Configuration de FlexConnect avec authentification sur le WLC Catalyst 9800

Table des matières

- Introduction
- Conditions préalables
- Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
- Configurations
    - Configuration AAA sur les WLC 9800
    - Configuration d'un réseau local sans fil (WLAN)
    - Configuration du profil des politiques
    - Configuration des balises des politiques
    - Configuration du profil flexible
    - Configuration des balises de site
  - Authentification locale avec serveur RADIUS externe
- Vérifier
- Dépannage

Introduction

Ce document décrit comment configurer FlexConnect avec l'authentification centrale ou locale sur le contrôleur LAN sans fil Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- FlexConnect
- 802.1x

Composants utilisés

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

- C980-CL, Cisco IOS-XE® 17.3.4

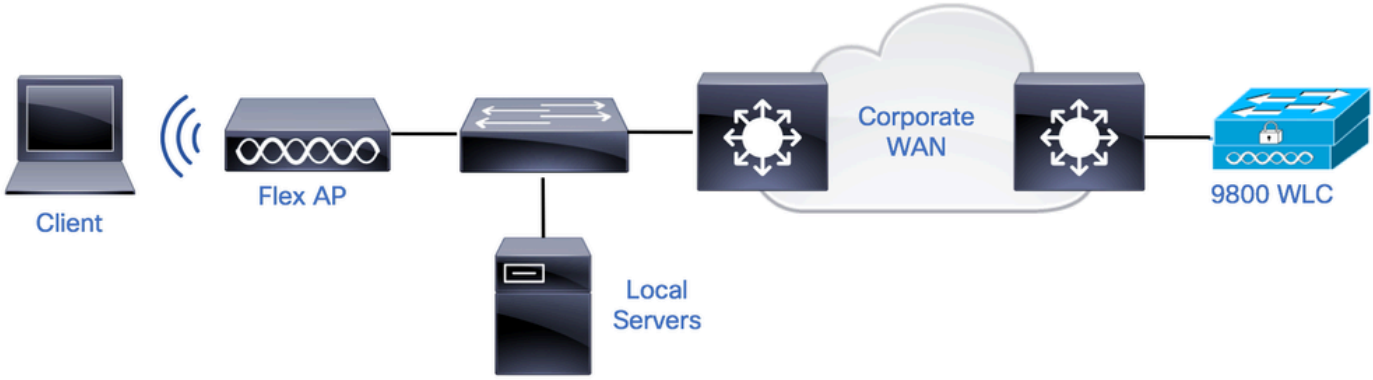
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

FlexConnect est une solution sans fil pour le déploiement de bureaux distants. Il vous permet de configurer des points d'accès (AP) dans des emplacements distants à partir du bureau de l'entreprise via une liaison WAN (Wide Area Network) sans devoir déployer un contrôleur dans chaque emplacement. Les points d'accès FlexConnect peuvent commuter le trafic de données client localement et effectuer l'authentification client localement lorsque la connexion au contrôleur est perdue. En mode connecté, les points d'accès FlexConnect peuvent également effectuer une authentification locale.

Configurer

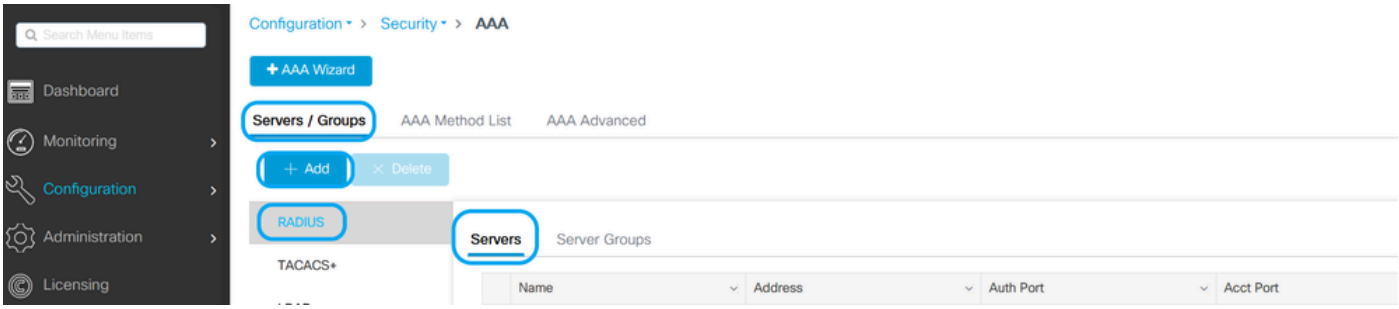
Diagramme du réseau



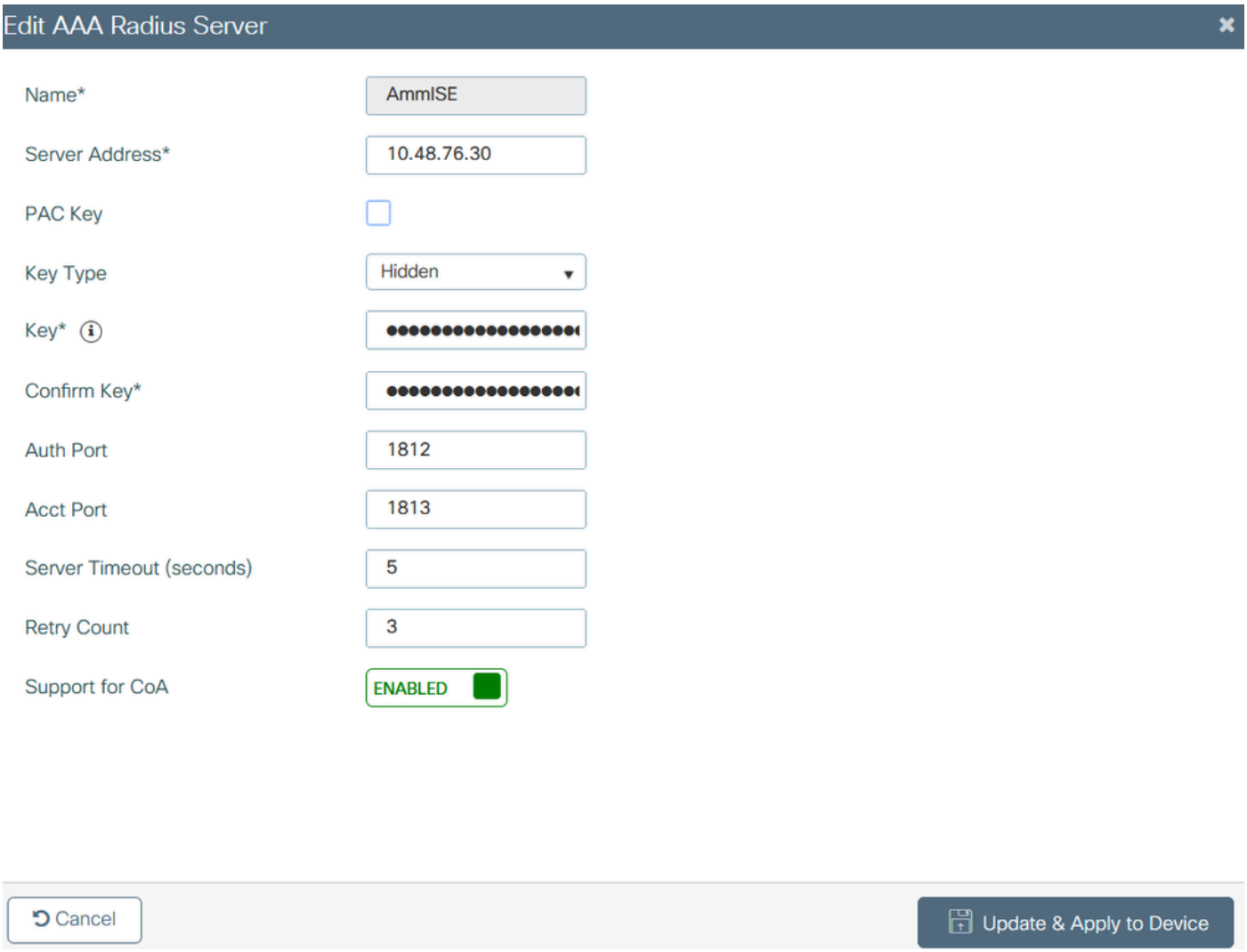
Configurations

Configuration AAA sur les WLC 9800

Étape 1 : déclaration du serveur RADIUS **À partir de la GUI :** Accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add et entrez les informations du serveur RADIUS.

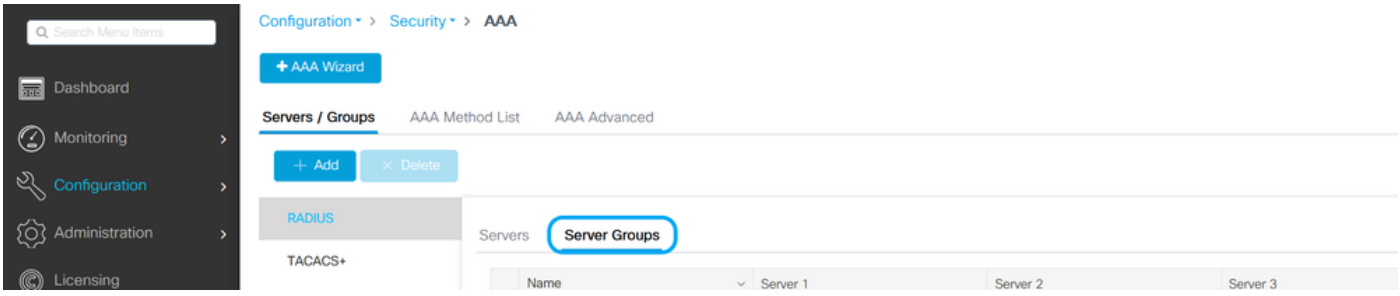


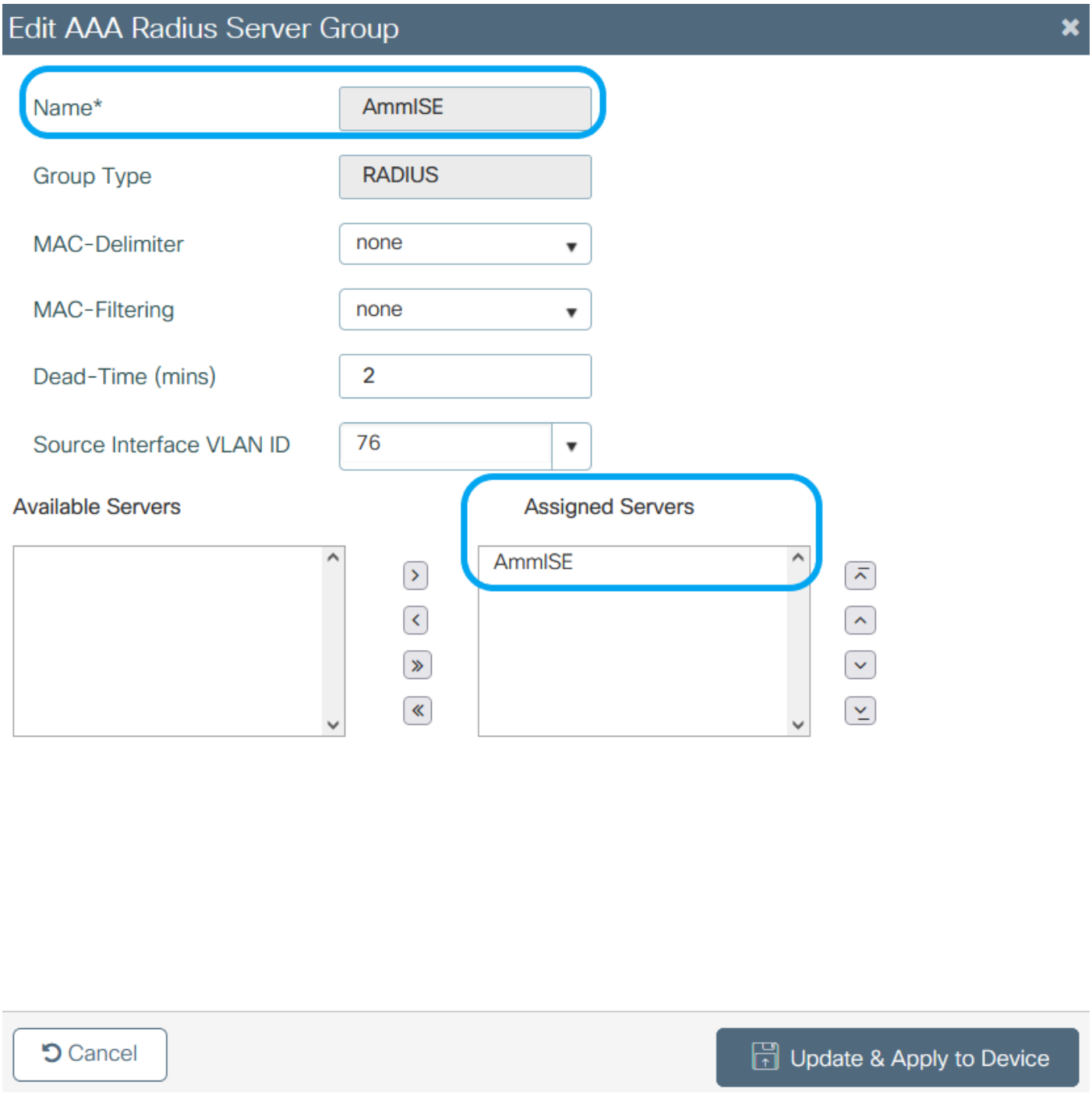
Assurez-vous que la prise en charge de CoA est activée si vous prévoyez d'utiliser tout type de sécurité qui nécessite CoA à l'avenir.



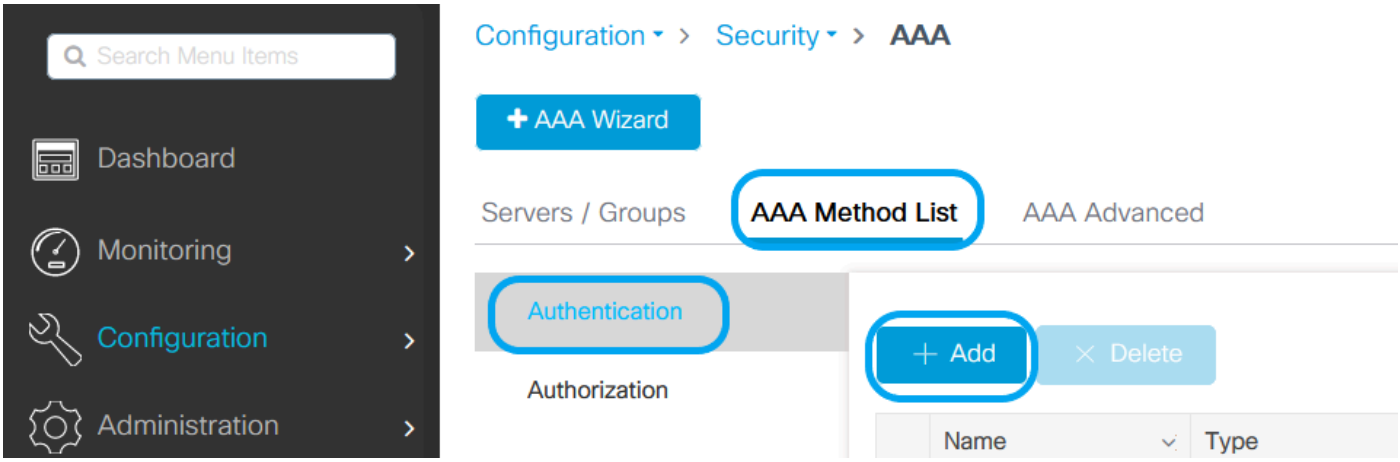
Remarque : Remarque : Radius CoA n'est pas pris en charge dans le déploiement d'authentification locale Flex Connect. .

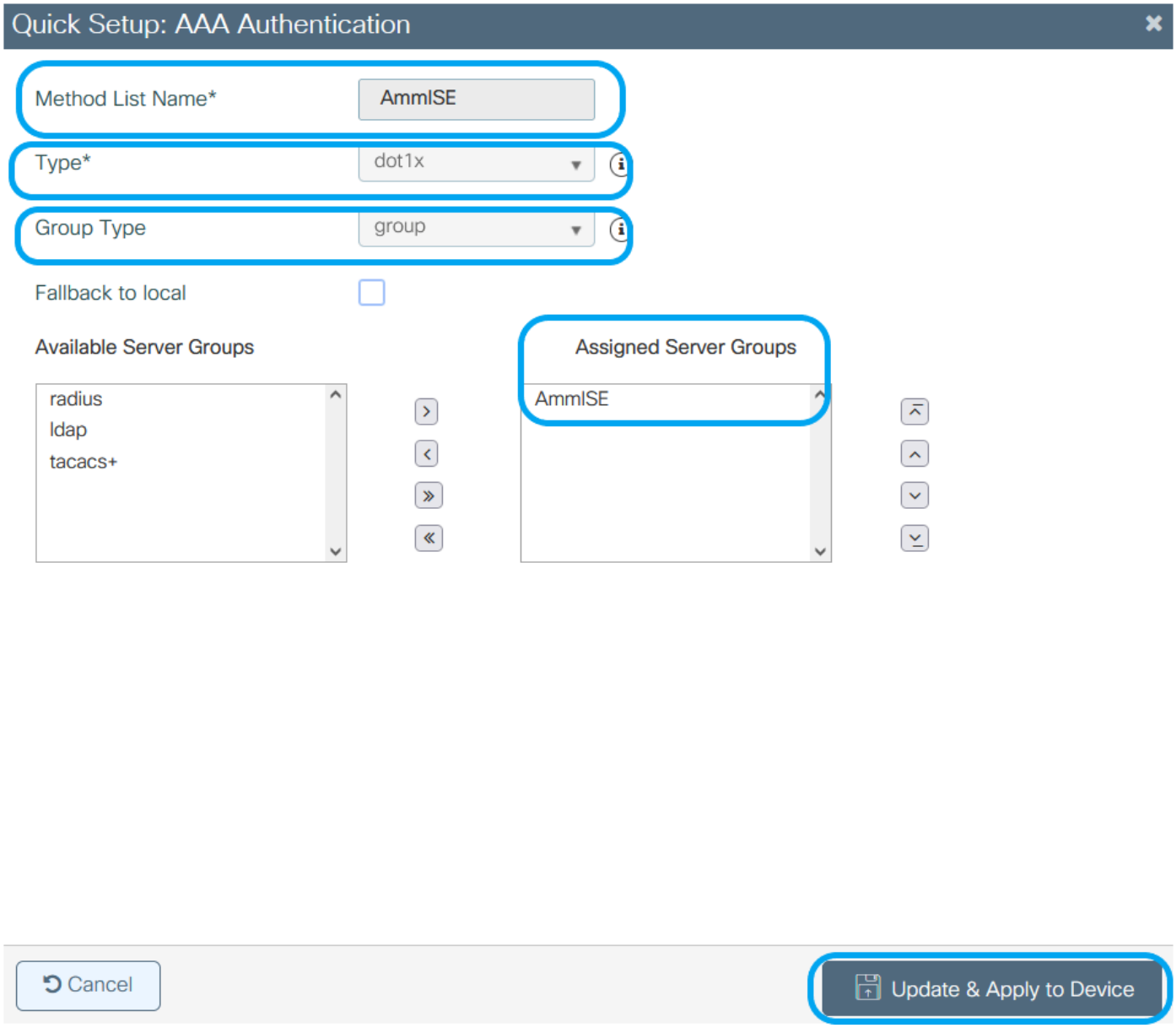
Étape 2. Ajout du serveur RADIUS à un groupe RADIUS. **À partir de l'interface utilisateur graphique :** Accédez à Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.





Étape 3 : création d'une liste de méthodes d'authentification **À partir de la GUI :** Accédez à Configuration > Security > AAA > AAA Method List > Authentication > + Add





À partir de 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

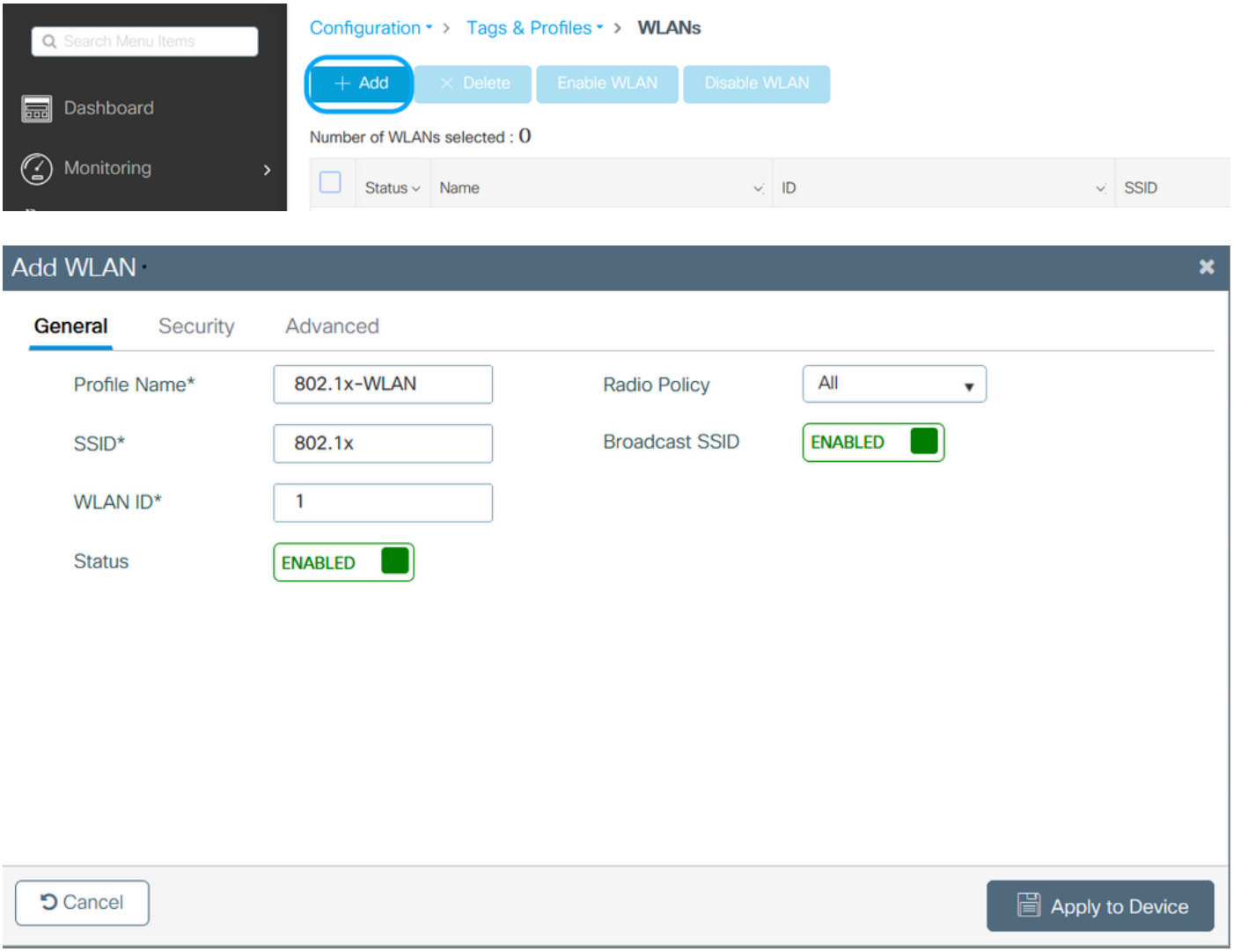
# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

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

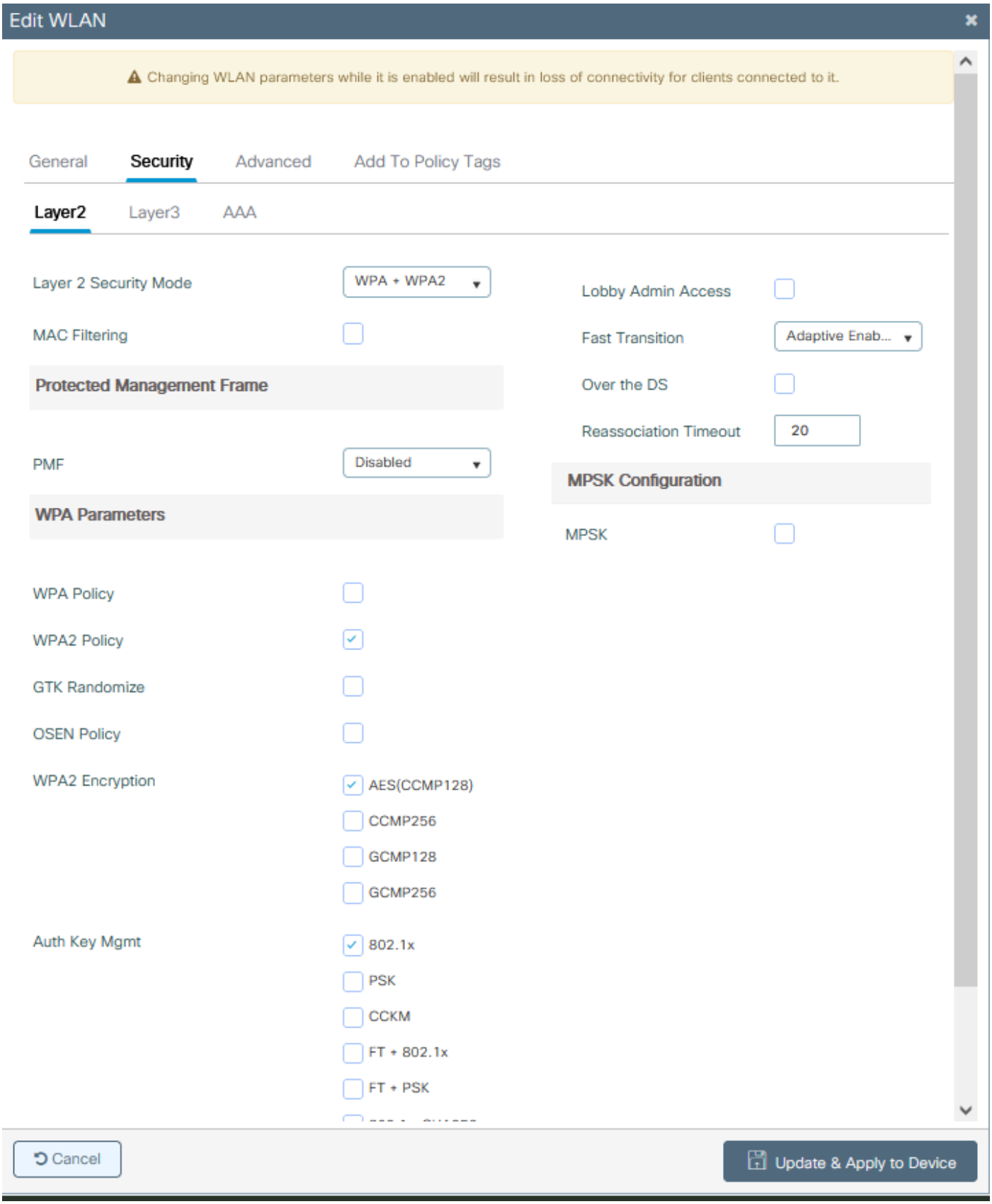
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Configuration d’un réseau local sans fil (WLAN)

Étape 1. **À partir de l’interface utilisateur :** Accédez à Configuration > Wireless > WLANs et cliquez sur +Add pour créer un nouveau WLAN, et entrez les informations WLAN. Cliquez ensuite sur Apply to Device.

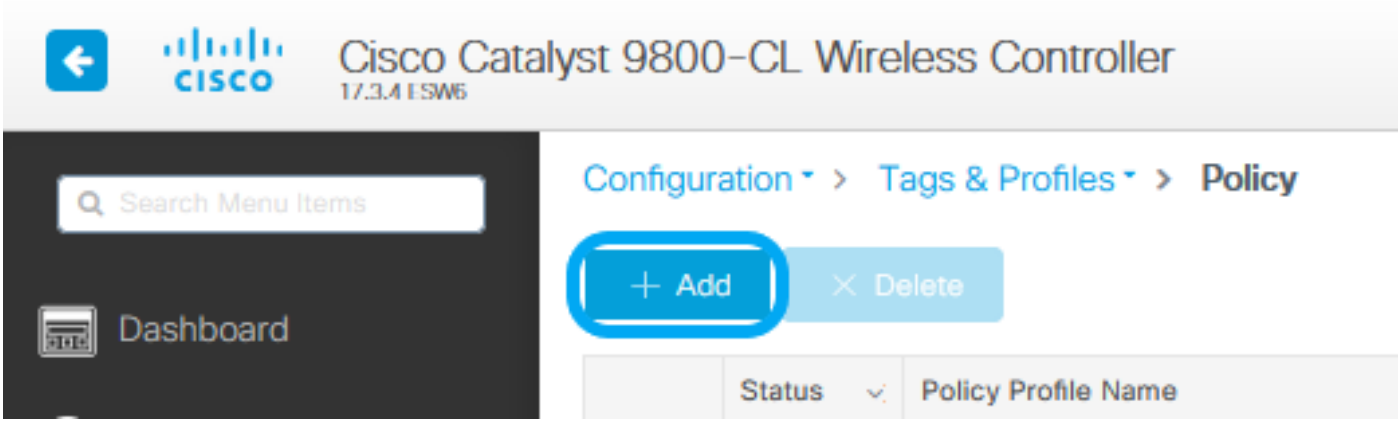


Étape 2. **À partir de l’interface utilisateur graphique : Accédez à l'onglet** Security pour configurer le mode de sécurité Layer2/Layer3 tant que la méthode de cryptage et la liste d'authentification au cas où 802.1x est utilisé. Cliquez ensuite sur Update & Apply to Device.

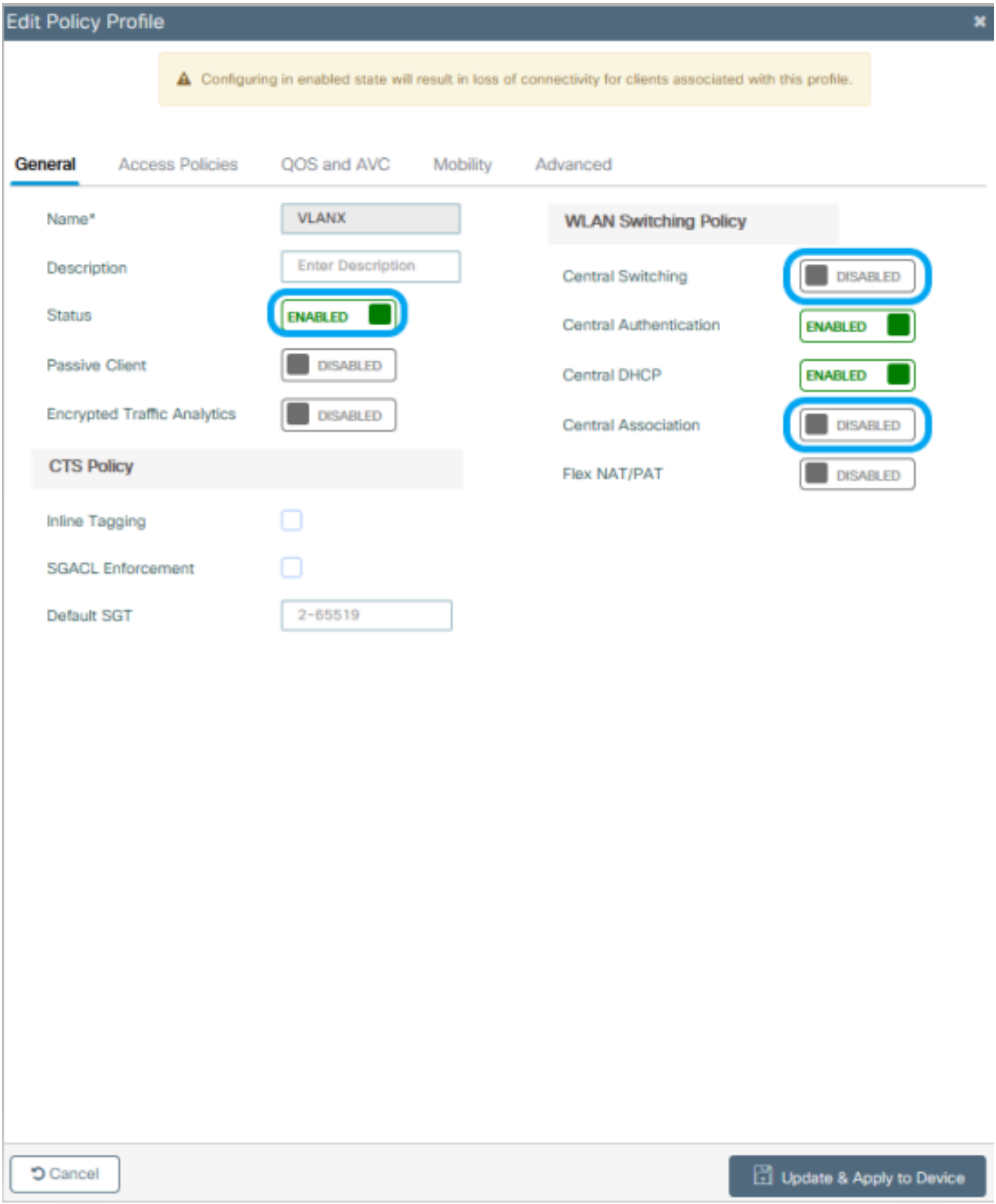


Configuration du profil des politiques

Étape 1. **À partir de l'interface graphique :** Accédez à Configuration > Tags & Profiles > Policy et cliquez sur +Add pour créer un profil de stratégie.



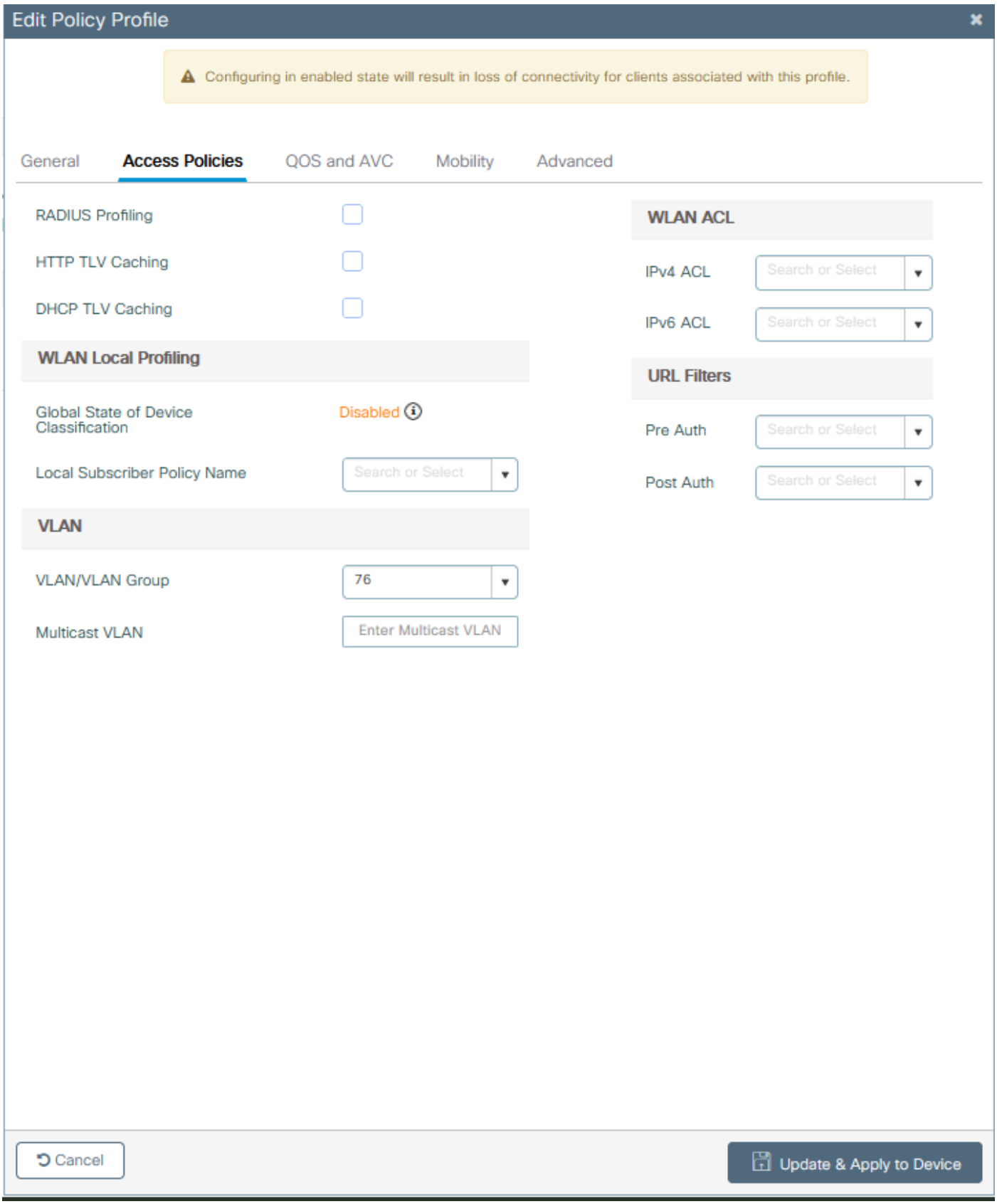
Étape 2. Ajoutez le nom et décochez la case Commutation centrale. Avec cette configuration, le contrôleur gère l'authentification client et le point d'accès FlexConnect commute localement les paquets de données client.



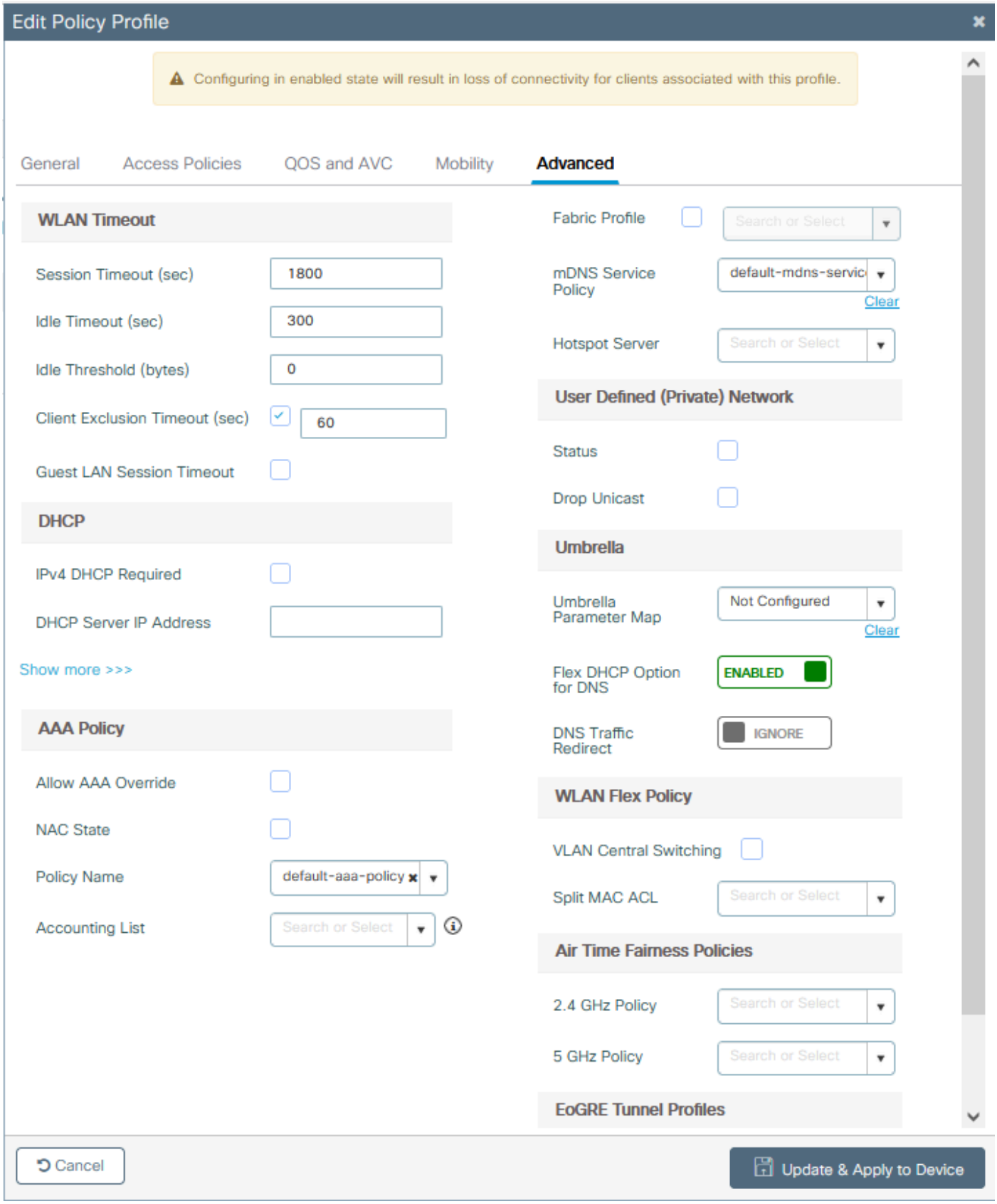
Remarque : L'association et la commutation doivent toujours être appariées, si la commutation centrale est désactivée, l'association centrale doit également être désactivée sur tous les profils de stratégie lorsque des points d'accès Flexconnect sont utilisés.

Étape 3. **À partir de l'interface utilisateur graphique : Accédez à l'onglet** Access Policies pour attribuer le VLAN auquel les clients sans fil peuvent être attribués lorsqu'ils se connectent à ce WLAN par défaut.
Vous pouvez sélectionner un nom de VLAN dans la liste déroulante ou, comme pratique recommandée, saisir

manuellement un ID de VLAN.

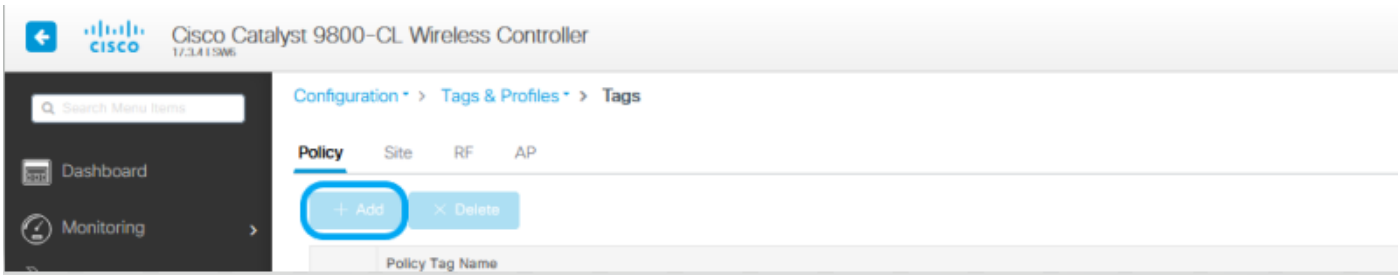


Étape 4. **À partir de l'interface utilisateur graphique :** Accédez à l'onglet Advanced pour configurer les délais d'expiration WLAN, DHCP, WLAN Flex Policy et la stratégie AAA au cas où ils sont utilisés. Cliquez ensuite sur Update & Apply to Device.

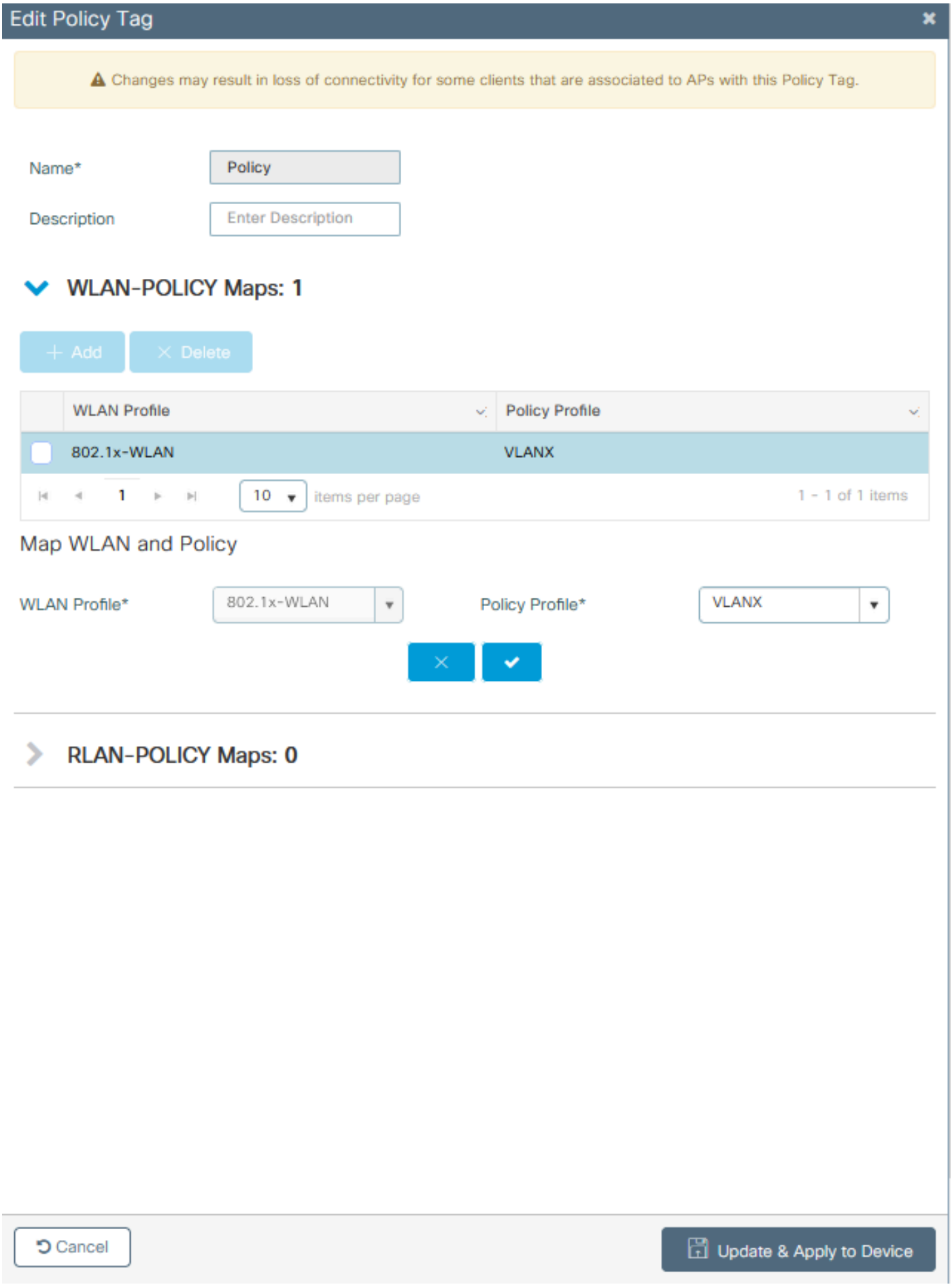


Configuration des balises des politiques

Étape 1. **À partir de l'interface graphique :** Accédez à Configuration > Tags & Profiles > Tags > Policy > +Add.

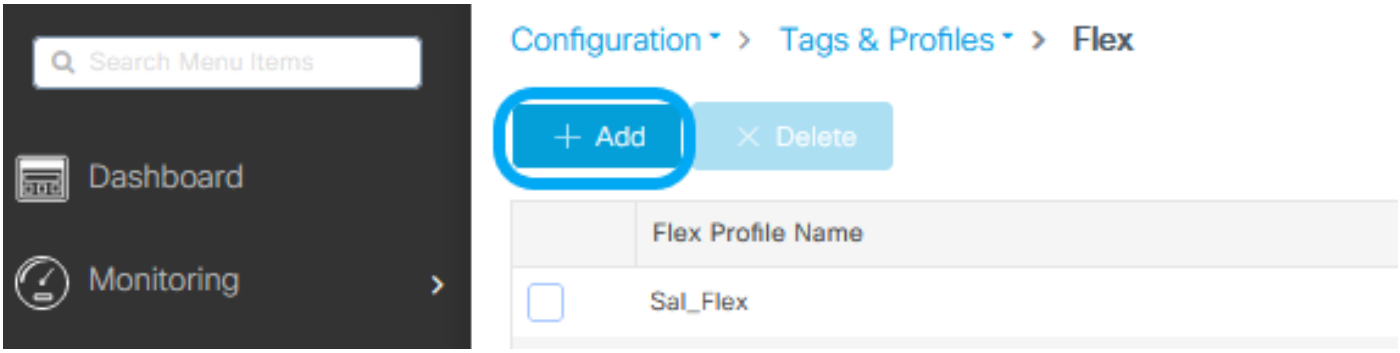


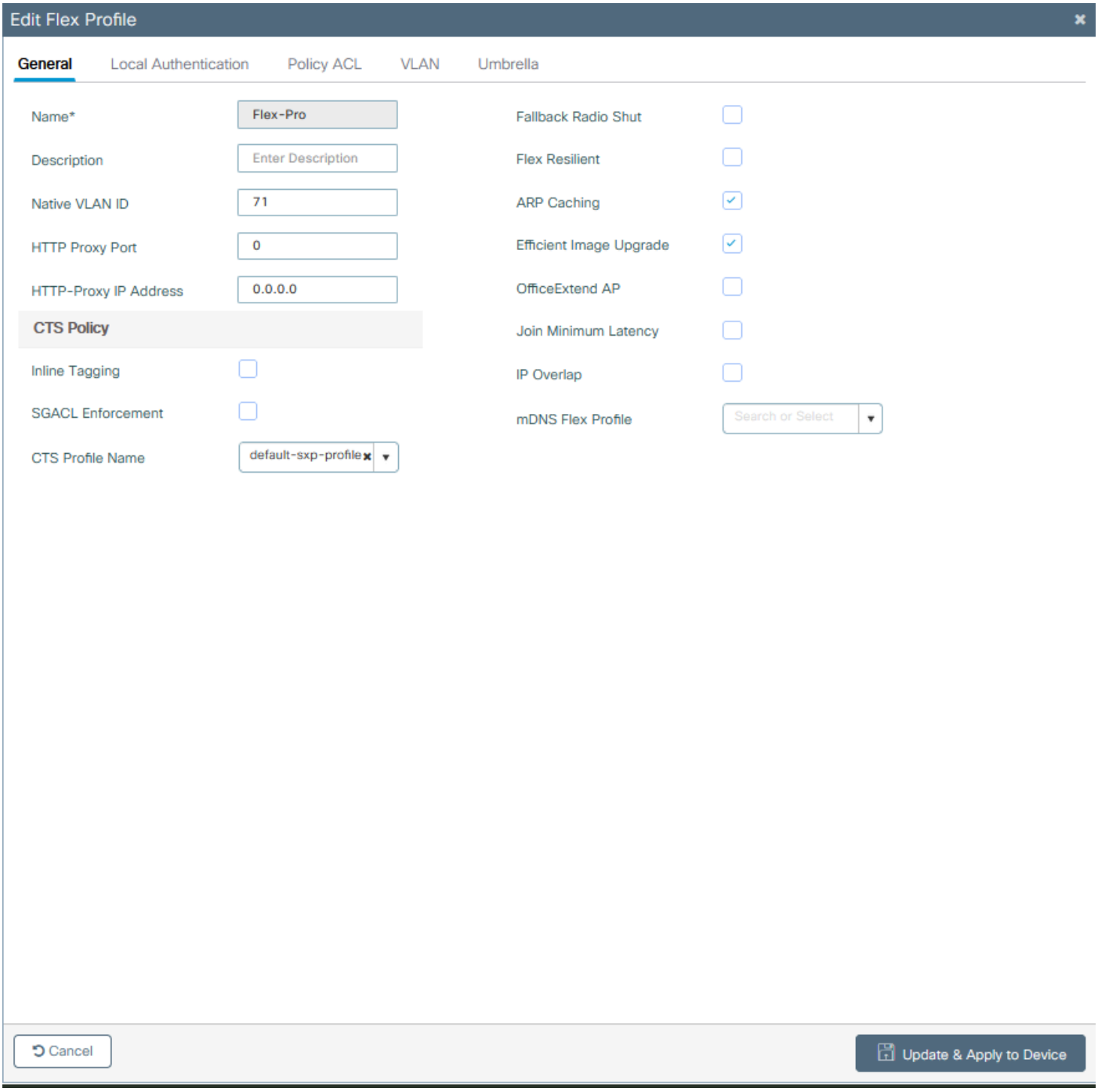
Étape 2. Attribuez un nom et mappez le profil de stratégie et le profil WLAN créés avant.



Configuration du profil flexible

Étape 1. **À partir de la GUI :** Accédez à Configuration > Tags & Profiles > Flex et cliquez sur +Add pour en créer un nouveau.

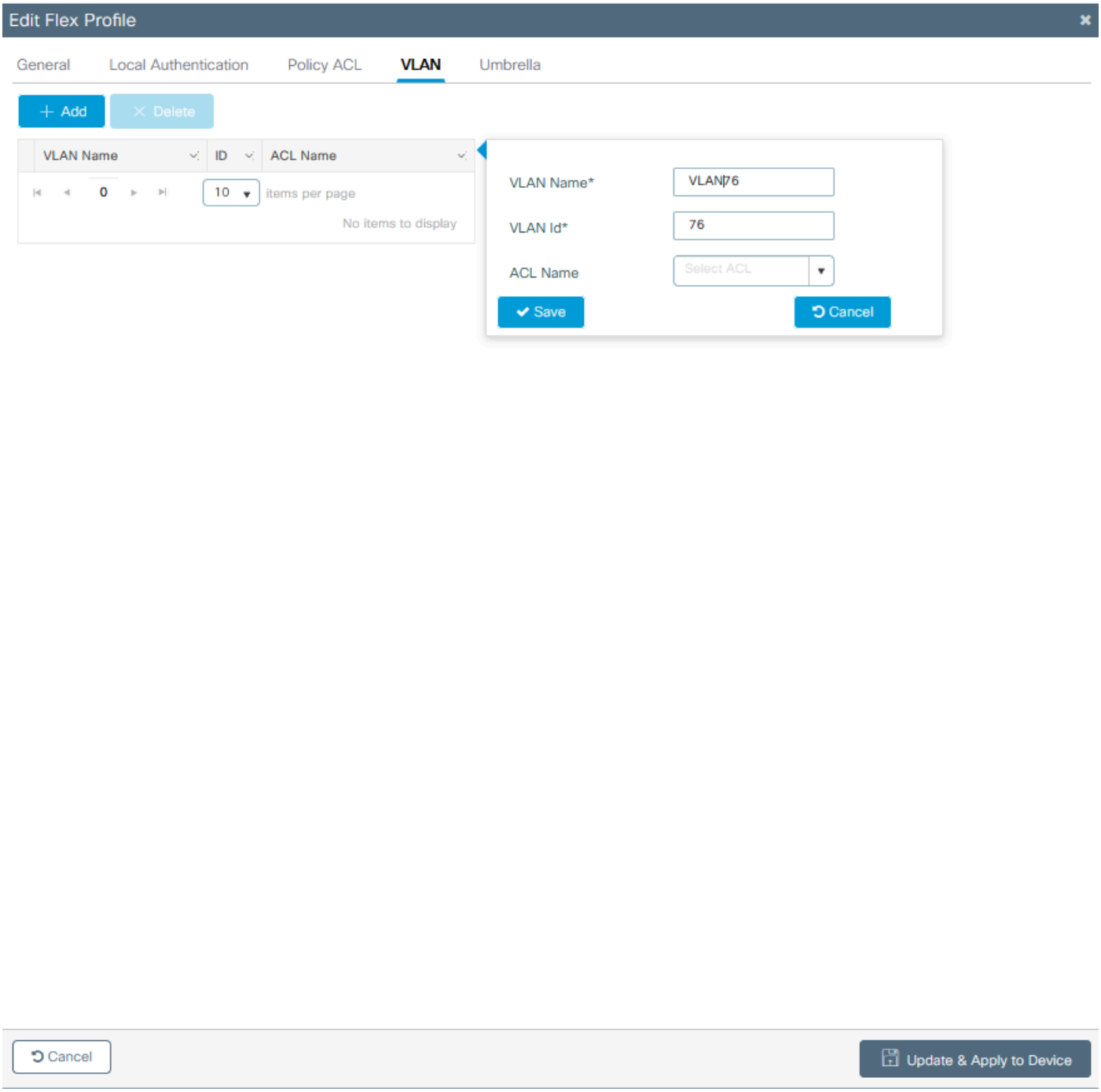




Remarque : L'ID de VLAN natif fait référence au VLAN utilisé par les AP qui peuvent obtenir ce profil flexible attribué, et il doit s'agir du même ID de VLAN configuré comme natif sur le

port de commutateur où les AP sont connectés.

Étape 2. Sous l'onglet VLAN, ajoutez les VLAN nécessaires, ceux affectés par défaut au WLAN via un profil de stratégie, ou ceux envoyés par un serveur RADIUS. Cliquez ensuite sur Update & Apply to Device.



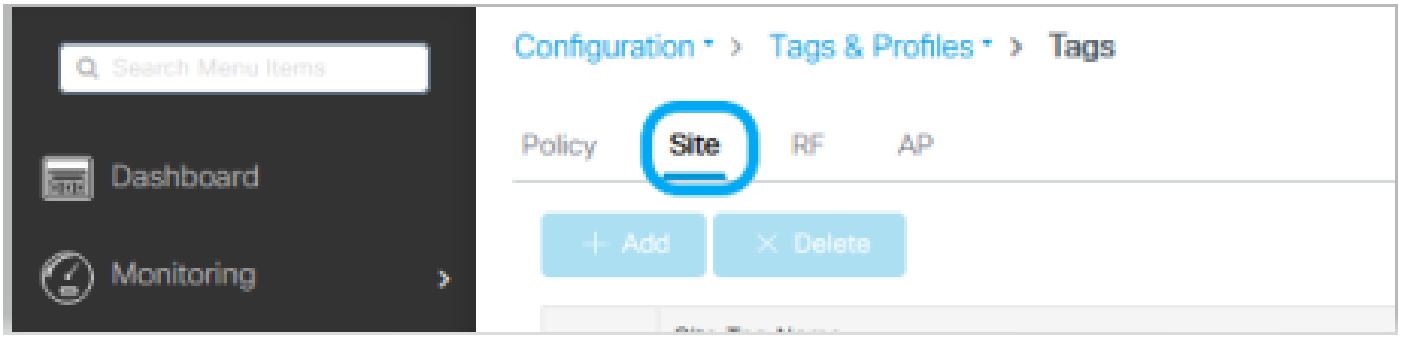
Remarque : pour Policy Profile, lorsque vous sélectionnez le VLAN par défaut affecté au SSID. Si vous utilisez un nom de VLAN à cette étape, assurez-vous que vous utilisez le même nom de VLAN dans la configuration Flex Profile, sinon les clients ne pourront pas se connecter au WLAN.

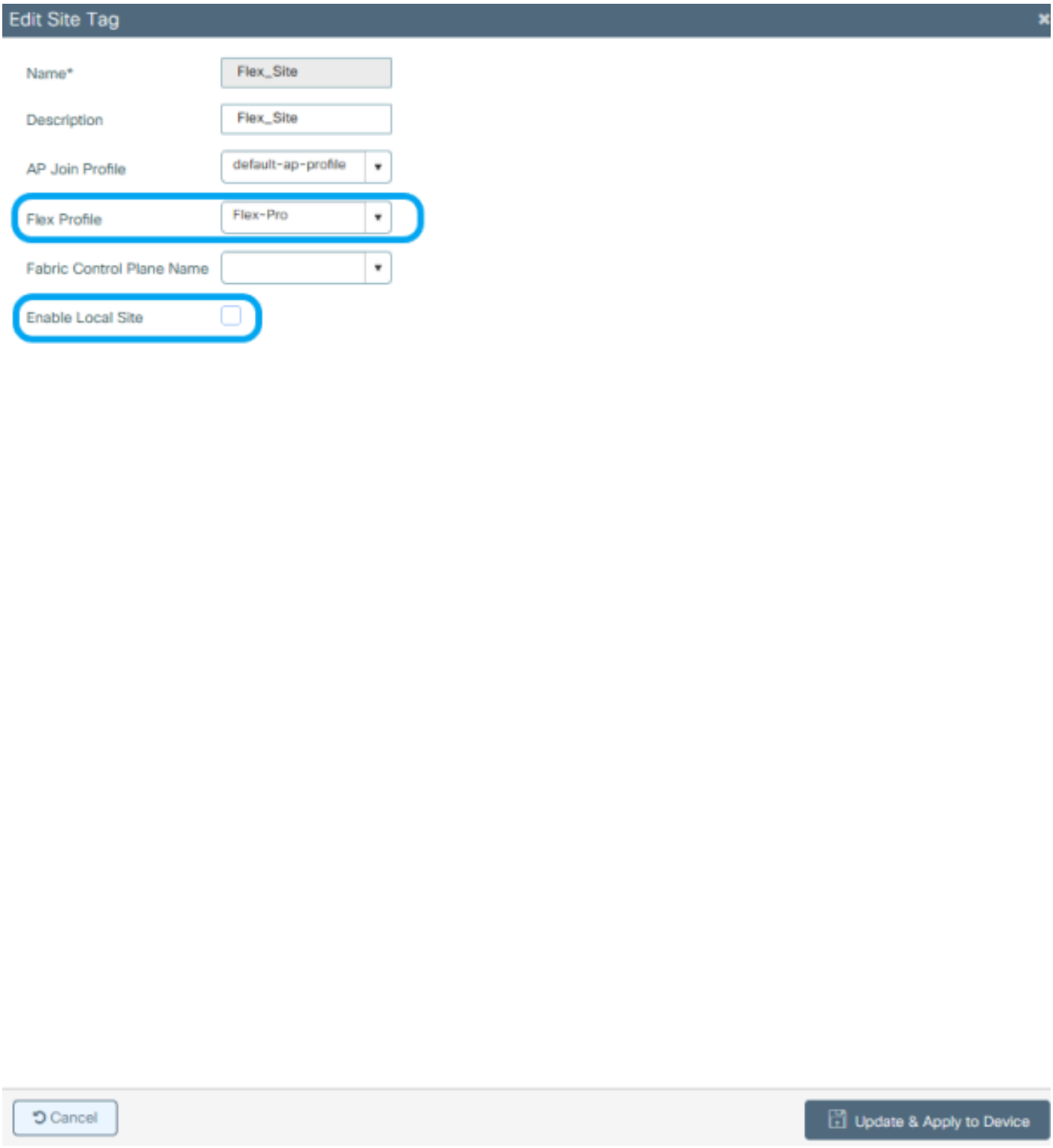
Remarque : Pour configurer une liste de contrôle d'accès pour flexConnect avec remplacement AAA, configurez-la uniquement sur « liste de contrôle d'accès de stratégie »,

si une liste de contrôle d'accès est attribuée à un VLAN spécifique, ajoutez une liste de contrôle d'accès sur lorsque vous ajoutez le VLAN, puis ajoutez la liste de contrôle d'accès sur la « liste de contrôle d'accès de stratégie ».

Configuration des balises de site

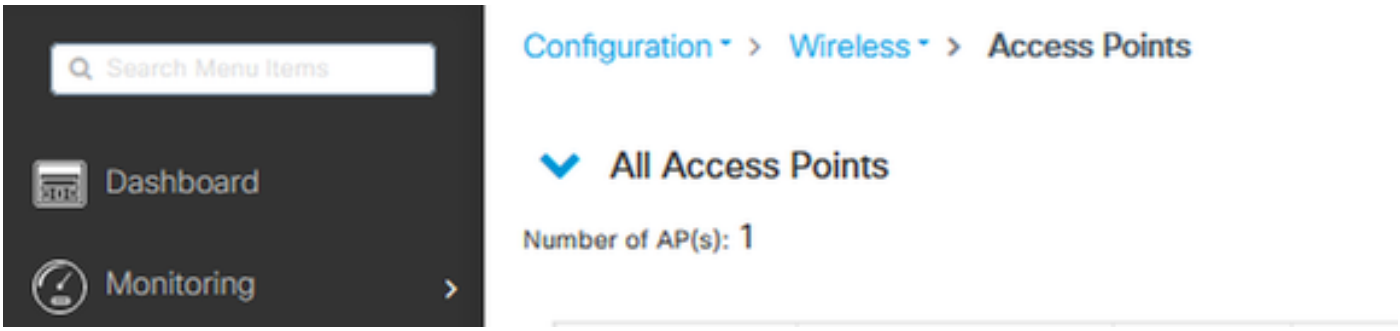
Étape 1. **À partir de l'interface utilisateur : Accédez à** Configuration > Tags & Profiles > Tags > Site et cliquez sur +Add pour créer une nouvelle balise de site. Décochez la case Enable Local Site pour permettre aux points d'accès de commuter le trafic de données client localement, et ajoutez le profil flexible créé précédemment.

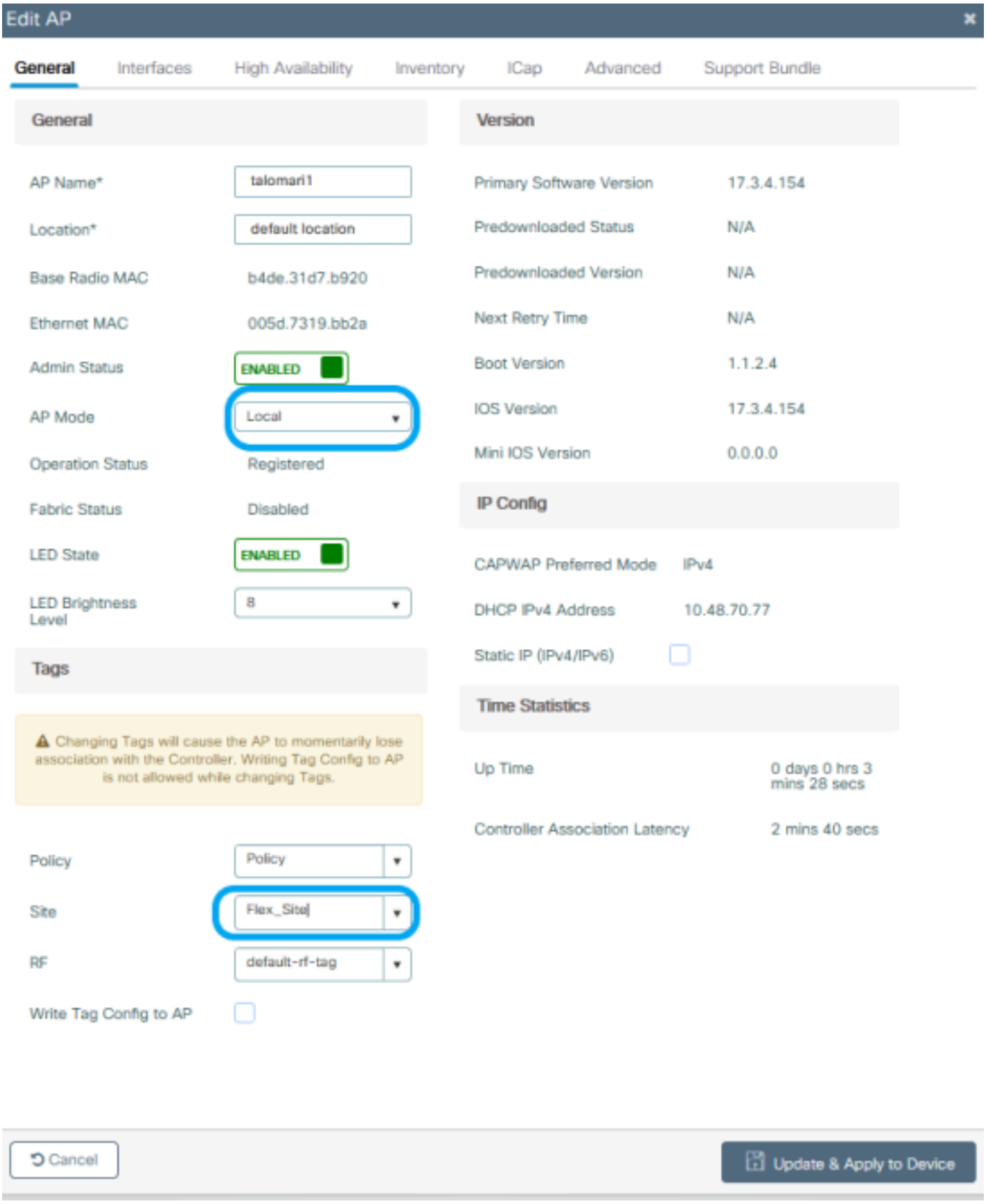




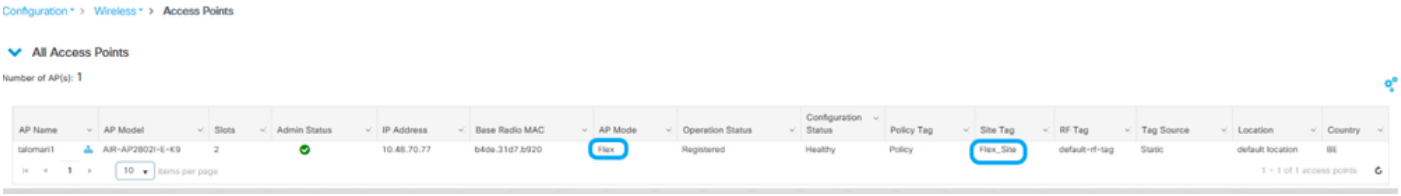
Remarque : Comme l'option Activer le site local est désactivée, les points d'accès auxquels cette balise de site est attribuée peuvent être configurés en mode FlexConnect.

Étape 2. **À partir de l'interface utilisateur graphique :** Accédez à Configuration > Wireless > Access Points > AP name pour ajouter le Site Tag et le Policy Tag à un AP associé. Cela peut entraîner le point d'accès à redémarrer son tunnel CAPWAP et à se joindre à nouveau au WLC 9800.


Search Menu Items
Dashboard
Monitoring
Configuration
Wireless
Access Points
All Access Points
Number of AP(s): 1

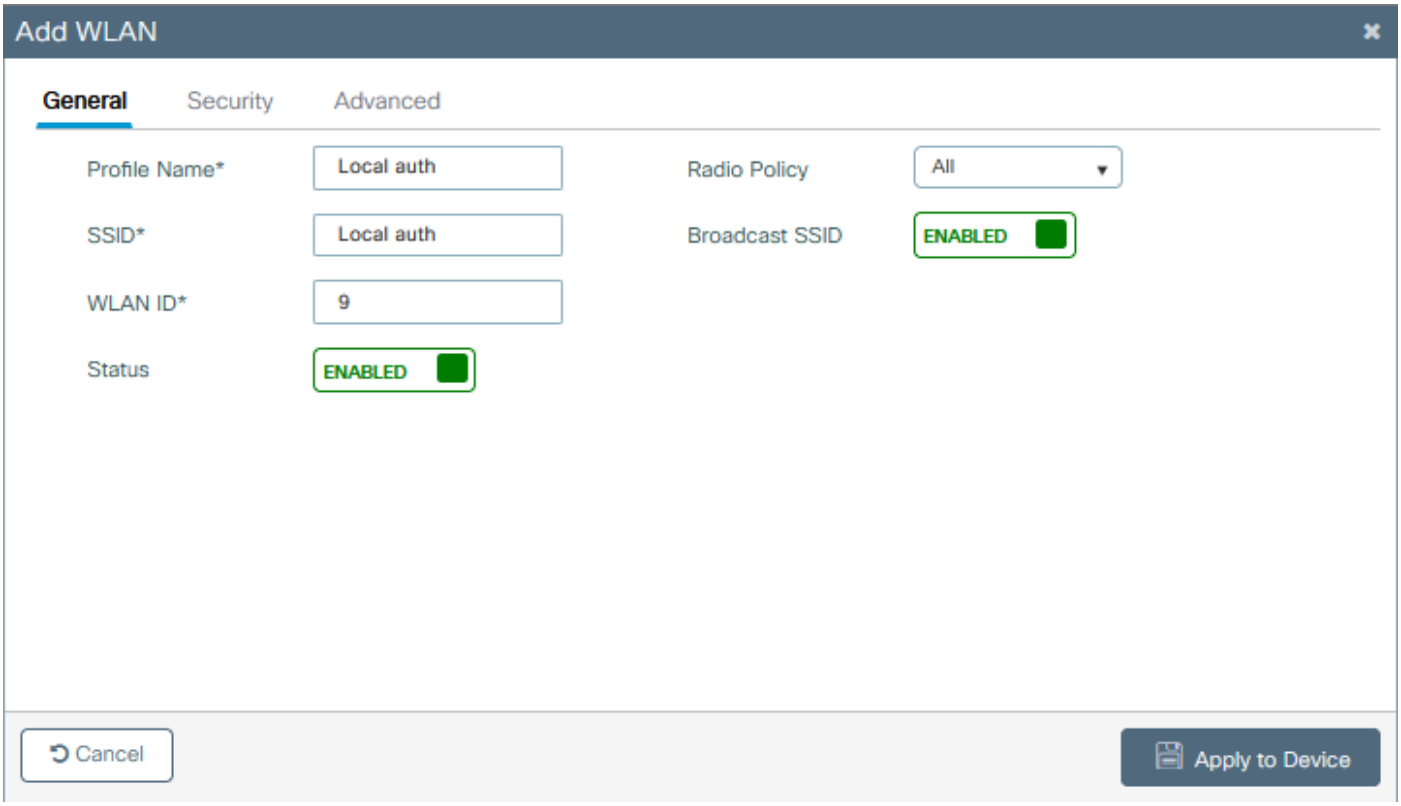


Une fois que le point d'accès se reconnecte, notez qu'il est maintenant en mode FlexConnect.

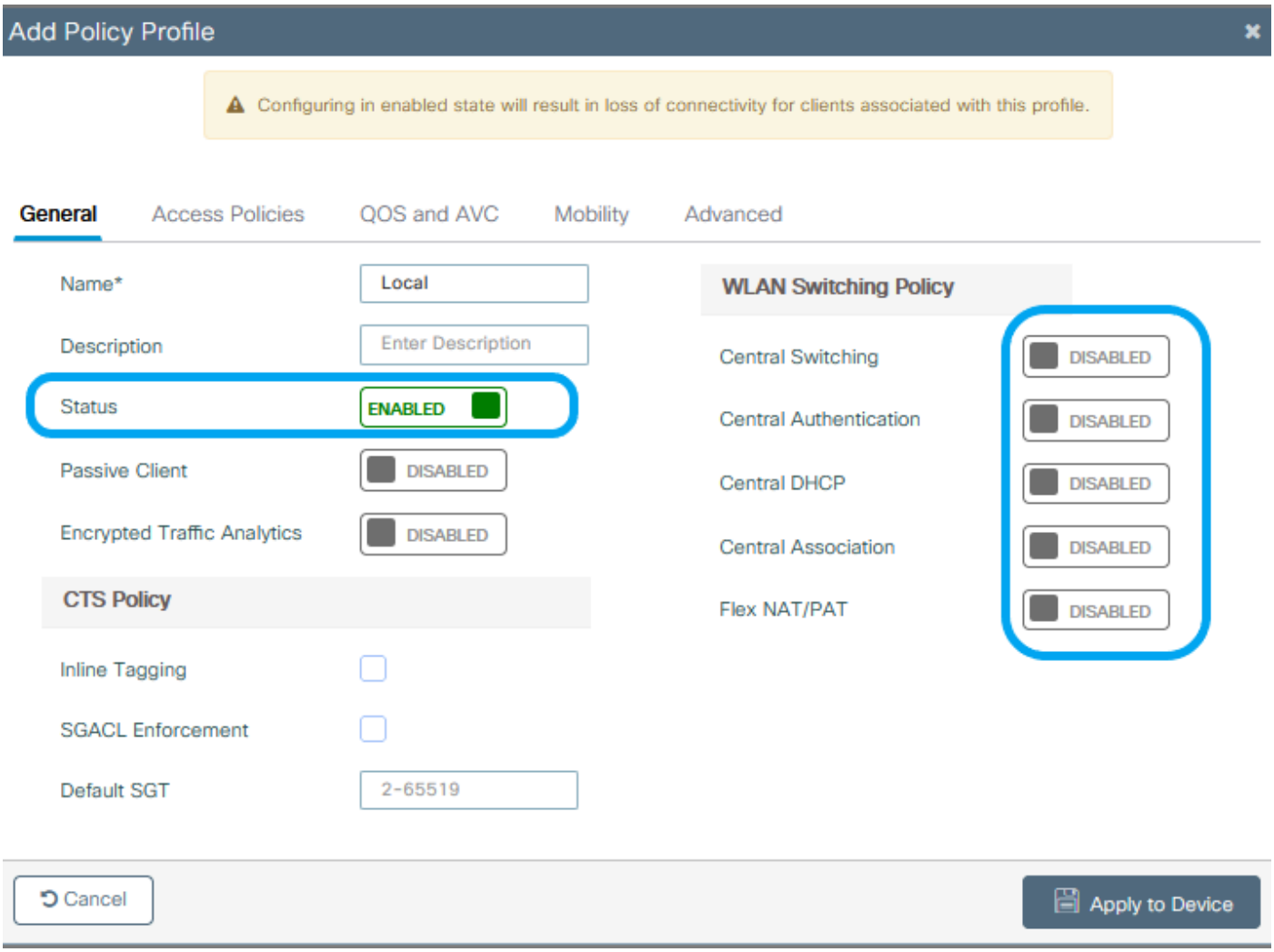


Authentification locale avec serveur RADIUS externe

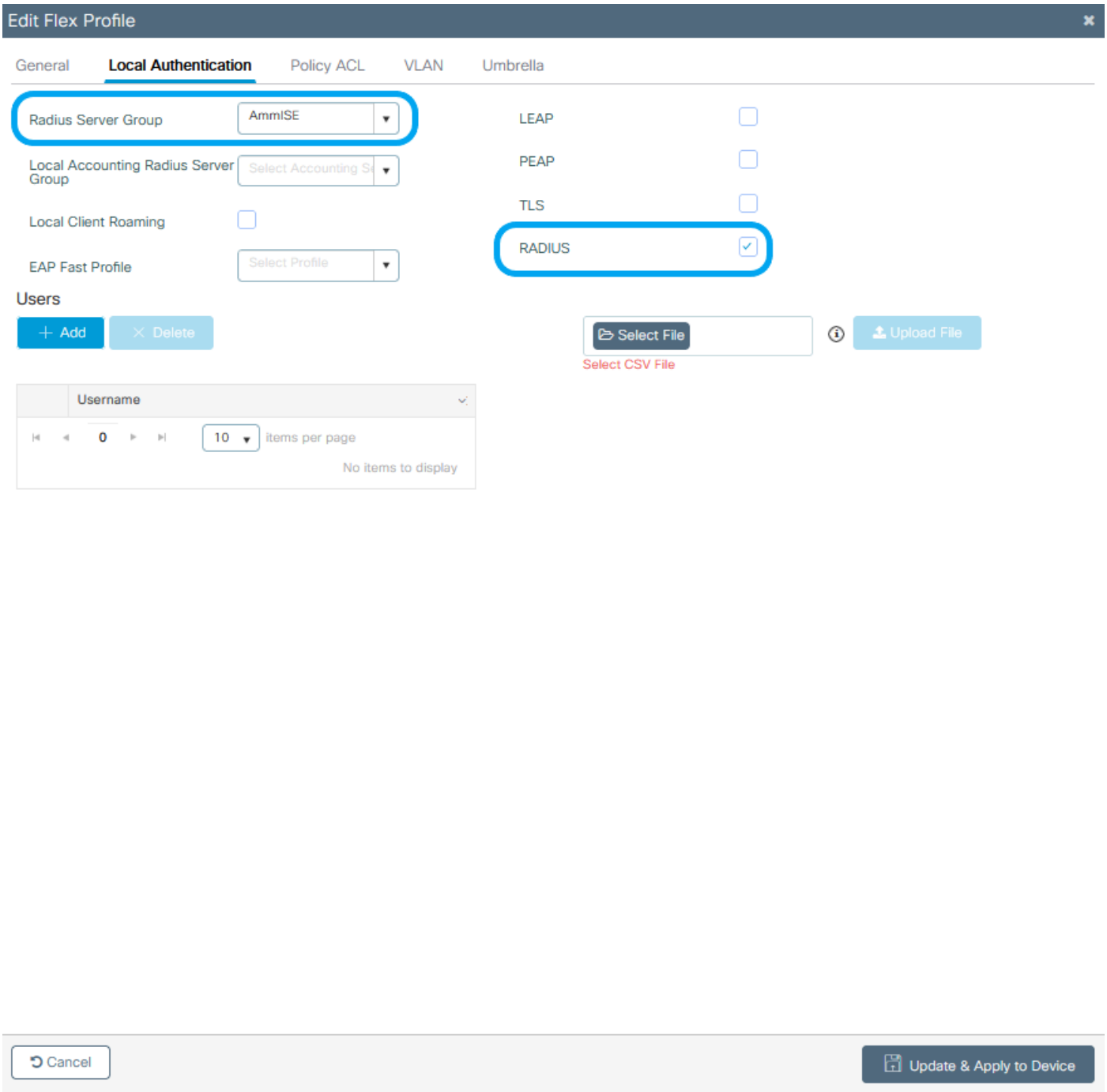
Étape 1 : ajout du point d'accès en tant que périphérique réseau au serveur RADIUS Pour un exemple, référez-vous à Comment utiliser Identity Service Engine (ISE) comme serveur RADIUS
Étape 2 : création d'un WLAN.
La configuration peut être la même que celle précédemment configurée.



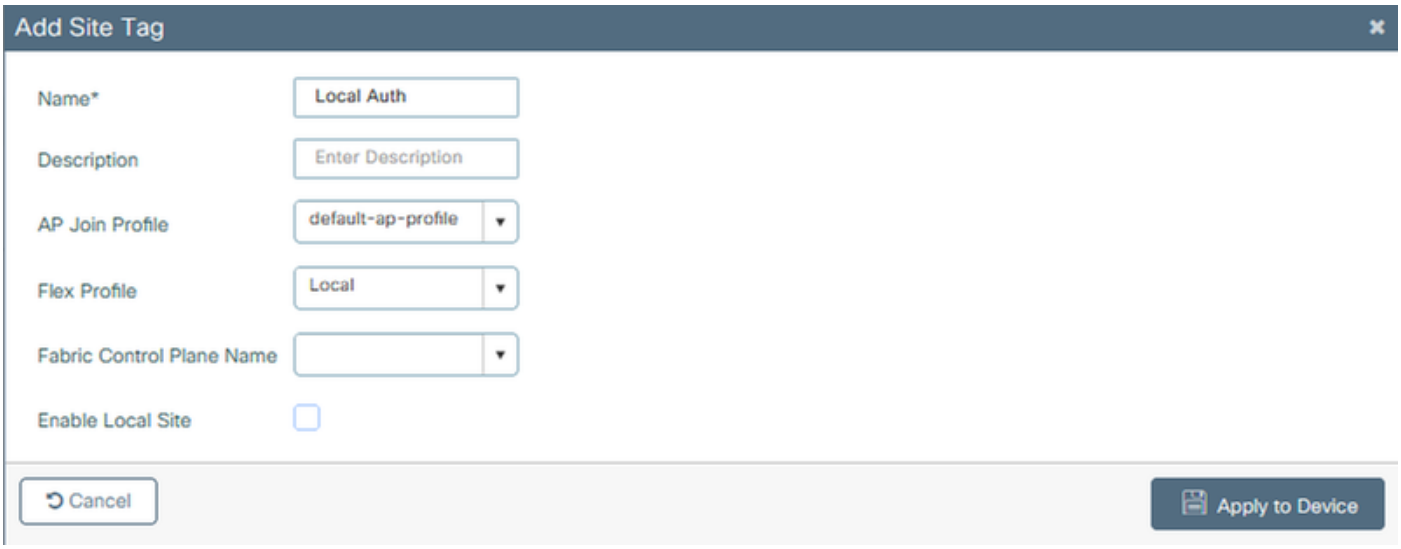
Étape 3 : configuration du profil de stratégie
Vous pouvez soit en créer un nouveau, soit utiliser le précédemment configuré. Cette fois, décochez les cases Commutation centrale, Authentification centrale, DHCP central, et Association centrale activée.



Étape 4 : configuration des balises de stratégie
Associez le WLAN configuré et le profil de stratégie créé.
Étape 5 : configuration du profil flexible.
Créez un profil flexible, accédez à l'onglet Authentification locale, configurez le groupe de serveurs Radius et cochez la case RADIUS.



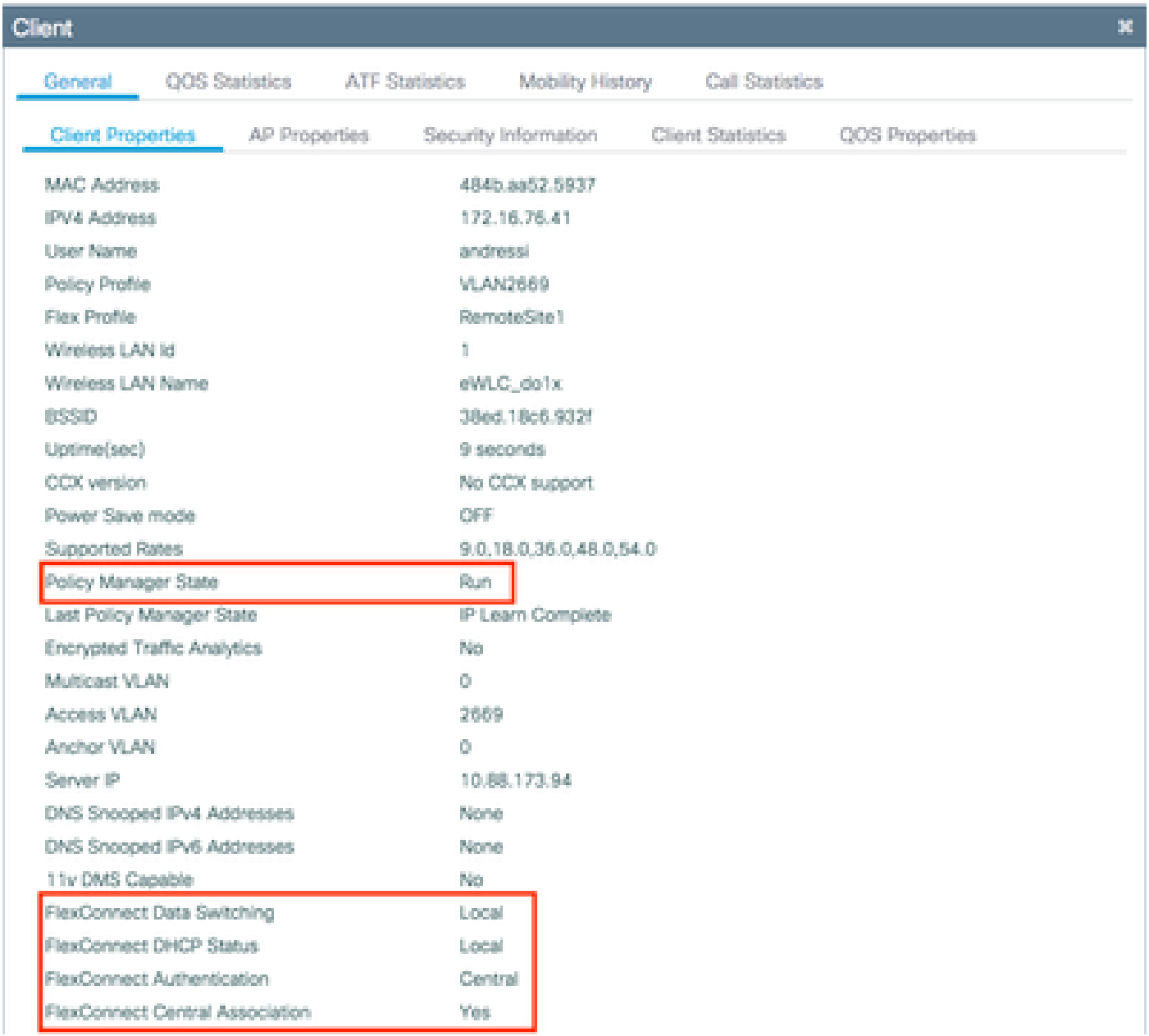
Étape 6 : configuration des balises de site
Configurez le profil paramétrable configuré à l'étape 5 et décochez la case Enable Local Site.



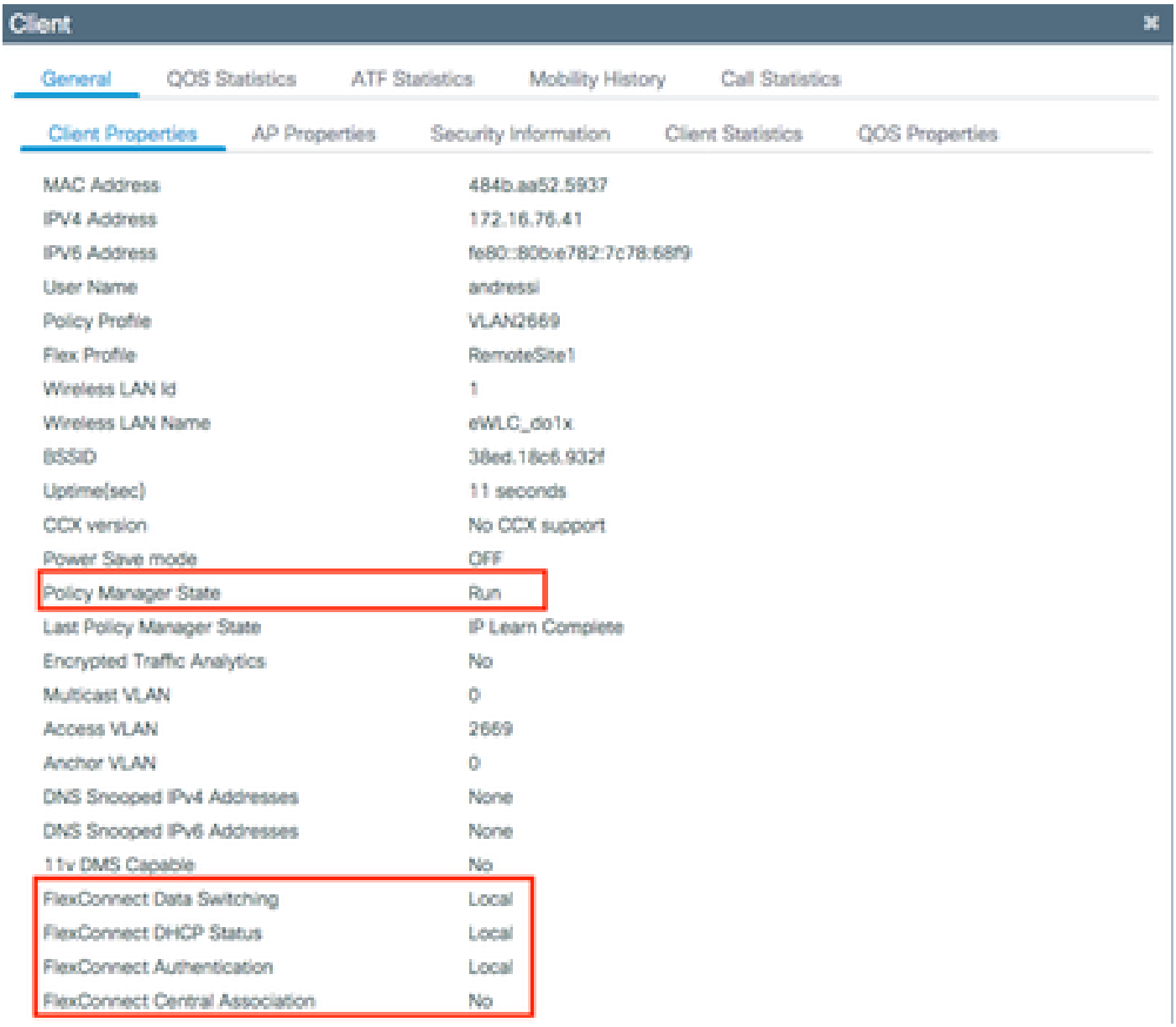
Vérifier

À partir de la GUI : Accédez à Surveillance > Sans fil > Clients et confirmez l'état de Policy Manager et les paramètres FlexConnect.

Authentification centrale :



Authentification locale :



Vous pouvez utiliser ces commandes pour vérifier la configuration actuelle:

À partir de CLI :

```
# 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 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.

Remarque : En fonction 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 passer par 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 dans le temps jusqu'à quand le problème s'est produit.

À partir de CLI :

```
# show clock
```

Étape 2. Collectez les syslogs à partir de la mémoire tampon du contrôleur ou du syslog externe, comme dicté par la configuration du système. Cela permet d'obtenir un aperçu rapide de l'état du système et des erreurs éventuelles.

À partir de CLI :

```
# show logging
```

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

À partir de CLI :

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:
```

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

Remarque : Si vous trouvez une condition 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 augmenterait le volume de journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque le débogage n'est pas actif.

Étape 4. Si vous supposez 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.

À partir de CLI :

```
# 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.

À partir de CLI :

```
# 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 suivi actif radio

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 peut fournir des traces de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (adresse MAC du client dans ce cas). Afin d'activer le débogage conditionnel, passez par ces étapes.

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

À partir de CLI :

```
# 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.

À partir de CLI :

```
# 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 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 les débogages si le problème est reproduit avant que le temps de surveillance par défaut ou configuré ne soit écoulé.

À partir de CLI :

```
# 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'activité d'adresse MAC. Vous pouvez copier le fichier .log ra trace sur un serveur externe ou afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA

À partir de CLI :

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

Copiez le fichier sur un serveur externe :

À partir de CLI :

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

Affichez-en le contenu :

À partir de CLI :

```
# 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 vous avez examiné en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.

À partir de CLI :

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

Remarque : Ce résultat de commande renvoie des suivis pour tous les niveaux de journalisation pour tous les processus et est assez volumineux. 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 :

À partir de CLI :

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

Affichez-en le contenu :

À partir de CLI :

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

Étape 11. Supprimer les conditions de débogage

À partir de CLI :

```
# clear platform condition all
```

Remarque : Assurez-vous de toujours supprimer les conditions de débogage après un 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.