Configurer l'authentification locale en mode FlexConnect

Table des matières

- Introduction
  - Informations générales
    - Présentation et exigences de FlexConnect
    - Modes de fonctionnement
    - itinérance rapide et sécurisée
    - Mode haut de gamme FlexConnect
    - Prise en charge de Wi-Fi 7 FlexConnect
    - Scénarios de résilience FlexConnect
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configurer les serveurs AAA
  - Configurer le mode FlexConnect sur le site distant
  - Configurer un WLAN 802.1x avec authentification locale à l'aide d'un serveur RADIUS externe
  - Configuration d'ISE
  - Configuration du WLAN PSK avec authentification locale
- Vérifier
- Dépannage
  - Scénario autonome
- Informations connexes

Introduction

Ce document décrit le fonctionnement de l'authentification locale FlexConnect et comment la configurer à l'aide du contrôleur sans fil (WLC) de la gamme Cisco Catalyst 9800

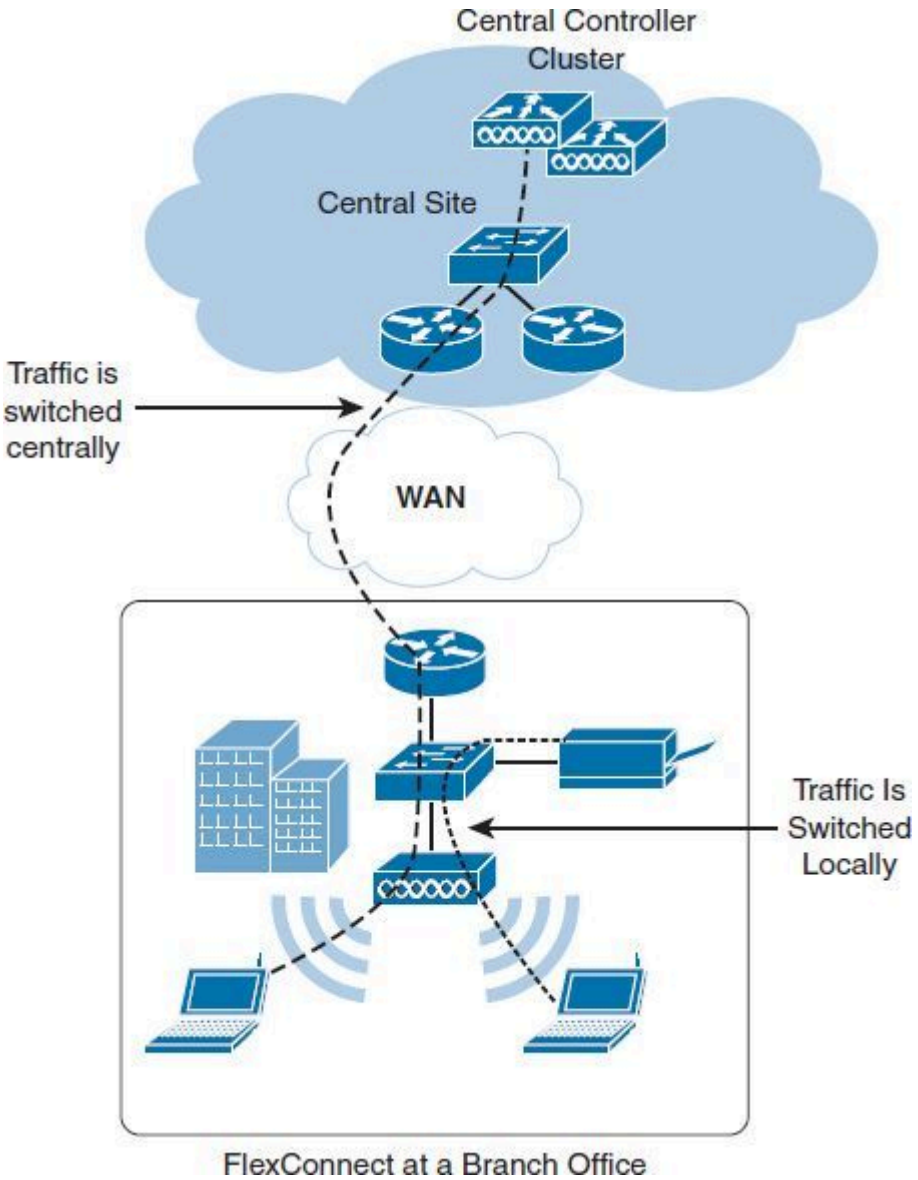
Informations générales

Présentation et exigences de FlexConnect

FlexConnect permet au point d'accès (AP) des bureaux distants ou des filiales de se connecter à

un contrôleur centralisé tout en permettant le traitement local du trafic sans fil. Contrairement aux déploiements sans fil centralisés traditionnels où tout le trafic sans fil est tunnellisé vers le contrôleur à l'aide de CAPWAP (Control and Provisioning of Wireless Access Points) — FlexConnect permet au trafic d'être commuté localement et géré directement par le point d'accès de la filiale. Cette commutation locale offre au point d'accès un certain degré d'autonomie, ce qui permet à des services clés tels que la sécurité, l'itinérance et la qualité de service (QoS) de fonctionner indépendamment du contrôleur.

Bien que FlexConnect soit principalement conçu pour la commutation du trafic local, il offre également la possibilité de commuter de manière centralisée des SSID spécifiques (Service Set Identifier) en cas de besoin. Par exemple, si un certain trafic doit passer par un pare-feu central, ces SSID peuvent être renvoyés au contrôleur via CAPWAP pour une commutation centralisée. Cette double fonctionnalité permet à un point d'accès FlexConnect unique de prendre simultanément en charge les réseaux locaux sans fil commutés localement et de manière centralisée.



Un point d'accès FlexConnect déployé dans une filiale commute localement un SSID tandis qu'un autre est commuté de manière

Modes de fonctionnement

Les points d'accès FlexConnect fonctionnent en deux modes : mode connecté et mode autonome.

- En mode connecté, le point d'accès maintient une connexion active au contrôleur via le canal de contrôle CAPWAP.
- Le mode autonome est un état de secours qui se produit lorsque le point d'accès perd la connectivité au contrôleur.

Dans des conditions normales, les points d'accès FlexConnect fonctionnent en mode connecté, où le contrôleur gère des services critiques tels que l'authentification centralisée, le profilage client et la gestion des ressources radio (RRM). Alors que le point d'accès est censé rester dans ce mode la plupart du temps, il passe automatiquement en mode autonome si la communication avec le contrôleur est perdue. En mode autonome, le point d'accès continue à fonctionner, commutant localement le trafic et permettant aux clients de rester connectés. Les points d’accès authentifient indépendamment les clients sans transmettre de demandes d’authentification à un contrôleur central. Cependant, certains services dépendants du contrôleur, tels que RRM et l'authentification client centralisée, deviennent temporairement indisponibles.

Par exemple, si une panne WAN (Wide Area Network) interrompt la connexion entre le point d'accès et le contrôleur mais que l'accès Internet reste actif, le point d'accès passe en mode autonome et continue à traiter le trafic commuté localement sans interruption. Les clients existants restent connectés, mais les nouveaux clients nécessitant une authentification centrale ne peuvent pas se connecter au réseau, sauf si l'authentification locale est configurée. Les points d'accès FlexConnect peuvent être configurés pour effectuer une authentification locale pendant les pannes de réseau étendu, assurant ainsi un service continu même lorsque le contrôleur est inaccessible.

En mode autonome, ces fonctionnalités ne sont pas disponibles pour le point d'accès :

- Authentification Web du client
- Authentification des invités (redirection du portail)
- Tous les SSID commutés de manière centralisée
- RRM
- Mobilité de couche 3 IPv6

- Profilage natif
- Classification des politiques
- Passerelle de découverte de service
- Mises à jour de configuration

Pour obtenir la liste complète des fonctionnalités et des configurations WLAN prises en charge en mode autonome (authentification locale), reportez-vous à la matrice des fonctionnalités : Matrice de fonctionnalités des points d'accès sans fil Cisco

Un scénario de défaillance FlexConnect courant implique une perte complète ou une dégradation significative du WAN, ce qui perturbe le canal de contrôle CAPWAP. Lorsque le point d'accès perd la connectivité au contrôleur en raison de problèmes de réseau étendu, il passe immédiatement en mode autonome.

En cas de panne d'un réseau étendu, l'objectif principal est de rétablir la communication avec le contrôleur aussi rapidement que possible afin de reprendre toutes les fonctionnalités.

Lorsqu'un point d'accès FlexConnect passe en mode autonome en raison d'une défaillance du réseau étendu, les clients actifs restent connectés et peuvent circuler de manière transparente entre les points d'accès au sein de la balise de domaine/site FlexConnect, mais l'itinérance entre différentes balises de site FlexConnect peut nécessiter une réauthentification complète. Cependant, les nouveaux clients qui tentent de se connecter au WLAN commuté localement ne peuvent pas s'authentifier, car le serveur AAA (Authentication, Authorization, and Accounting Server) à l'emplacement central est inaccessible.

itinérance rapide et sécurisée

L'authentification EAP (Extensible Authentication Protocol) introduit une latence plus élevée que l'authentification PSK (Pre-Shared Key) en raison de l'échange de trames EAP avec le serveur AAA. Cependant, avec l'itinérance sécurisée rapide, un client subit une authentification 802.1X/EAP complète uniquement lors de son association initiale avec le réseau. Sur les itinéraires suivants vers les AP voisins, l'échange EAP est contourné, laissant seulement la connexion en quatre étapes, ce qui est beaucoup plus rapide puisqu'il n'implique pas le serveur AAA. Ce tableau présente les différentes méthodes d'itinérance rapide et sécurisée prises en charge par le WLC 9800 dans les déploiements en mode local et FlexConnect.

Fonctionnalité	Mode local	FlexConnect (mode connecté ; Authentification	FlexConnect (Mode connecté - Authentification	FlexConnect (autonome)

		centrale)	locale)	
Mise en cache des clés rémanentes (SKC)	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
Mise en cache des clés opportuniste (OKC)	Pris en charge	Pris en charge	Pris en charge	Pris en charge (jusqu'à expiration de la session client)
Gestion centralisée des clés Cisco (CCKM)	Pris en charge	Pris en charge	Pris en charge	Non pris en charge
FT-802.11r/ Adaptive 11r (Fast Transition) (Over the Air)	Pris en charge	Pris en charge	Pris en charge	Pris en charge (jusqu'à expiration de la session client)
FT-802.11r/ Adaptive 11r (Fast Transition) (sur DS)	Pris en charge	Pris en charge	Non pris en charge	Non pris en charge

En mode autonome, l'itinérance rapide dépend de la clé stockée en mémoire cache qui reste valide. Lorsque la session/PMK (Pairwise Master Key) mise en cache expire, le point d'accès ne peut pas obtenir de nouvelles informations de clé dérivées du contrôleur tant que la connectivité du contrôleur n'est pas restaurée.

Mode haut de gamme FlexConnect

À partir de la version 17.8.1 de Cisco IOS XE, la capacité du site Flex a été augmentée pour accueillir 300 points d'accès et 3 000 clients 802.1x.

La propagation PMK permet aux points d'accès d'un même site FlexConnect de partager des informations PMK, réduisant ainsi le besoin d'un échange EAP complet pendant l'itinérance. La propagation PMK n'est pas activée par défaut.

Utilisez ces commandes pour vérifier la propagation PMK et pour activer PMK :

- show wireless stats pmk-propagation
- propagation pmk

Prise en charge de Wi-Fi 7 FlexConnect

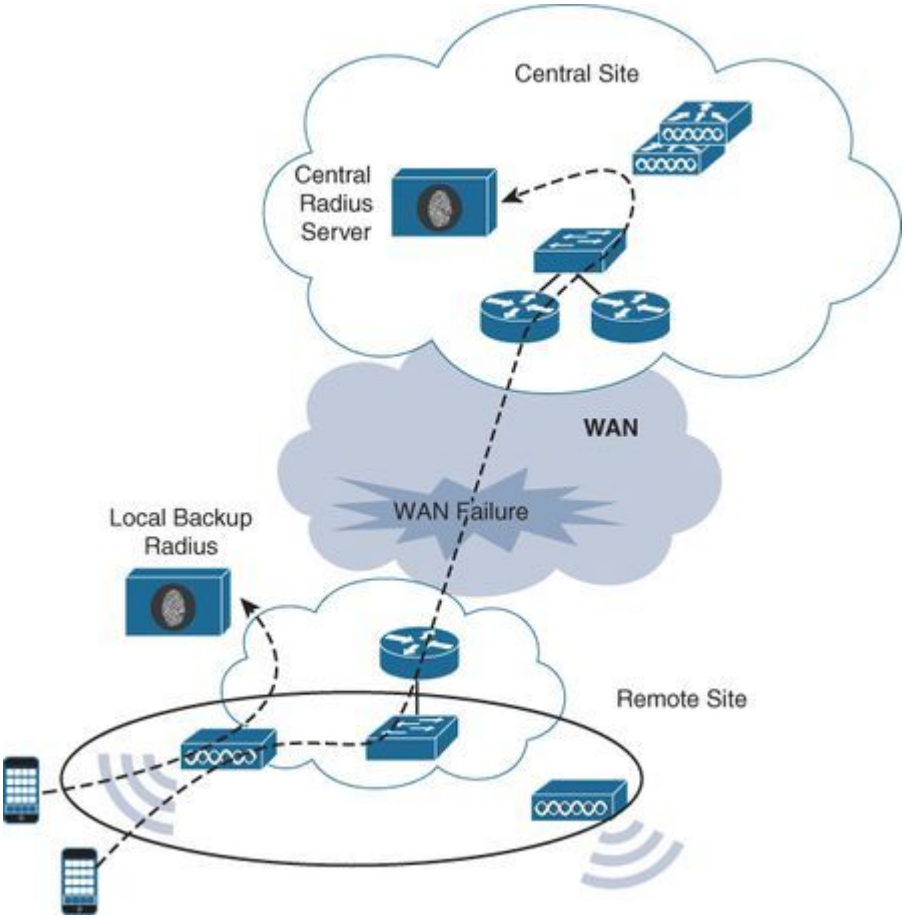
Ce tableau récapitule les fonctionnalités FlexConnect prises en charge par la famille de points d'accès CW917x Wi-Fi 7.

Fonctionnalité	Soutien
Commutation locale	Pris en charge
Commutation centrale	Pris en charge
Mappage WLAN-VLAN	Pris en charge
Authentification locale avec RADIUS externe	Pris en charge
WPA3-Entreprise	Pris en charge
Itinérance rapide FT-802.11r	Pris en charge
Fonctionnement multiliaison (MLO)	Pris en charge
Authentification locale avec RADIUS interne	Non pris en charge
WPA3-Entreprise-192	Non pris en charge

Scénarios de résilience FlexConnect

1. Dans une configuration de résilience N+1, plusieurs contrôleurs actifs partagent un contrôleur de secours commun qui prend le relais en cas de défaillance d'un contrôleur actif. Lorsqu'un contrôleur principal se déconnecte, les points d'accès FlexConnect passent immédiatement en mode autonome et commencent à rechercher le contrôleur de secours. Pendant cette période de déconnexion, les clients à commutation centrale sont déconnectés des points d'accès. Une fois que les points d’accès localisent et synchronisent avec le contrôleur de secours, les clients nécessitant un accès aux SSID commutés de manière centralisée sont reconnectés. Pendant ce temps, les clients commutés localement restent inchangés et continuent à fonctionner sans remarquer l'interruption du service.
2. Fournir un serveur AAA de sauvegarde sur le site distant, accessible par le groupe FlexConnect. Lorsque l'authentification locale est activée, ce serveur RADIUS de sauvegarde n'est utilisé que lorsque les points d'accès passent en mode autonome ; il reste inactif tant que les points d'accès sont en mode connecté. Lorsque les points d'accès FlexConnect utilisent le serveur AAA de sauvegarde local pour l'authentification, les clés d'authentification sont distribuées sur tous les points d'accès du groupe FlexConnect, comme elles le seraient avec un serveur AAA centralisé. Cela garantit que les nouveaux clients peuvent continuer à se déplacer en toute transparence entre les points d'accès sans

avoir besoin de s'authentifier à nouveau, même lorsque le serveur RADIUS de sauvegarde est utilisé.
3. Toute méthode présente dans la matrice de fonctionnalités des points d'accès sans fil Cisco qui permet l'authentification locale.



Les clients s'authentifient auprès d'un serveur AAA de sauvegarde local lorsque le serveur AAA central devient indisponible en raison d'une défaillance du réseau étendu

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Contrôleur sans fil Catalyst C9800-CL pour le cloud avec Cisco IOS® XE Dublin 17.18.3
- Point d'accès Catalyst CW9164I-ROW v17.18.3.18
- Point d'accès Aironet® AIR-AP2802I-E-K9 v17.18.3.18
- 2 x Identity Services Engine v3.2.0.542

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

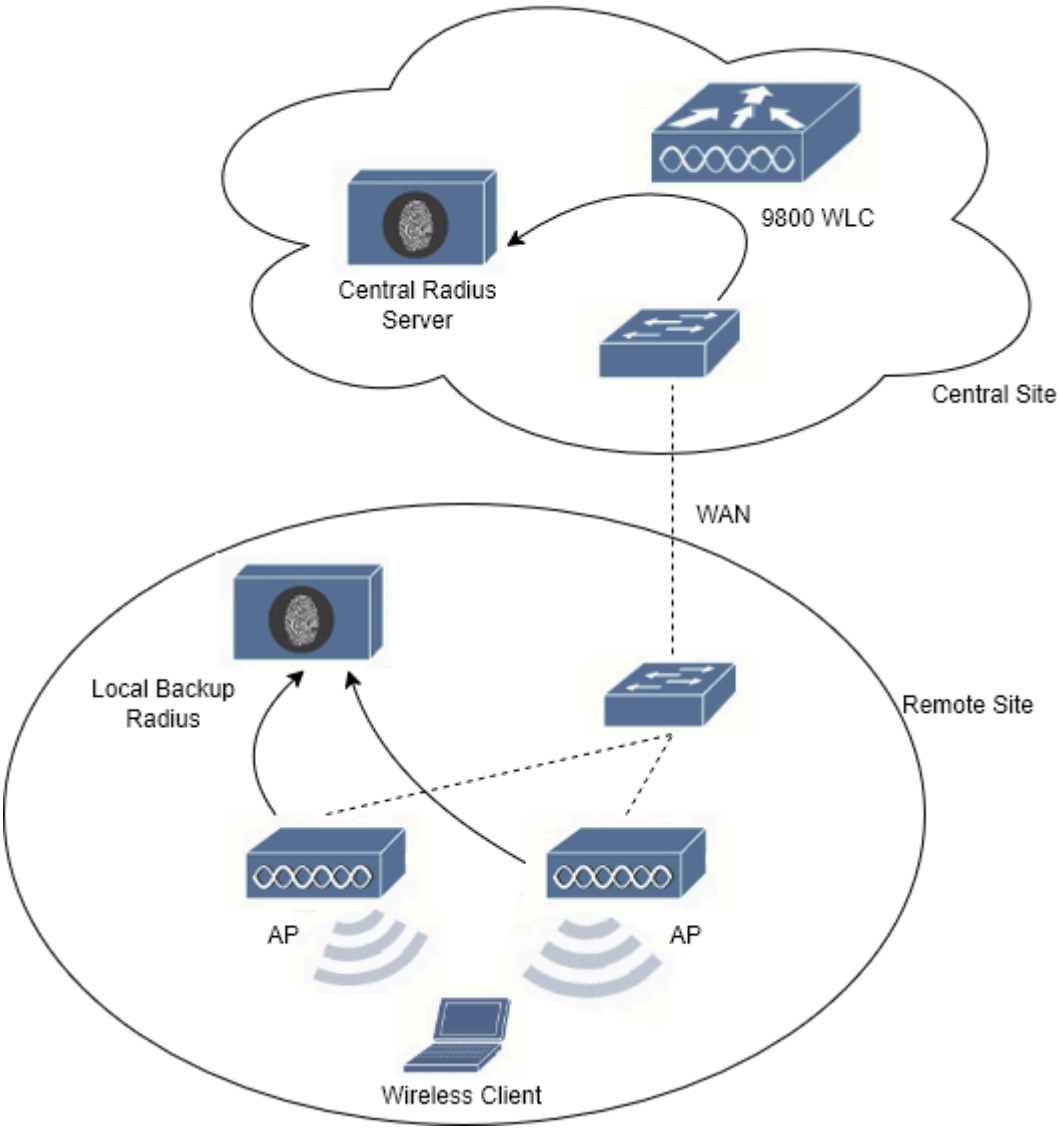


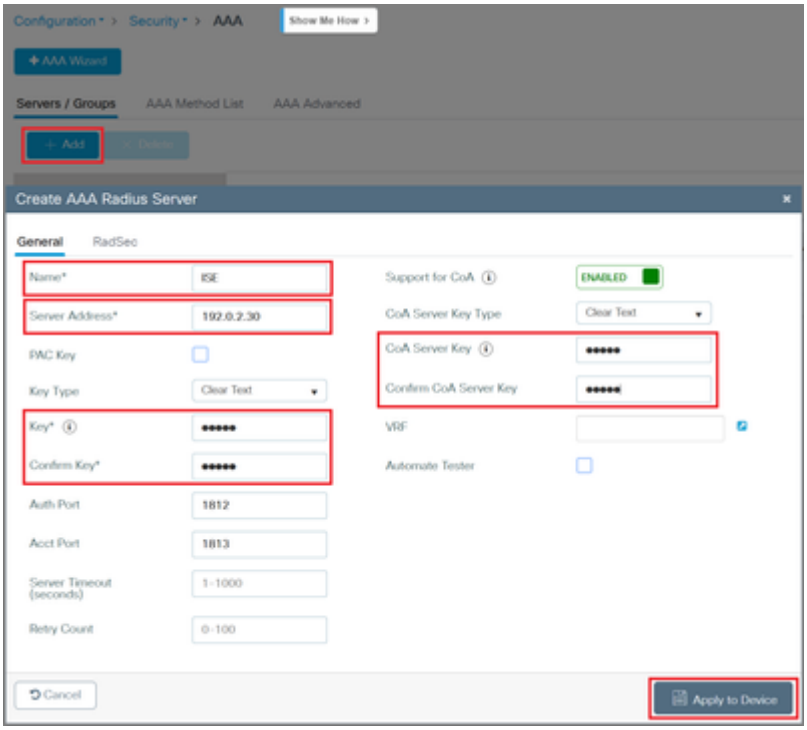
Diagramme du réseau

Configurer les serveurs AAA

Étape 1. Pour configurer un WLAN 802.1x, vous devez créer le groupe de serveurs AAA sur le WLC 9800.

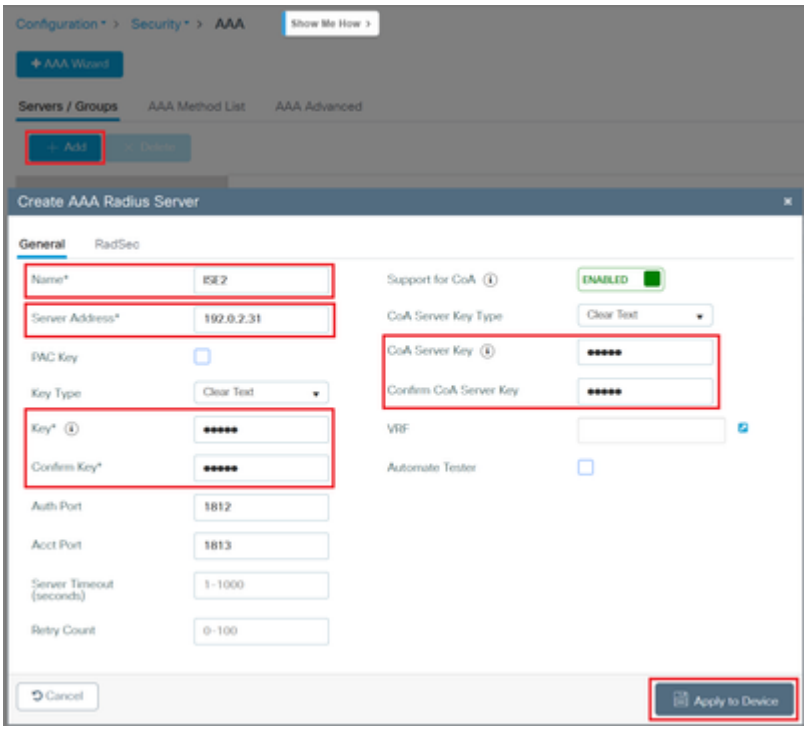
Créez un serveur AAA pour chaque site : l'un sur le site central et l'autre sur le site distant.

Accédez à Configuration > Security > AAA > Server/Groups > Servers et sélectionnez +Add. Donnez un nom au serveur, son adresse IP, la clé (et la clé de confirmation), activez la prise en charge CoA (changement d'autorisation) et entrez la clé du serveur CoA (et confirmez la clé du serveur CoA). Les clés doivent être identiques.



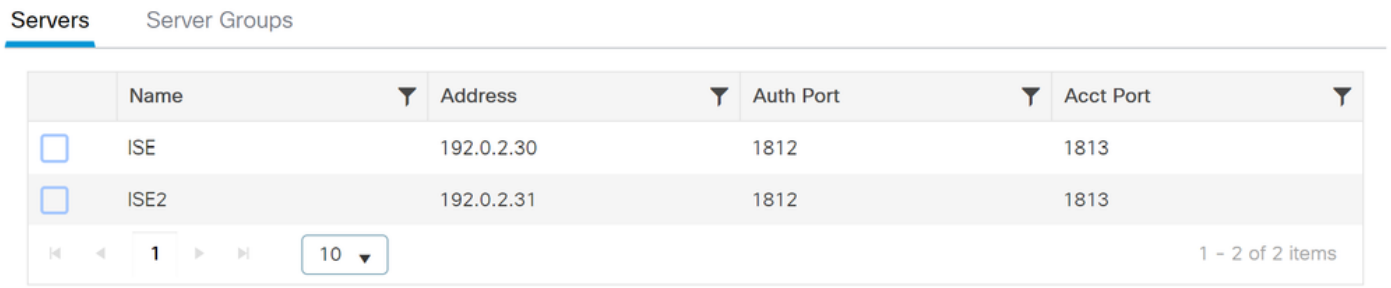
Cliquez sur Apply to Device.

Étape 2. Créez l’autre serveur AAA :

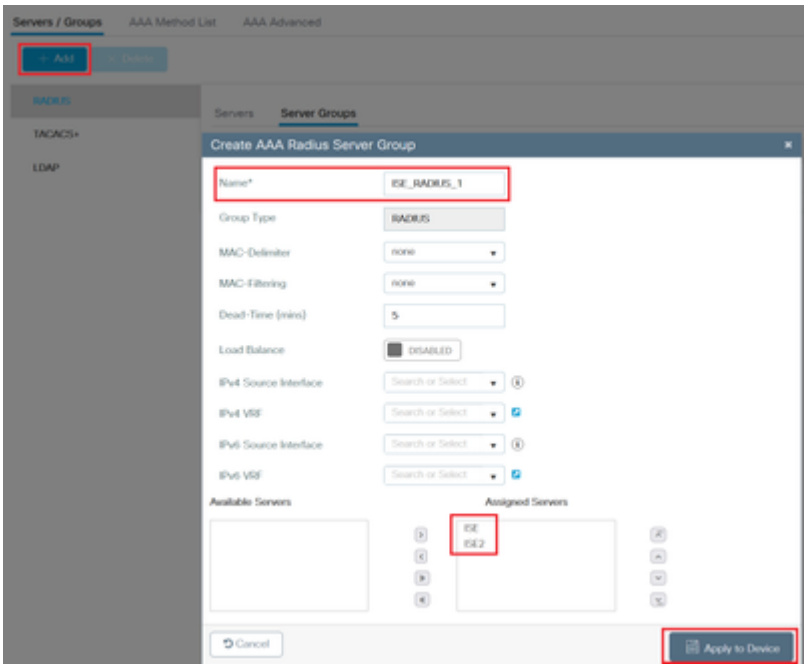


Cliquez sur Apply to Device.

Vous voyez maintenant vos serveurs AAA configurés :

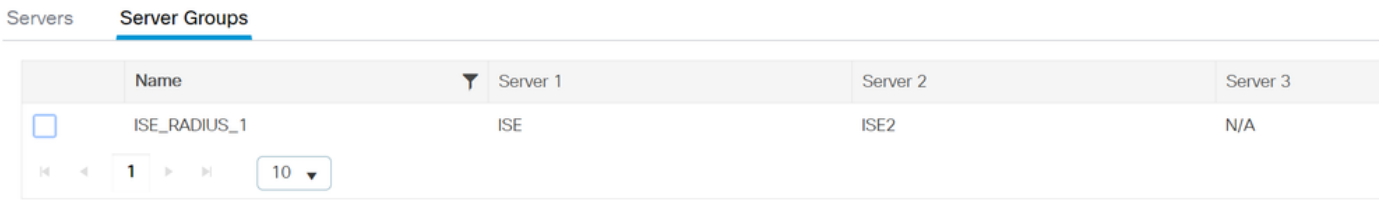


Étape 3. Accédez à Configuration > Security > AAA > Server/Groups > Server Groups et sélectionnez +Add. Donnez un nom au serveur de groupe et sélectionnez les serveurs AAA précédemment créés dans la colonne Assigned Servers :



Cliquez sur Apply to Device.

Vous voyez ensuite le groupe de serveurs AAA configuré :



CLI :

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

Configurer le mode FlexConnect sur le site distant

Étape 1 : configuration de FlexConnect sur le site distant

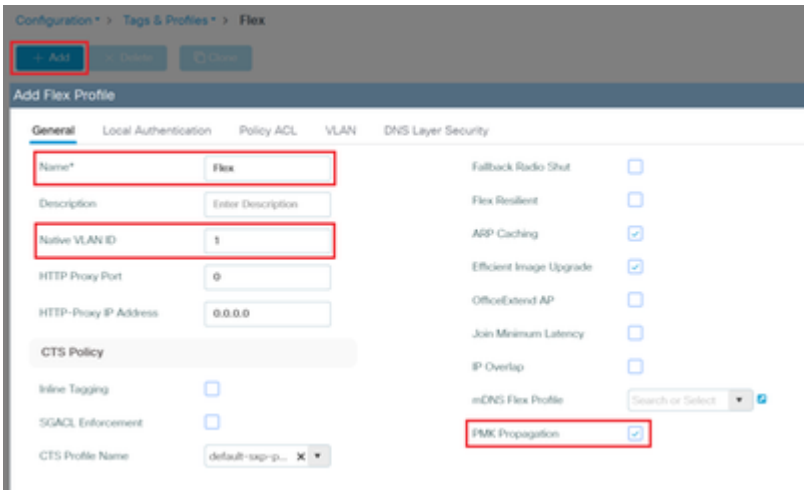
Utilisez ce guide pour passer en mode Flex : Understanding FlexConnect on Catalyst 9800 Wireless Controller.

Les points d'accès de ce guide/de ces travaux pratiques utilisent le même profil flexible.

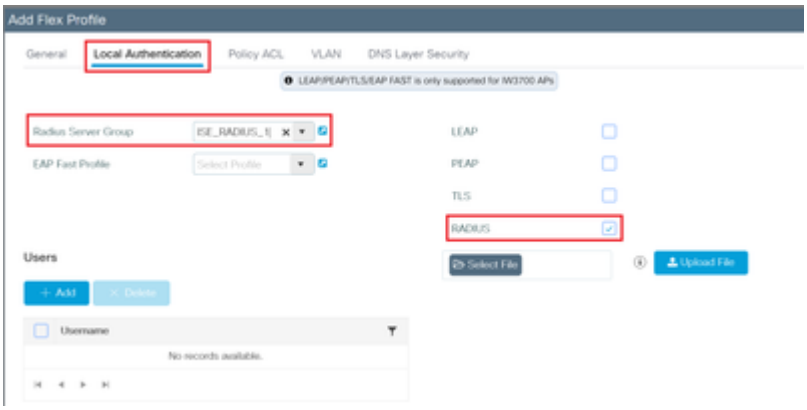
Étape 2. Accédez à Configuration > Tags & Profiles > Flex.

Créez un nouveau nom de profil flexible avec +Ajouter. Dans l'onglet General, attribuez un nom au profil, entrez l'ID du VLAN natif (Virtual Local Area Network) et activez la propagation PMK.

Activez la propagation PMK pour faciliter l'itinérance transparente des clients sans fil en partageant les informations PMK entre les points d'accès au sein d'un site unique.

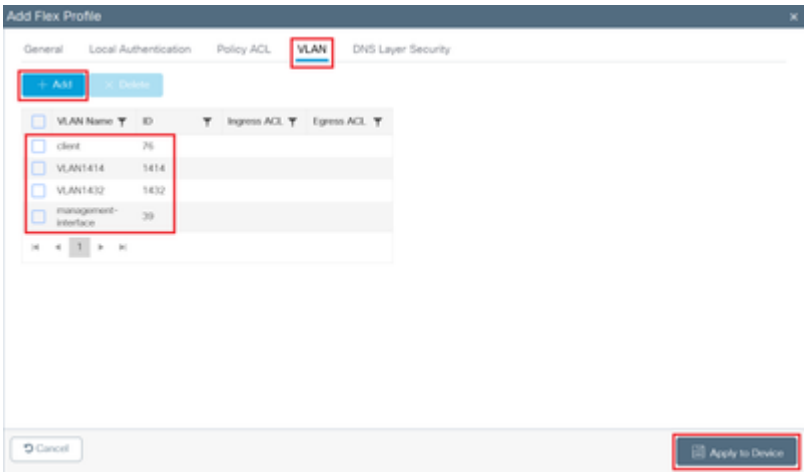


Étape 3. Pour le WLAN 802.1x, sous l'onglet Local Authentication, sélectionnez le groupe de serveurs Radius et activez RADIUS :



Conseil : Pour un WLAN PSK, vous n'avez pas besoin d'ajouter quoi que ce soit dans cet onglet.

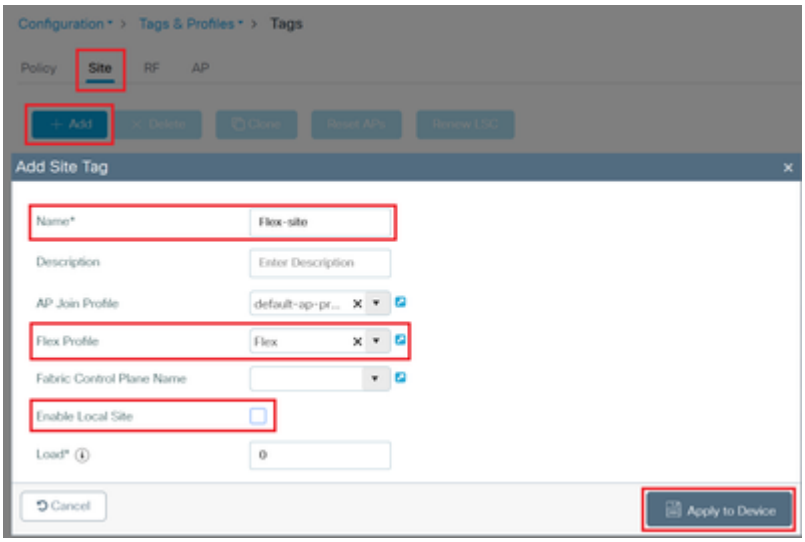
Étape 4. Sous l'onglet VLAN, ajoutez tous les VLAN utilisés par les clients, les points d'accès et le serveur RADIUS. Assurez-vous que chaque nom de VLAN correspond à l'ID de VLAN correct :



À la fin, cliquez sur Update & Apply to Device.

Étape 5. Accédez à Configuration > Tags & Profiles > Tags > Site et sélectionnez +Add.

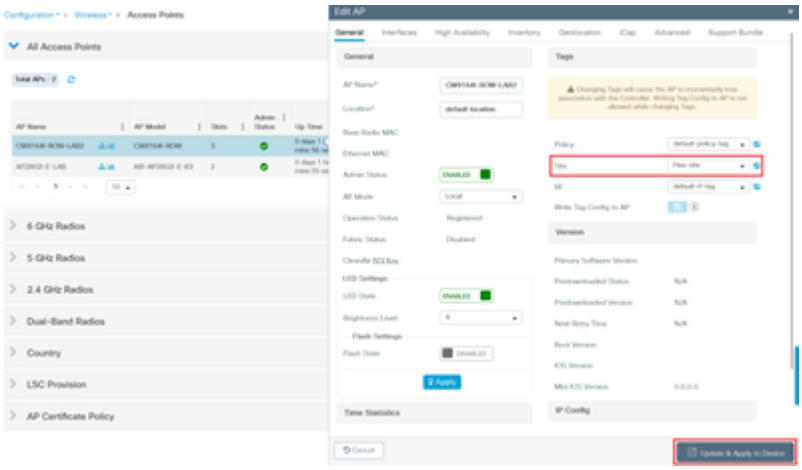
Créez la balise de site avec le profil paramétrable créé précédemment. Donnez-lui un nom, sélectionnez le profil Flex approprié et désactivez Activer le site local. Assurez-vous que le profil de jonction AP est le bon.



Cliquez sur Apply to Device.

Étape 6. Accédez à Configuration > Wireless > Access Points.

Sélectionnez votre AP, sur General > Tags changez le Site Tag à la balise précédemment configurée :



Cliquez sur Update & Apply to Device.

L'AP se déconnecte du WLC et se reconnecte avec le mode Flex AP.

Sur la même page, lorsque l'AP se joint de nouveau, vous pouvez vérifier le mode AP sur la colonne AP Mode.

Si vous sélectionnez le point d'accès, il affiche la nouvelle balise Site :



CLI :

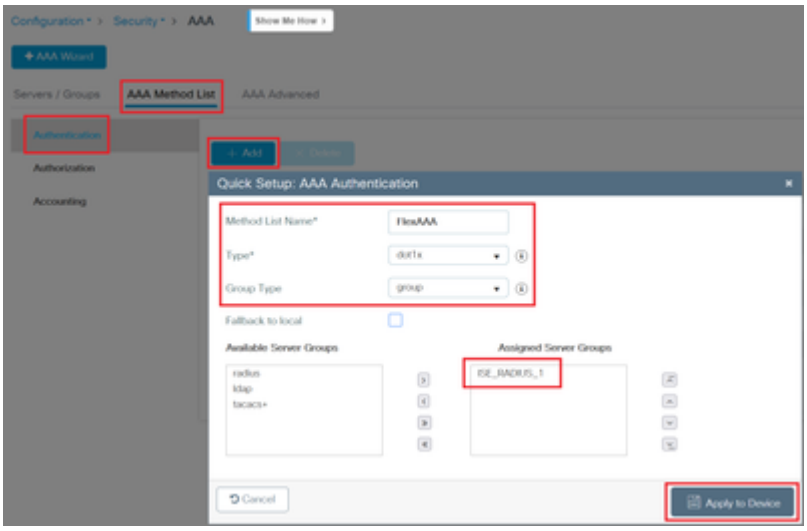
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Configurer le WLAN 802.1x avec l'authentification locale à l'aide d'un serveur RADIUS externe

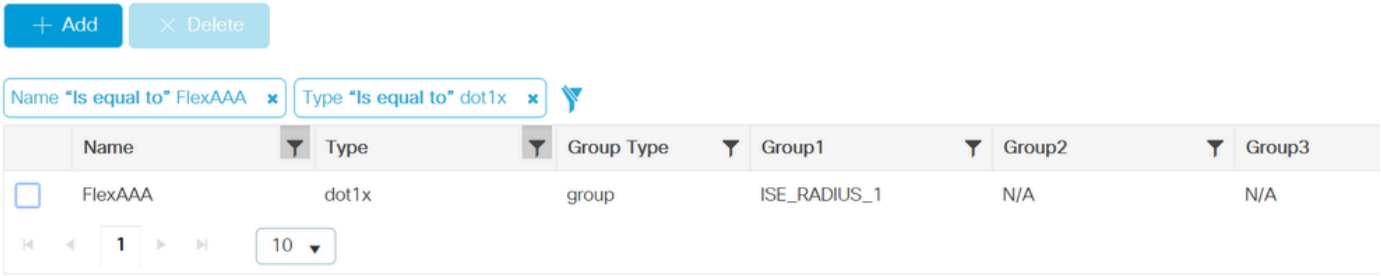
Étape 1 : création de la liste des méthodes d’authentification

Accédez à Configuration > Security > AAA, sur AAA Method List > Authentication tab.

Sélectionnez +Add, donnez un nom au nom de la liste de méthodes, sélectionnez dot1x comme type, sélectionnez group comme type de groupe et attribuez le groupe de serveurs AAA dans la colonne Assigned Server Groups :



Vous voyez maintenant la liste des méthodes AAA créées :



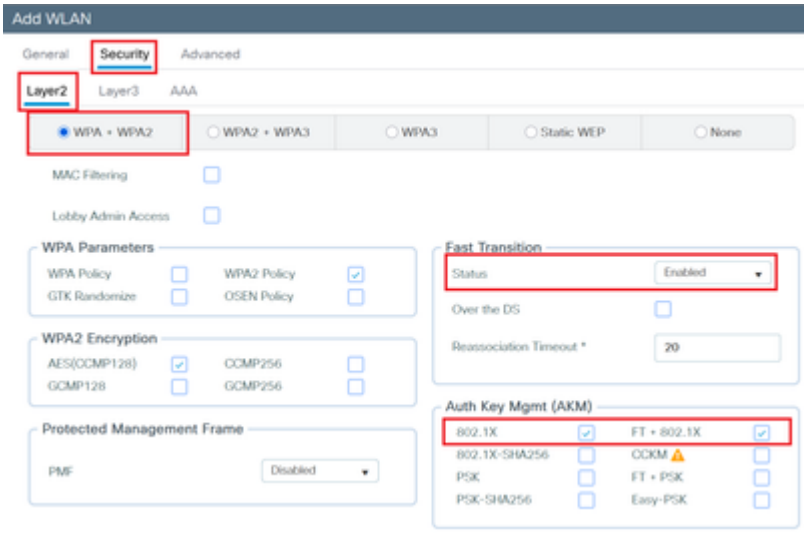
Étape 2 : création du WLAN

Accédez à Configuration > Tags & Profiles > WLANs, sélectionnez +Add.

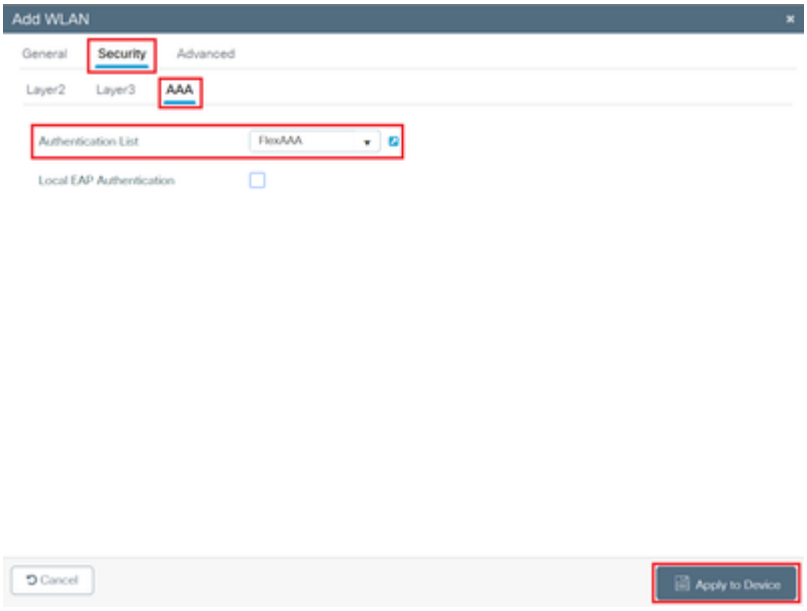
Dans la balise General, créez un nom pour le nom de profil, le SSID et l'état enable :



Étape 3. Accédez à Security > Layer 2 tab, sélectionnez WPA+WPA2 (Wi-Fi Protected Access), Fast Transition as Enabled, Auth Key Mgmt 802.1X and FT+802.1X :



Étape 4. Accédez à Security > AAA tab, sur le Authentication List menu déroulant sélectionnez la liste créée précédemment :



Cliquez sur Update & Apply to Device.

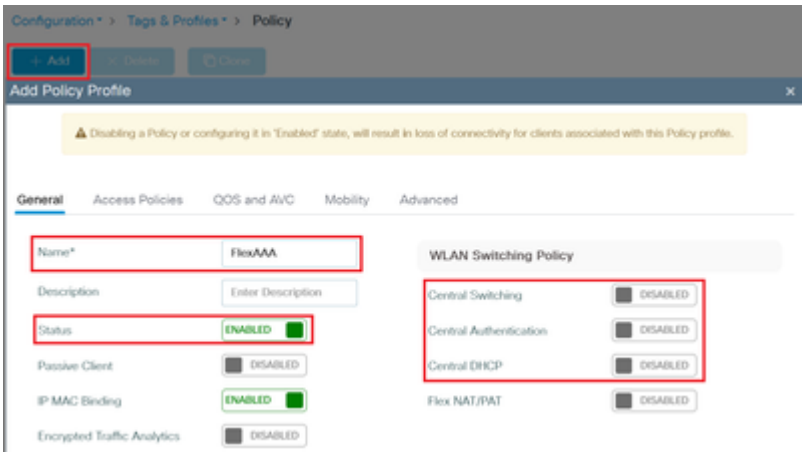
Vous voyez ensuite le WLAN créé :



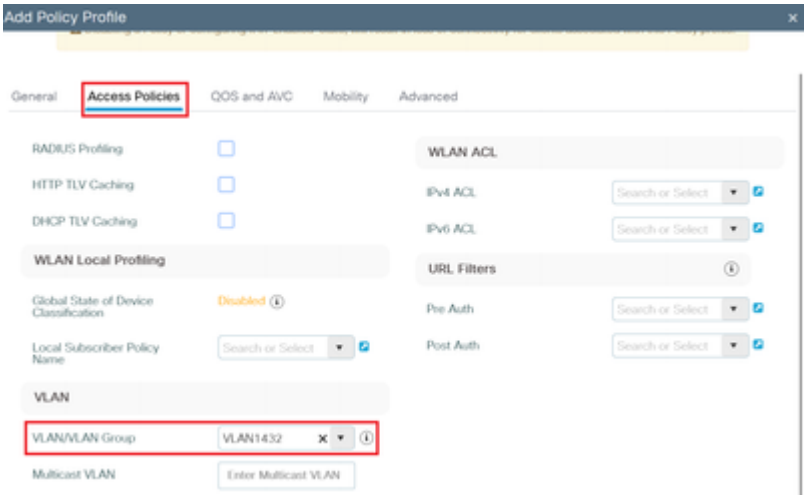
Étape 5. Création du profil de stratégie

Accédez à Configuration > Tags & Profiles > Policy.

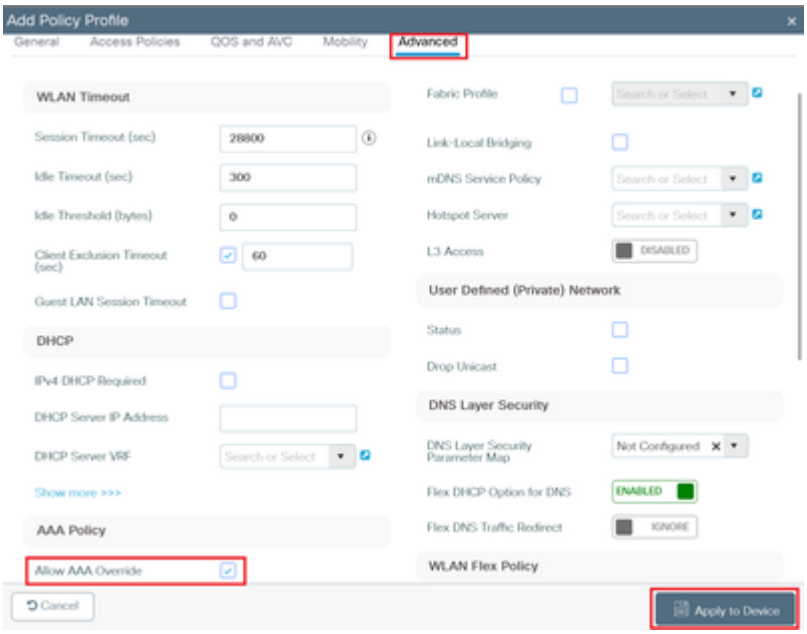
Sélectionnez +Add et, dans l'onglet General, attribuez un nom au profil de stratégie, activez l'état et désactivez la commutation centrale, l'authentification centrale et le protocole DHCP (Dynamic Host Configuration Protocol) central :



Étape 6. Accédez à l'onglet Access Policies, sélectionnez le VLAN :

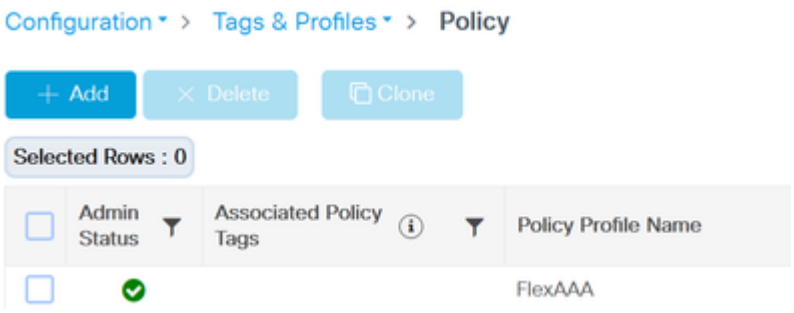


Étape 7. Accédez à l'onglet Advanced, activez Allow AAA Override. :



Cliquez sur Update & Apply to Device.

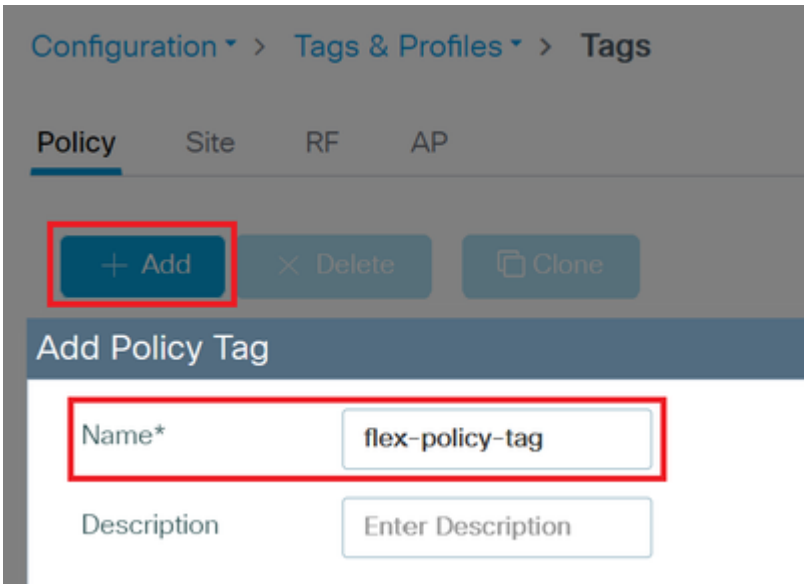
Vous pouvez voir le profil de stratégie dans la liste :



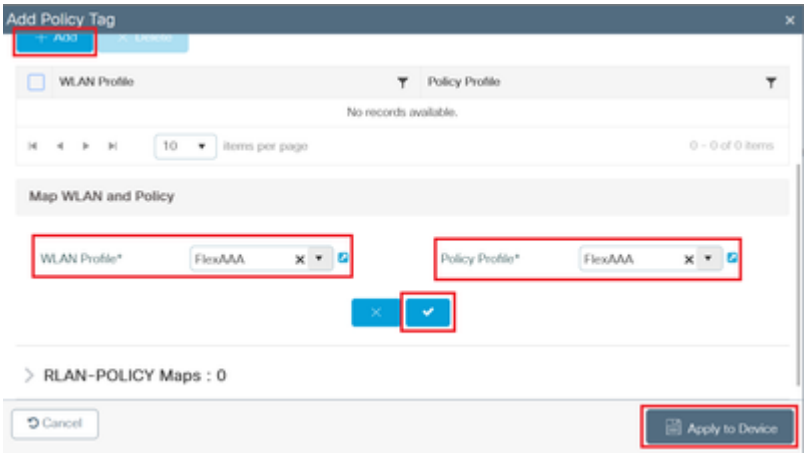
Étape 8. Créer une balise de stratégie

Accédez à Configuration > Tags & Profiles > Tags

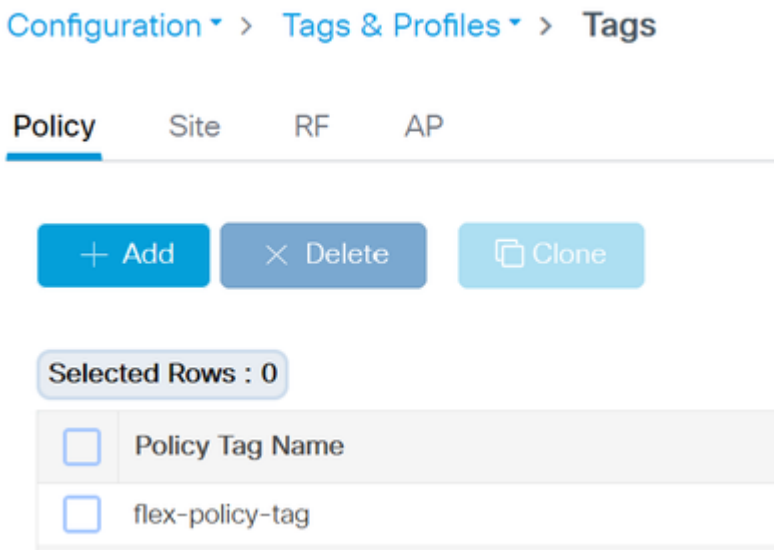
Dans l'onglet Stratégie, sélectionnez +Ajouter. Attribuez un nom à la balise de stratégie :



Faites défiler vers le bas et sélectionnez +Add sous WLAN-POLICY Maps. Dans Profil WLAN, sélectionnez le WLAN précédemment créé dans le menu déroulant. Dans Profil de stratégie, sélectionnez le profil de stratégie précédemment créé dans le menu déroulant. Cliquez sur le bouton de vérification, puis sur Apply to Device :

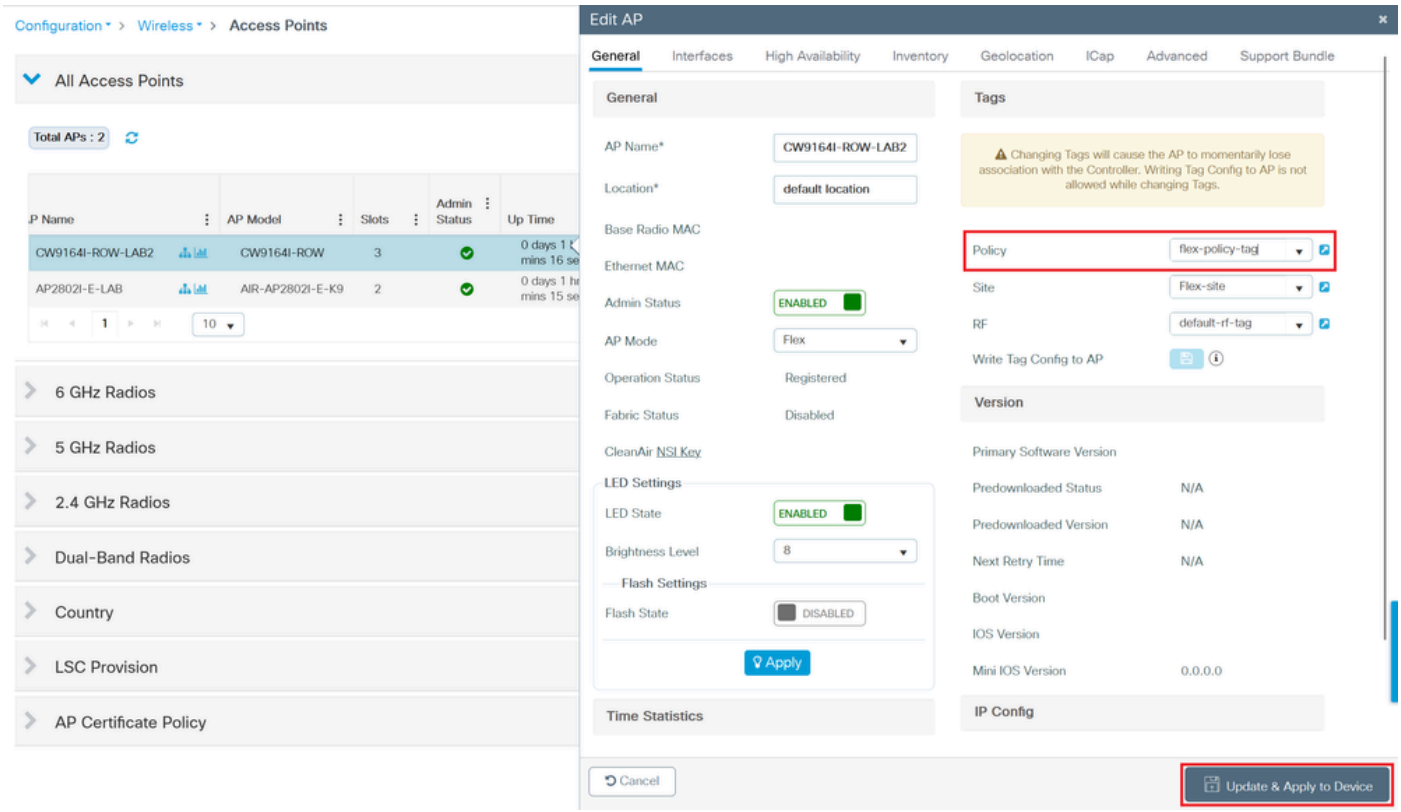


Vous pouvez voir la balise de stratégie dans la liste :



Étape 9. Attribuez la balise de stratégie à la balise AP.

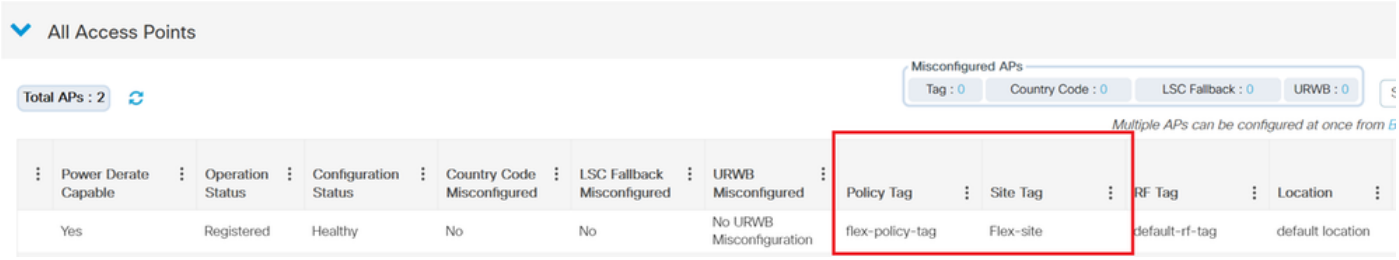
Accédez à Configuration > Wireless > Access Points. Sélectionnez le point d'accès pour modifier la balise.



Cliquez sur Update & Apply to Device.

Le point d'accès se sépare et se joint à nouveau avec la nouvelle balise de stratégie.

Lorsque le point d'accès se reconnecte, vous pouvez vérifier la liste des points d'accès, confirmer que le point d'accès est en mode flexible et les balises attribuées :



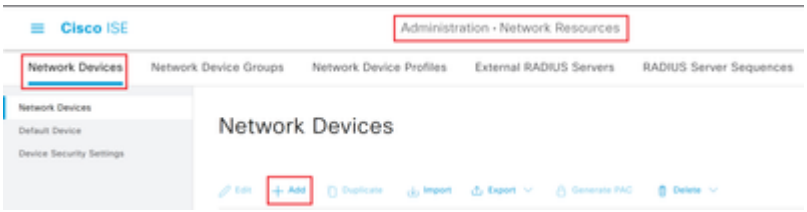
CLI :

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

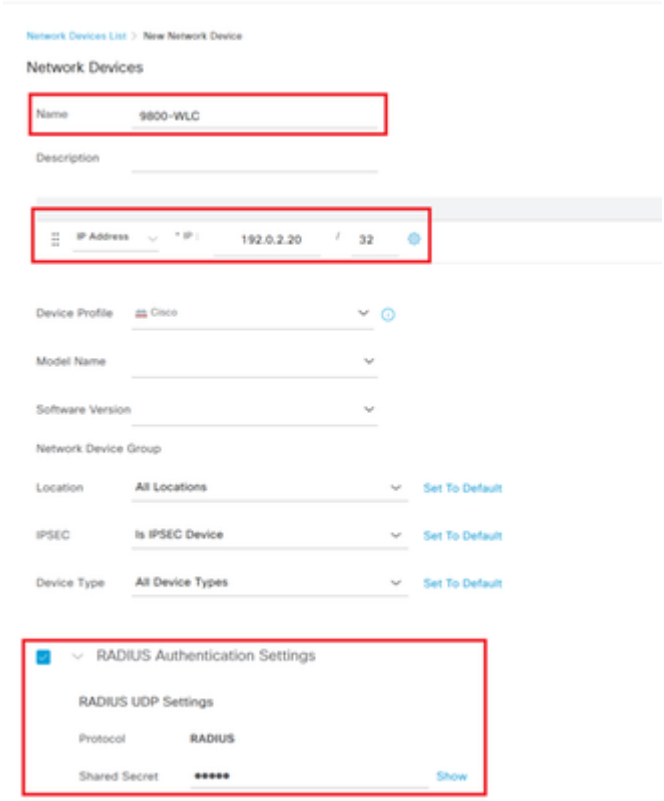
Configuration d'ISE

Vous devez maintenant configurer ISE pour pouvoir authentifier les clients lorsqu'ils sont dans l'authentification locale.

Étape 1.Accédez à Administration > Network Resources > Network Devices. Sélectionnez +Ajouter.



Étape 2 : ajout du WLC 9800 Donnez-lui un nom, ajoutez son adresse IP, activez les paramètres d'authentification RADIUS et ajoutez la clé secrète partagée. Cette clé doit être la même que celle que vous avez configurée précédemment lorsque vous avez créé les serveurs AAA sur le WLC 9800.



Dans l'angle inférieur droit, cliquez sur Save.

Étape 3. Nous devons ajouter les points d'accès à la liste des périphériques réseau pour qu'ils puissent agir en tant qu'authentificateurs/redirecteurs AAA lorsque le site distant perd la liaison WAN (et lorsque les points d'accès passent en mode autonome).

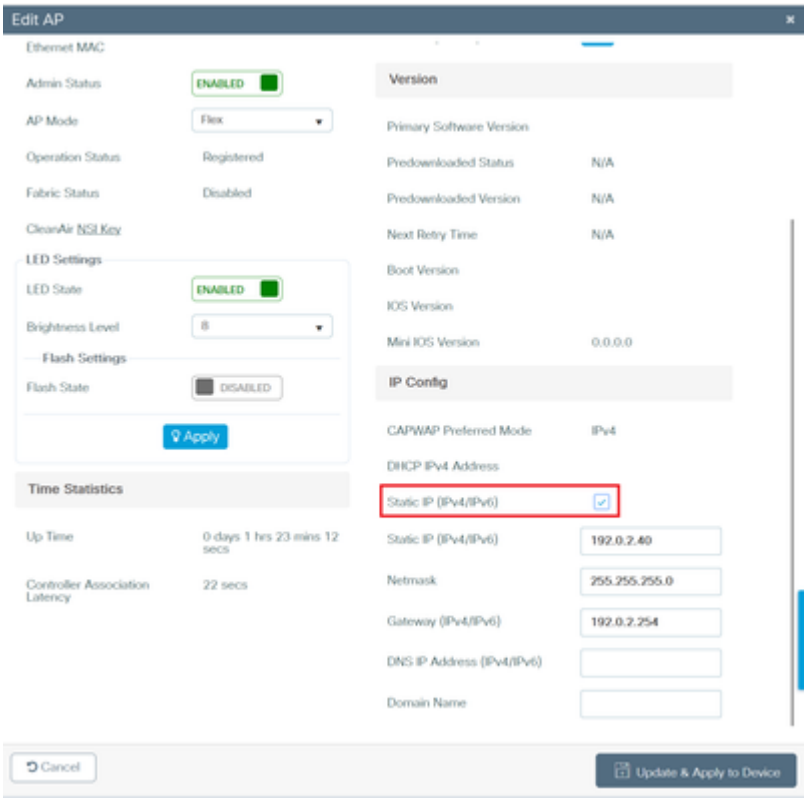
Accédez à Configuration > Wireless > Access Points sur l'interface graphique utilisateur du WLC 9800 et prenez note de chaque adresse IP AP.

Remarque : Configurez l'adresse IP de chaque point d'accès flexible sur Static. Lorsque

---

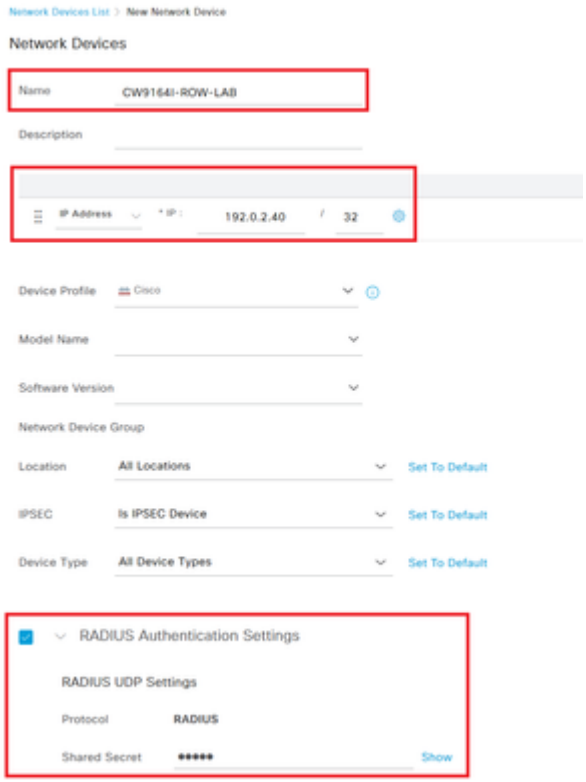
les points d'accès perdent et reprennent la connexion au WLC 9800, ils peuvent revenir avec une adresse IP différente de DHCP, et donc perdre la communication avec ISE.

Activez l'IP statique (IPv4/IPv6). Cliquez sur Update & Apply to Device :



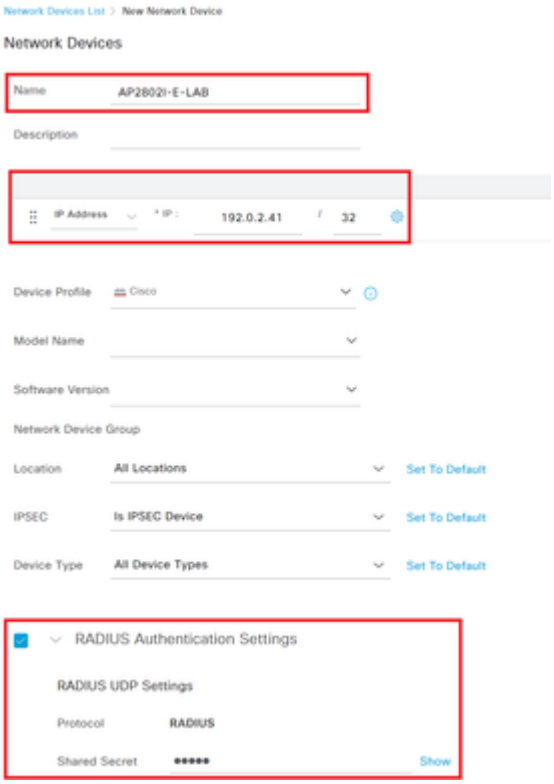
Étape 4. De nouveau sur ISE, accédez à Administration > Network Resources > Network Devices. Sélectionnez +Ajouter.

Ajoutez vos points d'accès en tant que périphériques réseau, avec la même configuration que le WLC 9800 :



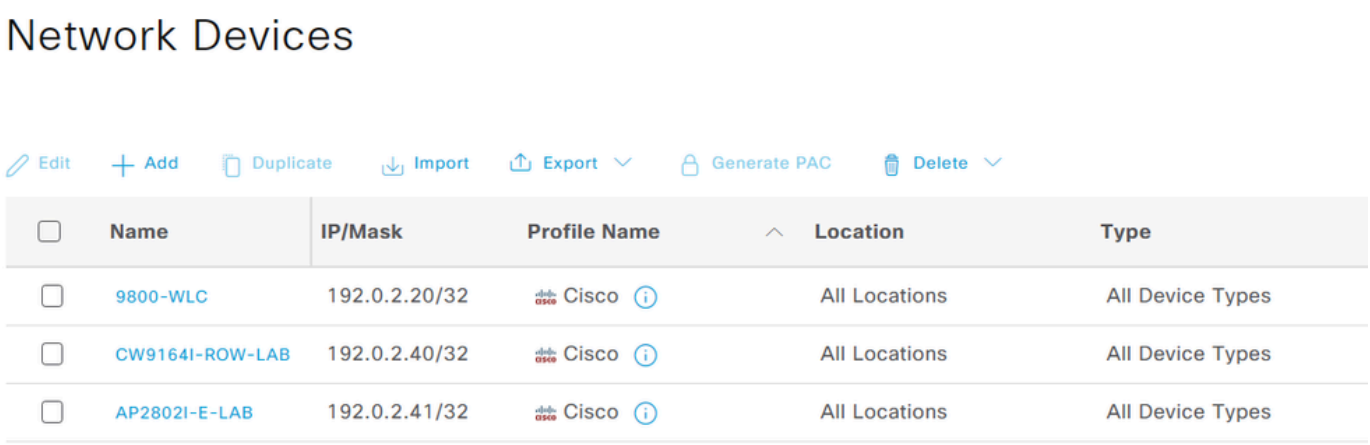
Dans l'angle inférieur droit, cliquez sur Save.

Pour le deuxième point d'accès :



Dans l'angle inférieur droit, cliquez sur Save.

Vous pouvez voir cette liste de périphériques réseau :

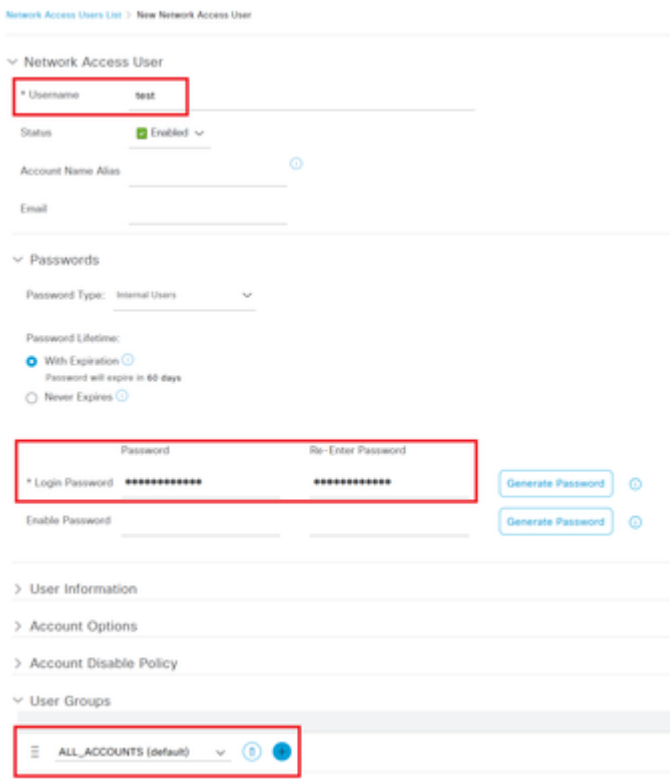


Si vos points d'accès se trouvent dans des plages d'adresses IP contiguës, vous pouvez utiliser la fonctionnalité de masque pour configurer une seule entrée qui définit le secret partagé pour un groupe entier (sinon tous) de points d'accès. Il n'est pas réellement nécessaire de configurer un périphérique réseau par point d'accès dans ISE. Notez cependant qu'en utilisant des caractères génériques et des masques, vous laissez de la place à un périphérique non autorisé pour essayer d'agir en tant que redirecteur vers ISE.

Étape 5. Accédez à Administration > Identity Management > Identities, sur l'onglet Users, et créez un utilisateur pour l'authentification 802.1x. Sélectionnez +Ajouter :

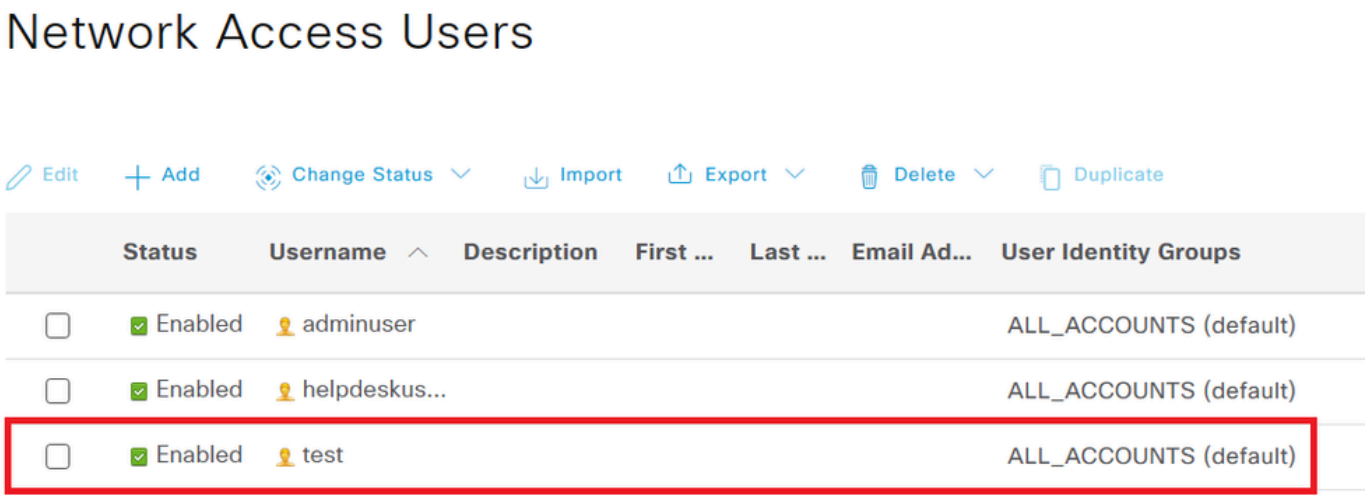


Créez un nom d'utilisateur, le mot de passe (et saisissez le même mot de passe dans le champ Re-Enter Password), puis sélectionnez ALL_ACCOUNTS (par défaut) dans le menu déroulant User Groups (Groupes d'utilisateurs) :

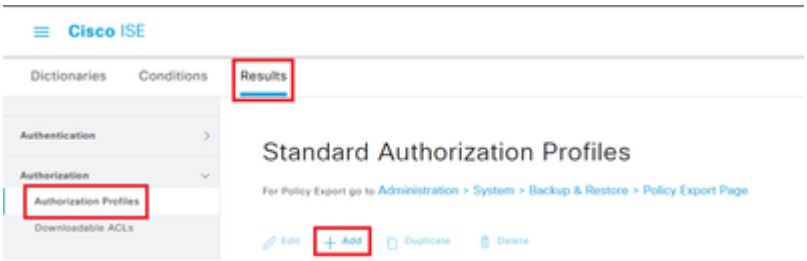


Dans l'angle inférieur droit, cliquez sur Submit.

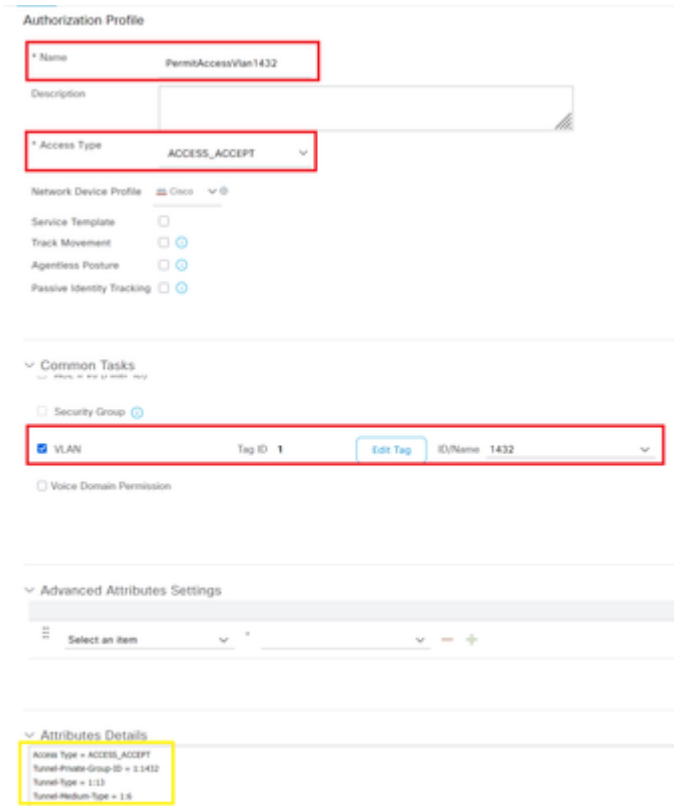
Vous pouvez voir l'utilisateur dans la liste Utilisateurs d'accès au réseau :



Étape 6. Accédez à Policy > Policy Elements > Results. Dans l'onglet Autorisation > Profils d'autorisation, sélectionnez +Ajouter.



Créez le profil d'autorisation pour le VLAN auquel les clients d'authentification locaux sont affectés :

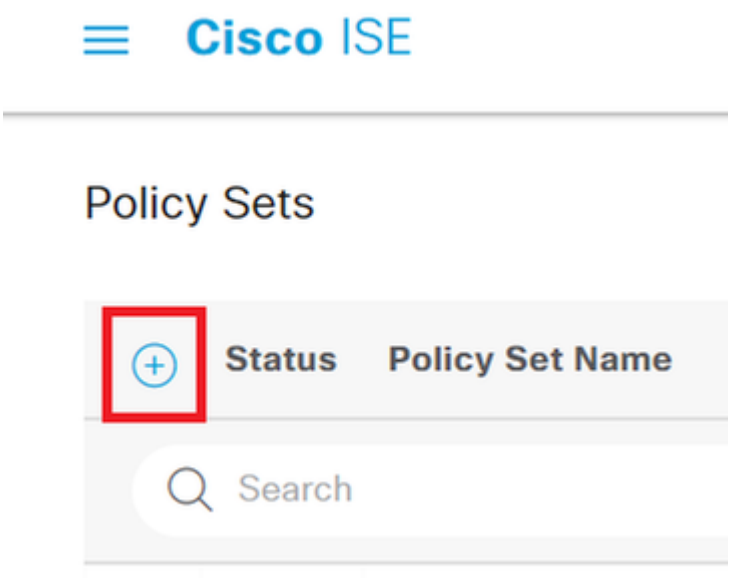


Dans l'angle inférieur droit, cliquez sur Submit.

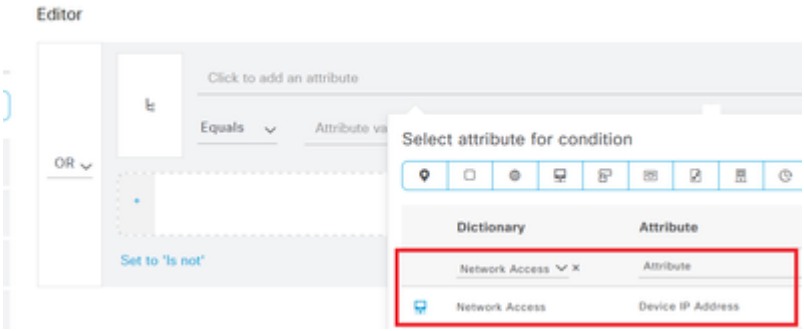
Vous voyez les détails des attributs que l'ISE envoie aux WLC/AP dans un scénario réussi.

Étape 7. Accédez à Policy > Policy Sets. Créez un nouvel ensemble de stratégies.

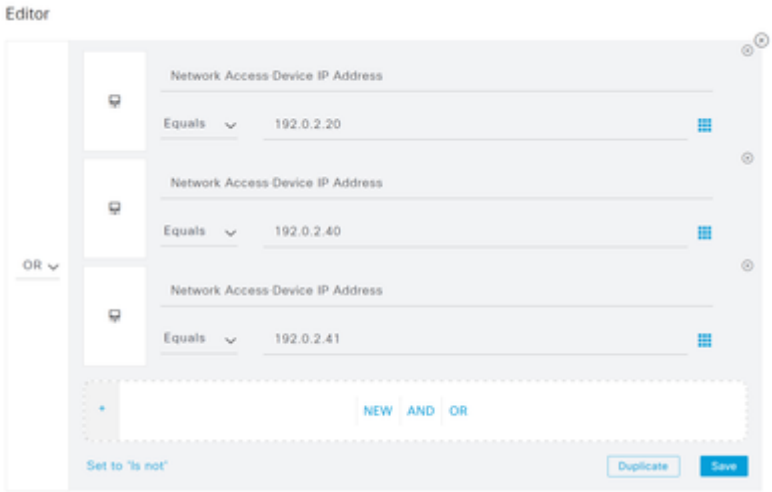
Cliquez sur le signe + :



Attribuez un nom à l'ensemble de stratégies. Dans la colonne Conditions, ajoutez la règle OR et ajoutez le dictionnaire Accès réseau, avec l'attribut Adresse IP du périphérique, sélectionnez Égal à :

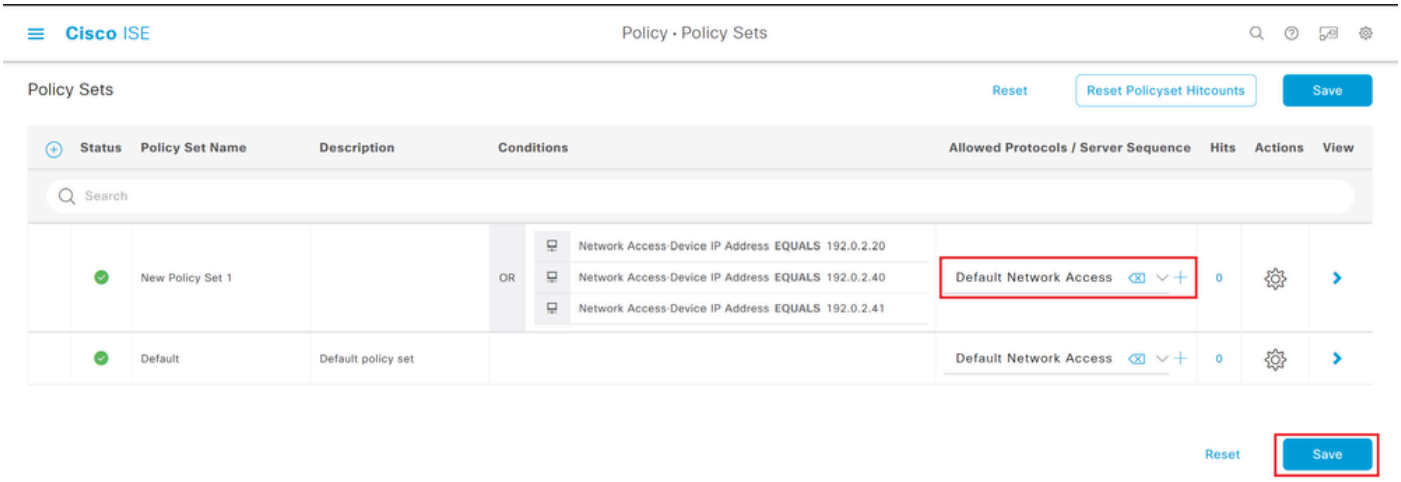


Ajoutez les adresses IP du WLC 9800 et des points d'accès :

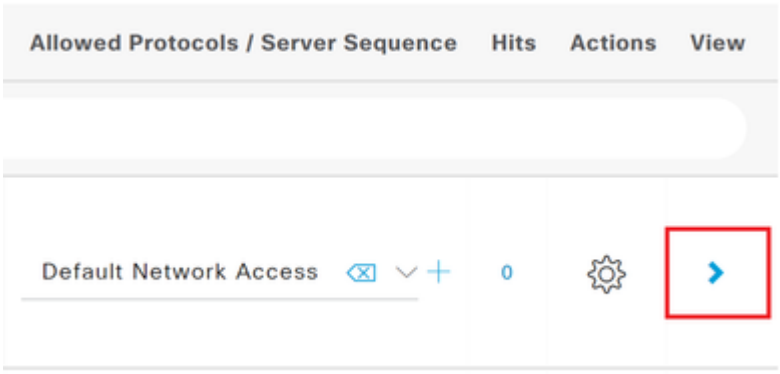


Dans l'angle inférieur droit, cliquez sur Use.

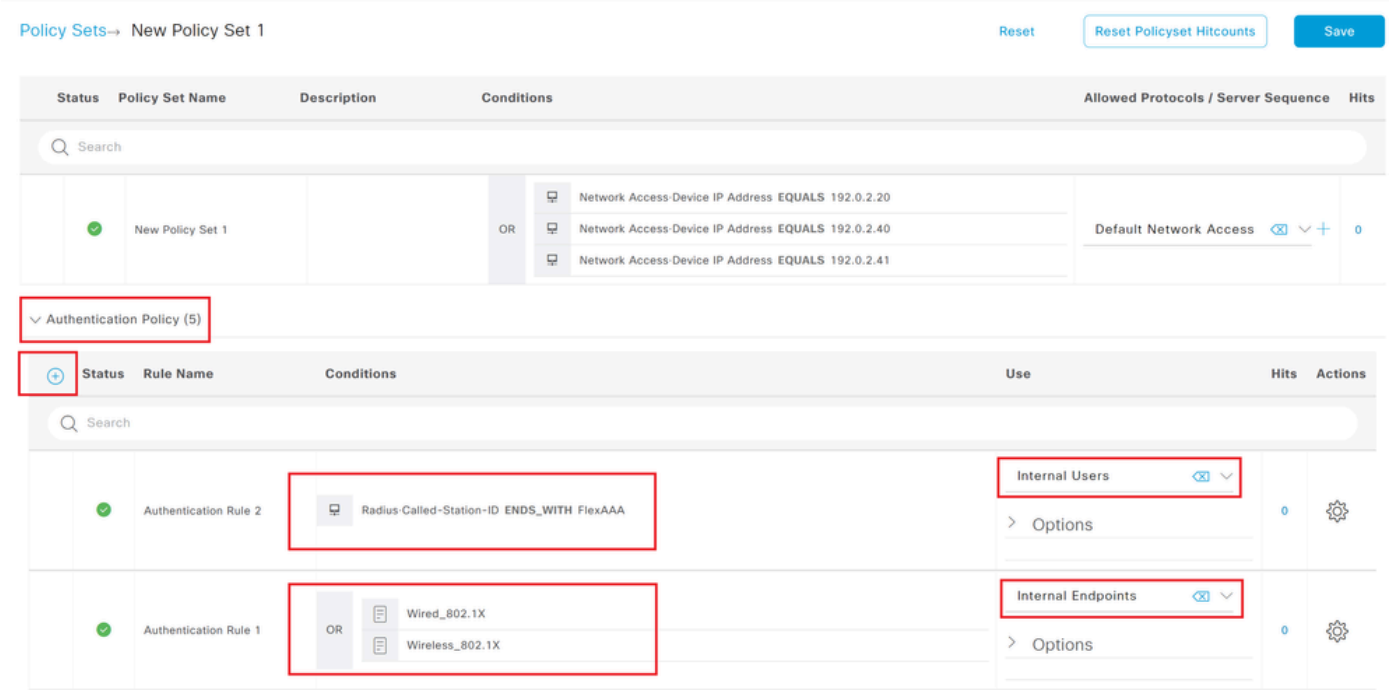
Étape 8. Dans la colonne Protocoles autorisés, sélectionnez Accès réseau par défaut. À la fin, cliquez sur Save:



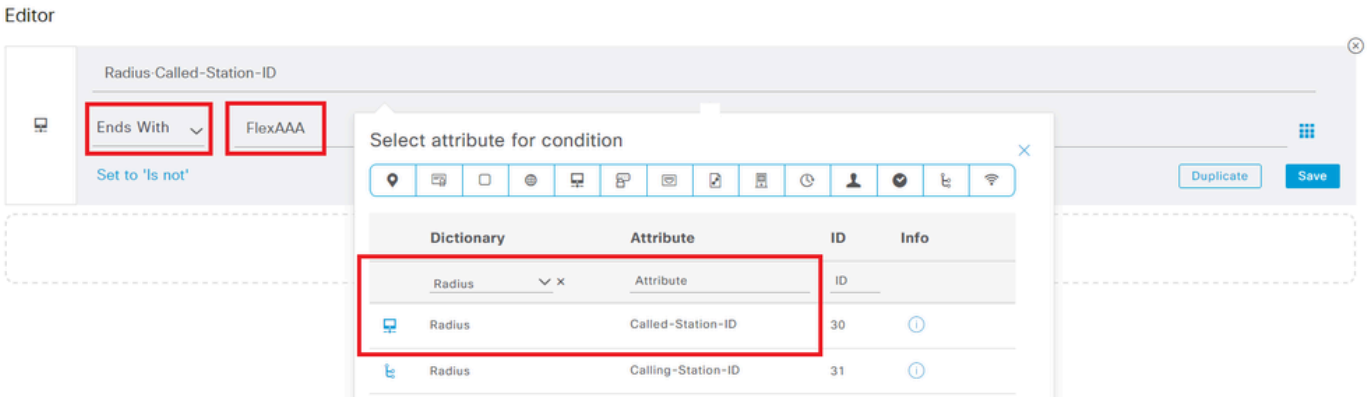
Étape 9. Dans la colonne Vue, cliquez sur le signe fléché :



Étape 10. Développez Authentication Policy, créez deux nouvelles stratégies : l'une pour le nom WLAN, l'autre pour la configuration 802.1X :

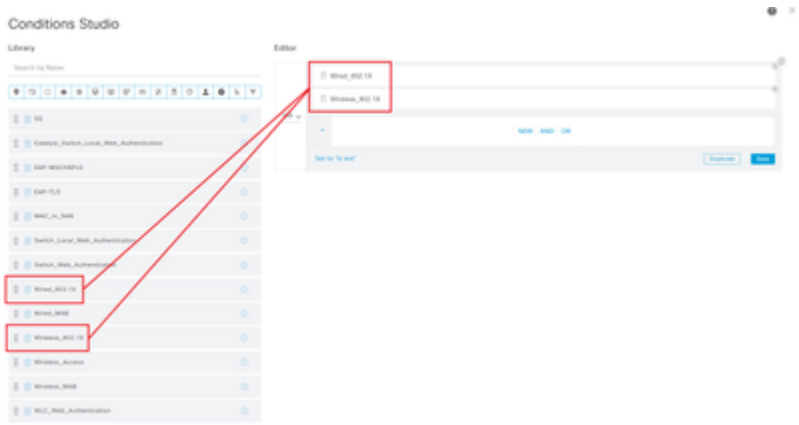


Pour le nom du WLAN, créez la Condition avec le dictionnaire Radius et Attribute Called-Station-ID. Sélectionnez Ends With et tapez le nom du WLAN :



Dans l'angle inférieur droit, cliquez sur Use. Pour cette stratégie, dans la colonne Utiliser, sélectionnez Utilisateurs internes.

Étape 11. Pour la stratégie 802.1X, créez la condition avec la bibliothèque Wired_802.1X et Wireless_802.1X disponible sur ISE. Vous pouvez faire glisser et déposer ces éléments, puis sélectionner la condition OU :



Dans l'angle inférieur droit, cliquez sur Use. Pour cette stratégie, dans la colonne Use, sélectionnez Internal Endpoints.

Étape 12. Faites défiler jusqu'à Authorization Policy et créez une nouvelle stratégie. Donnez-lui un nom et créez la même condition que celle créée pour le nom WLAN sur la politique d'authentification.

Dans la colonne Profiles, sélectionnez dans le menu déroulant le profil PermitAccessVlan1432 :



Dans l'angle inférieur droit, cliquez sur Save.

Configuration du WLAN PSK avec authentification locale

Étape 1. Configurez d'abord les points d'accès en mode Flex, comme décrit dans la section Configurer le mode FlexConnect sur le site distant.

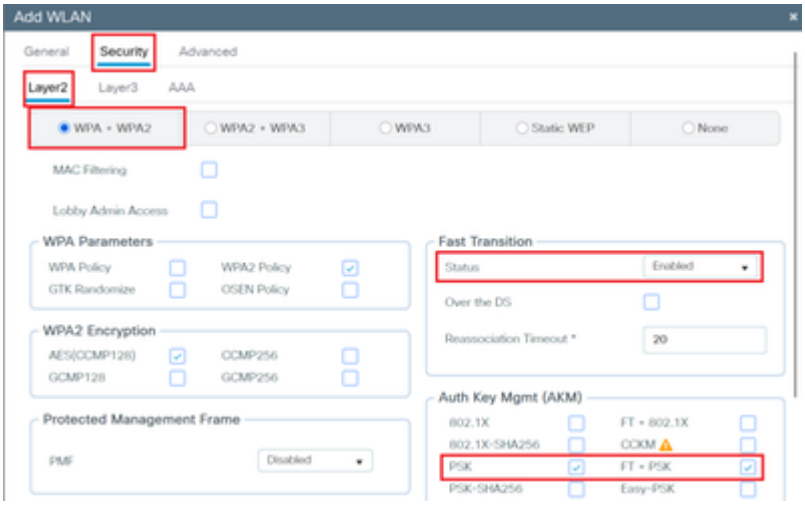
Étape 2 : création du WLAN

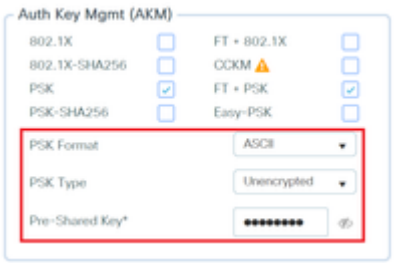
Accédez à Configuration > Tags & Profiles > WLANs, sélectionnez +Add.

Dans la balise General, créez un nom pour le nom de profil, le SSID et l'état enable :



Étape 3. Accédez à Sécurité > Couche 2 onglet sélectionnez WPA+WPA2, Transition rapide comme activé, Auth Key Mgmt PSK et FT+PSK, choisissez le format PSK et le type PSK que vous voulez, et tapez la clé pré-partagée que vous voulez que vos clients utilisent :





Cliquez sur Update & Apply to Device.

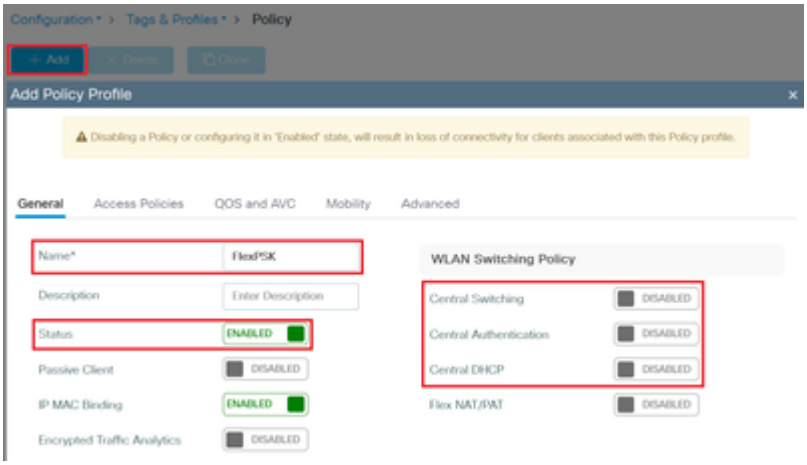
Vous pouvez voir le WLAN créé :



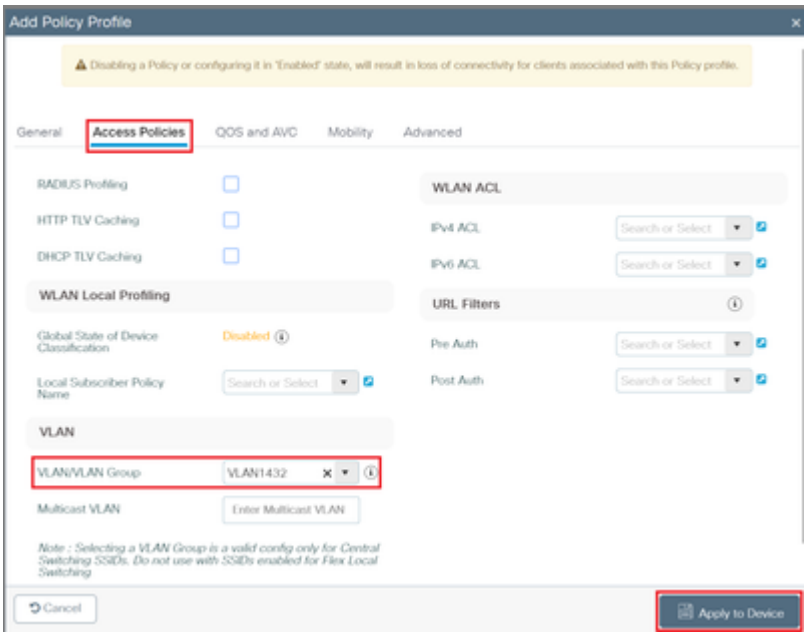
Étape 4 : création du profil de stratégie

Accédez à Configuration > Tags & Profiles > Policy.

Sélectionnez +Add et, dans l'onglet General, attribuez un nom au profil de stratégie, activez l'état et désactivez la commutation centrale, l'authentification centrale et le DHCP central :

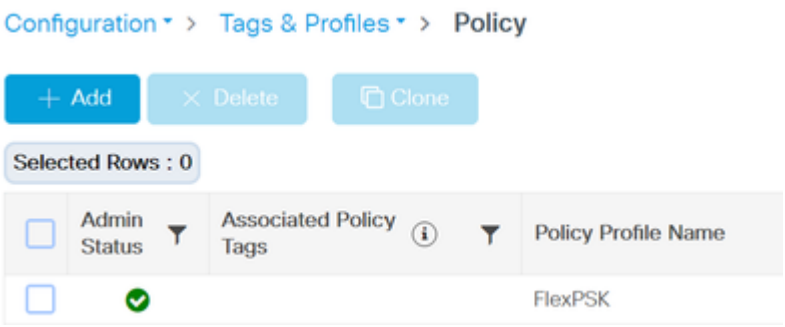


Étape 5. Accédez à l'onglet Access Policies, sélectionnez le VLAN :



Cliquez sur Update & Apply to Device.

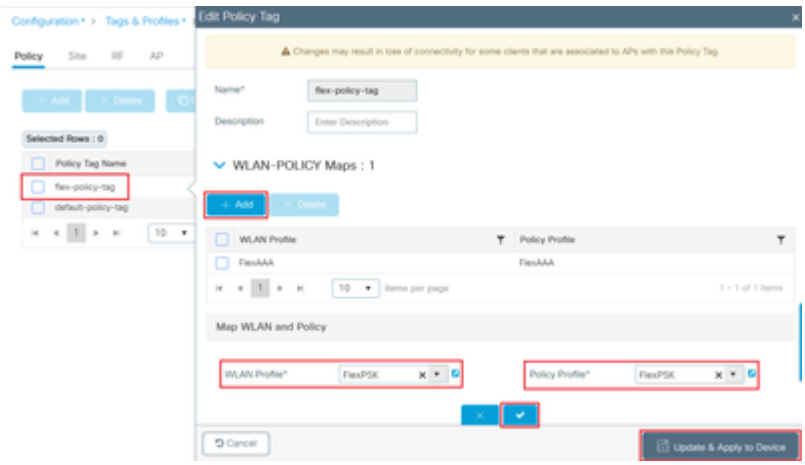
Vous pouvez voir le profil de stratégie dans la liste :



Étape 6. Vous pouvez créer une nouvelle balise de stratégie ou modifier la balise existante.

Accédez à Configuration > Tags & Profiles > Tags pour modifier la balise de stratégie existante. Sélectionnez la balise à modifier.

Sélectionnez +Add sous WLAN-POLICY Maps. Dans Profil WLAN, sélectionnez le WLAN précédemment créé dans le menu déroulant. Dans Profil de stratégie, sélectionnez le profil de stratégie précédemment créé dans le menu déroulant. Cliquez sur le bouton de vérification, puis sur Apply to Device :



Si la balise de stratégie est déjà assignée sur l'AP, vous n'avez pas besoin de faire autre chose.

Si ce n'est pas le cas, attribuez la balise de stratégie sur la balise AP. Accédez à Configuration > Wireless > Access Points. Sélectionnez le point d'accès pour modifier la balise de stratégie, puis cliquez sur « Mettre à jour et appliquer au périphérique ».

Le point d'accès se sépare et se joint à nouveau avec la nouvelle balise de stratégie.

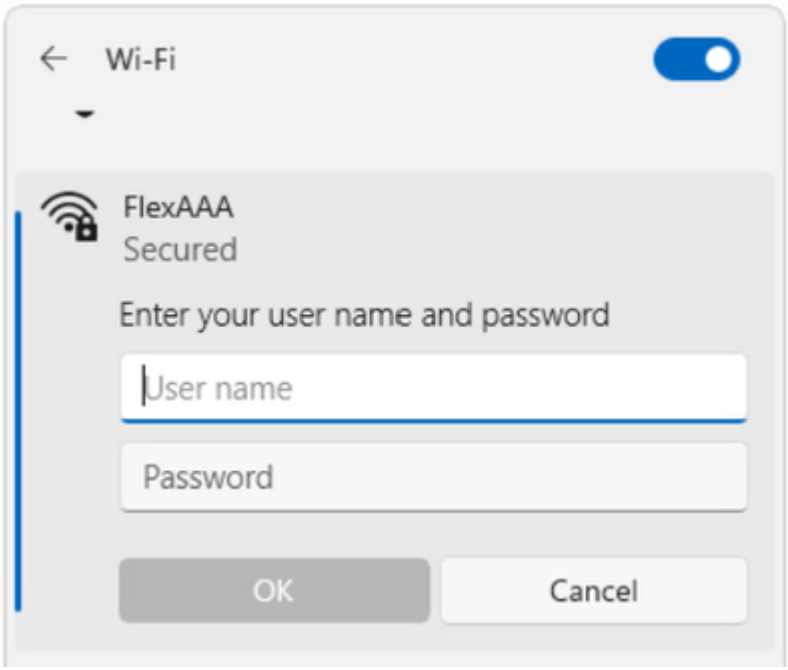
Lorsque le point d'accès se reconnecte, vous pouvez vérifier la liste des points d'accès, confirmer que le point d'accès est en mode flexible et qu'il a les balises assignées correctes.

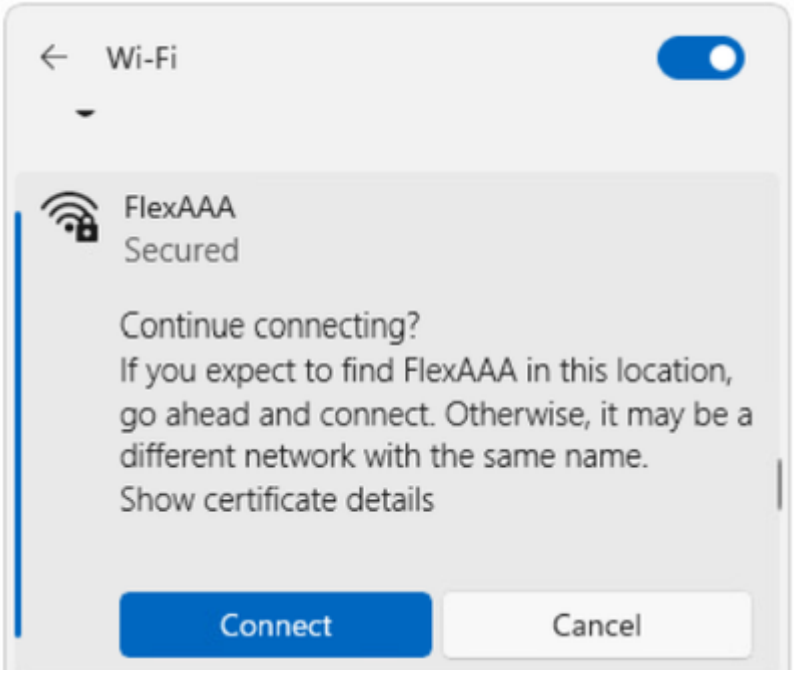
CLI :

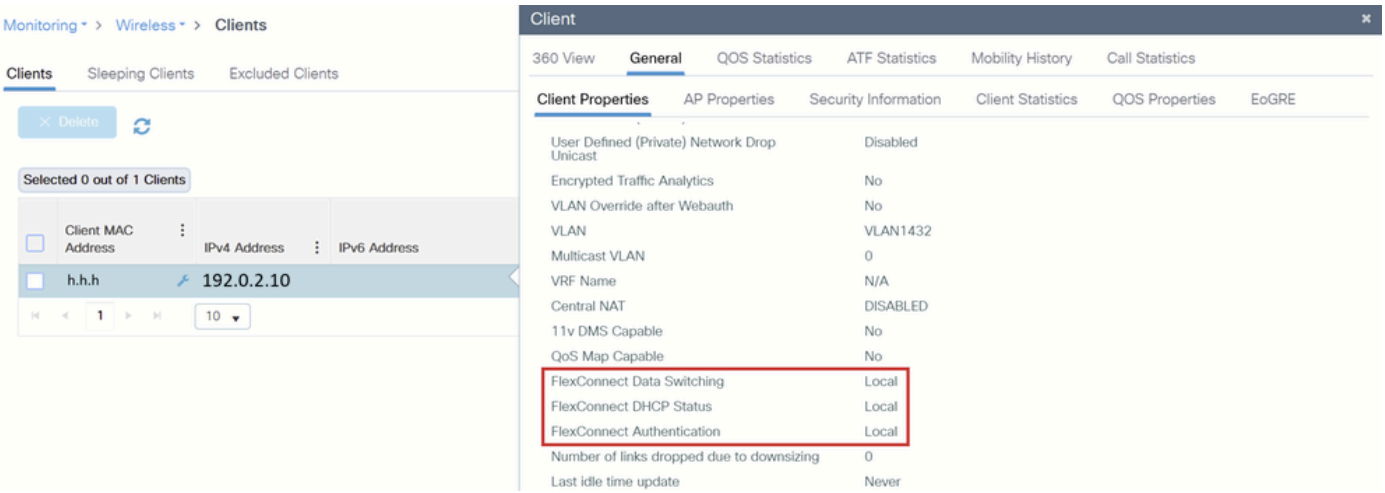
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Vérifier

Pour le WLAN 802.1x :


Wi-Fi
FlexAAA
Secured
Enter your user name and password
User name
Password
OK
Cancel


Wi-Fi
FlexAAA
Secured
Continue connecting?
If you expect to find FlexAAA in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details
Connect
Cancel


Monitoring > Wireless > Clients
Clients
Sleeping Clients
Excluded Clients
Delete
Selected 0 out of 1 Clients
Client MAC Address
IPv4 Address
IPv6 Address
h.h.h
192.0.2.10
1
10
Client
360 View
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
Client Properties
AP Properties
Security Information
Client Statistics
QOS Properties
EoGRE
User Defined (Private) Network Drop Unicast
Disabled
Encrypted Traffic Analytics
No
VLAN Override after Webauth
No
VLAN
VLAN1432
Multicast VLAN
0
VRF Name
N/A
Central NAT
DISABLED
11v DMS Capable
No
QoS Map Capable
No
FlexConnect Data Switching
Local
FlexConnect DHCP Status
Local
FlexConnect Authentication
Local
Number of links dropped due to downsizing
0
Last idle time update
Never

CLI :

```
C9800-1#show wireless client mac-address      h.h.h        detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

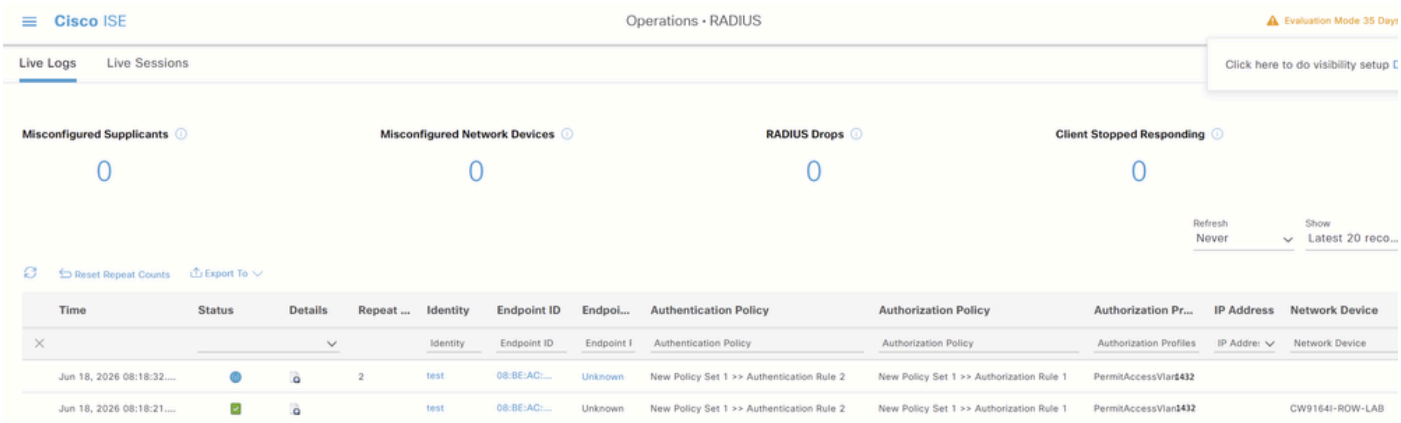
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

Sur l'interface CLI AP :

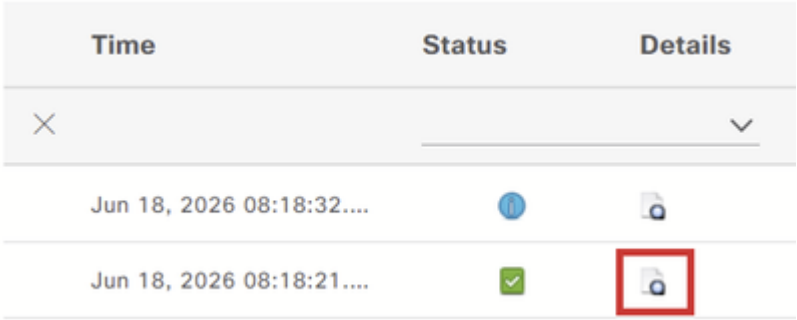
```
CW9164I-ROW-LAB#show dot11 clients

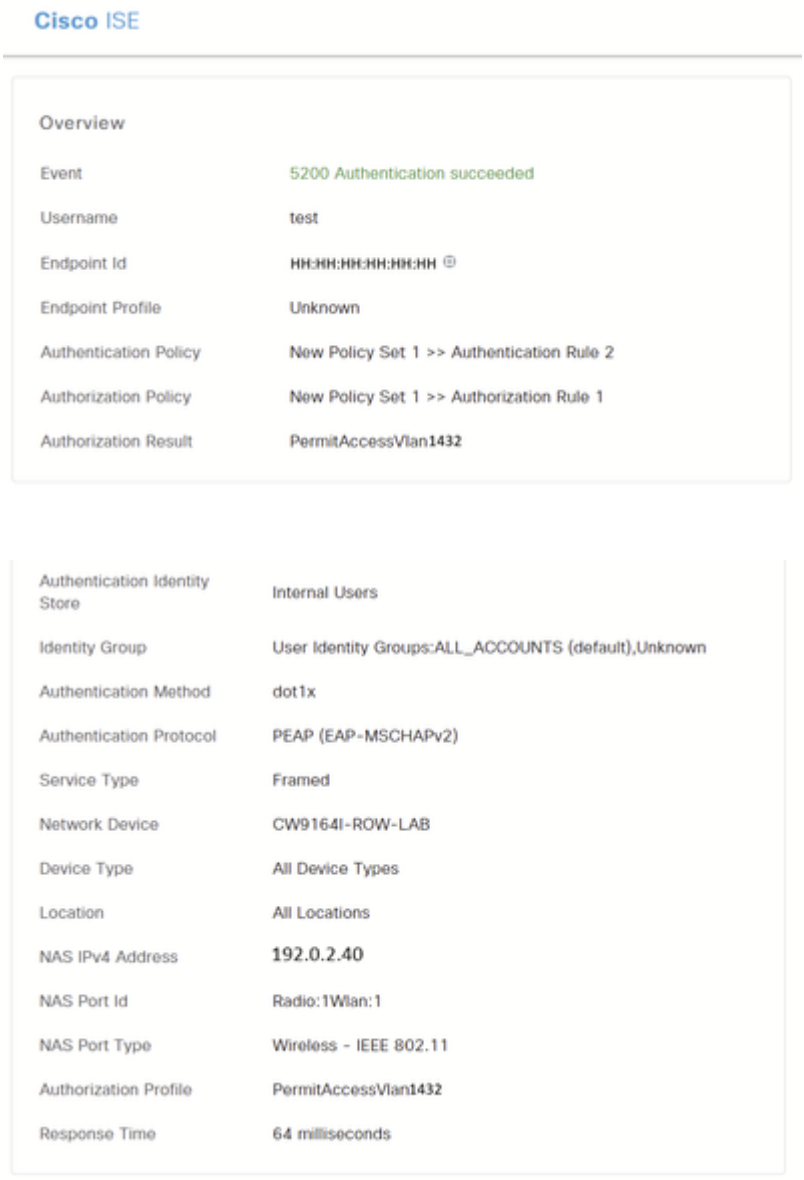
Total dot11 clients: 1
      Client MAC    Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH           1       1  33   FlexAAA  -45 MCS9ISS           No         No
```

Sur ISE

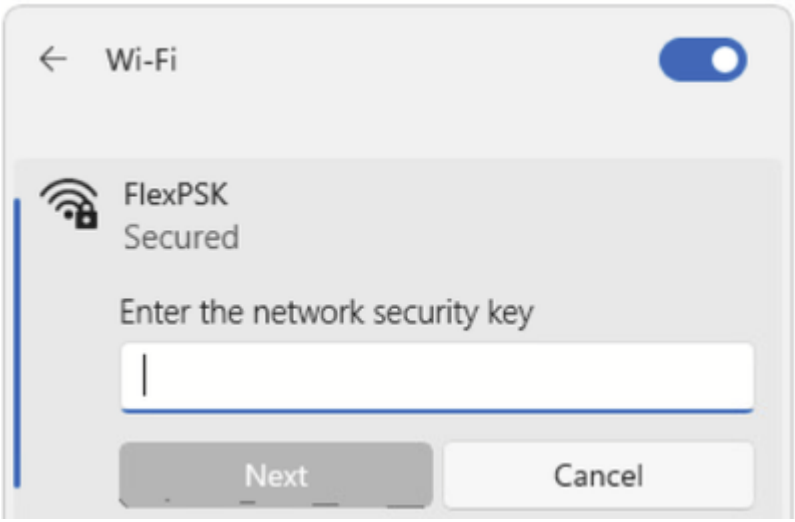


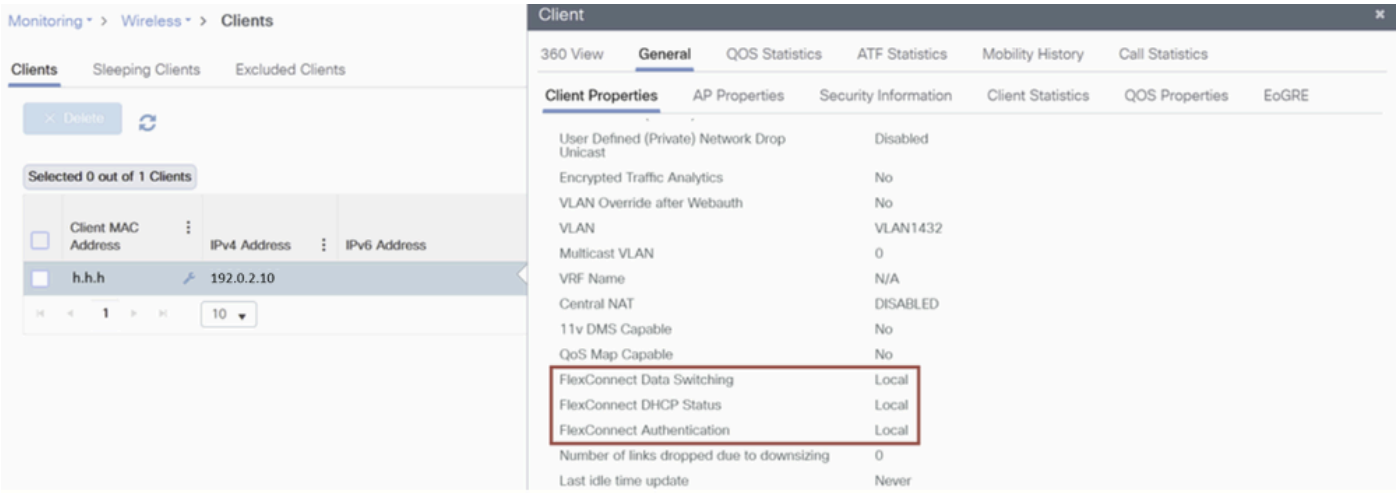
IP Address	Network Device	Device Port	Identity Group	Posture ...	Server
IP Addre:	Network Device	Device Port	Identity Group	Posture Sta	Server
		Radio:1Wlan:1			ISE1
	CW9164I-ROW-LAB	Radio:1Wlan:1	User Identity Groups:ALL_ACCOUNTS (default),Unknown		ISE1





Pour WLAN PSK :





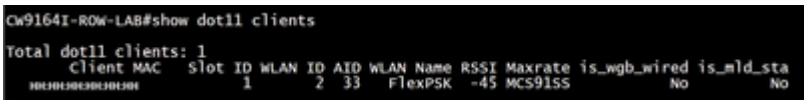
CLI :

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

Sur AP CLI :



Dépannage

Activez les débogages AP et RA trace avec l'adresse MAC du client, en synchronisation.

Sur l'AP, activez ces débogages :

debug flexconnect event
debug flexconnect pmk
debug flexconnect dot11r
debug dot11 client management information
debug dot11 client management critical
debug dot11 client management errors
debug dot11 client management events

Pour le WLAN 802.1x :

Les journaux de débogage AP avec authentification réussie :

Le point d'accès gère la gestion de la machine d'état 802.11 et des clés locales.
Le point d'accès traite l'association et prépare le client pour l'authentification.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

Le point d'accès traite l'autorisation, applique la priorité VLAN et fait passer le client à l'état FWD (Forwarding).

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
```

```
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

Journaux de suivi RA pour la même authentification réussie :

La trace RA enregistre l'orchestration de la session par le WLC. Le WLC valide l'identité et la stratégie du client.
WLC reconnaît l'association FlexConnect.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

Le WLC transmet la stratégie au point d'accès.

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

Autorisation réussie.

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

Paramètres du client.
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1} : [point11] [18318] : (remarque) : MAC :

hhhh.hhhh.hhh Paramètres d'entrée du chemin de données du client - ssid : FlexAAA, slot_id : 1 bssid ifid : 0x0, id_radio : 0x90400008, id_wlan : 0xf0400004

Le WLC apprend l'IP via DHCP/ARP local.
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1} : [client-iplearn] [18318] : (remarque) : MAC : hhhh.hhhh.hhhh L'apprentissage de l'adresse IP du client a réussi. Méthode : IP Snooping IP : 192.0.2.10

Le client est entièrement connecté.
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1} : [errmsg] [18318] : (info) : %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE : R0/1: wncd : Entrée de nom d'utilisateur (test) associée au ssid (FlexAAA) pour le périphérique avec MAC : hhhh.hhhh.hhhh sur le canal (48)
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1} : [client-orch-state] [18318] : (remarque) : MAC : hhhh.hhhh.hhhh Transition d'état du client : S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

Scénario autonome

Comportement lors de la perte de connectivité AP-WLC et récupération ultérieure.

L'AP est joint au WLC. Le client effectue une authentification 802.1X réussie, et le point d'accès fait passer le client à l'état FWD (Forwarding).

Sur les journaux en direct ISE RADIUS, nous voyons la session client.

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

Le point d'accès n'atteint pas le WLC, épuise son nombre de retransmissions et passe en mode autonome. Les clients existants restent connectés localement.

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
```

```
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

Mais le client est toujours connecté :

CW9164I-ROW-LAB2#show dot11 clients

Nombre total de clients dot11 : 1
ID de logement MAC client ID WLAN AID Nom WLAN RSSI Max rate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 Non Non

Lorsque le client se déplace vers un autre point d'accès en mode autonome, la connexion EAP échoue en raison de l'impossibilité d'atteindre le serveur RADIUS. Le client n'est plus autorisé et est supprimé du point d'accès.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

Le point d’accès envoie la session client au serveur RADIUS de sauvegarde.

Le point d'accès retrouve la connectivité au WLC. Le point d'accès repasse en mode connecté et synchronise les informations de session du client local avec le WLC.

La session client passe entre les noeuds ISE principal et de secours en fonction de l'état de connectivité du point d'accès.

Le point d'accès et le client apparaissent comme connectés sur le WLC, et le client n'a pas

remarqué de déconnexions ou de battement lorsque la connectivité entre le point d'accès et le WLC était en panne.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, ma
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASS
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No

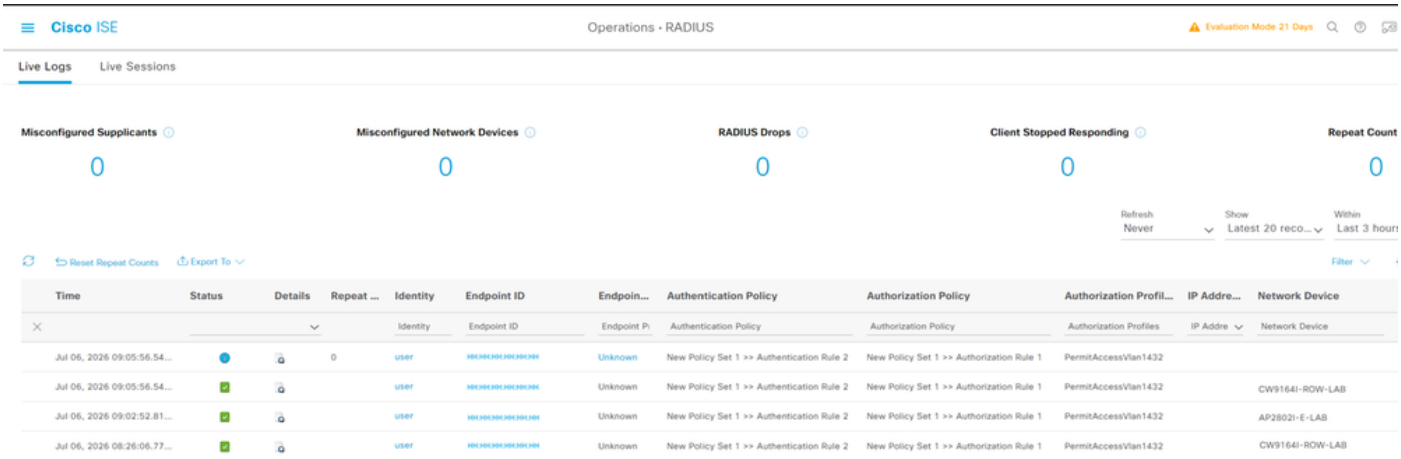


*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
```

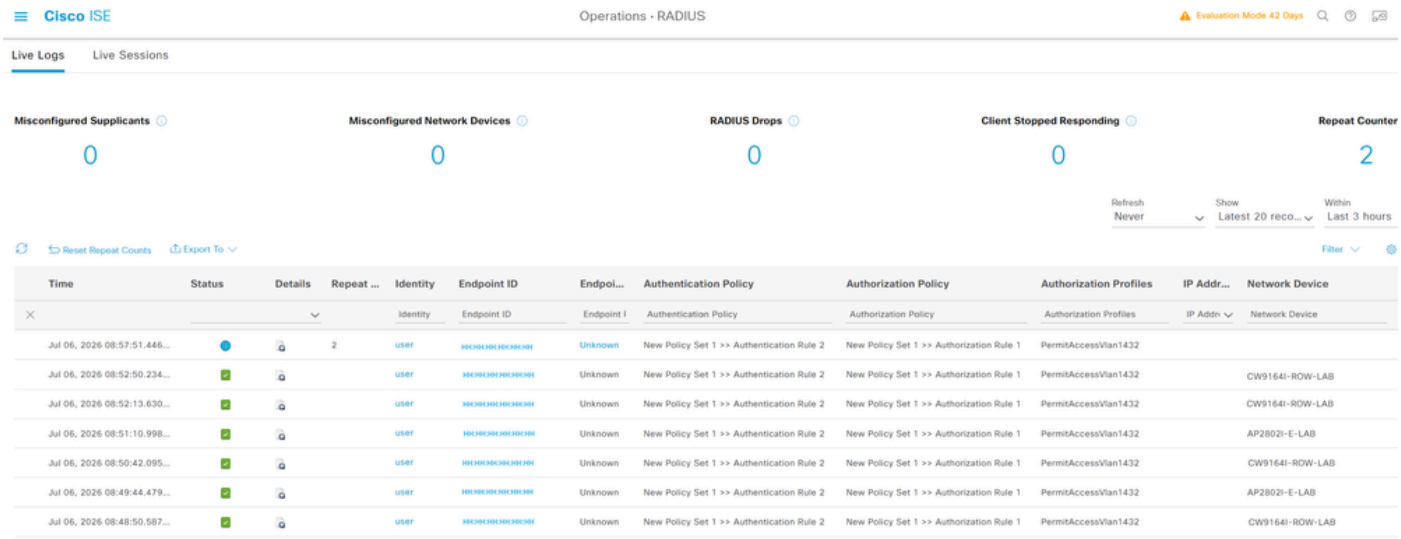
```
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
```

```
CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



ISE principal : Enregistre la session initiale (08:26:06) et la session reprise après la restauration de la connectivité WLC (09:02:52).



Sauvegarde ISE : Capture l'activité de session (08:48:50 - 08:57:51) pendant que le point d'accès fonctionnait en mode autonome.

La première session a eu lieu à 08:26:06, après quoi l'AP a perdu la connectivité au WLC et est passé en mode autonome.

La session 09:02:52 est la première session après qu'AP a rétabli la connectivité avec le WLC.

Informations connexes

- CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, 2nd Edition
- Guide de configuration du logiciel du contrôleur sans fil de la gamme Cisco Catalyst 9800, Cisco IOS XE 17.8.x - Chapitre : FlexConnect
- Notes de version du contrôleur sans fil Cisco Catalyst 9800, Cisco IOS XE Cupertino version 17.8.x
- Matrice de fonctionnalités des points d'accès sans fil Cisco
- Assistance technique de Cisco et téléchargements

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.