Configuration de l'intégration WLC 9800 avec Aruba ClearPass - & Dot1x Déploiement de FlexConnect pour les filiales

Contenu

Introduction

Ce document décrit l'intégration du contrôleur sans fil Catalyst 9800 avec Aruba ClearPass Policy Manager (CPPM) et Microsoft Active Directory (AD) pour fournir l'authentification dot1x aux clients sans fil dans un déploiement Flexconnect.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez connaissance de ces rubriques et qu'elles aient été configurées et vérifiées :

- Contrôleur sans fil Catalyst 9800
- Serveur Aruba ClearPass (nécessite une licence de plate-forme, une licence d'accès, une licence embarquée)
- Windows AD opérationnel
- Autorité de certification (CA) facultative
- Serveur DHCP opérationnel
- Serveur DNS opérationnel (requis pour la validation de la liste de révocation de certificats)
- ESXi
- Tous les composants pertinents sont synchronisés sur NTP et vérifiés pour avoir l'heure correcte (requise pour la validation du certificat)
- Connaissance des sujets : Déploiement du C9800 et nouveau modèle de configurationFonctionnement de FlexConnect sur C9800 Authentification Dot1x

Components Used

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

- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX, 4800 points d'accès
- Aruba ClearPass, correctif 6-8-0-109592 et 6.8-3
- Serveur MS Windows Active Directory (GP configuré pour l'émission automatique de certificats basés sur une machine vers les terminaux gérés)Serveur DHCP avec option 43 et option 60Serveur DNSServeur NTP pour synchroniser tous les composantsAC

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

Flux de trafic

Dans un déploiement d'entreprise type avec plusieurs filiales, chaque filiale est configurée pour fournir un accès point1x aux employés de l'entreprise. Dans cet exemple de configuration, PEAP est utilisé pour fournir un accès dot1x aux utilisateurs de l'entreprise via une instance ClearPass déployée dans le data center central (DC). Les certificats d'ordinateur sont utilisés conjointement avec la vérification des informations d'identification des employés sur un serveur Microsoft AD.

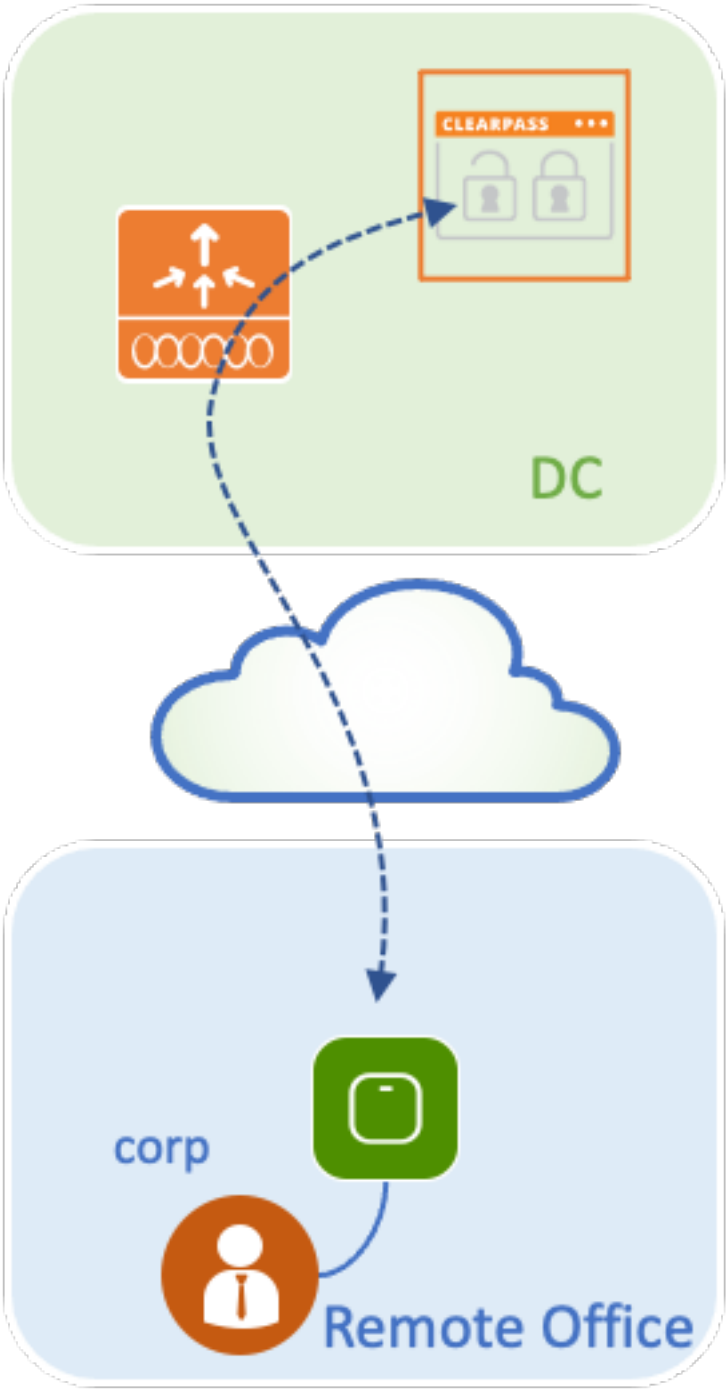
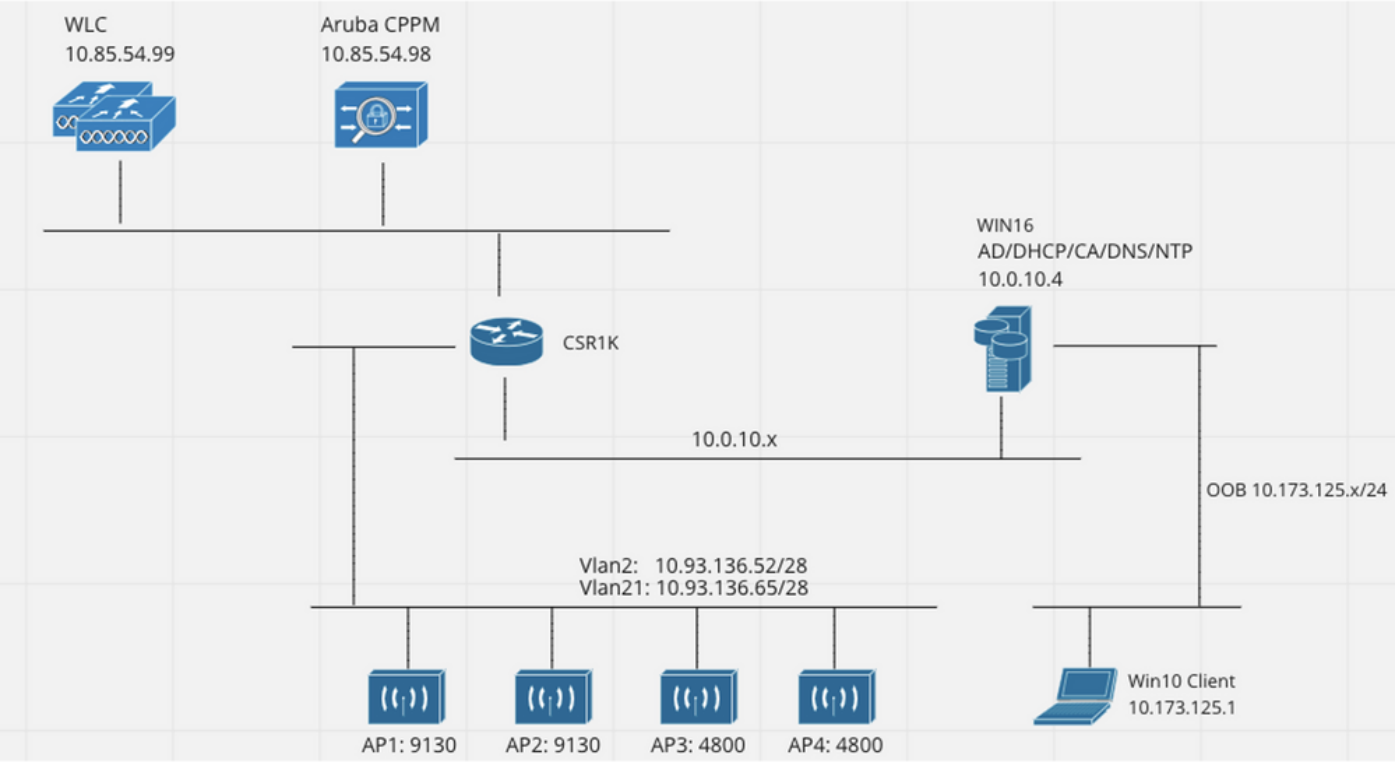
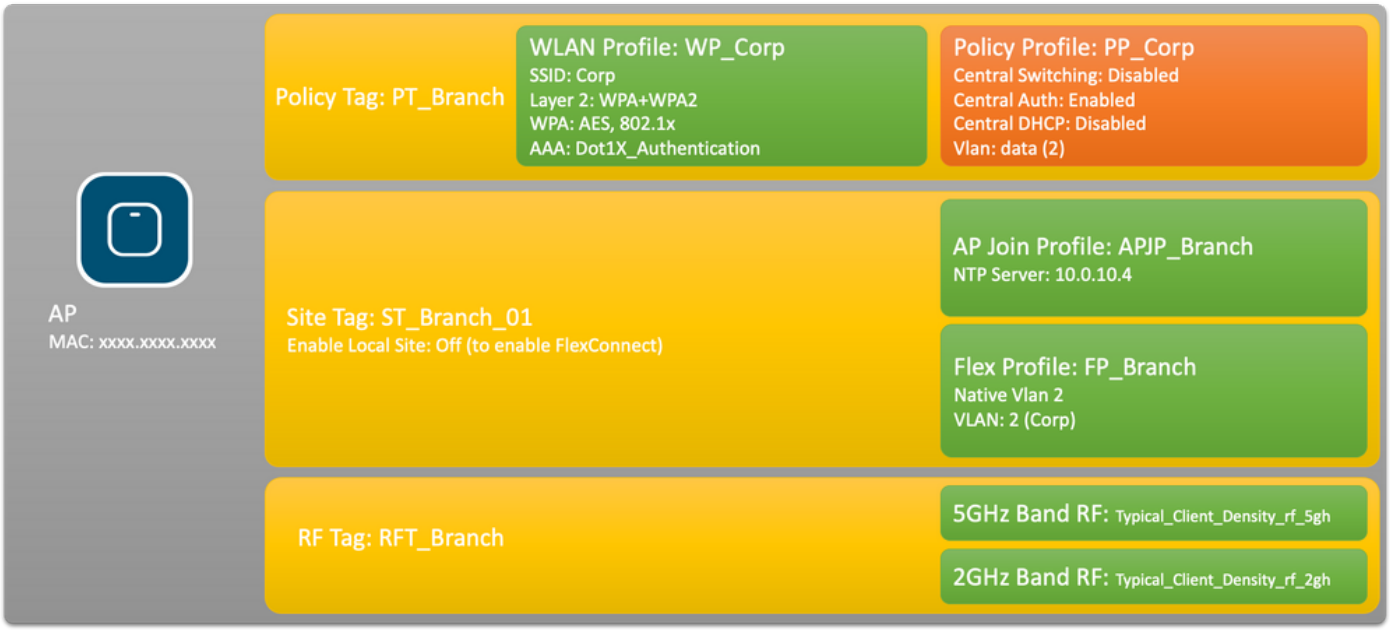


Diagramme du réseau



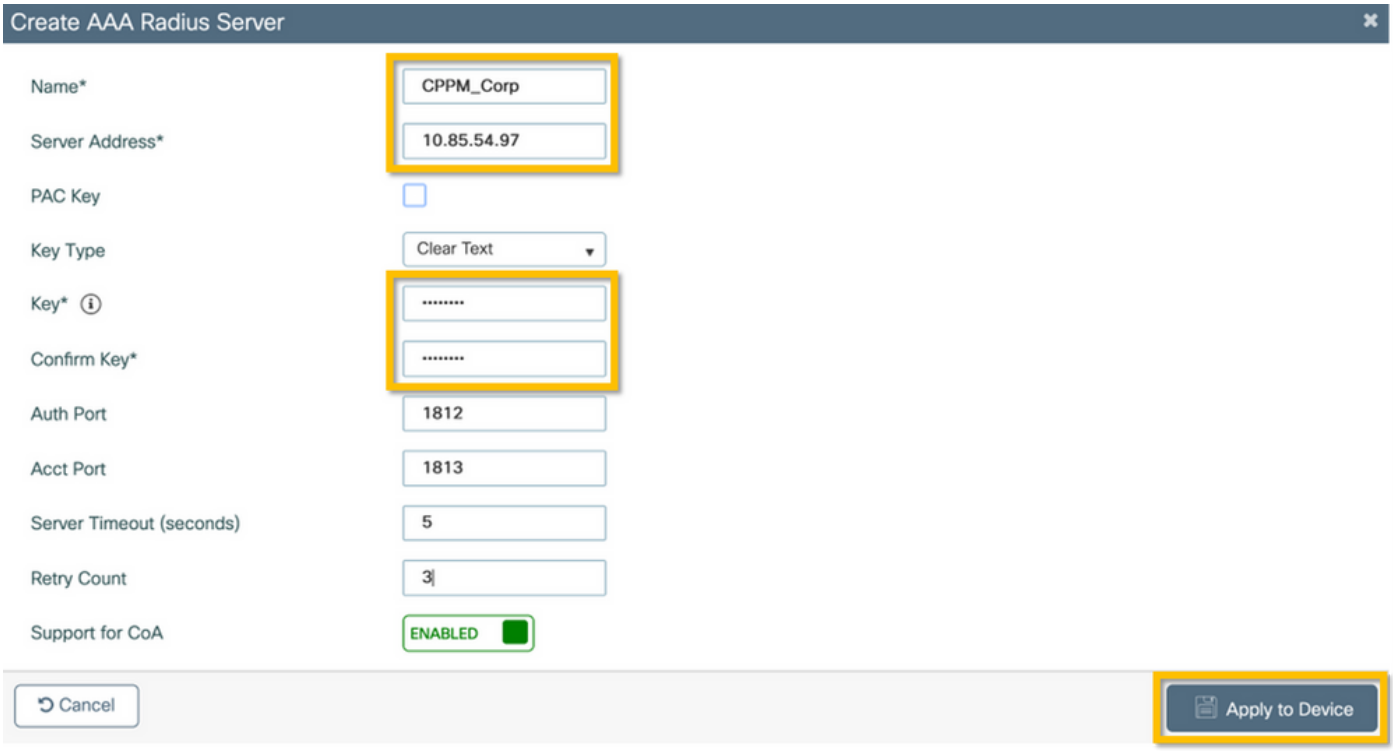
Configuration du contrôleur sans fil Catalyst 9800

Dans cet exemple de configuration, le nouveau modèle de configuration sur C9800 est utilisé pour créer les profils et les balises nécessaires pour fournir un accès dot1x aux filiales de l'entreprise. La configuration résultante est résumée dans le schéma.

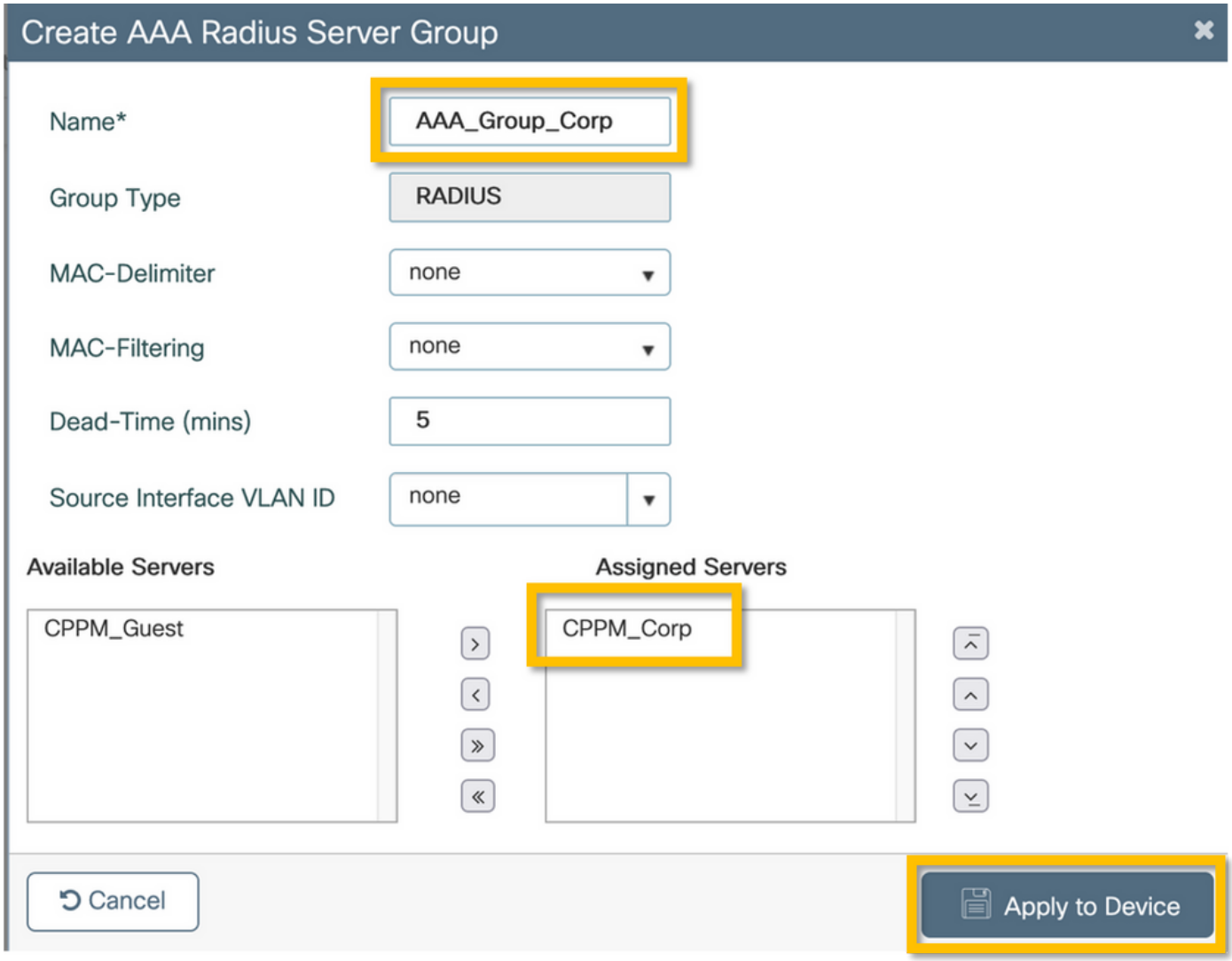


C9800 - Configuration des paramètres AAA pour dot1x

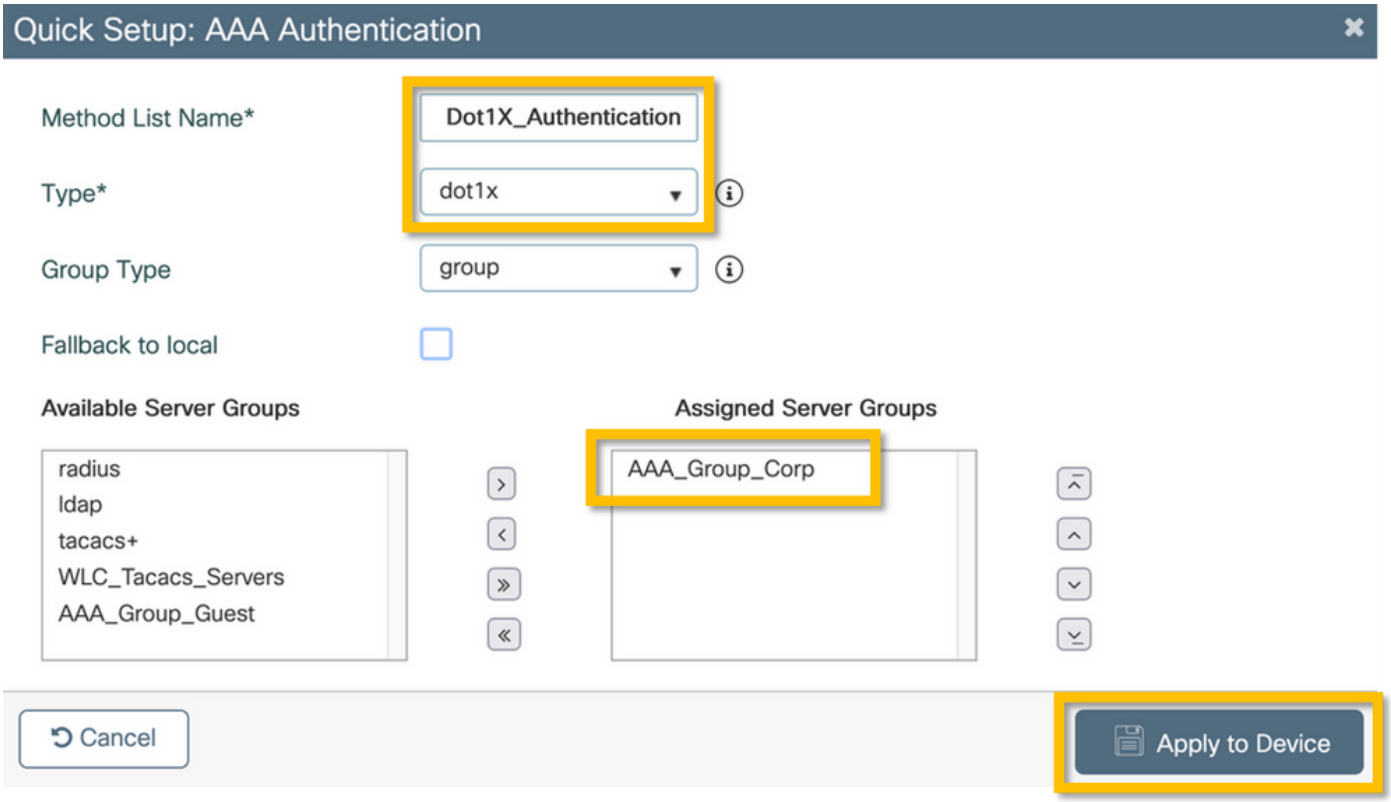
Étape 1 : ajout du serveur Aruba ClearPass Policy Manager « Corp » à la configuration du WLC 9800 Accédez à **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers.** Cliquez sur **+Add** et entrez les informations du serveur RADIUS. Cliquez sur le bouton **Apply to Device** comme illustré dans cette image.



Étape 2. Définissez un groupe de serveurs AAA pour les utilisateurs de l'entreprise. Accédez à **Configuration > Security > AAA > Servers/Groups > RADIUS > Groups** et cliquez sur **+Add,** entrez le nom du groupe de serveurs RADIUS et attribuez les informations du serveur RADIUS. Cliquez sur le bouton **Apply to Device (Appliquer au périphérique)** comme illustré dans cette image.

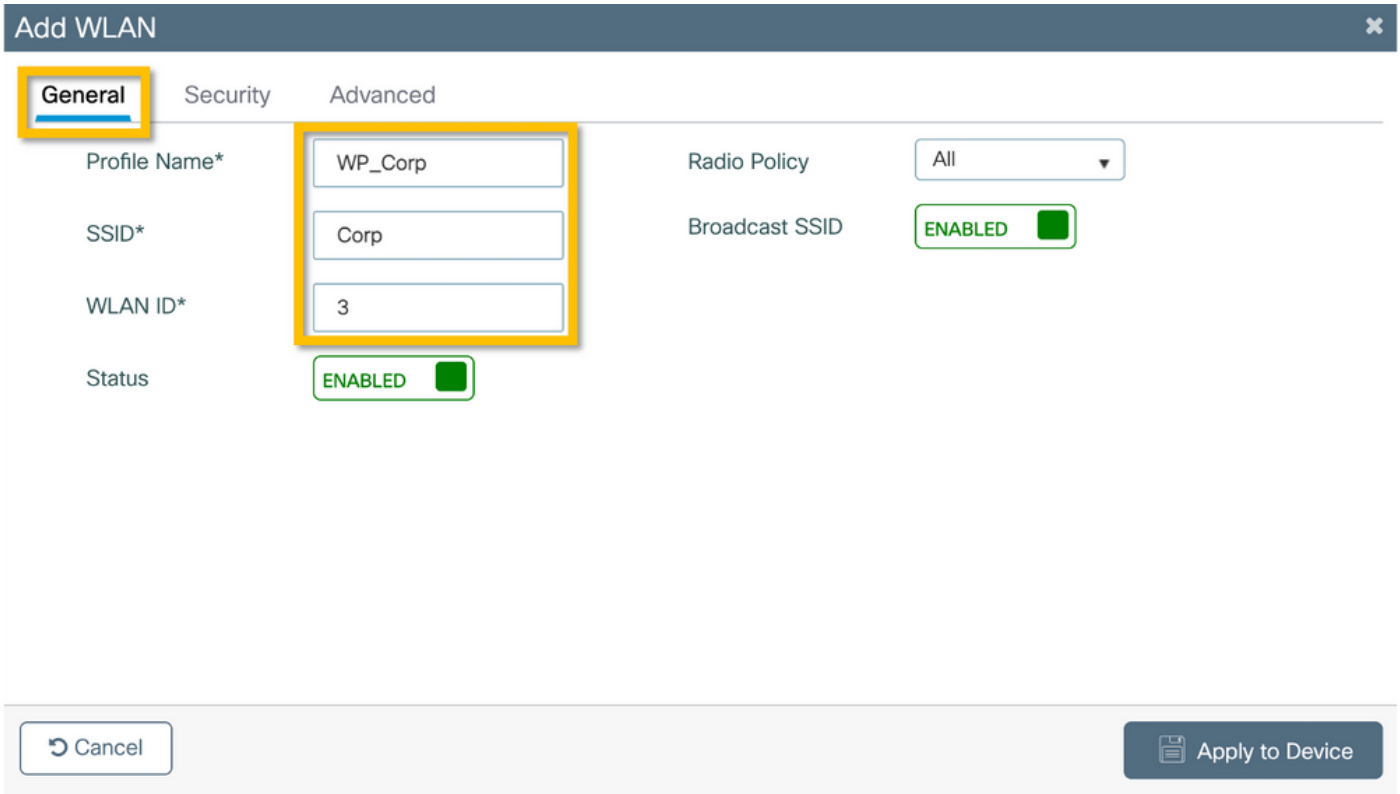


Étape 3 : définition de la liste de méthodes d'authentification dot1x pour les utilisateurs de l'entreprise Accédez à **Configuration > Security > AAA > AAA Method List > Authentication** et cliquez sur **+Add**. Sélectionnez **Type dot1x** dans le menu déroulant. Cliquez sur le bouton **Apply to Device** comme illustré dans cette image.

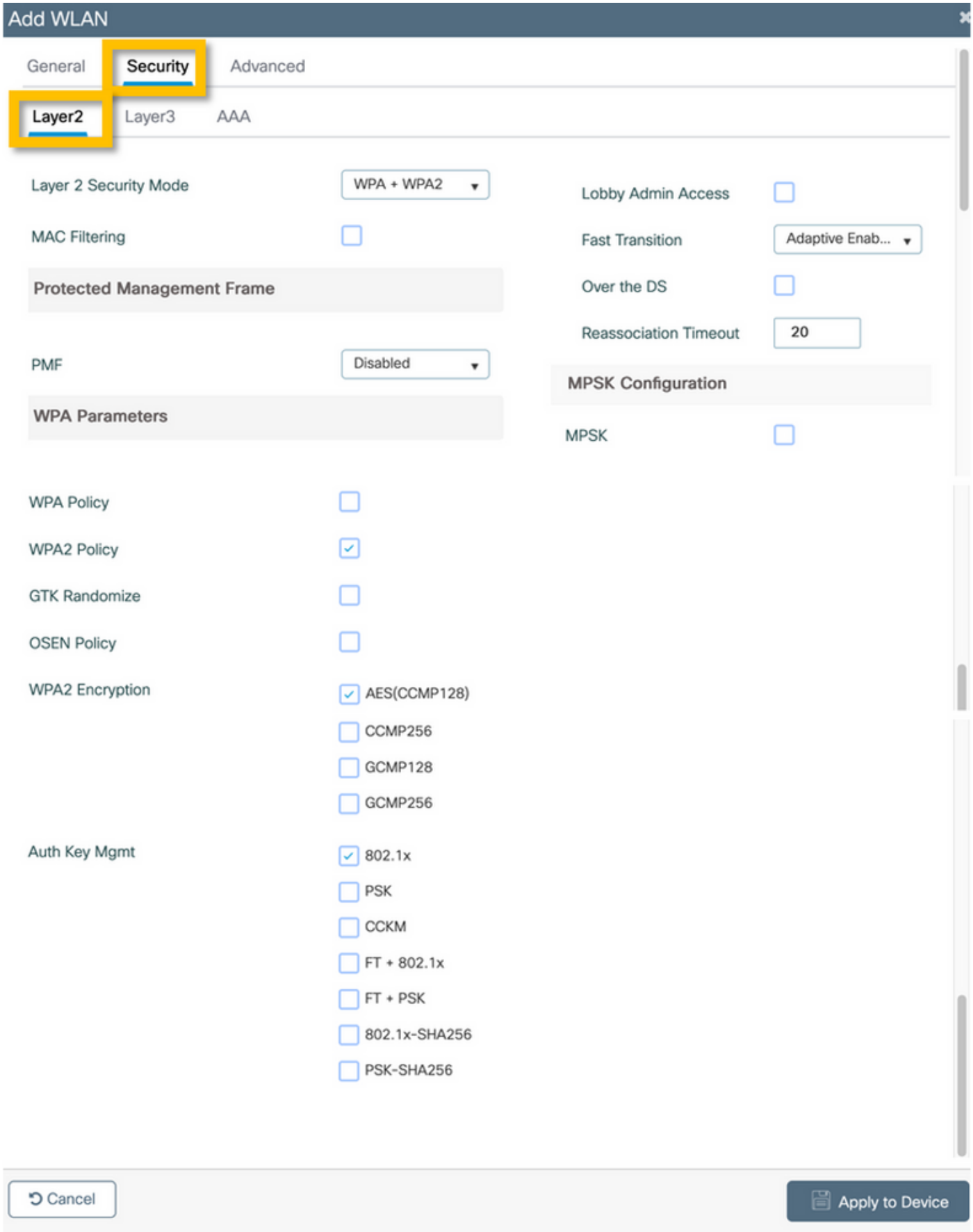


C9800 - Configuration du profil WLAN « Corp »

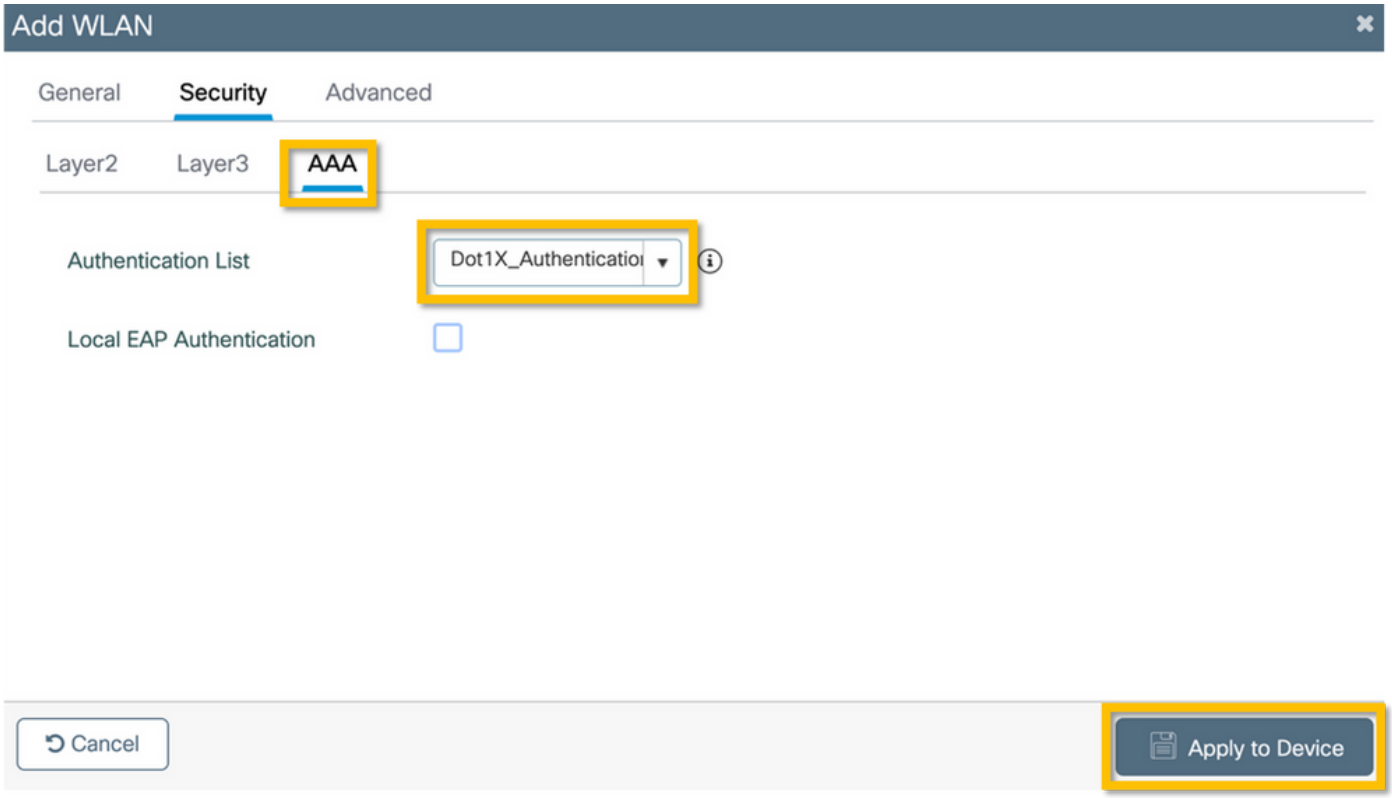
Étape 1. Accédez à **Configuration > Tags & Profiles > Wireless** et cliquez sur **+Add**. Entrez un nom de profil, le SSID « Corp » et un ID WLAN qui n'est pas déjà utilisé.



Étape 2. Accédez à l'onglet **Security** et au sous-onglet **Layer2**. Il est inutile de modifier les paramètres par défaut de cet exemple de configuration.

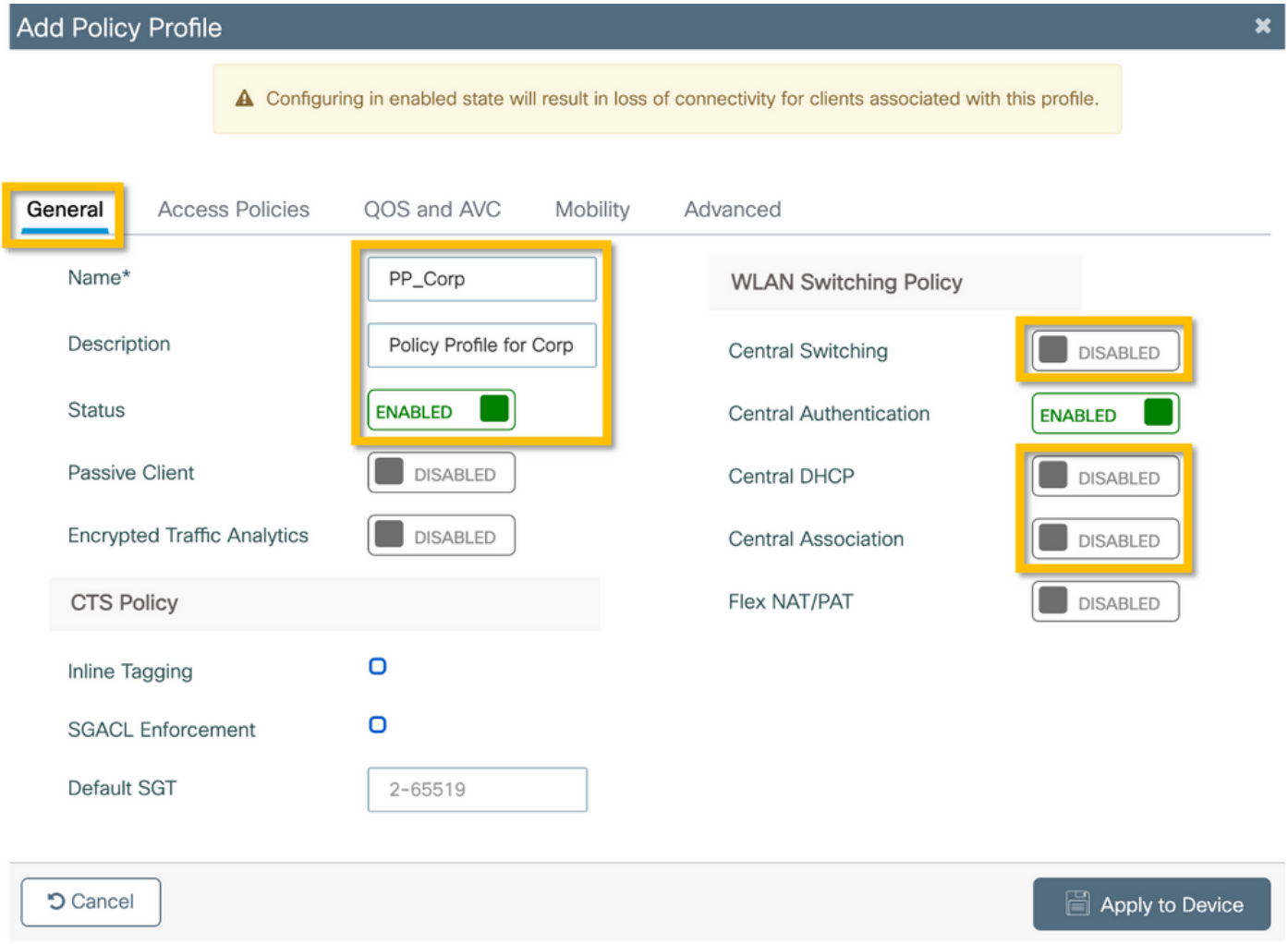


Étape 3. Accédez au sous-onglet **AAA** et sélectionnez la liste de méthodes d'authentification configurée précédemment. Cliquez sur le bouton **Apply to Device (Appliquer au périphérique)** comme illustré dans cette image.

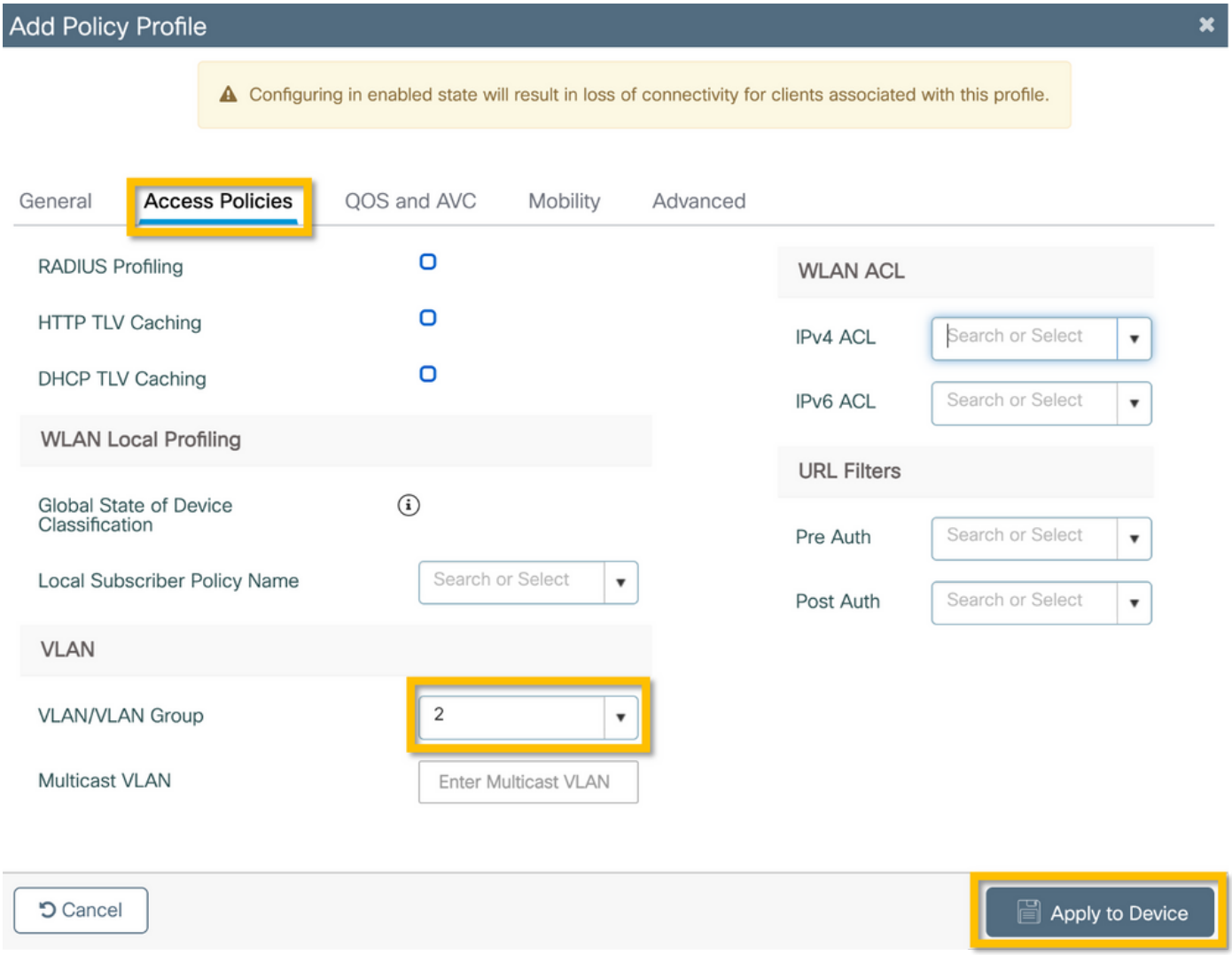


C9800 - Configuration du profil de stratégie

Étape 1. Accédez à **Configuration > Tags & Profiles > Policy** et cliquez sur **+Add** et entrez un nom et une description de profil de stratégie. Activez la stratégie et désactivez la commutation centrale, le protocole DHCP et l'association, car le trafic utilisateur de l'entreprise est commuté localement au niveau du point d'accès, comme illustré dans l'image.



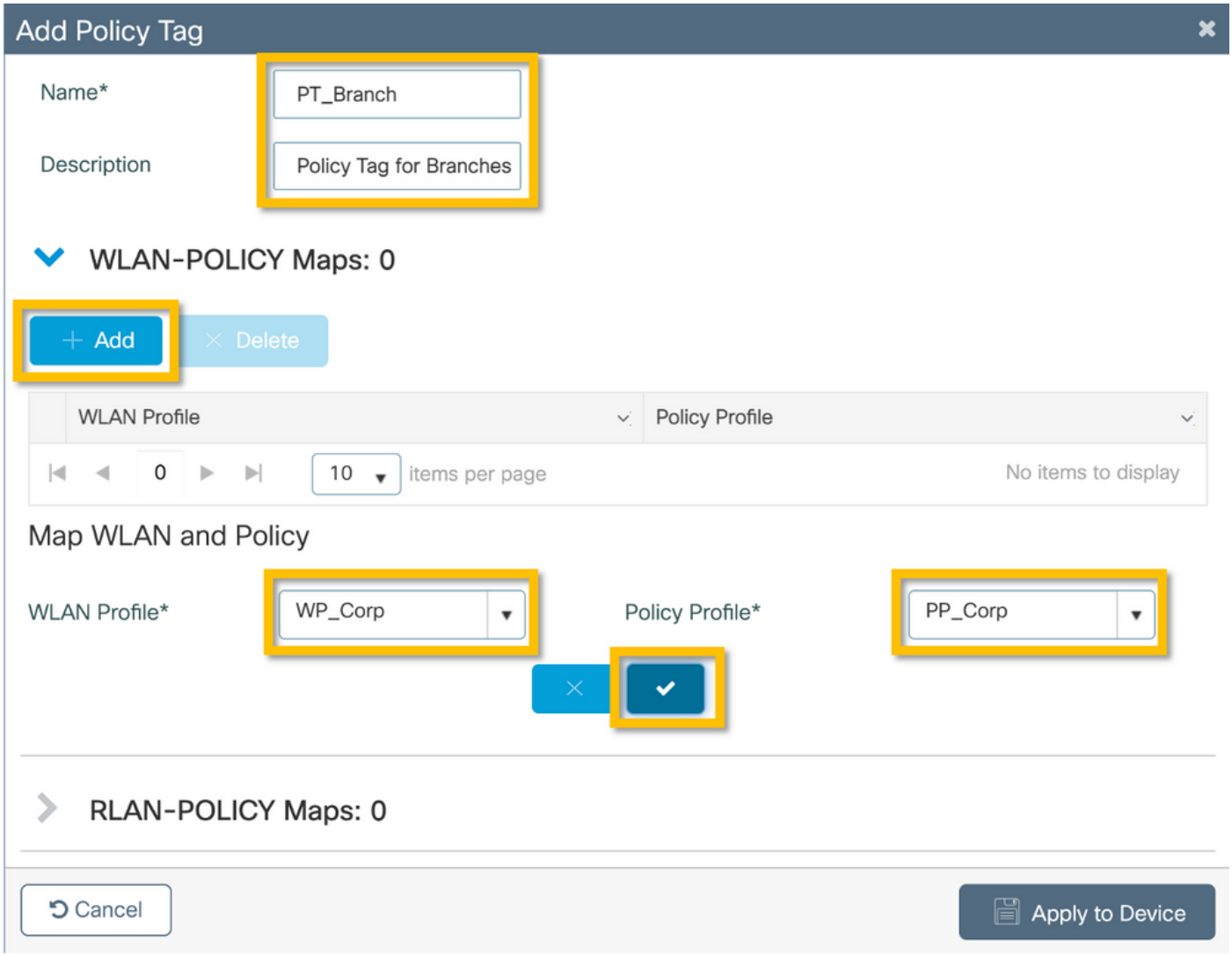
Étape 2. Accédez à l'onglet **Access Policies** et entrez manuellement l'ID du VLAN à utiliser au niveau de la filiale pour le trafic utilisateur de l'entreprise. Ce VLAN n'a pas besoin d'être configuré sur le C9800 lui-même. Il doit être configuré dans le profil flexible, comme détaillé plus loin. Ne sélectionnez pas de nom de VLAN dans la liste déroulante (voir ID de bogue Cisco CSCvn48234) pour plus d'informations). Cliquez sur le bouton **Apply to Device (Appliquer au périphérique)** comme illustré dans cette image.



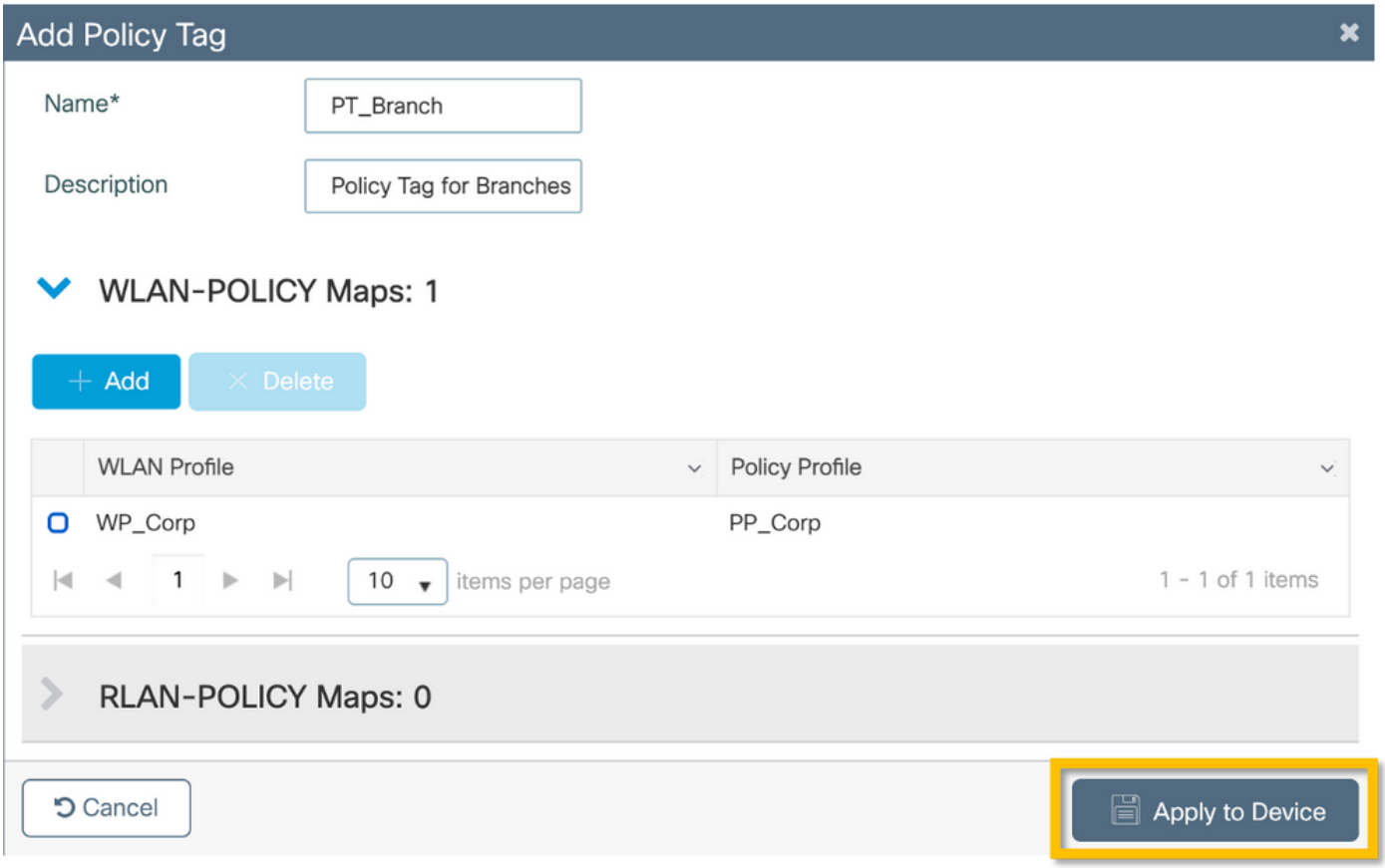
C9800 - Configurer la balise de stratégie

Une fois le profil WLAN (WP_Corp) et le profil de stratégie (PP_Corp) créés, une balise de stratégie doit à son tour être créée pour lier ces profils WLAN et de stratégie. Cette balise de stratégie est appliquée aux points d'accès. Attribuez cette balise de stratégie aux points d'accès pour déclencher la configuration de ces derniers afin d'activer les SSID sélectionnés sur eux.

Étape 1. Accédez à **Configuration > Tags & Profiles > Tags**, sélectionnez l'onglet **Policy** et cliquez sur **+Add**. Saisissez le nom et la description de la balise de stratégie. Cliquez sur **+Add** sous **WLAN-POLICY Maps**. Sélectionnez le profil WLAN et le profil de stratégie créés précédemment, puis cliquez sur le bouton de coche comme illustré dans cette image.



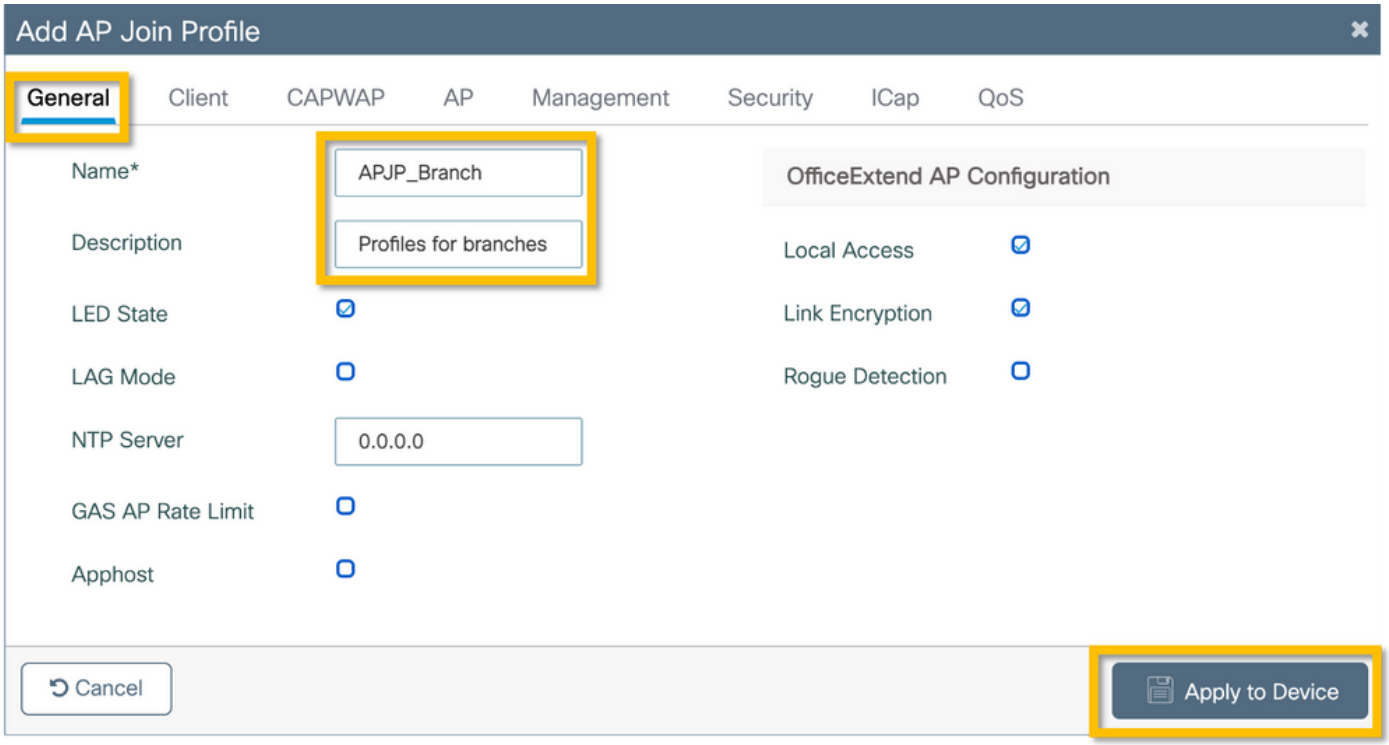
Étape 2. Vérifiez et cliquez sur le bouton **Apply to Device** comme illustré dans cette image.



C9800 - Profil de jonction AP

Les profils de jointure AP et les profils flexibles doivent être configurés et attribués aux points d'accès avec des balises de site. Une balise de site différente doit être utilisée pour chaque branche afin de prendre en charge la transition rapide 802.11r (FT) au sein d'une branche, tout en limitant la distribution de la PMK client entre les AP de cette branche uniquement. Il est important de ne pas réutiliser la même balise de site entre plusieurs branches. Configurez un profil de jonction AP. Vous pouvez utiliser un seul profil de jointure AP si toutes les branches sont similaires, ou créer plusieurs profils si certains des paramètres configurés doivent être différents.

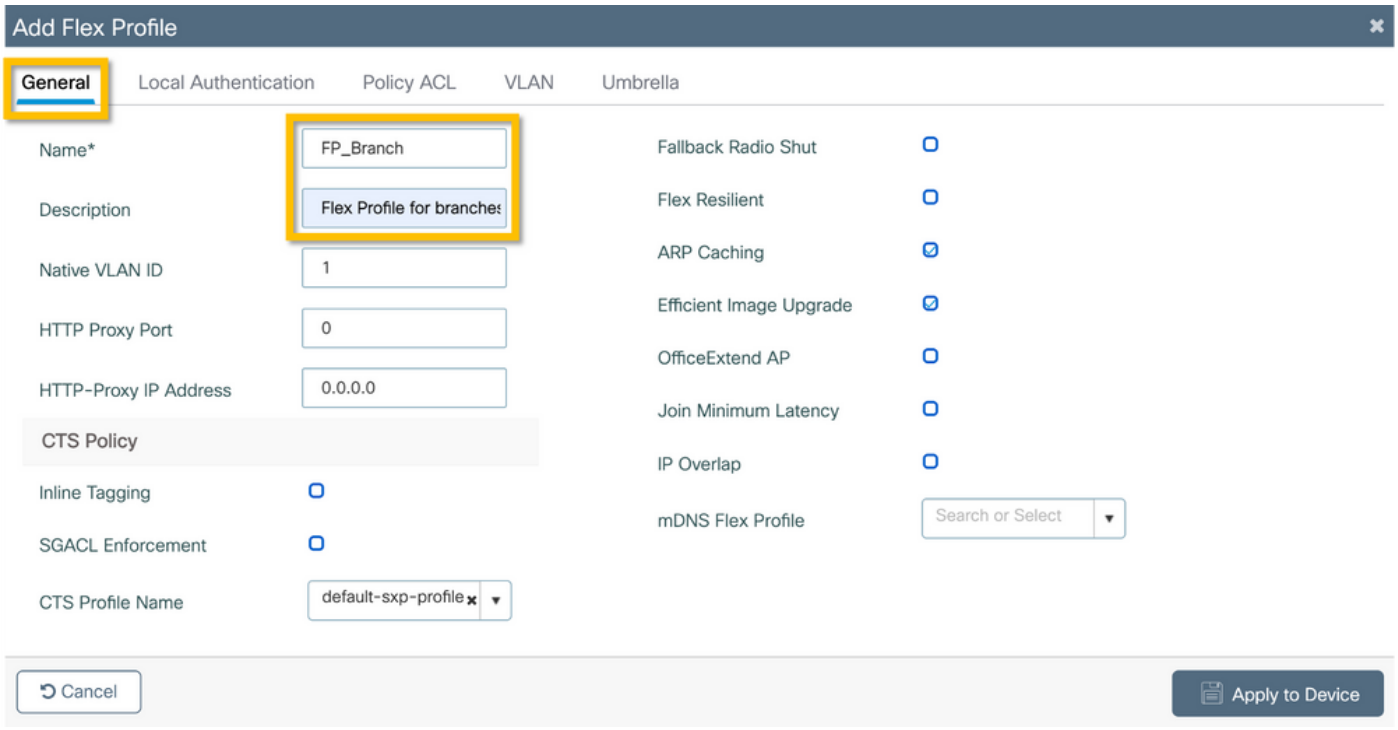
Étape 1. Accédez à **Configuration > Tags & Profiles > AP Join** et cliquez sur **+Add**. Entrez le nom et la description du profil de connexion AP. Cliquez sur le bouton **Apply to Device (Appliquer au périphérique)** comme illustré dans cette image.



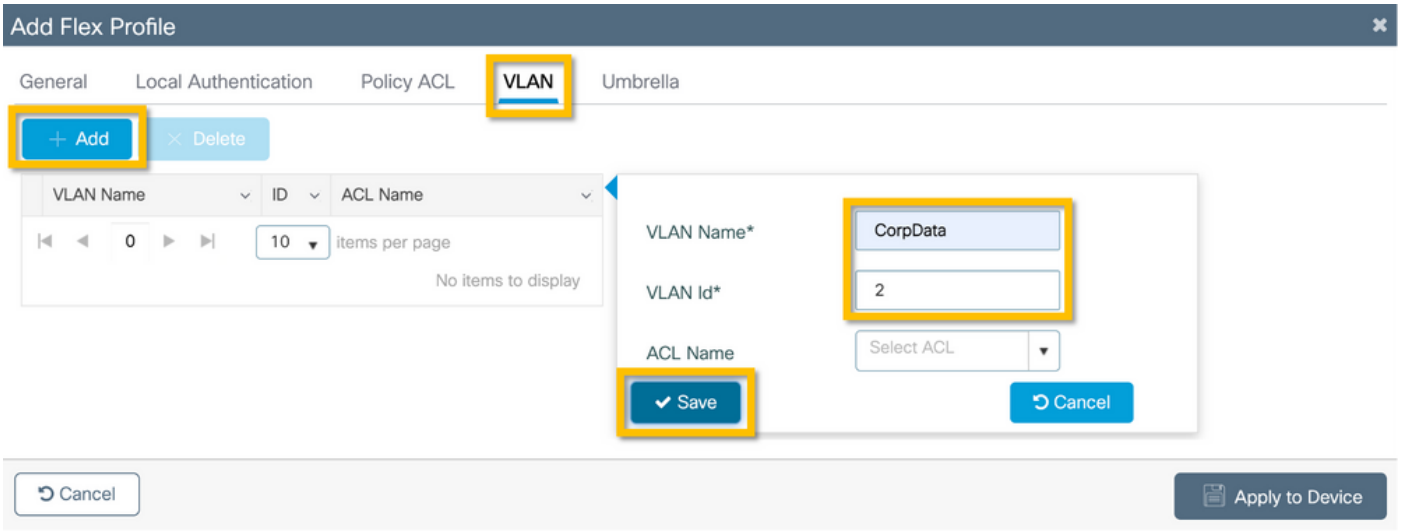
C9800 - Profil flexible

Configurez maintenant un profil flexible. Là encore, vous pouvez utiliser un profil unique pour toutes les branches si celles-ci sont similaires et ont le même mappage VLAN/SSID. Vous pouvez également créer plusieurs profils si certains des paramètres configurés, tels que les affectations VLAN, sont différents.

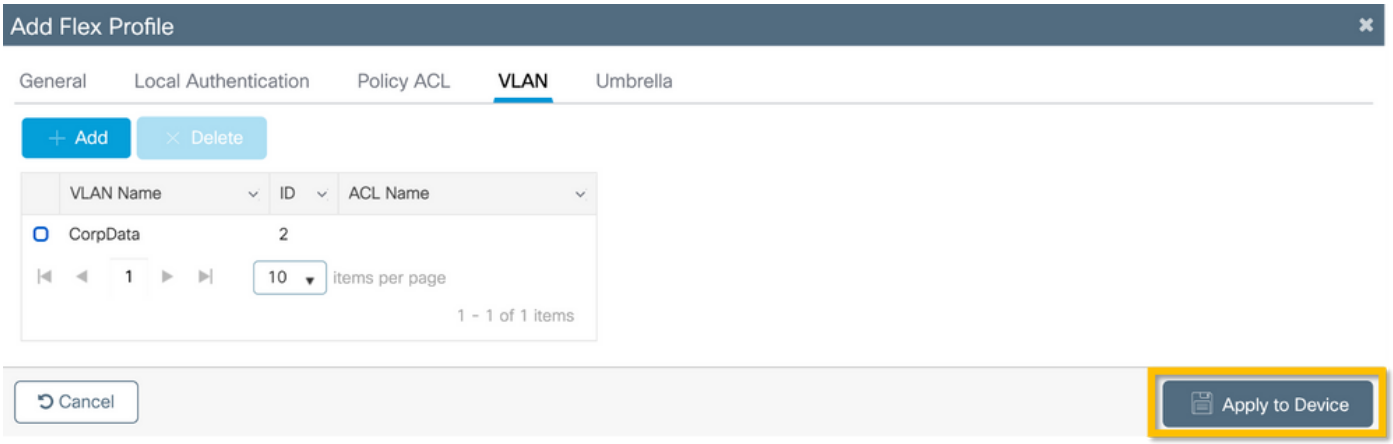
Étape 1. Accédez à **Configuration > Tags & Profiles > Flex** et cliquez sur **+Add**. Entrez le nom et la description du profil Flex.



Étape 2. Accédez à l'onglet **VLAN** et cliquez sur **+Add**. Entrez le nom et l'ID du VLAN local au niveau de la branche que le point d'accès doit utiliser pour commuter localement le trafic utilisateur de l'entreprise. Cliquez sur le bouton **Save** comme illustré dans cette image.



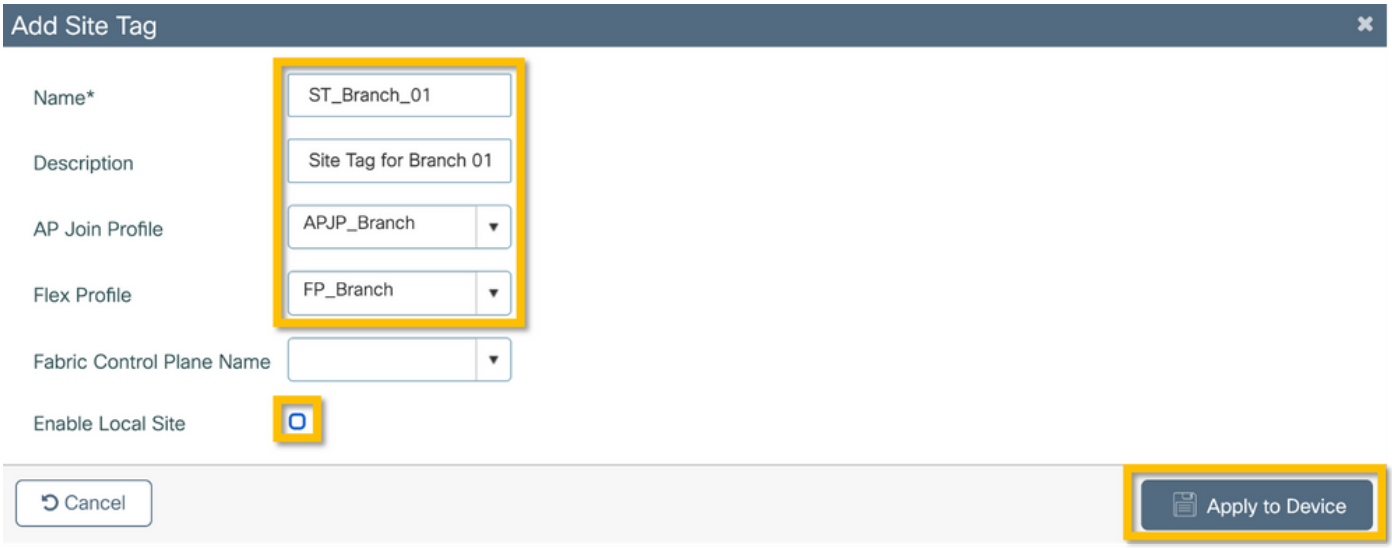
Étape 3. Vérifiez et cliquez sur le bouton **Apply to Device** comme illustré dans cette image.



C9800 - Étiquette de site

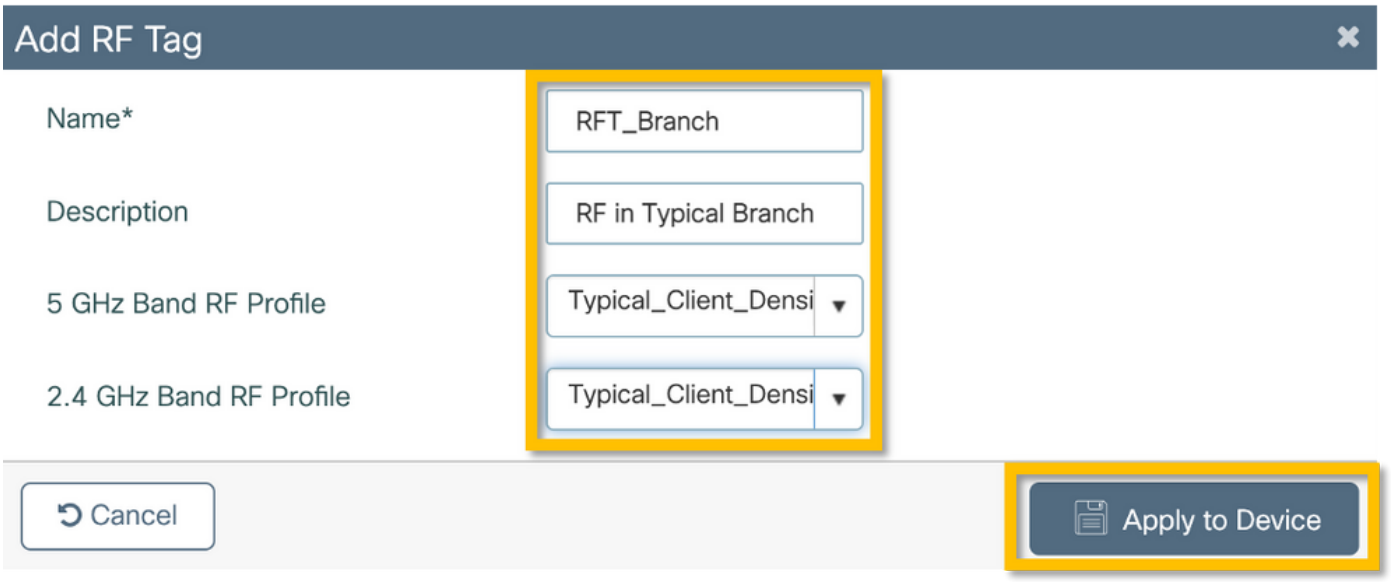
Les balises de site sont utilisées pour attribuer des profils de jointure et des profils flexibles aux points d'accès. Comme mentionné précédemment, une balise de site différente doit être utilisée pour chaque branche afin de prendre en charge la transition rapide 802.11r (FT) au sein d'une branche, tout en limitant la distribution de la PMK client entre les points d'accès de cette branche uniquement. Il est important de ne pas réutiliser la même balise de site entre plusieurs branches.

Étape 1. Accédez à **Configuration > Tags & Profiles > Tags**, sélectionnez l'onglet **Site** et cliquez sur **+Add**. Entrez un nom et une description de balise de site, sélectionnez le profil de connexion AP créé, décochez la case **Enable Local Site**, et enfin sélectionnez le profil flexible créé précédemment. Désactivez la case à cocher **Enable Local Site** pour changer le point d'accès de **Local Mode** à **FlexConnect**. Enfin, cliquez sur le bouton **Apply to Device** comme illustré dans cette image.



C9800 - Étiquette RF

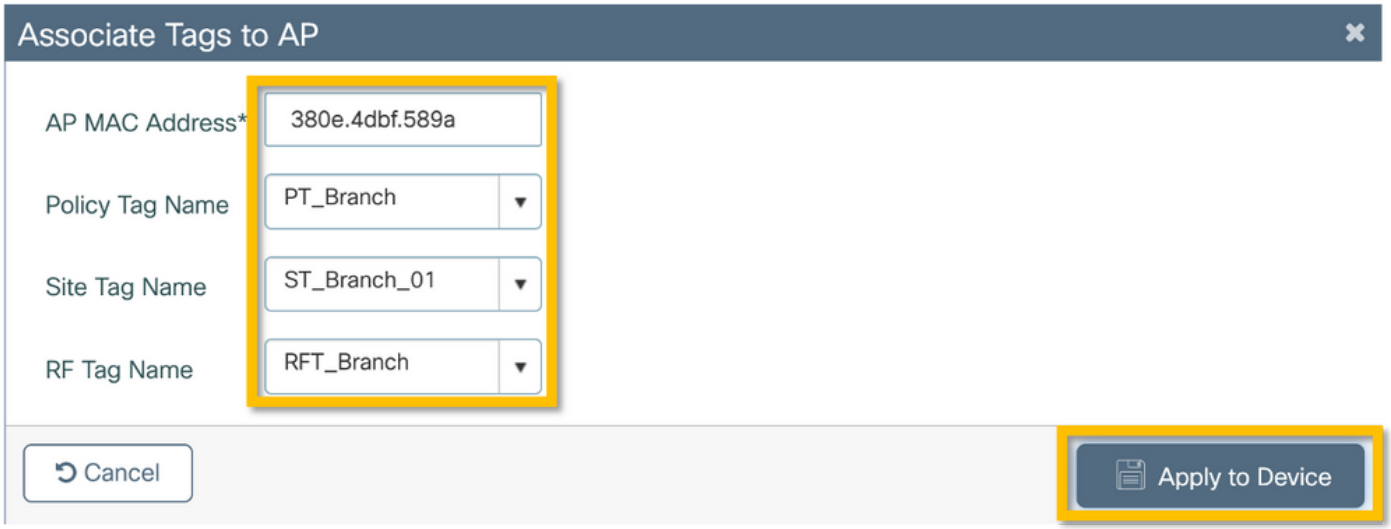
Étape 1. Accédez à **Configuration > Tags & Profiles > Tags**, sélectionnez l'onglet **RF** et cliquez sur **+Add.** Entrez un nom et une description pour la balise RF.Sélectionnez les **profils RF** définis par le système **dans le menu déroulant**. Cliquez sur le bouton **Apply to Device (Appliquer au périphérique)** comme illustré dans cette image.



C9800 - Attribuer des balises au point d'accès

Maintenant que les balises sont créées et incluent les différentes stratégies et profils requis pour configurer les points d'accès, nous devons les attribuer aux points d'accès. Cette section explique comment exécuter manuellement une balise statique attribuée à un point d'accès, en fonction de son adresse MAC Ethernet. Pour les environnements de production de produits, il est recommandé d'utiliser le workflow Cisco DNA Center AP PNP ou d'utiliser une méthode de téléchargement CSV statique en masse disponible dans le 9800.

Étape 1. Accédez à **Configure > Tags & Profiles > Tags**, sélectionnez l'onglet **AP**, puis l'**onglet Static**. Cliquez sur **+Add** et entrez l'adresse MAC du point d'accès, puis sélectionnez la balise de stratégie, la balise de site et la balise RF précédemment définies. Cliquez sur le bouton **Apply to Device** comme illustré dans cette image.



Configurer Aruba CPPM

Configuration initiale du serveur Aruba ClearPass Policy Manager

Aruba clearpass est déployé via le modèle OVF sur le serveur ESXi avec ces ressources :

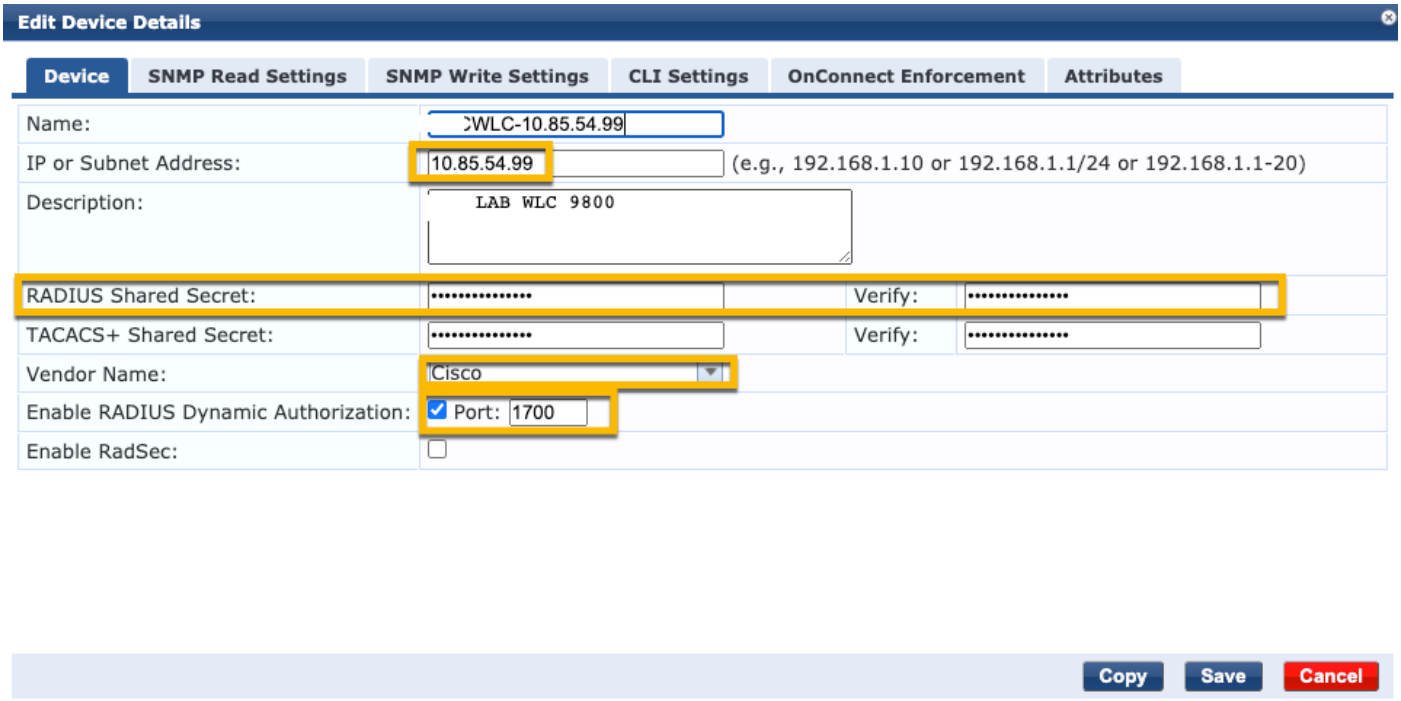
- 2 CPU virtuels réservés
- 6 Go de RAM
- Disque de 80 Go (à ajouter manuellement après le déploiement initial de la machine virtuelle avant la mise sous tension de la machine)

Appliquer les licences

Appliquez la licence de la plate-forme via : **Administration > Server Manager > Licensing**. Ajout **d'accès et intégration**

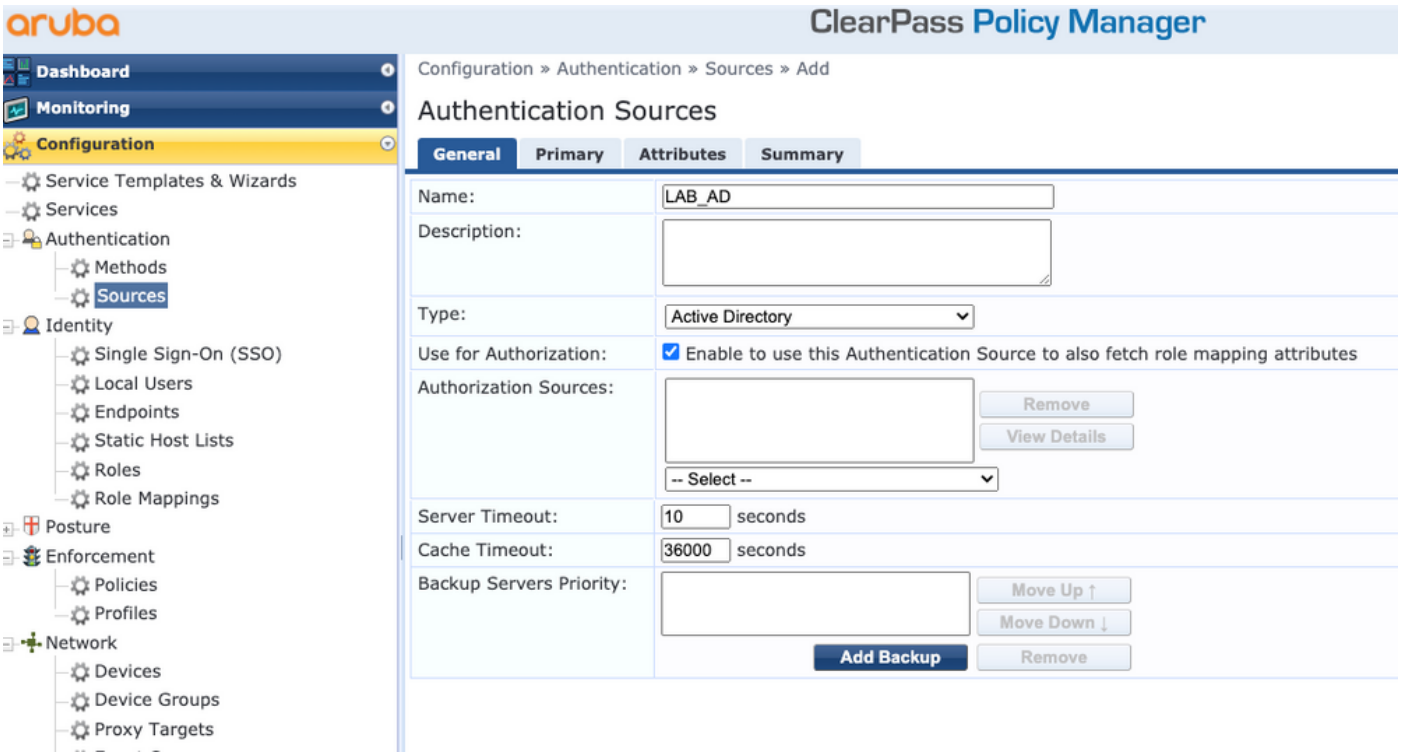
Ajout du contrôleur sans fil C9800 en tant que périphérique réseau

Accédez à **Configuration > Network > Devices > Add** comme indiqué dans cette image.



Configurer CPPM pour utiliser Windows AD comme source d'authentification

Accédez à **Configuration > Authentication > Sources > Add**. Sélectionnez **le type : Active Directory** à partir du menu déroulant, comme illustré dans cette image.



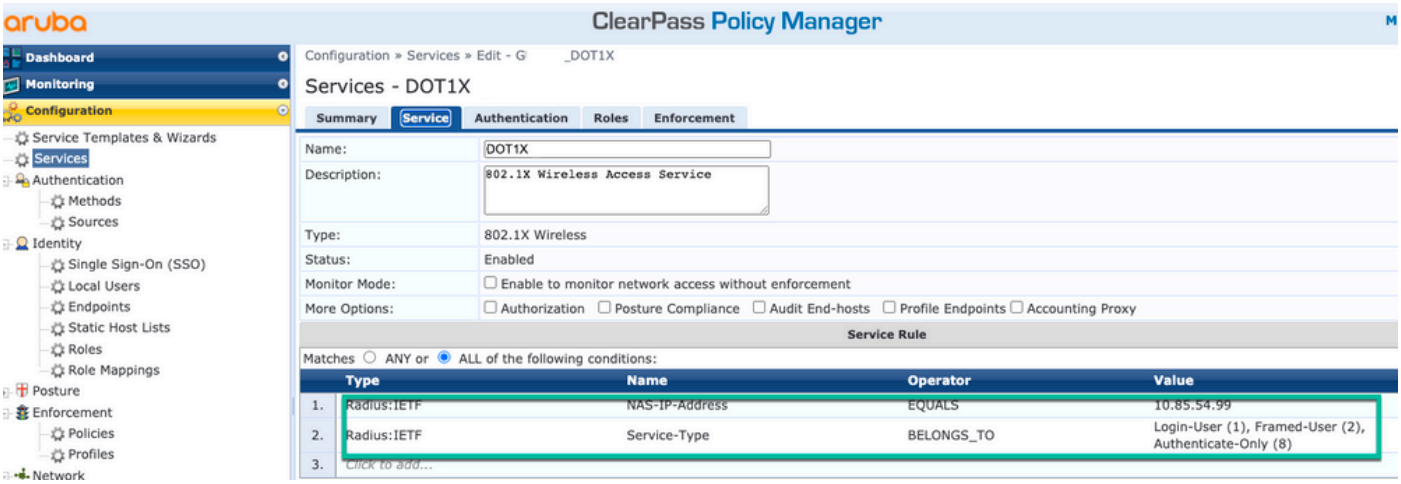
Configurer CPPM Service d'authentification Dot1X

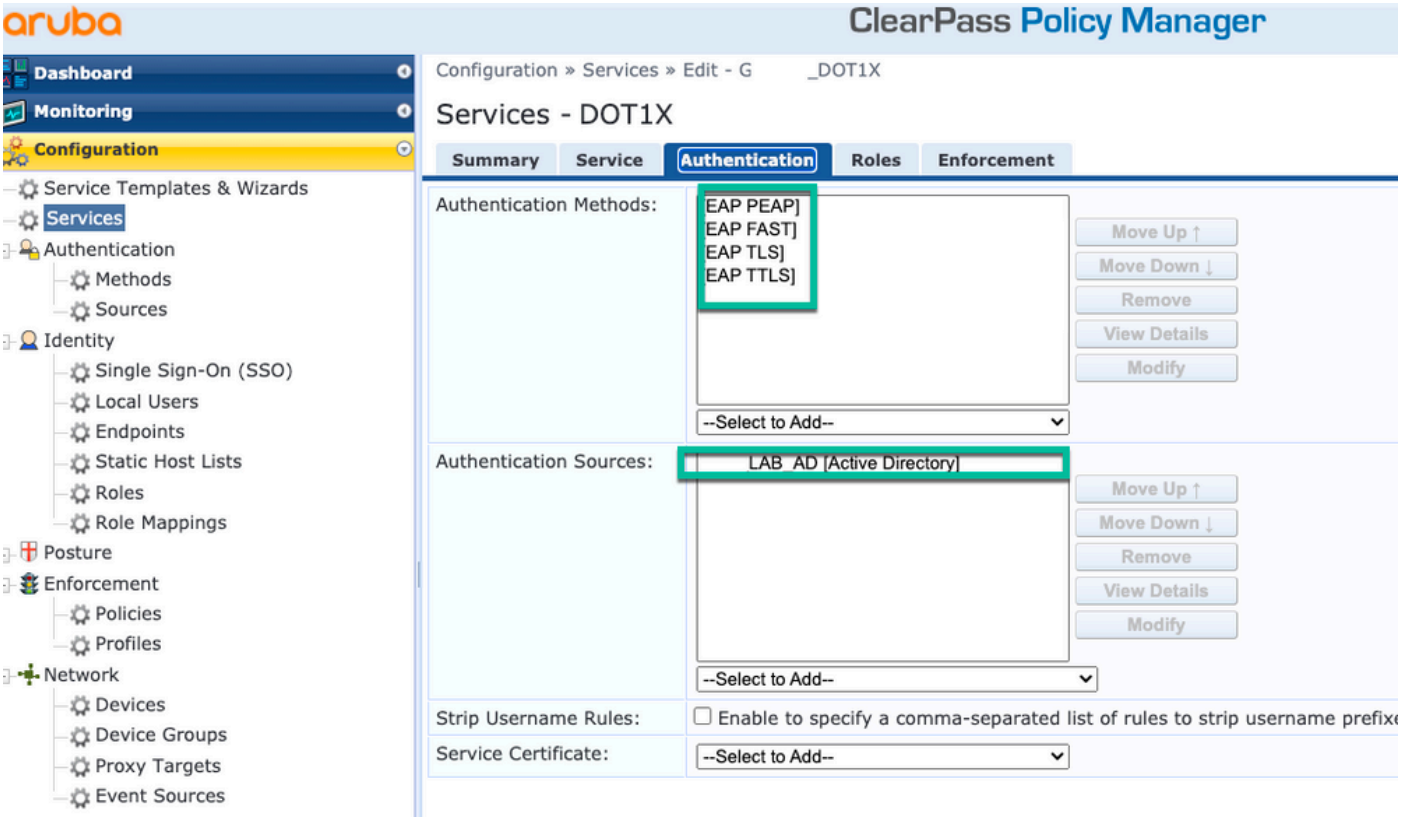
Étape 1. Créez un « service » correspondant à plusieurs attributs RADIUS :

- Rayon:IETF | Nom : Adresse IP du NAS | EST ÉGAL À | <ADRESSE IP>
- Rayon:IETF | Nom : Type de service | EST ÉGAL À |1,2,8

Étape 2. Pour la production, il est recommandé de faire correspondre un nom SSID au lieu de

'NAS-IP-Address' afin qu'une condition suffise dans un déploiement multi-WLC.
Radius:Cisco:Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID





Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide des meilleures pratiques de déploiement du Cisco 9800

- Comprendre le modèle de configuration des contrôleurs sans fil Catalyst 9800
- Présentation de FlexConnect sur le contrôleur sans fil Catalyst 9800
- **Support et documentation techniques - Cisco Systems**

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.