Configuration du maillage sur les contrôleurs LAN sans fil Catalyst 9800

Table des matières

Introduction

Ce document décrit un exemple de configuration de base sur la façon de joindre un point d'accès maillé au contrôleur LAN sans fil (WLC) Catalyst 9800

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- Configuration des LAP
- Contrôle et fourniture de points d'accès sans fil (CAPWAP)
- Configuration d'un serveur DHCP externe
- Configuration des commutateurs Cisco

Composants utilisés

Cet exemple utilise un point d'accès léger (1572AP et 1542) qui peut être configuré en tant que point d'accès racine (RAP) ou point d'accès maillé (MAP) pour se connecter au WLC Catalyst 9800. La procédure est identique pour les points d'accès 1542 ou 1562. Le RAP est connecté au WLC Catalyst 9800 via un commutateur Cisco Catalyst.

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

- C9800-CL v16.12.1
- Commutateur de couche 2 Cisco
- Points d'accès extérieurs légers de la gamme Cisco Aironet 1572 pour la section Bridge
- Cisco Aironet 1542 pour la section Flex+Bridge

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

Étude de cas 1 : mode pont

Diagramme du réseau

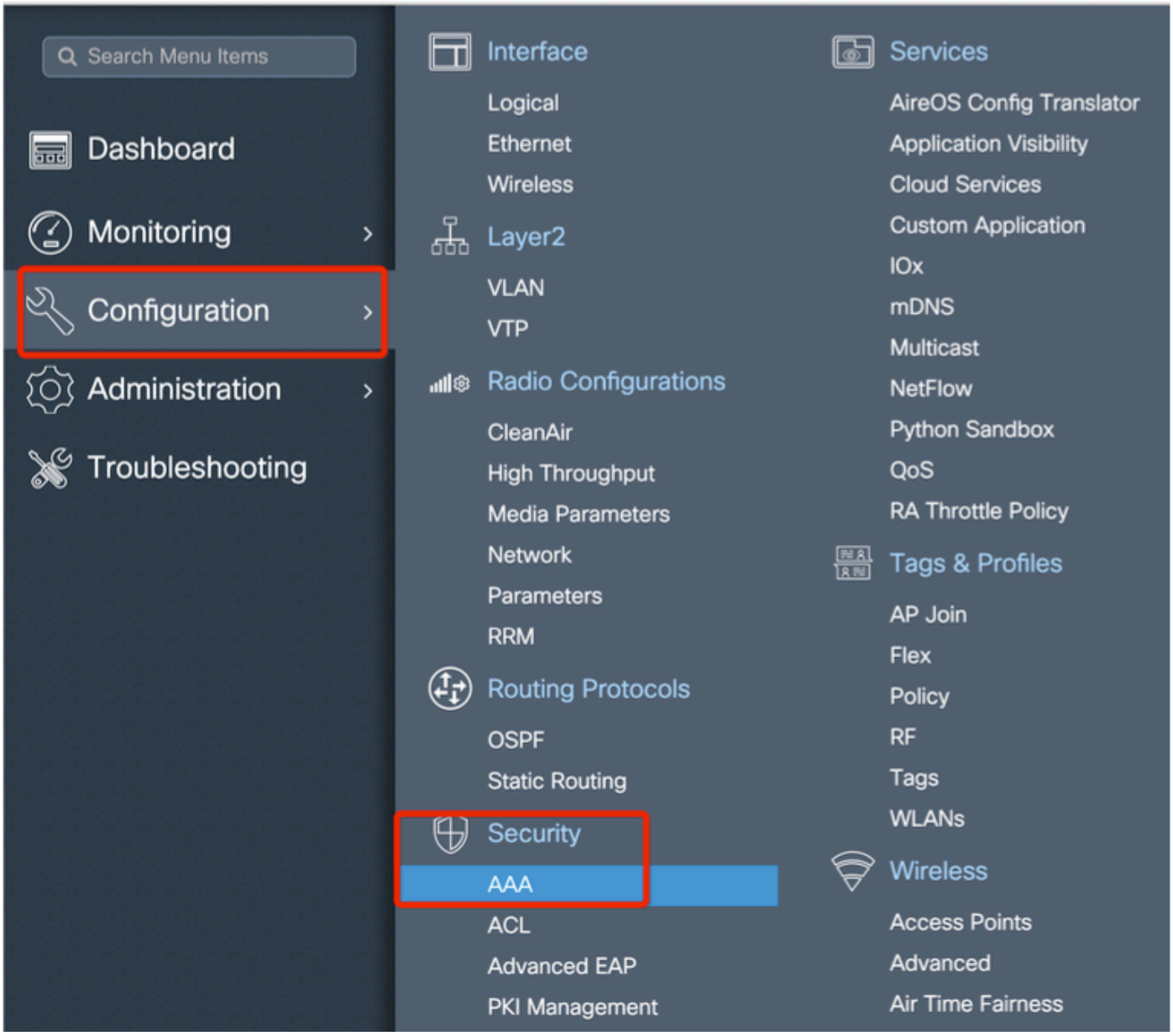
Configurations

Un point d'accès maillé doit être authentifié pour qu'il rejoigne le contrôleur 9800. Cette étude de cas considère que vous joignez l'AP en mode local d'abord au WLC, puis le convertissez en mode maillé Bridge (alias).

Pour éviter l'attribution de profils de jointure AP, utilisez cet exemple mais configurez la méthode de téléchargement d'informations d'identification d'autorisation aaa par défaut de sorte que tout AP maillé soit autorisé à joindre le contrôleur.

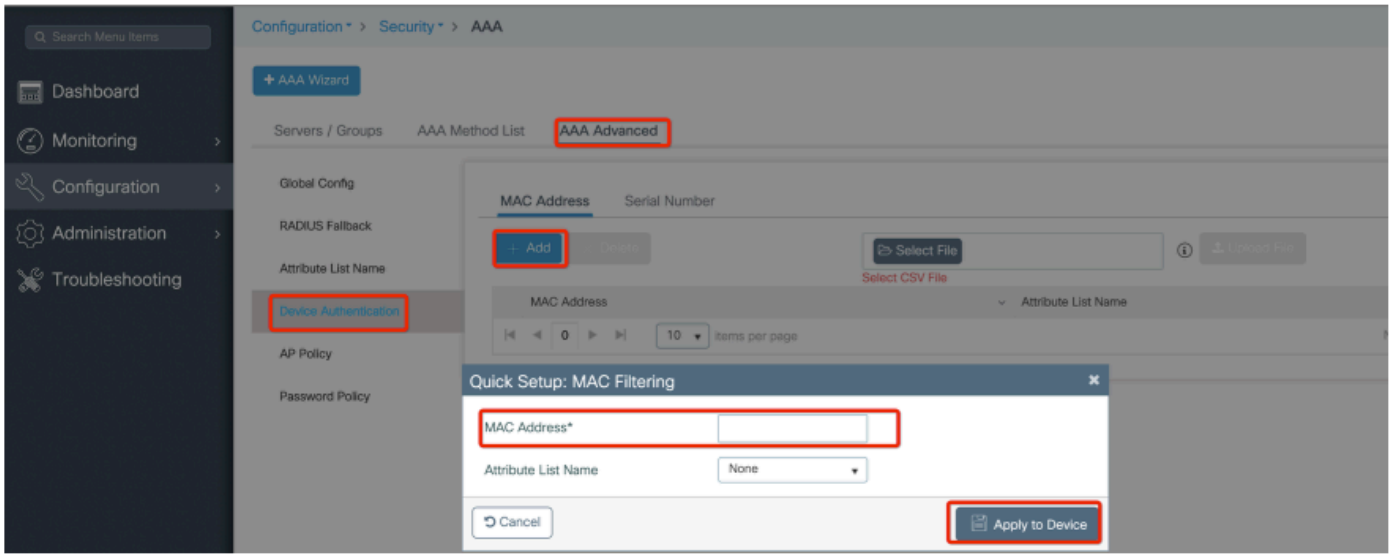
Étape 1 : configurez les adresses MAC RAP/MAP sous Device Authentication.

Accédez à Configuration > AAA > AAA Advanced > Device Authentication .



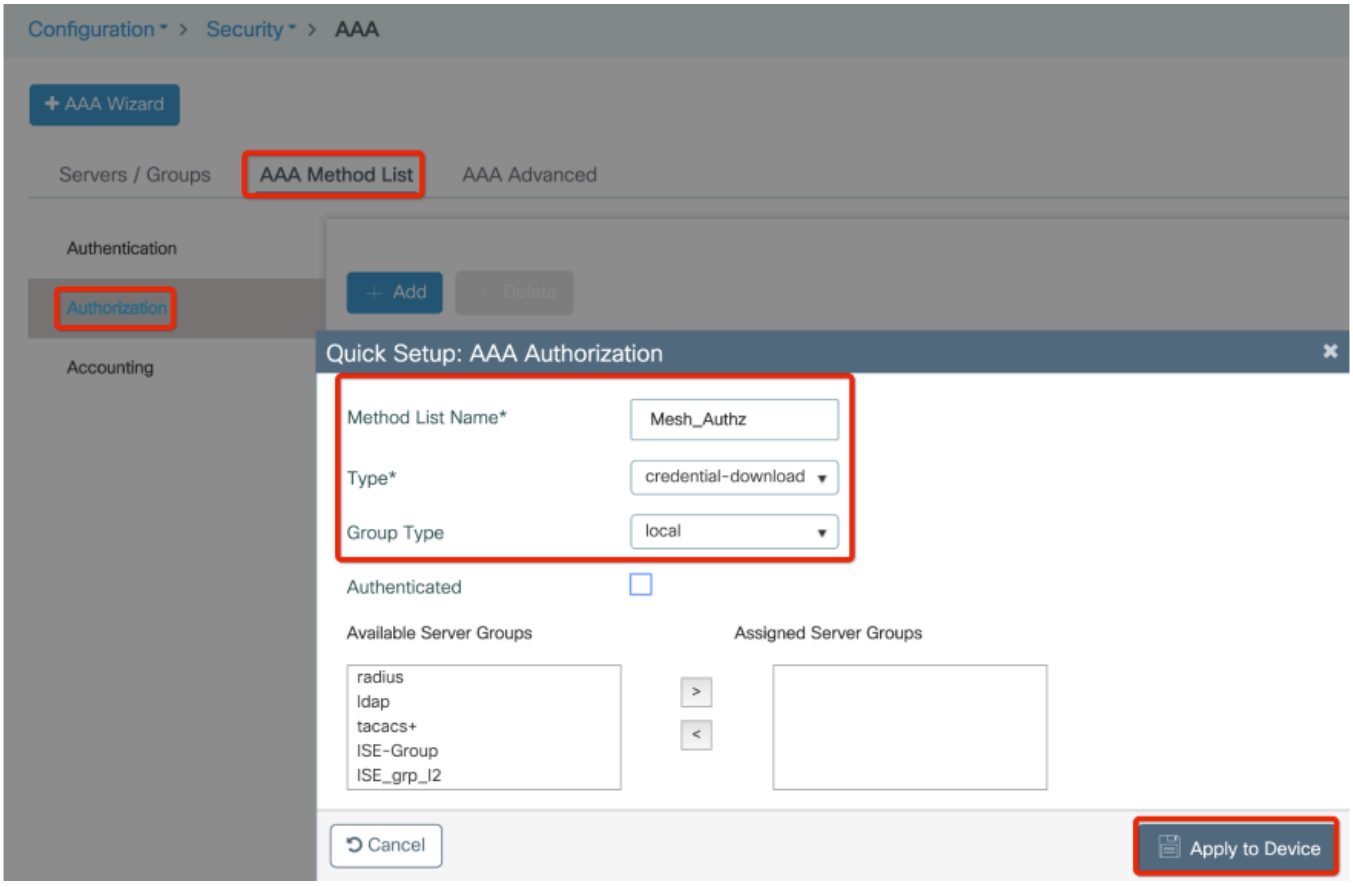
Ajoutez l'adresse MAC Ethernet de base des points d'accès maillés, sans caractères spéciaux, sans point (.) ni point (:)

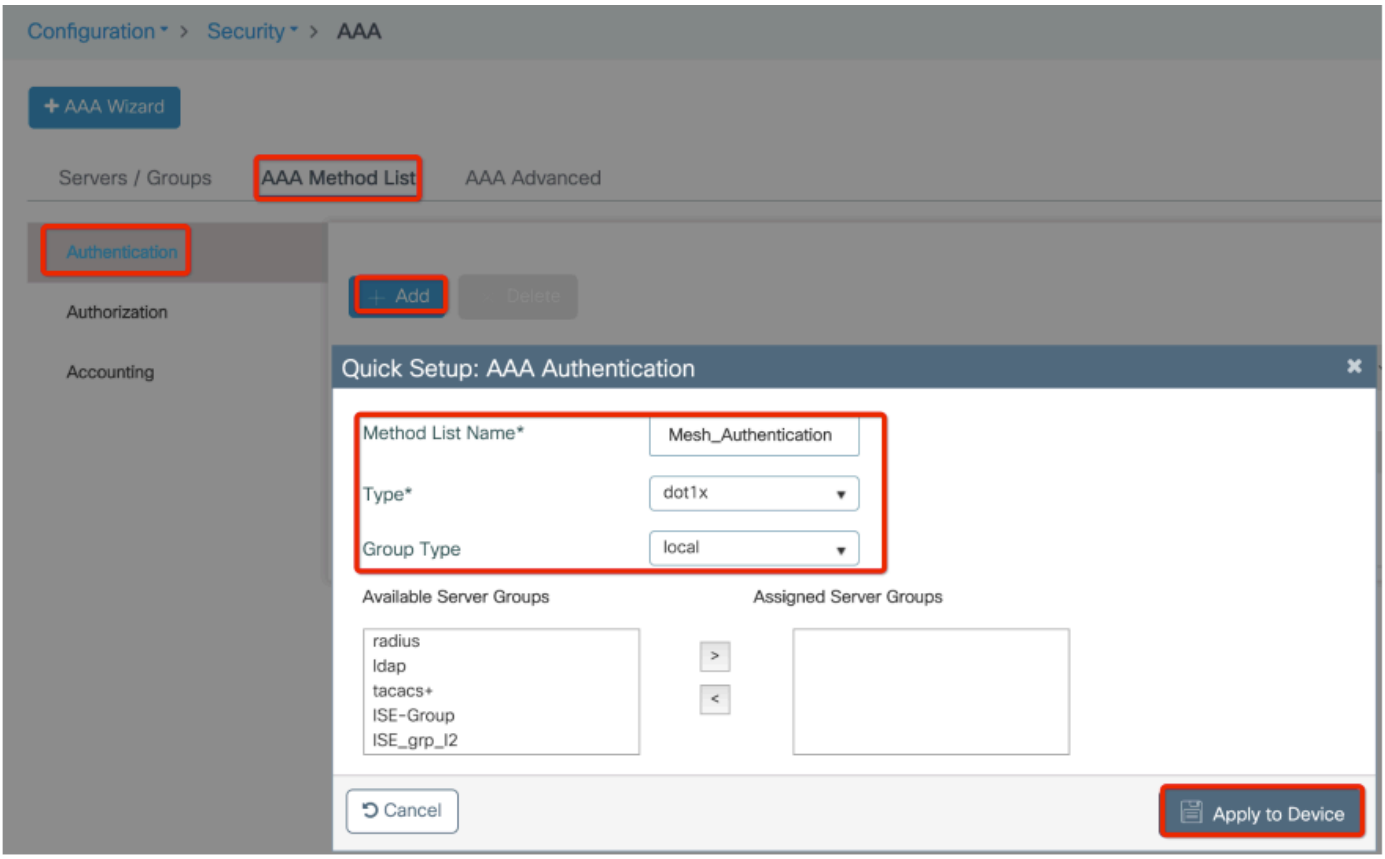
Important : à partir de la version 17.3.1, iSi des délimiteurs d'adresse MAC tels que '.', ' : ' ou '-' sont ajoutés, l'AP ne peut pas se joindre. Il y a actuellement 2 améliorations ouvertes pour ceci : ID de bogue Cisco CSCvv43870 et ID de bogue Cisco CSCvr07920. À l'avenir, le 9800 accepte tous les formats d'adresse MAC.



Étape 2 : Configurez la liste des méthodes d'authentification et d'autorisation.

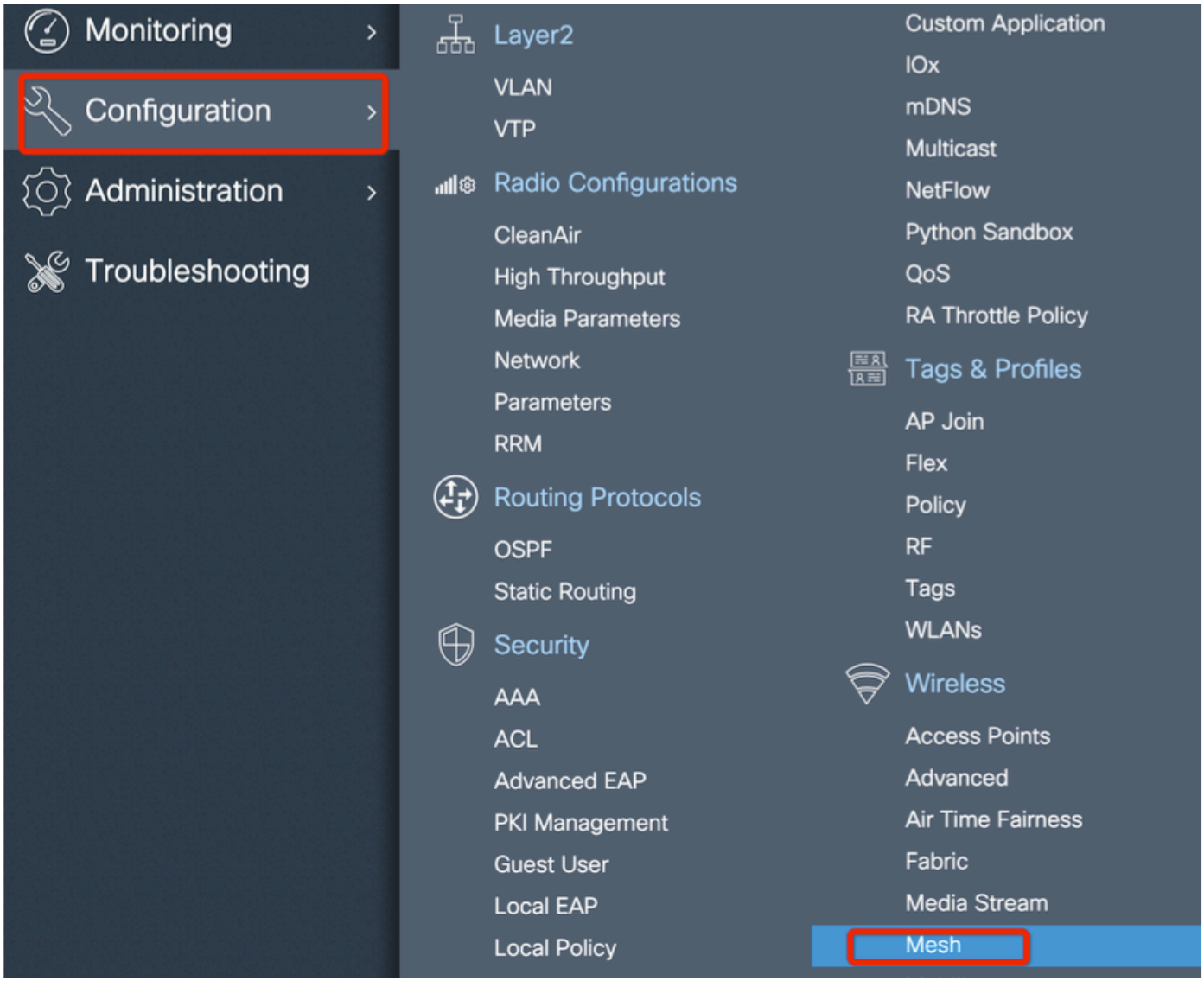
Accédez à Configuration > Security > AAA > AAA Method list > Authentication et créez la liste de méthodes d'authentification et la liste de méthodes d'autorisation.



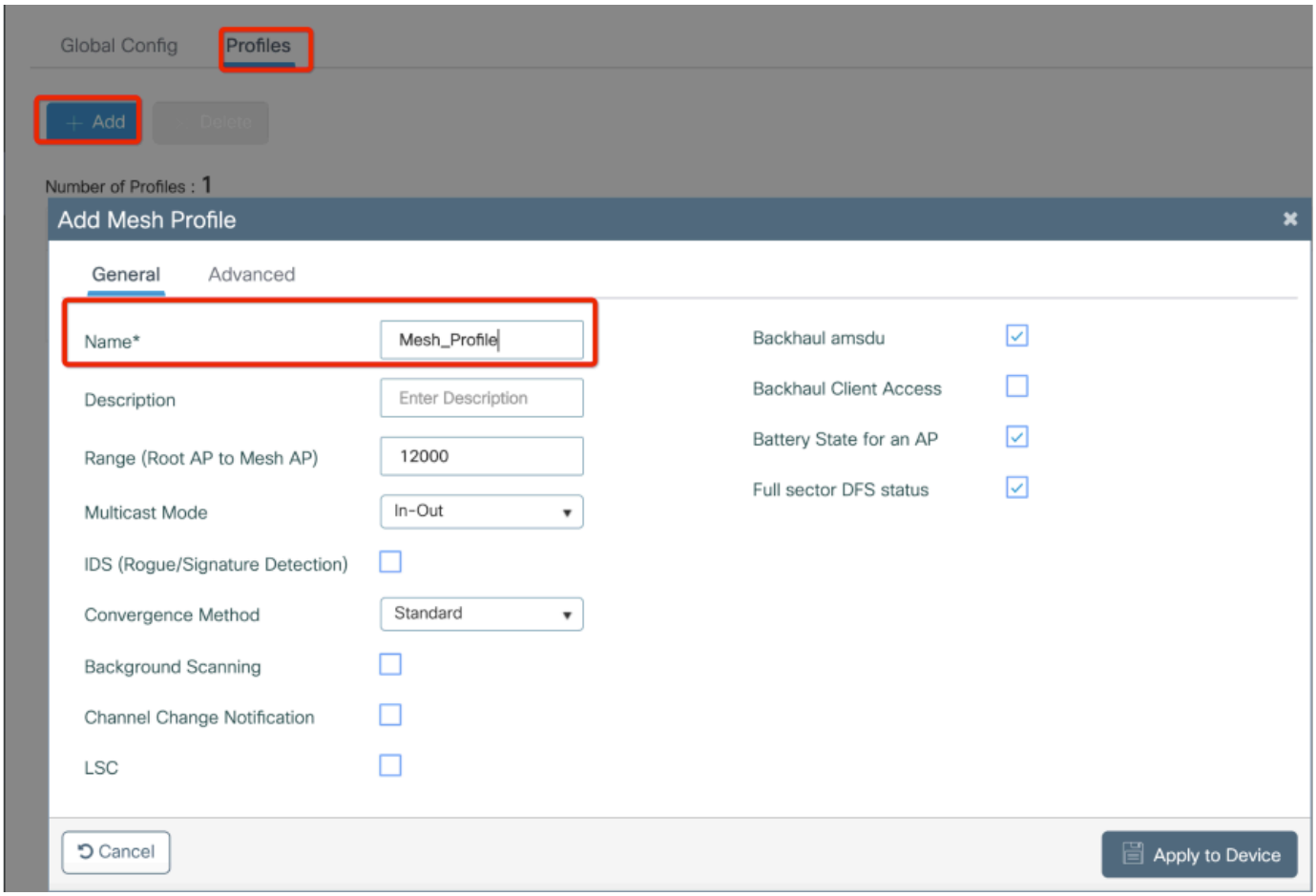


Étape 3 : Configurez les paramètres de maillage global.

Accédez à Configuration> Maillage> Paramètres globaux. Au départ, nous pouvons conserver ces valeurs par défaut.

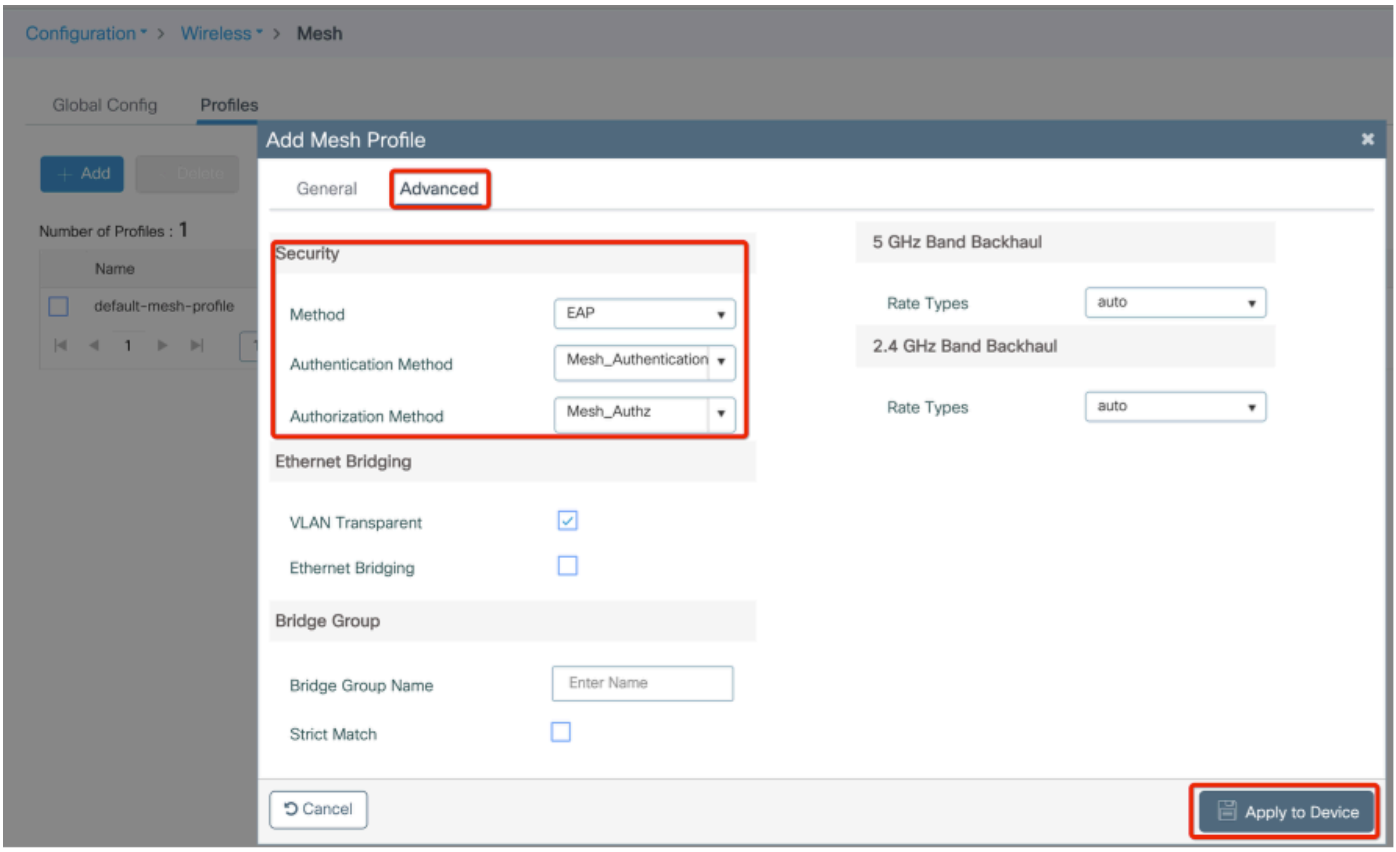


Étape 4 : Créez un nouveau profil de maillage sous Configuration > Mesh > Profile > +Add

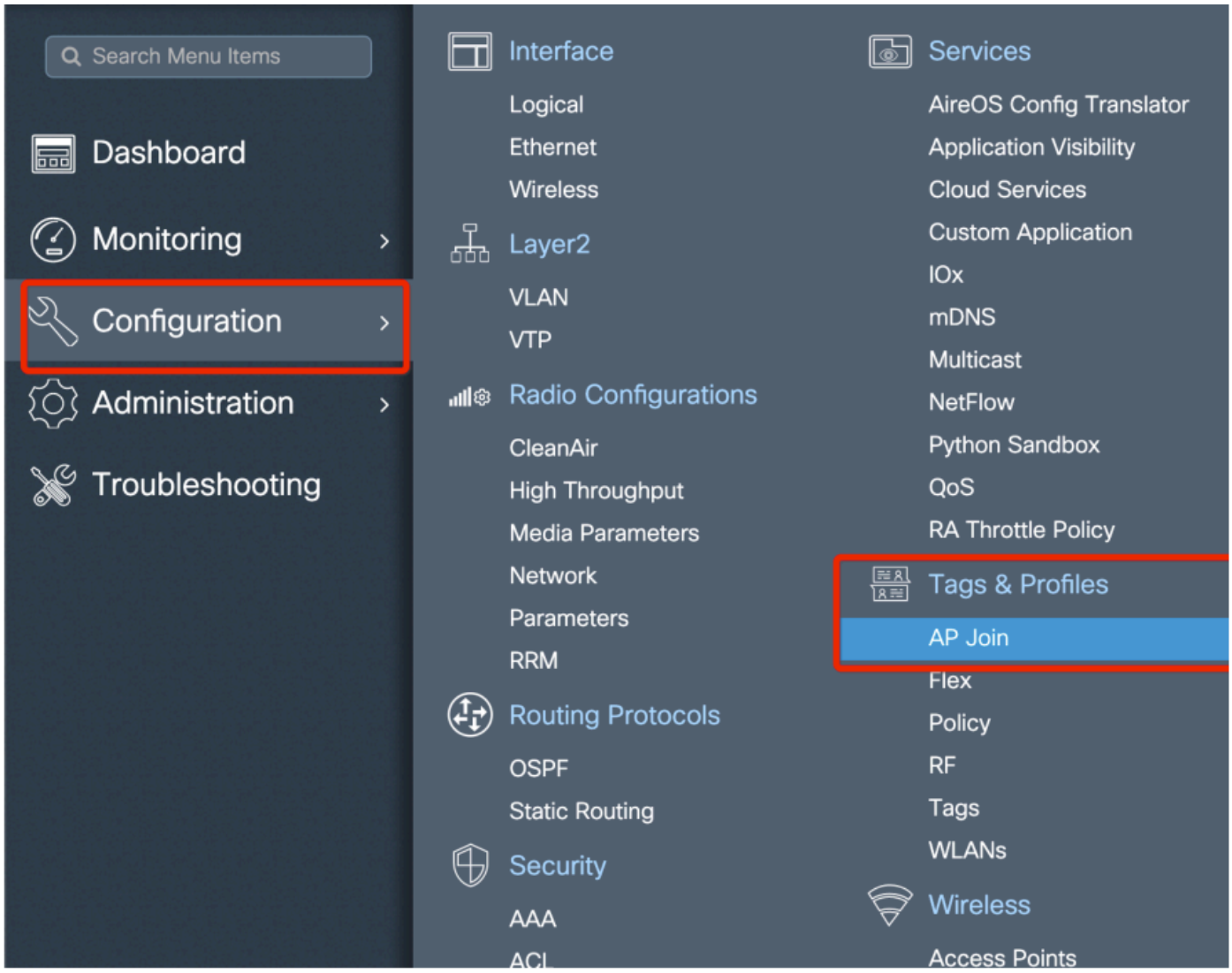


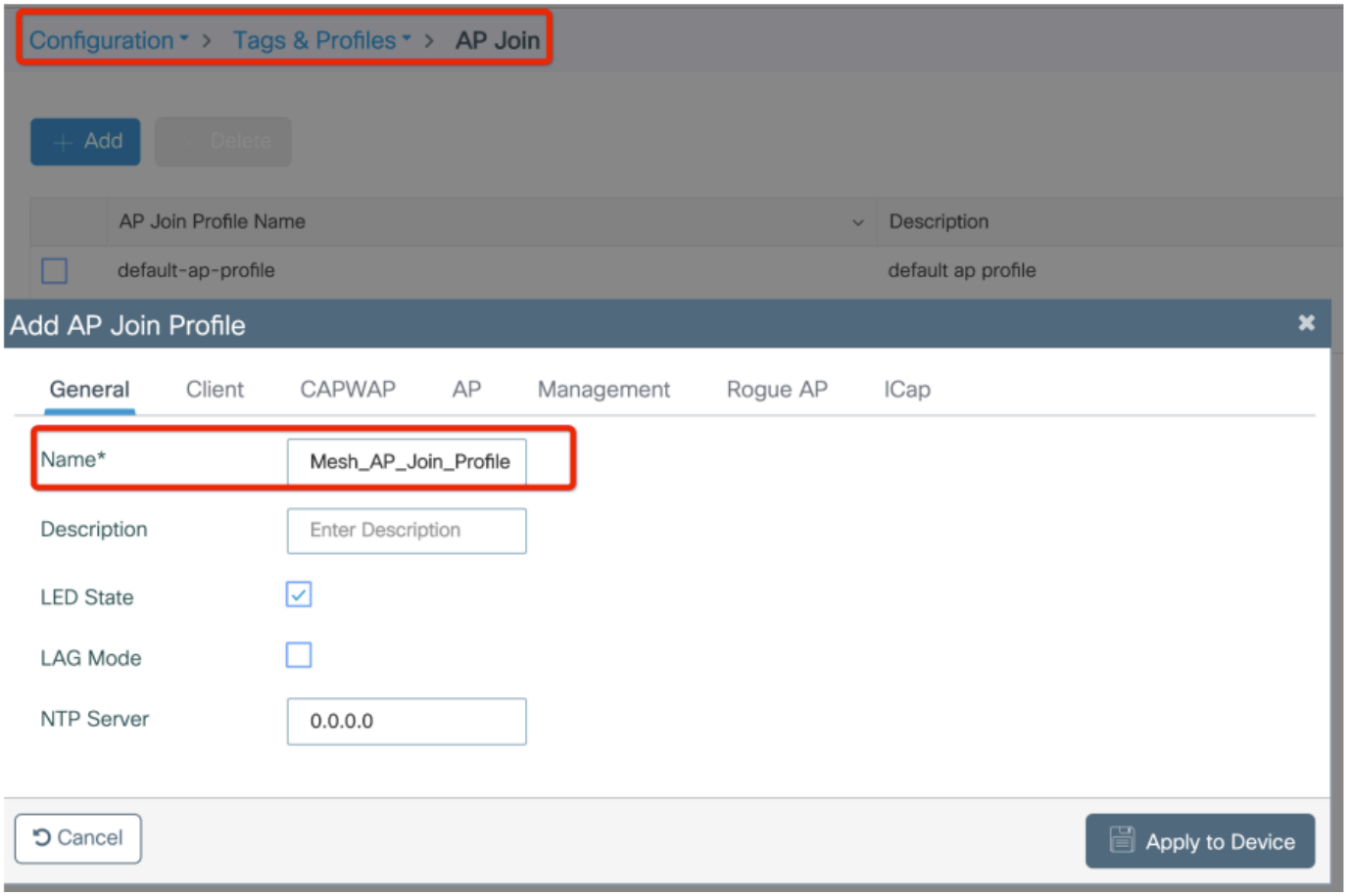
Cliquez sur le profil de maillage créé pour modifier les paramètres généraux et avancés du profil.

Dans le schéma, comme illustré, nous devons mapper le profil d'authentification et d'autorisation créé avant le profil Mesh

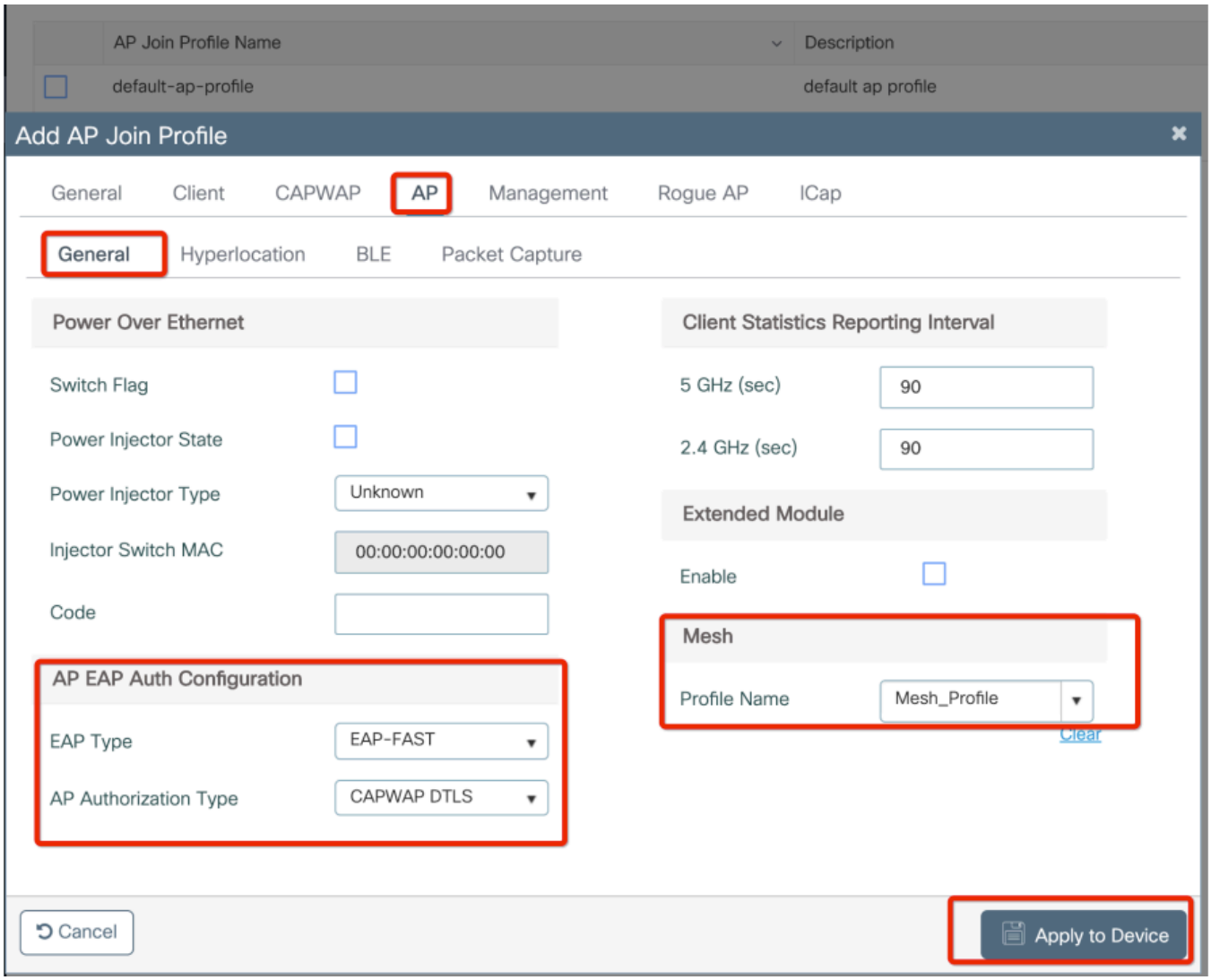


Étape 5 : Créez un nouveau profil de jointure AP. Allez à Configurer > Balises et profils : AP Join.

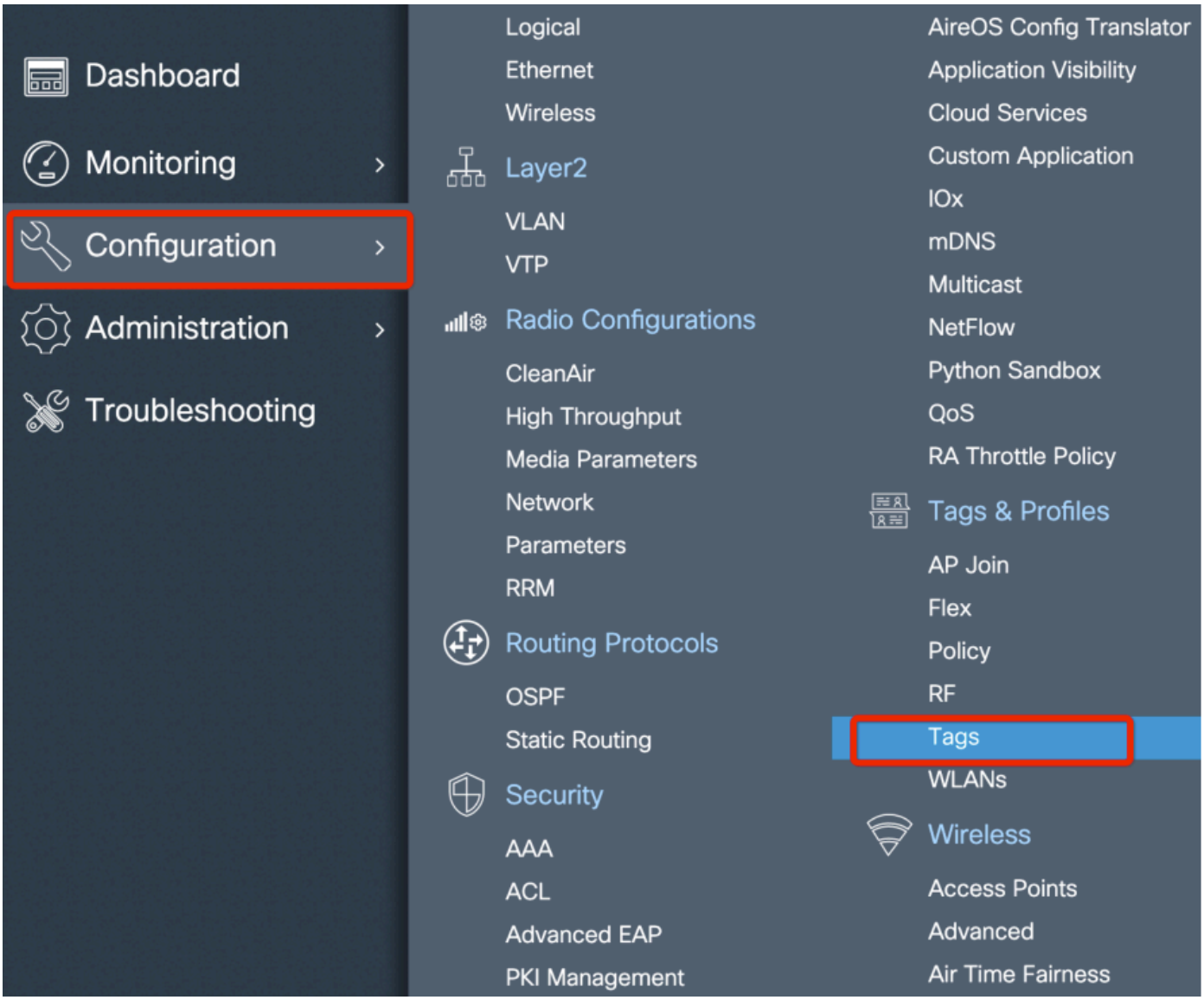

Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Interface
Logical
Ethernet
Wireless
Layer2
VLAN
VTP
Radio Configurations
CleanAir
High Throughput
Media Parameters
Network
Parameters
RRM
Routing Protocols
OSPF
Static Routing
Security
AAA
ACL
Services
AireOS Config Translator
Application Visibility
Cloud Services
Custom Application
IOx
mDNS
Multicast
NetFlow
Python Sandbox
QoS
RA Throttle Policy
Tags & Profiles
AP Join
Flex
Policy
RF
Tags
WLANs
Wireless
Access Points



Appliquez le profil de maillage précédemment configuré et configurez l'authentification AP EAP :

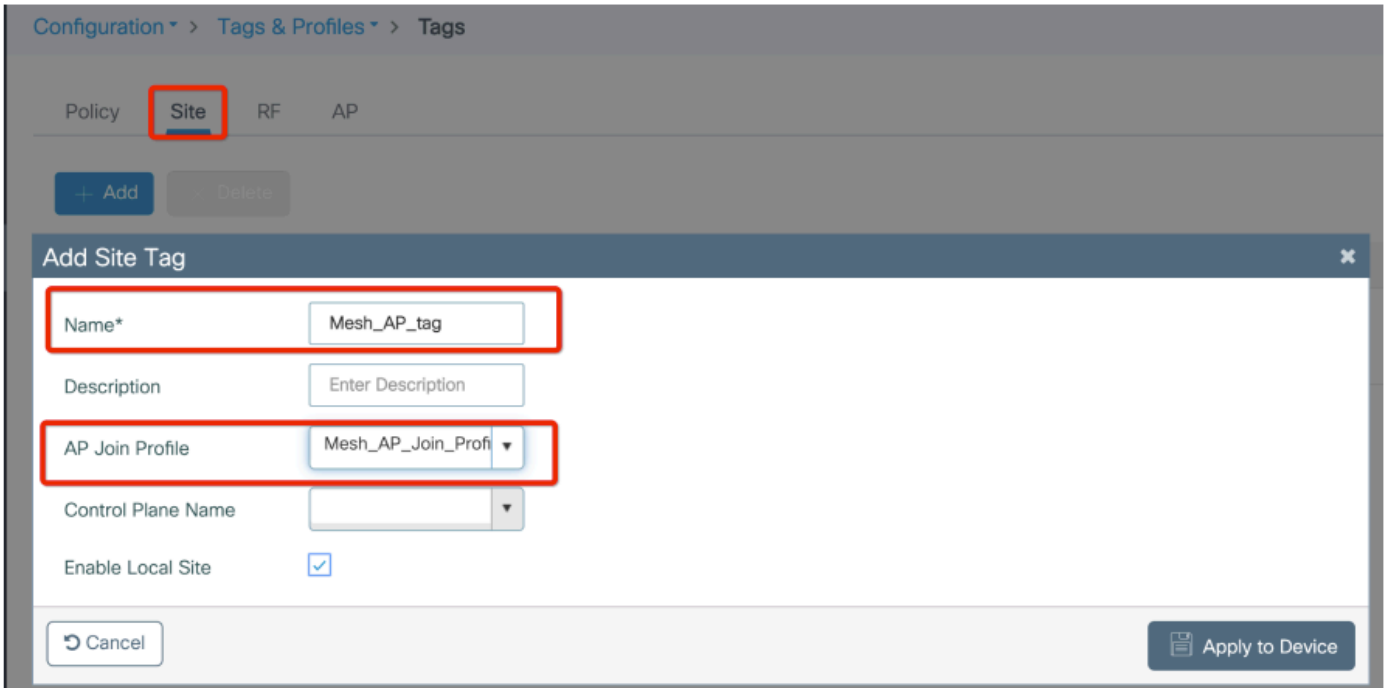


Étape 6 : Créez une balise d'emplacement de maillage comme illustré.

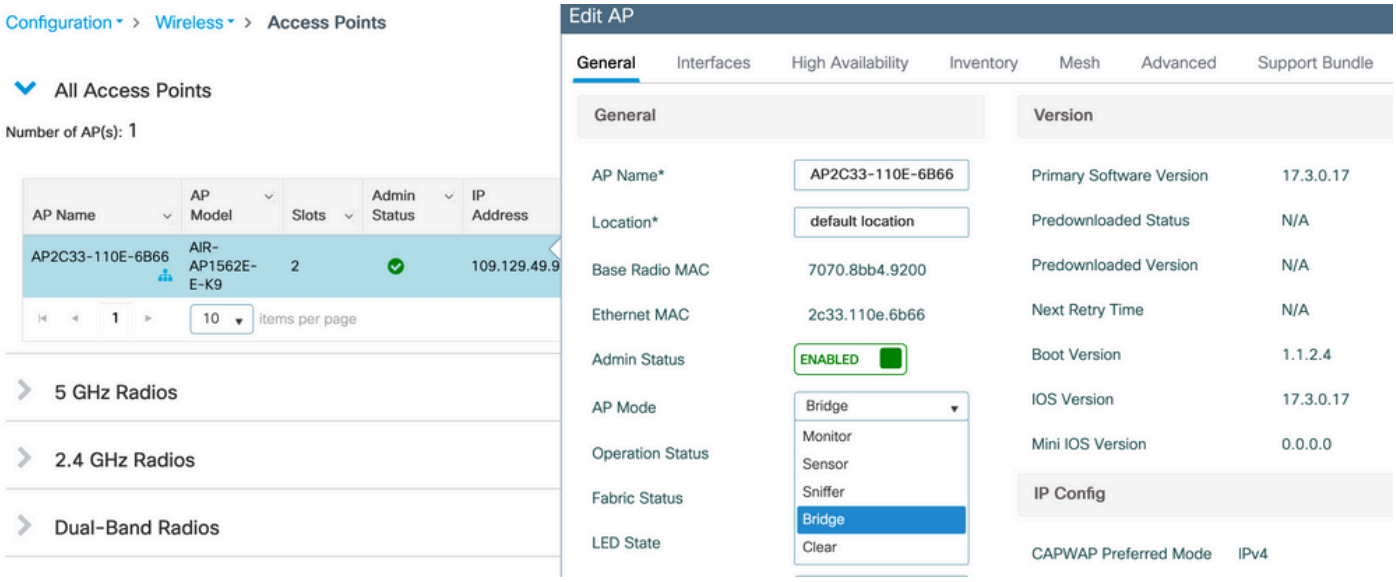


configuration Cliquez sur l'étiquette d'emplacement de maillage créée à l'étape 6 pour la configurer.

Accédez à l'onglet Site et appliquez-lui le profil de jonction d'AP maillé précédemment configuré :



Étape 7. Convertissez le point d'accès en mode Pont.



via l'interface de ligne de commande, vous pouvez utiliser cette commande sur l'AP :

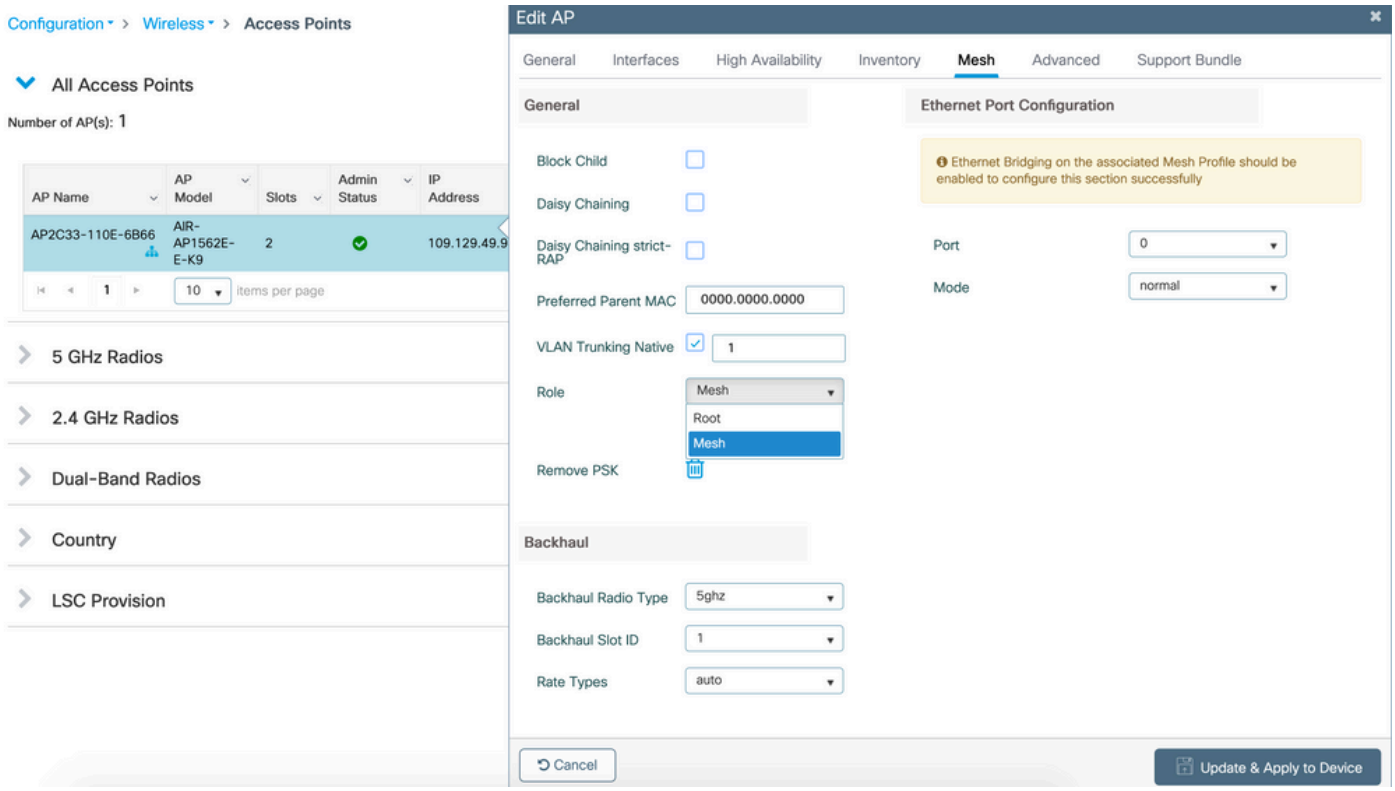
```
capwap ap mode bridge
```

Le point d'accès redémarre et se reconnecte en mode pont.

Étape 8. Vous pouvez maintenant définir le rôle du point d'accès : soit le point d'accès racine, soit le point d'accès maillé.

Le point d'accès racine est celui avec une connexion câblée au WLC tandis que le point d'accès maillé joint le WLC via sa radio qui essaie de se connecter à un point d'accès racine.

Un point d'accès maillé peut joindre le WLC via son interface câblée une fois qu'il n'a pas réussi à trouver un point d'accès racine via sa radio, à des fins de provisionnement.

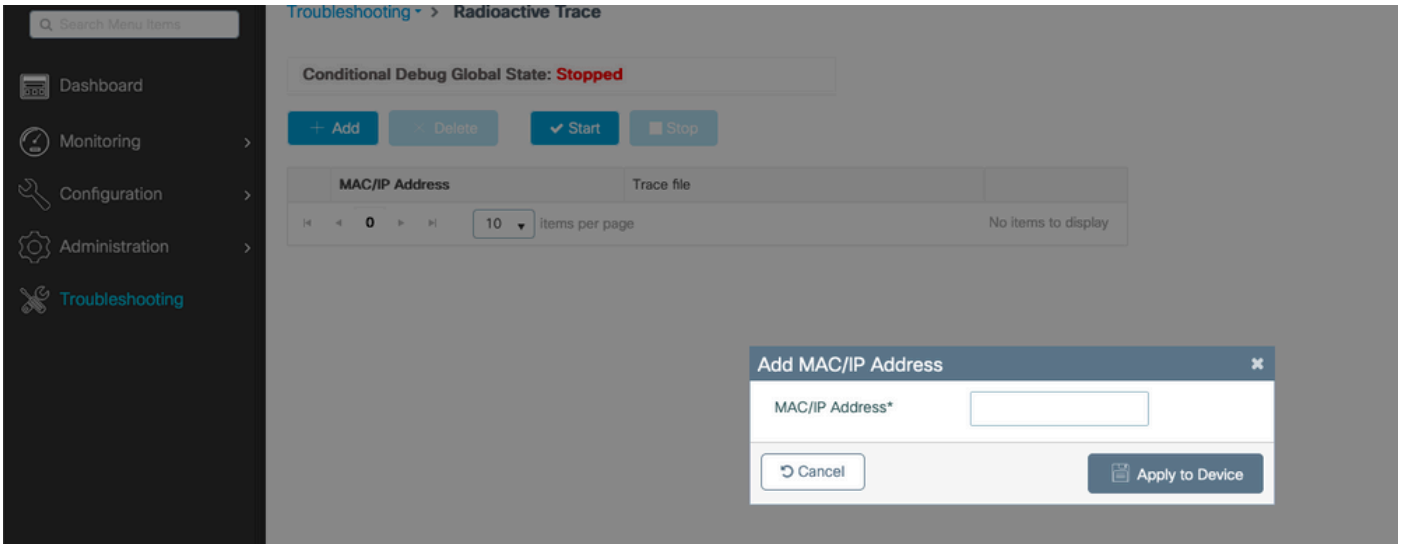


Vérifier

```
aaa new-model
aaa local authentication default authorization default
!
!
aaa authentication dot1x default local
aaa authentication dot1x Mesh_Authentication local
aaa authorization network default local
aaa authorization credential-download default local
aaa authorization credential-download Mesh_Authz local
username 111122223333 mac
wireless profile mesh Mesh_Profile
 method authentication Mesh_Authentication
 method authorization Mesh_Authz
wireless profile mesh default-mesh-profile
 description "default mesh profile"
wireless tag site Mesh_AP_Tag
 ap-profile Mesh_AP_Join_Profile
ap profile Mesh_AP_Join_Profile
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
 mesh-profile Mesh_Profile
```

Dépannage

Dans la page Troubleshoot > Radioactive Trace web UI, cliquez sur add et entrez l'adresse MAC de l'AP.



Cliquez sur Start et attendez que le point d'accès essaie de joindre à nouveau le contrôleur.

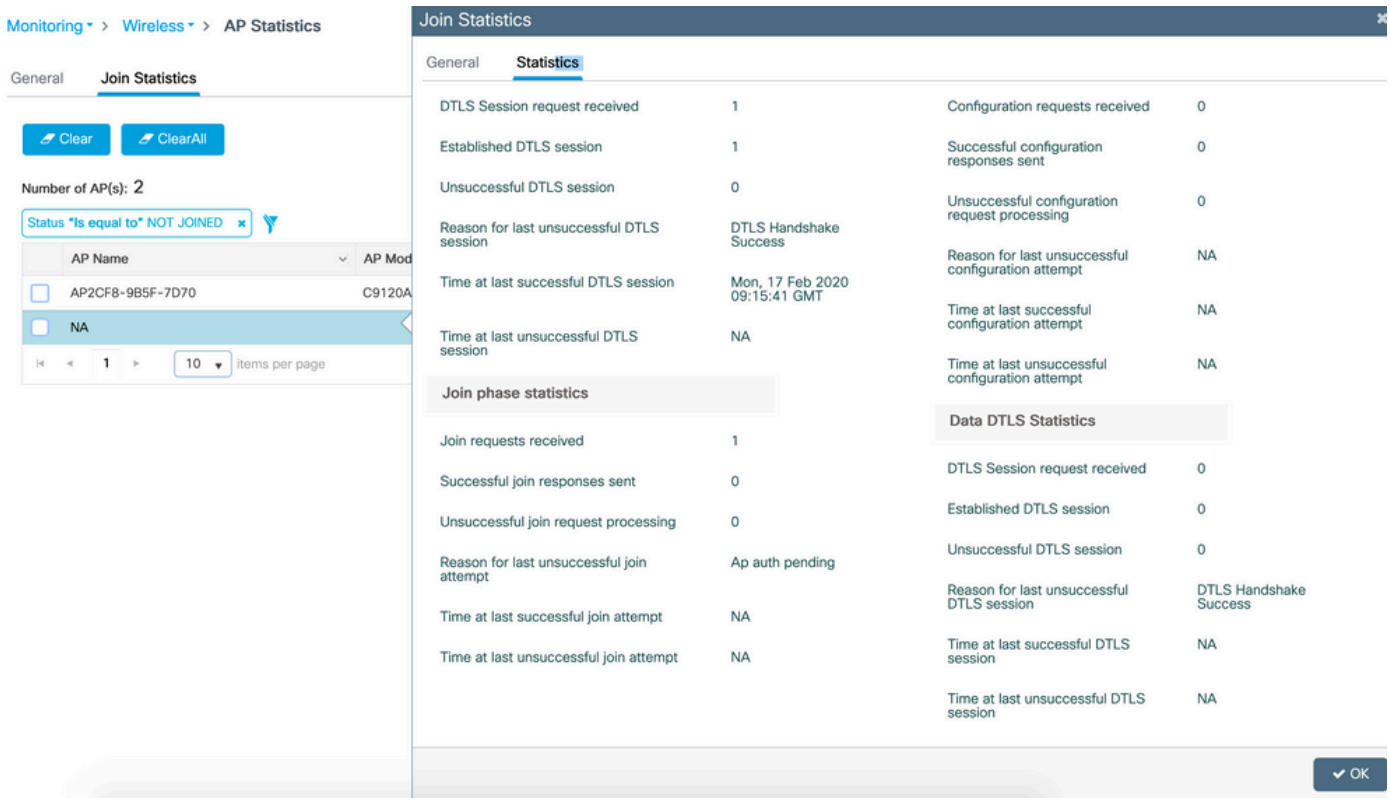
Une fois terminé, cliquez sur Generate et choisissez une période pour collecter les journaux (les 10 ou 30 dernières minutes par exemple).

Cliquez sur le nom du fichier Trace pour le télécharger à partir de votre navigateur.

Voici un exemple de point d'accès non joint en raison d'un nom de méthode d'autorisation aaa incorrect qui a été défini :

```
019/11/28 13:08:38.269 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [23388]: (info): DTLS record type: 23, appli
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (info): 00a3.8e95.6c40 Ap auth p
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): Failed to initialize auth
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): 00a3.8e95.6c40 Auth reque
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get wtp r
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get ap ta
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (ERR): Session-IP: 192.168.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (info): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.289 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [23038]: (debug): instance :0 port:38932MAC
```

La même chose peut être vu plus facilement dans le tableau de bord de l'interface utilisateur Web lorsque vous cliquez sur AP non joint. "Ap auth pending" est l'indice qui pointe vers l'authentification de l'AP lui-même :

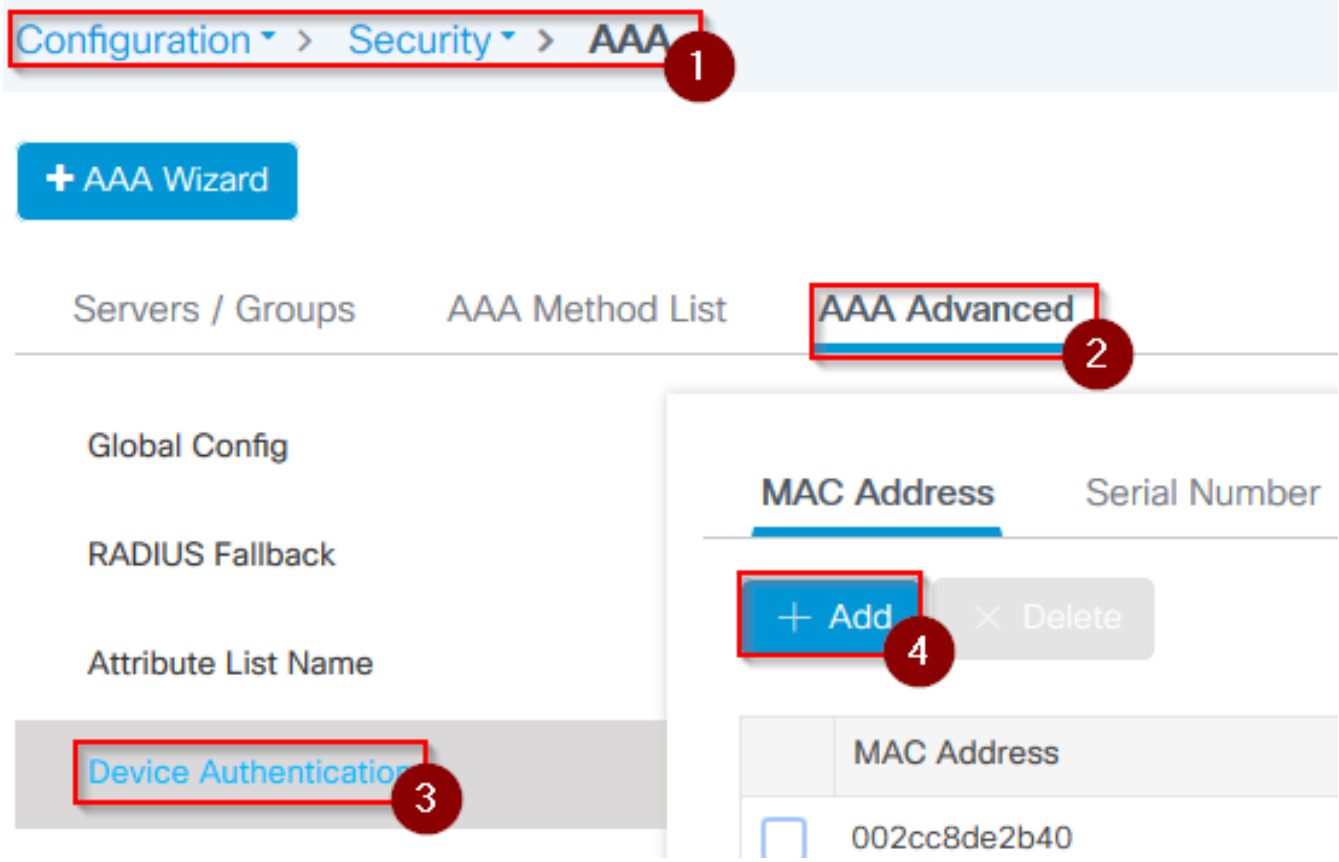


Étude de cas 2 : Flex + Bridge

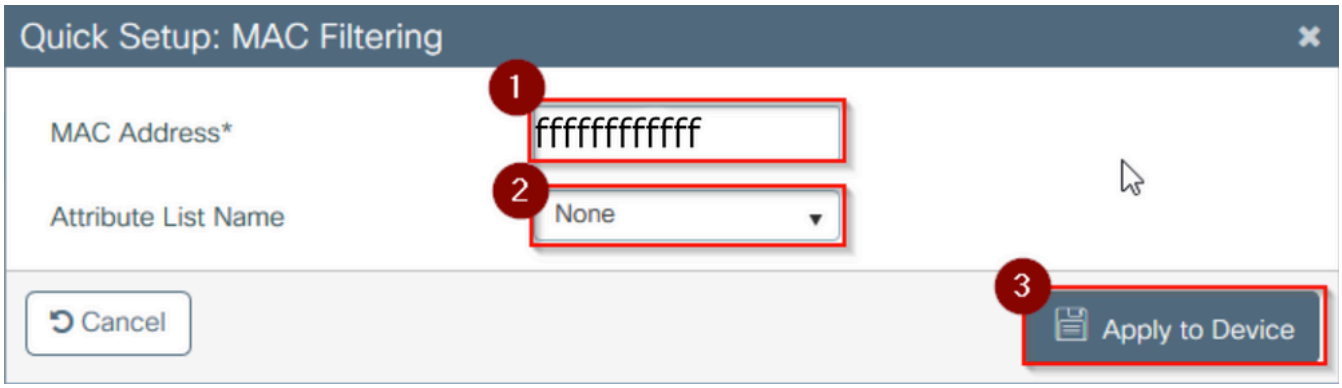
Cette section met en évidence le processus de jonction d'un AP 1542 en mode Flex+bridge avec l'authentification EAP effectuée localement sur le WLC.

Configurer

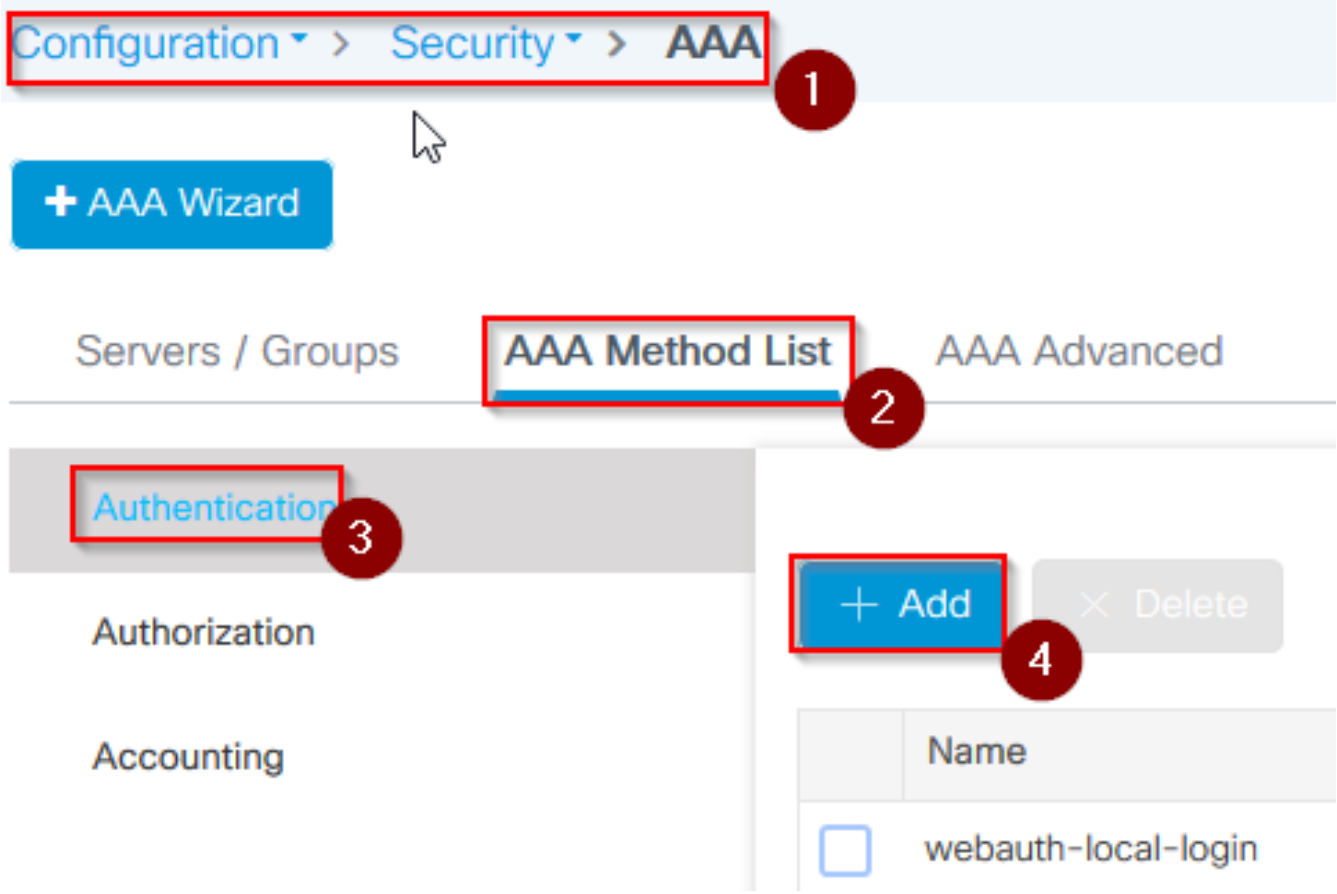
- Étape 1. Accédez à Configuration > Security > AAA > AAA Advanced > Device Authentication



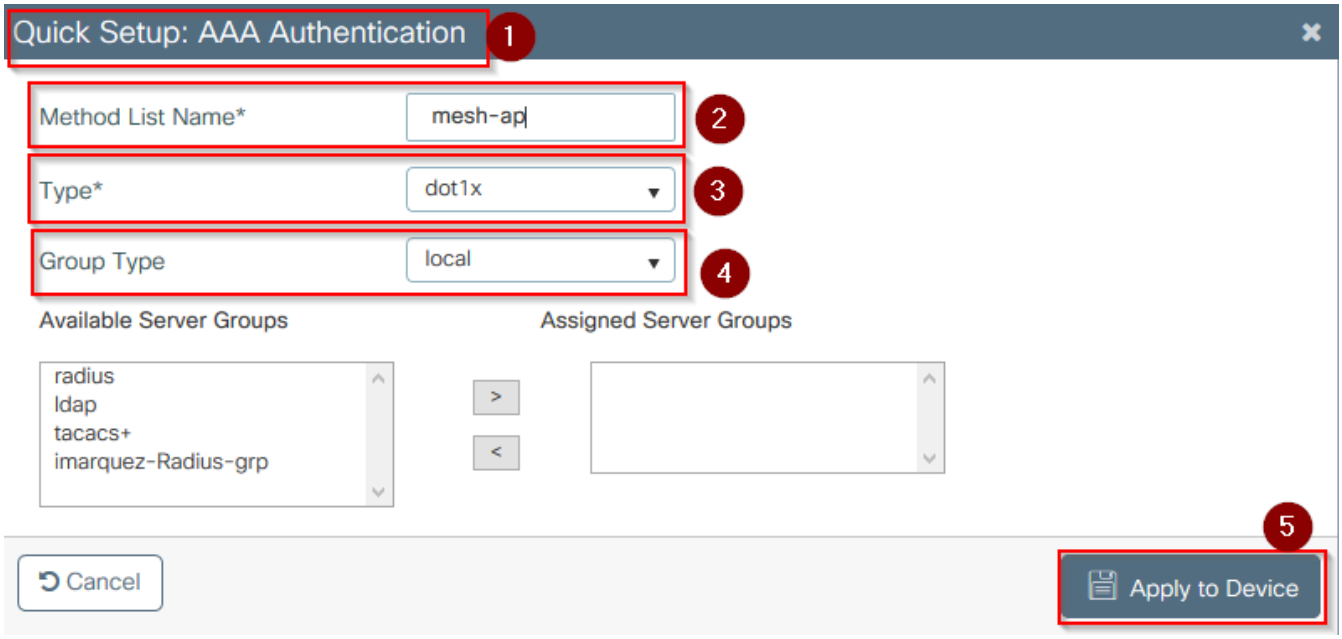
- Étape 2. Sélectionnez Device Authentication, puis Add
- Étape 3. Tapez l'adresse MAC Ethernet de base de l'AP à joindre au WLC, laissez le champ Attribute List Name vide, et sélectionnez Apply to Device



- Étape 4. Accédez à Configuration > Security > AAA > AAA Method List > Authentification
- Étape 5. Sélectionnez Add, la fenêtre AAA Authentication s'affiche



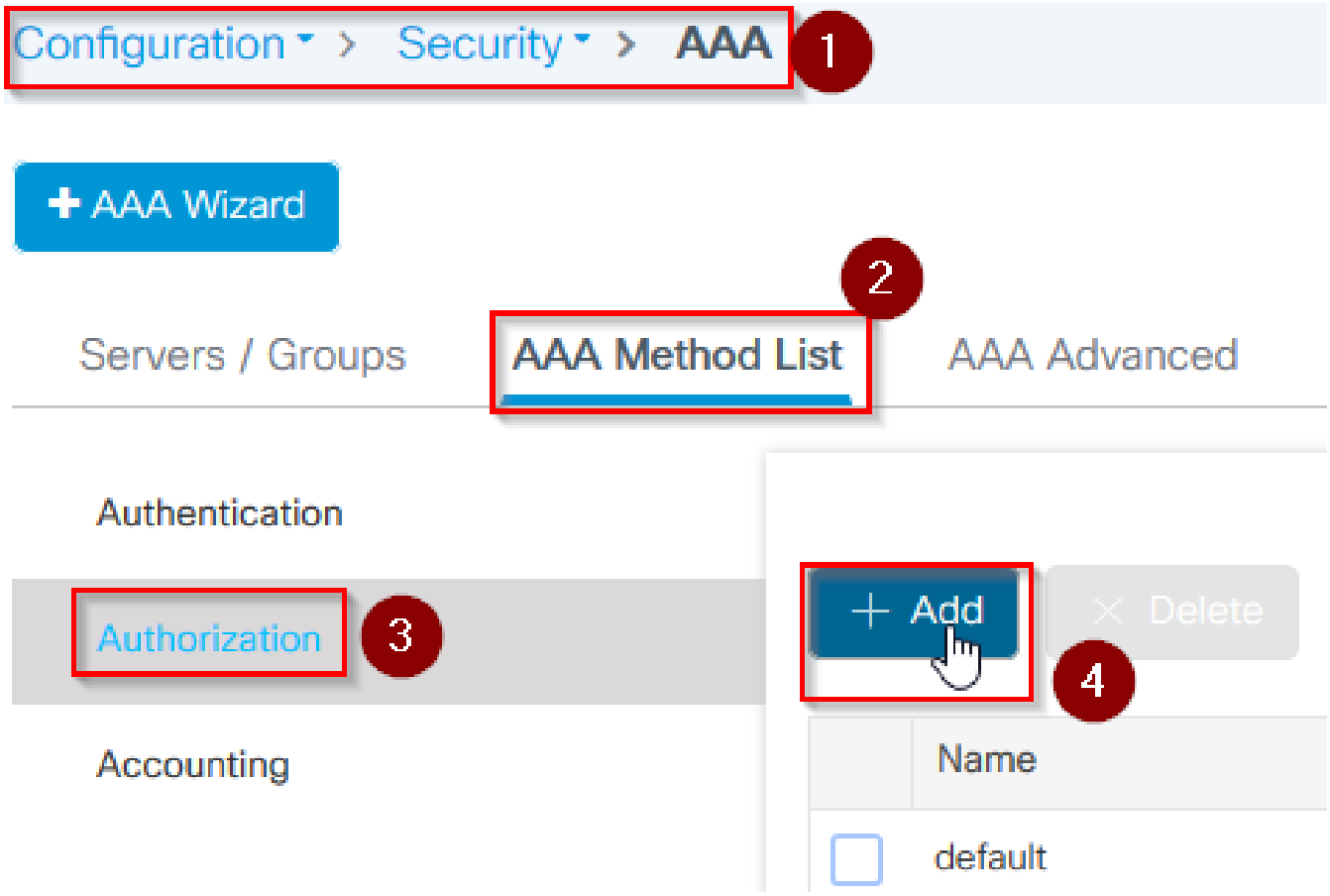
- Étape 6. Tapez un nom dans la liste Nom de la méthode, sélectionnez 802.1x dans la liste déroulante Type* et local pour le type de groupe, puis sélectionnez Apply to Device



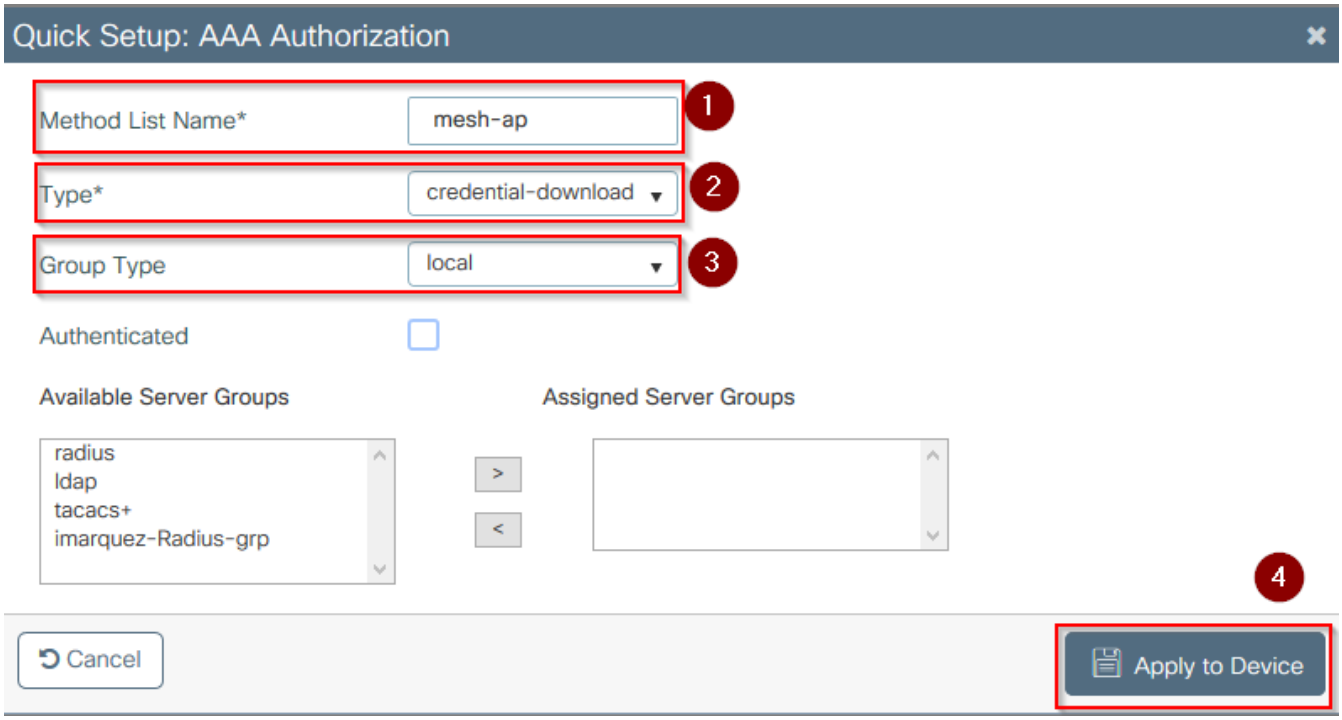
- Étape 6b. Si vos AP rejoignent directement en mode pont et qu'aucune balise de site et de stratégie n'a été attribuée auparavant, répétez l'étape 6, mais pour la méthode par défaut.
- Configurez une méthode d'authentification dot1x aaa qui pointe vers local (CLI aaa authentication dot1x default local)

- Étape 7. Accédez à Configuration > Security > AAA > AAA Method List > Autorisation

- Étape 8. Sélectionnez Add, la fenêtre AAA Authorization s'affiche



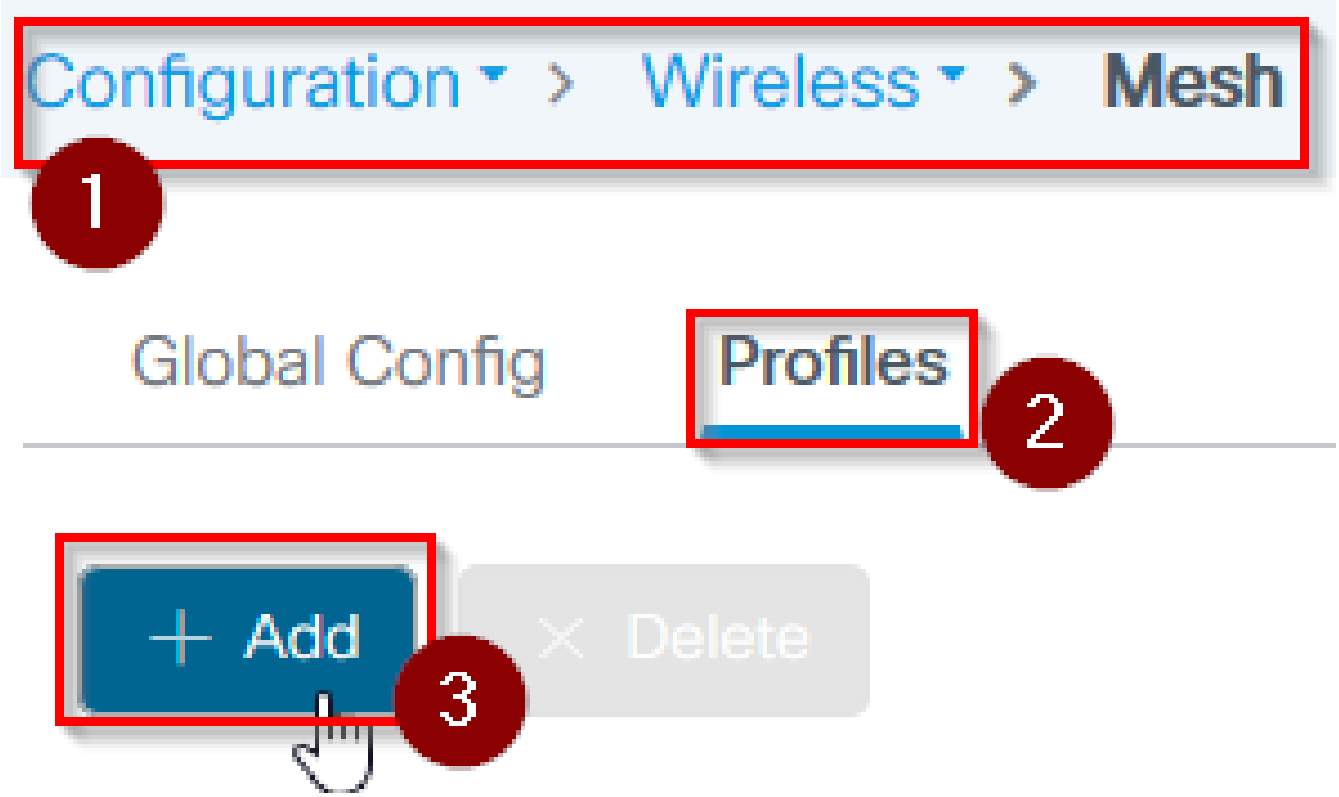
- Étape 9. Saisissez un nom dans le champ Method List Name, sélectionnez Credential download dans la liste déroulante Type* et local pour le champ Group Type, puis sélectionnez Apply to Device



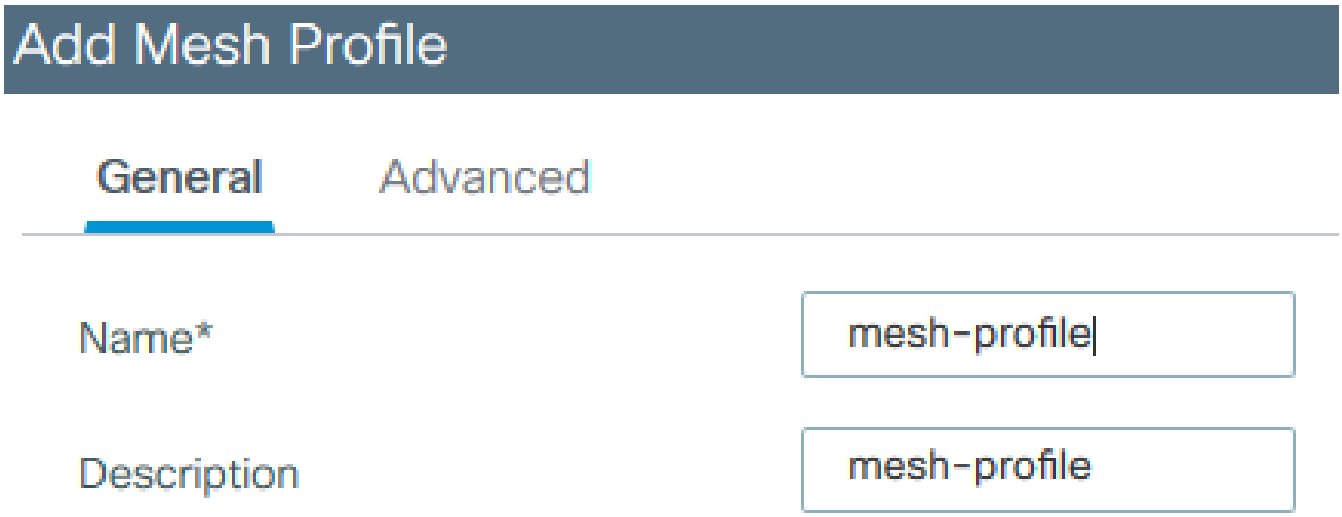
- Étape 9b. Si votre point d'accès se connecte directement en mode Bridge (c'est-à-dire qu'il

ne se connecte pas d'abord en mode local), répétez l'étape 9 pour la méthode de téléchargement des informations d'identification par défaut (CLI aaa autorisation credential-download default local)

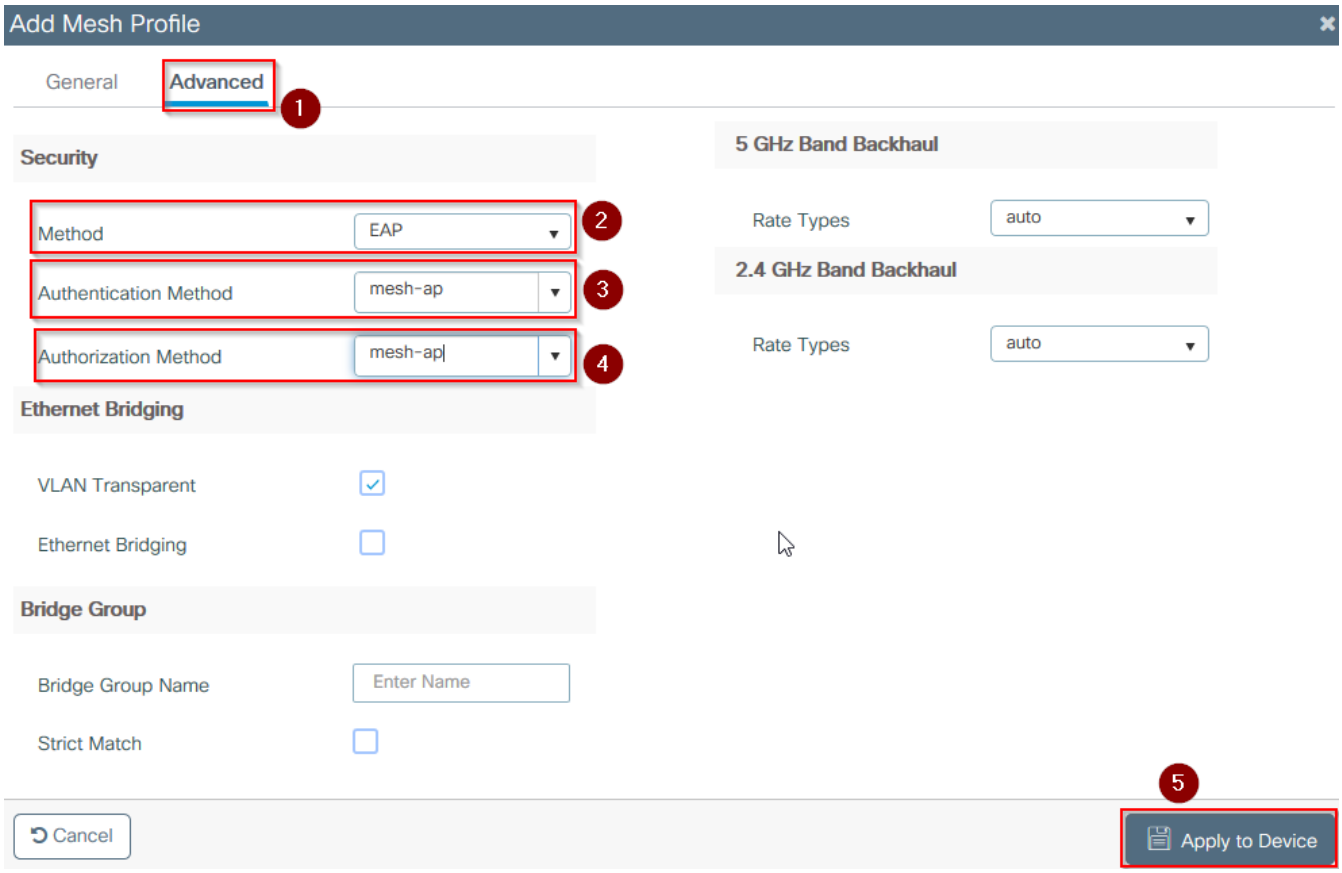
- Étape 10. Accédez à Configuration > Wireless > Mesh > Profiles
- Étape 11. Sélectionnez Ajouter, la fenêtre contextuelle Ajouter un profil de maillage apparaît



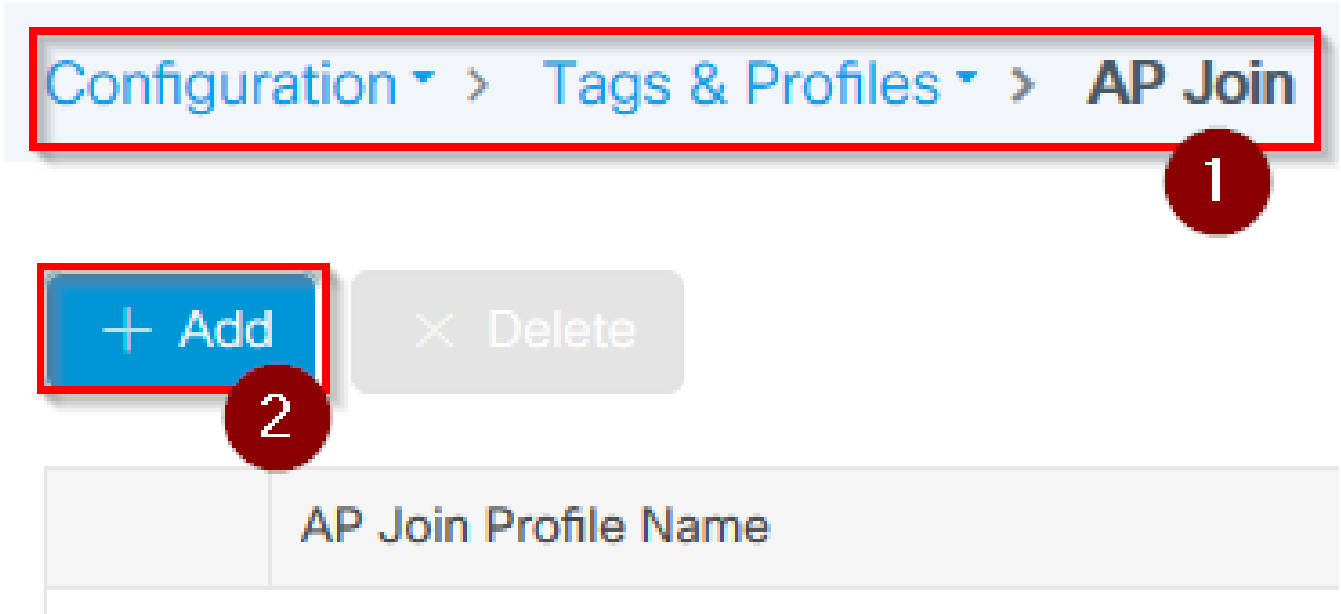
- Étape 12. Dans l'onglet Général, définissez un nom et une description pour le profil de maillage

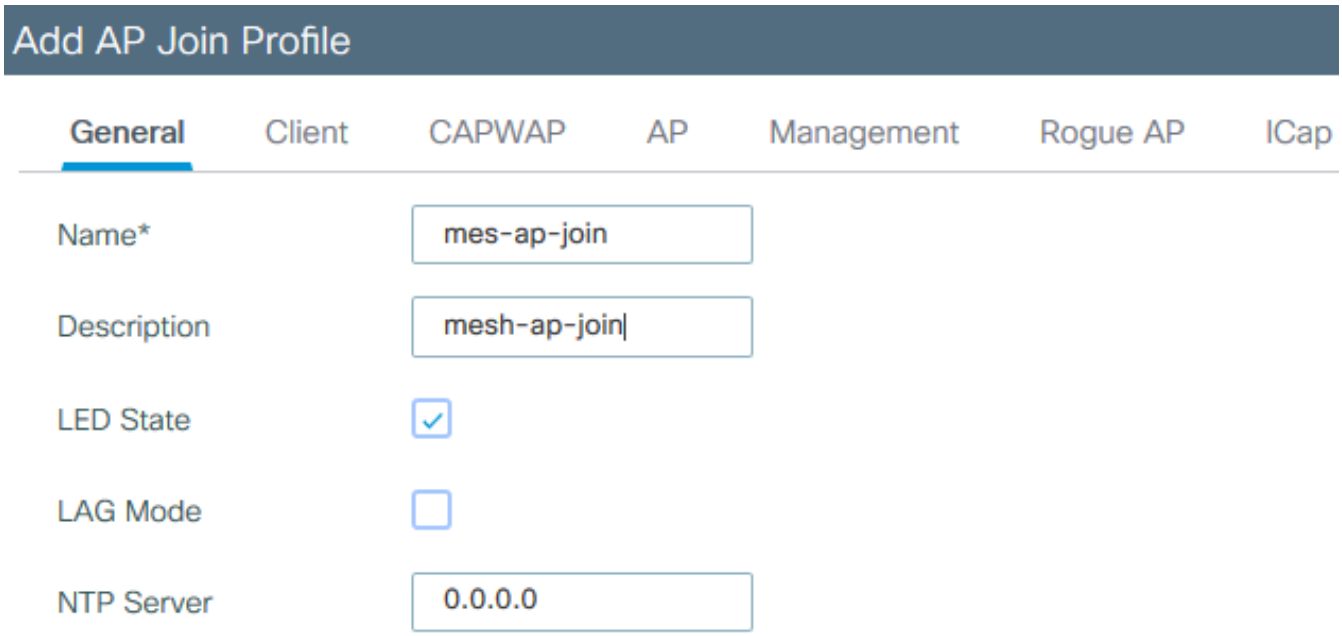


- Étape 13. Sous l'onglet Advanced, sélectionnez EAP pour le champ Method
- Étape 14. Sélectionnez le profil d'autorisation et d'authentification défini aux étapes 6 et 9, puis sélectionnez Apply to Device (Appliquer au périphérique)

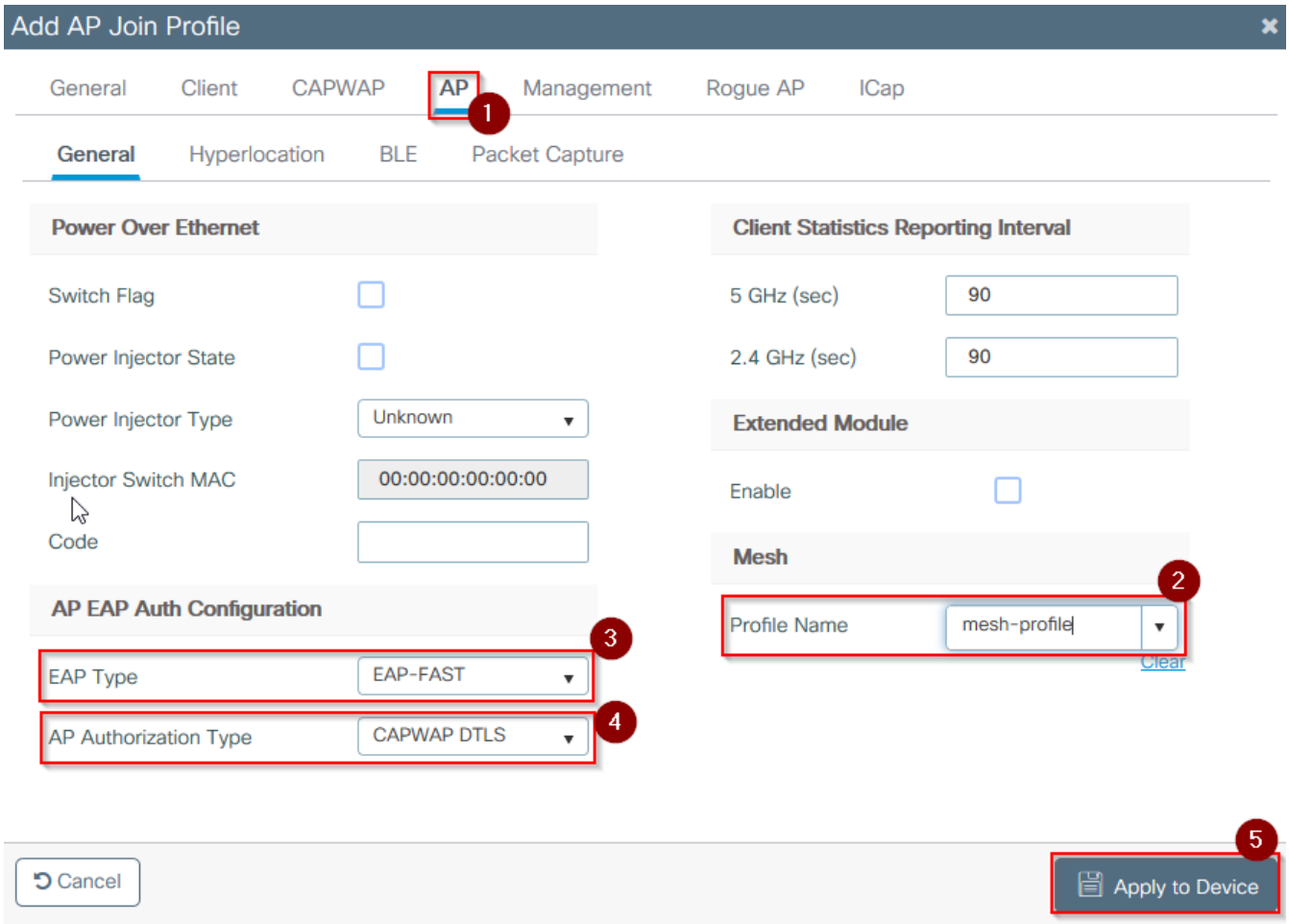


- Étape 15. Accédez à Configuration > Tag & Profiles > AP Join > Profile
- Étape 16. Sélectionnez Add, la fenêtre contextuelle AP Join Profile apparaît, définissez un nom et une description pour le profil AP Join



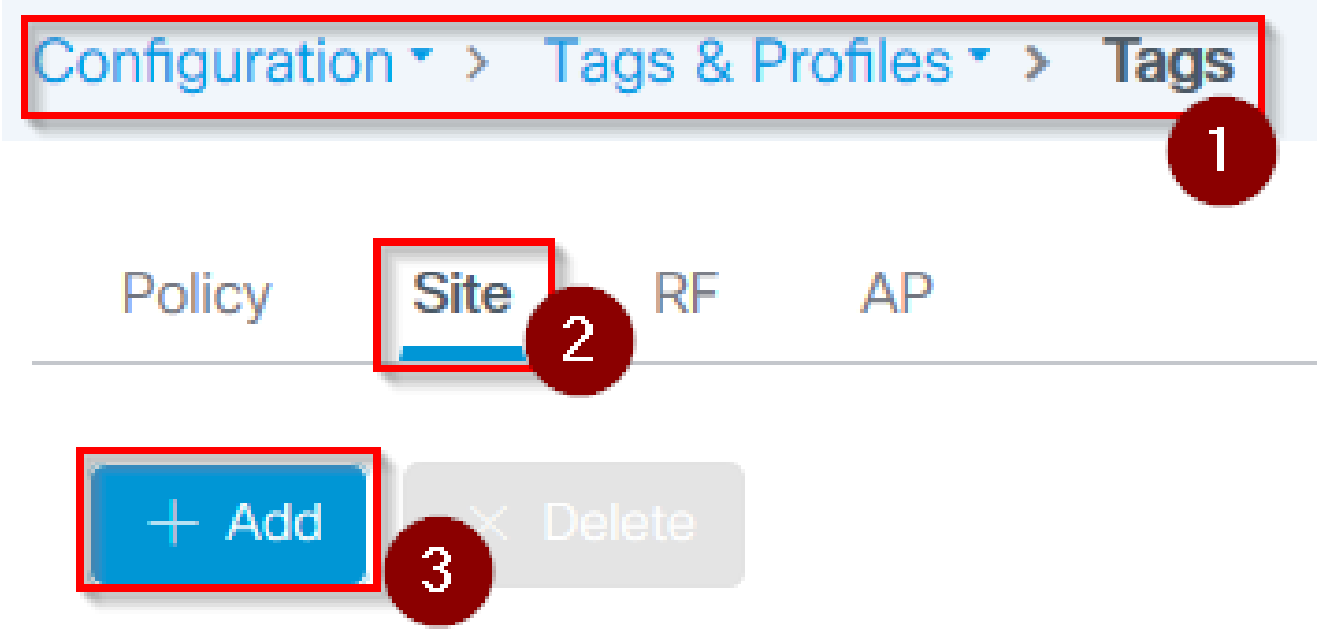


- Étape 17. Accédez à l'onglet AP et sélectionnez le profil de maillage créé à l'étape 12 dans la liste déroulante Nom du profil de maillage
- Étape 18. Assurez-vous que EAP-FAST et CAPWAP DTLS sont définis pour les champs respectivement EAP Type et AP Authorization Type
- Stéo 19. Sélectionnez Apply to Device

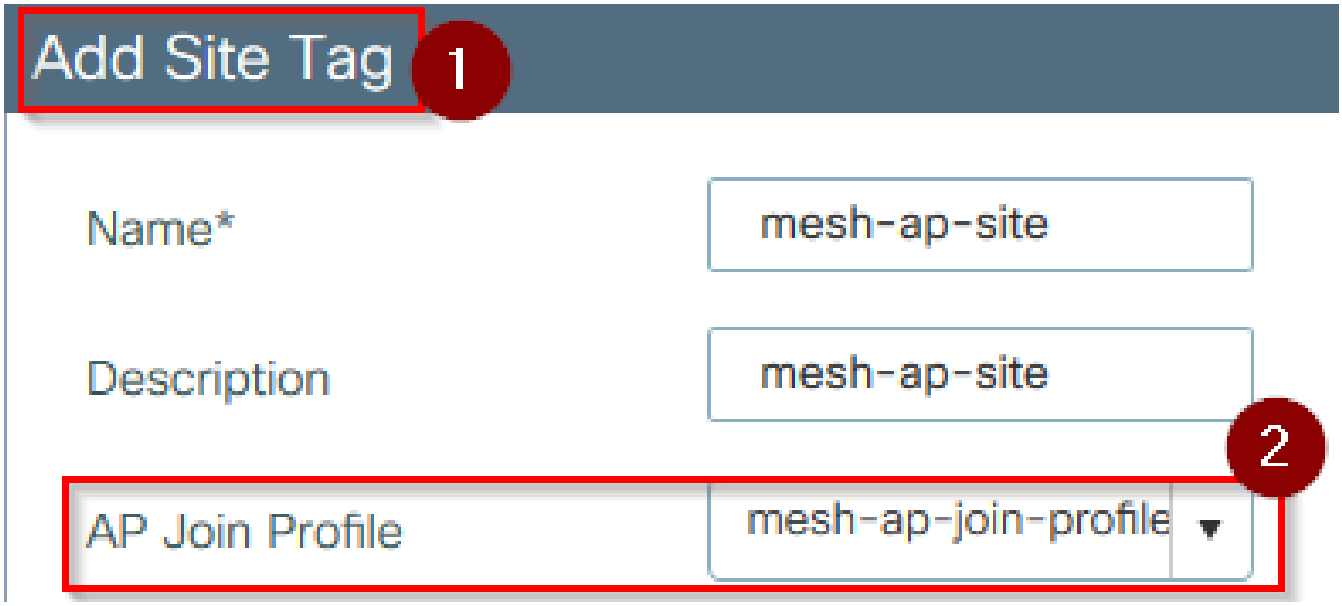


- Étape 20. Accédez à Configuration > Tag & Profiles > Tags > Site

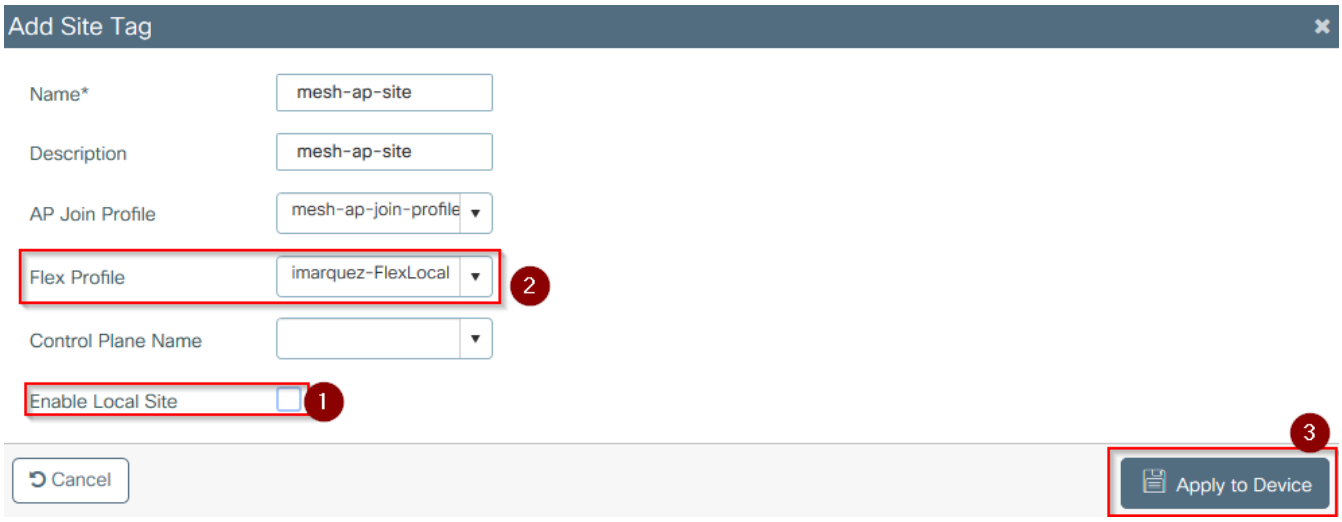
- Étape 21. Sélectionnez Add, la fenêtre contextuelle Site Tag s'affiche



-
- Étape 22. Entrez un nom et une description pour la balise de site



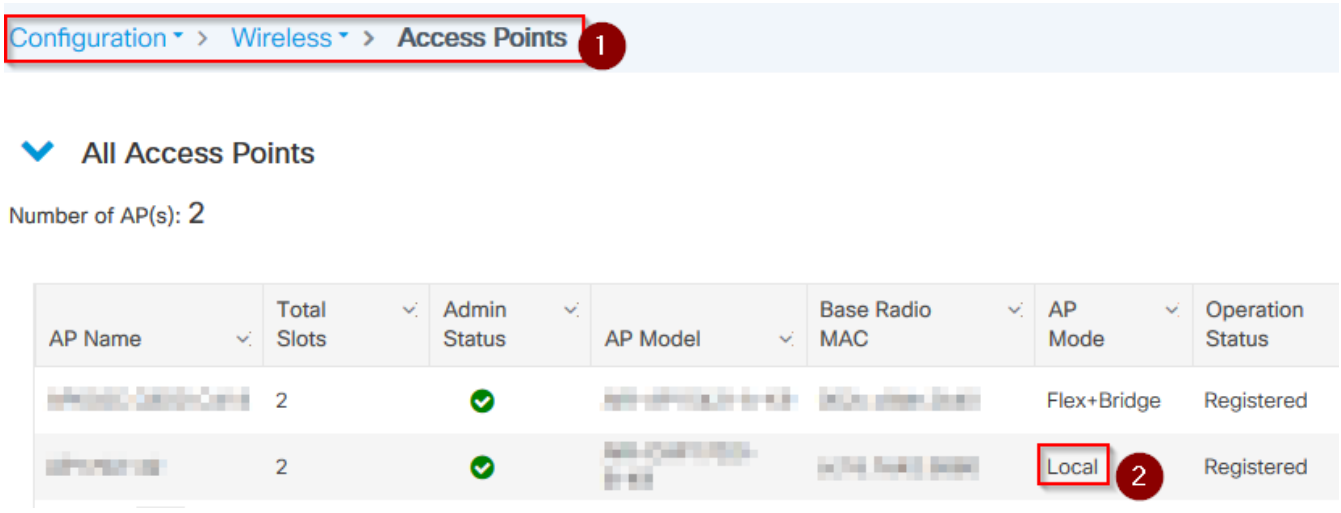
- Étape 23. Sélectionnez le profil de jointure AP créé à l'étape 16 dans la liste déroulante AP Join Profile
- Étape 24. Au bas de la fenêtre contextuelle Balise du site, décochez la case Enable Local Site pour activer la liste déroulante Flex Profile.
- Étape 35. Dans la liste déroulante Flex Profile, sélectionnez le profil Flex Profile que vous souhaitez utiliser pour l'AP



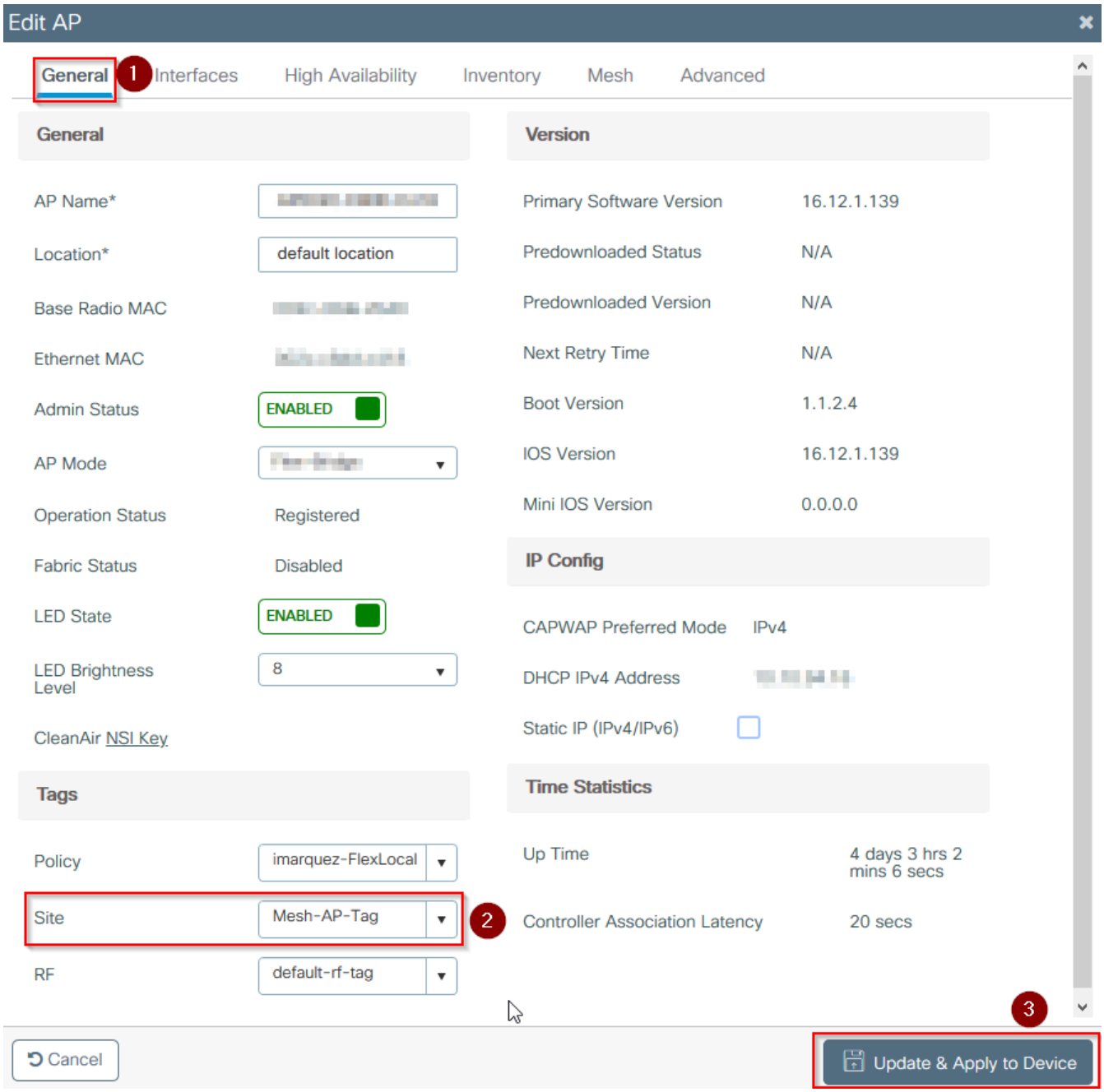
- Étape 36. Connectez le point d'accès au réseau et assurez-vous qu'il est en mode local.
- Étape 37. Pour vous assurer que le point d'accès est en mode local, émettez la commande capwap ap mode local.

  Le point d'accès doit avoir un moyen de trouver le contrôleur, soit la diffusion L2, DHCP Option 43, la résolution DNS ou la configuration manuelle.

- Étape 38. Le point d'accès rejoint le WLC, assurez-vous qu'il est répertorié dans la liste AP, naviguez vers Configuration > Wireless > Access Points > All Access Points



- Étape 39. Sélectionnez le point d'accès, la fenêtre contextuelle AP apparaît.
- Étape 40. Sélectionnez la balise de site créée à l'étape 22 sous Général > Balises > onglet Site dans la fenêtre contextuelle AP, sélectionnez Mettre à jour et appliquer au périphérique



- Étape 41. L'AP redémarre et doit joindre le WLC en mode Flex + Bridge

Notez que cette méthode joint d'abord le point d'accès en mode local (où il n'effectue pas l'authentification dot1x) pour appliquer la balise de site avec le profil maillé, puis bascule le point d'accès en mode pont.

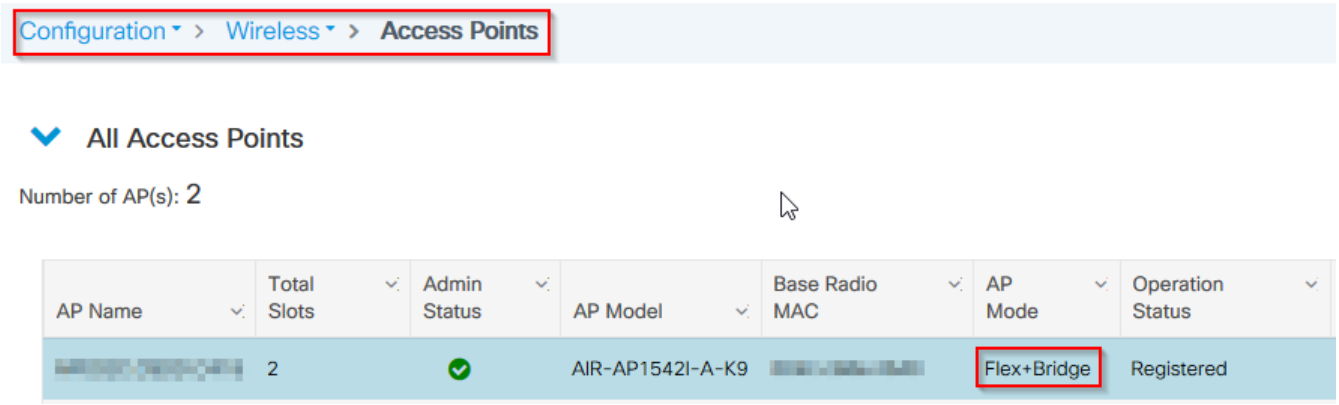
Pour joindre un AP qui est bloqué en mode Bridge (ou Flex+Bridge), configurez les méthodes par défaut (aaa authentication dot1x default local et aaa authorization cred default local).

Le point d'accès est alors capable de s'authentifier et vous pouvez assigner les balises par la suite.

Vérifier

Assurez-vous que le mode AP est affiché sous la forme Flex + Bridge, comme illustré dans cette

image.



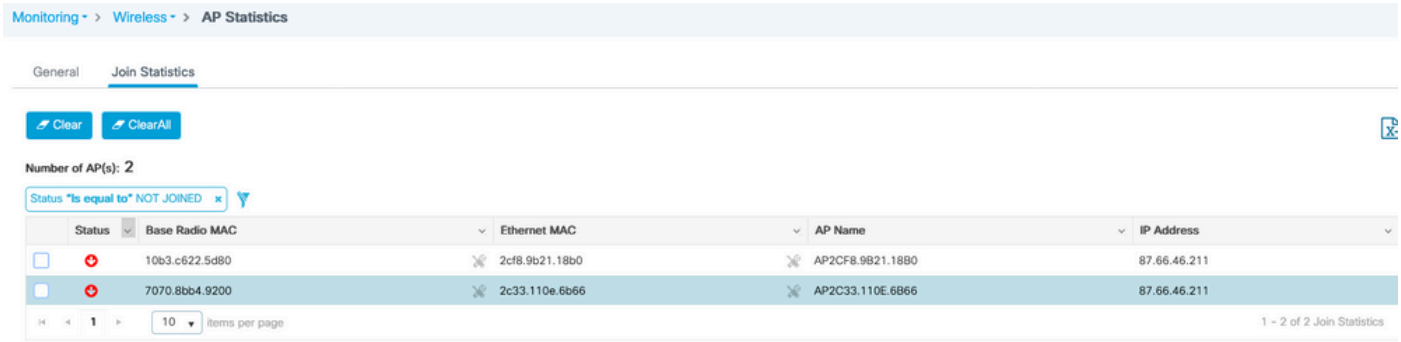
Exécutez ces commandes à partir de l'interface de ligne de commande du WLC 9800 et recherchez l'attribut AP Mode. Il doit être répertorié comme Flex+Bridge

```
aaa authorization credential-download mesh-ap local
aaa authentication dot1x mesh-ap local
wireless profile mesh default-mesh-profile
 description "default mesh profile"
wireless tag site meshsite
 ap-profile meshapjoin
 no local-site
ap profile meshapjoin
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
 mesh-profile mesh-profile
```

Dépannage

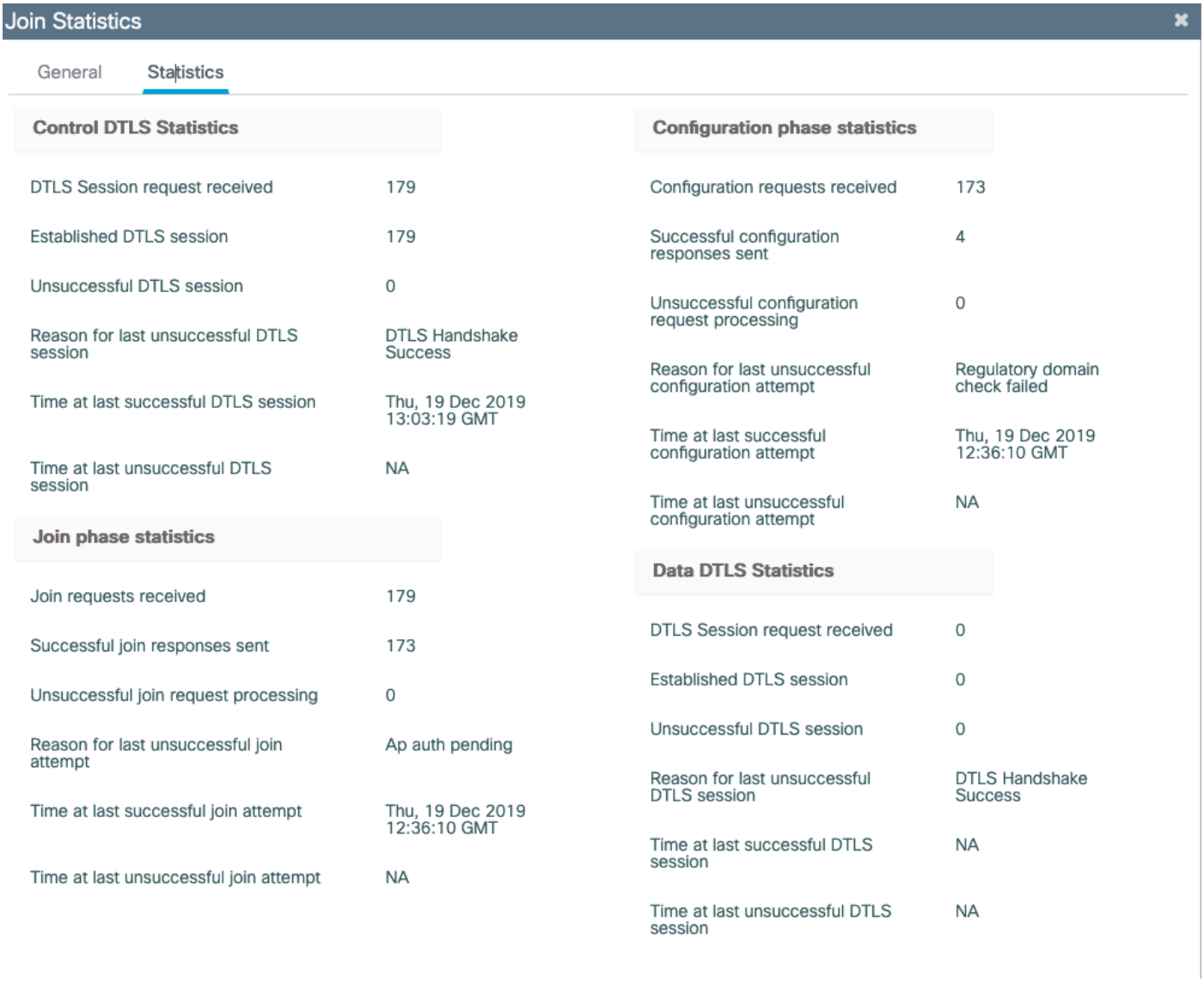
Assurez-vous que les commandes aaa authentication dot1x default local et aaa authorization cred default local sont présentes. Ils sont nécessaires si votre AP n'a pas été pré-joint en mode local.

Le tableau de bord principal 9800 a un widget qui affiche les points d'accès qui ne peuvent pas se joindre. Cliquez dessus pour obtenir la liste des points d'accès qui ne parviennent pas à se connecter :



Cliquez sur le point d'accès spécifique pour voir la raison pour laquelle il n'est pas joint. Dans ce cas, nous voyons un problème d'authentification (AP auth pending) parce que la balise de site n'a pas été assignée à l'AP.

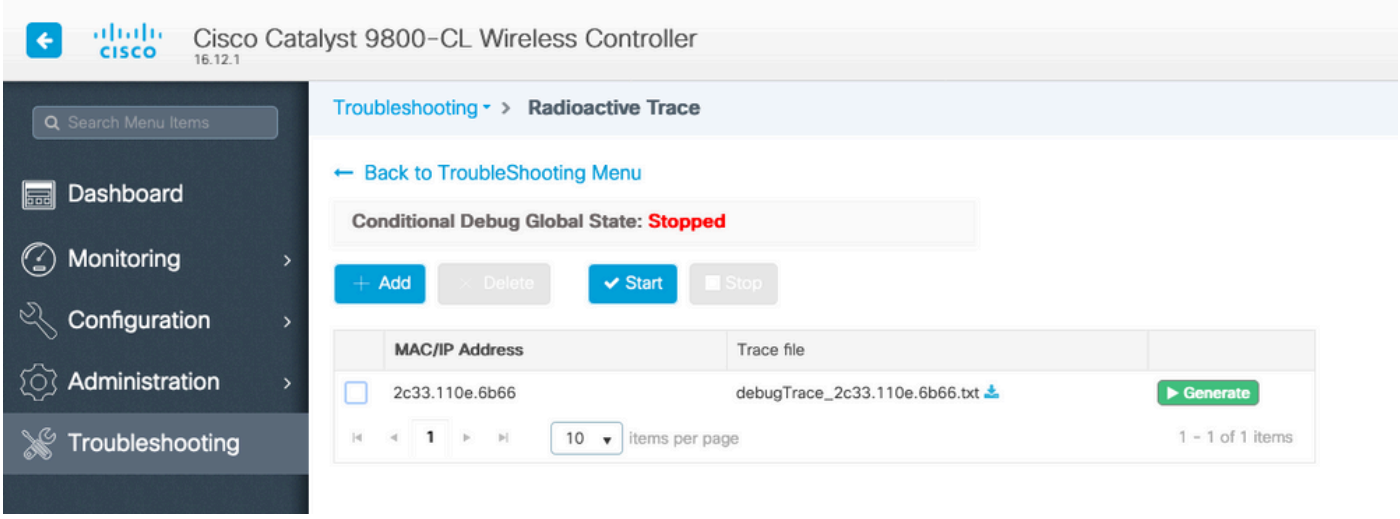
Par conséquent, le 9800 n'a pas choisi la méthode d'authentification/autorisation nommée pour authentifier le point d'accès :



Pour un dépannage plus avancé, accédez à la page Troubleshooting > Radioactive Trace sur l'interface utilisateur Web.

Si vous entrez l'adresse MAC de l'AP, vous pouvez immédiatement générer un fichier pour obtenir les journaux toujours actifs (au niveau de notification) de l'AP qui tente de se joindre.

Cliquez sur Démarrer pour activer le débogage avancé pour cette adresse MAC. La prochaine fois que les journaux sont générés, générez les journaux, les journaux de niveau de débogage pour la jointure AP sont affichés.


Cisco Catalyst 9800-CL Wireless Controller
16.12.1
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Troubleshooting > Radioactive Trace
Back to TroubleShooting Menu
Conditional Debug Global State: Stopped
Add
Delete
Start
Stop
MAC/IP Address
Trace file
2c33.110e.6b66
debugTrace_2c33.110e.6b66.txt
Generate
1
10
items per page
1 - 1 of 1 items

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.