Configurer l’iPSK du contrôleur WLC Catalyst 9800 avec ISE

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

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

- Restrictions

Configuration du WLC 9800

Configuration ISE

Dépannage

- Dépannage du WLC 9800
- Dépannage d'ISE

Références

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

Exigences

- Connaissance de la configuration de base d’un WLAN sur le 9800
- Capacité à adapter la configuration à votre déploiement

Composants utilisés

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

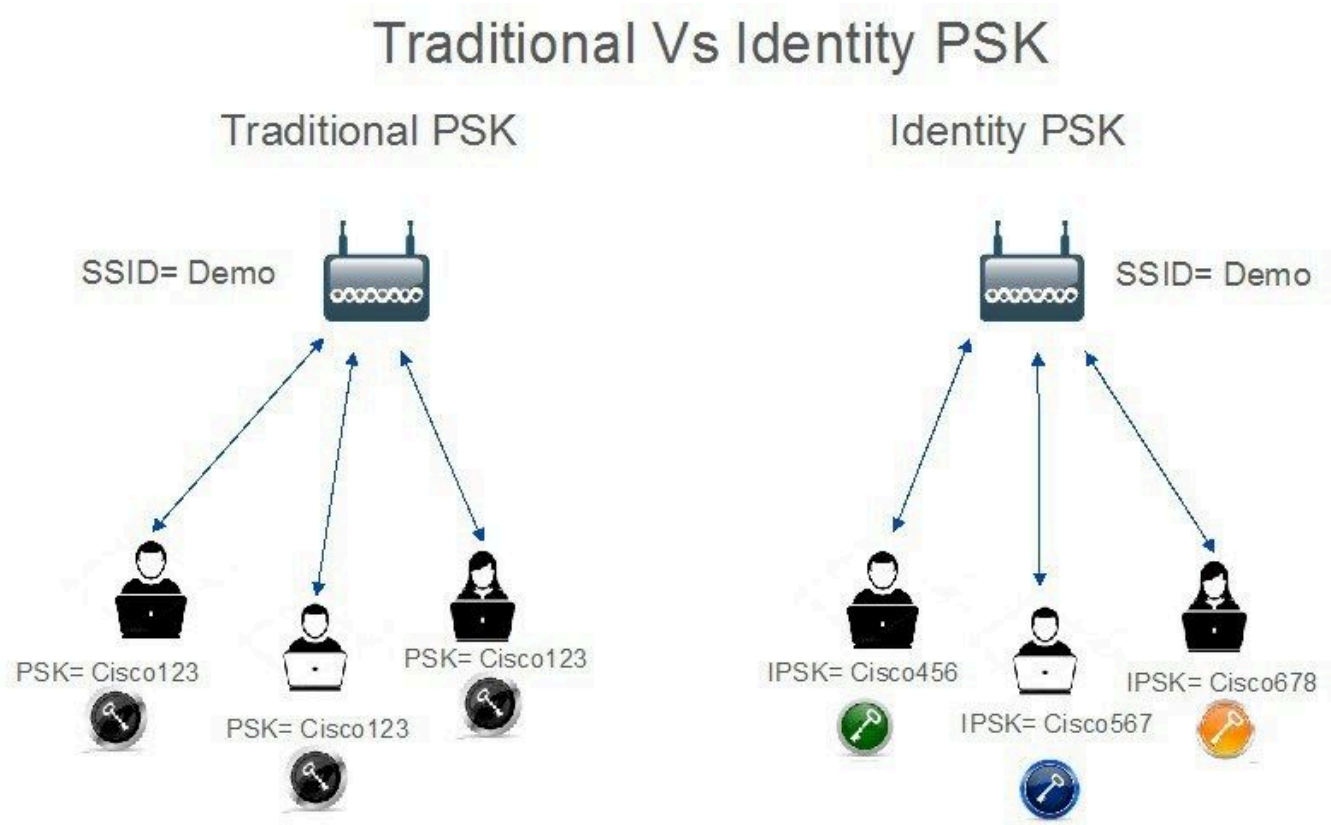
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

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 brèche est le changement de PSK lui-même. Cela a un impact sur tous les utilisateurs, car de nombreux périphériques finaux doivent être mis à jour avec la nouvelle clé afin d'accéder à nouveau au réseau.

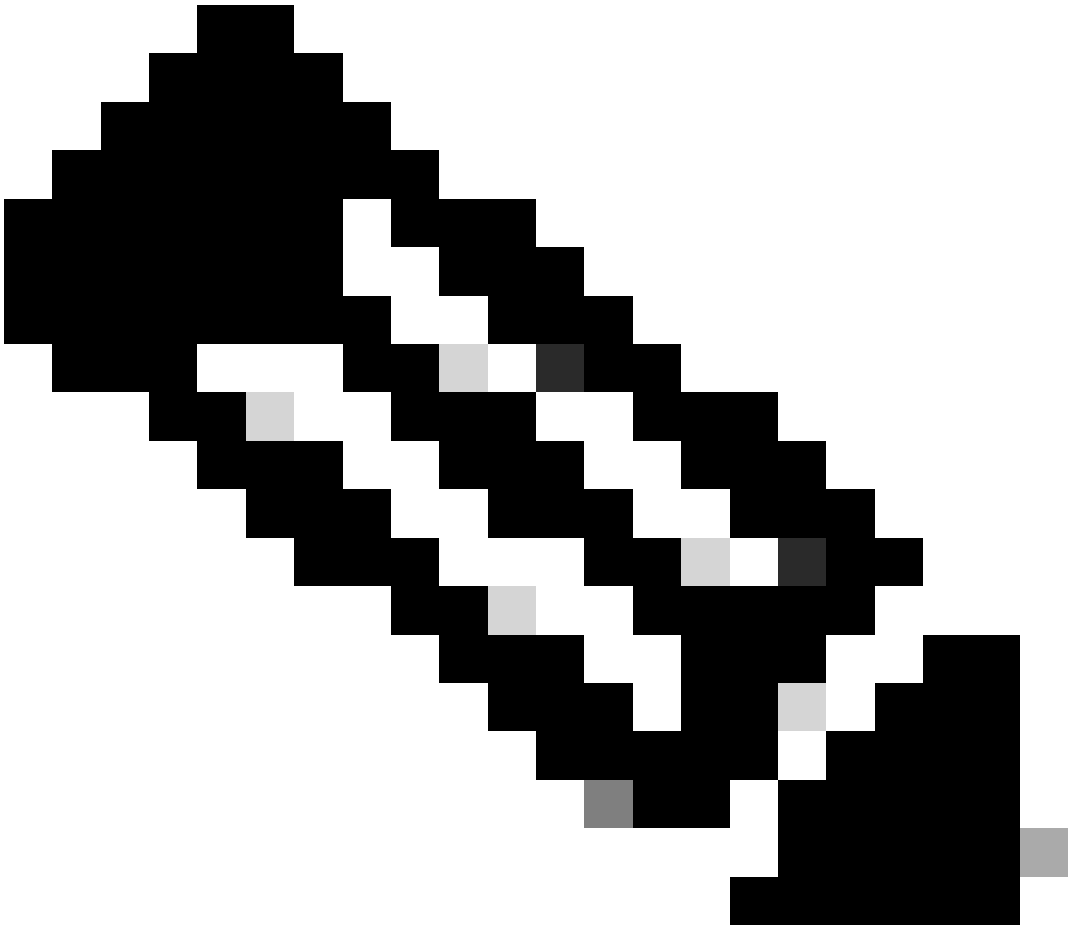
Avec Identity PSK (iPSK), des clés pré-partagées uniques sont créées pour des individus ou un groupe d'utilisateurs sur le même SSID à l'aide d'un serveur RADIUS. Ce type de configuration est extrêmement utile dans les réseaux où les périphériques clients finaux ne prennent pas en charge l'authentification dot1x, mais où un schéma d'authentification plus sécurisé et plus 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.



Restrictions

- Un WLC dont le filtrage Mac et le remplacement AAA sont activés avec ISE configuré, permet aux périphériques configurés IPSK de se connecter au WLAN avec des adresses MAC configurées sur ISE.
- Les périphériques dont les adresses MAC sont configurées sur ISE ne peuvent pas se connecter au PSK générique WLAN, mais uniquement avec IPSK configuré pour ce périphérique.
- Les périphériques dont les adresses non MAC sont configurées sur ISE peuvent se connecter à un réseau local sans fil avec une clé prépartagée générique uniquement.

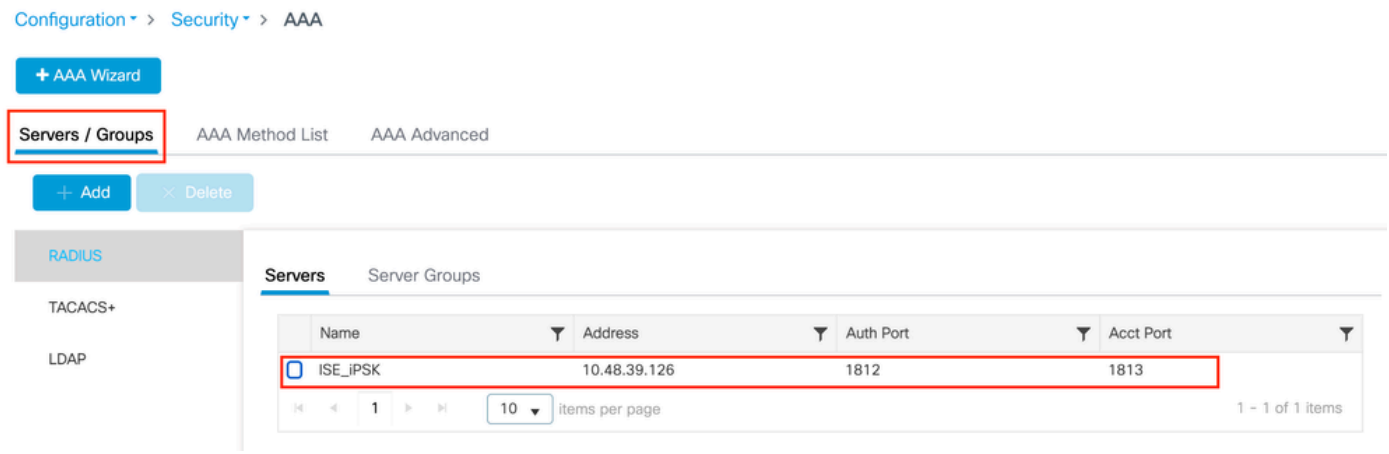
- IPSK prend en charge les modes Local et Flexconnect (authentification centrale et commutation locale). L'authentification locale n'est pas prise en charge.
- IPSK prend en charge FSR et la mise en cache des clés est effectuée pour des itinéraires plus rapides afin d'éviter une connexion RADIUS sur chaque itinéraire.
- Pour activer la validité de l'IPSK à certaines heures planifiées - la planification/validité de l'heure peut être exploitée en utilisant l'attribut radius session-timeout dans la réponse radius.



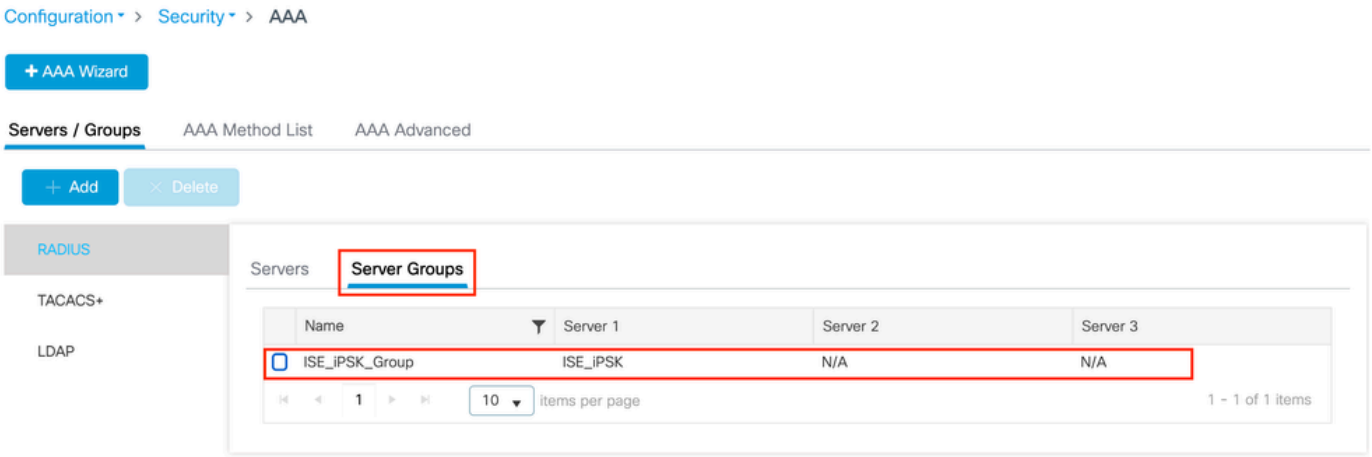
Remarque : iPSK est entièrement pris en charge avec WPA3-SAE

Configuration du WLC 9800

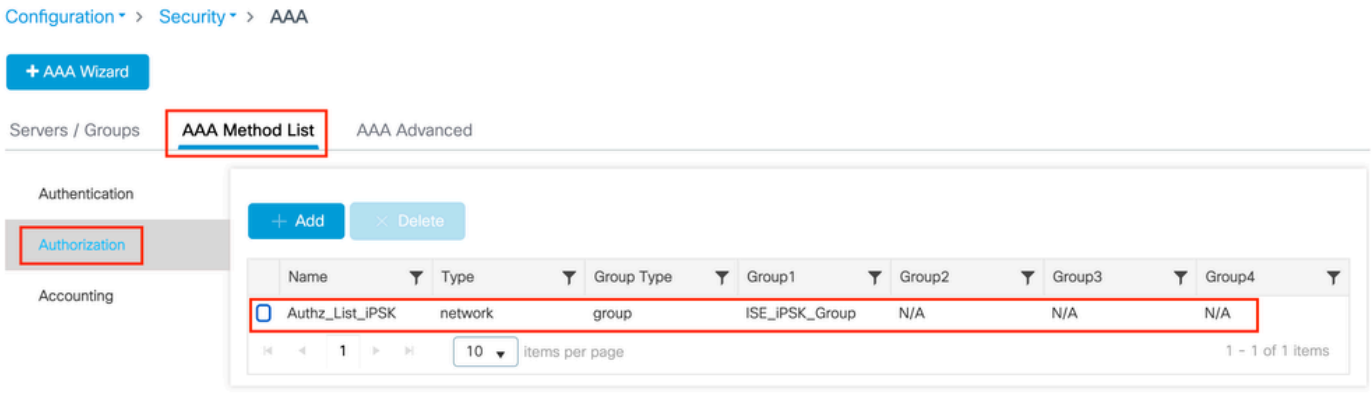
Sous Configuration > Security > AAA > Servers/Groups > Servers, ajoutez l'ISE en tant que serveur RADIUS :



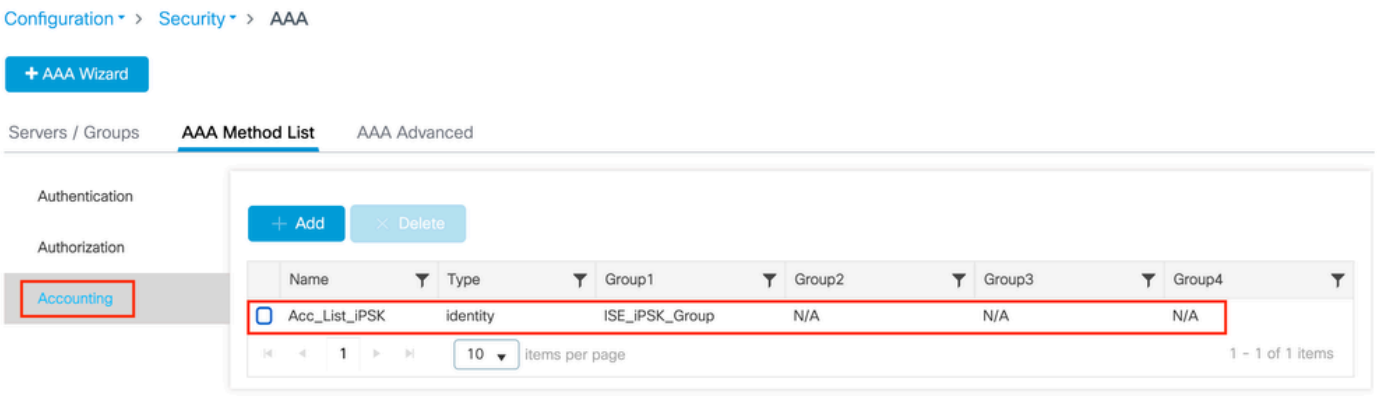
Sous Configuration > Security > AAA > Servers/Groups > Server Groups, créez un groupe de serveurs RADIUS et ajoutez-y le serveur ISE précédemment créé :



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 :



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 :



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

```
radius server

 address ipv4

         auth-port 1812 acct-port 1813
 key 0


aaa group server radius

 server name


aaa authorization network

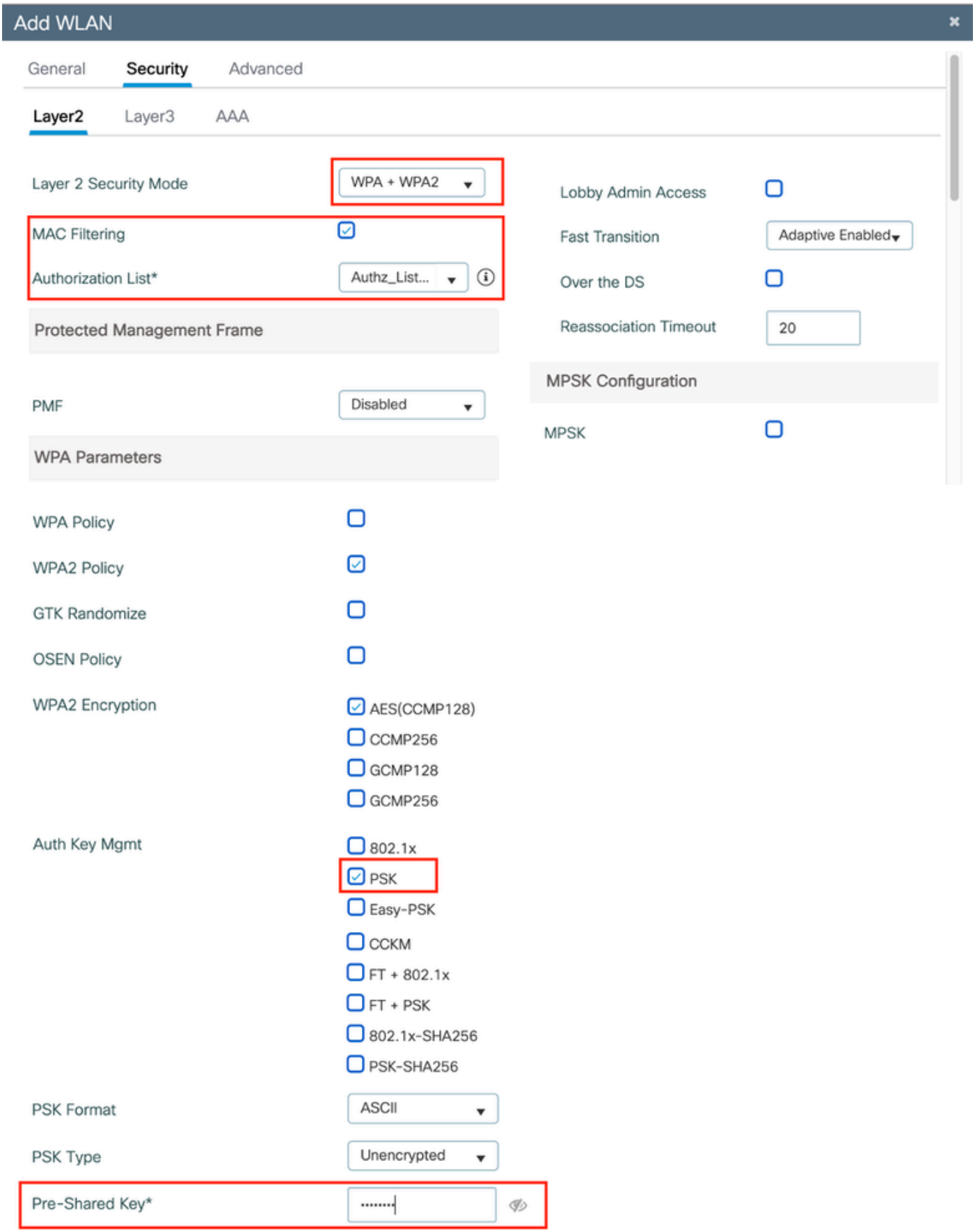
             group

aaa accounting identity

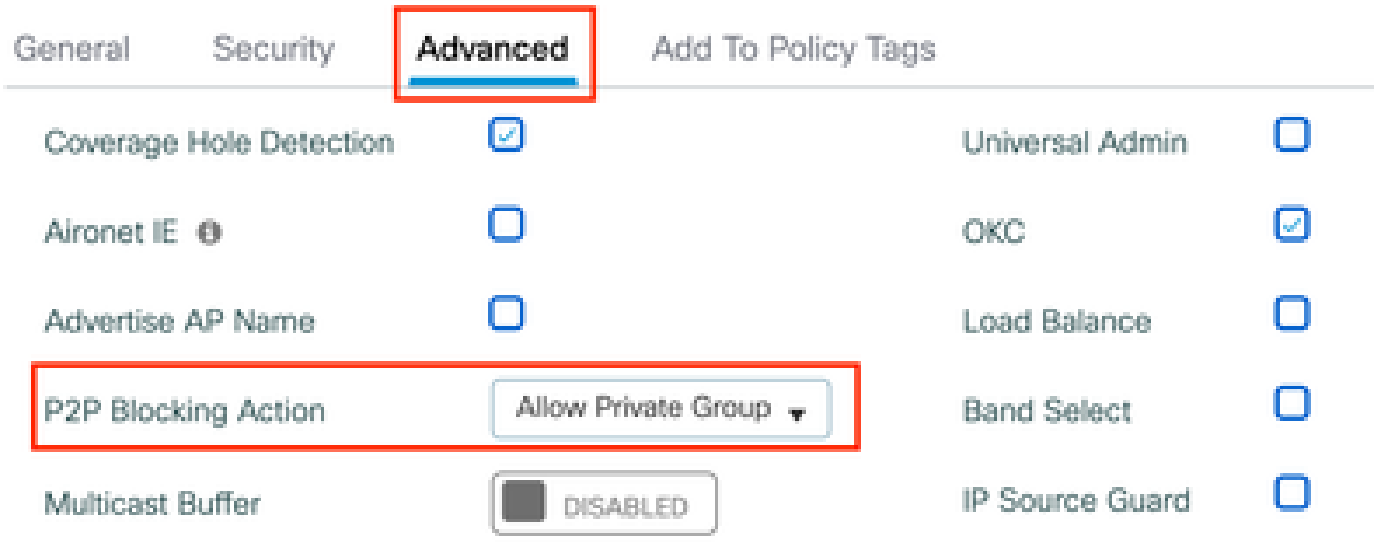
               start-stop group
```

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

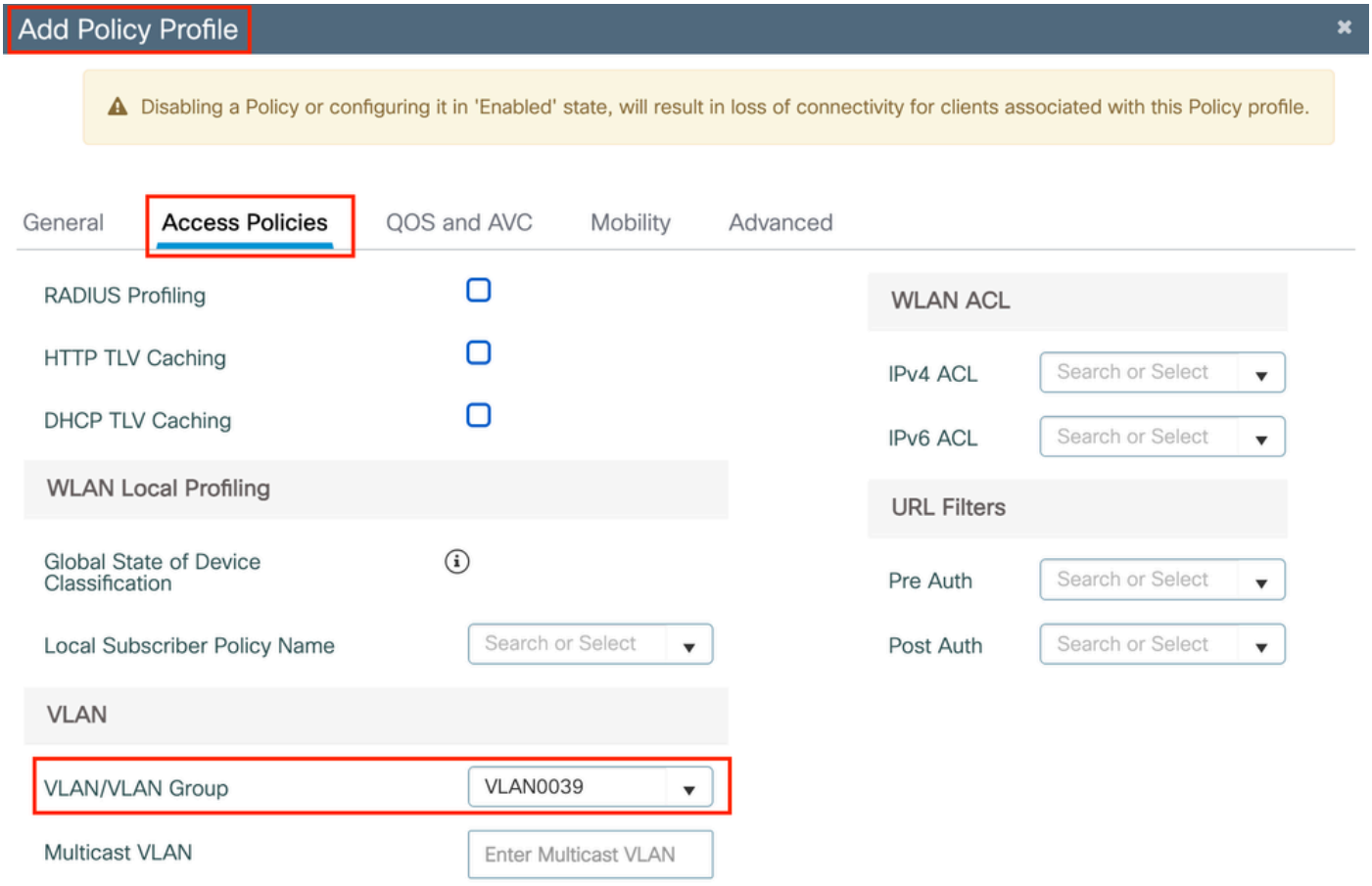
- Activez le filtrage MAC et définissez la liste d’autorisations sur celle créée précédemment
- Sous Auth Key Mgmt enable PSK
- Le champ de clé pré-partagée peut être rempli avec n'importe quelle valeur. Cette opération est effectuée uniquement pour répondre aux exigences de la conception de l'interface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



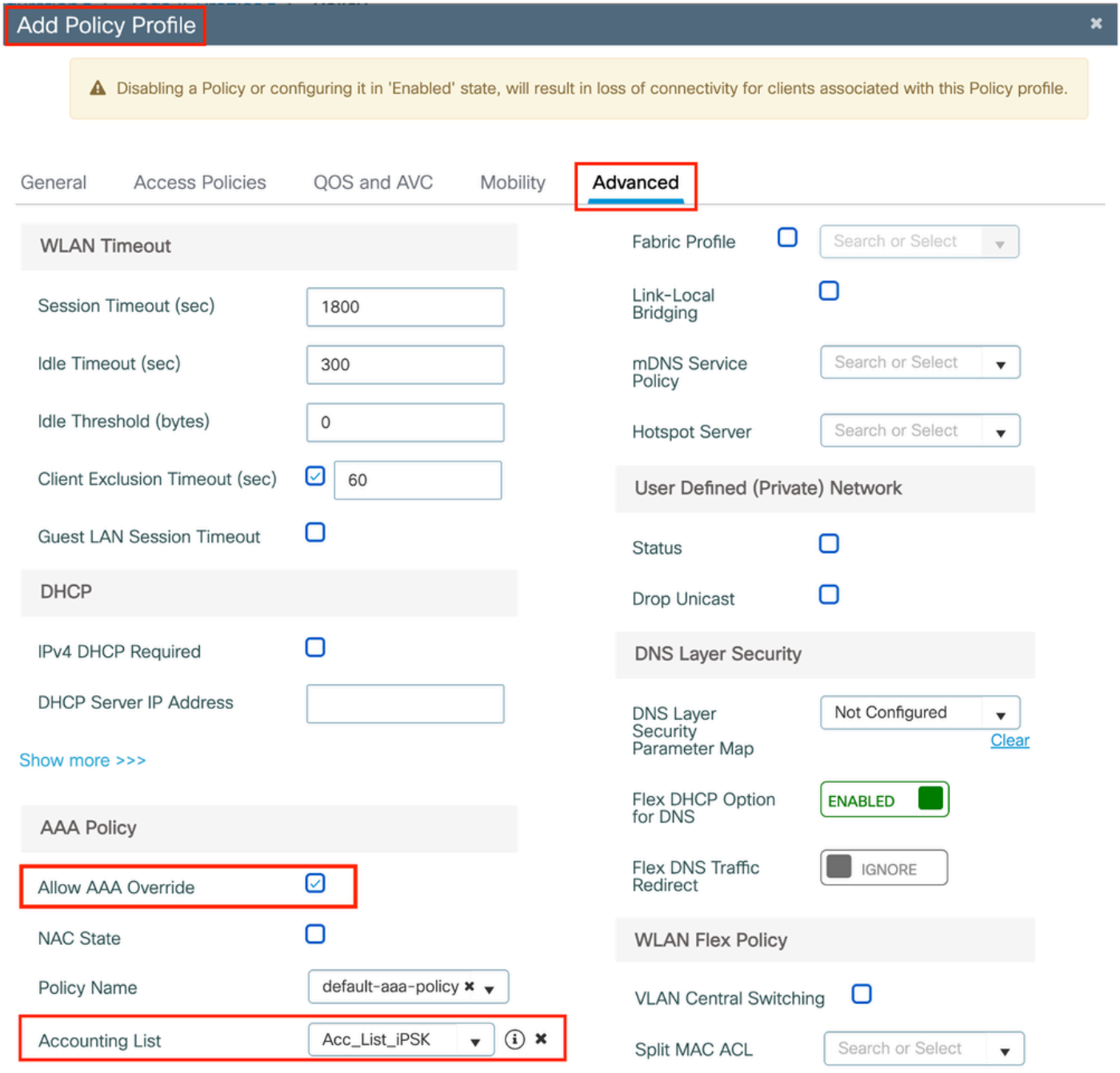
La séparation des utilisateurs peut être réalisée sous l'onglet Avancé. Sa définition sur Allow Private Group permet aux utilisateurs utilisant la même clé prépartagée de communiquer entre eux, tandis que les utilisateurs utilisant une autre clé prépartagée sont bloqués :



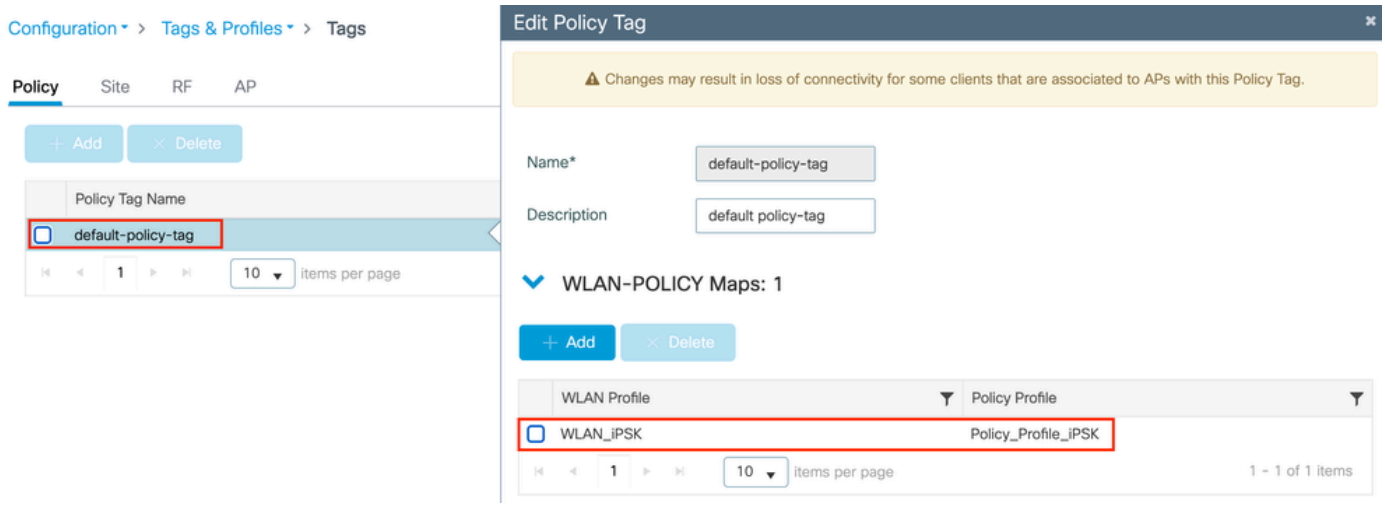
Sous Configuration > Tags & Profiles > Policy, créez un nouveau profil de stratégie. Dans l'onglet Access Policies, définissez le VLAN ou le groupe de VLAN que ce WLAN utilise :



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



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



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

```
wlan

 mac-filtering

 security wpa psk set-key ascii 0

 no security wpa akm dot1x
 security wpa akm psk
 peer-blocking allow-private-group
 no shutdown

wireless profile policy

 aaa-override
 accounting-list

 vlan

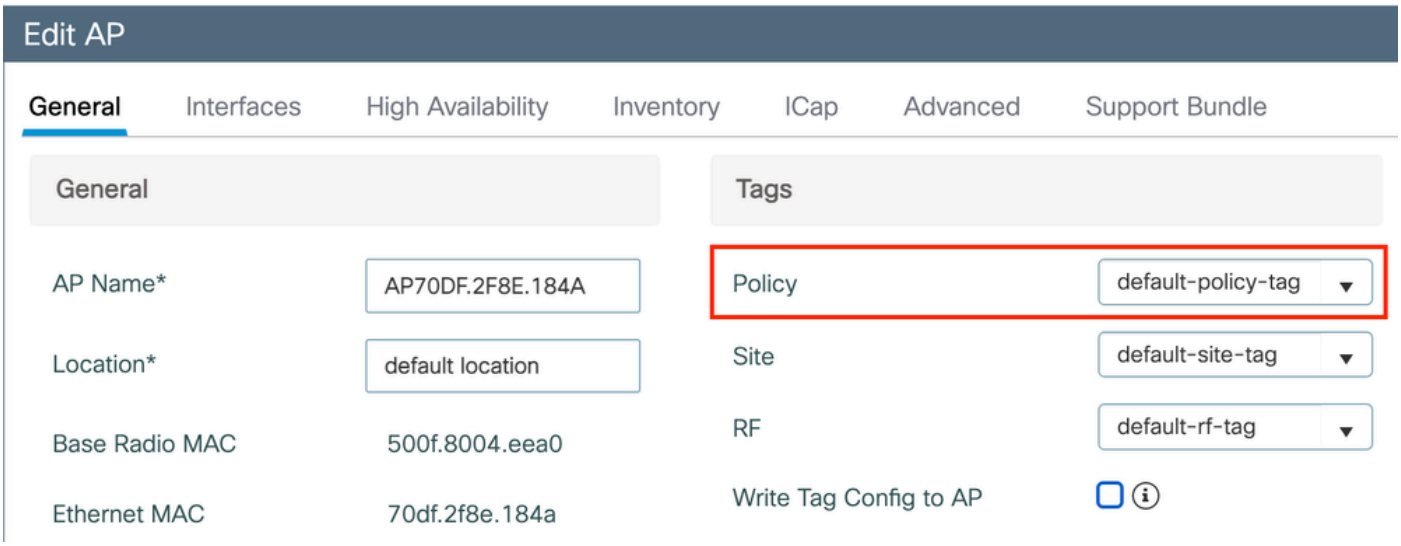
 no shutdown
```

```
wireless tag policy

 wlan

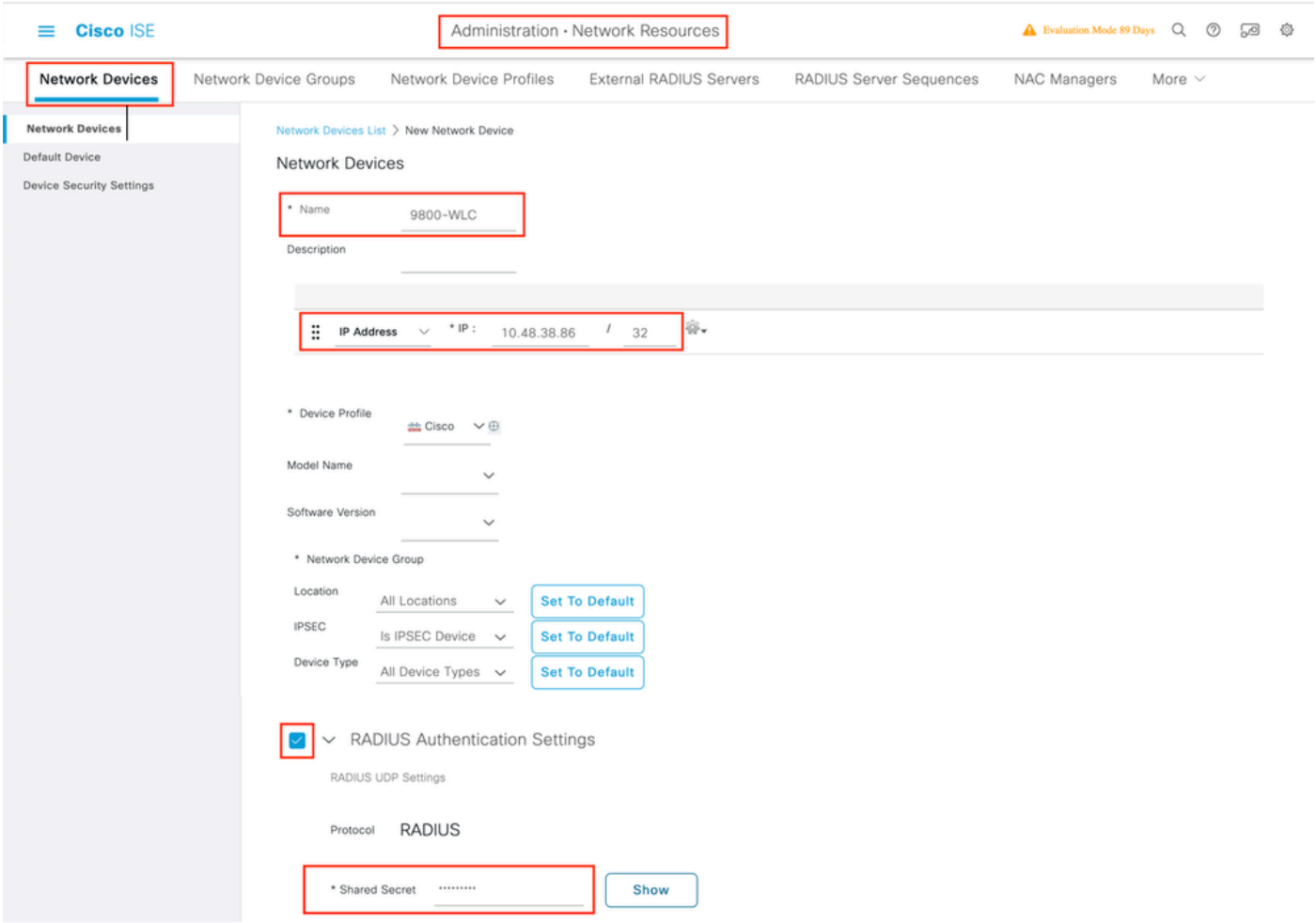
                  policy
```

Sous Configuration > Wireless > Access Points, assurez-vous que cette balise a été appliquée sur les points d'accès sur lesquels le WLAN doit être diffusé :

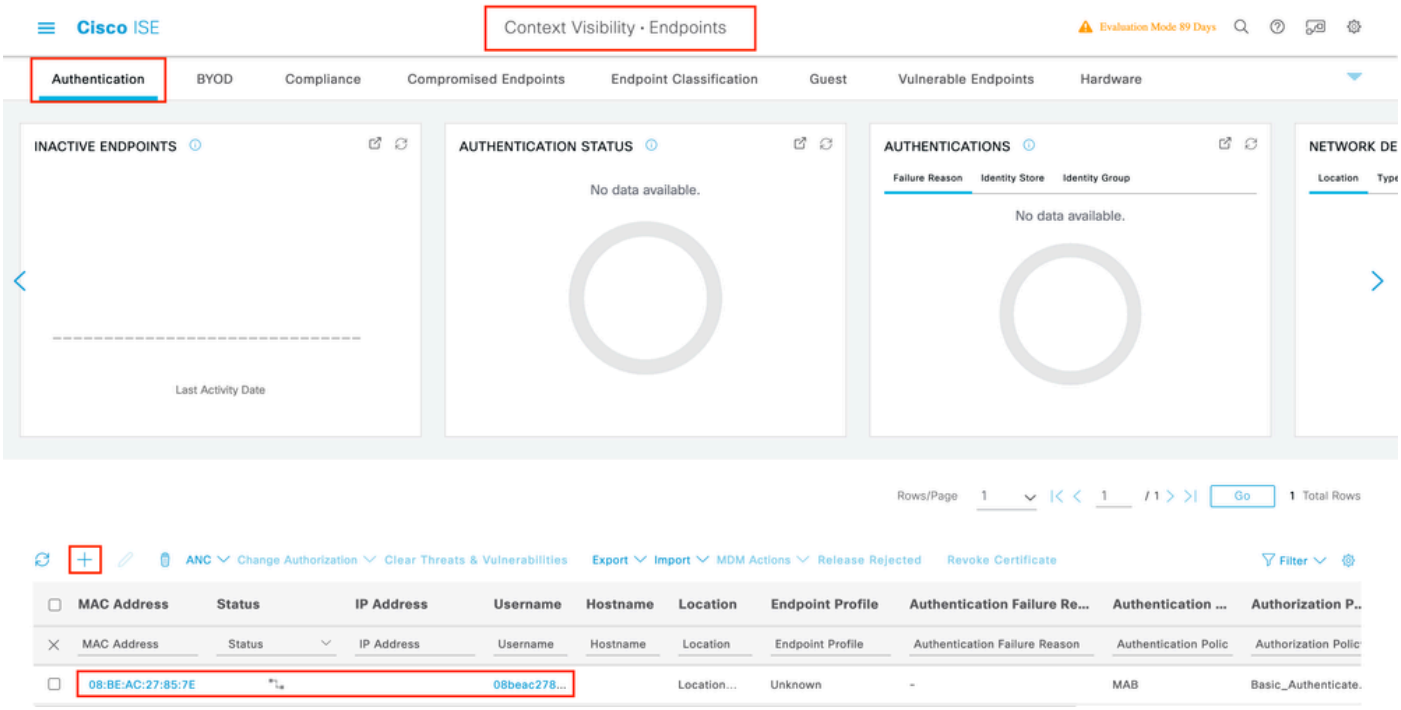


Configuration ISE

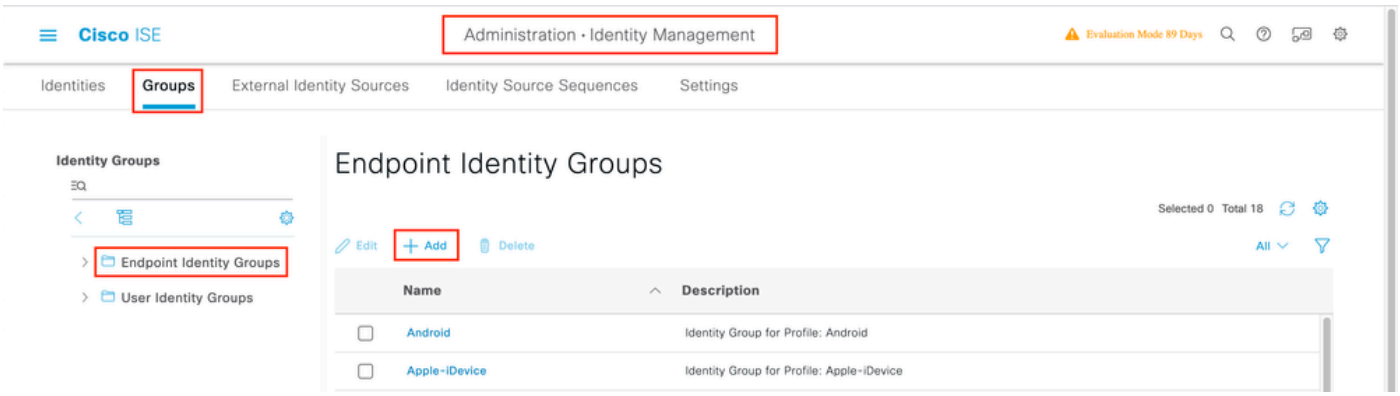
Ce guide de configuration couvre un scénario dans lequel la clé PSK du périphérique est déterminée en fonction de l'adresse MAC du client. Sous Administration > Network Resources > Network Devices, ajoutez un nouveau périphérique, spécifiez l'adresse IP, activez les paramètres d'authentification RADIUS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

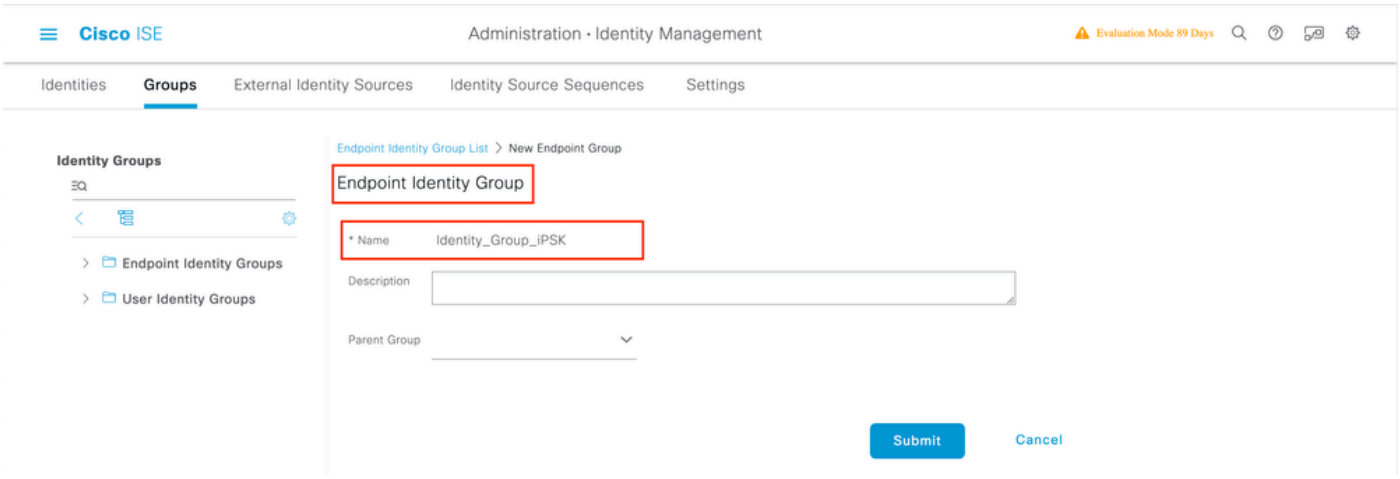


Sous Context Visibility > Endpoints > Authentication, ajoutez les adresses MAC de tous les périphériques (clients) qui se connectent au réseau iPSK :

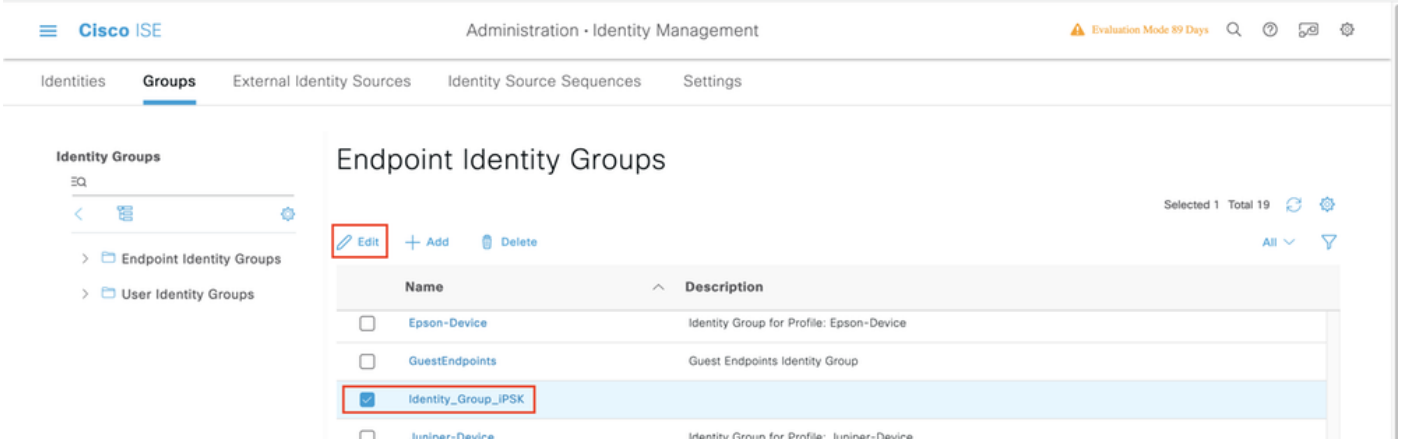


Sous Administration > Identity Management > Groups > Endpoint Identity Groups, créez un ou plusieurs groupes et attribuez-leur des utilisateurs. Chaque groupe peut être configuré ultérieurement pour utiliser une clé prépartagée différente pour se connecter au réseau.

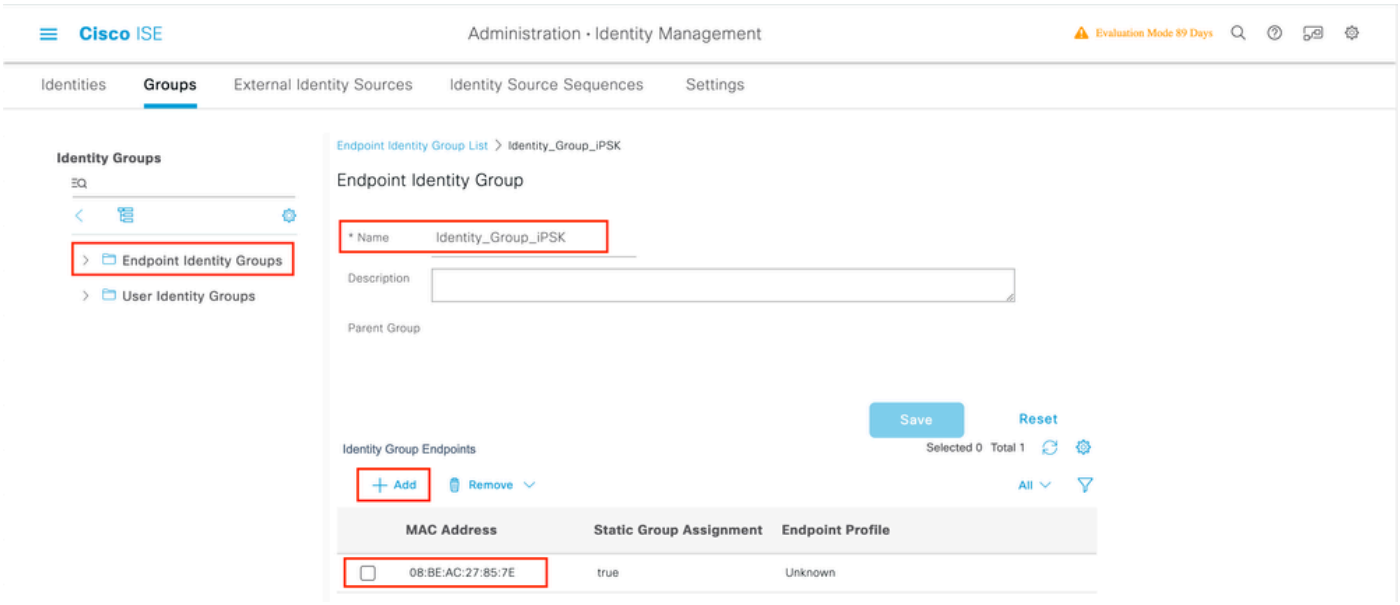




Une fois le groupe créé, vous pouvez lui attribuer des utilisateurs. Sélectionnez le groupe que vous avez créé, puis cliquez sur Edit :



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 » :



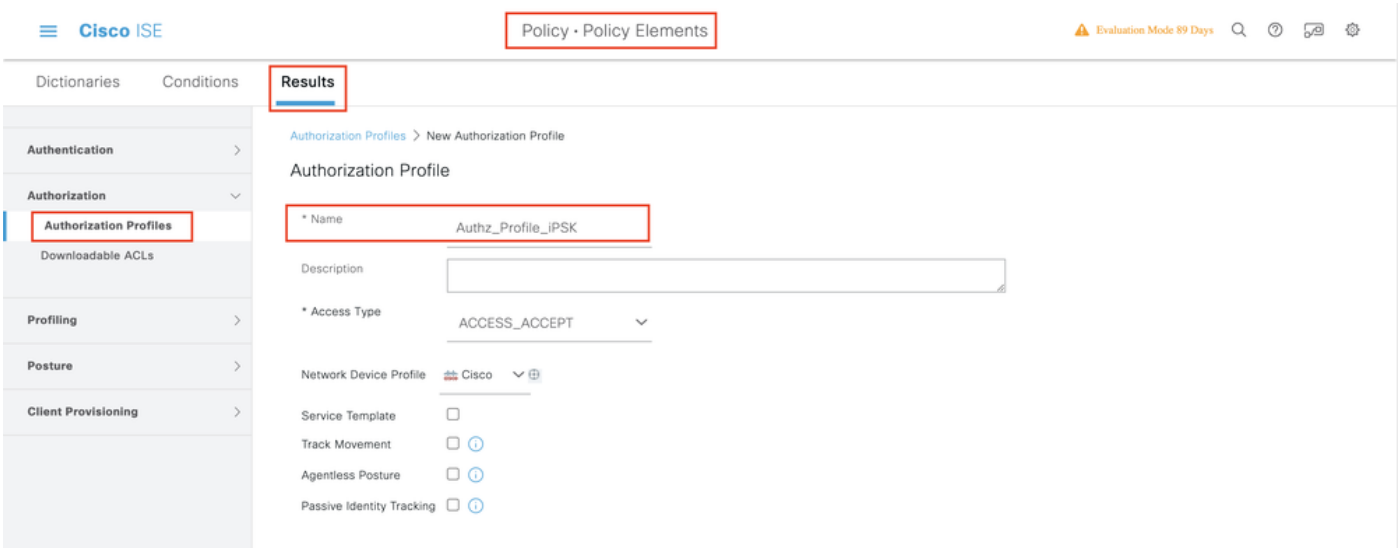
Sous Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation, créez un nouveau profil d'autorisation. Définissez les attributs comme suit :

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

```
// This is the psk that the user group is using
```

Pour chaque groupe d'utilisateurs qui doit 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.



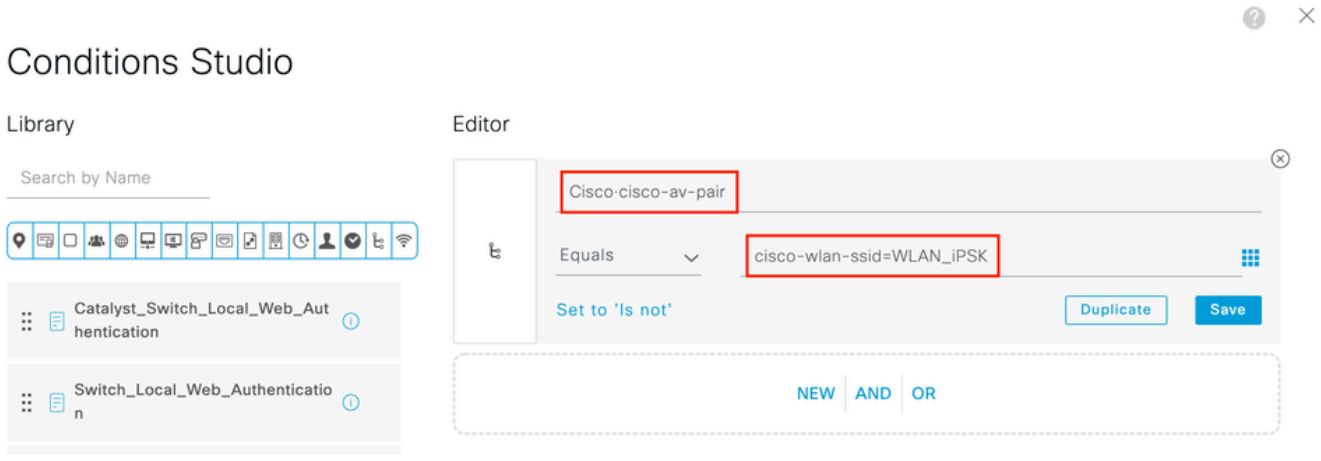
Sous Policy > Policy Sets, créez-en un nouveau. Pour s'assurer que le client correspond au jeu de stratégies, cette condition est utilisée :

<#root>

```
Cisco:cisco-av-pair
```

EQUALS

```
 cisco-wlan-ssid=WLAN_iPSK     // "WLAN_iPSK" is WLAN name
```



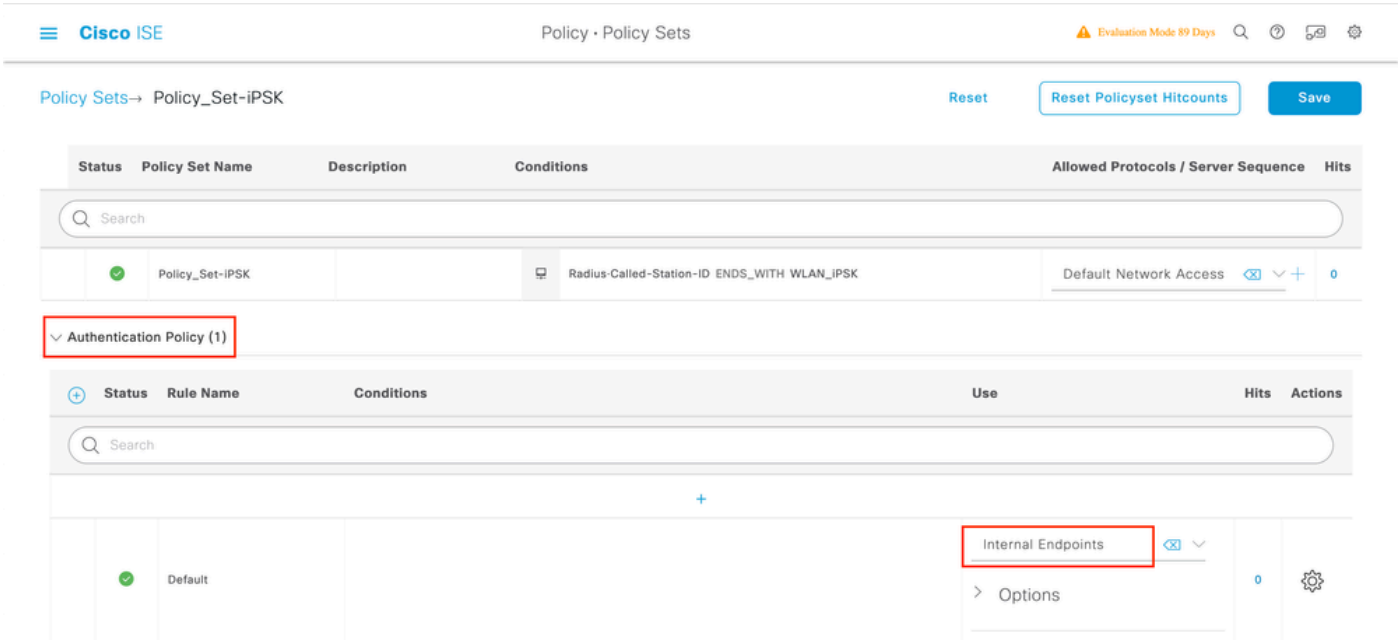
Des conditions supplémentaires peuvent être ajoutées pour sécuriser davantage la mise en correspondance des stratégies.



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 :



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



Sous Stratégie d'autorisation, créez une nouvelle règle pour chacun des groupes d'utilisateurs. À titre de condition, utilisez :

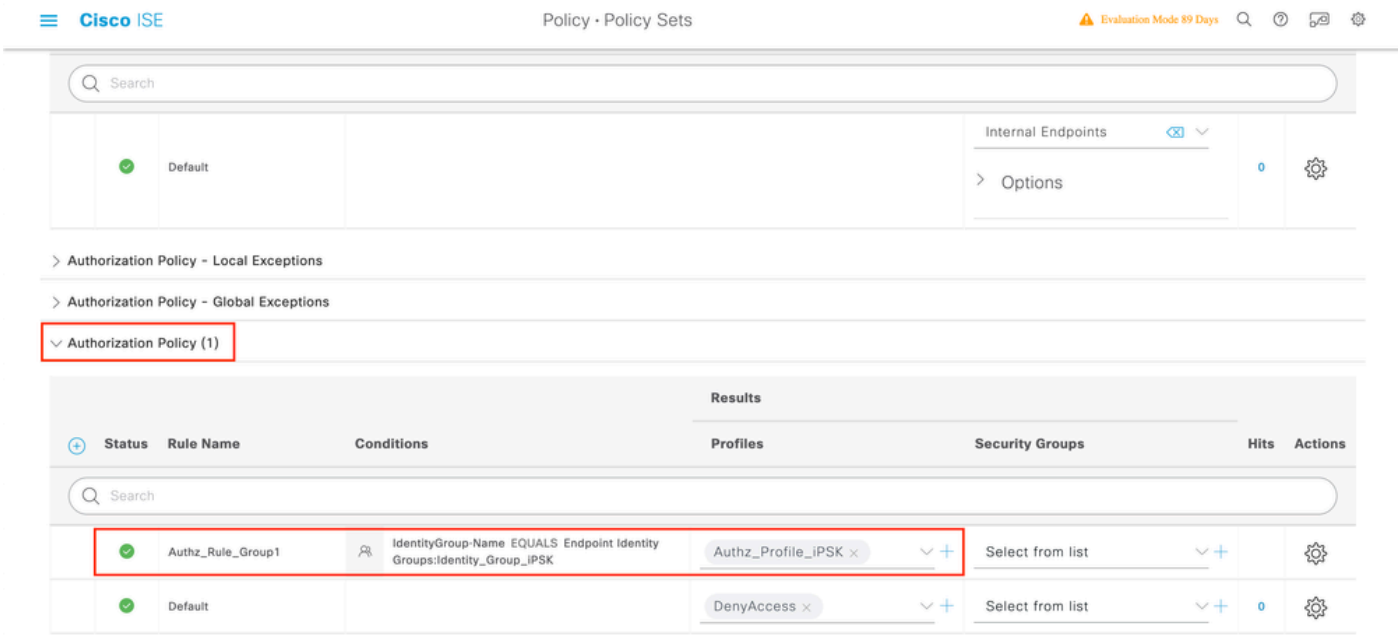
<#root>

```
IdentityGroup-Name
```

EQUALS

```
 Endpoint Identity Group:Identity_Group_iPSK      // "Identity_Group_iPSK" is name of the created endpo
```

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



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 :

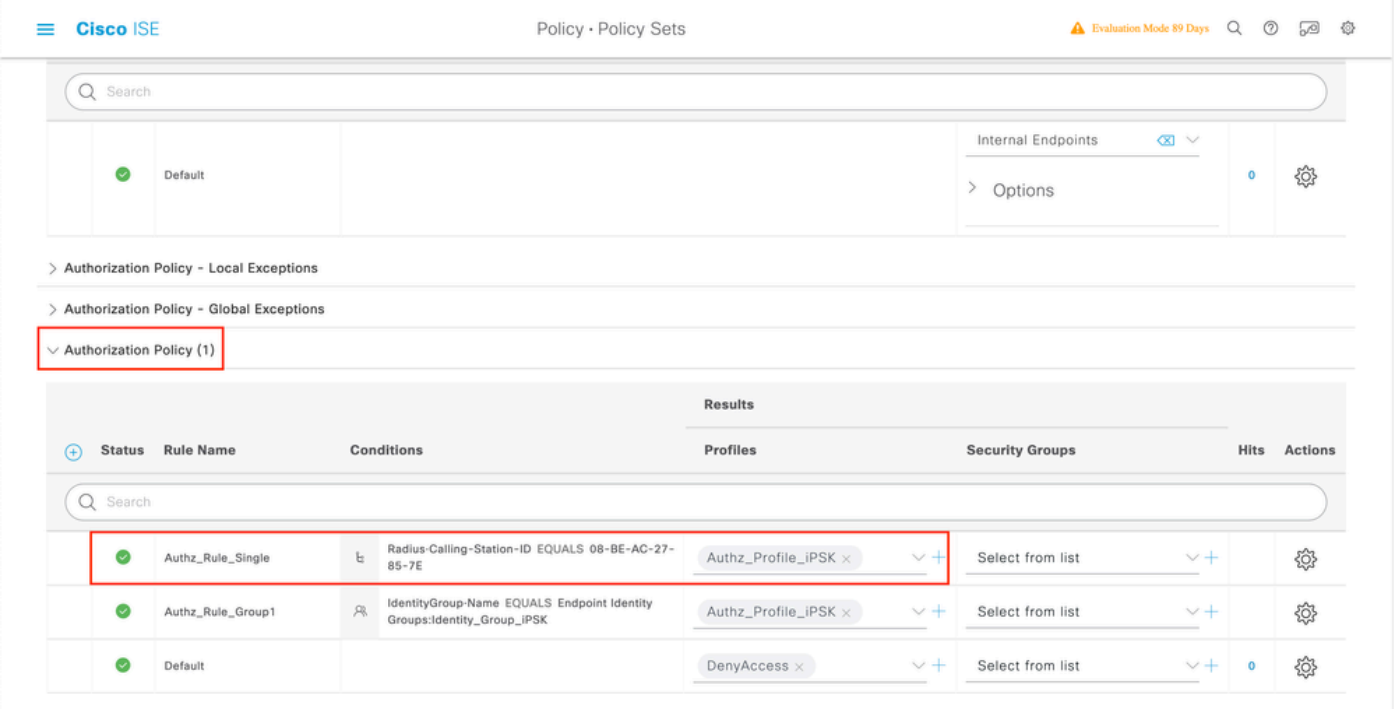
<#root>

```
Radius-Calling-Station-ID
```

EQUALS

```
 <client_mac_addr>
```

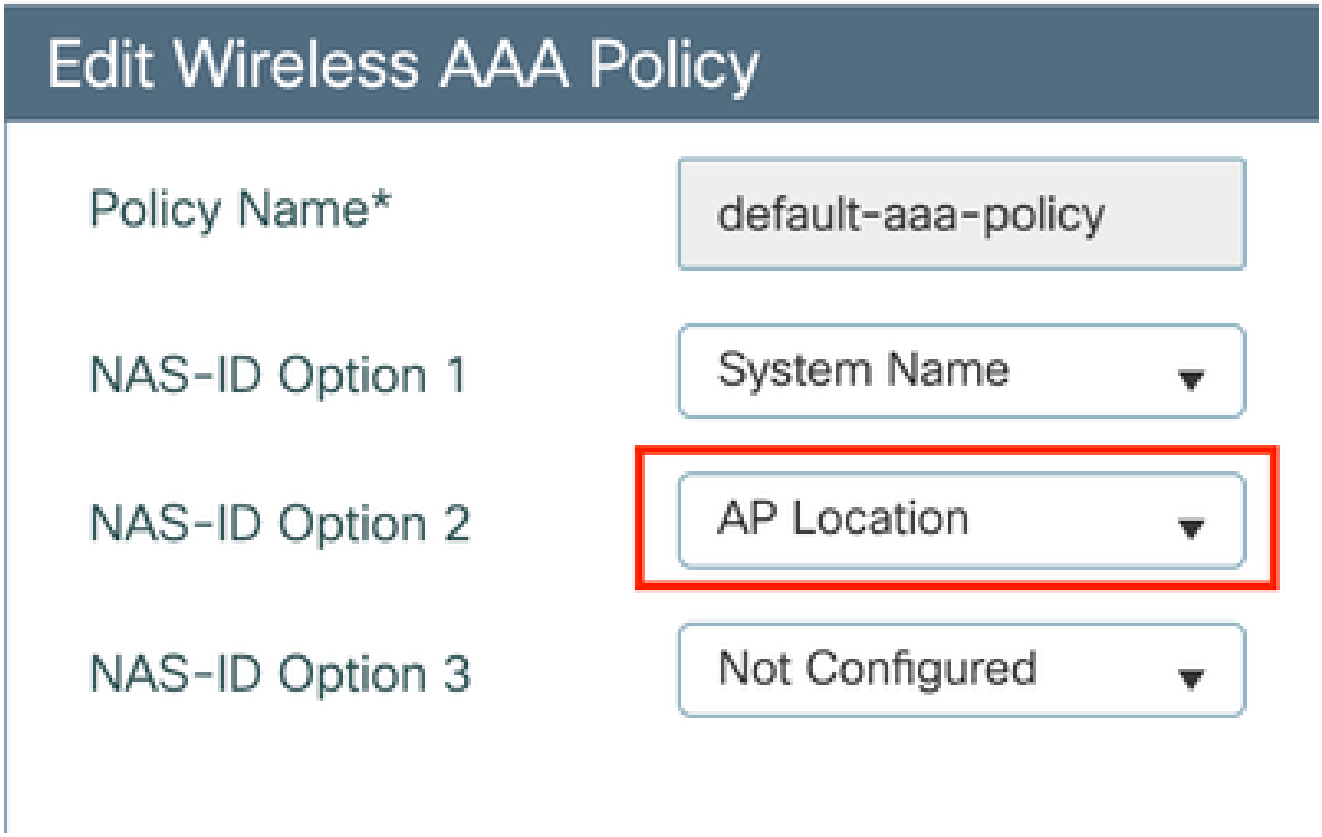
Remarque : Le délimiteur d'adresse MAC peut être configuré sur le WLC sous AAA > AAA Advanced > Global Config > Advanced Settings. Dans cet exemple, le caractère "-" a été utilisé.



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 :



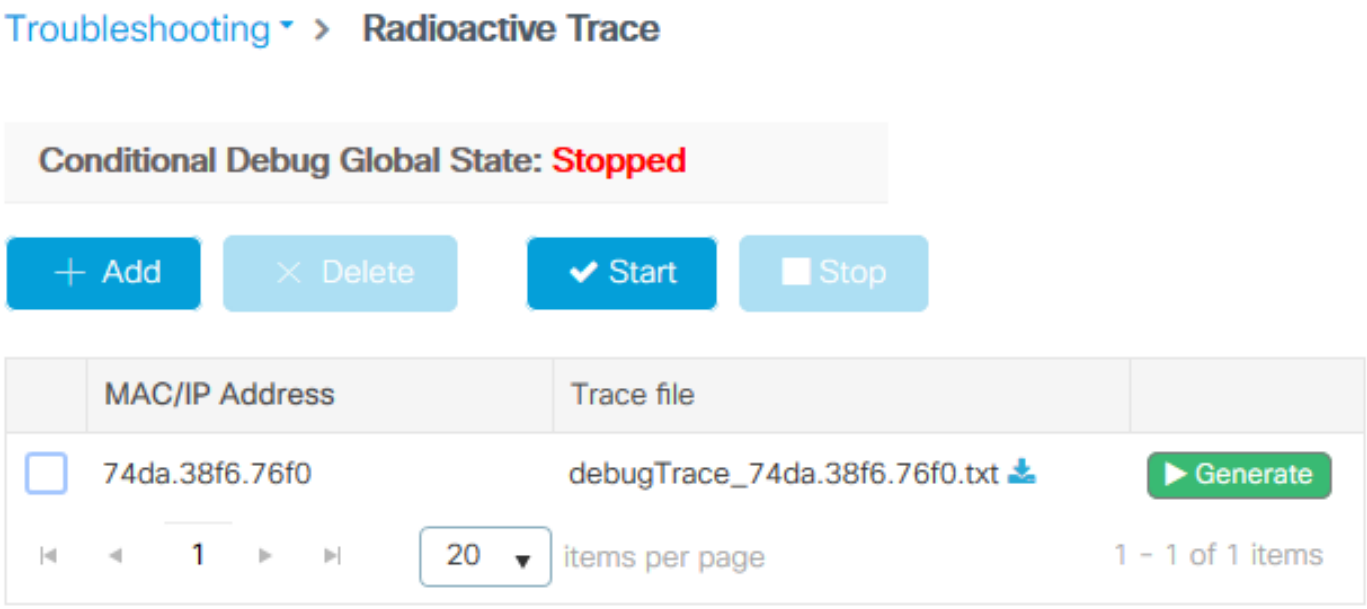
2. Correspondance basée sur le profilage du périphérique
   Dans ce scénario, le WLC doit être configuré pour profiler les périphériques globalement. Cela permet à un administrateur de configurer un mot de passe différent pour les ordinateurs portables et les périphériques téléphoniques. La classification 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 ACL ou VLAN id.

Dépannage

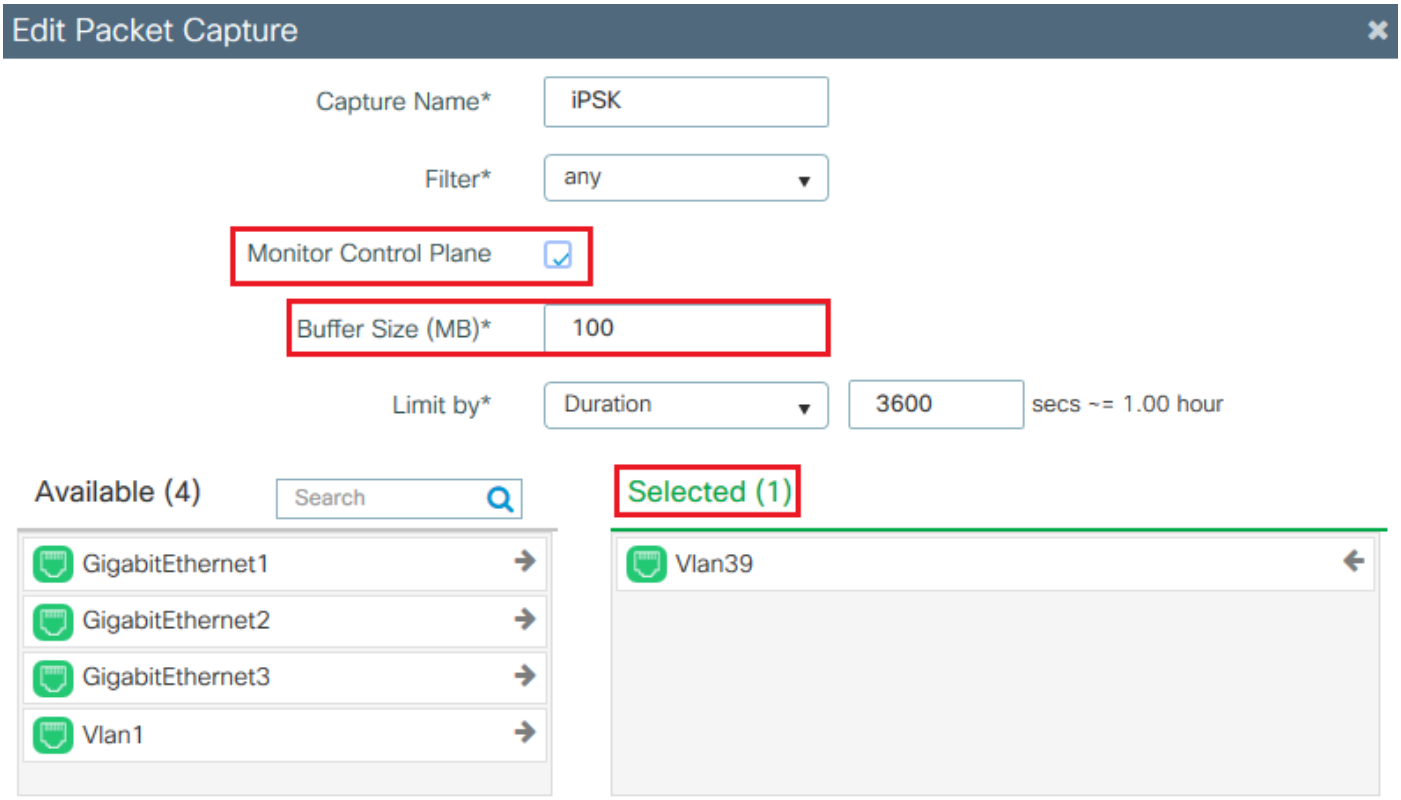
Dépannage du WLC 9800

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 Générer pour créer le fichier et le télécharger :



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 :

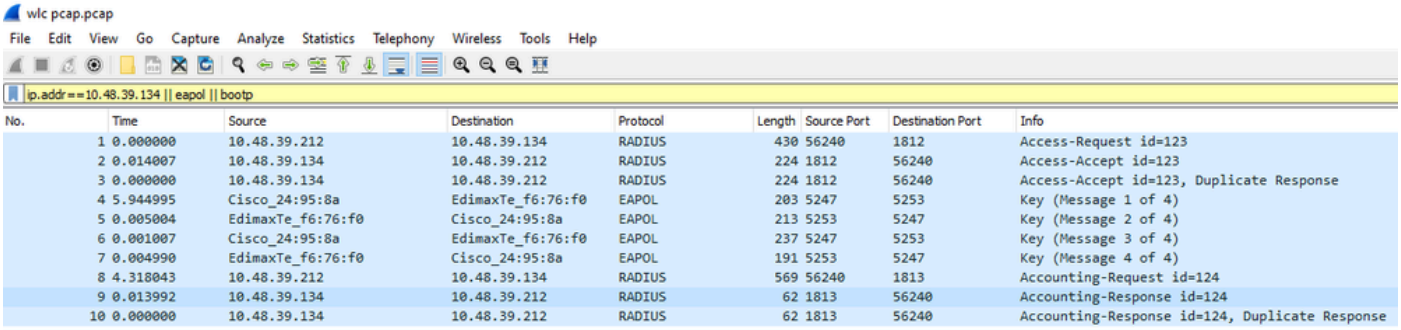


La capture de paquets d'une tentative d'authentification et de gestion des comptes réussie est

illustrée dans l'image ci-dessous. Utilisez ce filtre Wireshark pour filtrer tous les paquets appropriés pour ce client :

```
ip.addr==

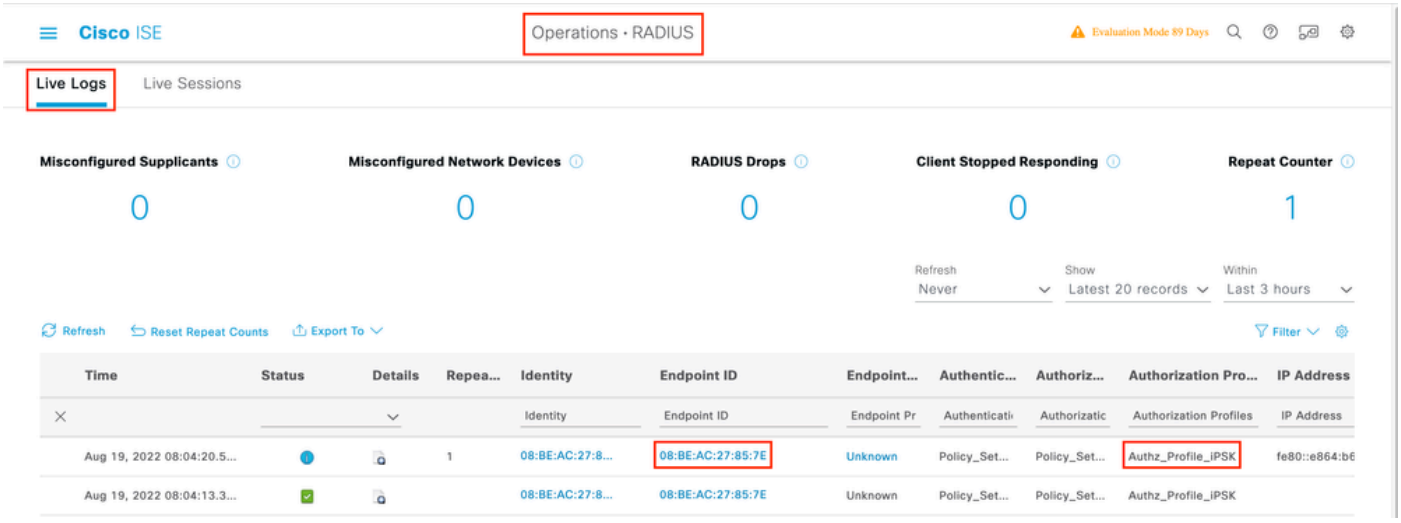
        || eapol || bootp
```



No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.48.39.212	10.48.39.134	RADIUS	430	56240	1812	Access-Request id=123
2	0.014007	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123
3	0.000000	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123, Duplicate Response
4	5.944995	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	203	5247	5253	Key (Message 1 of 4)
5	0.005004	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	213	5253	5247	Key (Message 2 of 4)
6	0.001007	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	237	5247	5253	Key (Message 3 of 4)
7	0.004990	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	191	5253	5247	Key (Message 4 of 4)
8	4.318043	10.48.39.212	10.48.39.134	RADIUS	569	56240	1813	Accounting-Request id=124
9	0.013992	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124
10	0.000000	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124, Duplicate Response

Dépannage d'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 :



Références

[8.5 Guide de déploiement des fonctionnalités Identity PSK]

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.