui attribuer des utilisateurs. Sélectionnez le groupe que vous avez créé et cliquez sur "Modifier" :

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail 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 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.

Dans la configuration du groupe, ajoutez l'adresse MAC du ou des clients que vous souhaitez affecter à ce groupe en cliquant sur le bouton « Ajouter » :

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is "Endpoint Identity Group List > Identity\_Group\_IPSK". The main form is titled "Endpoint Identity Group" and contains the following fields:

- \* Name: Identity\_Group\_IPSK
- Description: (empty text area)
- 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 "+ Add" button. A table below shows one endpoint:

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

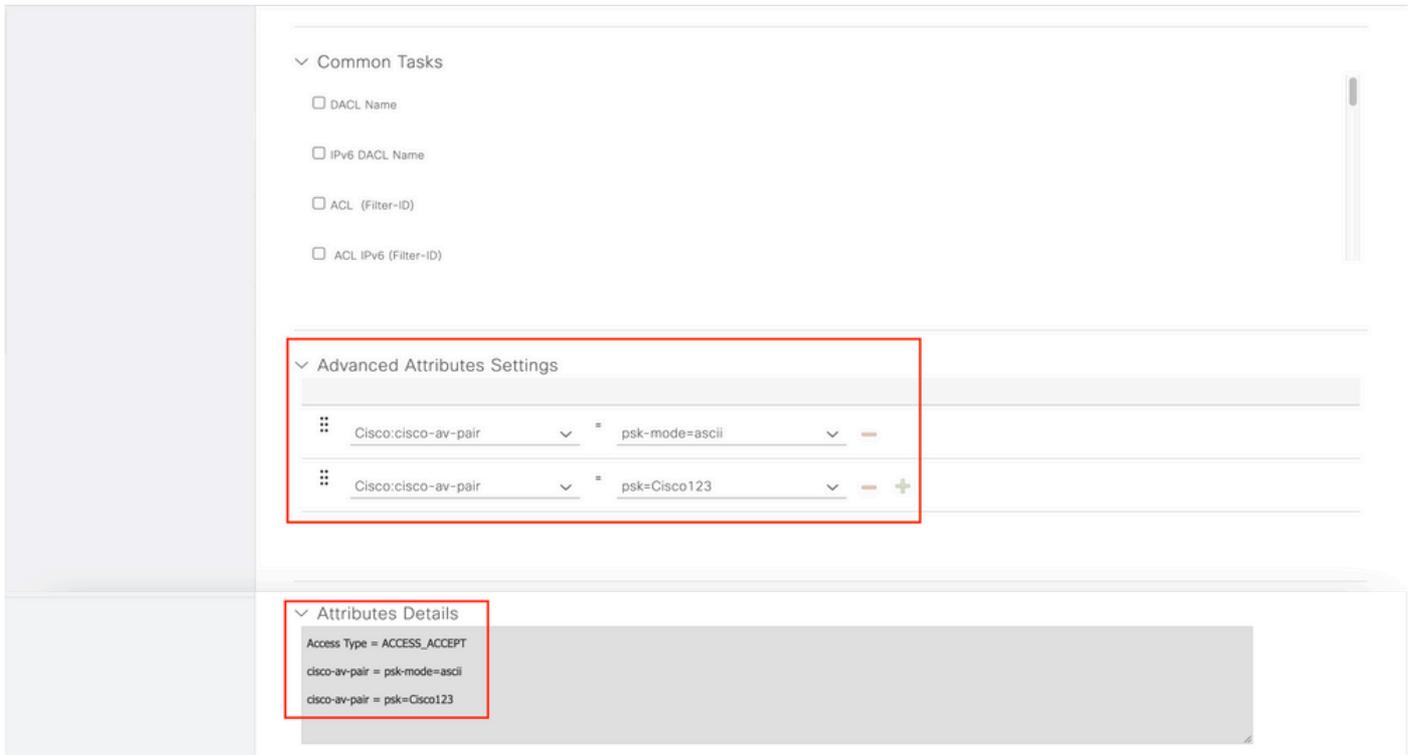
Sous Stratégie > **Éléments de stratégie** > Résultats > Autorisation > Profils d'autorisation, créez un nouveau profil d'autorisation. Définissez les attributs comme suit :

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

Pour chaque groupe d'utilisateurs devant utiliser une clé prépartagée différente, créez un résultat supplémentaire avec une paire av-psk différente. D'autres paramètres tels que ACL et VLAN override peuvent également être configurés ici.

The screenshot shows the Cisco ISE Administration interface for Policy Elements. The breadcrumb trail is "Policy > Policy Elements". The main form is titled "Authorization Profile" and contains the following fields:

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

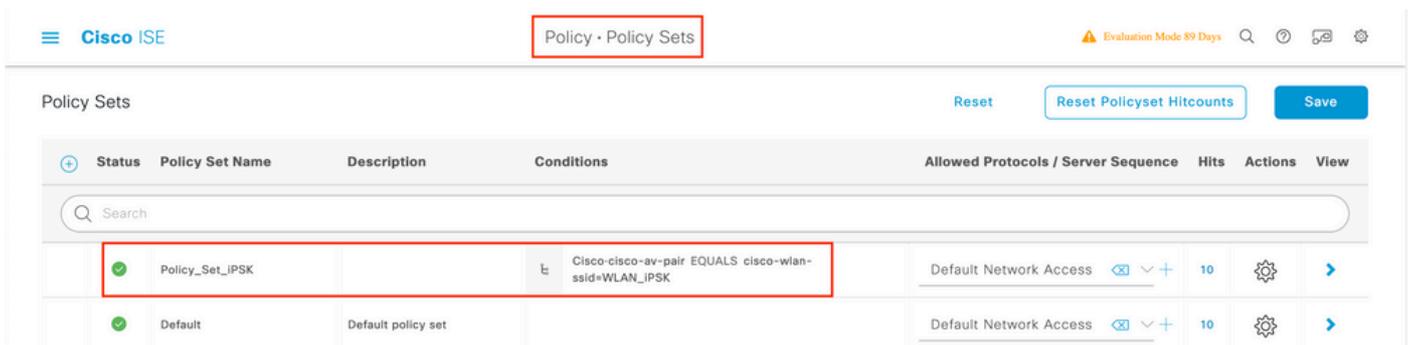


Sous **Policy > Policy Sets**, créez-en un nouveau. Pour vous assurer que le client correspond au jeu de stratégies, utilisez la condition suivante :

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



Des conditions supplémentaires peuvent être ajoutées pour sécuriser davantage la mise en correspondance des stratégies.



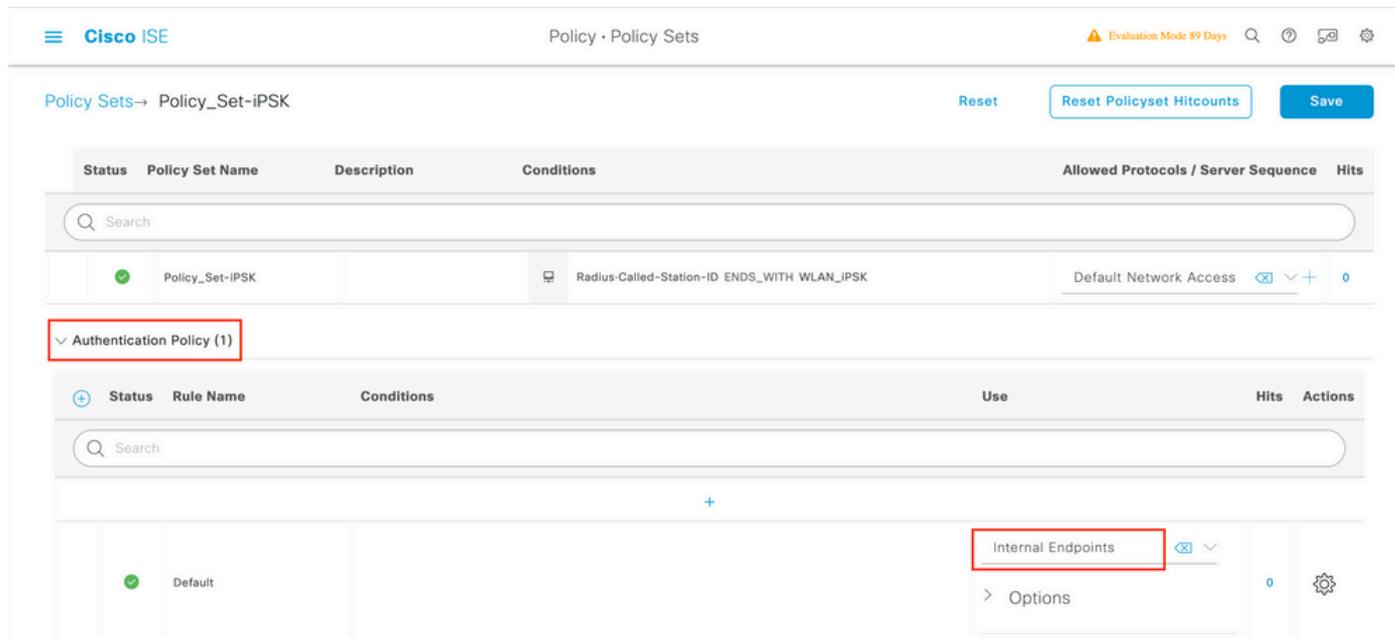
Accédez à la configuration du jeu de stratégies iPSK nouvellement créé en cliquant sur la flèche

bleue à droite de la ligne Jeu de stratégies :



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		

Assurez-vous que la **stratégie d'authentification** est définie sur « Terminaux internes » :



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	

Sous **Stratégie d'autorisation**, créez une nouvelle règle pour chacun des groupes d'utilisateurs. Comme condition, utilisez :

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

le **résultat** étant le **profil d'autorisation** précédemment créé. Assurez-vous que la règle **par défaut** reste en bas et pointe vers **DenyAccess**.

The screenshot shows the Cisco ISE Policy Sets interface. At the top, there is a search bar and navigation tabs for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (1)'. Below this is a table with columns: Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. The table contains three rows: 'Authz\_Rule\_Group1' (highlighted with a red box), 'Authz\_Rule\_Group1' (not visible in the screenshot), and 'Default'. The 'Authz\_Rule\_Group1' row has a status of 'On', a condition of 'IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity\_Group\_IPSK', and a profile of 'Authz\_Profile\_IPSK'. The 'Default' row has a status of 'On', a profile of 'DenyAccess', and 0 hits.

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

Si chaque utilisateur doit avoir un mot de passe différent, au lieu de créer des groupes de terminaux et des règles correspondant à ce groupe de terminaux, une règle avec cette condition peut être créée :

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

**Note:** Le délimiteur d'adresse MAC peut être configuré sur le WLC sous **AAA > AAA Advanced > Global Config > Advanced Settings**. Dans cet exemple, le caractère "-" a été utilisé.

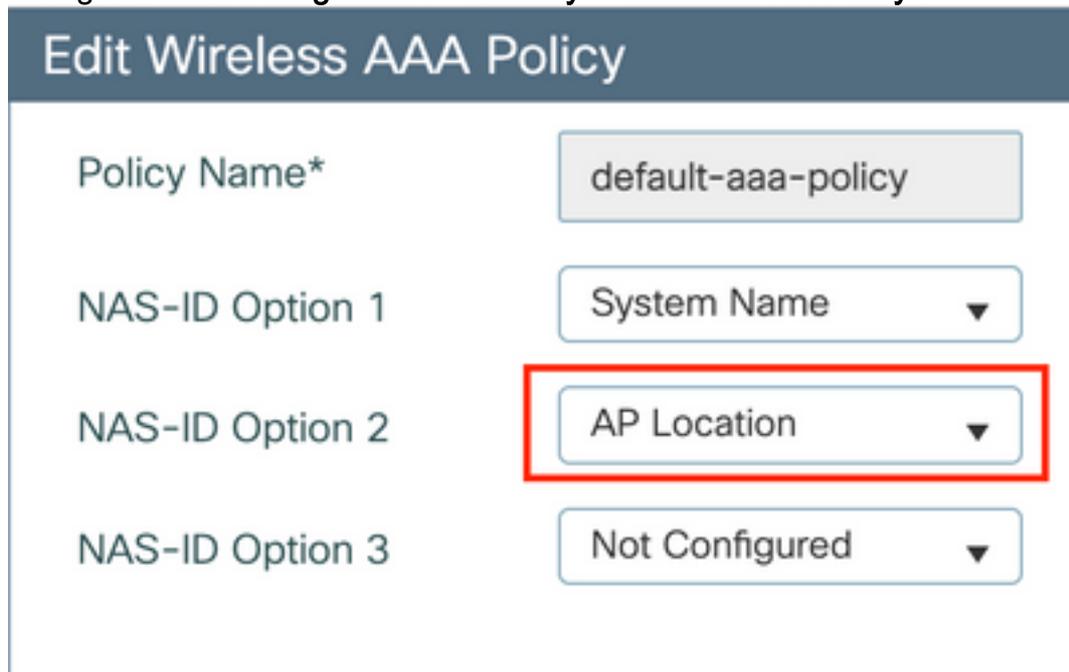
The screenshot shows the Cisco ISE Policy Sets interface. At the top, there is a search bar and navigation tabs for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (1)'. Below this is a table with columns: Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. The table contains three rows: 'Authz\_Rule\_Single' (highlighted with a red box), 'Authz\_Rule\_Group1', and 'Default'. The 'Authz\_Rule\_Single' row has a status of 'On', a condition of 'Radius-Calling-Station-ID EQUALS 08-BE-AC-27-85-7E', and a profile of 'Authz\_Profile\_IPSK'. The 'Authz\_Rule\_Group1' row has a status of 'On', a condition of 'IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity\_Group\_IPSK', and a profile of 'Authz\_Profile\_IPSK'. The 'Default' row has a status of 'On', a profile of 'DenyAccess', and 0 hits.

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

Les règles de la stratégie d'autorisation permettent d'utiliser de nombreux autres paramètres afin de spécifier le mot de passe utilisé par l'utilisateur. Voici quelques-unes des règles les plus couramment utilisées :

### 1. Correspondance basée sur l'emplacement de l'utilisateur

Dans ce scénario, le WLC doit envoyer des informations d'emplacement AP à l'ISE. Cela permet aux utilisateurs d'un emplacement d'utiliser un mot de passe, alors que les utilisateurs d'un autre emplacement utilisent un mot de passe différent. Vous pouvez le configurer sous **Configuration > Security > Wireless AAA Policy** :



The screenshot shows the 'Edit Wireless AAA Policy' configuration page. The form contains the following fields:

Field	Value
Policy Name*	default-aaa-policy
NAS-ID Option 1	System Name
NAS-ID Option 2	AP Location
NAS-ID Option 3	Not Configured

## 2. Correspondance basée sur le profilage du périphérique

Dans ce scénario, le WLC doit être configuré pour profiler les périphériques globalement. Cela permet à un administrateur de configurer un mot de passe différent pour les ordinateurs portables et les téléphones. La classification globale des périphériques peut être activée sous **Configuration > Wireless > Wireless Global**. Pour la configuration du profilage de périphérique sur ISE, consultez le [Guide de conception du profilage ISE](#).

En plus de renvoyer la clé de cryptage, puisque cette autorisation se produit à la phase d'association 802.11, il est entièrement possible de renvoyer d'autres attributs AAA à partir d'ISE tels que l'ACL ou l'ID de VLAN.

## Dépannage

### Dépannage du WLC 9800

Sur le WLC, la collecte de traces radioactives doit être plus que suffisante pour identifier une majorité de problèmes. Cela peut être fait dans l'interface Web du WLC sous **Troubleshooting > Radioactive Trace**. Ajoutez l'adresse MAC du client, appuyez sur **Démarrer** et essayez de reproduire le problème. Cliquez sur **Generate** pour créer le fichier et le télécharger :

## 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

**Important** : les iPhones sur les smartphones IOS 14 et Android 10 utilisent une adresse MAC aléatoire lors de l'association au réseau. Cette fonctionnalité peut complètement casser la configuration iPSK. Assurez-vous que cette fonctionnalité est désactivée !

Si les traces radioactives ne suffisent pas à identifier le problème, les captures de paquets peuvent être collectées directement sur le WLC. Sous **Troubleshooting > Packet Capture**, ajoutez un point de capture. Par défaut, WLC utilise l'interface de gestion sans fil pour toutes les communications AAA RADIUS. Augmentez la taille de la mémoire tampon à 100 Mo si le WLC a un nombre élevé de clients :

### 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 ←

La capture de paquets d'une tentative d'authentification et de gestion des comptes réussie est illustrée dans l'image ci-dessous. Utilisez ce filtre Wireshark pour filtrer tous les paquets appropriés pour ce 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

## Dépanner ISE

La principale technique de dépannage sur Cisco ISE est la page **Live Logs**, qui se trouve sous **Operations > RADIUS > Live Logs**. Ils peuvent être filtrés en plaçant l'adresse MAC du client dans le champ ID de point de terminaison. L'ouverture d'un rapport ISE complet donne plus de détails sur la raison de la panne. Assurez-vous que le client applique la stratégie ISE appropriée :

**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

Refresh Reset Repeat Counts Export To Filter

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.