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

Table des matières

Introduction

Ce document décrit comment configurer un réseau local sans fil (WLAN) avec la sécurité d'authentification MAC sur le WLC Cisco Catalyst 9800.

Conditions préalables

Exigence

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Adresse MAC :
- Contrôleurs sans fil Cisco Catalyst 9800
- Identity Service Engine (ISE)

Composants utilisés

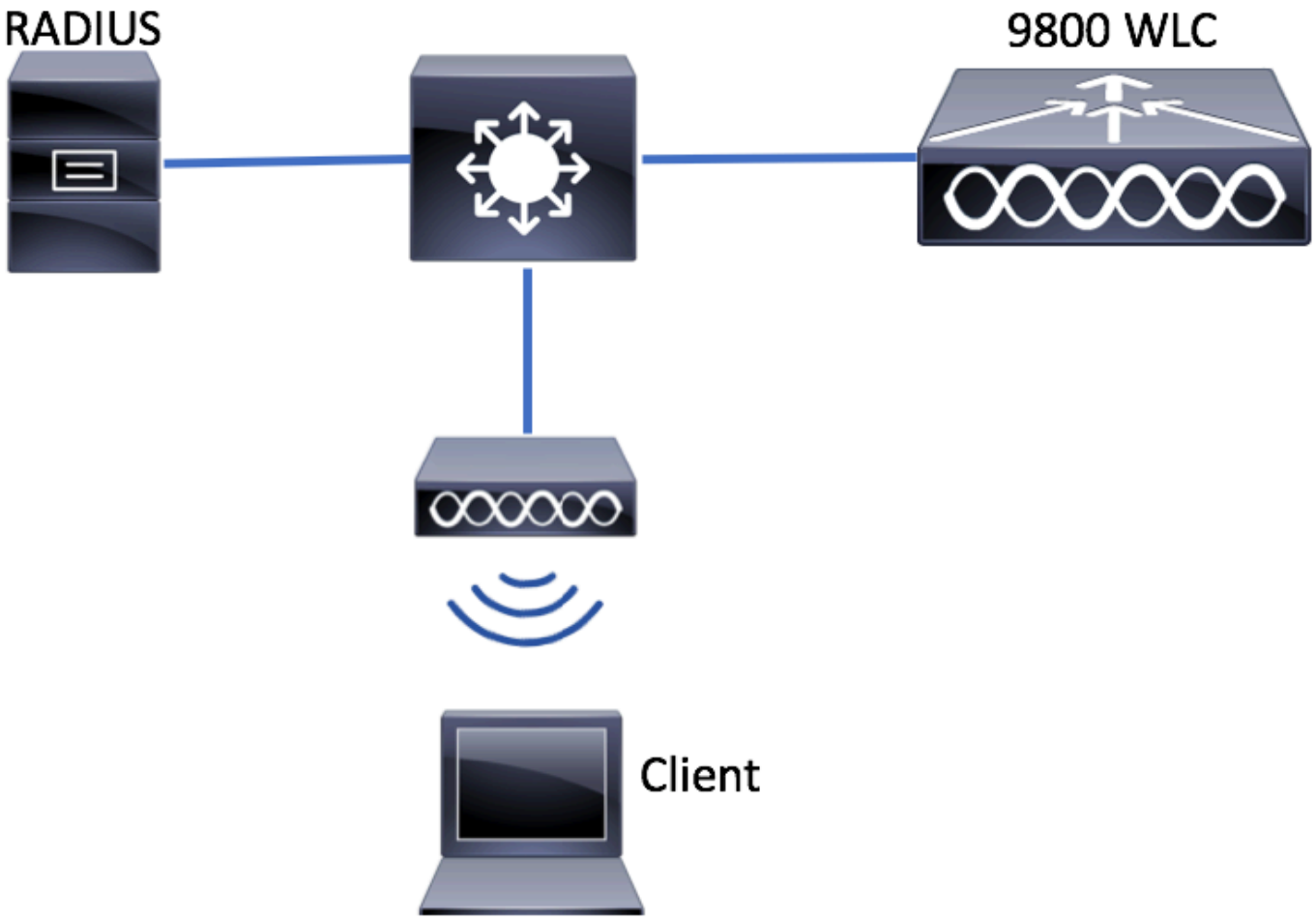
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco IOS® XE Gibraltar v16.12
- 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.

Configurer

Diagramme du réseau



Configuration AAA sur un contrôleur WLC 9800

Authentification des clients avec un serveur externe

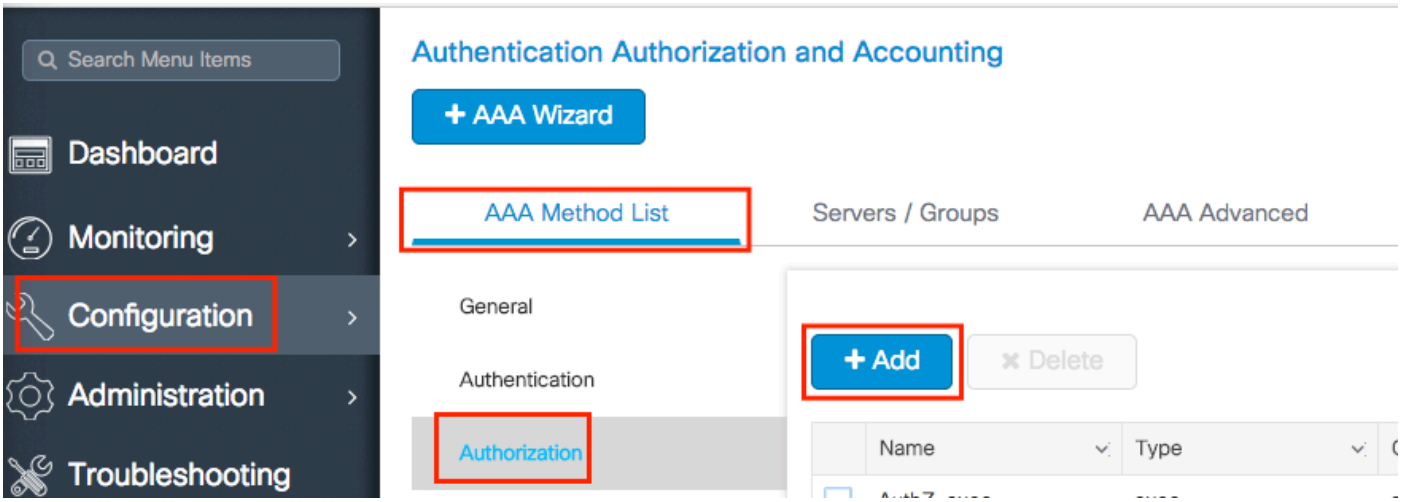
IUG:

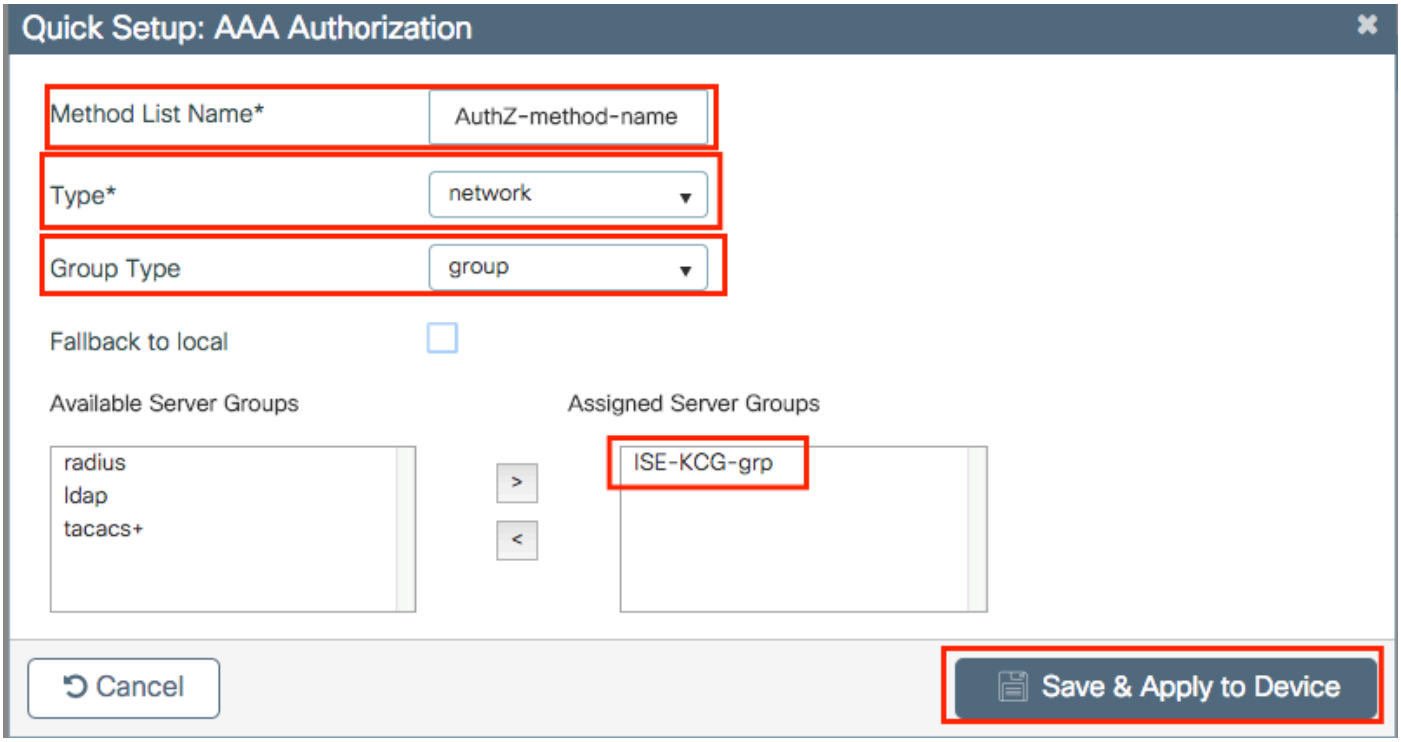
Lisez les étapes 1 à 3 de la section « Configuration AAA sur les WLC 9800 » à partir de ce lien :

[Configuration AAA sur le WLC de la gamme 9800]

Étape 4. Créez une méthode de réseau d'autorisation.

Naviguez jusqu'àConfiguration > Security > AAA > AAA Method List > Authorization > + Addet créez-le.





CLI :

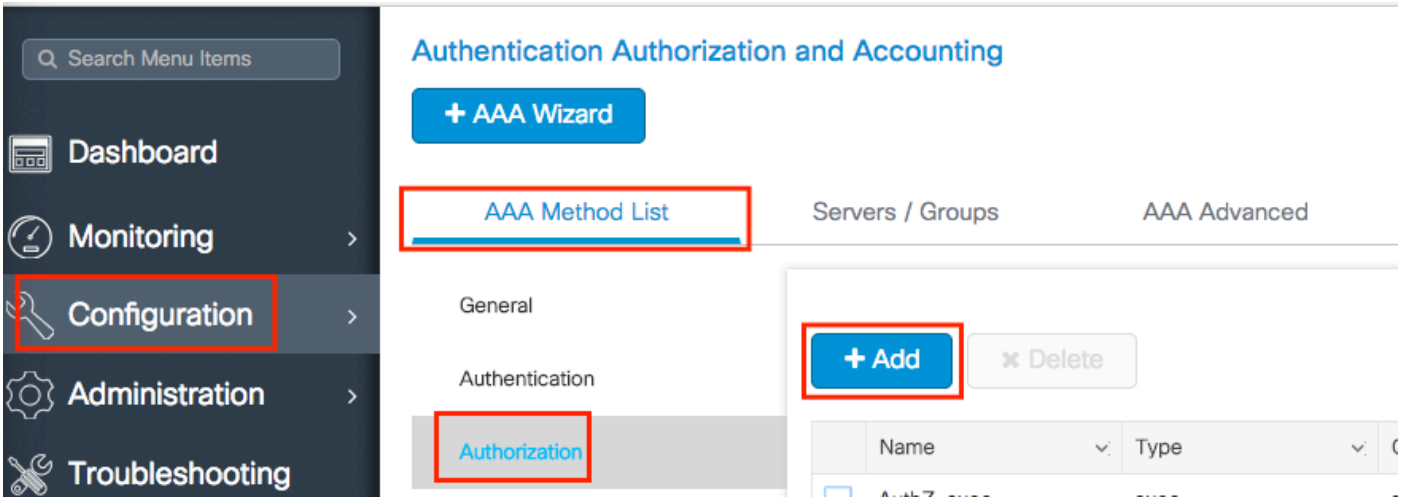
```
# config t
# aaa new-model

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

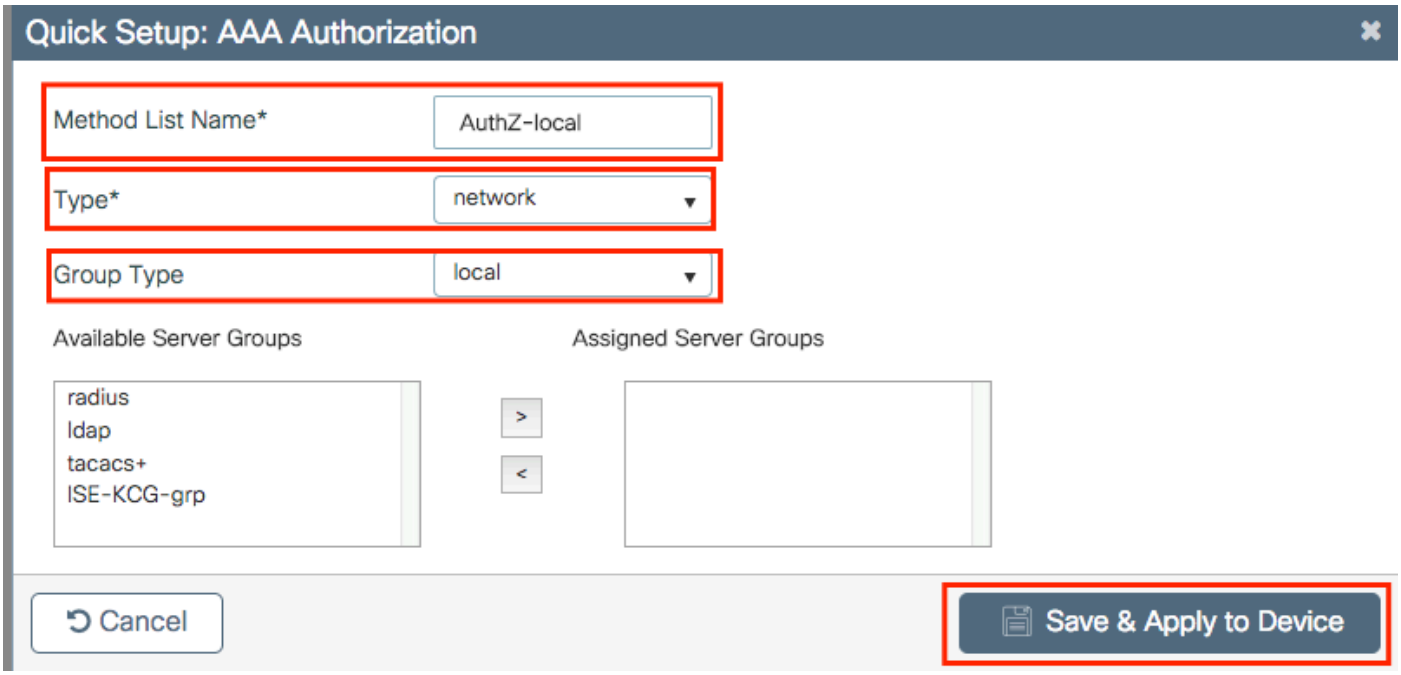
```
# exit

# 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 network <AuthZ-method-name> group <radius-grp-name>
```

Authentifier les clients localement

Créez une méthode de réseau d'autorisation local.

Naviguez jusqu'àConfiguration > Security > AAA > AAA Method List > Authorization > + Addet créez-le.





CLI :

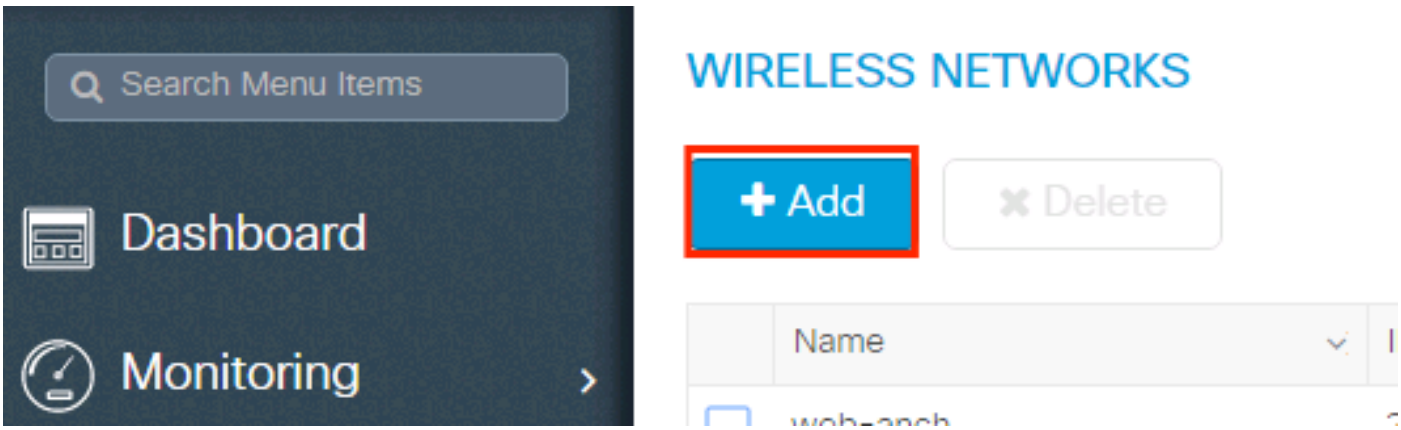
```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

Configuration d’un réseau local sans fil (WLAN)

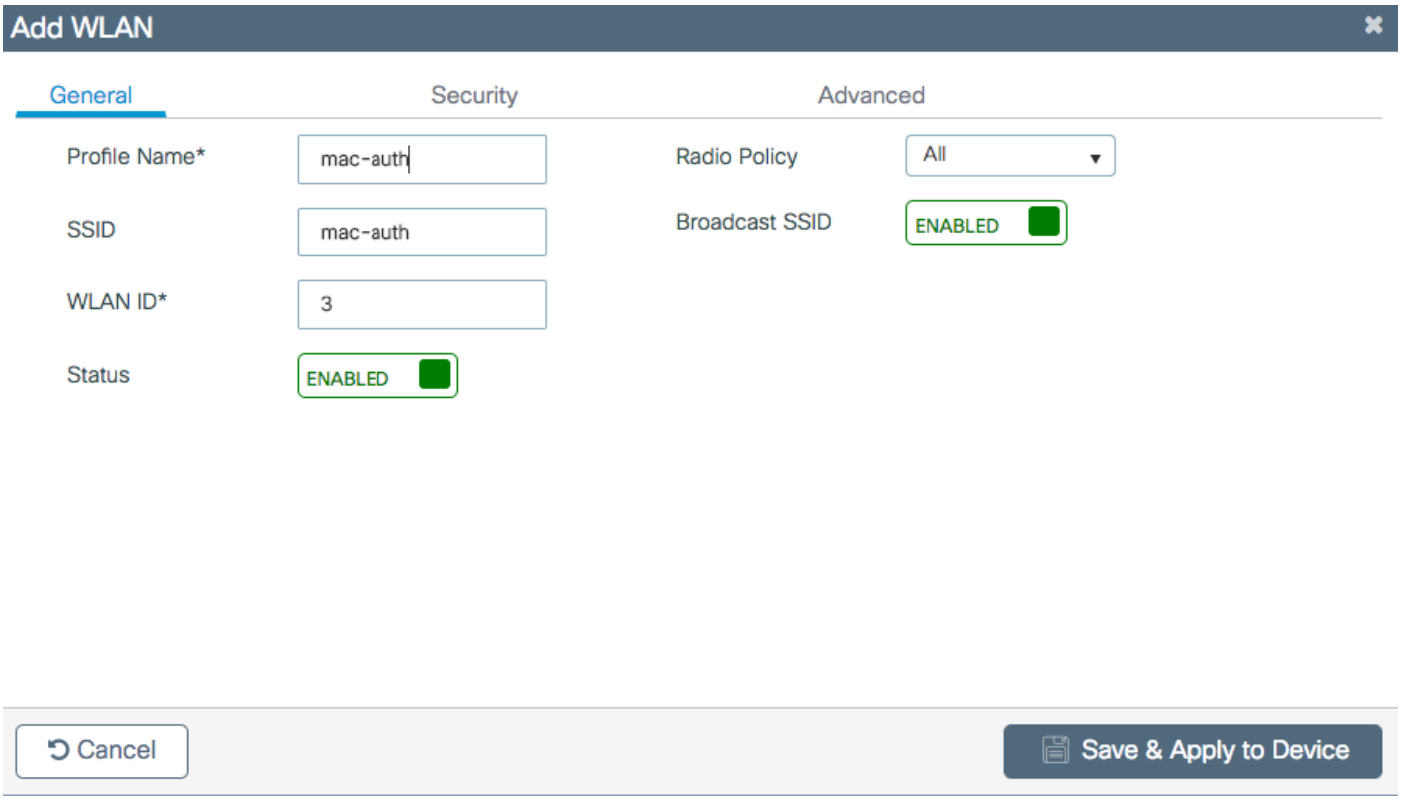
IUG:

Étape 1. Créez le WLAN.

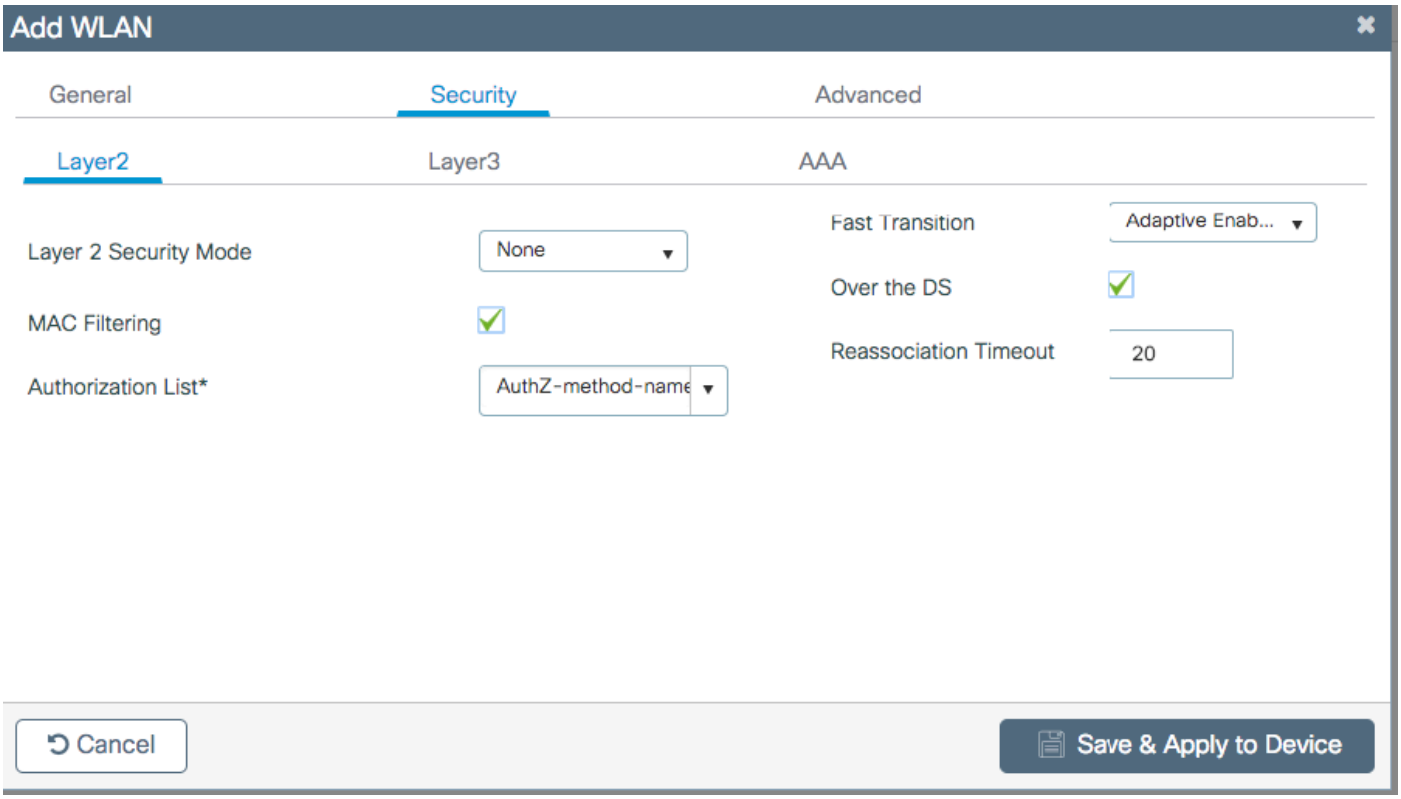
Accédez au réseauConfiguration > Wireless > WLANs > + Addet configurez-le si nécessaire.



Étape 2. Entrez les informations sur le réseau WLAN.



Étape 3. Accédez à l'Securityonglet et désactivezLayer 2 Security Modeet activezMAC Filtering. DansAuthorization List, sélectionnez la méthode d'autorisation créée à l'étape précédente. Cliquez ensuite surSave & Apply to Device.



CLI :

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

Configuration du profil des politiques

Vous devez activeraaa-overridedans le profil de stratégie pour vous assurer que le filtrage MAC par SSID fonctionne correctement.

Configuration du profil de stratégie sur le WLC 9800

Configuration des balises des politiques

Balise de stratégie sur le WLC 9800

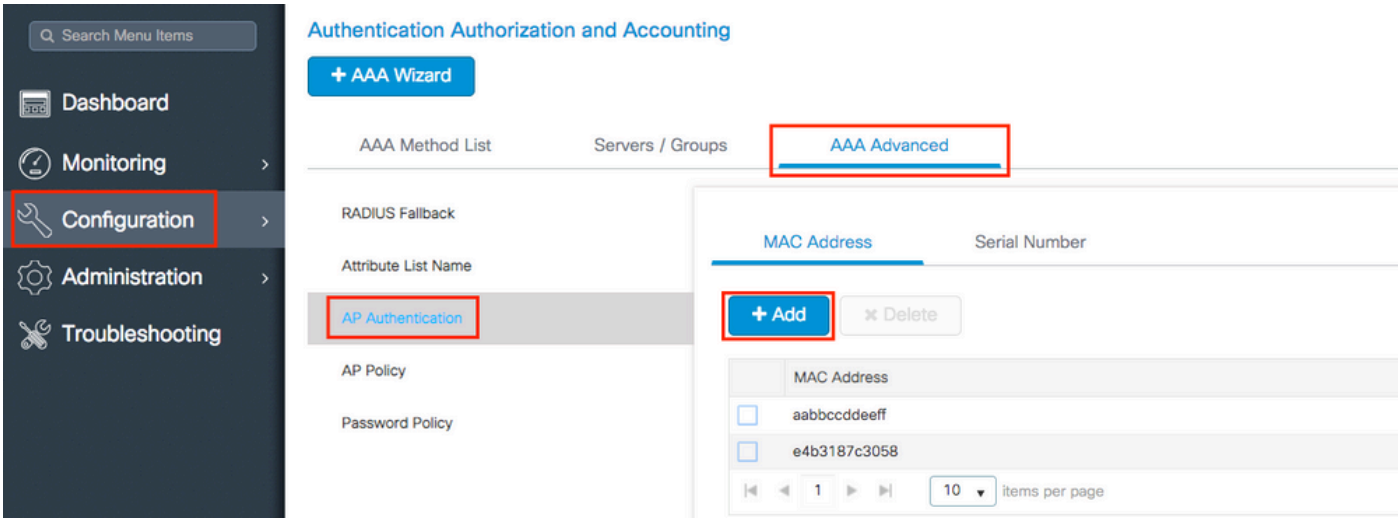
Attribution de balise de stratégie

Attribution de balise de stratégie sur le WLC 9800

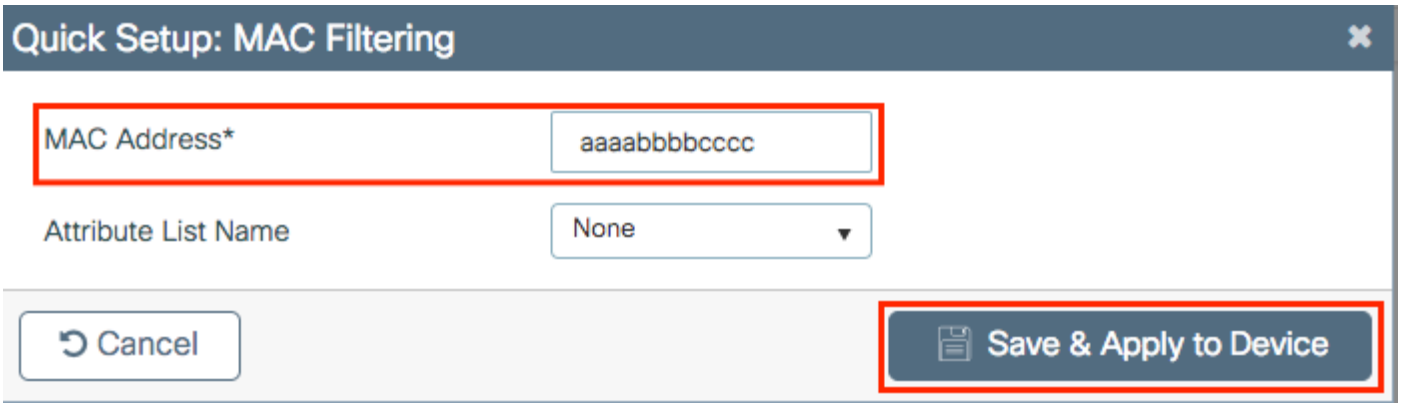
Enregistrez l'adresse MAC autorisée.

Enregistrez localement l'adresse MAC sur le WLC pour l'authentification locale

Accédez àConfiguration > Security > AAA > AAA Advanced > AP Authentication > + Add.



Écrivez l'adresse MAC en minuscules sans séparateur, puis cliquez surSave & Apply to Device.



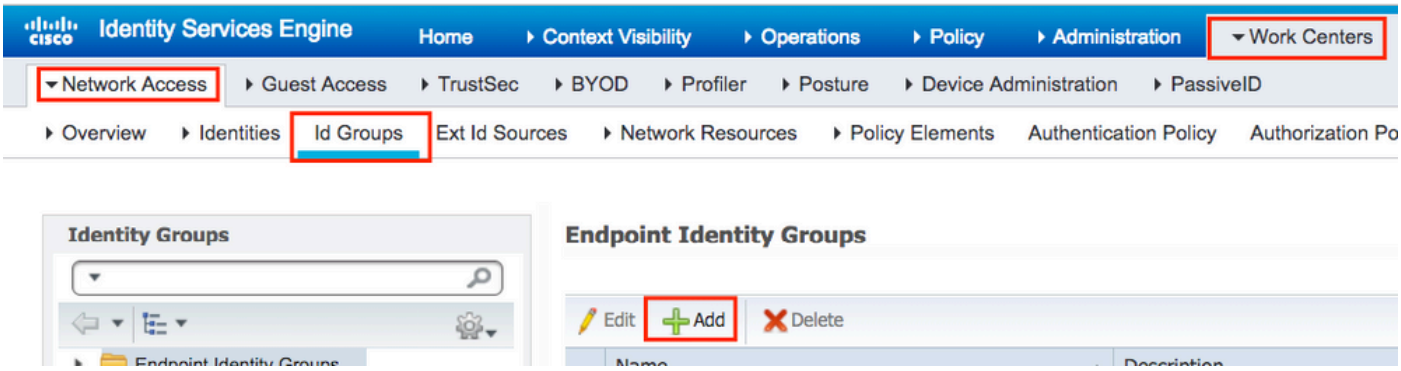
Remarque : dans les versions antérieures à 17.3, l'interface utilisateur Web a modifié tout format MAC que vous avez entré dans le format « sans séparateur » affiché dans l'illustration. Dans la version 17.3 et les versions ultérieures, l'interface utilisateur Web respecte la conception que vous avez entrée et il est donc essentiel de ne pas entrer de séparateur. Bogue d'amélioration L'ID de bogue Cisco CSCv43870 suit la prise en charge de plusieurs formats pour l'authentification MAC.

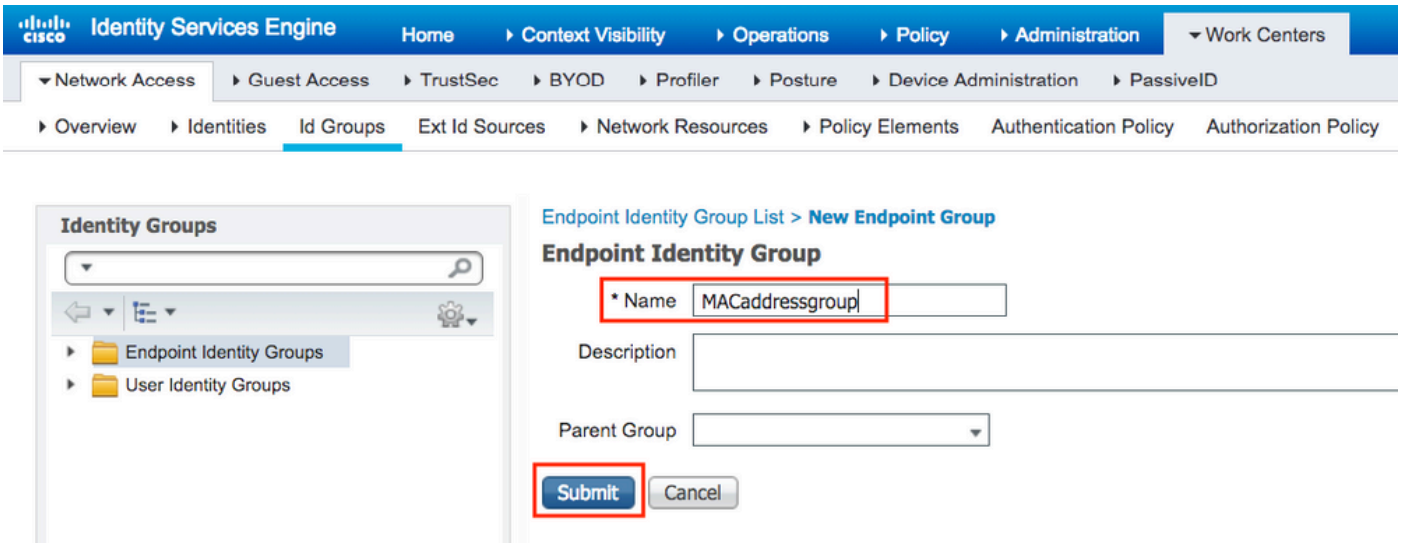
CLI :

```
# config t
# username <aabbccddeeff> mac
```

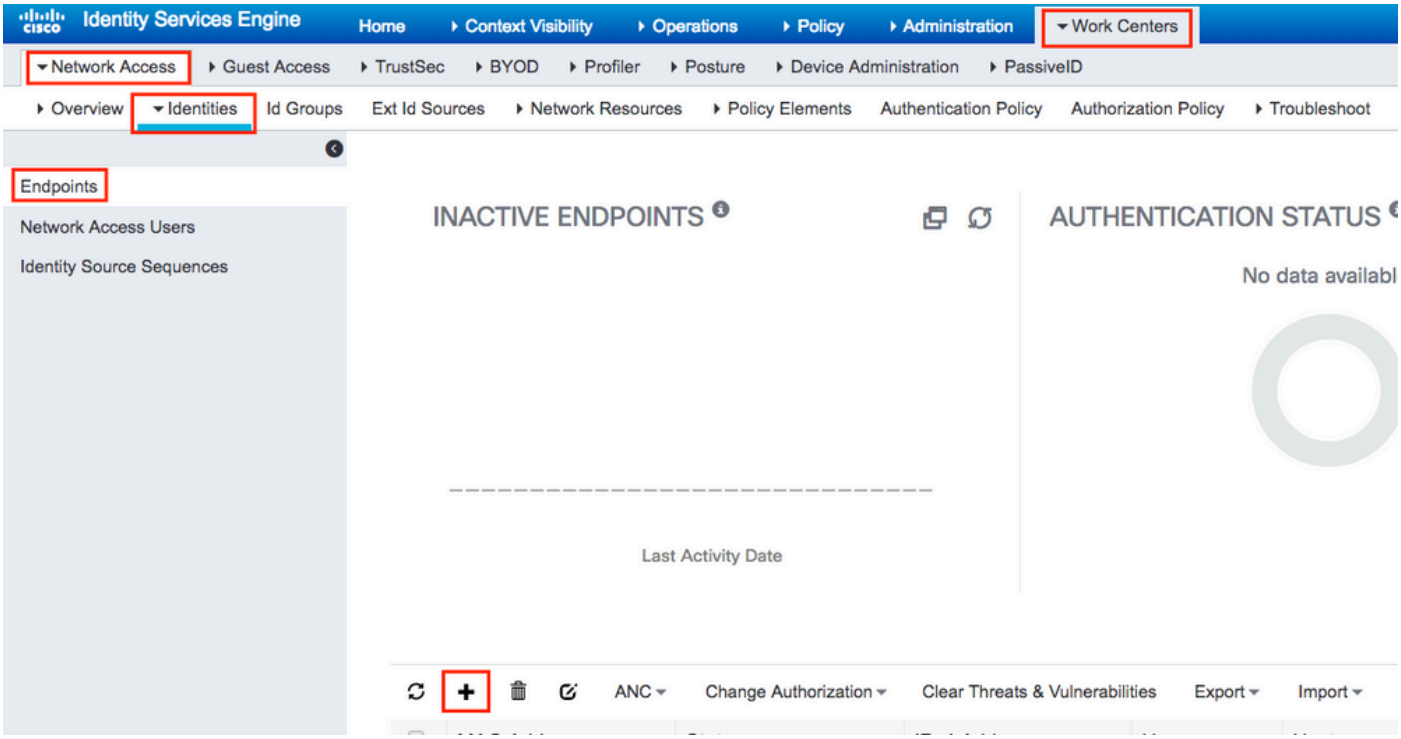
Saisissez l'adresse MAC dans la base de données ISE Endpoint

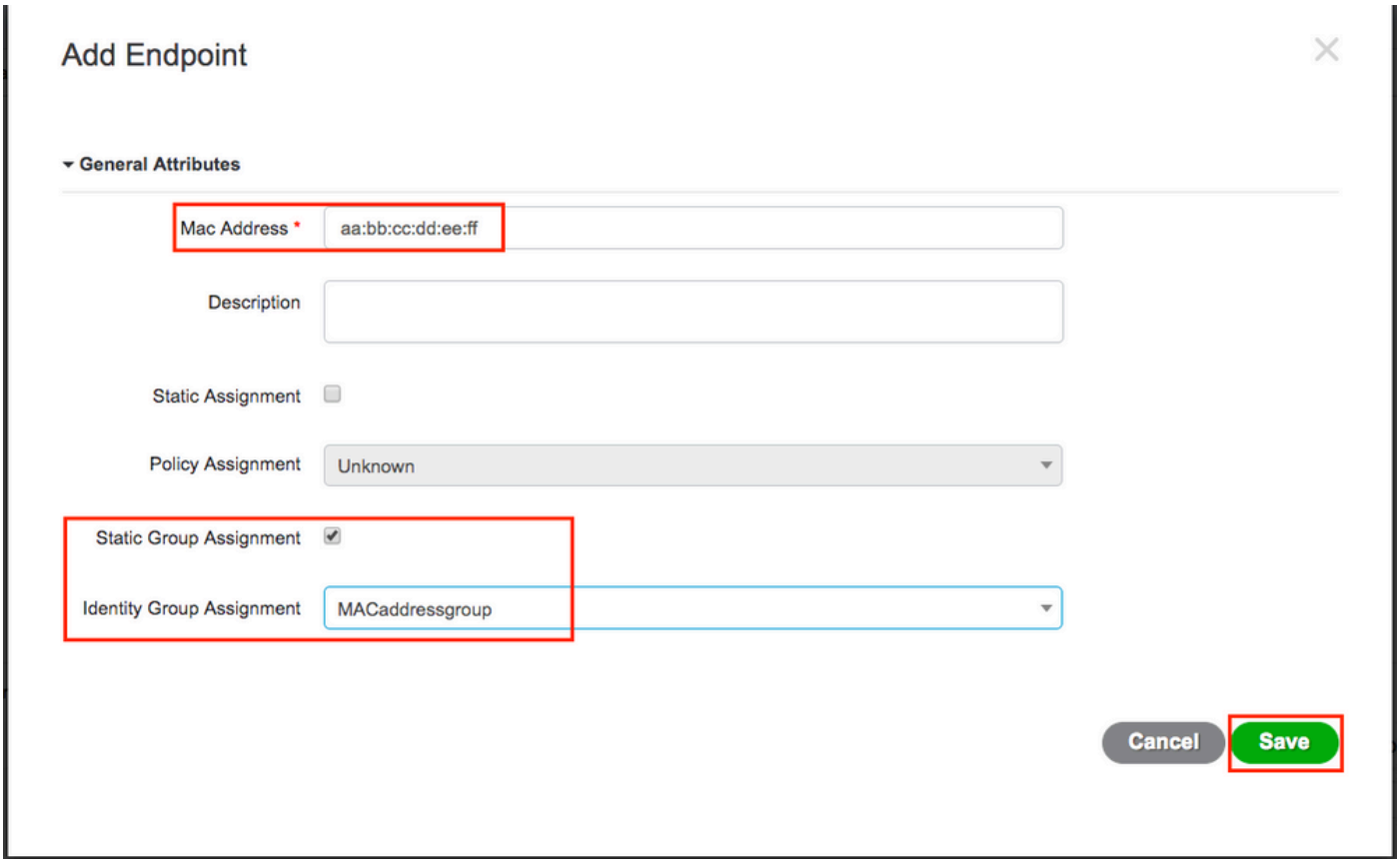
Étape 1. (Facultatif) Créez un nouveau groupe de terminaux.
Accédez àWork Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add.





Étape 2. Accédez àWork Centers > Network Access > Identities > Endpoints > +Add.





Configuration ISE

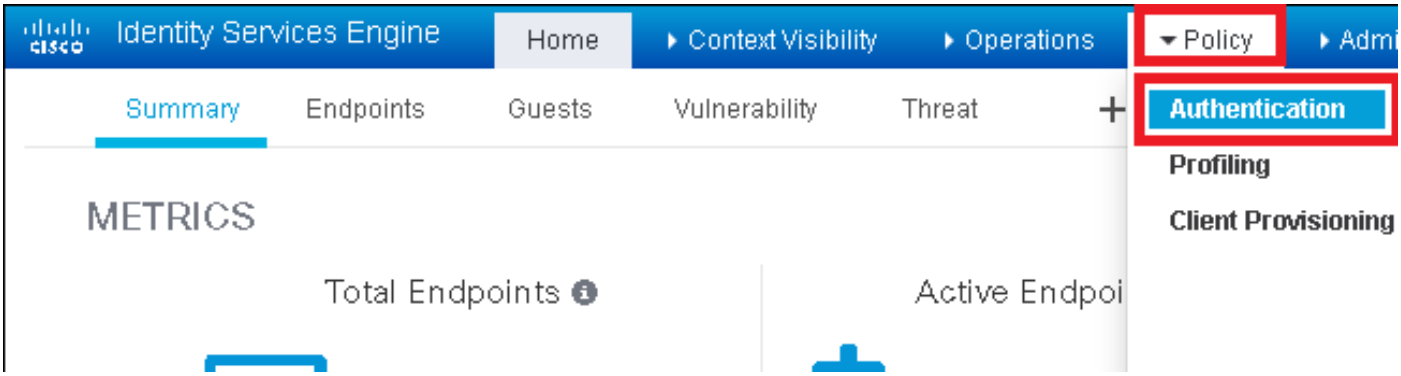
Ajouter un contrôleur WLC 9800 à ISE.

Lisez les instructions dans ce lien : [Déclarez WLC à ISE](#).

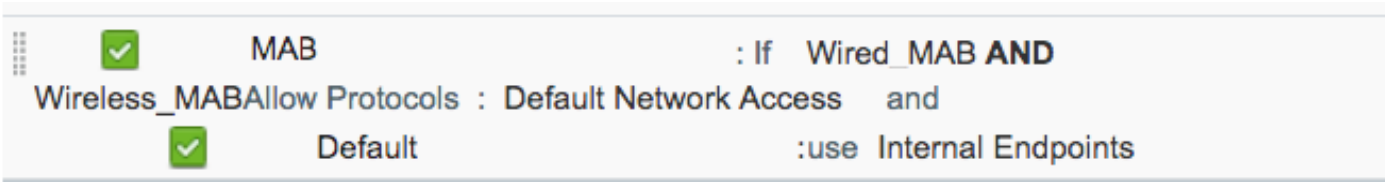
Créer une règle d'authentification

Les règles 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) et limiter les méthodes d'authentification qu'il est autorisé à utiliser.

Étape 1. Naviguez jusqu'à Policy > Authentication comme indiqué dans l'image.
Vérifiez que la règle MAB par défaut existe sur votre ISE.



Étape 2. Vérifiez que la règle d'authentification par défaut pour MAB existe déjà :

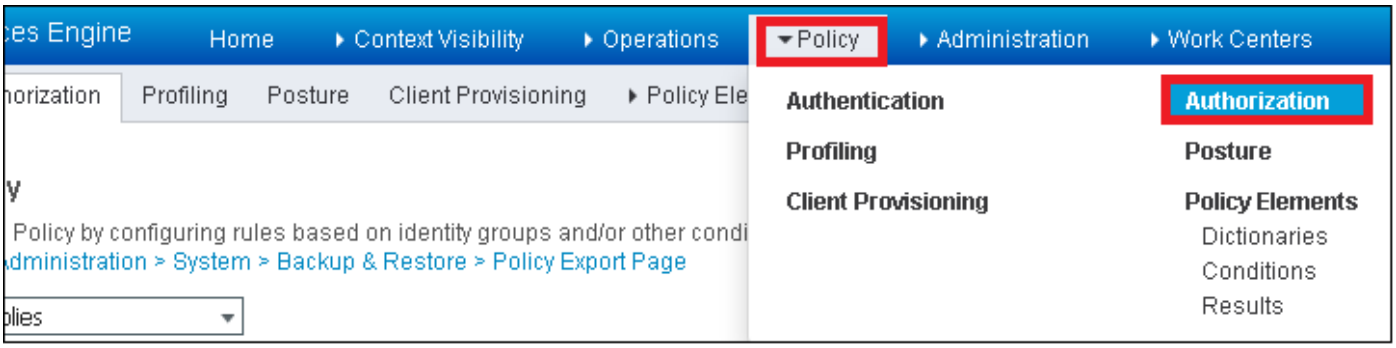


Sinon, vous pouvez en ajouter un nouveau lorsque vous cliquez surInsert new row above.

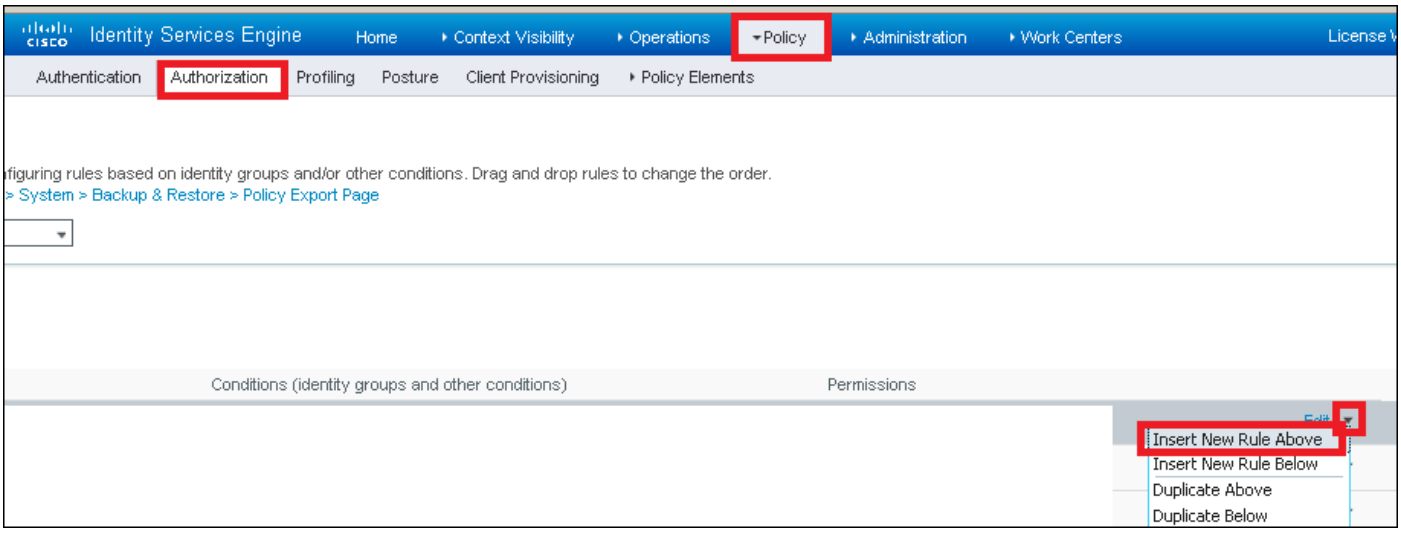
Création de règle d'autorisation

La règle d'autorisation est celle qui détermine quelles autorisations (quel profil d'autorisation) s'appliquent au client.

Étape 1. Naviguez jusqu'àPolicy > Authorizationcomme indiqué dans l'image.

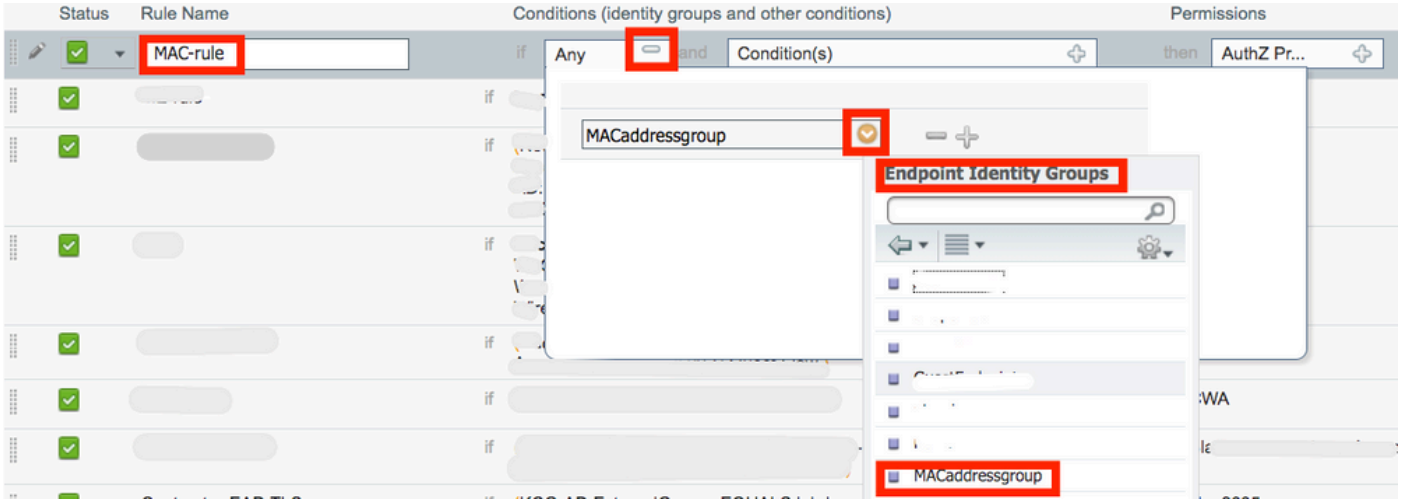


Étape 2. Insérez une nouvelle règle comme illustré dans l'image.

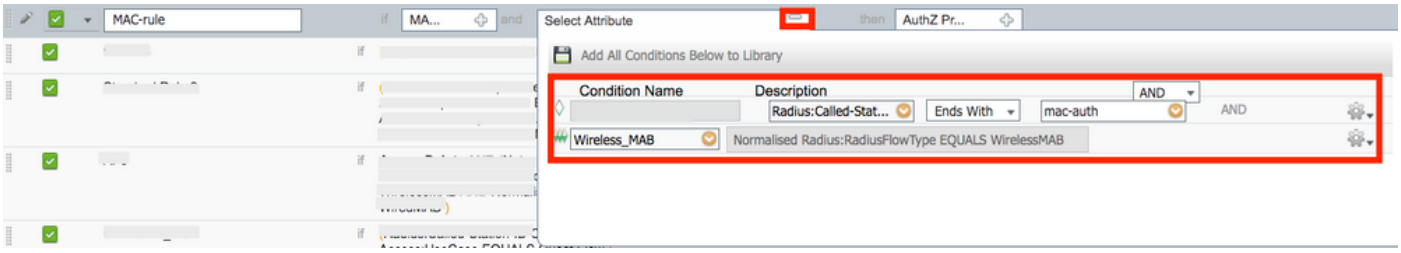


Étape 3. Saisissez les valeurs.

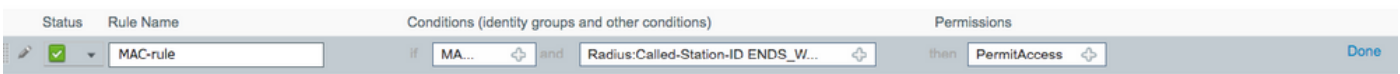
Commencez par choisir un nom pour la règle et le groupe d'identités dans lequel le point de terminaison est stocké (**MACaddressgroup**), comme illustré dans l'image.



Après cela, choisissez d'autres conditions qui font entrer le processus d'autorisation dans cette règle. Dans cet exemple, le processus d'autorisation applique cette règle s'il utilise Wireless MAB et que l'ID de la station appelée (le nom du SSID) se termine par`mac-auth`comme indiqué dans l'image.



Enfin, choisissez le profil d'autorisation qui est affecté, dans ce cas, aux clients qui ont appliqué`PermitAccess`cette règle. Cliquez sur`Done`et enregistrez-le.



Vérifier

Vous pouvez utiliser ces commandes pour vérifier la configuration actuelle:

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Dépannage

Le WLC 9800 offre des fonctionnalités de suivi ALWAYS-ON. Cela garantit que toutes les erreurs, avertissements et messages 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.

Remarque : bien que cela dépende du volume de journaux générés, 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 via SSH/Telnet au WLC 9800 et lire ces étapes (assurez-vous que vous consignez la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du contrôleur afin de pouvoir suivre les journaux depuis le moment où 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 permet d'avoir un aperçu rapide de l'état et des erreurs du système, 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 Tracing 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 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. Si l'adresse MAC soumise au test n'était pas répertoriée comme condition à l'étape 3., collectez les traces 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). Afin d'activer le débogage conditionnel, lisez ces étapes.

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.

Ces commandes commencent 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 commande debug wireless mac
par adresse mac.

Remarque : vous ne voyez pas le résultat de l'activité du client sur 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. Vous pouvez copier lera trace .logfichier 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 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. Contactez le TAC Cisco pour vous aider à analyser ces traces.

Vous pouvez copier le fichierra-internal-FILENAME.txtsur un serveur externe ou 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.

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.