Configurer la liste d'autorisation AP du contrôleur sans fil Catalyst 9800

Table des matières

Introduction

Ce document décrit comment configurer la stratégie d'authentification du point d'accès (AP) du contrôleur LAN sans fil Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 9800 WLC
- Accès aux contrôleurs sans fil via l'interface de ligne de commande (CLI)

Composants utilisés

Cisco recommande les versions matérielles et logicielles suivantes :

- WLC 9800 v17.3

- AP 1810 W
- AP 1700
- Identity Service Engine (ISE) v2.2

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.

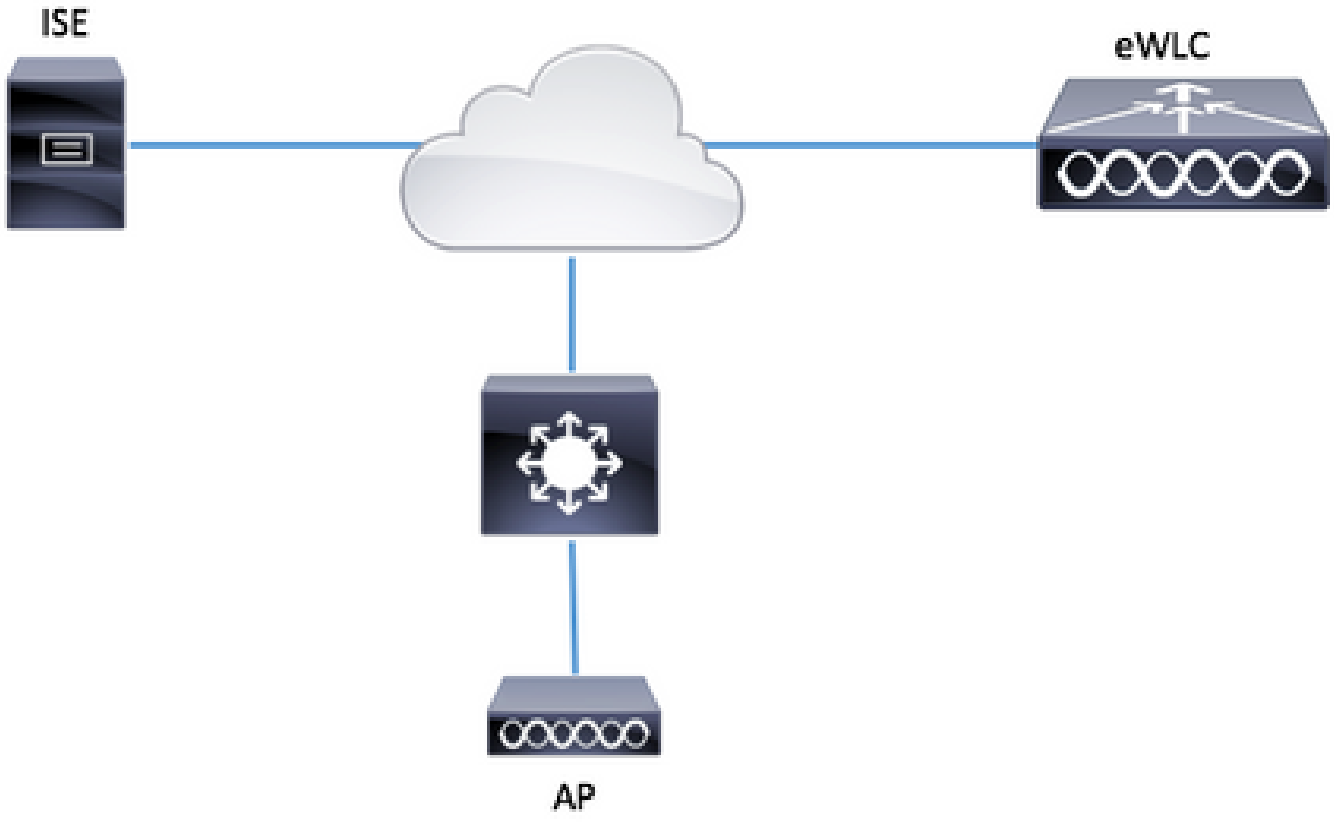
Informations générales

Pour autoriser un point d'accès, l'adresse MAC Ethernet du point d'accès doit être autorisée sur la base de données locale avec le contrôleur LAN sans fil 9800 ou sur un serveur RADIUS (Remote Authentication Dial-In User Service) externe.

Cette fonctionnalité garantit que seuls les points d'accès autorisés peuvent rejoindre un contrôleur LAN sans fil Catalyst 9800. Ce document ne couvre pas le cas de points d'accès maillés (série 1500) qui nécessitent une entrée de filtre MAC pour joindre le contrôleur, mais ne tracent pas le flux d'autorisation typique des points d'accès (voir références).

Configurer

Diagramme du réseau



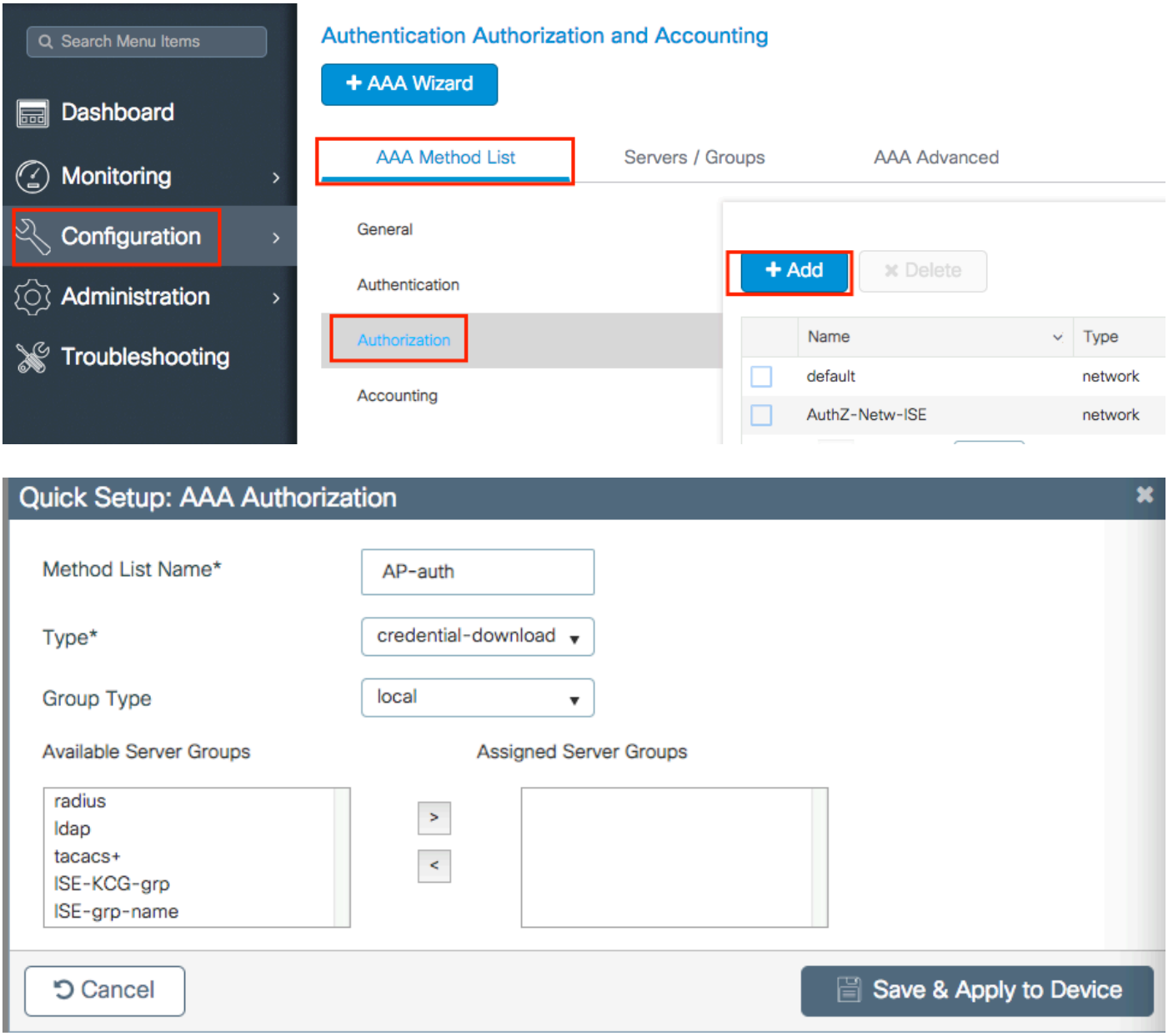
Configurations

Liste d'autorisation MAC AP - Local

Les adresses MAC des points d'accès autorisés sont stockées localement dans le WLC 9800.

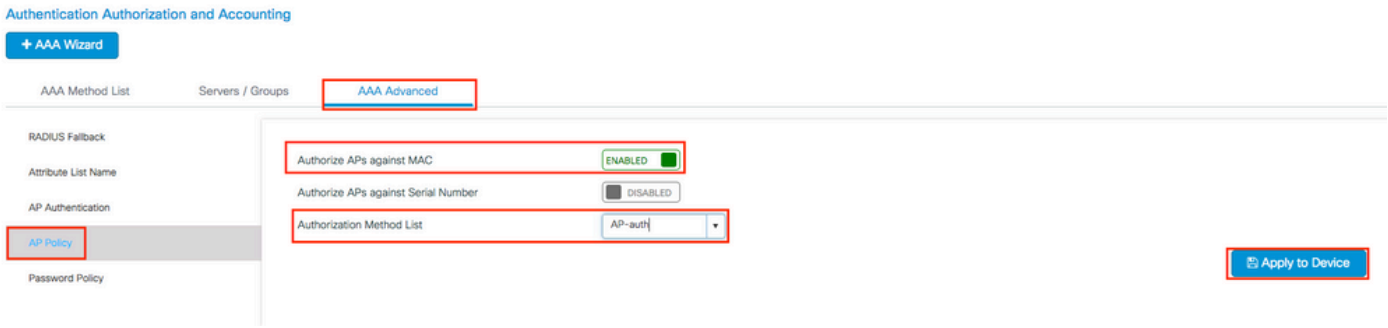
Étape 1. Créez une liste de méthodes de téléchargement des informations d'identification d'autorisation locale.

Accédez à Configuration > Security > AAA > AAA Method List > Authorization > + Add.



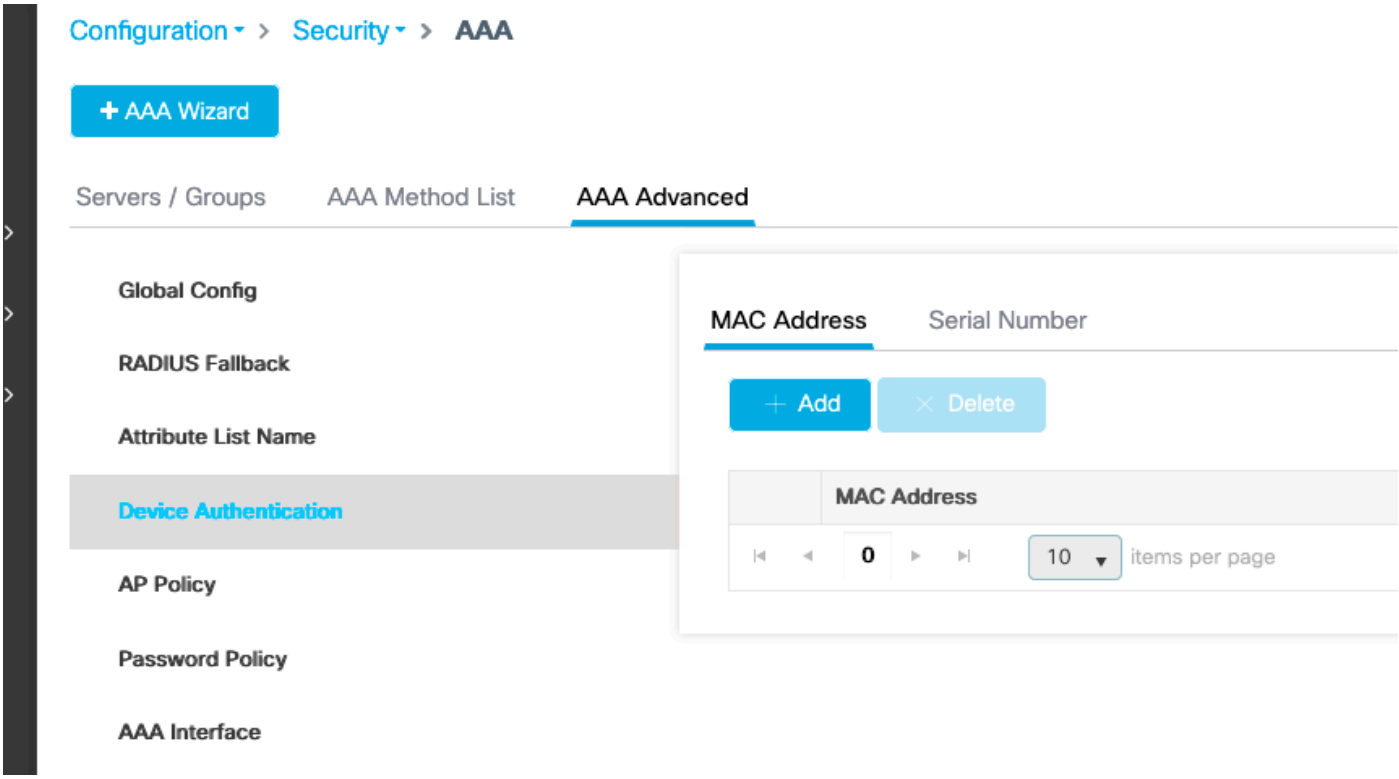
Étape 2. Activez l'autorisation MAC AP.

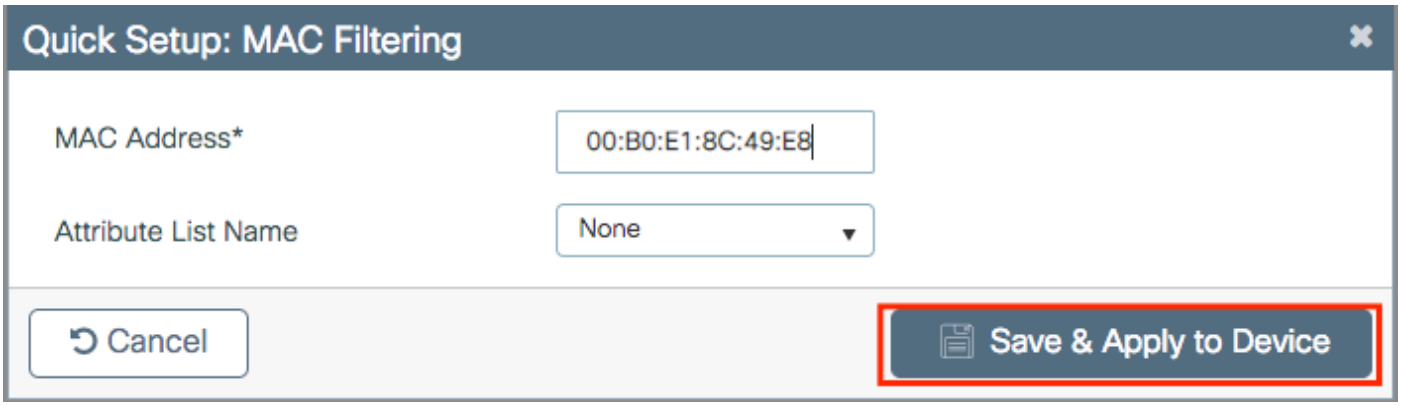
Accédez à Configuration > Security > AAA > AAA Advanced > AP Policy. Activez Authorize APs against MAC et sélectionnez la liste de méthodes d'autorisation créée à l'étape 1.



Étape 3. Ajoutez l'adresse MAC Ethernet AP.

Accédez à Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add.





Remarque : l'adresse MAC Ethernet AP doit être dans l'un de ces formats lorsqu'elle est entrée dans l'interface utilisateur Web (xx : xx : xx : xx : xx : xx (ou) xxxx.xxxx.xxxx (ou) xx-xx-xx-xx-xx-xx) dans la version 16.12. Dans la version 17.3, ils doivent être au format xxxxxxxxxxxx sans séparateur. Le format de l'interface de ligne de commande est toujours xxxxxxxxxxxx, quelle que soit la version (dans la version 16.12, l'interface utilisateur Web supprime les séparateurs dans la configuration). L'ID de bogue Cisco CSCv43870 permet l'utilisation de n'importe quel format dans l'interface de ligne de commande ou l'interface utilisateur Web dans les versions ultérieures.

CLI :

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

Liste d'autorisation MAC AP - Serveur RADIUS externe

Configuration WLC 9800

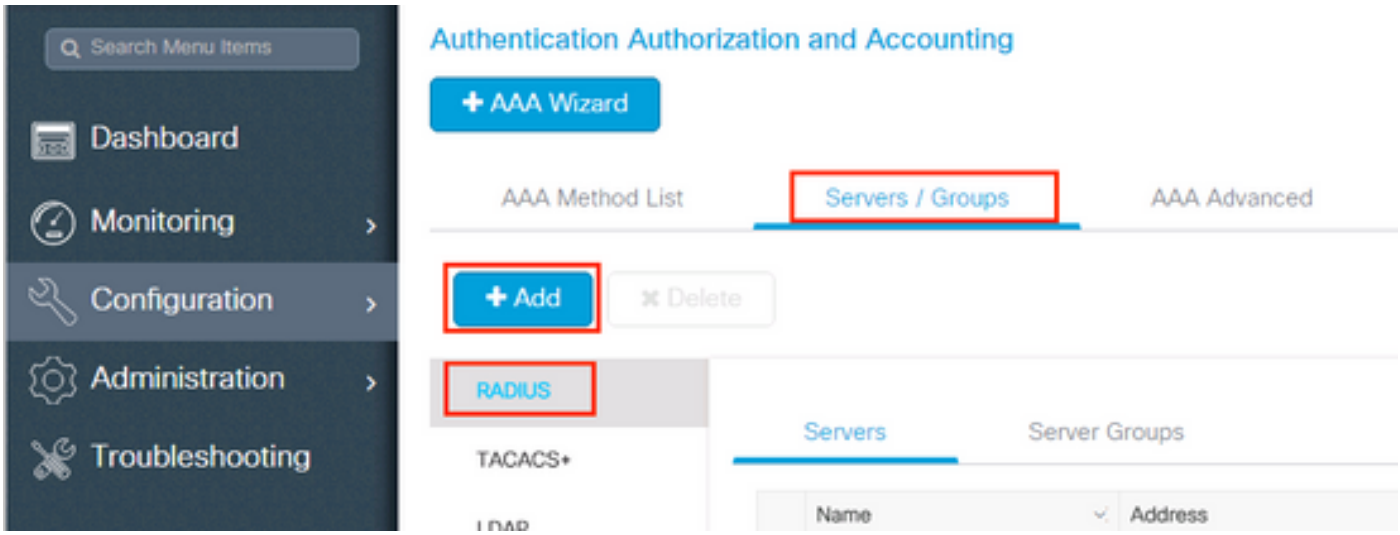
Les adresses MAC des points d'accès autorisés sont stockées sur un serveur RADIUS externe, dans cet exemple ISE.

Sur ISE, vous pouvez enregistrer l'adresse MAC des points d'accès en tant que noms d'utilisateur/mot de passe ou en tant que terminaux. Au cours de ces étapes, vous êtes invité à choisir l'une ou l'autre des méthodes.

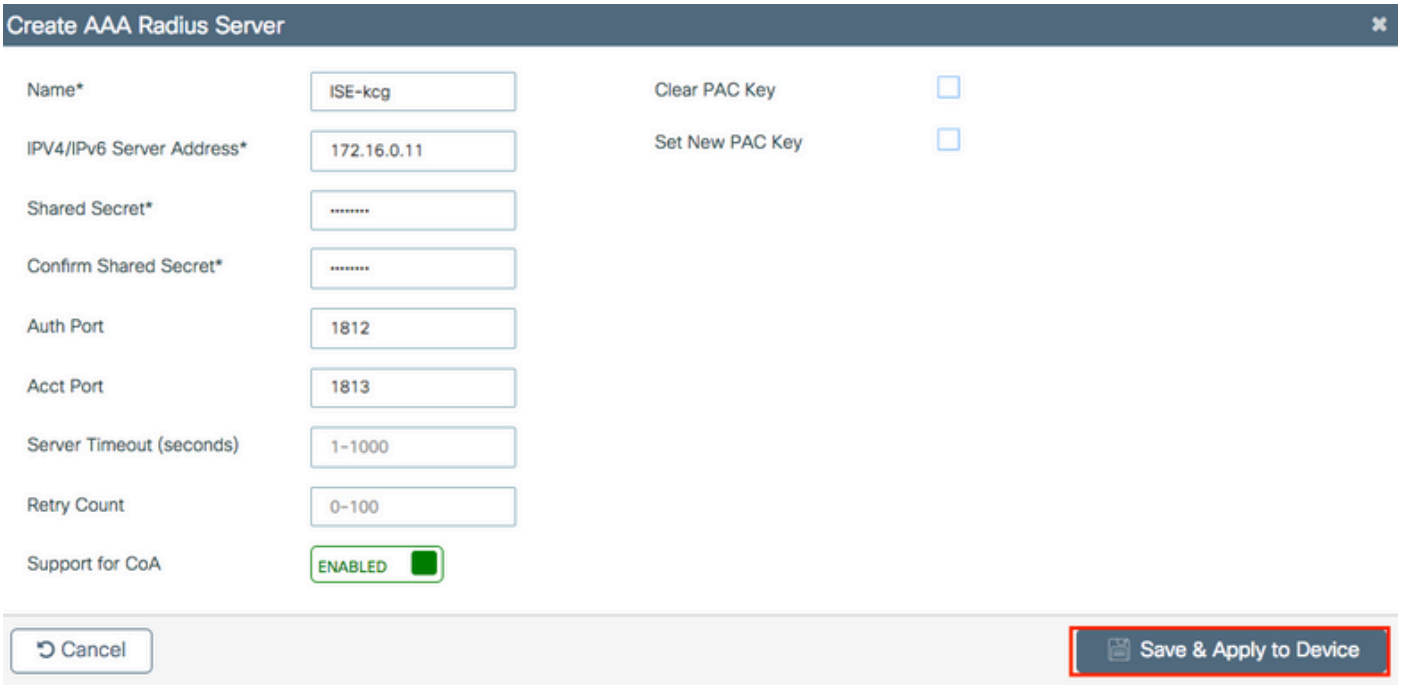
IUG:

Étape 1. Déclarez le serveur RADIUS.

Accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add et entrez les informations du serveur RADIUS.



Assurez-vous que la fonction Support for CoA est activée si vous prévoyez utiliser l'authentification Web centralisée (ou tout type de sécurité nécessitant CoA) à l'avenir.

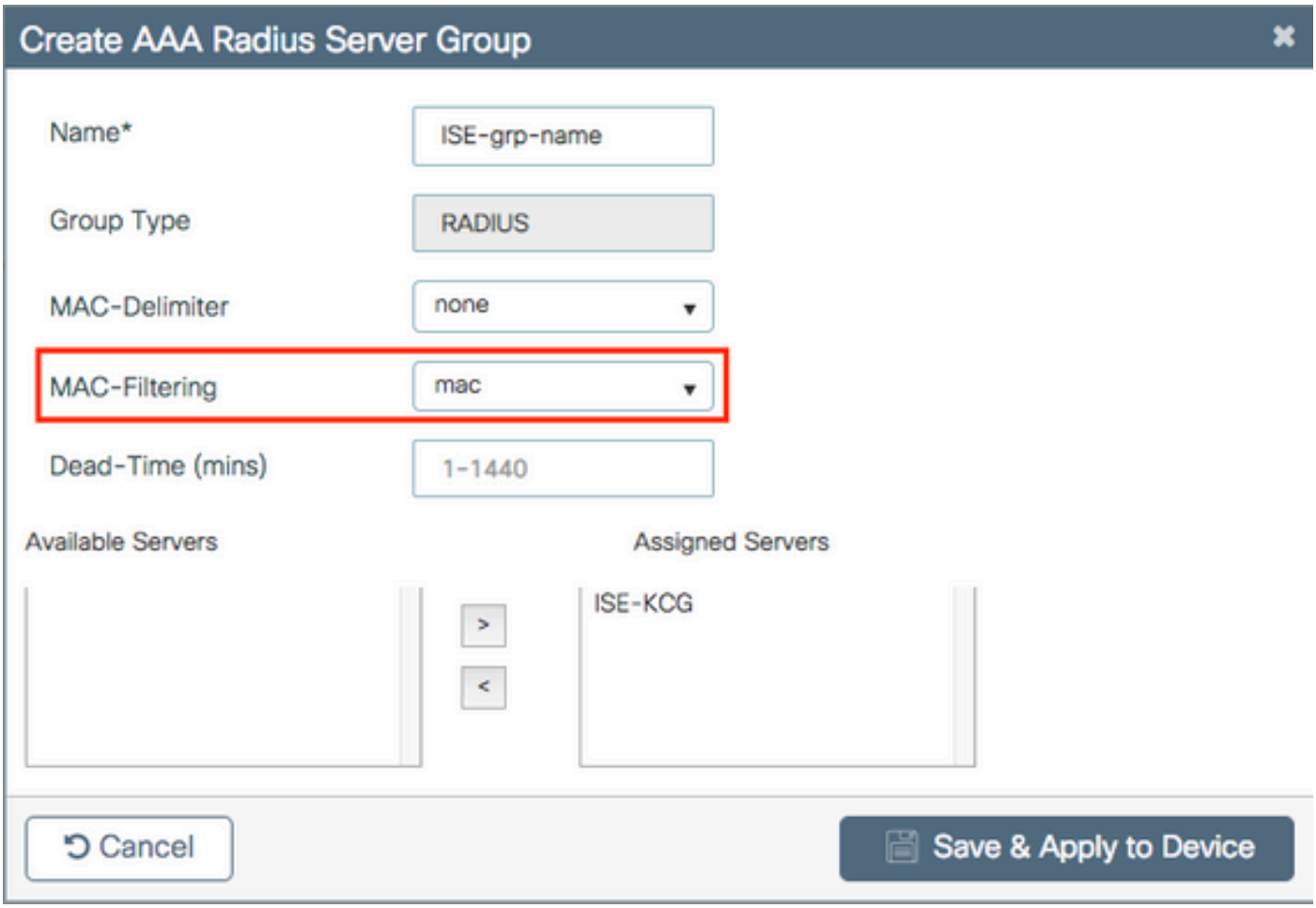


Étape 2. Ajoutez le serveur RADIUS à un groupe RADIUS.

Accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.

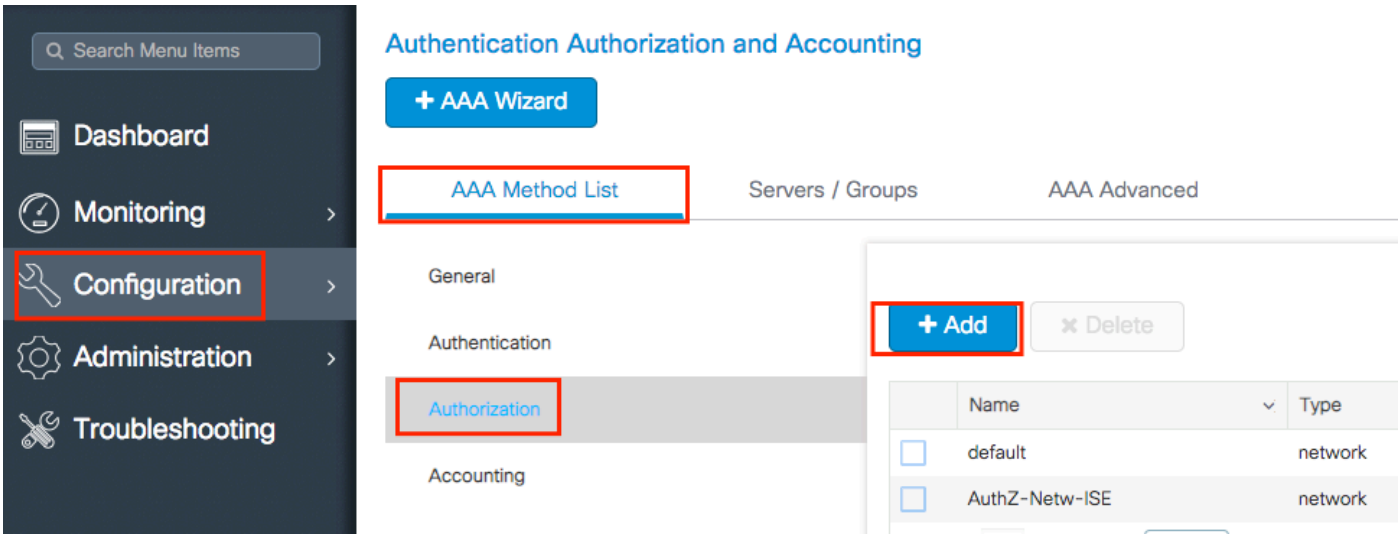
Pour qu'ISE authentifie l'adresse MAC AP en tant que noms d'utilisateur, laissez MAC-Filtering comme none.

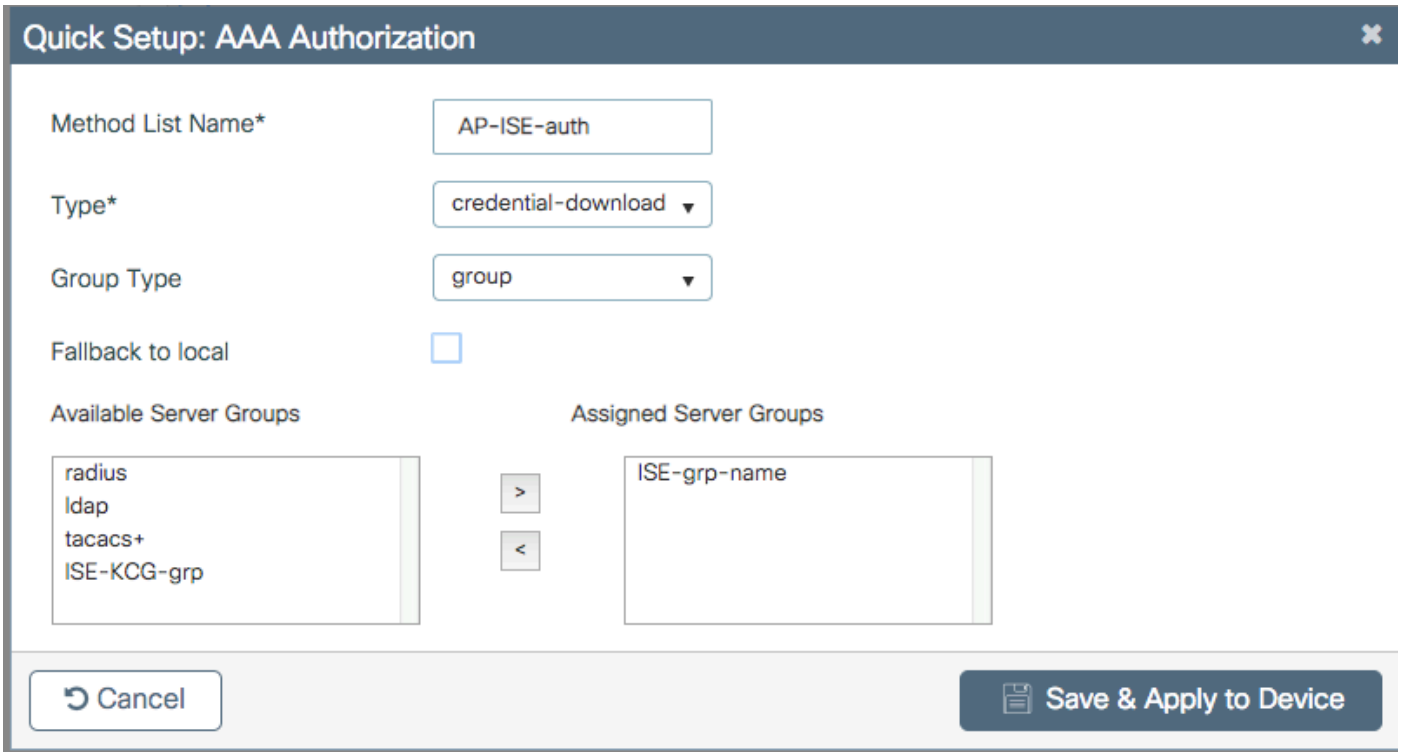
Pour qu'ISE authentifie l'adresse MAC du point d'accès en tant que terminaux, remplacez MAC-Filtering par MAC.



Étape 3. Créez une liste de méthodes de téléchargement des informations d'identification d'autorisation.

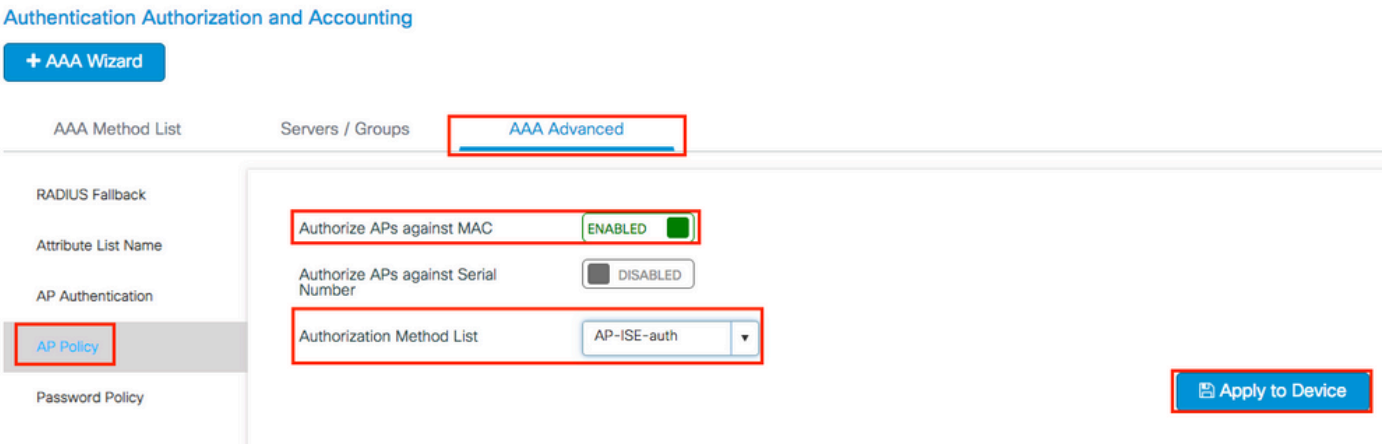
Accédez à Configuration > Security > AAA > AAA Method List > Authorization > + Add.





Étape 4. Activez l'autorisation MAC AP.

Accédez à Configuration > Security > AAA > AAA Advanced > AP Policy. Activez Authorize APs against MAC et sélectionnez la liste de méthodes d'autorisation créée à l'étape 3.



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 authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

Configuration ISE

Étape 1. Pour ajouter un WLC 9800 à ISE :

Déclarer le WLC 9800 sur ISE

Choisissez de configurer l'adresse MAC de l'AP en fonction de l'authentification avec les étapes requises :

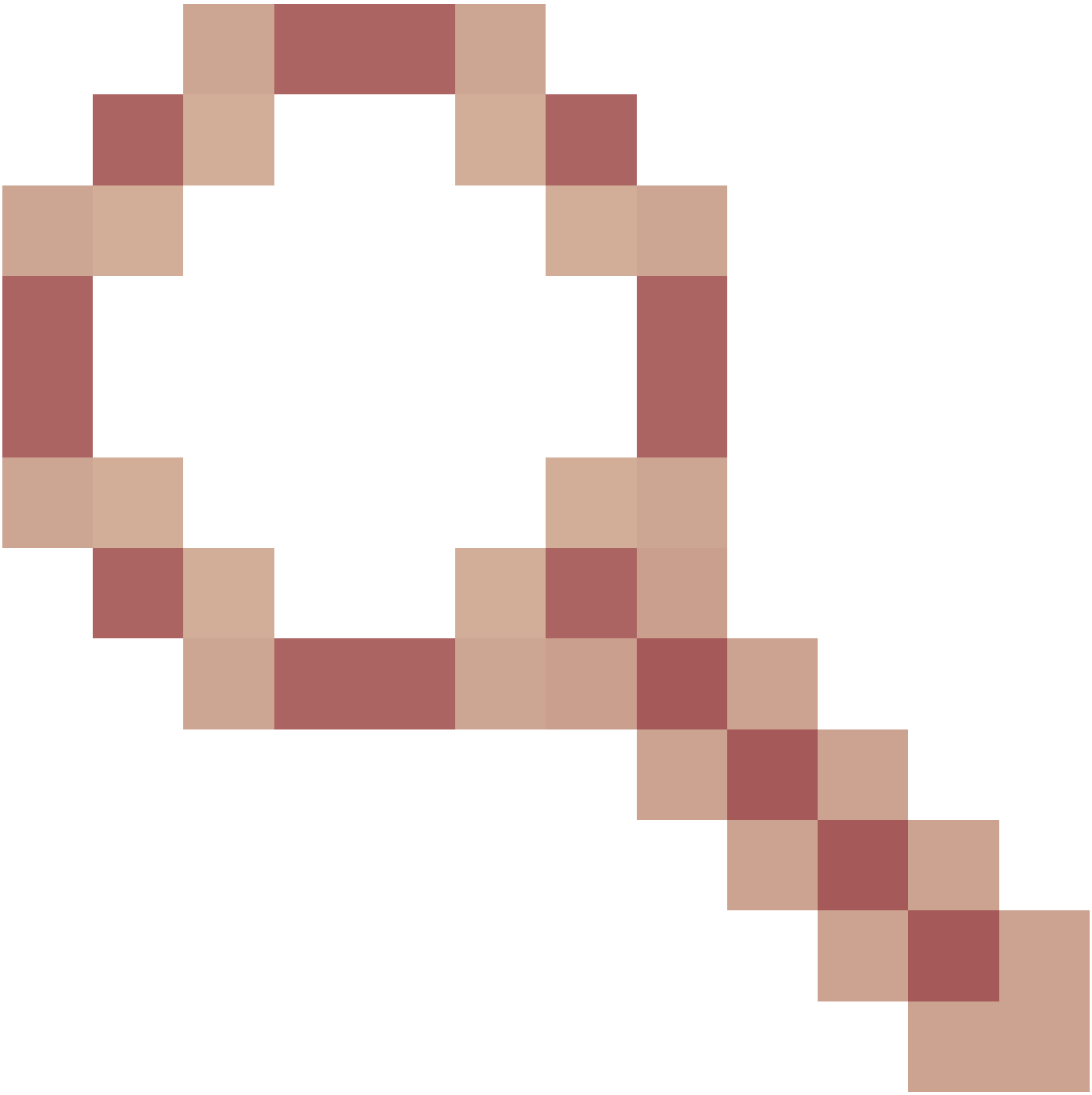
Configurez USE pour authentifier l'adresse MAC en tant que terminaux

Configurer ISE pour authentifier l'adresse MAC comme nom d'utilisateur/mot de passe

Configurer ISE pour authentifier les adresses MAC en tant que terminaux

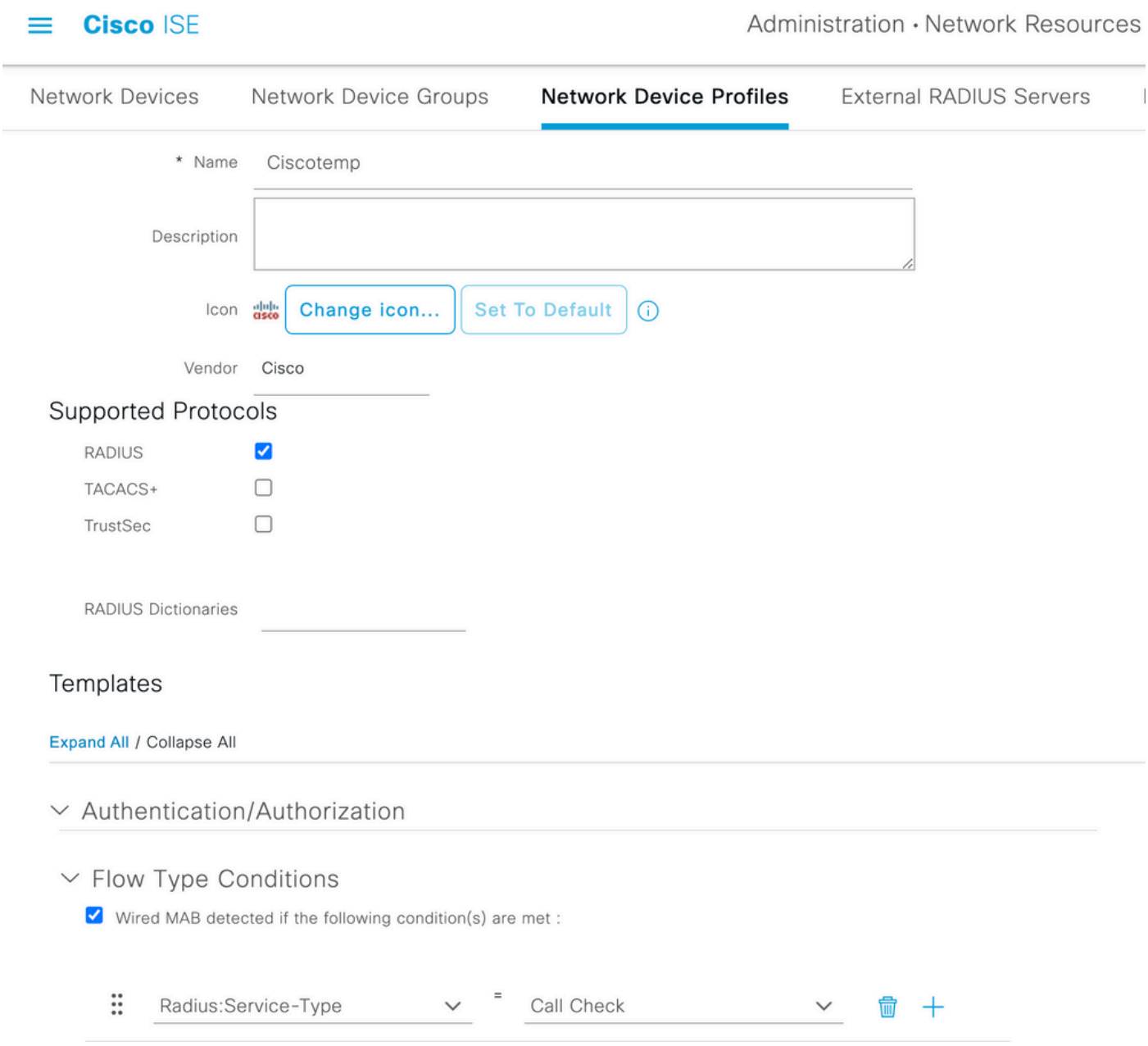
Étape 2. (Facultatif) Créez un groupe d'identité pour les points d'accès.

Comme le 9800 n'envoie pas l'attribut NAS-port-Type avec l'autorisation AP (bogue Cisco IDCSCvy74904),



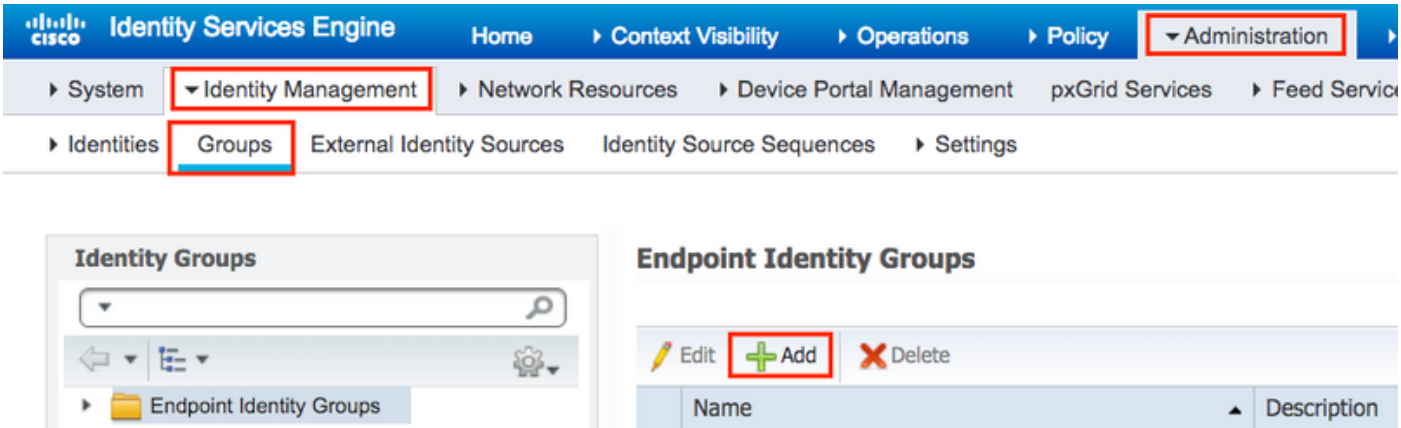
ISE ne reconnaît pas une autorisation AP comme un workflow MAB. Par conséquent, il n'est pas possible d'authentifier un AP si l'adresse MAC de l'AP est placée dans la liste des points d'extrémité, sauf si vous modifiez les flux de travail MAB pour ne pas exiger l'attribut NAS-PORT-type sur ISE.

Accédez à Administrator > Network device profile et créez un nouveau profil de périphérique. Activez RADIUS et ajoutez service-type=call-check pour Wired MAB. Vous pouvez copier le reste du profil Cisco d'origine. L'idée est d'avoir aucune condition de type de port nas pour le MAB filaire.

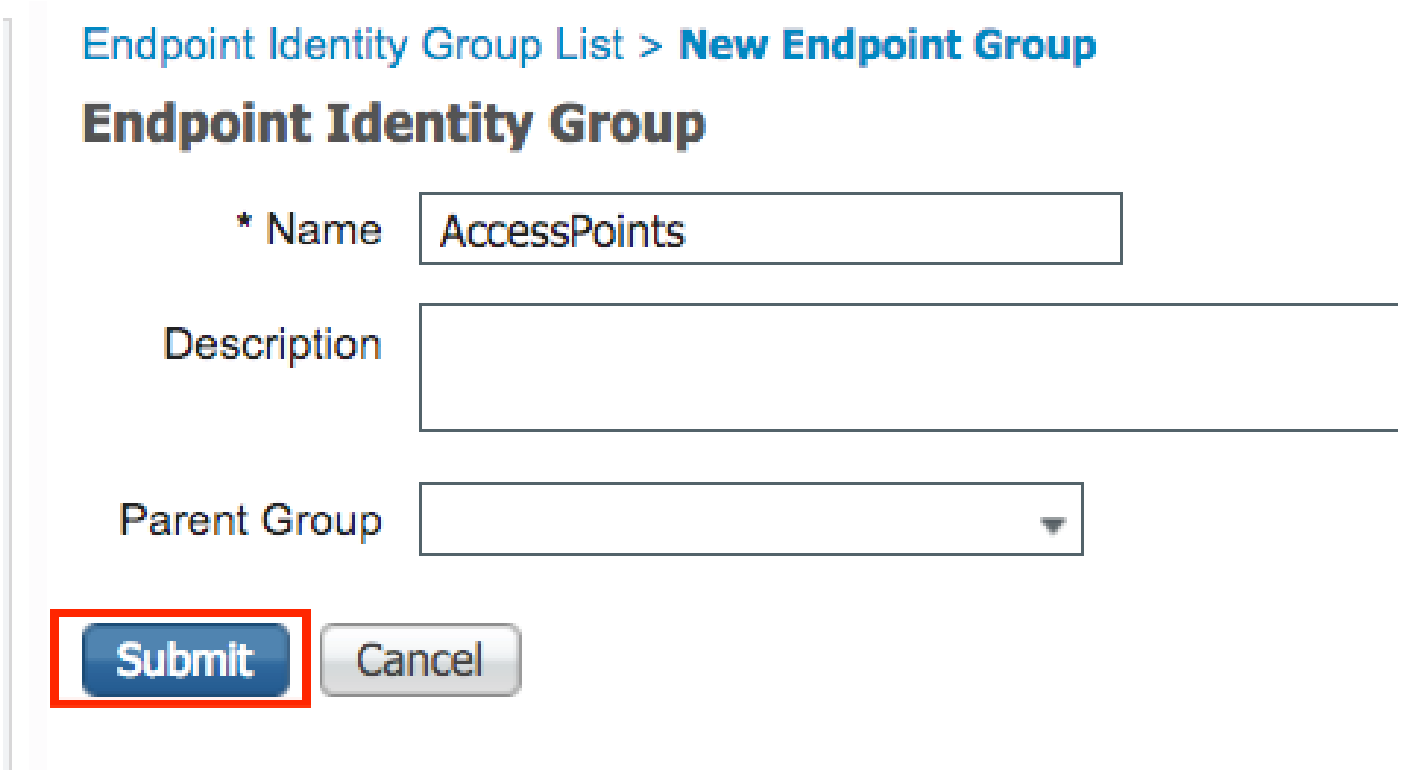


Retournez à l'entrée de périphérique réseau pour le 9800 et définissez son profil sur le profil de périphérique nouvellement créé.

Accédez à Administration > Identity Management > Groups > Endpoint Identity Groups > + Add.

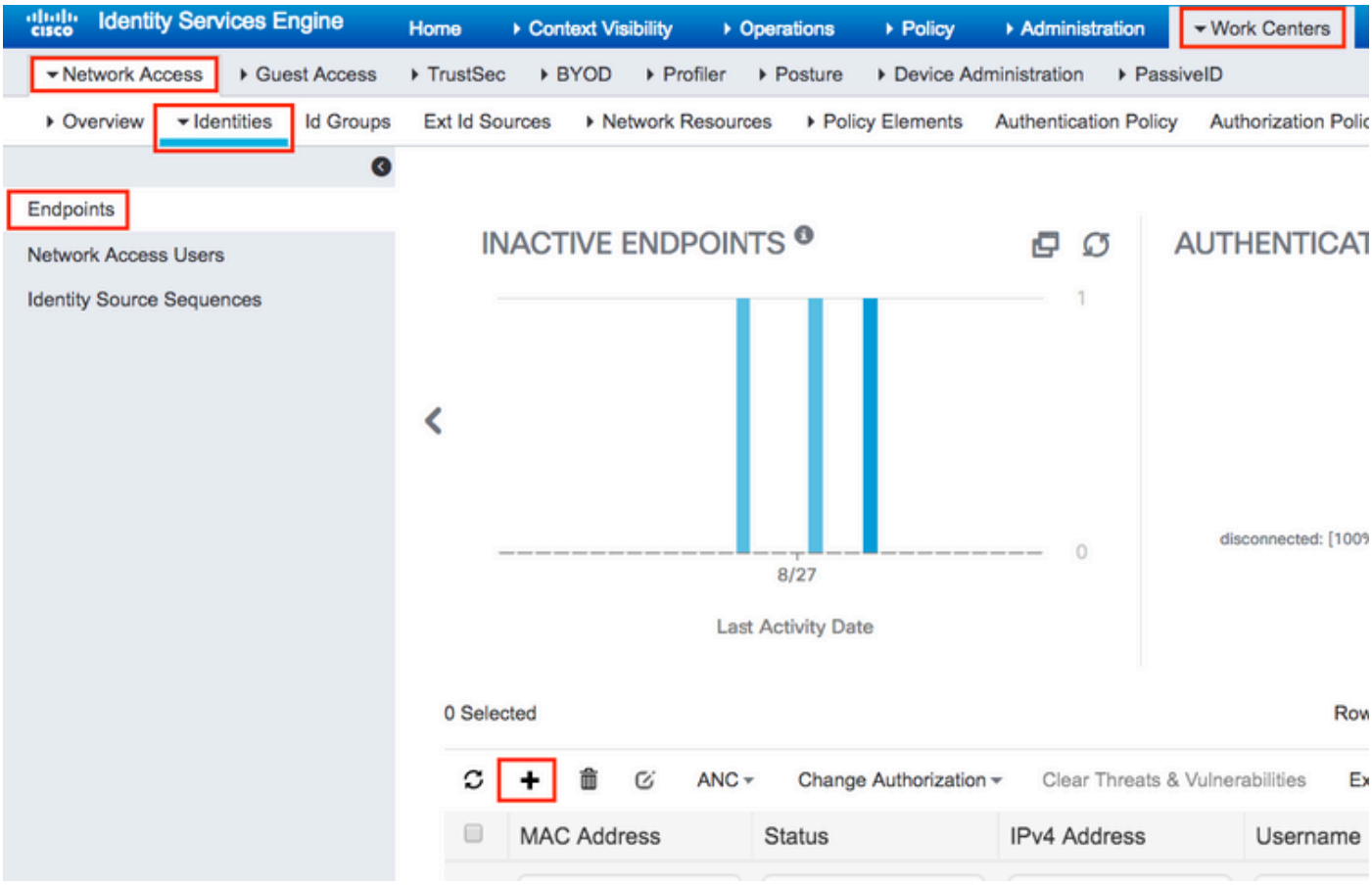


Choisissez un nom et cliquez sur Submit.

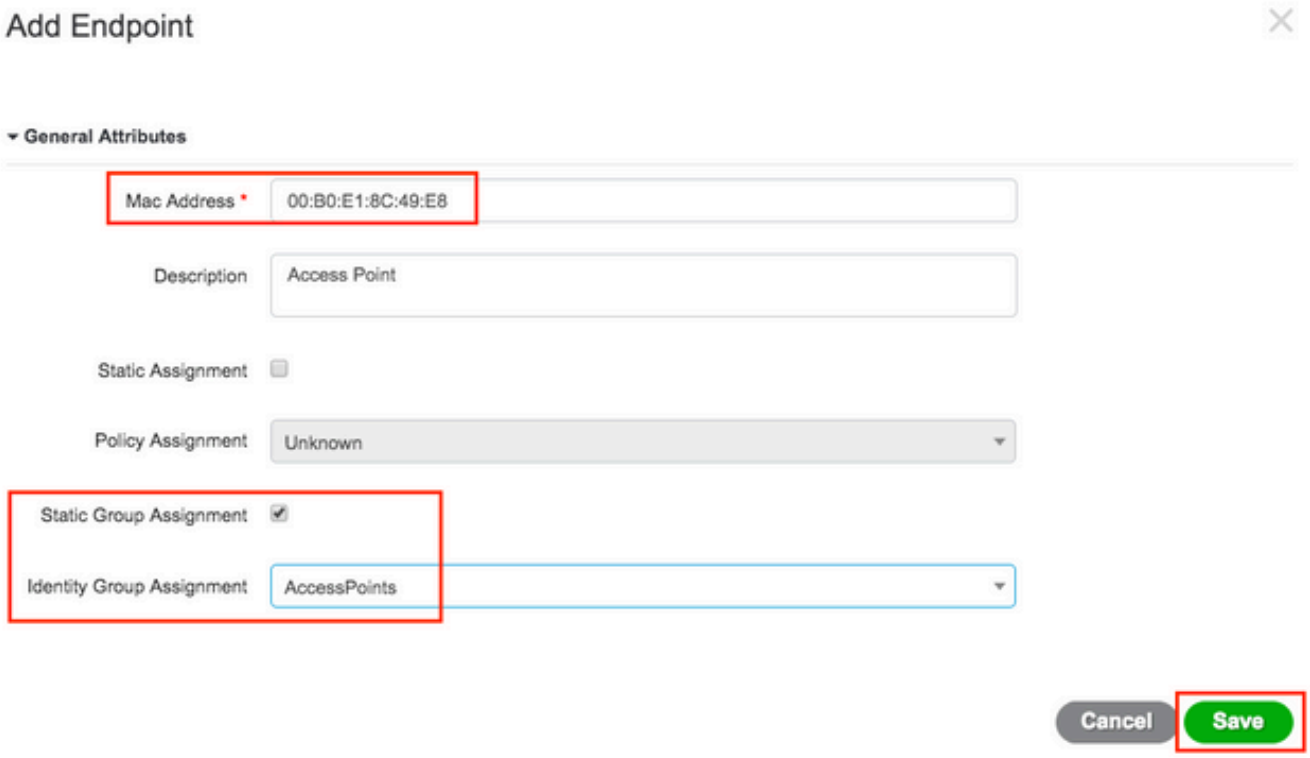


Étape 3. Ajoutez l'adresse MAC Ethernet AP à son groupe d'identité de point d'extrémité.

Accédez à Work Centers > Network Access > Identities > Endpoints > +.

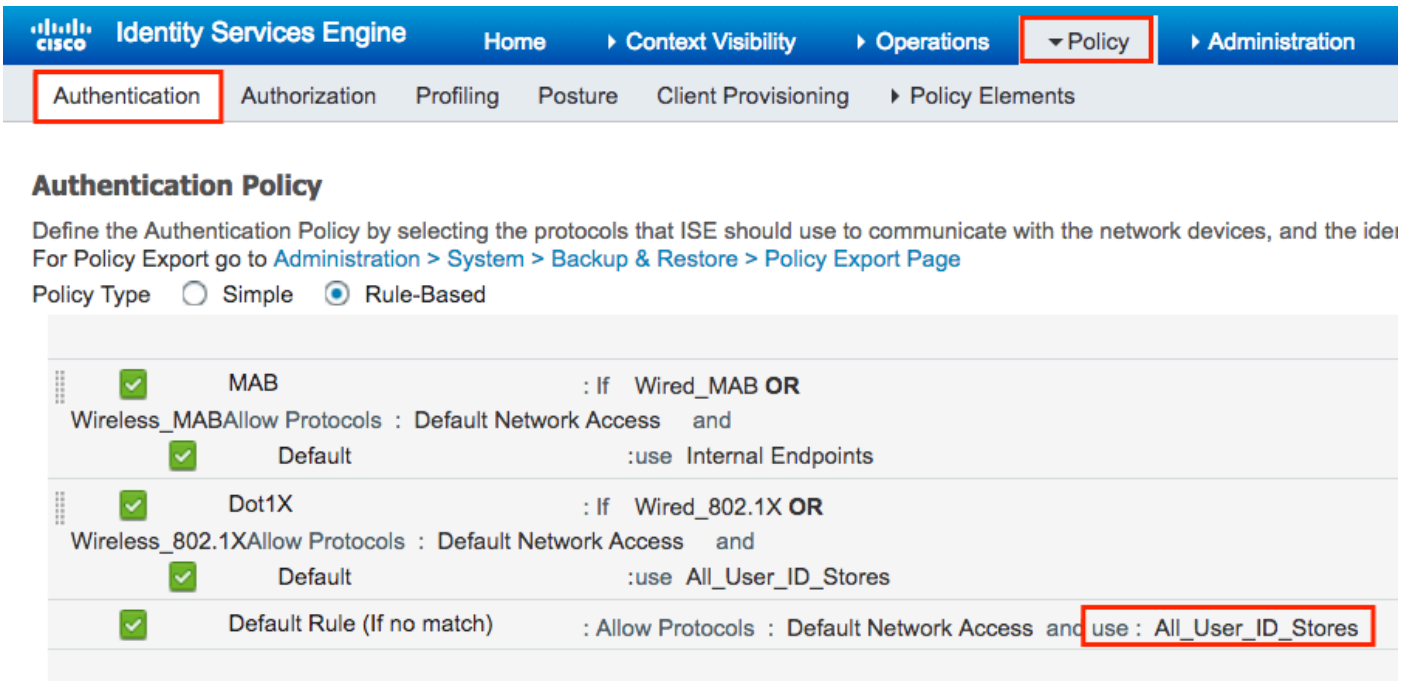


Saisissez les informations requises.

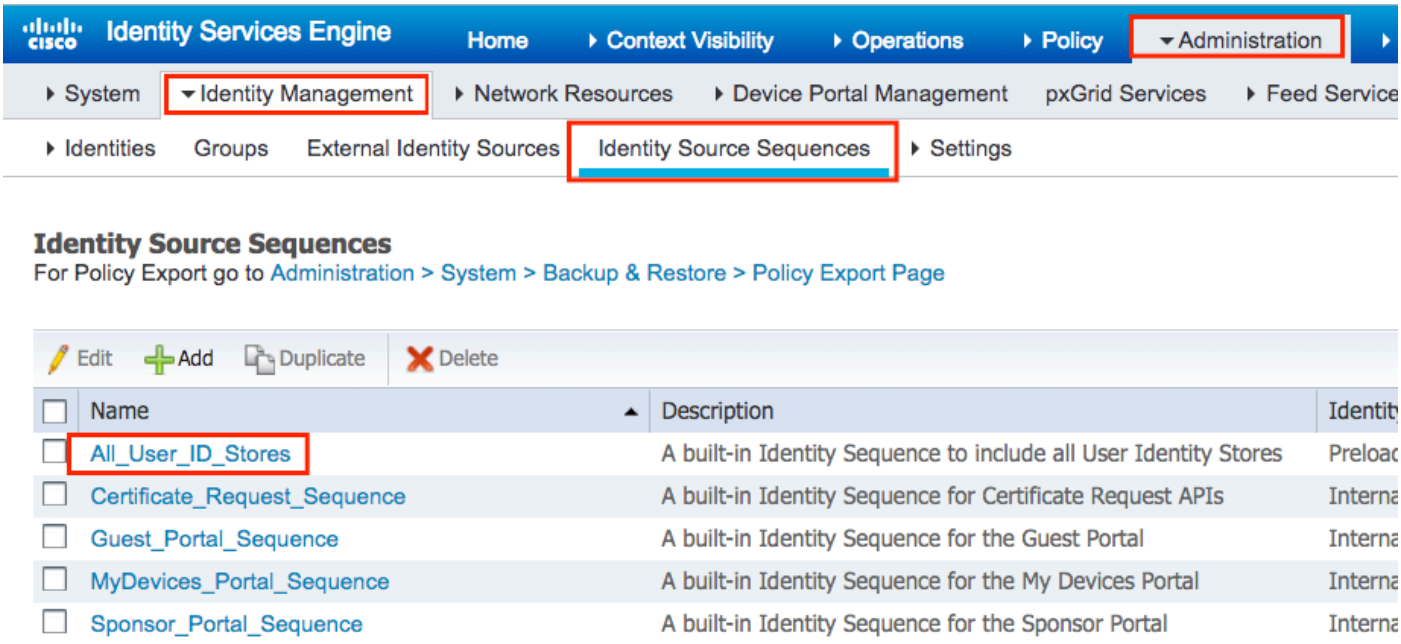


Étape 4. Vérifiez le magasin d'identités utilisé sur votre règle d'authentification par défaut qui contient les points de terminaison internes.

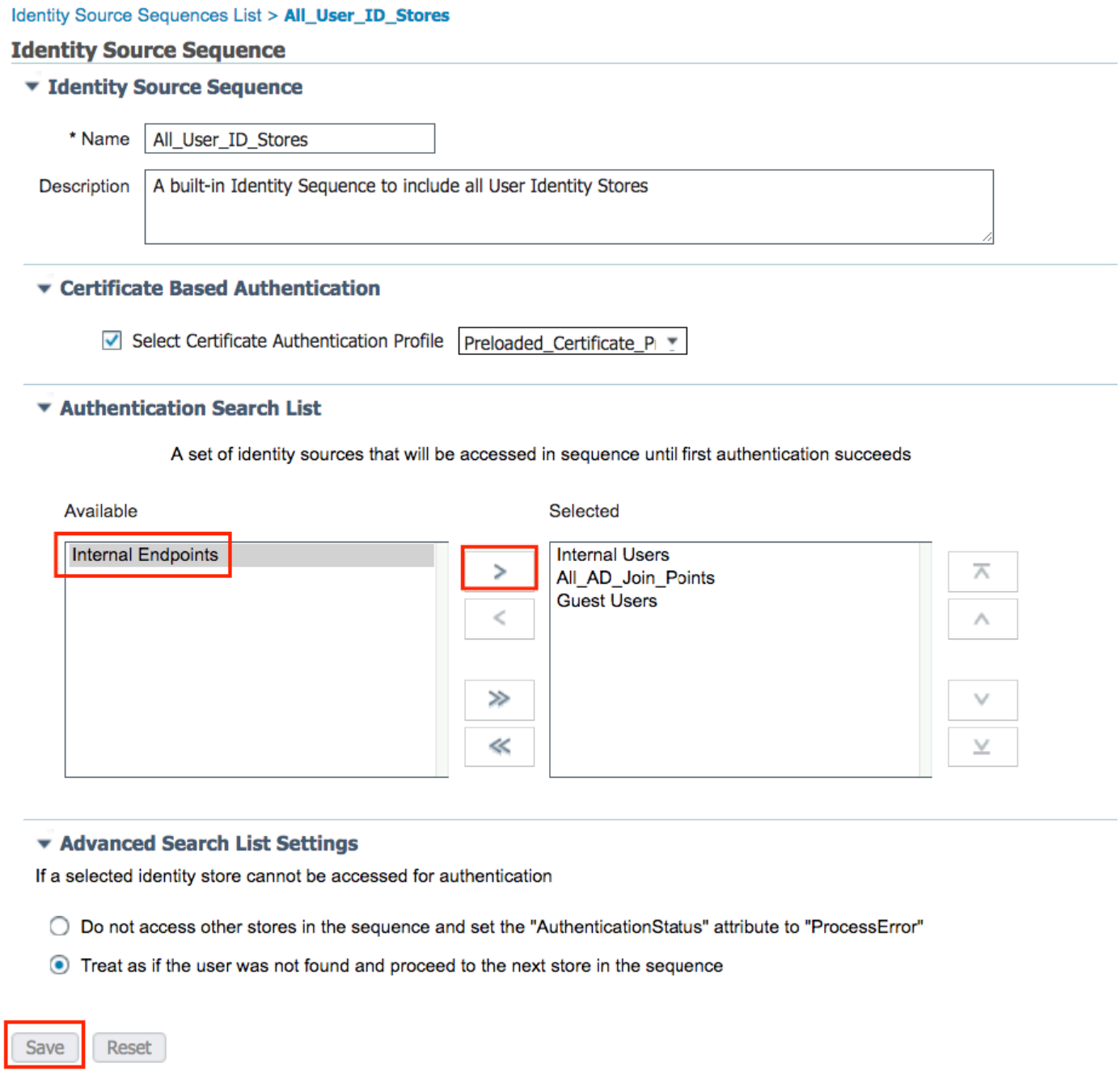
A. Accédez à Policy > Authentication et prenez note de la banque d'identités.



B. Accédez à Administration > Identity Management > Identity Source Sequences > Identity Name.



C. Assurez-vous que les terminaux internes lui appartiennent. Sinon, ajoutez-les.



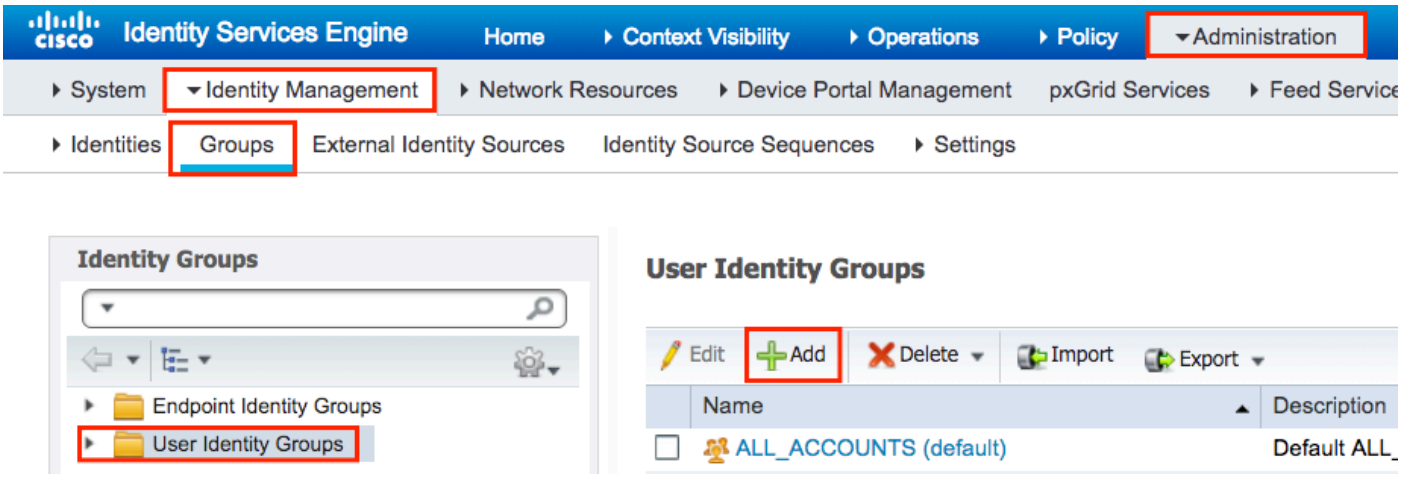
Configurer ISE pour authentifier l'adresse MAC comme nom d'utilisateur/mot de passe

Cette méthode est déconseillée car elle nécessite des stratégies de mot de passe inférieures pour autoriser le même mot de passe que le nom d'utilisateur.

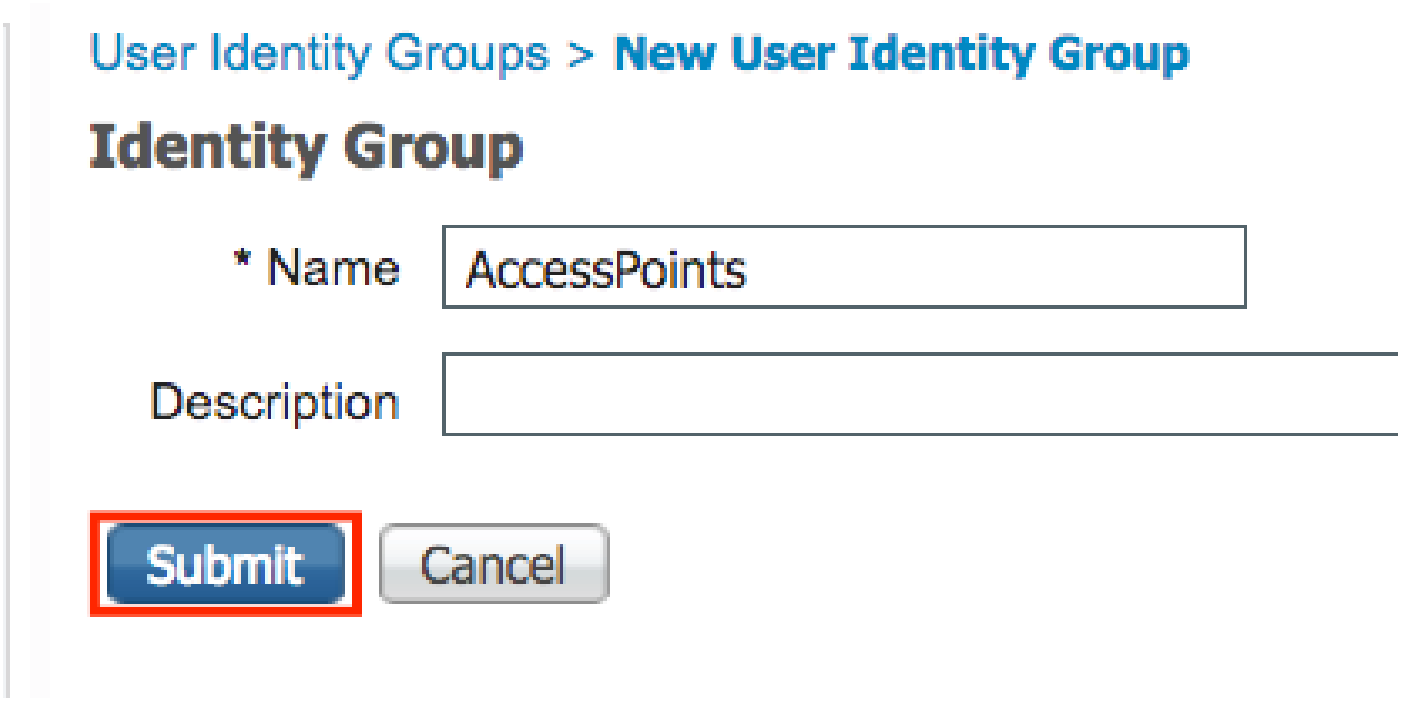
Il peut toutefois s'agir d'une solution de contournement si vous ne pouvez pas modifier votre profil de périphérique réseau.

Étape 2. (Facultatif) Créez un groupe d'identité pour les points d'accès.

Accédez à Administration > Identity Management > Groups > User Identity Groups > + Add.

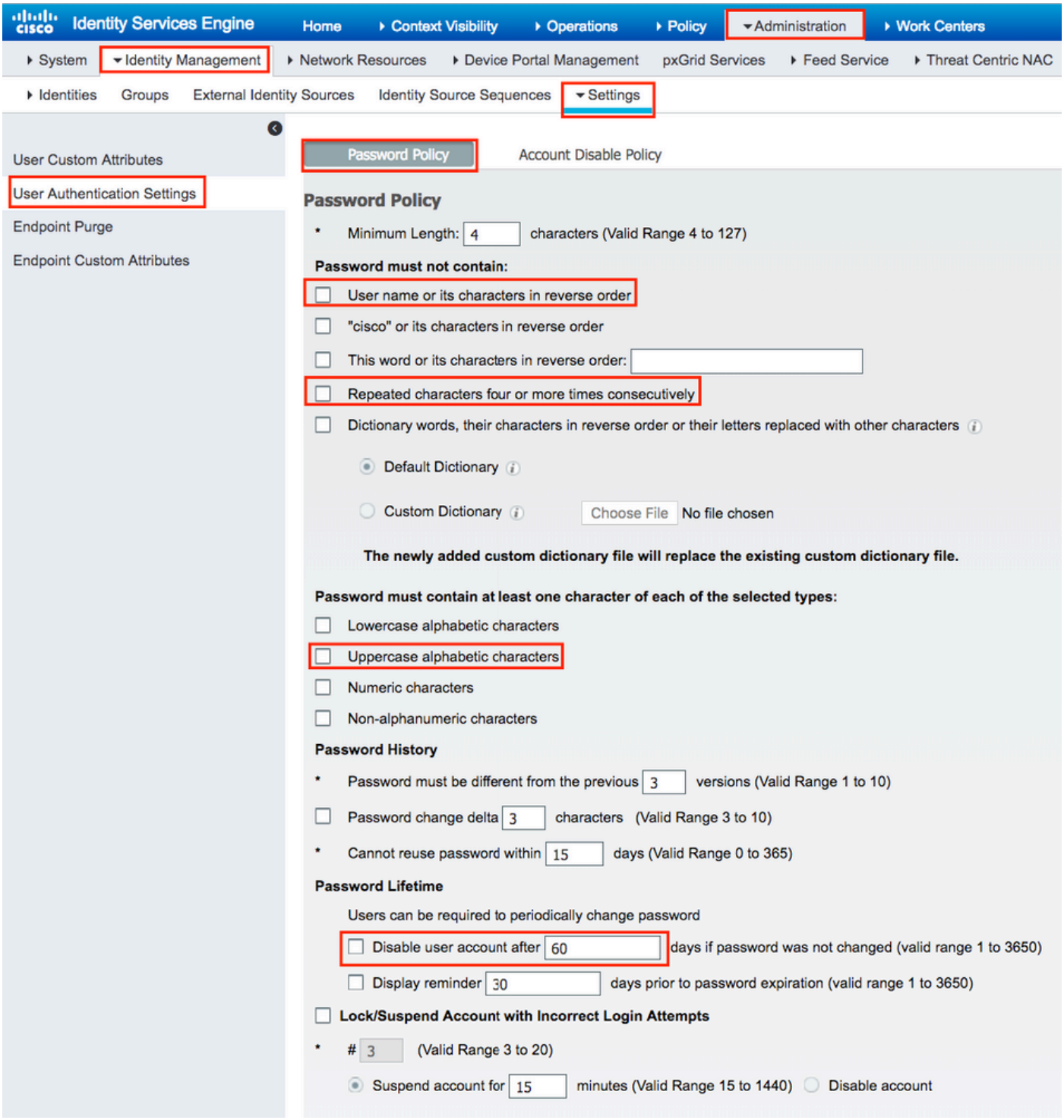


Choisissez un nom et cliquez sur Submit.



Étape 3. Vérifiez que votre stratégie de mot de passe actuelle vous permet d'ajouter une adresse MAC comme nom d'utilisateur et mot de passe.

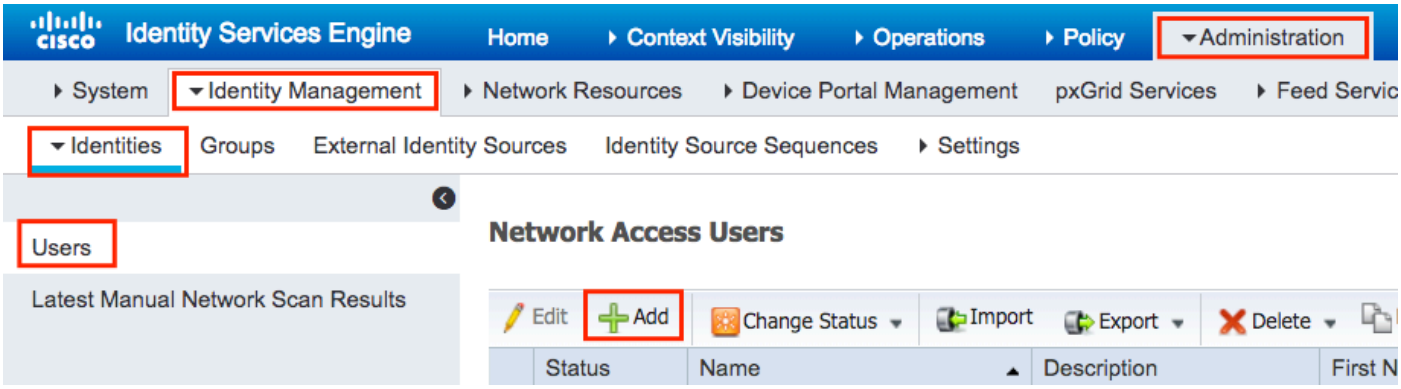
Accédez à Administration > Identity Management > Settings > User Authentication Settings > Password Policy et assurez-vous que ces options au moins sont désactivées :



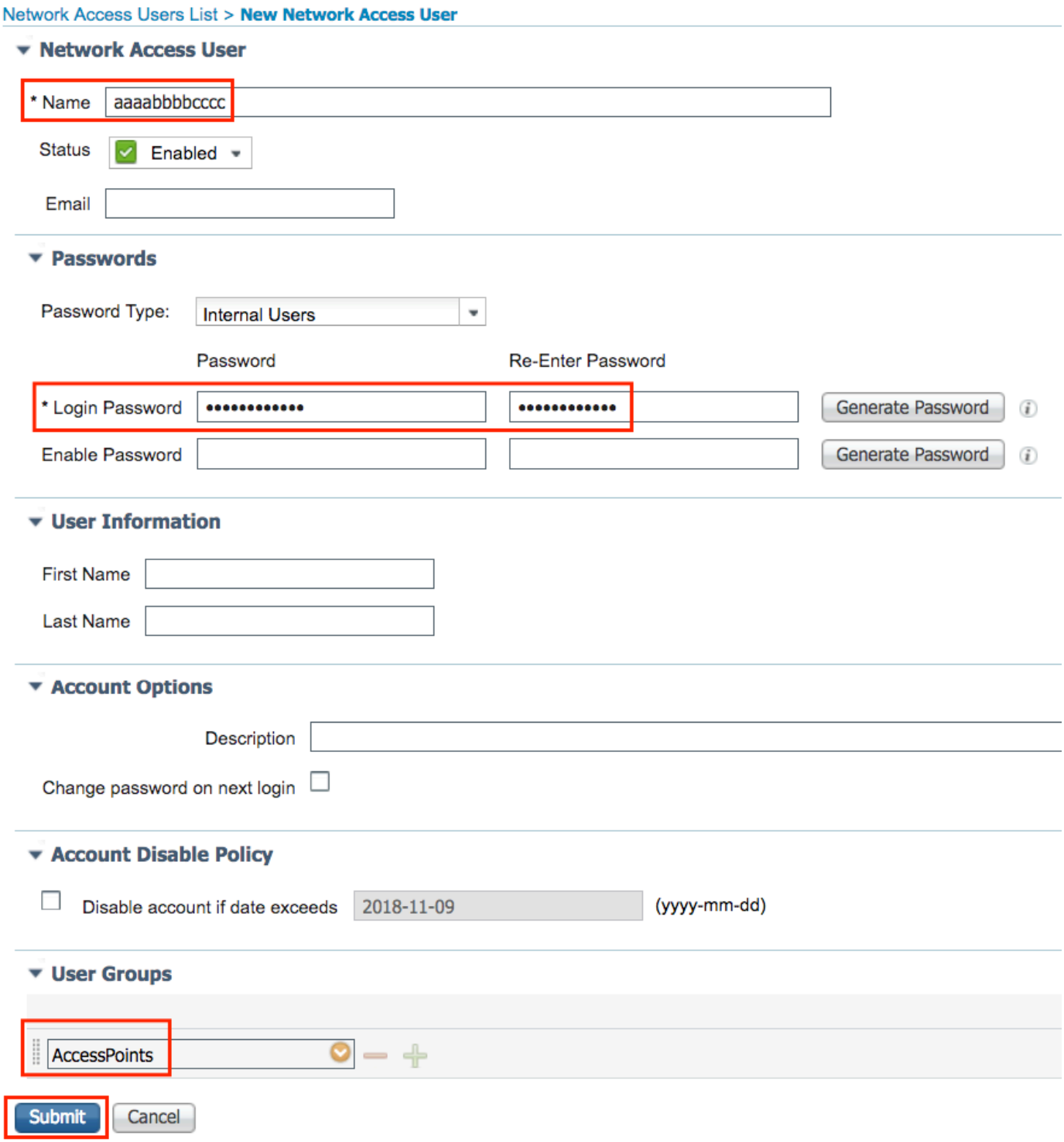
Remarque : vous pouvez également désactiver l'option Disable user account after XX days si le mot de passe n'a pas été modifié.Comme il s'agit d'une adresse MAC, le mot de passe ne change jamais.

Étape 4. Ajoutez l'adresse MAC Ethernet AP.

Accédez à Administration > Identity Management > Identities > Users > + Add.



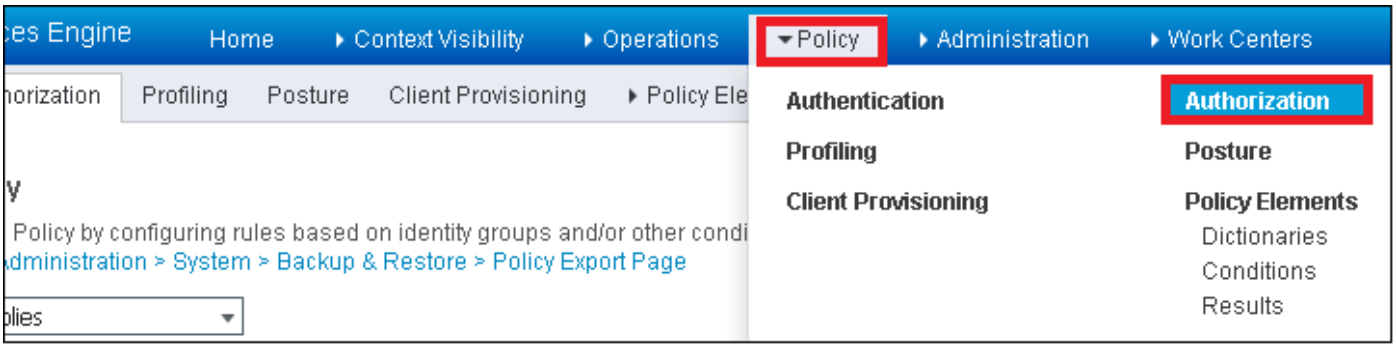
Saisissez les informations requises.



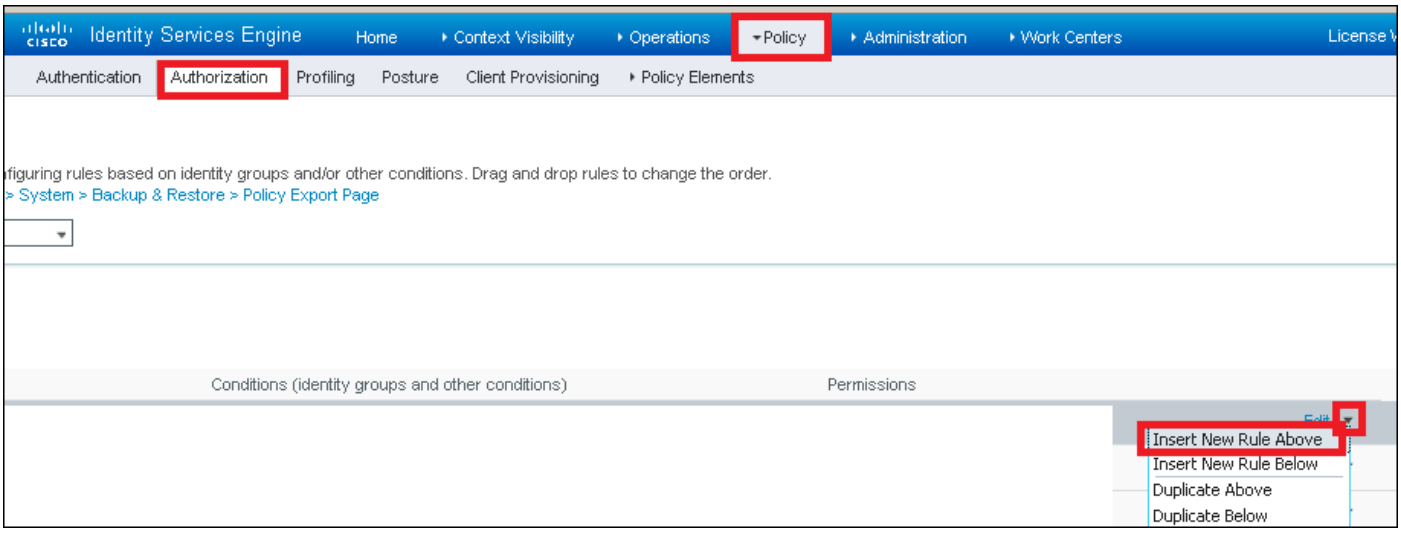
Remarque : les champs Nom et Mot de passe de connexion doivent correspondre à l'adresse MAC Ethernet du point d'accès, tous en minuscules et sans séparateur.

Stratégie d'autorisation pour authentifier les AP

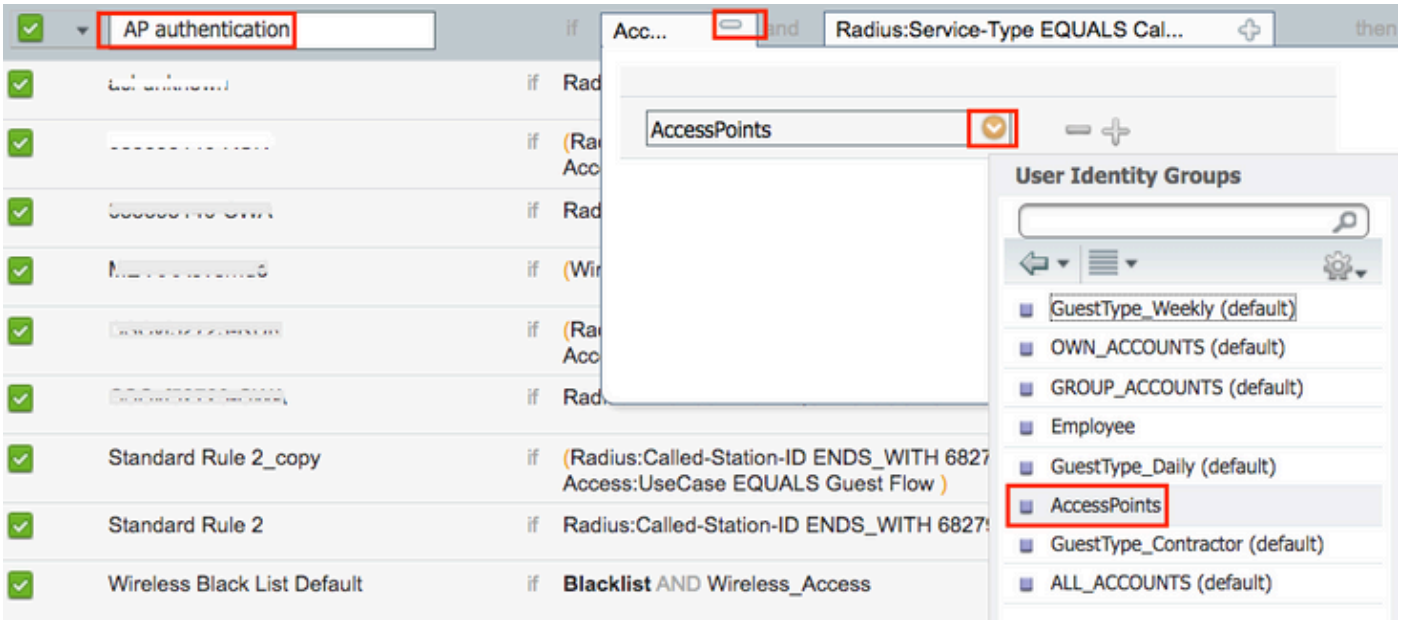
Accédez à Policy > Authorization comme indiqué dans l'image.



Insérez une nouvelle règle comme illustré dans l'image.

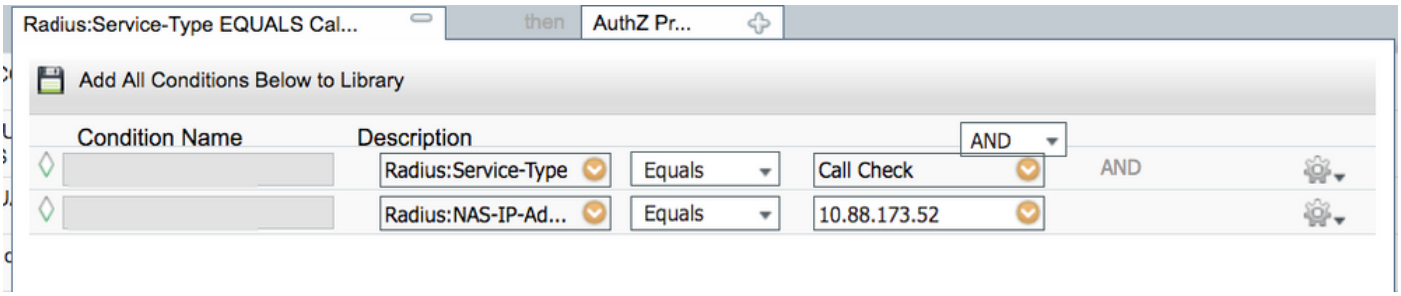


Commencez par sélectionner un nom pour la règle et le groupe Identité dans lequel le point d'accès est stocké (AccessPoints). Sélectionnez User Identity Groups si vous avez décidé d'authentifier l'adresse MAC en tant que nom d'utilisateur et mot de passe ou Endpoint Identity Groups si vous choisissez d'authentifier l'adresse MAC AP en tant que points d'extrémité.

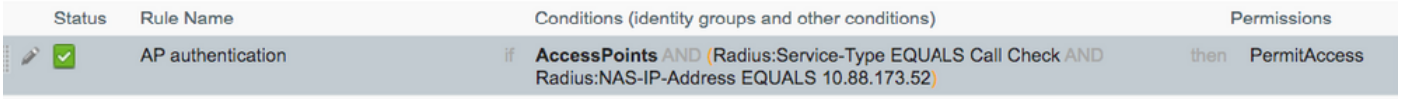


Ensuite, sélectionnez d'autres conditions qui font que le processus d'autorisation est soumis à cette règle. Dans cet exemple, le processus d'autorisation atteint cette règle s'il utilise la

vérification d'appel de type service et que la demande d'authentification provient de l'adresse IP 10.88.173.52.



Enfin, sélectionnez le profil d'autorisation attribué aux clients qui ont atteint cette règle, cliquez surTerminer et enregistrez-le comme indiqué dans l'image.



Remarque : les AP qui ont déjà rejoint le contrôleur ne perdent pas leur association. Cependant, si, après l'activation de la liste d'autorisation, ils perdent la communication avec le contrôleur et tentent de se joindre à nouveau, ils passent par le processus d'authentification. Si leurs adresses MAC ne sont pas répertoriées localement ou dans le serveur RADIUS, ils ne peuvent pas rejoindre le contrôleur.

Vérifier

Vérifiez si le WLC 9800 a activé la liste d'authentification AP.

<#root>

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

Vérifiez la configuration du rayon :

<#root>

```
#
show run aaa
```

Dépannage

Le WLC 9800 offre des fonctionnalités de suivi ALWAYS-ON. Cela garantit que toutes les erreurs liées à la jonction AP, les messages de niveau d'avertissement et d'avertissement sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une condition d'échec après qu'il se soit produit.

Remarque : le volume de journaux générés varie rétroactivement de quelques heures à plusieurs jours.

Pour afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter via SSH/Telnet au WLC 9800 à l'aide de ces étapes. (Veillez à consigner la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du contrôleur de sorte que vous puissiez suivre les journaux dans l'heure jusqu'à quand le problème s'est produit.

```
# show clock
```

Étape 2. Collectez les syslogs à partir de la mémoire tampon du contrôleur ou du syslog externe, comme dicté par la configuration système. Cela fournit un aperçu rapide de l'intégrité du système et des erreurs, le cas échéant.

```
# show logging
```

Étape 3. Vérifiez si les conditions de débogage sont activées.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Trace Configs:


Packet Infra debugs:

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

Remarque : si une condition est répertoriée, cela signifie que les traces sont consignées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmenterait le volume de 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 radio 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 de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (adresse MAC du client dans ce cas).

Étape 5. Assurez-vous 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 aussi augmenter ce délai pour qu’il atteigne 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 dans la session du 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 le débogage si le problème est reproduit avant la fin du temps de surveillance par défaut ou configuré.

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

Une fois le temps de surveillance écoulé ou le débogage sans fil arrêté, le WLC 9800 génère un fichier local avec le nom :

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Étape 9. Recueillir le fichier de l'activité de l'adresse MAC. Il est possible de copier le fichier de suivi RA .log sur un serveur externe ou d'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 vous ne trouvez toujours pas la cause première, collectez les journaux internes, qui peuvent vous offrir une vue plus détaillée des journaux de niveau de débogage. Vous n'avez pas besoin de déboguer à nouveau le client, car vous n'avez qu'à examiner 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 journalisation 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. Supprimez les conditions de débogage:

```
# clear platform condition all
```

Remarque : assurez-vous de toujours supprimer les conditions de débogage après une session de dépannage.

Références

Joindre des points d'accès maillés au WLC 9800

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.