# Configurer les SSID d’authentification MAC sur les contrôleurs sans fil Catalyst 9800

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configuration WLC
    - Configuration AAA sur les WLC 9800
    - Remarque sur la détection des serveurs morts AAA
    - Configuration du profil WLAN
    - Configuration du profil des politiques
    - Configuration des balises des politiques
    - Attribution de balise de stratégie
  - Configuration ISE
    - Déclarer le WLC sur ISE
    - Créer un nouvel utilisateur sur ISE
    - Créer un profil d’autorisation
    - Créer un ensemble de stratégies
    - Créer une stratégie d'authentification
    - Créer une stratégie d'autorisation
- Vérifier
- Dépannage
  - Dépannage sur le WLC
    - Débogage conditionnel et traçage Radio Active
  - Dépannage sur ISE


## Introduction

Ce document décrit comment configurer un WLAN avec la sécurité 802.1X sur un contrôleur sans fil de la gamme Cisco Catalyst 9800.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 802.1X

### Composants utilisés

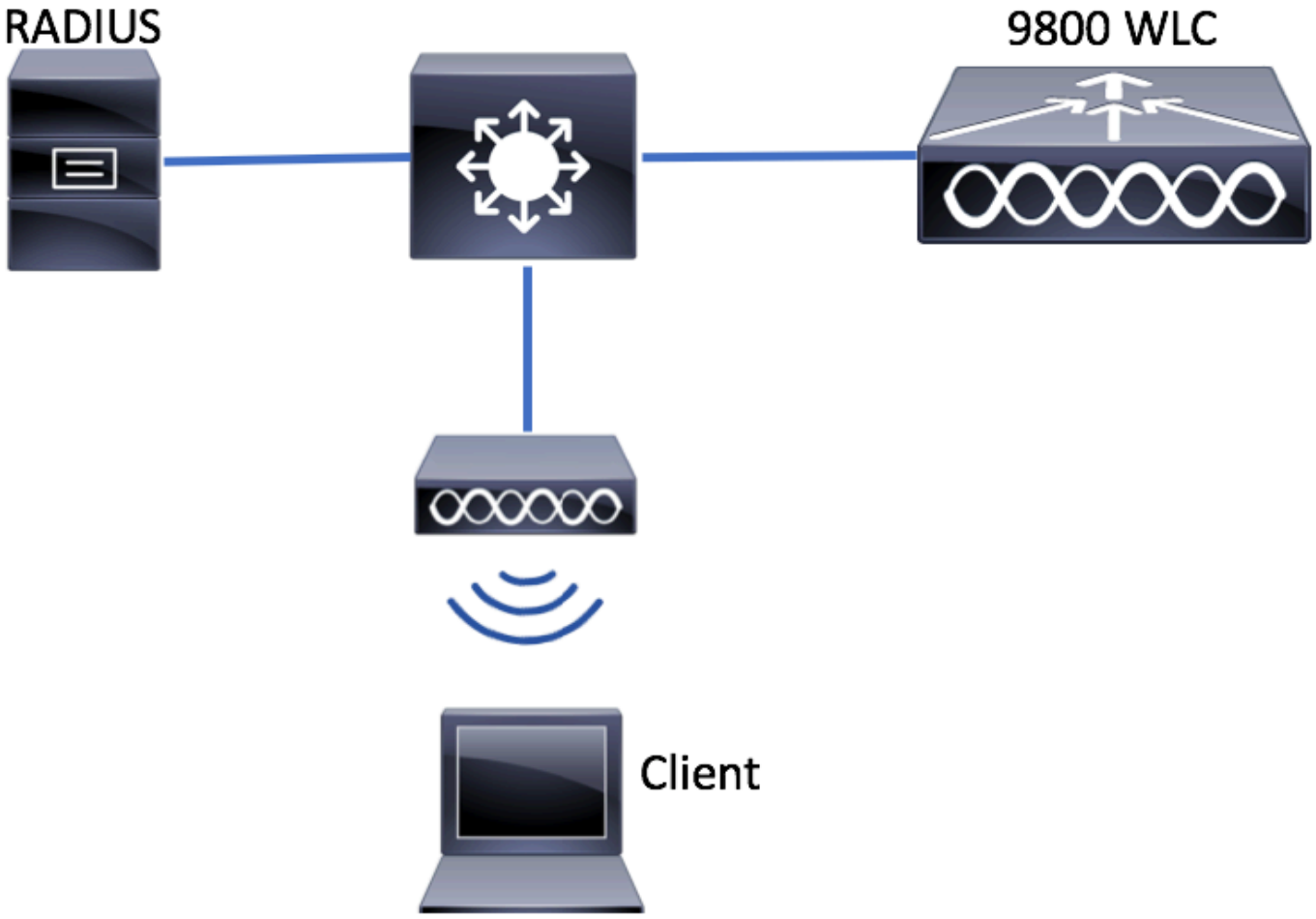
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme de contrôleurs sans fil Catalyst 9800 (Catalyst 9800-CL)
- Cisco IOS® XE 17.12.5
- 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.

## Configurer

### Diagramme du réseau

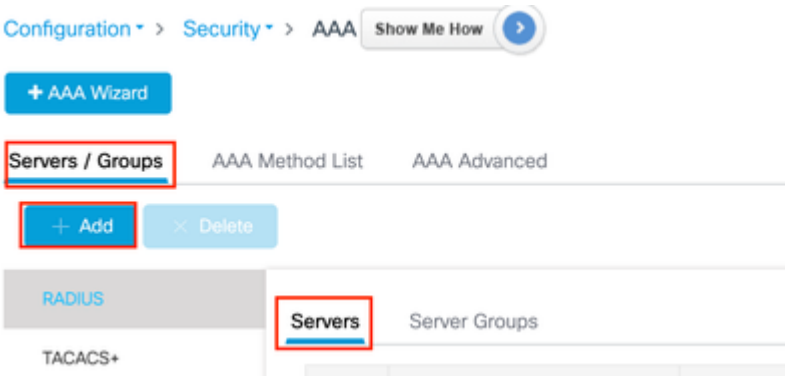



## Configuration WLC

### Configuration AAA sur les WLC 9800

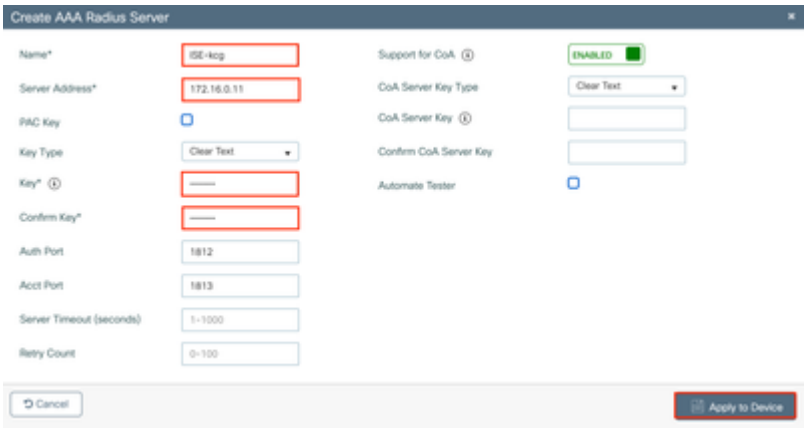
IUG:

Étape 1 : déclaration du serveur RADIUS Naviguez jusqu' **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add**au serveur RADIUS et saisissez-le.

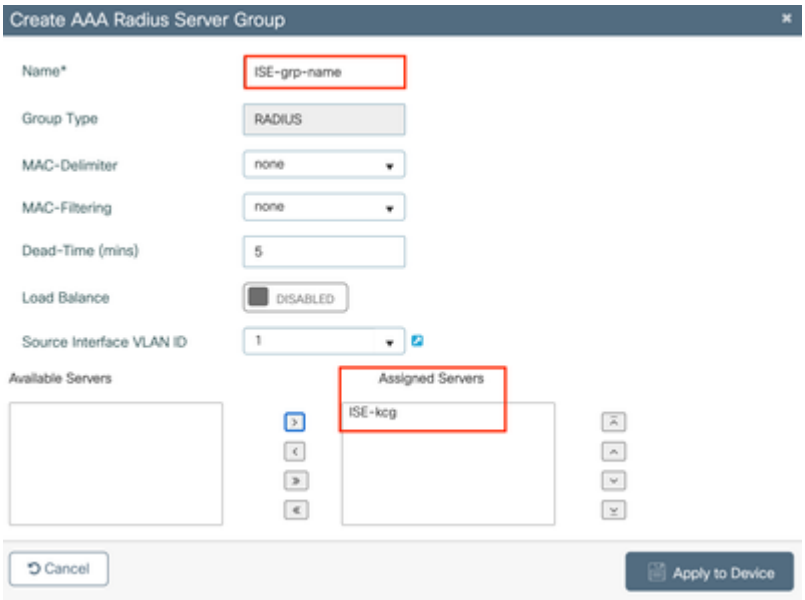



Assurez-vous que la prise en charge de CoA est activée et configurez la clé de serveur CoA si vous prévoyez d'utiliser l'authentification Web centrale (ou tout type de sécurité nécessitant un changement d'autorisation [CoA]) à l'avenir.

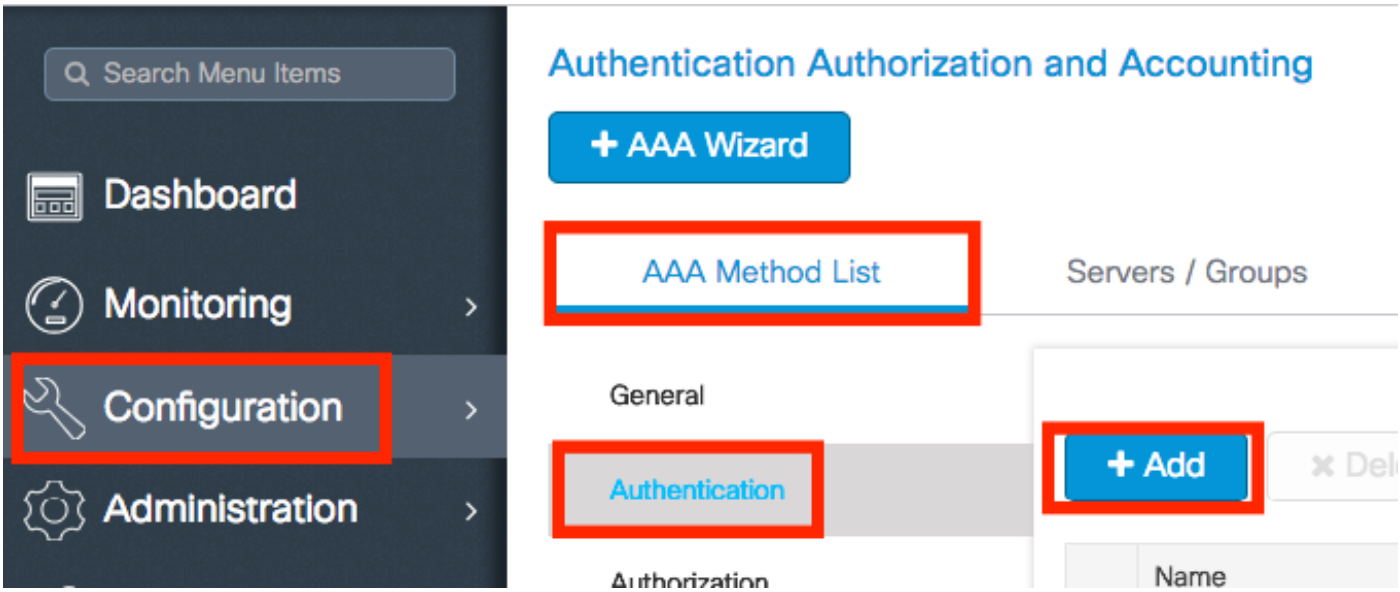
Remarque : La clé de serveur de changement d'autorisation (CoA) sur le WLC Cisco 9800 est un secret partagé utilisé pour authentifier les requêtes CoA entre le WLC et le serveur RADIUS. Cette clé doit correspondre à la configuration CoA sur le serveur RADIUS pour garantir une communication réussie. Assurez-vous que la clé du serveur CoA est configurée de manière sécurisée et cohérente sur tous les périphériques pour empêcher le rejet des messages CoA.



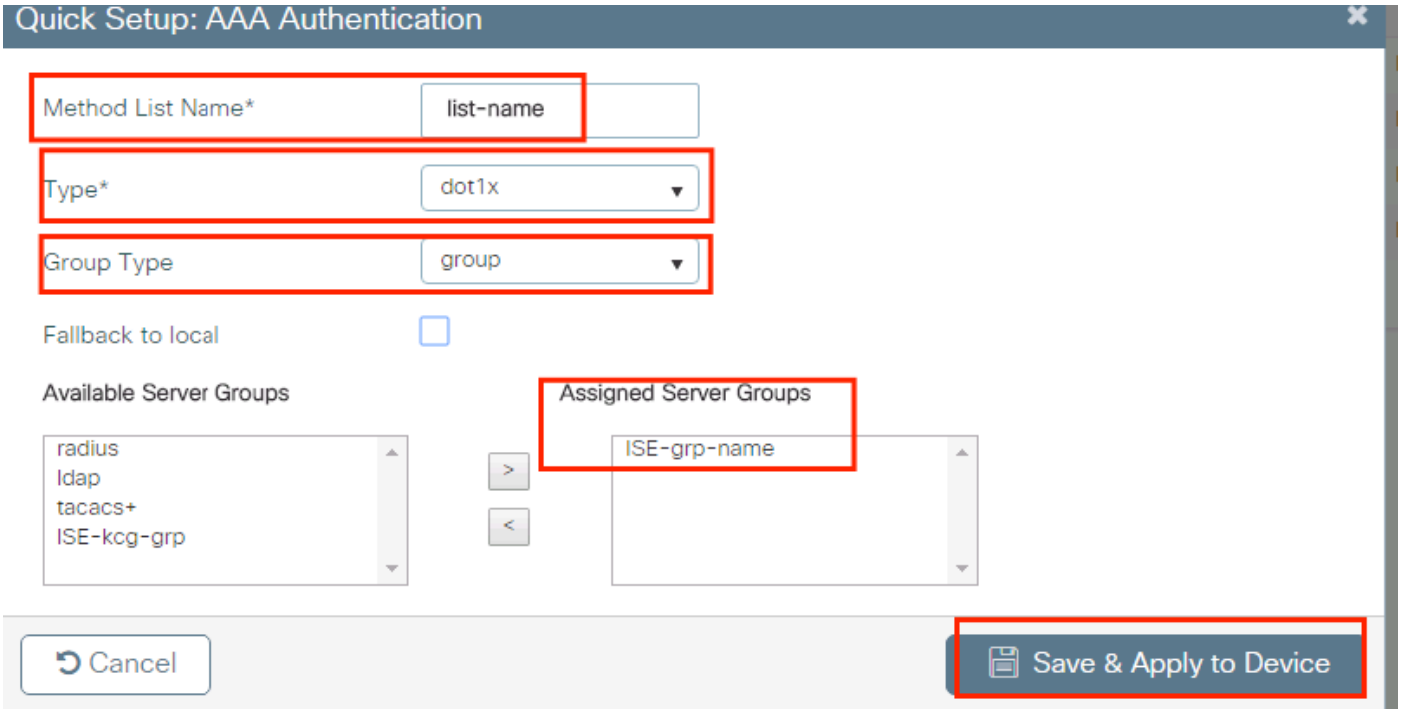

Étape 2 : ajout du serveur RADIUS à un groupe RADIUS Accédez à **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.** Attribuer un nom à votre groupe et déplacez le serveur que vous avez créé précédemment dans la liste des **Assigned Servers**.




Étape 3 : création d'une liste de méthodes d'authentification Naviguez jusqu'à **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.




Entrez l'information:




CLI :

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Remarque sur la détection de serveur mort AAA

Après avoir configuré votre serveur RADIUS, vous pouvez vérifier s'il est considéré comme ALIVE :

```
#show aaa servers | s WNCD
     Platform State from WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
```

```
Platform State from WNCD (3) : current UP
Platform State from WNCD (4) : current UP
...
```

Vous pouvez configurer le **dead criteria**, ainsi que le **deadtime** sur votre WLC, en particulier si vous utilisez plusieurs serveurs RADIUS.

```
#radius-server dead-criteria time 5 tries 3
#radius-server deadtime 5
```

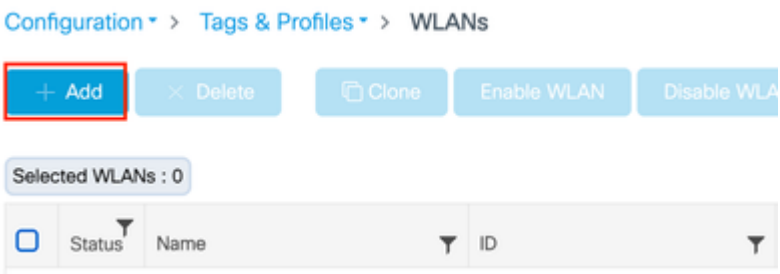
Remarque : Le **dead criteria** est le critère utilisé pour marquer un serveur RADIUS comme étant mort. Il se compose des éléments suivants : 1. Un délai d'attente (en secondes) qui représente le temps qui doit s'écouler entre le moment où le contrôleur a reçu pour la dernière fois un paquet valide du serveur RADIUS et le moment où le serveur est marqué comme étant mort. 2. Un compteur, qui représente le nombre de délais d'attente consécutifs qui doivent se produire sur le contrôleur avant que le serveur RADIUS soit marqué comme étant mort.

Remarque : La **deadtime** spécifie la durée (en minutes) pendant laquelle le serveur reste à l'état Dead après que les critères Dead l'aient marqué comme étant Dead. Une fois le délai d'attente expiré, le contrôleur marque le serveur comme étant UP (ALIVE) et informe les clients enregistrés du changement d'état. Si le serveur est toujours inaccessible après que l'état a été marqué comme UP et si les critères Dead sont satisfaits, le serveur est marqué de nouveau comme Dead pour l'intervalle de temps d'arrêt.

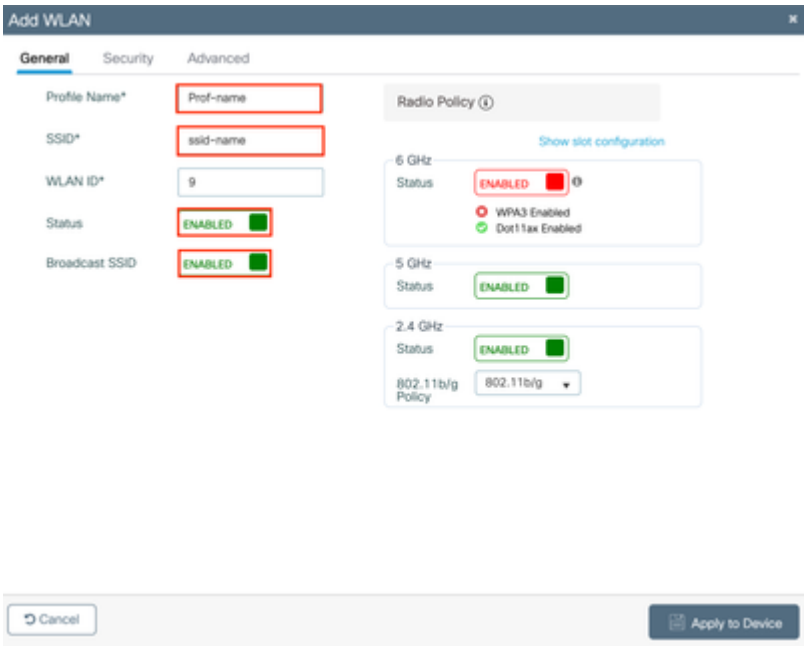
Configuration du profil WLAN

IUG:

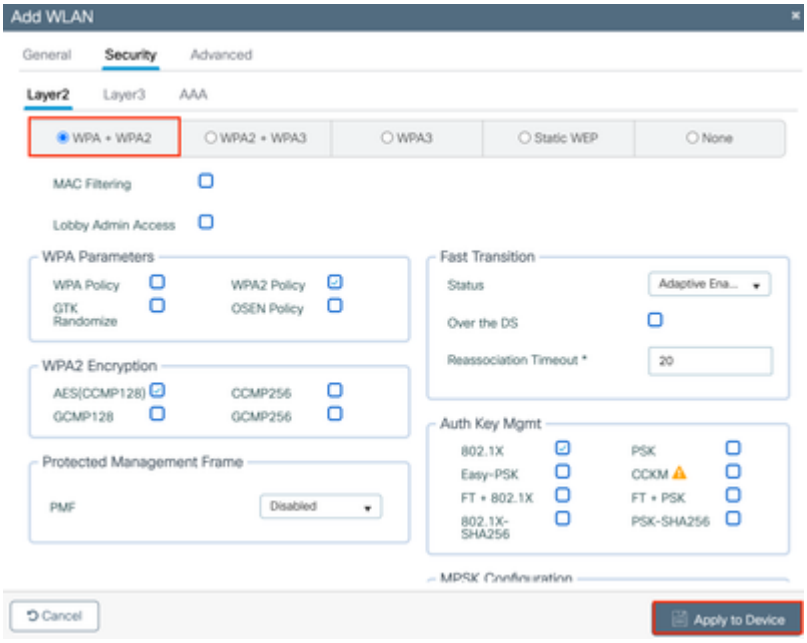
Étape 1 : création du WLAN Accédez à Configuration > Tags&Profiles > WLANs > + Add et configurez le réseau selon les besoins.



Étape 2. Entrez les informations WLAN :

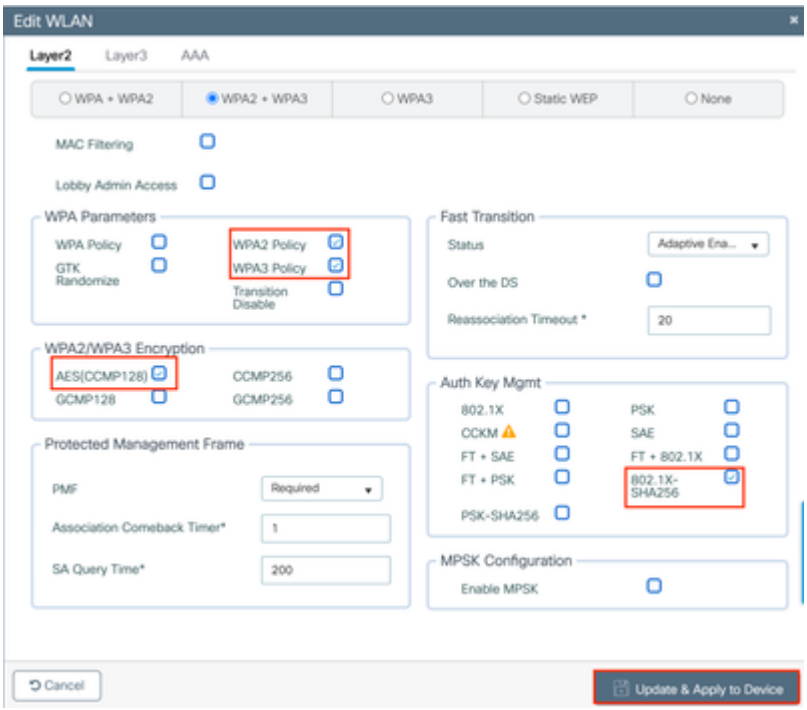



Étape 3a. Allez à l'onglet Security (sécurité) et sélectionnez la méthode de sécurité requise. Dans ce cas, WPA2 + 802.1x.

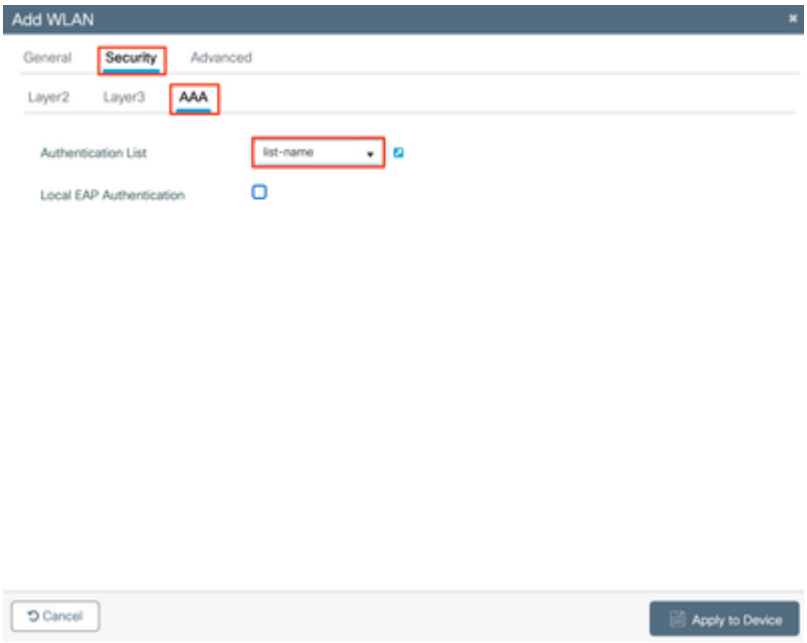


3b. Exemple de mode mixte WPA2+WPA3 :

Remarque : Le mode mixte WPA2+WPA3 sur le WLC Cisco 9800 permet une coexistence transparente des périphériques WPA3 modernes et des périphériques WPA2 existants, assurant à la fois la compatibilité et une sécurité améliorée lorsque cela est possible. Fast Transition (FT) est optionnel dans ce scénario, il devient obligatoire quand AKM FT+802.1x est activé.




Étape 4. Dans l'**Security** > **AAA** onglet, sélectionnez la méthode d'authentification créée à l'étape 3 dans la section AAA Configuration on 9800 WLC.




CLI :

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

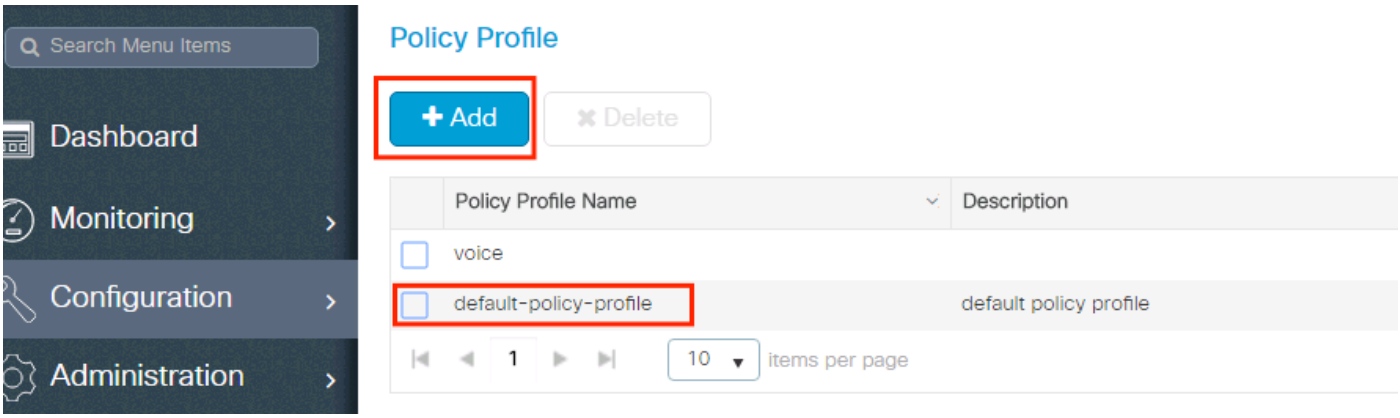
Configuration du profil des politiques

Dans un profil de stratégie, vous pouvez décider à quel VLAN attribuer les clients, entre autres paramètres (comme la liste de contrôle d'accès [ACL], la qualité de service [QoS], l'ancrage de mobilité, les minuteurs, etc.).

Vous pouvez utiliser votre profil de stratégie par défaut ou en créer un nouveau.

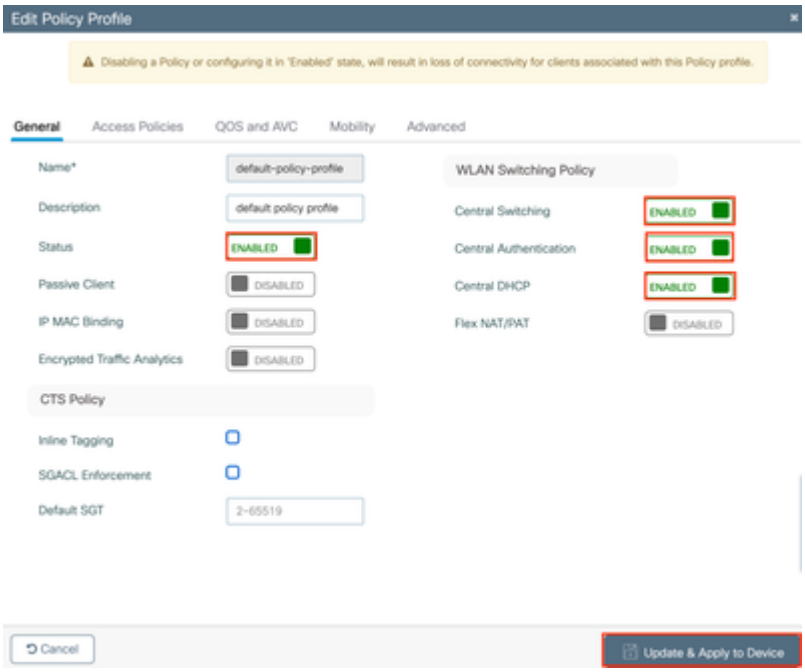
IUG:

Accédez à Configuration > Tags & Profiles > Policy Profile et configurez votre default-policy-profile ou créez-en un nouveau.

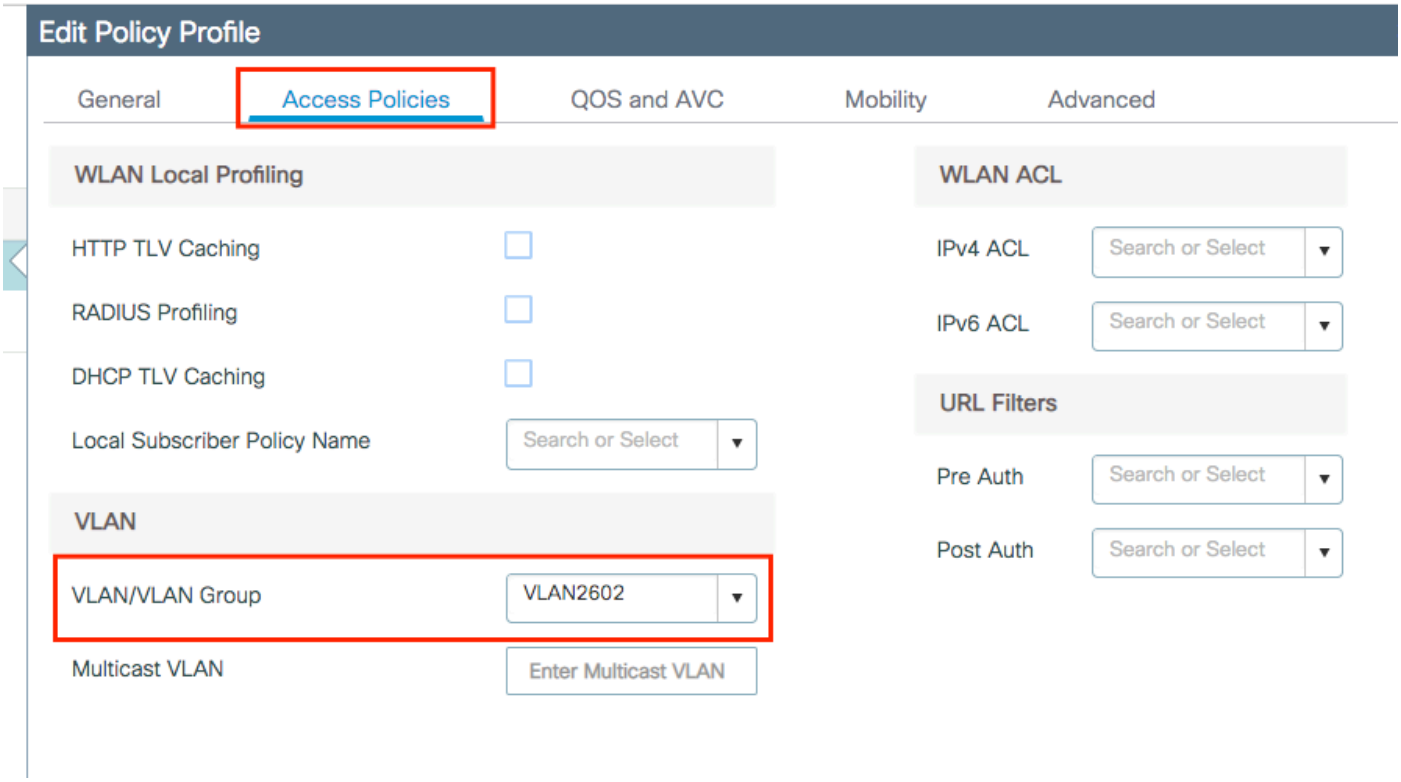



Assurez-vous que le profil est activé.

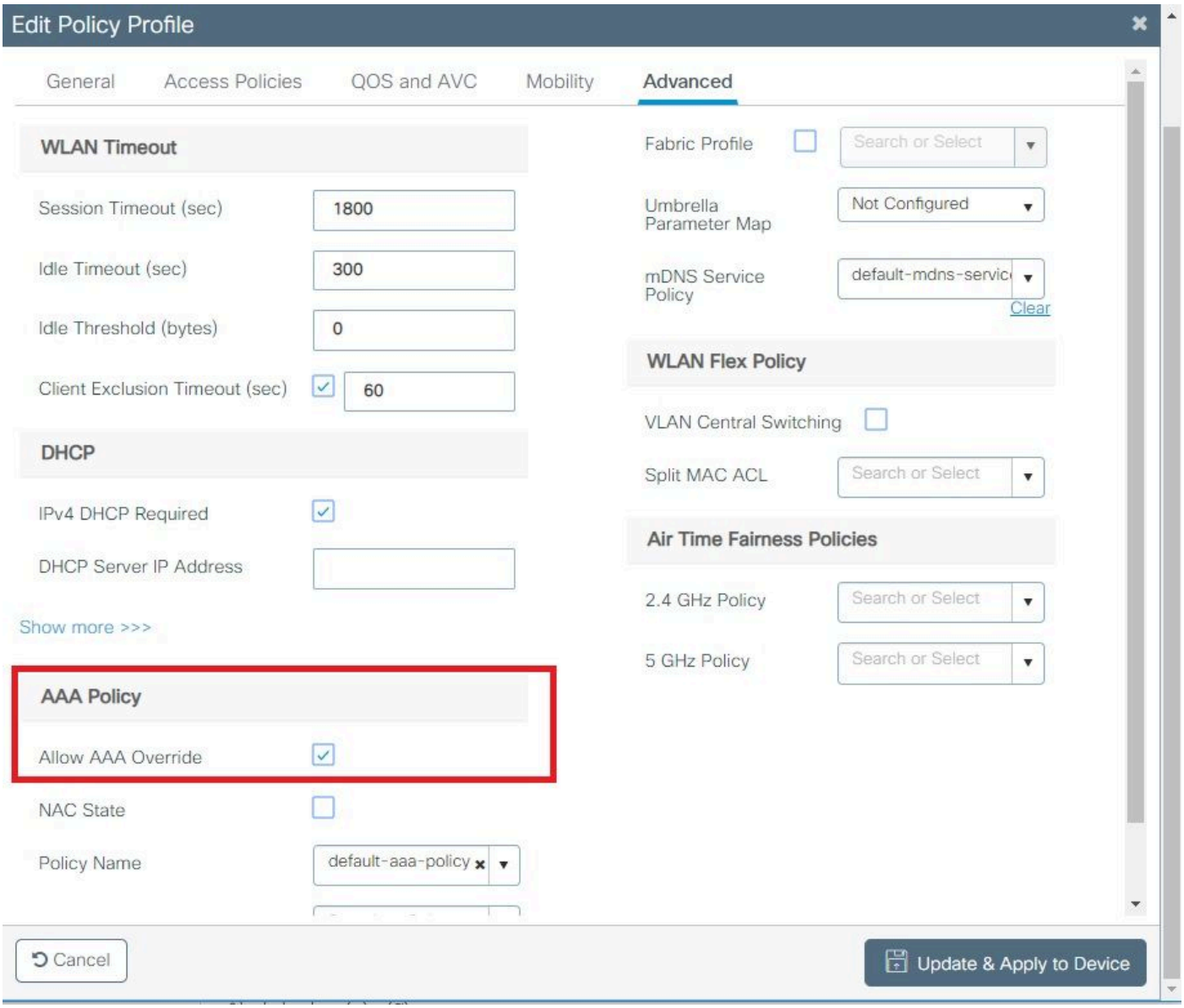
En outre, si votre point d'accès est en mode local, assurez-vous que la commutation centrale, l'authentification centrale et le DHCP central sont activés sur le profil de stratégie.




Sélectionnez le VLAN auquel les clients doivent être affectés dans l'onglet Access Policies.




Si vous prévoyez d'avoir des attributs de retour ISE dans l'Access-Accept comme l'attribution de VLAN, veuillez activer le remplacement AAA dans l'**Advanced**onglet :




CLI :

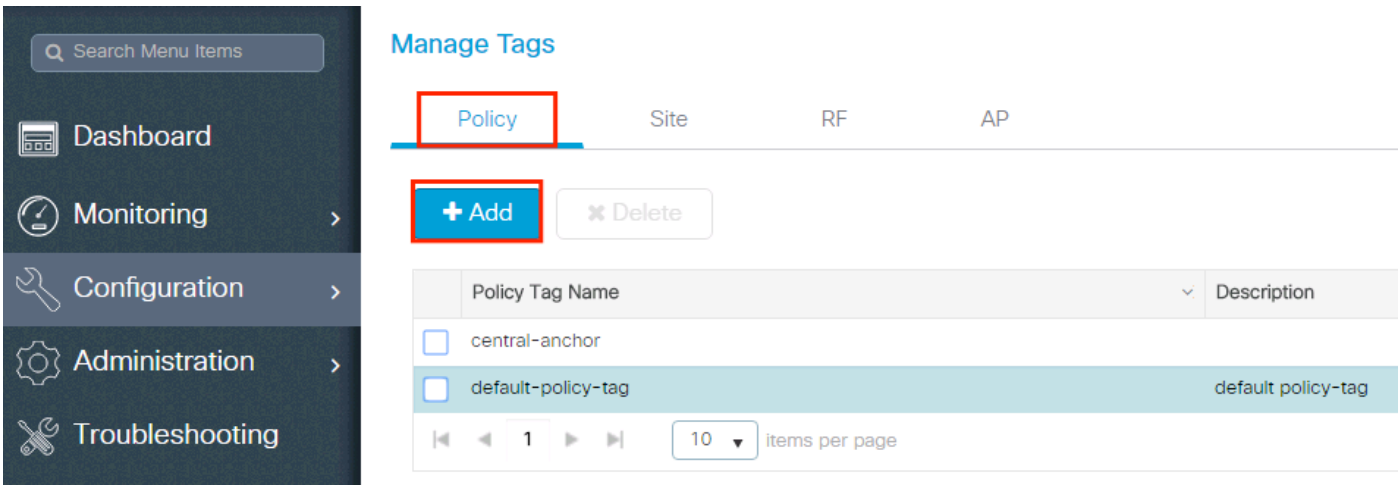
```
# config
# wireless profile policy <policy-profile-name>
# aaa-override
# central switching
# description "<description>"
# vlan <vlanID-or-VLAN_name>
# no shutdown
```

Configuration des balises des politiques

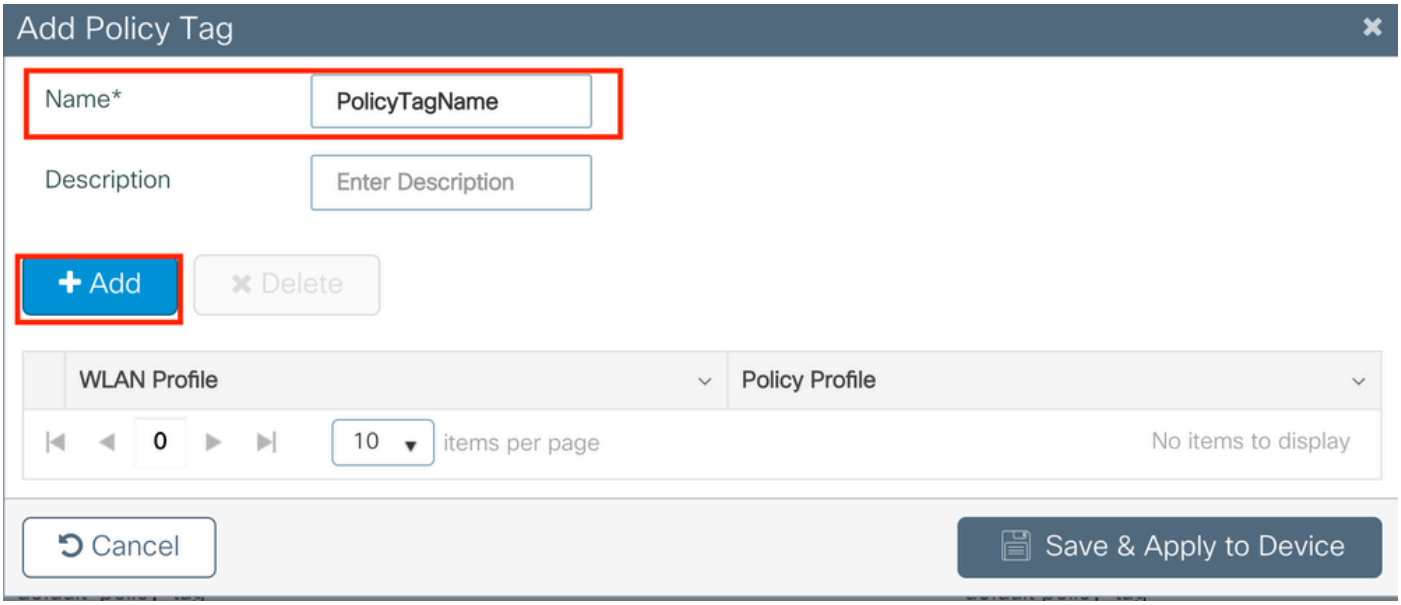
La balise de stratégie est utilisée pour lier le SSID au profil de stratégie. Vous pouvez soit créer une nouvelle balise de politiques, soit utiliser la balise de politique par défaut.

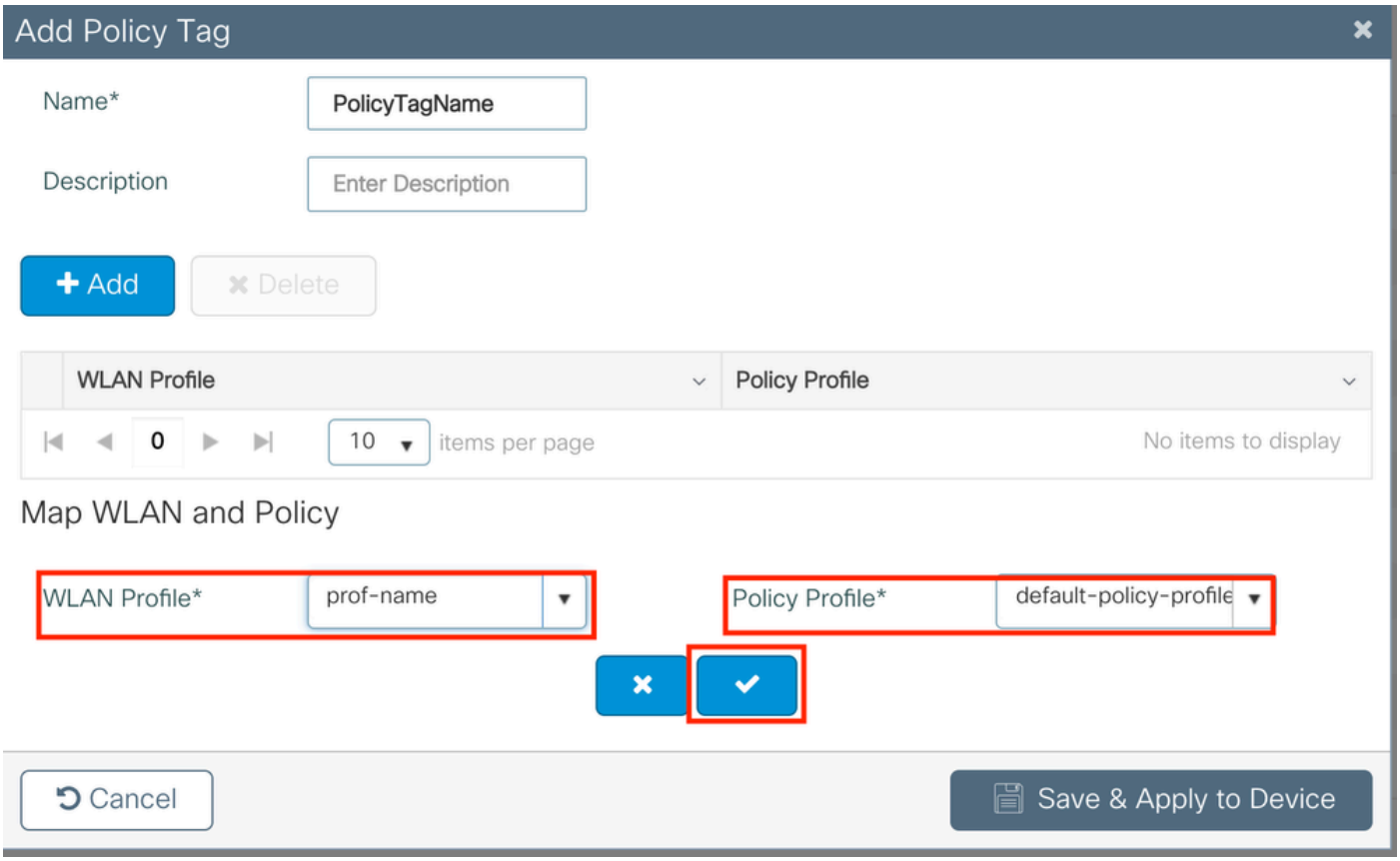
IUG:

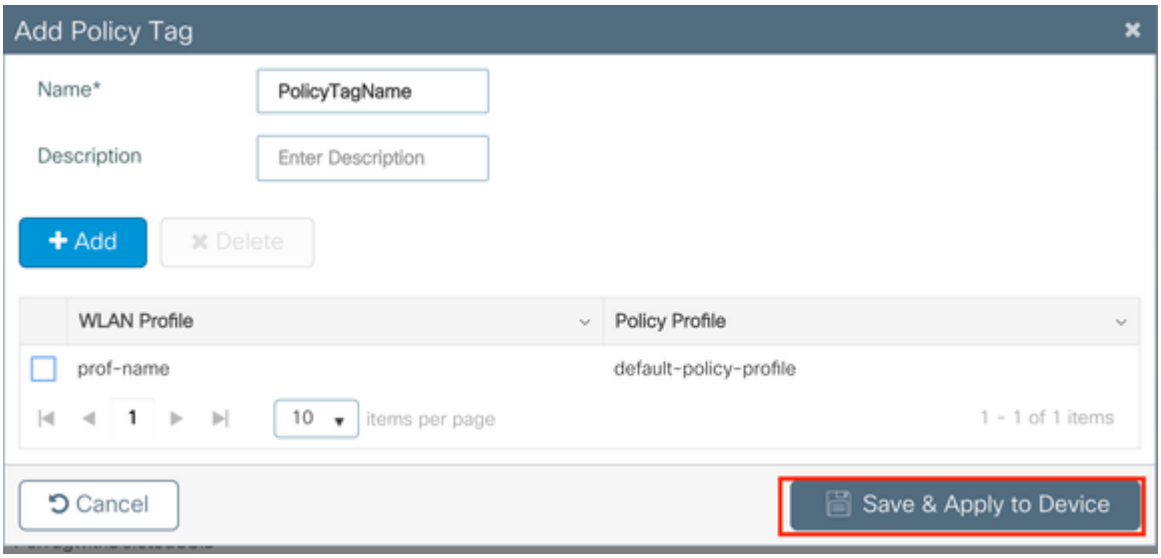
Naviguez jusqu'à **Configugation** > **Tags & Profiles** > **Tags** > **Policy** et ajoutez-en un nouveau si nécessaire.




Liez votre profil de réseau WLAN au profil de politiques souhaité.






CLI :

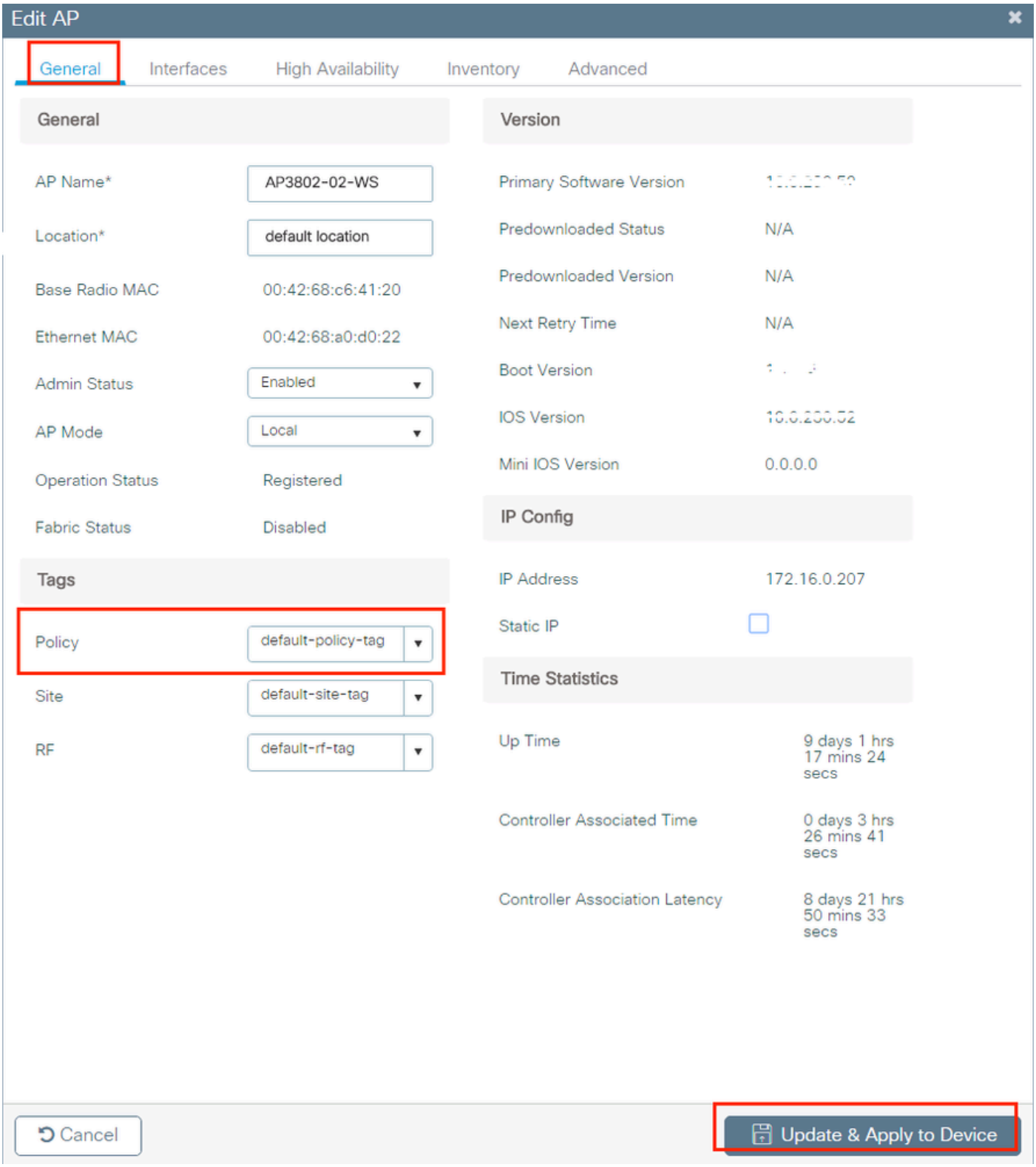
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Attribution de balise de stratégie

Affectez la balise de politiques aux points d'accès nécessaires.

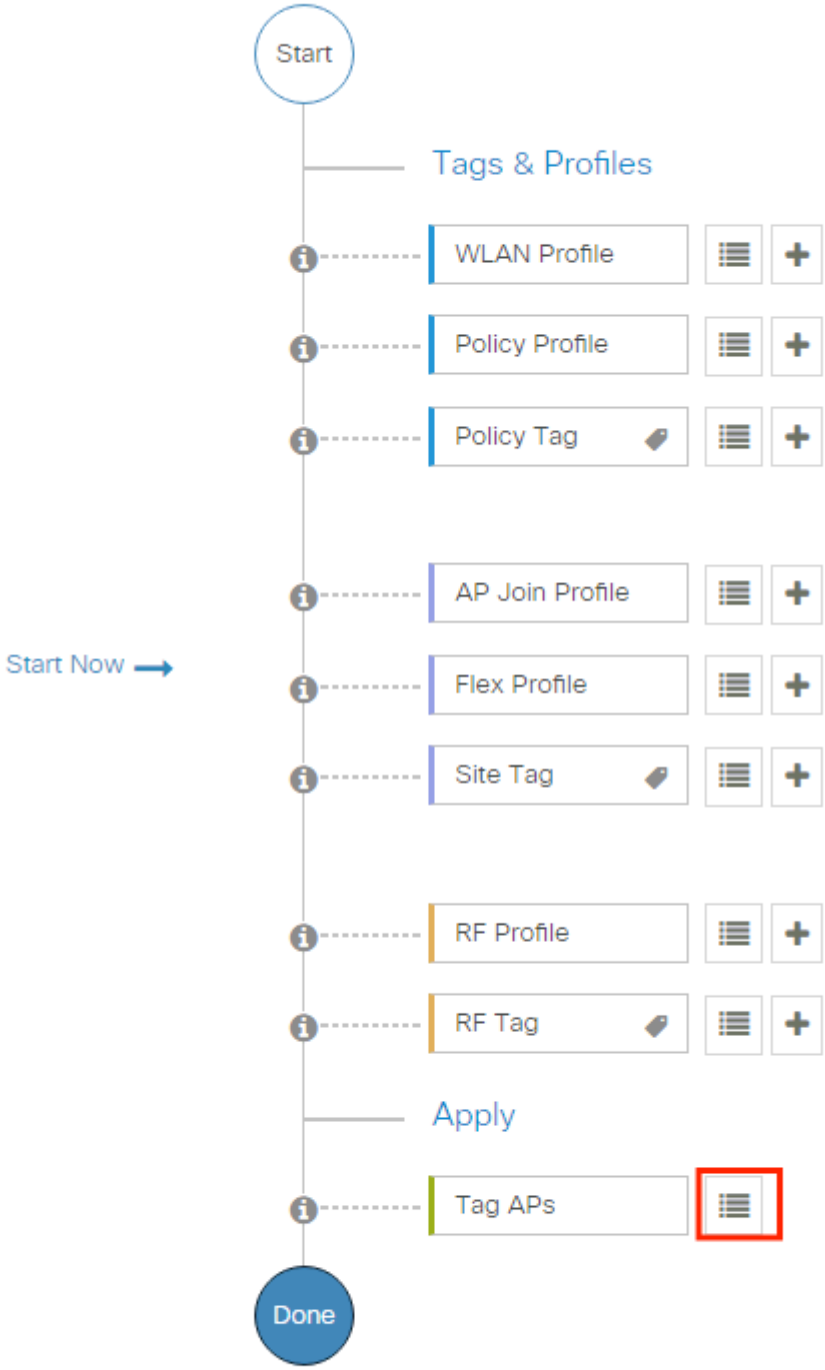
IUG:

Pour affecter la balise à un point d'accès, naviguez jusqu'à **Configuration > Wireless > Access Points > AP Name > General Tags**, affecter la balise de stratégie appropriée, puis cliquez sur **Update & Apply to Device**.

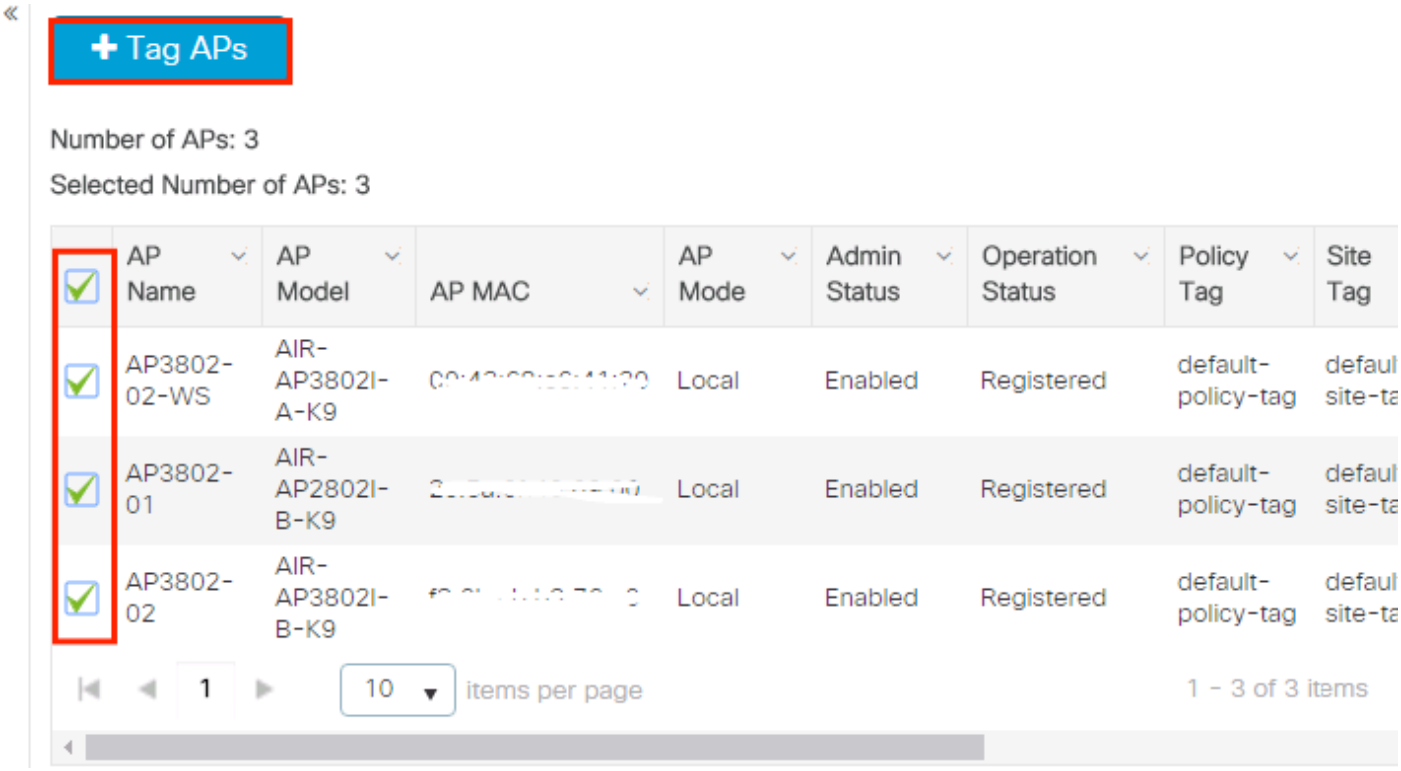


Remarque : Sachez que lorsque la balise de stratégie sur un AP est modifiée, elle abandonne son association au WLC 9800 et se joint à nouveau quelques instants plus tard.

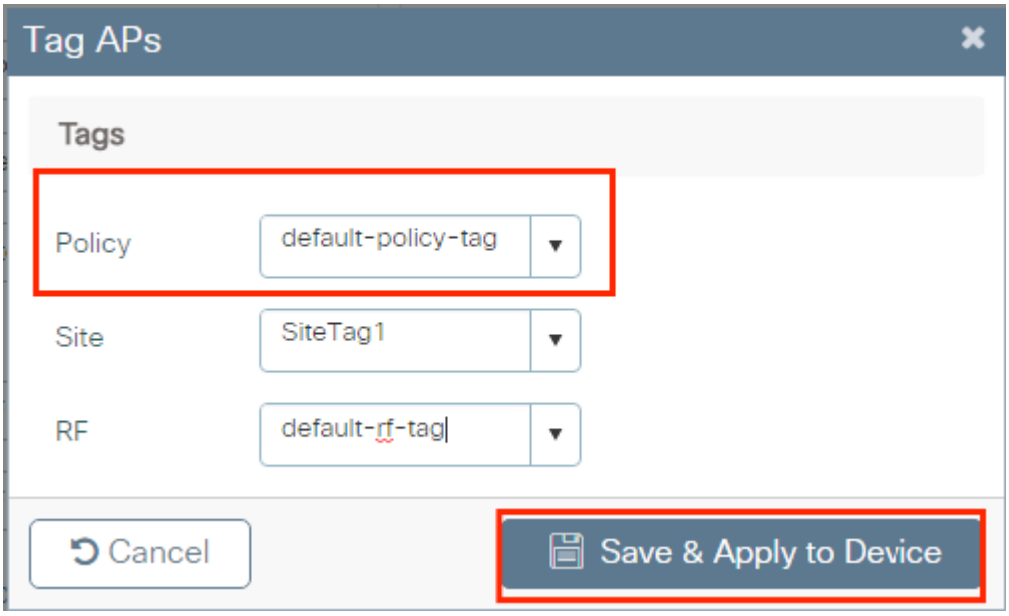
Pour attribuer la même balise de stratégie à plusieurs points d'accès, accédez à **Configuration** > **Wireless Setup** > **Advanced** > **Start Now** > **Apply**.



Sélectionnez les points d'accès auxquels vous souhaitez attribuer la balise et cliquez sur + Tag APs.




Sélectionnez les balises appropriées pour la politique, le site et la RF, puis cliquez sur Save& Apply to Device (Appliquer au périphérique) :




CLI :

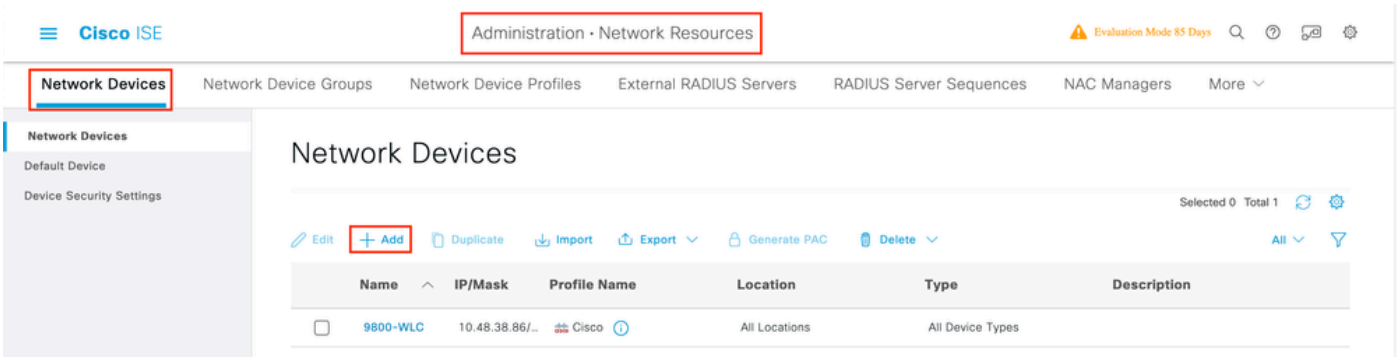
```
# config t
# ap <ethernet-mac-addr>
```

```
# policy-tag <policy-tag-name>
# end
```

## Configuration ISE

### Déclarer le WLC sur ISE

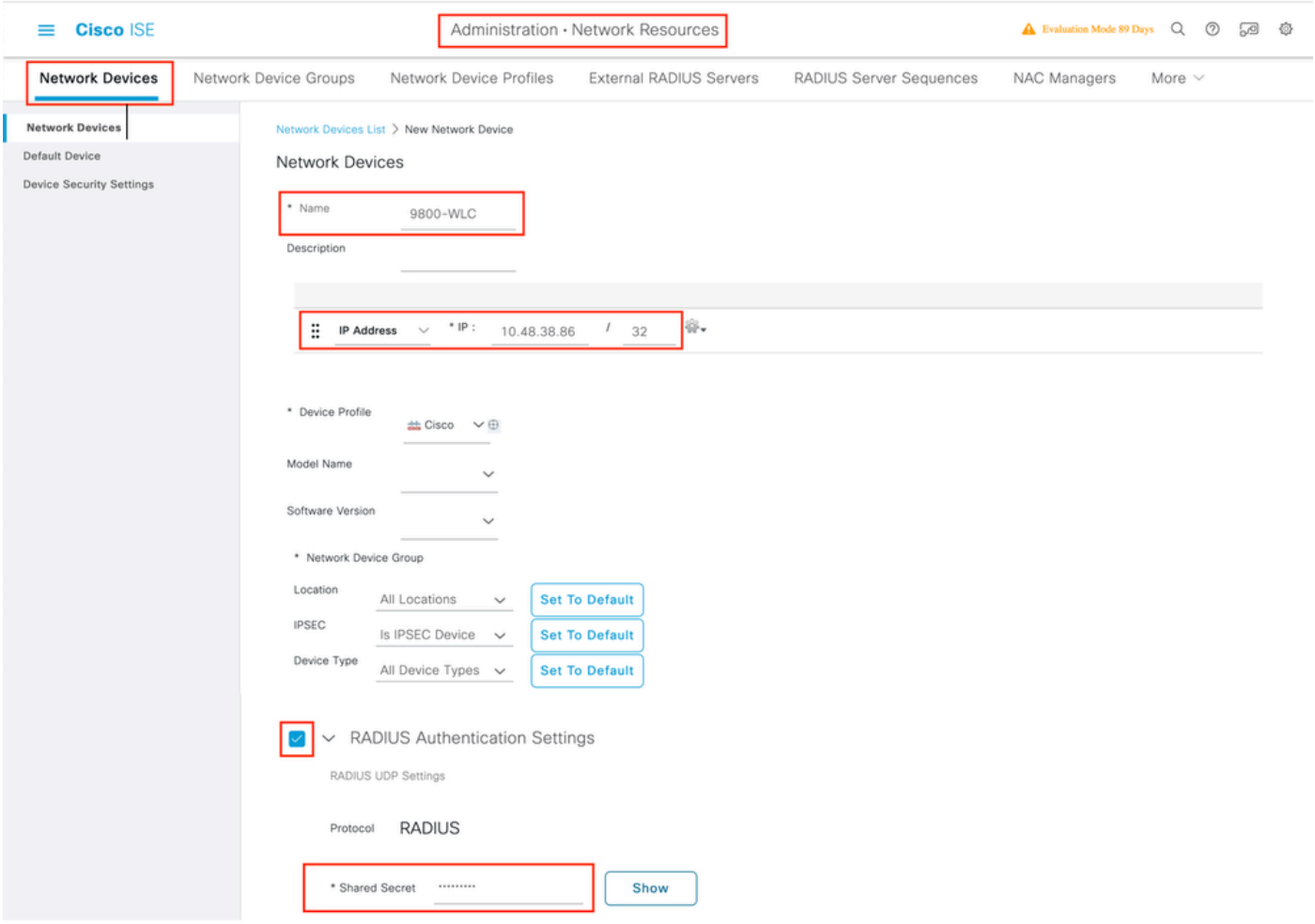
Étape 1. Ouvrez la console ISE et accédez à **Administration** > **Network Resources** > **Network Devices** > **Add** comme indiqué dans l'image.




Étape 2 : configuration du périphérique réseau

Il peut éventuellement s'agir d'un nom de modèle, d'une version de logiciel, d'une description et d'une affectation de groupes de périphériques réseau en fonction des types de périphériques, de l'emplacement ou des WLC.

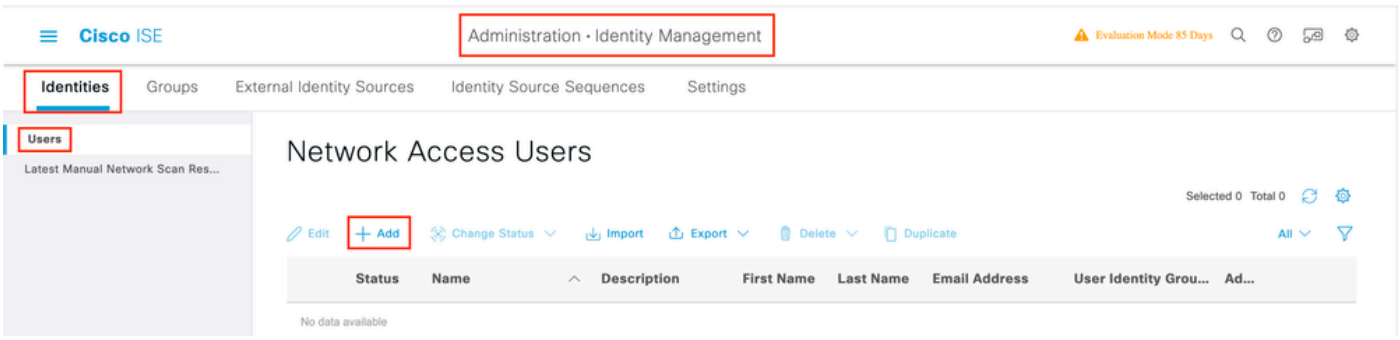
L'adresse IP correspond ici à l'interface WLC qui envoie les requêtes d'authentification. Par défaut, il s'agit de l'interface de gestion, comme illustré dans l'image :



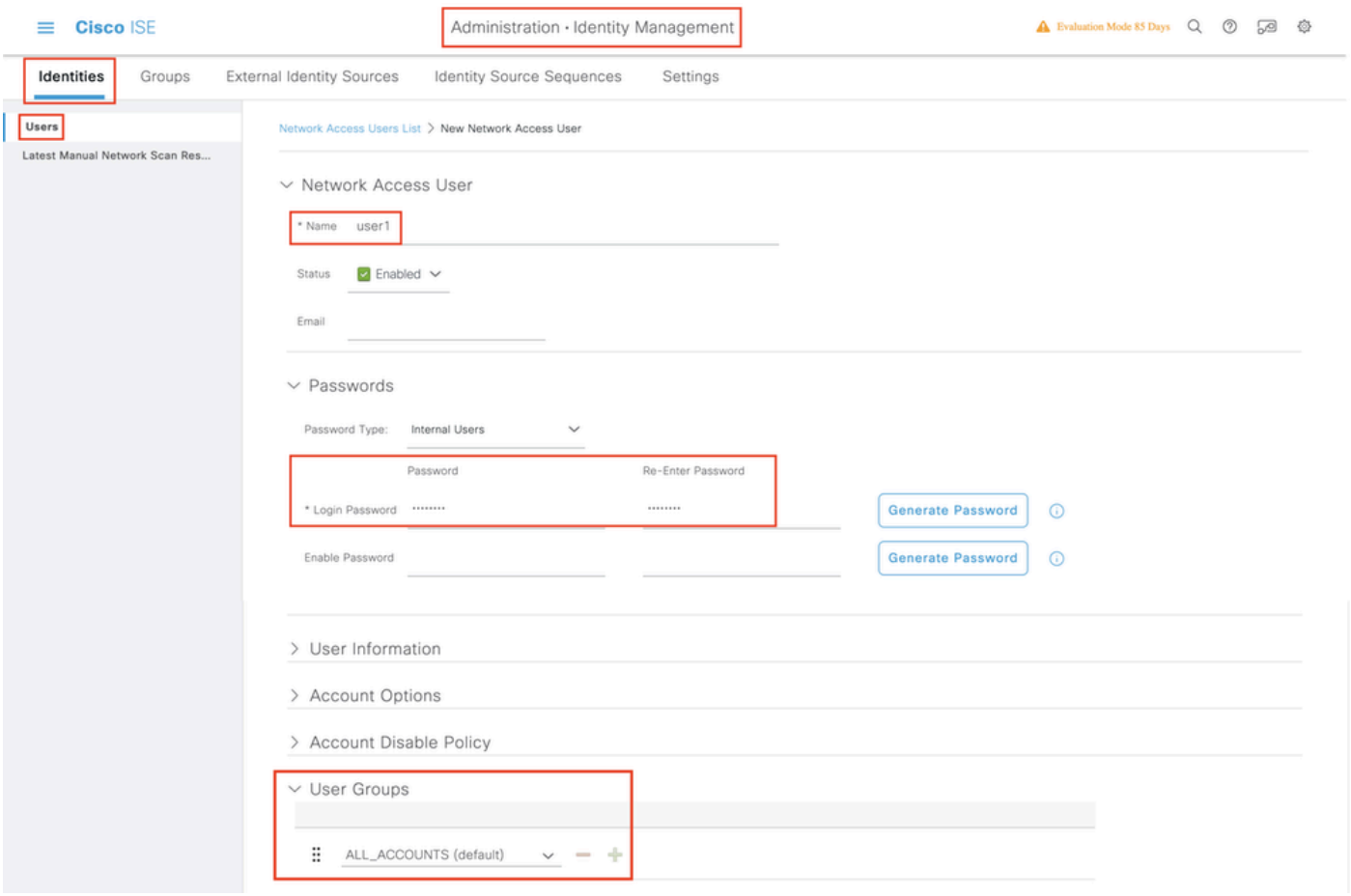

Pour plus d'informations sur **Network Device Groups** la révision du chapitre : Gérer les périphériques réseau à partir du Guide de l'administrateur de Cisco Identity Services Engine : Groupes de périphériques réseau.

Créer un nouvel utilisateur sur ISE

Étape 1. Naviguez **Administration** > **Identity Management** > **Identities** > **Users** > **Add** comme indiqué dans l'image :



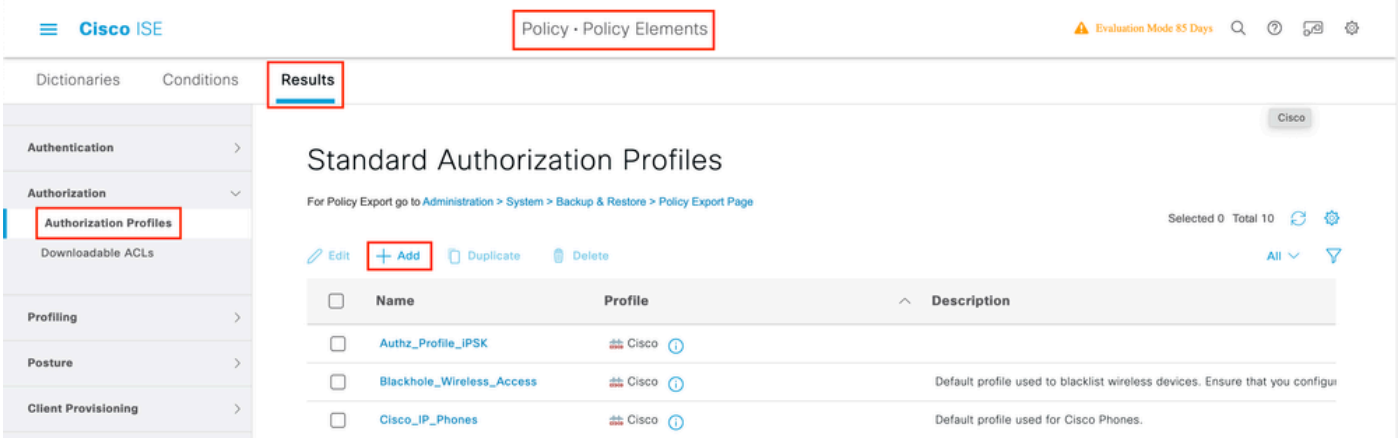
Étape 2. Entrez les informations relatives à l'utilisateur. Dans cet exemple, l'utilisateur appartient à un groupe appelé ALL_ACCOUNTS, mais il peut être ajusté selon les besoins, comme indiqué dans l'image:



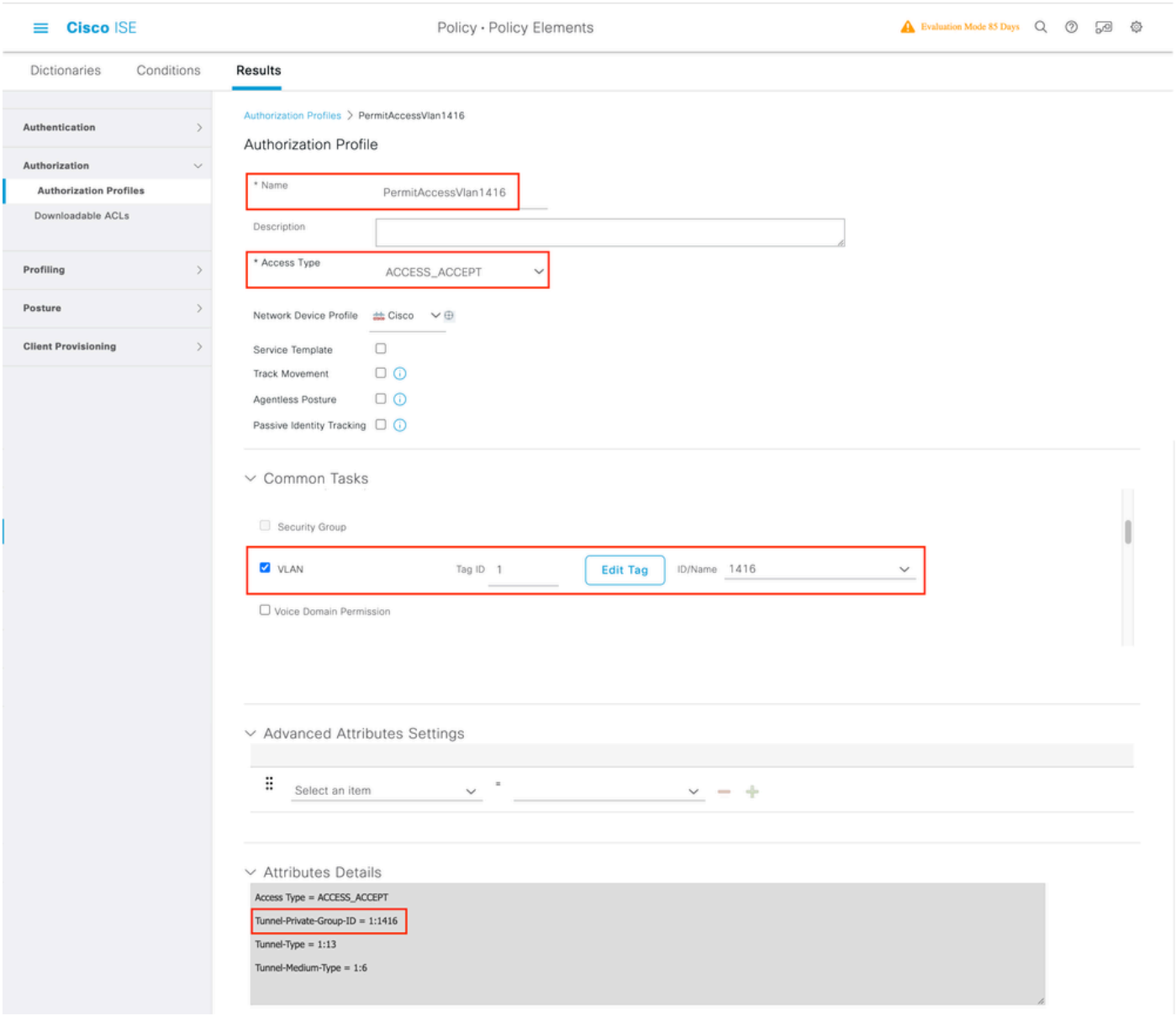

Créer un profil d'autorisation

Le **Authorization Profile** se compose d'un ensemble d'attributs renvoyés lorsqu'une condition est satisfaite. Le profil d'autorisation détermine si le client a accès ou non au réseau, les listes de contrôle d'accès (ACL) push, le remplacement de VLAN ou tout autre paramètre. Le profil d'autorisation présenté dans cet exemple envoie un accord d'accès pour le client et attribue le client au VLAN 1416.

Étape 1. Accédez à **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** et cliquez sur le **Add** bouton.

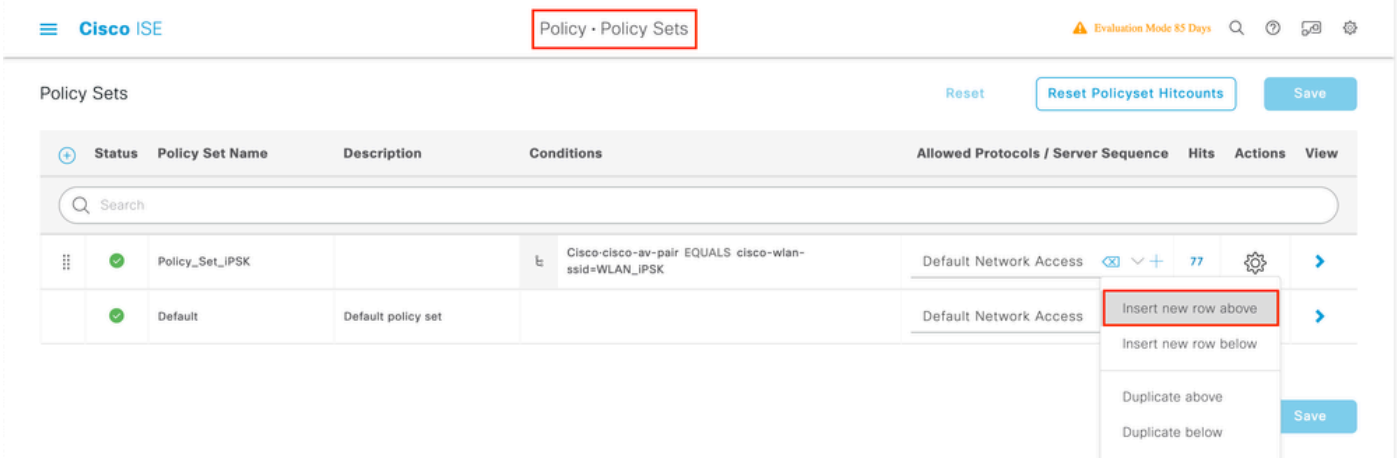



Étape 2. Entrez les valeurs indiquées dans l'image. Ici, nous pouvons retourner des attributs AAA override comme VLAN par exemple. Le WLC 9800 accepte les attributs de tunnel 64, 65, 81 qui utilisent l'ID ou le nom de VLAN, et accepte également l'utilisation de l'**AirSpace-Interface-Name**attribut.




Créer un ensemble de stratégies

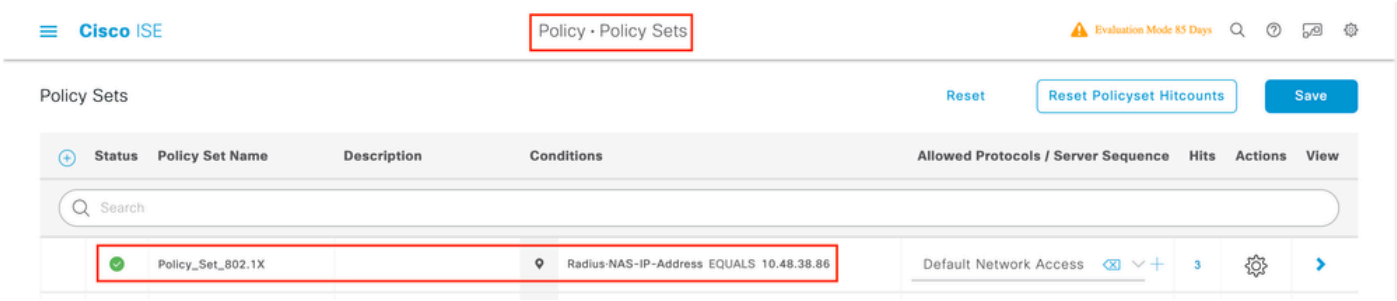
Un ensemble de stratégies définit un ensemble de règles d'authentification et d'autorisation. Pour en créer un, accédez à **Policy** > **Policy Sets**, cliquez sur l'engrenage du premier jeu de stratégies de la liste et sélectionnez, **Insert new row above** comme illustré dans cette image :




Configurez un nom et créez une condition pour cet ensemble de stratégies. Dans cet exemple, la condition spécifie que nous faisons correspondre le trafic qui provient du WLC :

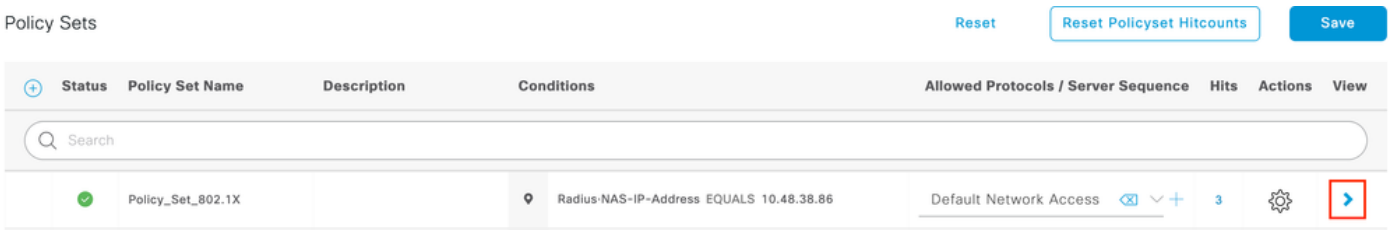
```
Radius:NAS-IP-Address EQUALS X.X.X.X      // X.X.X.X is the WLC IP address
```

Assurez-vous que **Default Network Access** est sélectionné sous **Allowed Protocols / Server Sequence.**




Créer une stratégie d'authentification

Pour configurer les stratégies d'authentification et d'autorisation, vous devez entrer la configuration du jeu de stratégies. Cela peut être fait si vous cliquez sur la flèche bleue à droite de la **Policy Set** ligne :



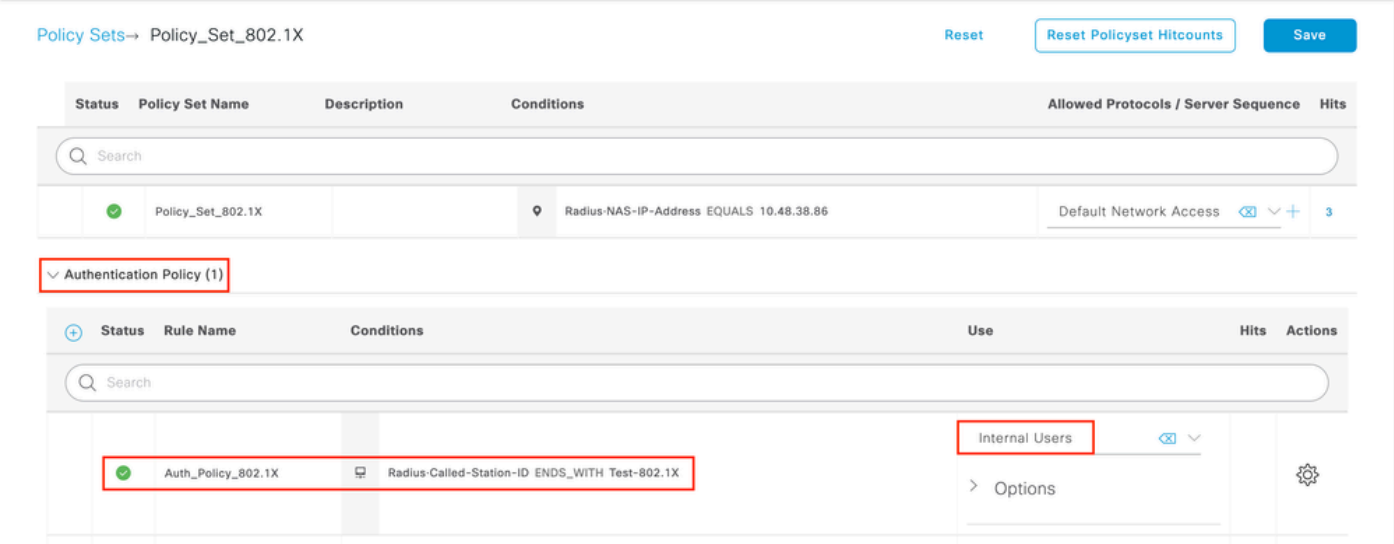
Les stratégies d'authentification sont utilisées pour vérifier si les informations d'identification des utilisateurs sont correctes (vérifier si l'utilisateur est réellement celui qu'il dit être). Sous **Authenticaton Policy**, créer une stratégie d'authentification et la configurer comme indiqué dans cette image. La condition de la stratégie utilisée dans cet exemple est la suivante :

```
RADIUS:Called-Station-ID ENDS_WITH

        //

       is the SSID of your WLAN
```

Choisissez également Internal Users dans l'**Use**onglet de cette stratégie d'authentification.




Créer une stratégie d'autorisation

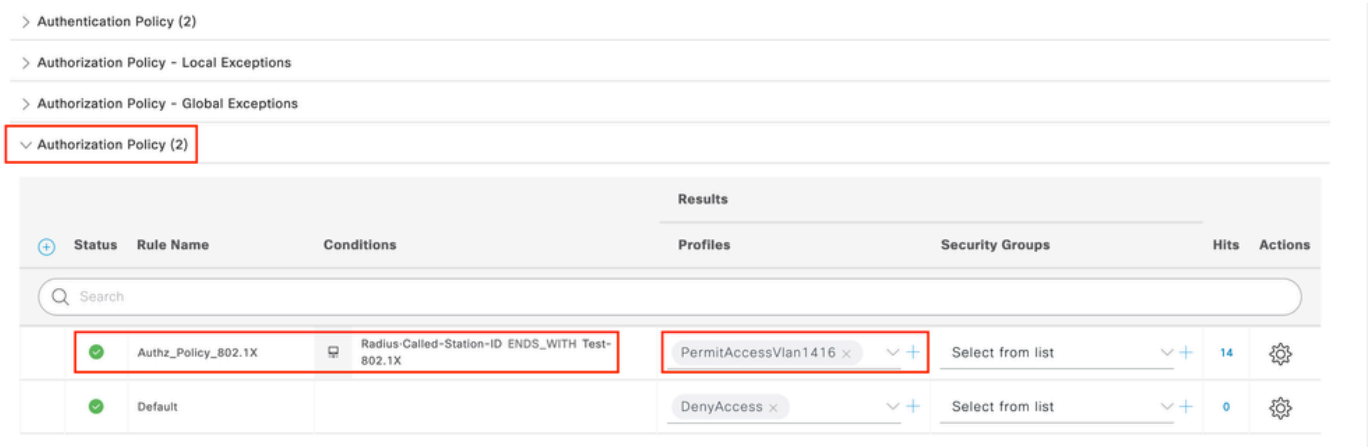
Sur la même page, accédez à **Authorization Policy** et créez-en une nouvelle. La condition de cette stratégie d'autorisation est la suivante :

```
RADIUS:Called-Station-ID ENDS_WITH
```

```
//

is the SSID of your WLAN
```

Sous l'**Result** > **Profiles**onglet de cette stratégie, sélectionnez la stratégie que **Authorization Profile** vous avez créée précédemment. ISE envoie alors les attributs corrects au WLC si l'utilisateur est authentifié.




À ce stade, toute la configuration pour le WLC et ISE est terminée, vous pouvez maintenant essayer de vous connecter à un client.

Pour plus d'informations sur les stratégies d'autorisation ISE, consultez le chapitre : Gérer les stratégies d'authentification à partir du Guide de l'administrateur de Cisco Identity Services Engine [Gérer les stratégies d'authentification]

Pour plus d'informations sur les sources d'identité ISE, consultez le chapitre : Gérer les utilisateurs et les sources d'identité externes à partir du Guide de l'administrateur de Cisco Identity Services Engine : [Sources d'identité]

# Vérifier

Vous pouvez utiliser ces commandes pour vérifier votre configuration actuelle :

```
# show run wlan // WLAN configuration
# show run aaa // AAA configuration (server, server group, methods)
# show aaa servers // Configured AAA servers
# show ap config general // AP's configurations
# show ap name <ap-name> config general // Detailed configuration of specific AP
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name>// Detailed information on given policy pr
```

# Dépannage



Remarque : L'utilisation d'équilibreurs de charge externes est correcte. Cependant, assurez-vous que votre équilibreur de charge fonctionne sur une base par client en utilisant l'attribut RADIUS call-station-id. L'utilisation du port source UDP n'est pas un mécanisme pris en charge pour équilibrer les requêtes RADIUS du 9800.

## Dépannage sur le WLC

Le WLC 9800 offre des fonctionnalités de suivi ALWAYS-ON. Cela garantit que tous les messages d'erreur, d'avertissement et de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une défaillance après qu'il se soit produit. Cela dépend du volume de journaux générés, mais généralement, vous pouvez revenir en arrière de quelques heures à plusieurs jours.

Afin d'afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter par SSH/Telnet au WLC 9800 et effectuer ces étapes : (Veillez à consigner la session dans un fichier texte).

Étape 1 : vérification de l’heure actuelle du WLC pour que vous puissiez suivre les journaux dans l’heure jusqu’à laquelle le problème s’est produit

```
# show clock
```

Étape 2 : collecte des syslogs à partir de la mémoire tampon du WLC ou du syslog externe, selon la configuration du système. Cela fournit un aperçu rapide de l’intégrité du système et des erreurs, le cas échéant.

```
# show logging
```

Étape 3 : vérification de l’activation des conditions de débogage

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

Remarque : Si une condition est répertoriée, cela signifie que les traces sont enregistrées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmente le volume des journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque vous ne procédez pas activement au débogage.

Étape 4. Supposons que l’adresse MAC testée n’était pas répertoriée comme condition à l’étape 3, collectez les suivis de niveau de notification toujours actif pour l’adresse MAC spécifique :

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe:

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Débogage conditionnel et traçage Radio Active

Si les traces toujours actives ne vous donnent pas suffisamment d'informations pour déterminer le déclencheur du problème en cours d'investigation, vous pouvez activer le débogage conditionnel et capturer la trace Radio Active (RA), qui fournit des traces au niveau du débogage pour tous les processus qui interagissent avec la condition spécifiée (l'adresse MAC du client dans ce cas).

Vous pouvez le faire via l'interface utilisateur graphique ou l'interface de ligne de commande.

CLI :

Afin d'activer le débogage conditionnel, effectuez ces étapes.

Étape 5. Vérifiez qu’aucune condition de débogage n’est activée.

```
# clear platform condition all
```

Étape 6. Activez la condition de débogage pour l’adresse MAC du client sans fil que vous souhaitez surveiller.

Cette commande commence à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez éventuellement augmenter ce délai jusqu'à 2085978494 secondes.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Remarque : Afin de surveiller plusieurs clients à la fois, exécutez la **<aaaa.bbbb.cccc>**commande de débogage sans fil mac par adresse MAC.

Remarque : vous ne voyez pas le résultat de l'activité du client sur une session de terminal, car tout est mis en mémoire tampon en interne pour être visualisé ultérieurement.

Étape 7. Reproduisez le problème ou le comportement que vous souhaitez surveiller.

Étape 8. Arrêtez les débogages si le problème est reproduit avant que le temps de surveillance par défaut ou configuré ne se soit écoulé.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Une fois que le temps de surveillance s'est écoulé ou que le débogage sans fil a été arrêté, le contrôleur WLC 9800 génère un fichier local du nom de :

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Étape 9. Collectez le fichier de l'exercice d'adressage MAC.  Vous pouvez copier le fichier ra trace.log sur un serveur externe ou afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA:

```
# dir bootflash: | inc ra_trace
```

Copiez le fichier sur un serveur externe :

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Affichez-en le contenu :

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 10. Si la cause première n'est toujours pas évidente, collectez les journaux internes, qui sont une vue plus détaillée des journaux de niveau de débogage. Vous n'avez pas besoin de déboguer à nouveau le client car nous examinons plus en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

Remarque : Cette sortie de commande retourne des traces pour tous les niveaux de log pour tous les processus et est assez volumineuse. Veuillez faire appel à Cisco TAC pour faciliter l'analyse de ces suivis.

Vous pouvez soit copier le fichier ra-internal-FILENAME.txt sur un serveur externe, soit afficher le résultat directement à l'écran.

Copiez le fichier sur un serveur externe :

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Affichez-en le contenu :

```
# more bootflash:ra-internal-<FILENAME>.txt
```

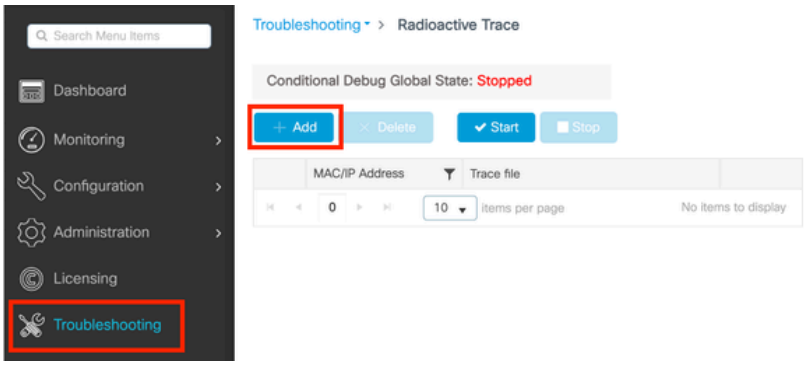
Étape 11. Supprimer les conditions de débogage

```
# clear platform condition all
```

Remarque : Veillez à toujours supprimer les conditions de débogage après une session de dépannage.

IUG:

Étape 1. Accédez à **Troubleshooting** > **Radioactive Trace** > + **Add** et spécifiez l'adresse MAC/IP du ou des clients que vous souhaitez dépanner.

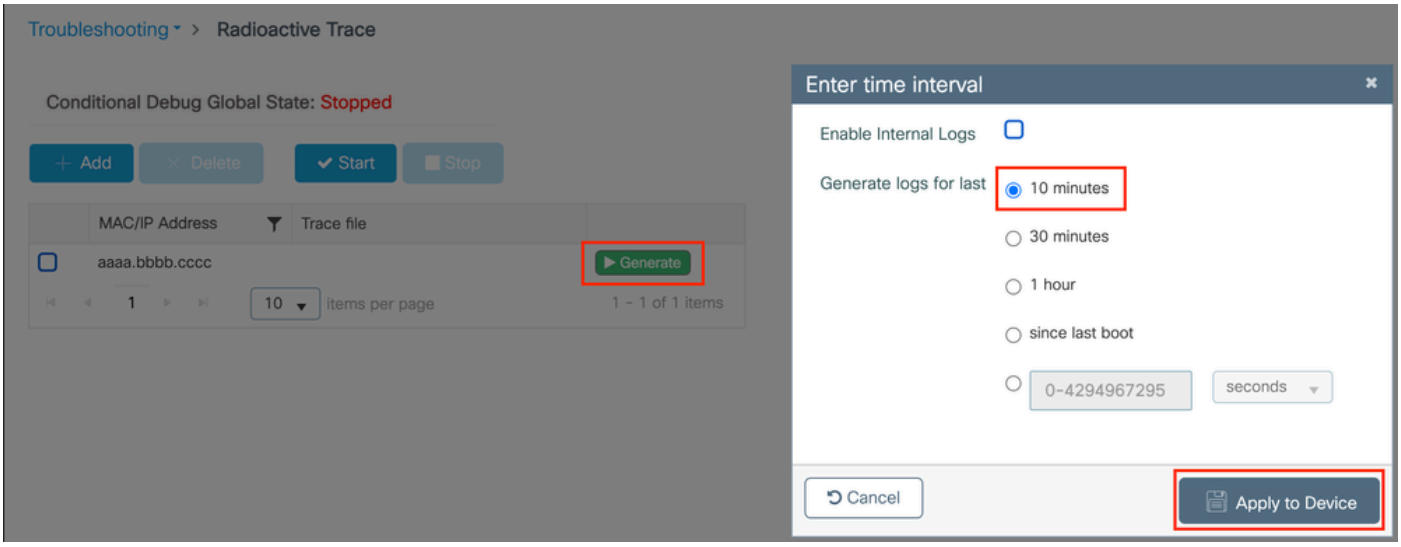



Étape 2. Cliquez sur Démarrer.

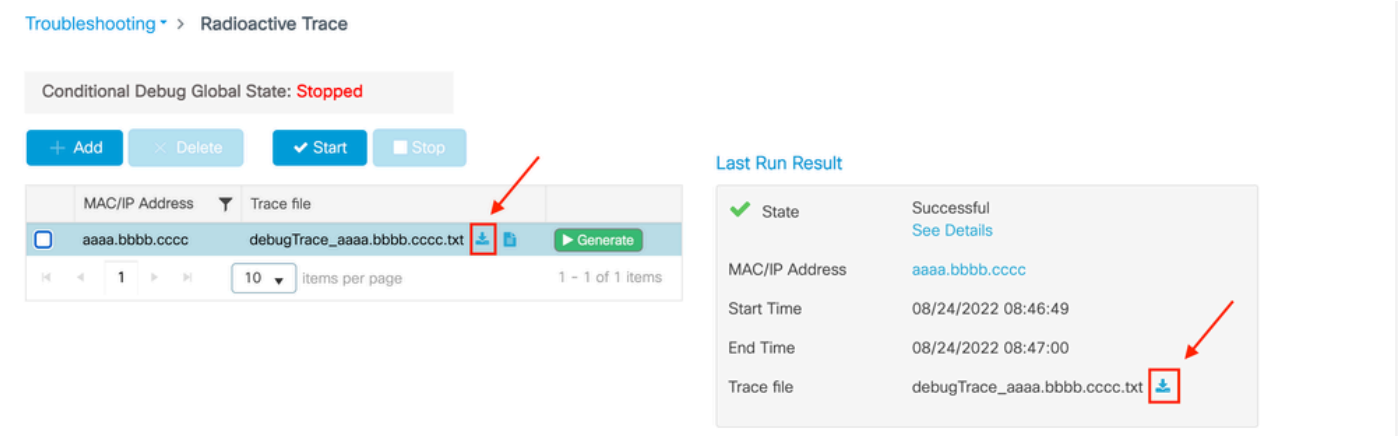
Étape 3. Reproduire le problème

Étape 4. Cliquez sur Stop.

Étape 5. Cliquez sur le **Generate** bouton, sélectionnez l'intervalle de temps pour lequel vous souhaitez obtenir les journaux, puis cliquez sur **Apply to Device**. In this example, the logs for the last 10 minutes are requested.

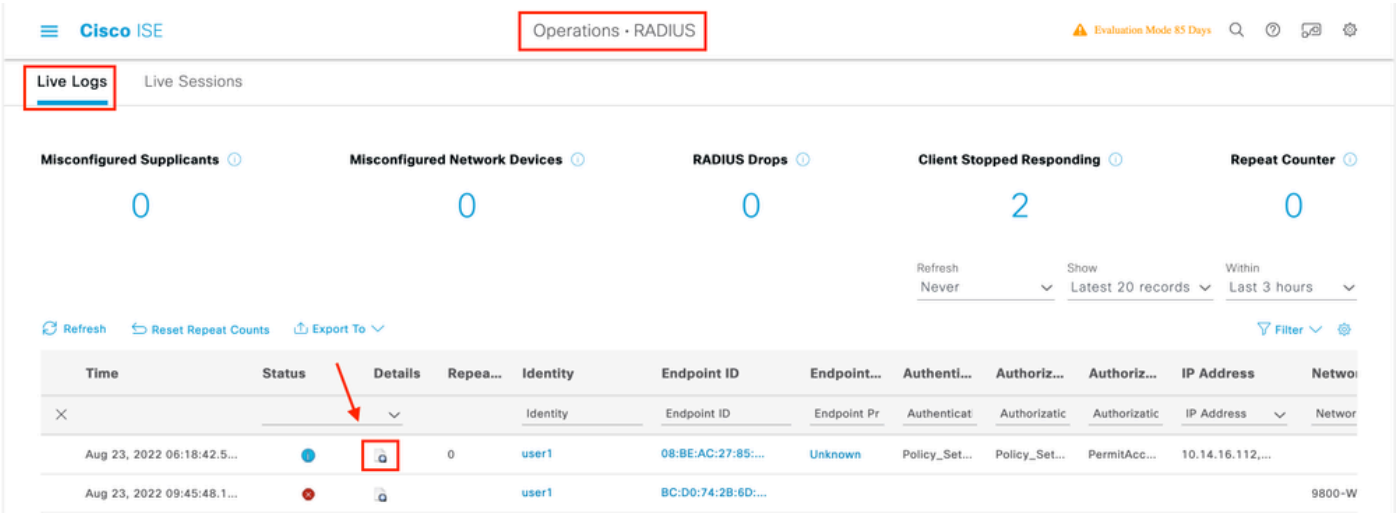



Étape 6. Téléchargez le logiciel Radioactive Trace sur votre ordinateur, cliquez sur le bouton de téléchargement et inspectez-le.




## Dépannage sur ISE

Si vous rencontrez des problèmes avec l'authentification du client, vous pouvez vérifier les journaux sur le serveur ISE. Accédez à **Operations** > **RADIUS** > **Live Logs** et vous voyez la liste des demandes d'authentification, ainsi que le jeu de stratégies qui a été mis en correspondance, le résultat de chaque demande, etc. Vous pouvez obtenir plus de détails en cliquant sur la loupe sous l'**Details**onglet de chaque ligne, comme le montre l'image :


Cisco ISE
Operations · RADIUS
Evaluation Mode 85 Days
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
2
Repeat Counter
0
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...
Authenti...
Authoriz...
Authoriz...
IP Address
Netwo
Identity
Endpoint ID
Endpoint Pr
Authenticat
Authorizatic
Authorizatic
IP Address
Networ
Aug 23, 2022 06:18:42.5...
0
user1
08:BE:AC:27:85:...
Unknown
Policy_Set...
Policy_Set...
PermitAcc...
10.14.16.112,...
Aug 23, 2022 09:45:48.1...
user1
BC:D0:74:2B:6D:...
9800-W

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.