Configuration de la position sur les WLC et ISE Catalyst 9800

Table des matières

Introduction

Ce document décrit comment configurer un WLAN de posture sur un WLC et ISE Catalyst 9800 via l'interface graphique utilisateur (GUI).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration générale du WLC 9800
- Configuration des profils et des politiques ISE

Composants utilisés

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

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- Identity Service Engine (ISE) v3.2
- Ordinateur portable Windows 10 Entreprise

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 fonctionnalités RADIUS NAC et CoA du contrôleur LAN sans fil

1. Le client s'authentifie en utilisant l'authentification dot1x.

2. RADIUS Access Accept transporte l'URL redirigée pour le port 80 et les ACL de pré-authentification qui inclut l'autorisation des adresses IP et des ports, ou le VLAN de quarantaine.

3. Le client est redirigé vers l'URL fournie dans access accept, et placé dans un nouvel état jusqu'à ce que la validation de position soit effectuée. Le client dans cet état parle au serveur ISE et se valide par rapport aux stratégies configurées sur le serveur NAC ISE.

4. L’agent NAC sur le client lance la validation de position (trafic vers le port 80) : L'agent envoie une requête de détection HTTP au port 80, que le contrôleur redirige vers l'URL fournie dans access accept. L’ISE sait que le client tente d’atteindre et répond directement au client. De cette façon, le client apprend l'adresse IP du serveur ISE et, à partir de maintenant, le client communique directement avec le serveur ISE.

5. Le WLC autorise ce trafic, car la liste de contrôle d’accès est configurée pour autoriser ce trafic. En cas de remplacement du VLAN, le trafic est ponté de manière à atteindre le serveur ISE.

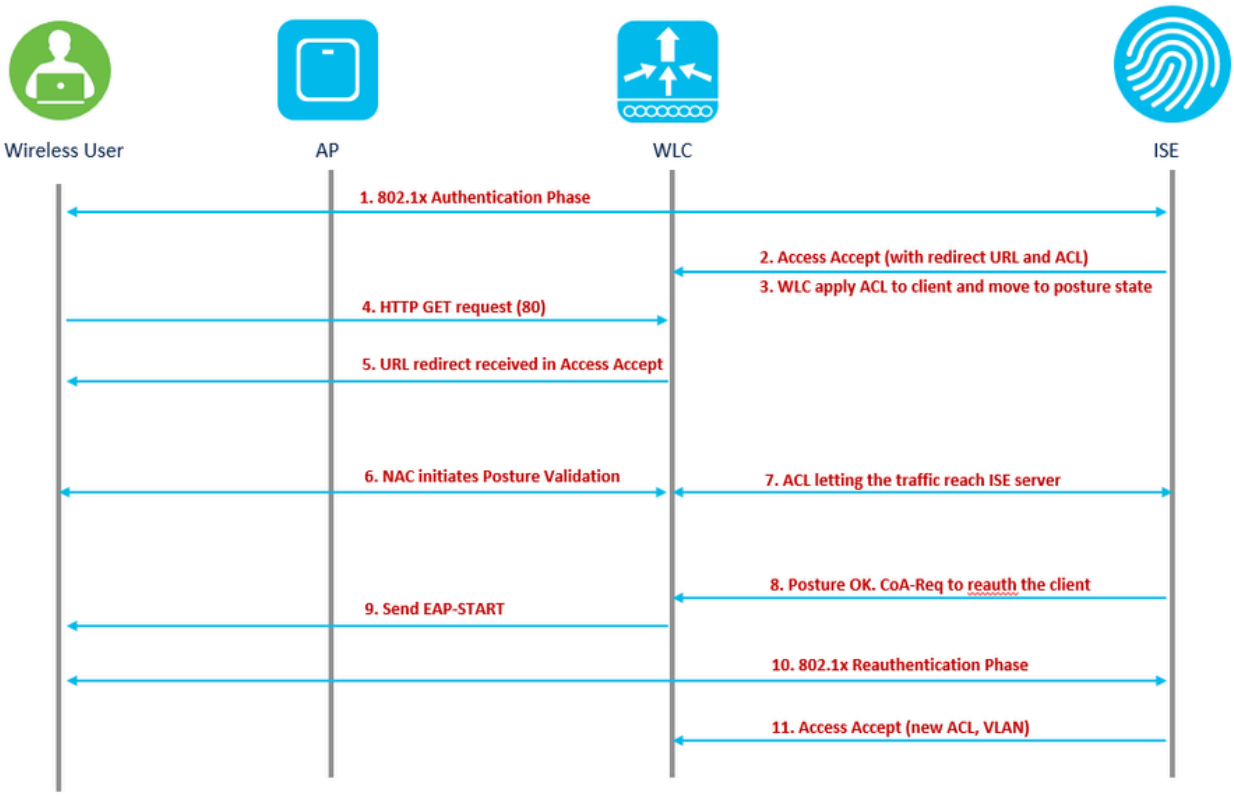
6. Une fois que le client ISE a terminé l’évaluation, une demande de CoA RADIUS avec service de réauthentification est envoyée au WLC. Ceci lance la ré-authentification du client (en envoyant EAP-START). Une fois la réauthentification réussie, l'ISE envoie l'acceptation d'accès avec une nouvelle liste de contrôle d'accès (le cas échéant) et aucune redirection d'URL, ou VLAN d'accès.

7. Le WLC prend en charge CoA-Req et Disconnect-Req conformément à la RFC 3576. Le WLC doit prendre en charge CoA-Req pour le service de ré-authentification, conformément à la RFC 5176.

8. Au lieu de listes de contrôle d’accès téléchargeables, des listes de contrôle d’accès préconfigurées sont utilisées sur le WLC. Le serveur ISE envoie simplement le nom de la liste de contrôle d'accès, qui est déjà configurée dans le contrôleur.

9. Cette conception fonctionne à la fois pour les VLAN et les ACL. Dans le cas d'une substitution de VLAN, nous redirigeons simplement le port 80 qui est redirigé et autorise (le pont) le reste du trafic sur le VLAN de quarantaine. Pour la liste de contrôle d’accès, la liste de contrôle d’accès de pré-authentification reçue dans access accept est appliquée.

Cette image fournit une représentation visuelle de ce flux de fonctionnalités :



workflow de fonction

Pour cet exemple d'utilisation, un SSID utilisé uniquement pour les utilisateurs d'entreprise est activé pour la position. Aucun autre cas d'utilisation, tel que BYOD, Invité ou tout autre, n'existe sur ce SSID.

Lorsqu'un client sans fil se connecte au SSID de posture pour la première fois, il doit télécharger et installer le module de posture sur le portail redirigé de l'ISE, puis l'appliquer avec les listes de contrôle d'accès appropriées en fonction du résultat du contrôle de posture (conforme/non conforme).

Configurer

Diagramme du réseau

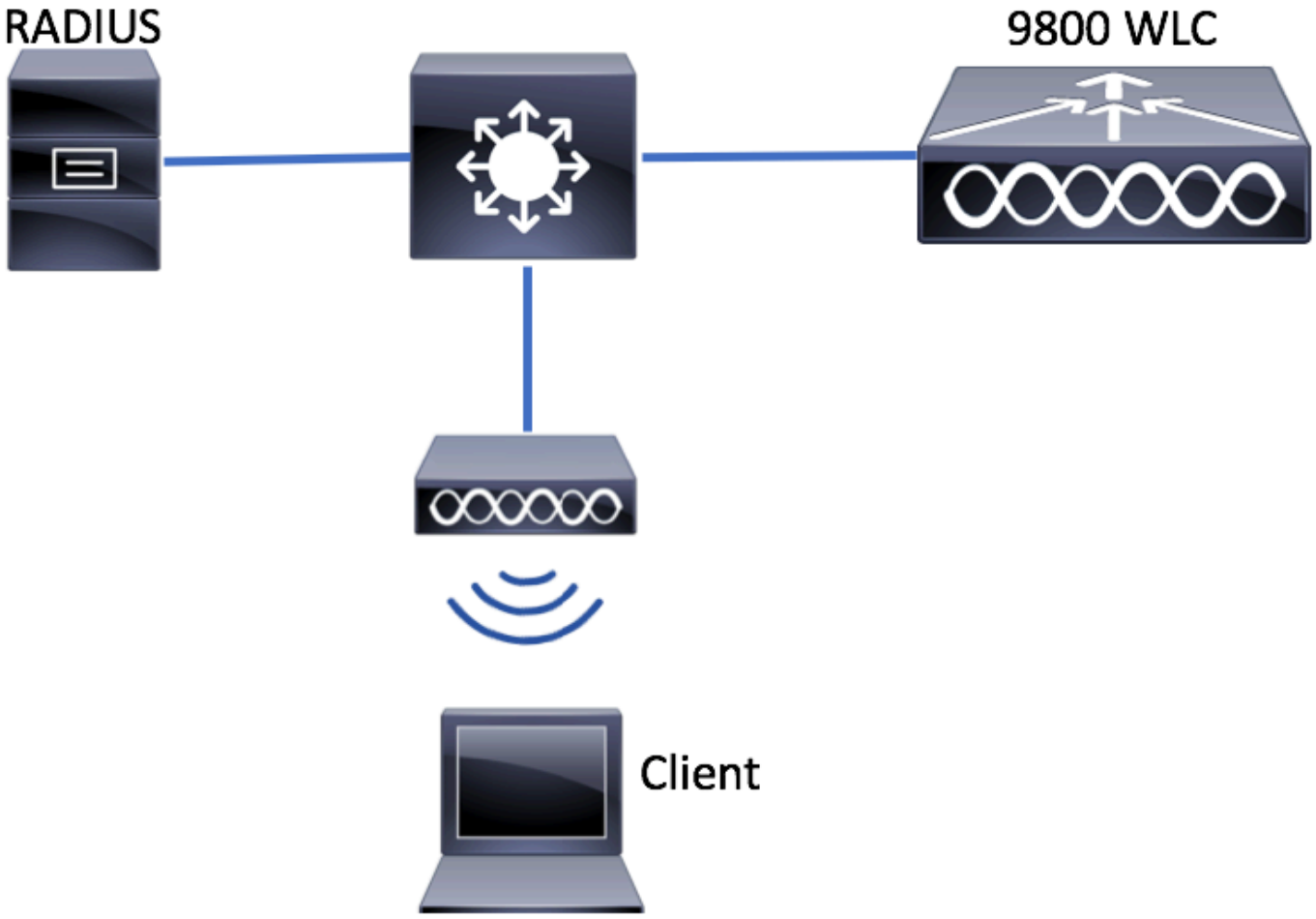
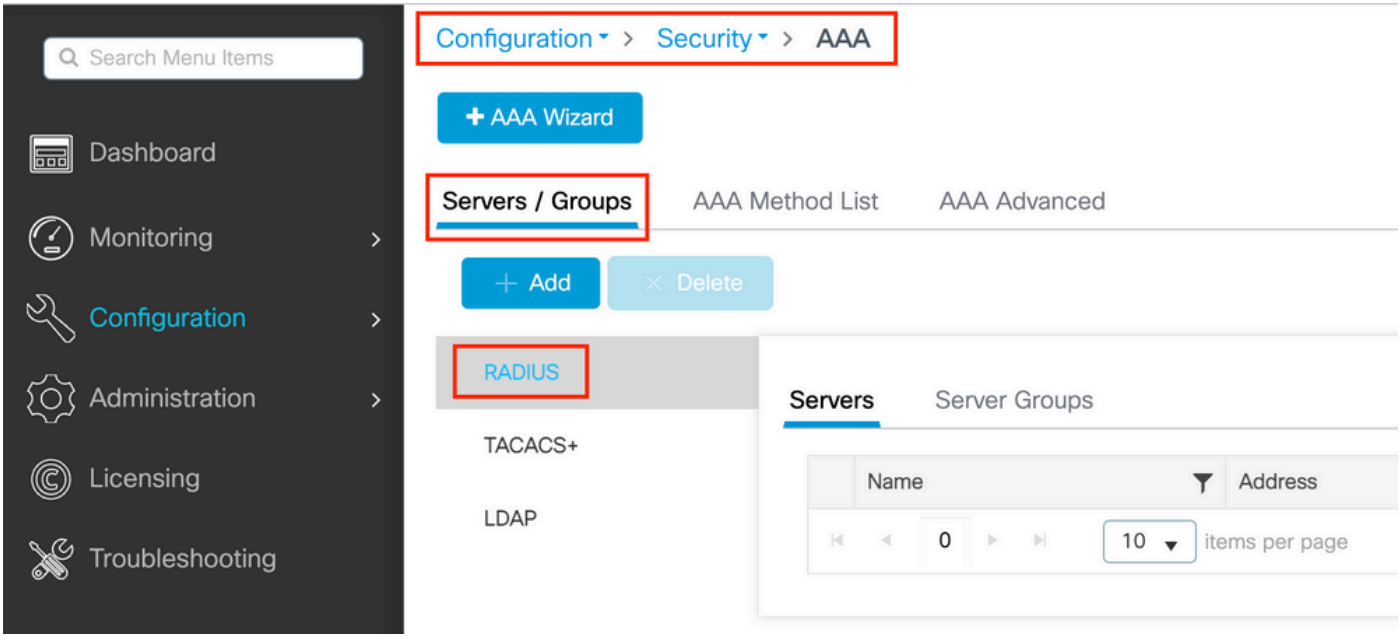


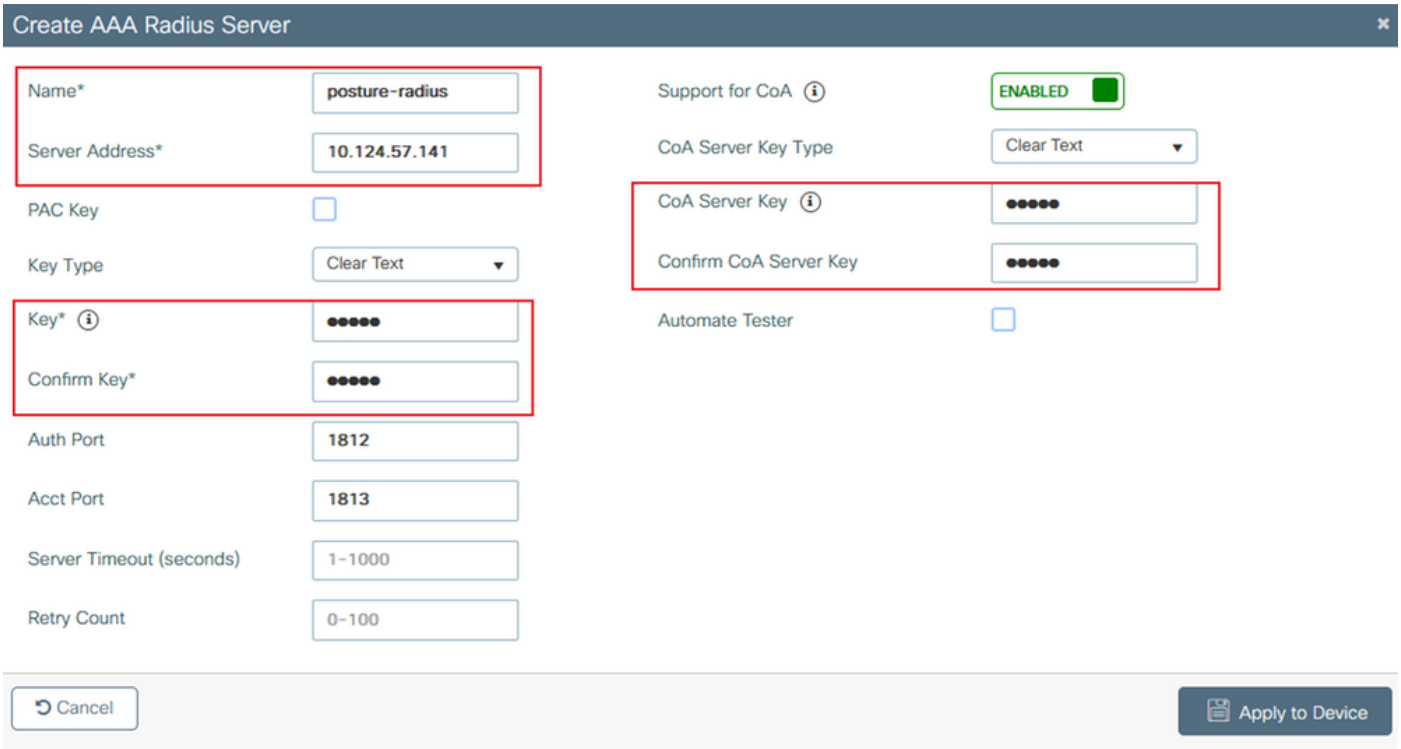
Diagramme du réseau

Configuration AAA sur un contrôleur WLC 9800

Étape 1 : ajout du serveur ISE à la configuration du WLC 9800 Accédez à Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add et entrez les informations du serveur RADIUS comme indiqué dans les images. Assurez-vous que la prise en charge CoA est activée pour NAC de posture.

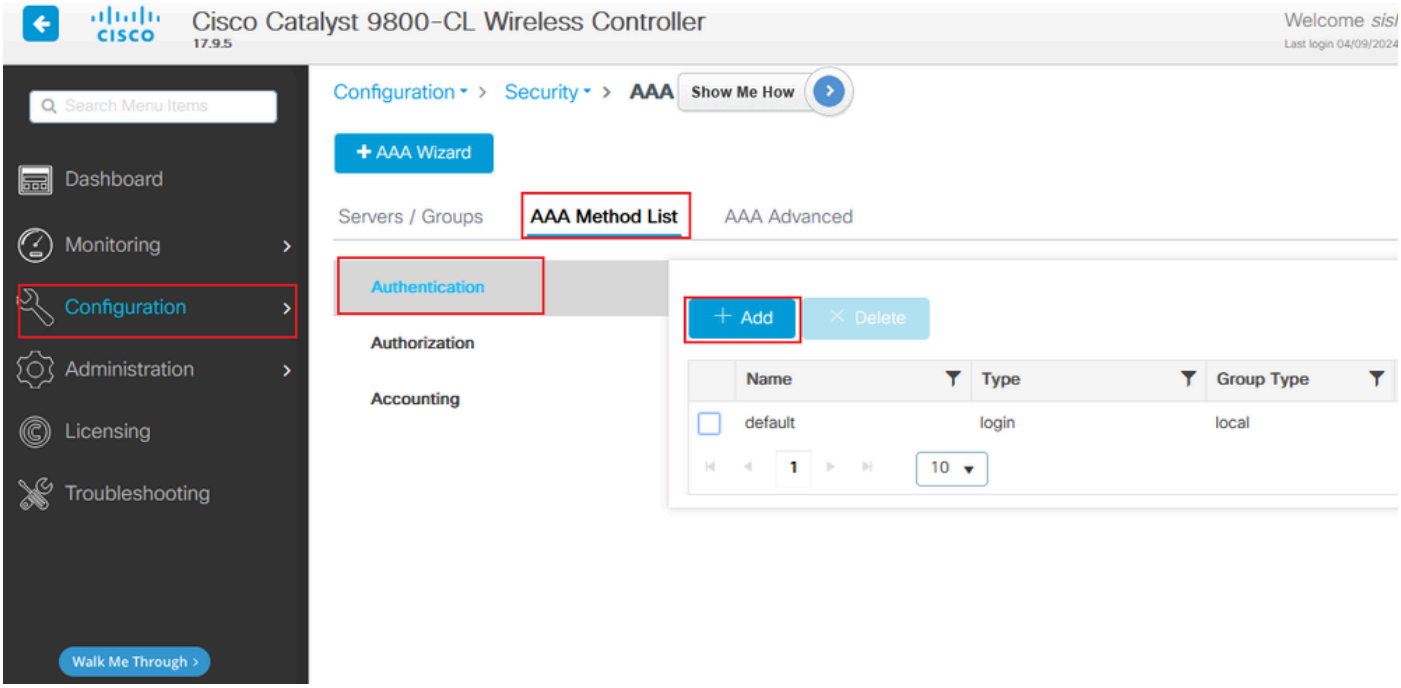


9800 créer un serveur radius

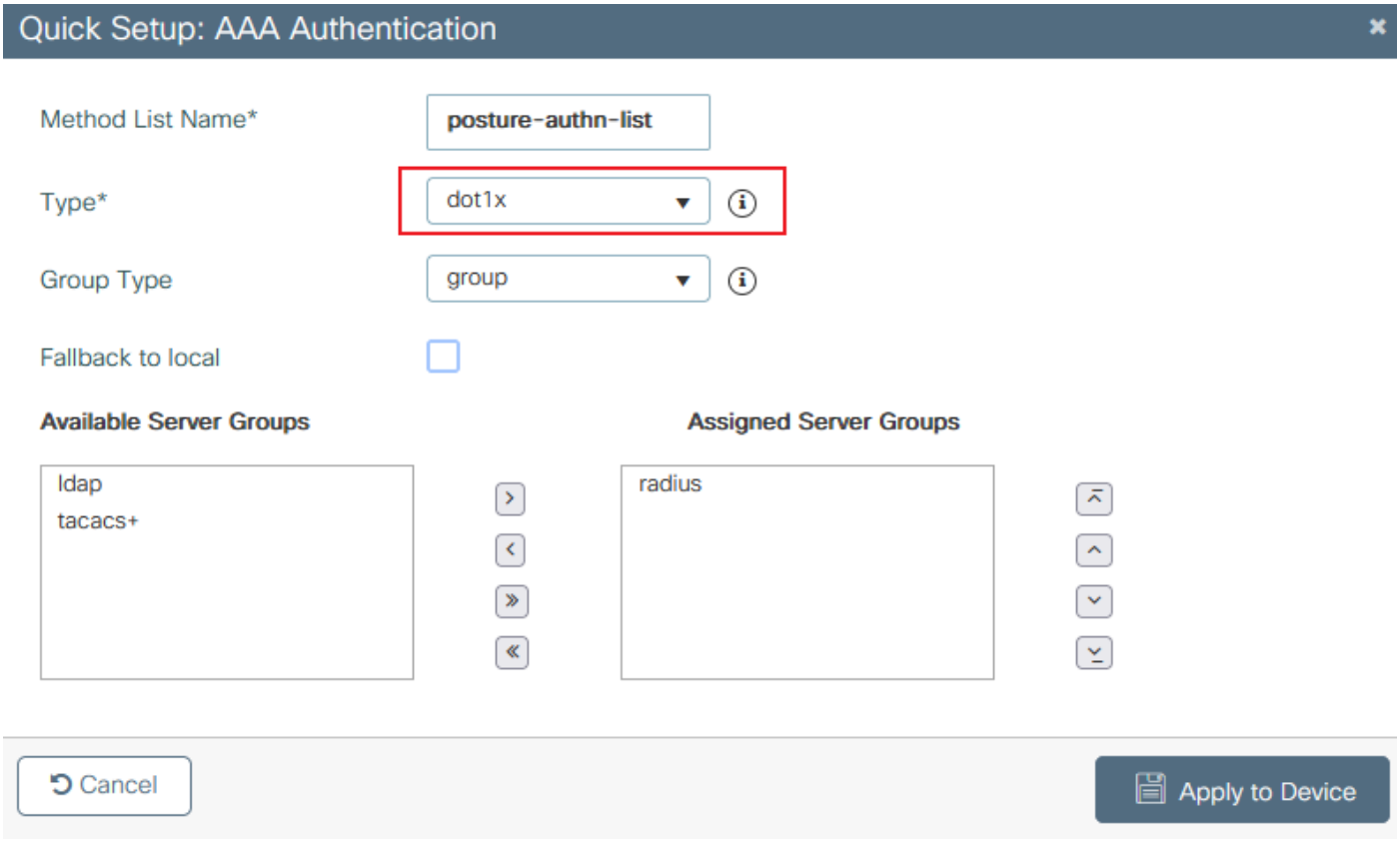


9800 créer les détails du rayon

Étape 2 : création d'une liste de méthodes d'authentification Accédez à Configuration > Security > AAA > AAA Method List > Authentication > + Add comme indiqué dans l'image :

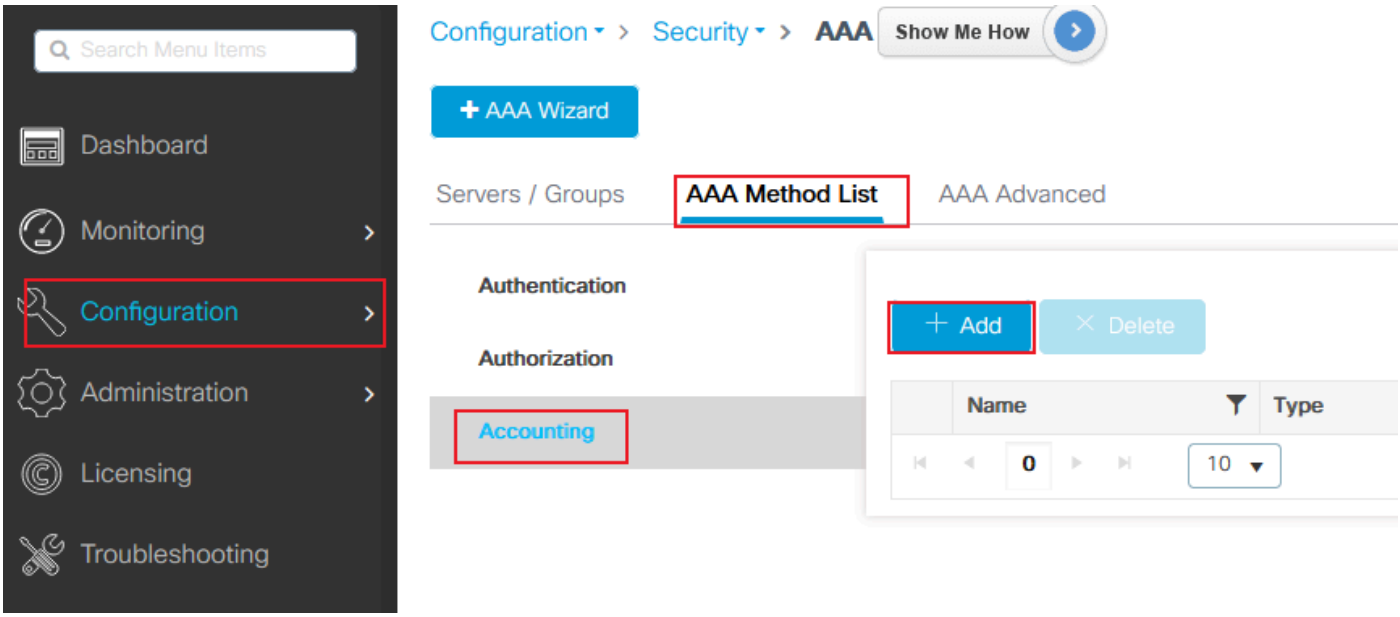


9800 ajouter une liste d'authentification

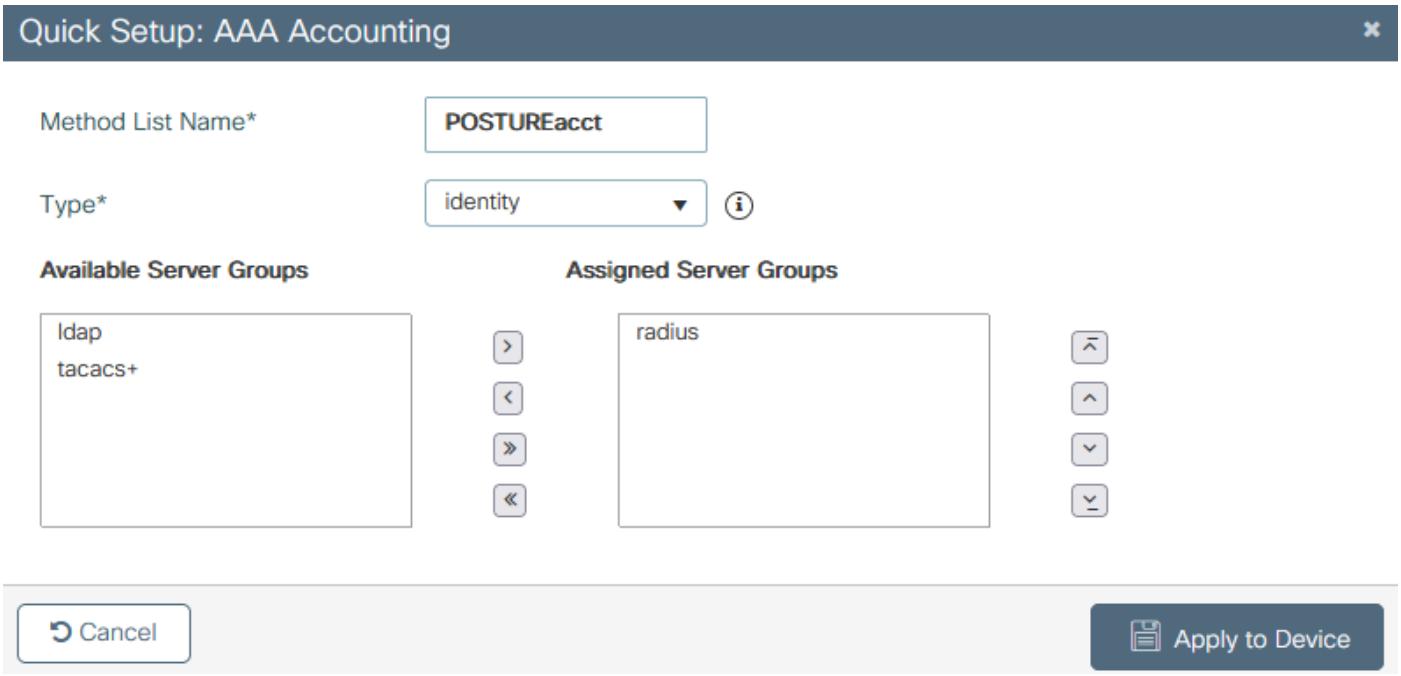


9800 créer les détails de la liste d'authentification

Étape 3. (Facultatif) Créez une liste de méthodes de comptabilisation comme indiqué dans l'image :



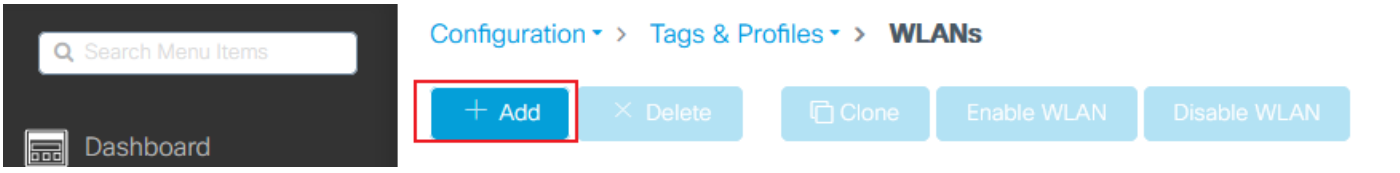
9800 ajouter une liste de comptes



9800 créer une liste de comptes - détails

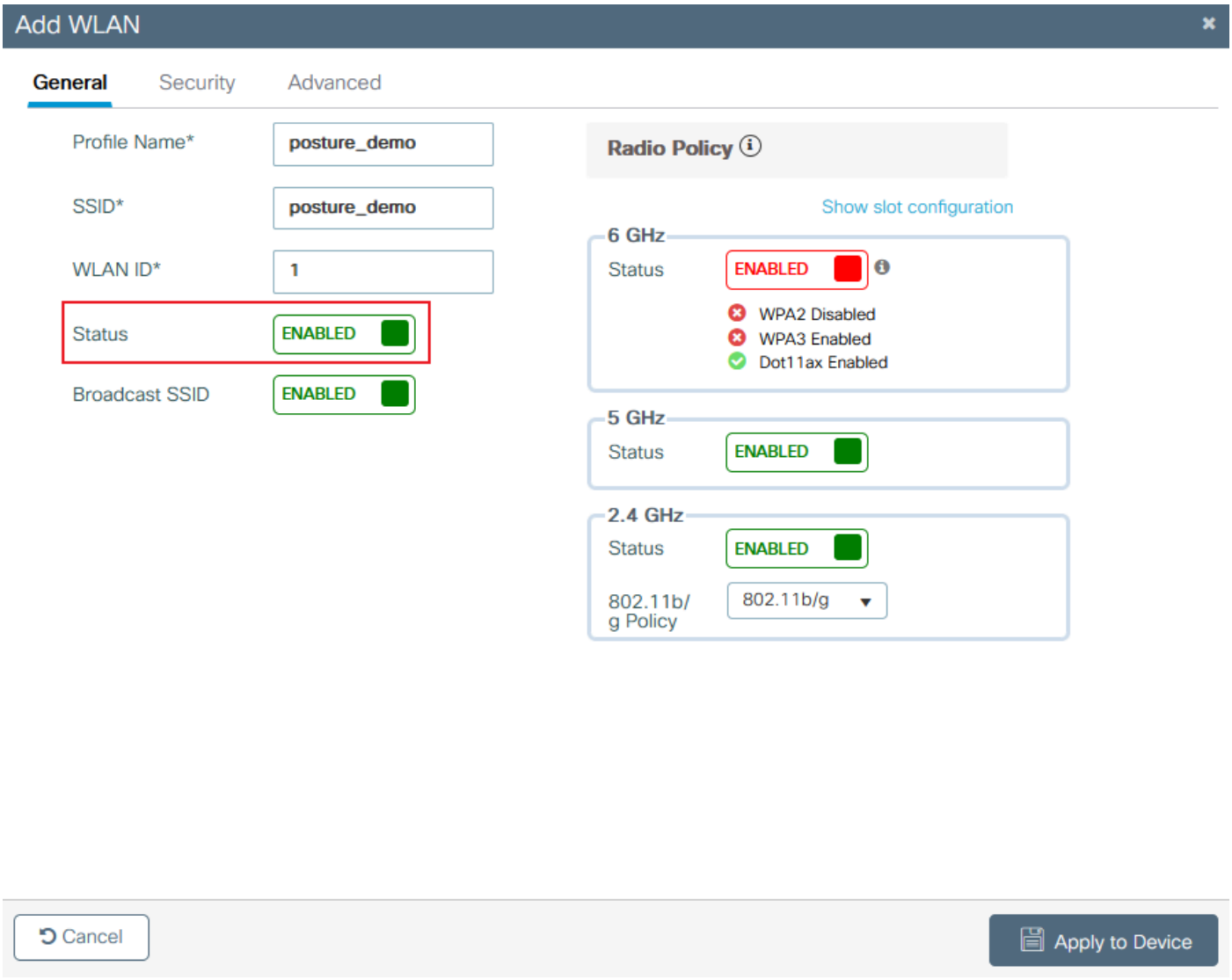
Configuration d’un réseau local sans fil (WLAN)

Étape 1 : création du WLAN Accédez à Configuration > Tags & Profiles > WLANs > + Add et configurez le réseau selon les besoins :



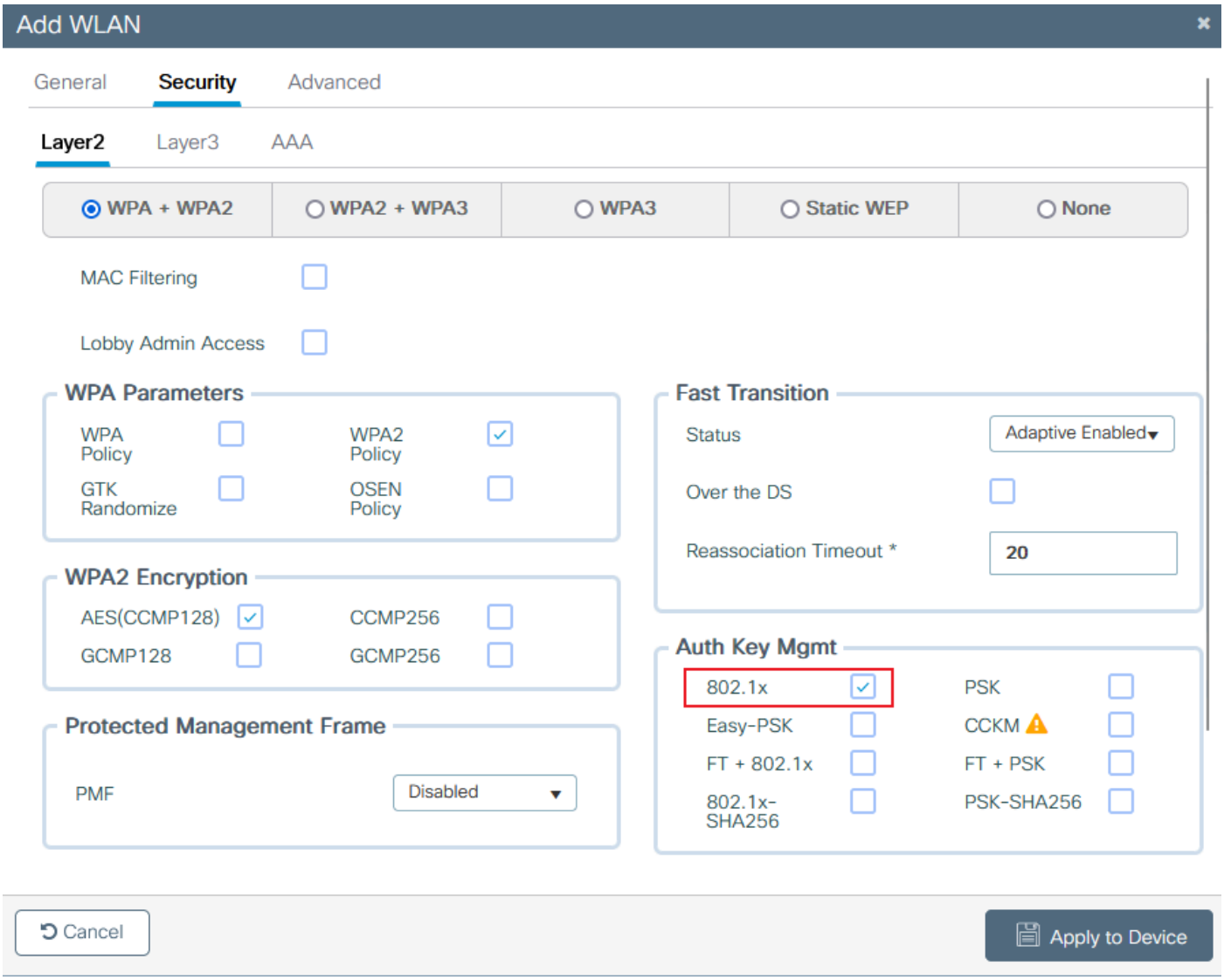
Ajout WLAN 9800

Étape 2. Entrez les informations générales du WLAN.

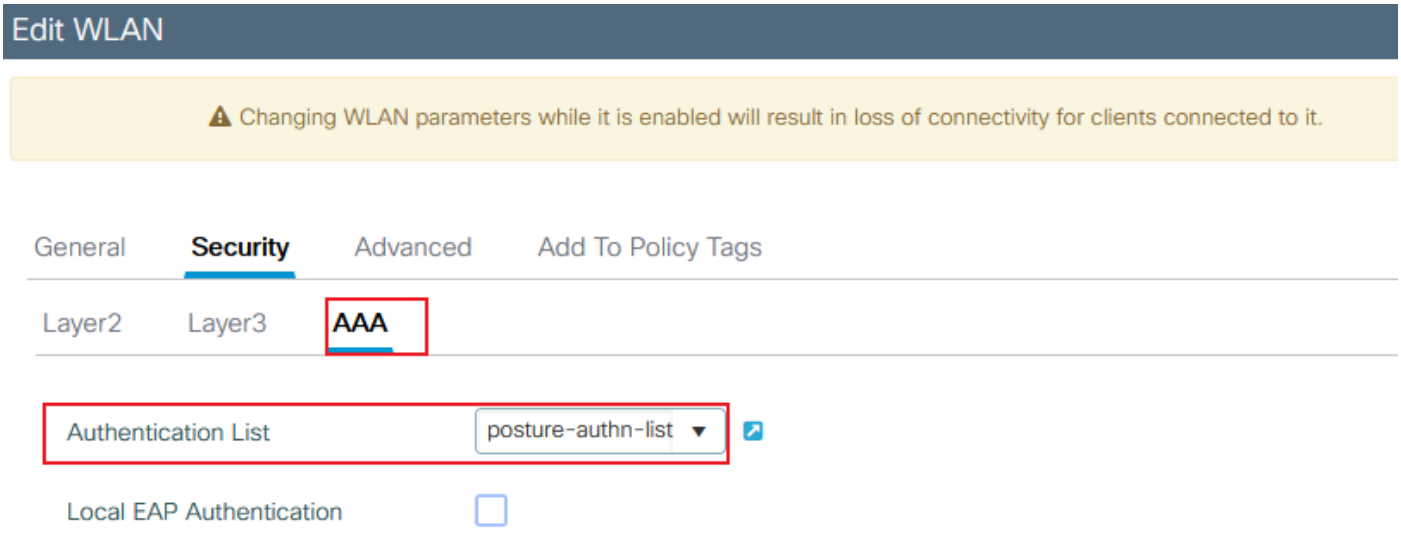


9800 créer un WLAN général

Étape 3. Accédez à l'onglet Security et choisissez la méthode de sécurité requise. Dans ce cas, choisissez 802.1x et la liste d'authentification AAA (que vous avez créée à l'étape 2. dans la section Configuration AAA) sont nécessaires :



9800 créer une sécurité WLAN L2

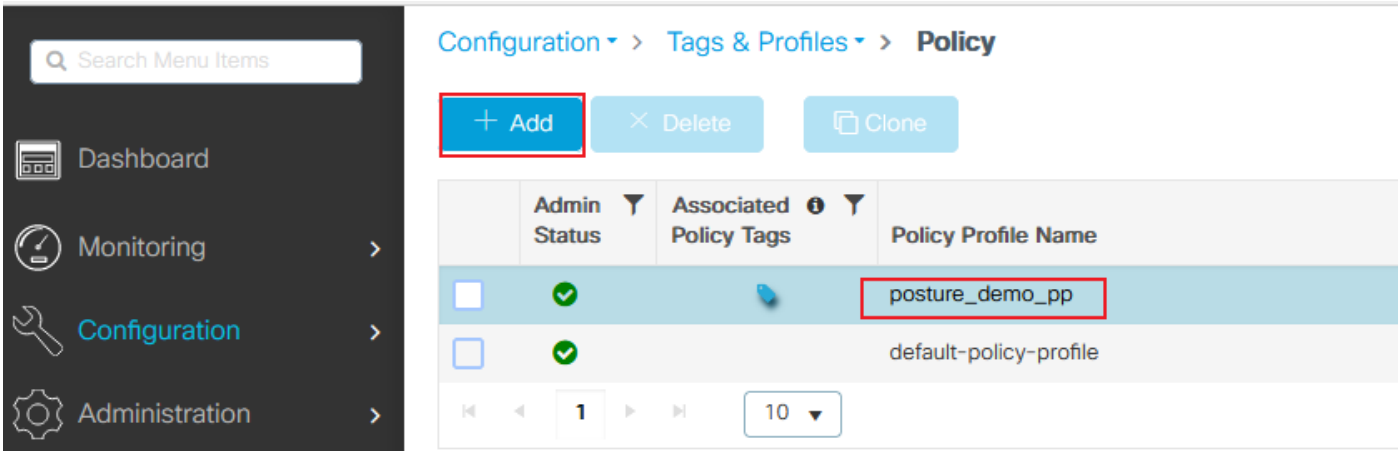


9800 créer une sécurité WLAN AAA

Configuration du profil des politiques

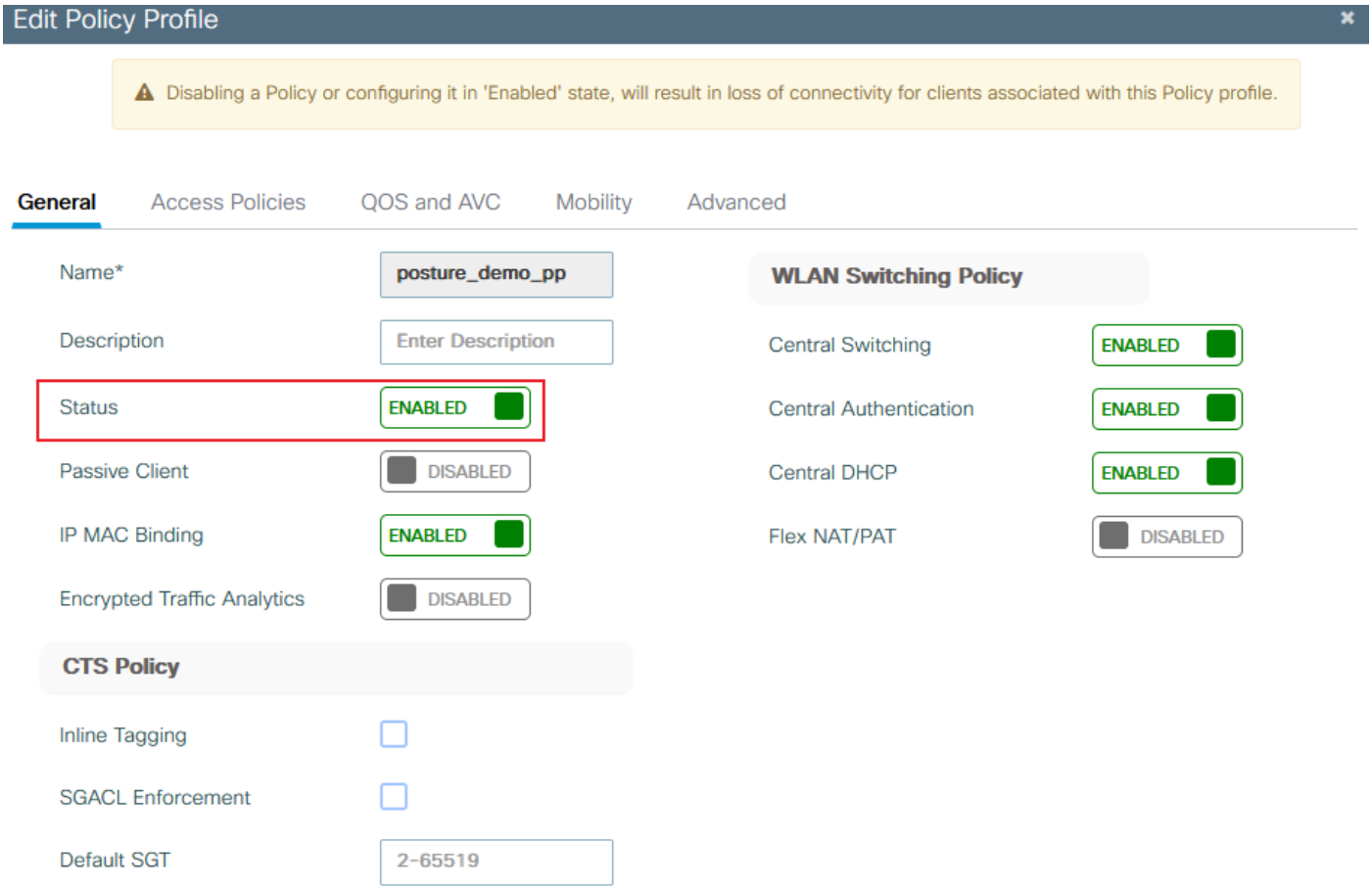
Dans un profil de stratégie, vous pouvez décider d'attribuer les clients à quel VLAN, entre autres paramètres (comme la liste de contrôle d'accès (ACL), la qualité de service (QoS), l'ancrage de mobilité, les minuteurs, etc.). Vous pouvez soit utiliser votre profil de politique par défaut, soit en créer un nouveau.

Étape 1. Créer un nouveau profil de stratégie. Accédez à Configuration > Tags & Profiles > Policy et créez-en une nouvelle :



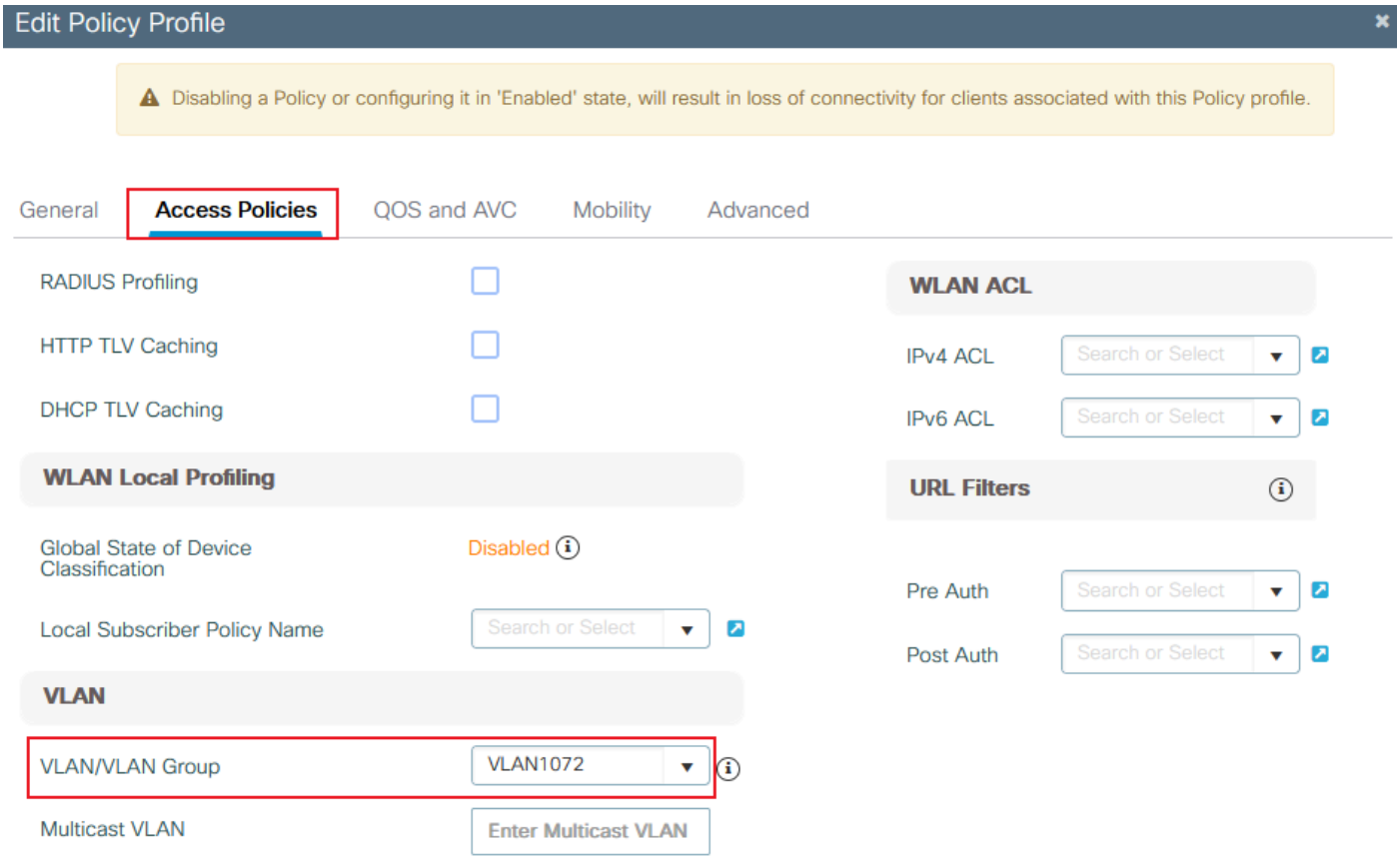
9800 ajouter un profil de stratégie

Assurez-vous que le profil est activé.



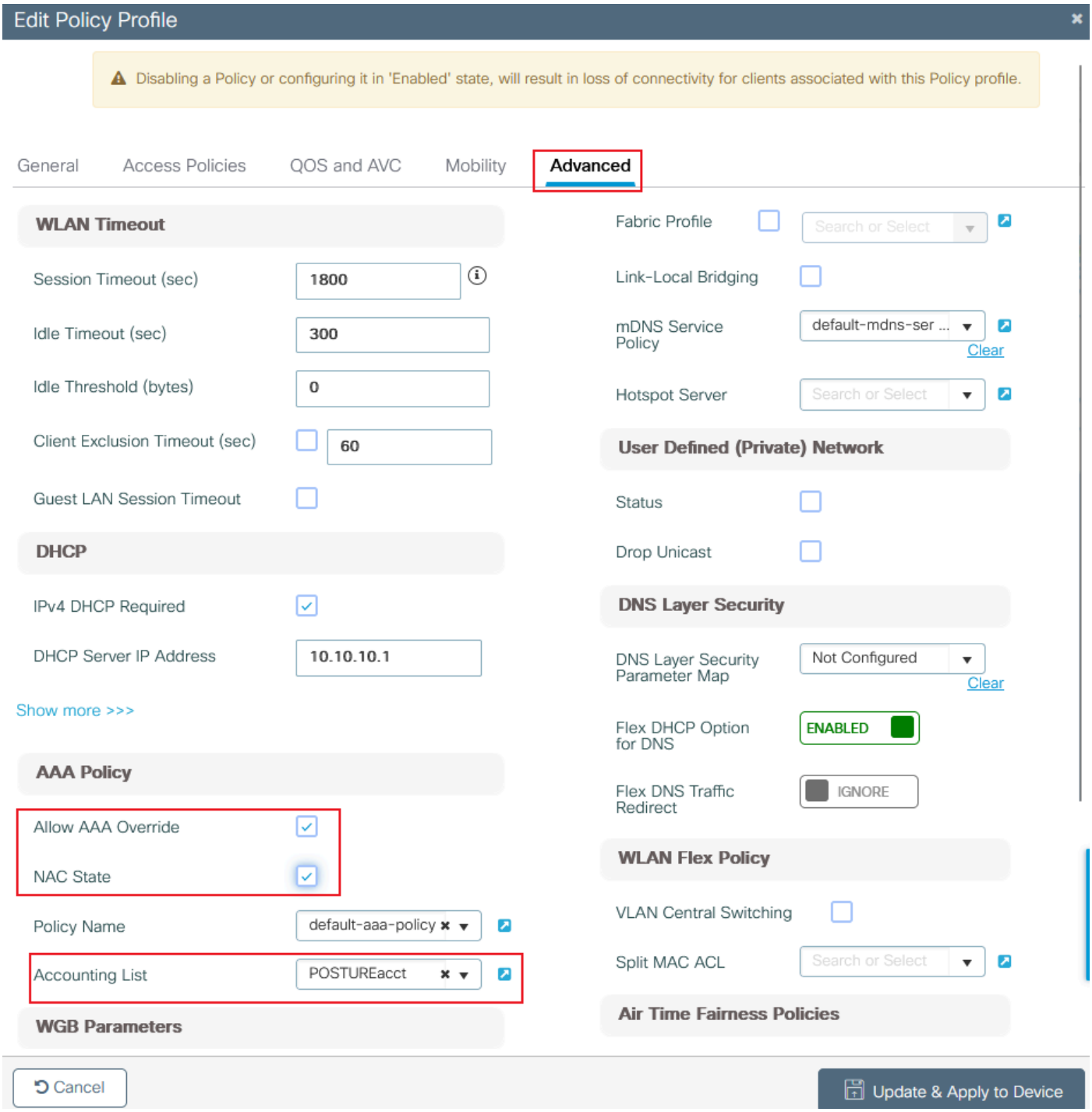
9800 créer un profil de stratégie général

Étape 2. Choisissez le VLAN. Accédez à l'onglet Access Policies et choisissez le nom de VLAN dans la liste déroulante ou tapez manuellement l'ID de VLAN. Ne configurez pas de liste de contrôle d’accès dans le profil de politique:



9800 créer un profil de stratégie VLAN

Étape 3 : configuration du profil de stratégie pour accepter les remplacements ISE (autoriser le remplacement AAA) et la modification de l'autorisation (état NAC) Vous pouvez également définir une méthode de gestion des comptes:

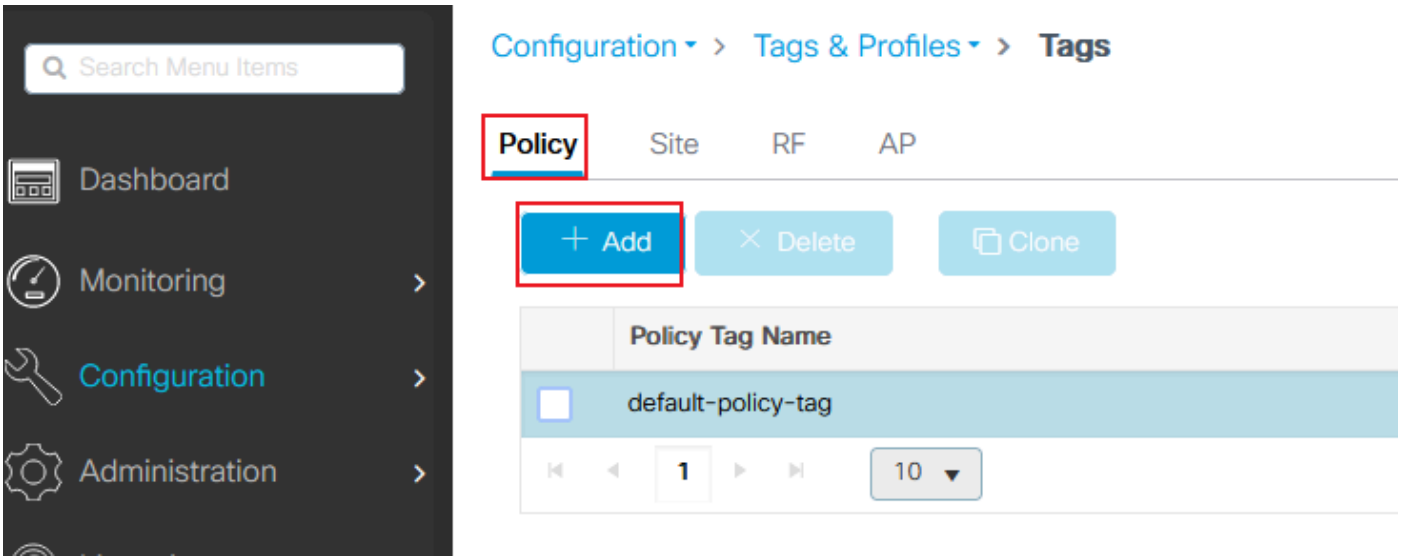


9800 créer un profil de stratégie Avancé

Configuration des balises des politiques

Vous pouvez associer votre SSID à votre profil de politiques dans la balise de politiques. Vous pouvez soit créer une nouvelle balise de politiques, soit utiliser la balise de politique par défaut.

Accédez à Configuration > Tags & Profiles > Tags > Policy et ajoutez-en un nouveau si nécessaire, comme indiqué dans l'image :



9800 policy tag add

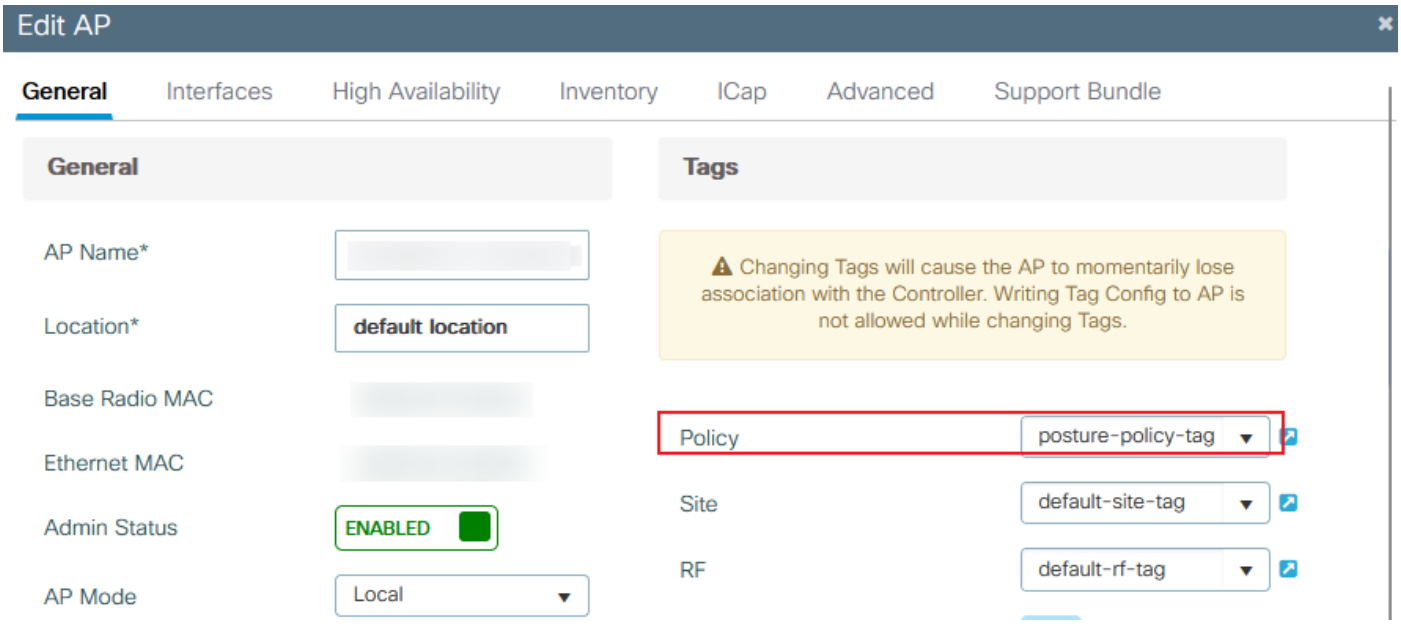
Liez votre profil de réseau WLAN au profil de politiques souhaité:



Détails de la balise de stratégie 9800

Affectation des balises des politiques

Affectez la balise de politiques aux points d'accès nécessaires. Accédez à Configuration > Wireless > Access Points > AP Name > General Tags, effectuez l'affectation nécessaire, puis cliquez sur Update & Apply to Device.



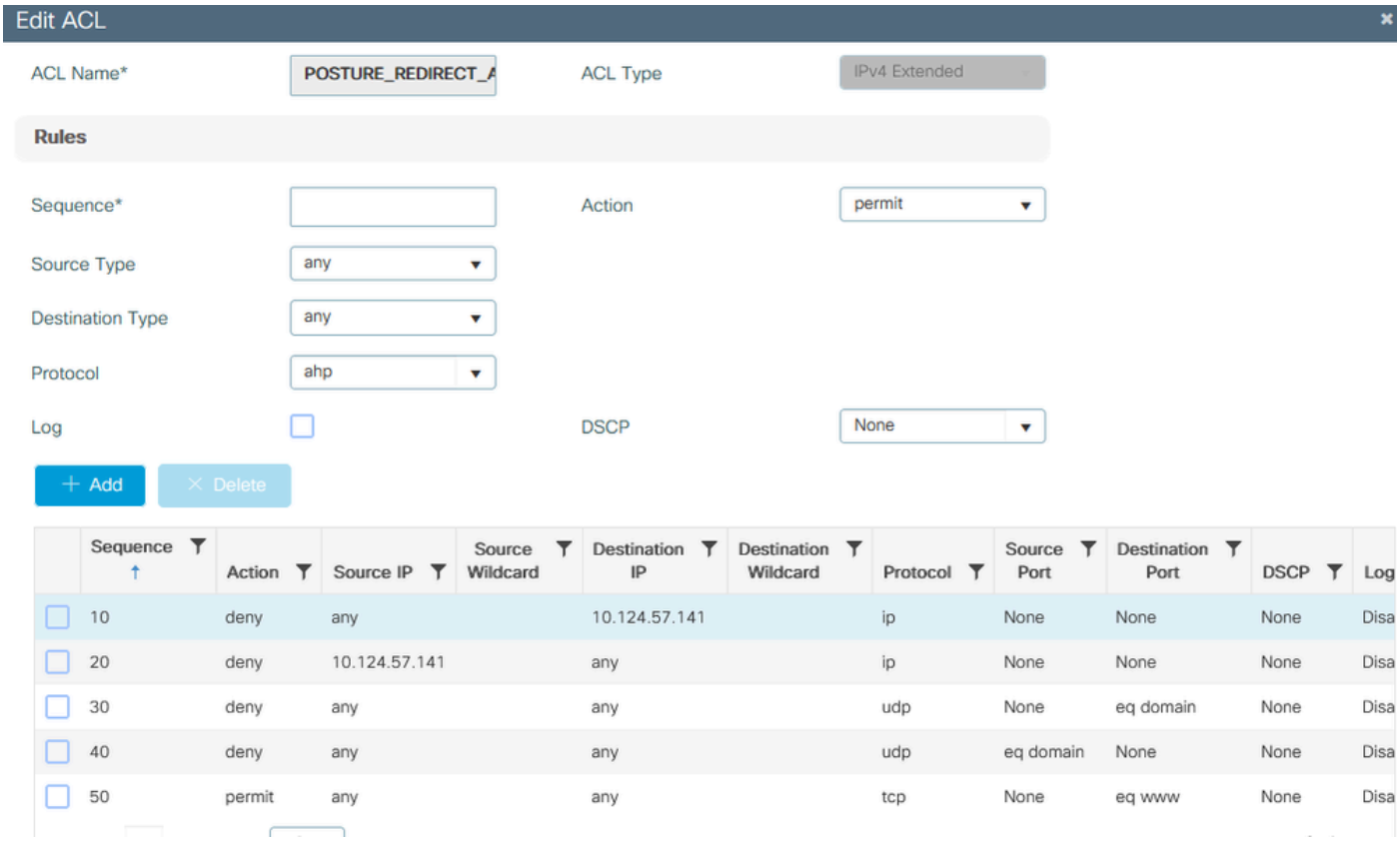
Affectation de balise de stratégie 9800

Configuration d'une liste de contrôle d'accès de redirection

Accédez à Configuration > Security > ACL > + Add pour créer une nouvelle liste de contrôle d'accès.

La liste de contrôle d'accès utilisée pour la redirection de Posture Portal a les mêmes exigences que l'authentification Web centrale (CWA).

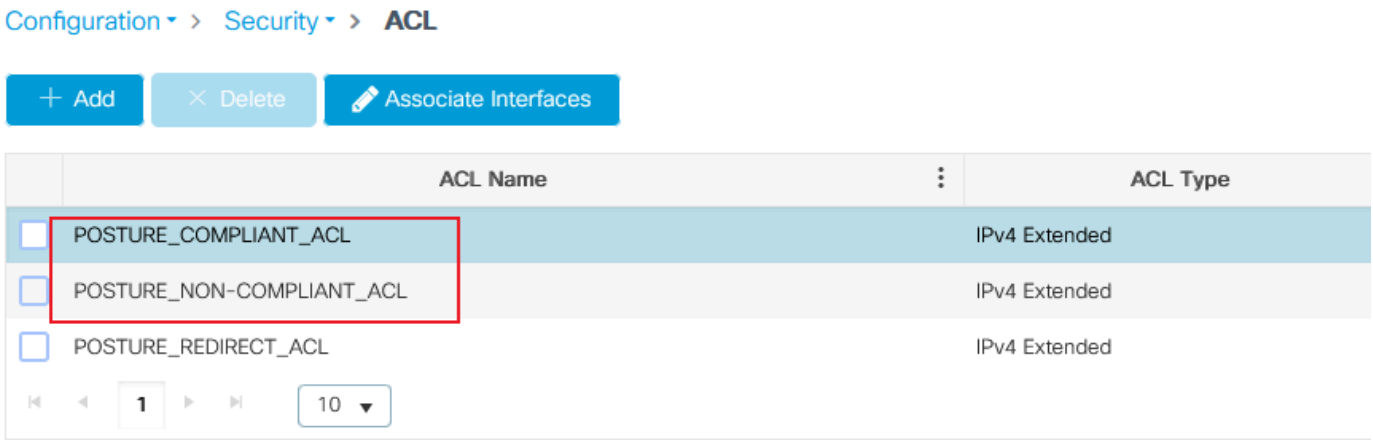
Vous devez refuser le trafic vers vos nœuds PSN ISE, refuser le DNS et autoriser tout le reste. Cette liste de contrôle d'accès de redirection n'est pas une liste de contrôle d'accès de sécurité, mais une liste de contrôle d'accès ponctuelle qui définit le trafic acheminé vers le processeur (en cas d'autorisation) pour un traitement ultérieur (comme la redirection) et le trafic restant sur le plan de données (en cas de refus) et qui évite la redirection. La liste de contrôle d'accès doit ressembler à ceci (remplacez 10.124.57.141 par votre adresse IP ISE dans cet exemple) :



Détails ACL de redirection 9800

Configuration ACL de stratégie

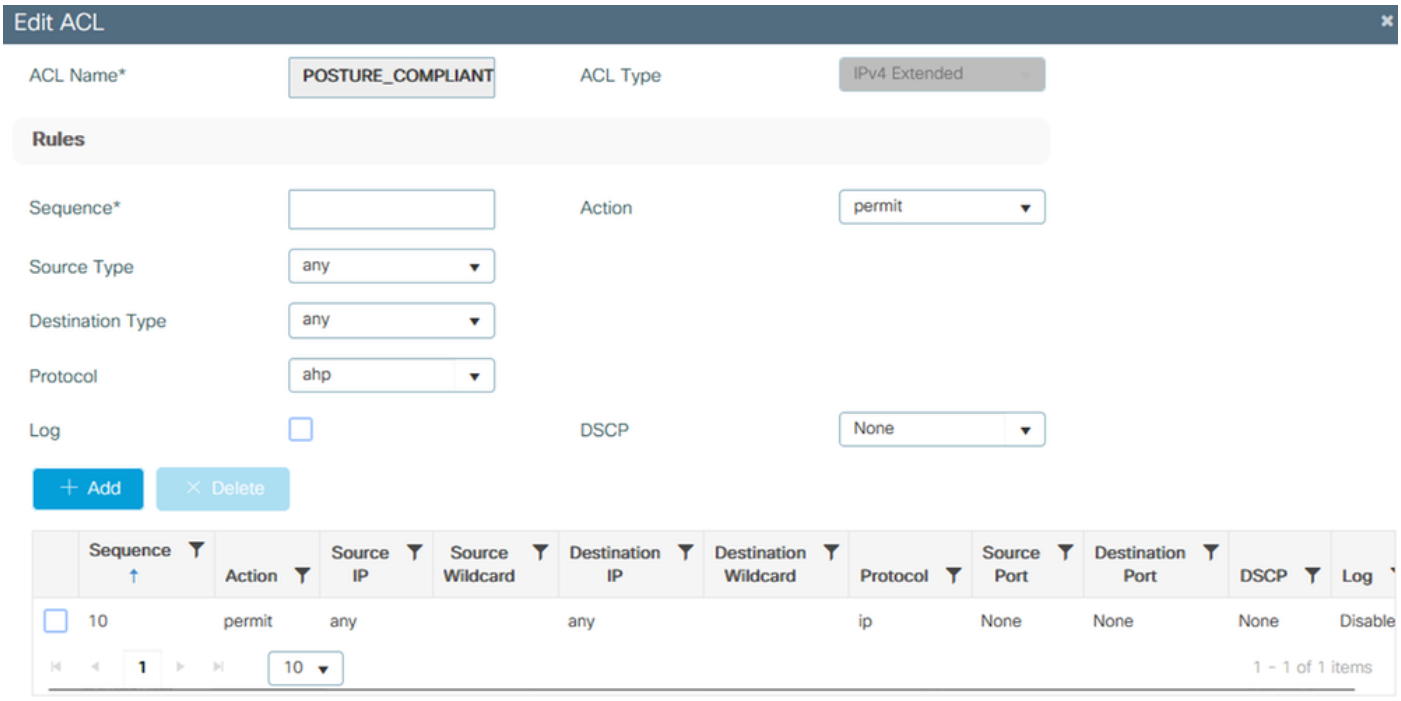
Dans ce cas, vous devez définir des listes de contrôle d'accès distinctes sur le WLC 9800 pour ISE pour autoriser les scénarios Conforme et Non-Conforme en fonction du résultat de la vérification de position.



9800 ACL général

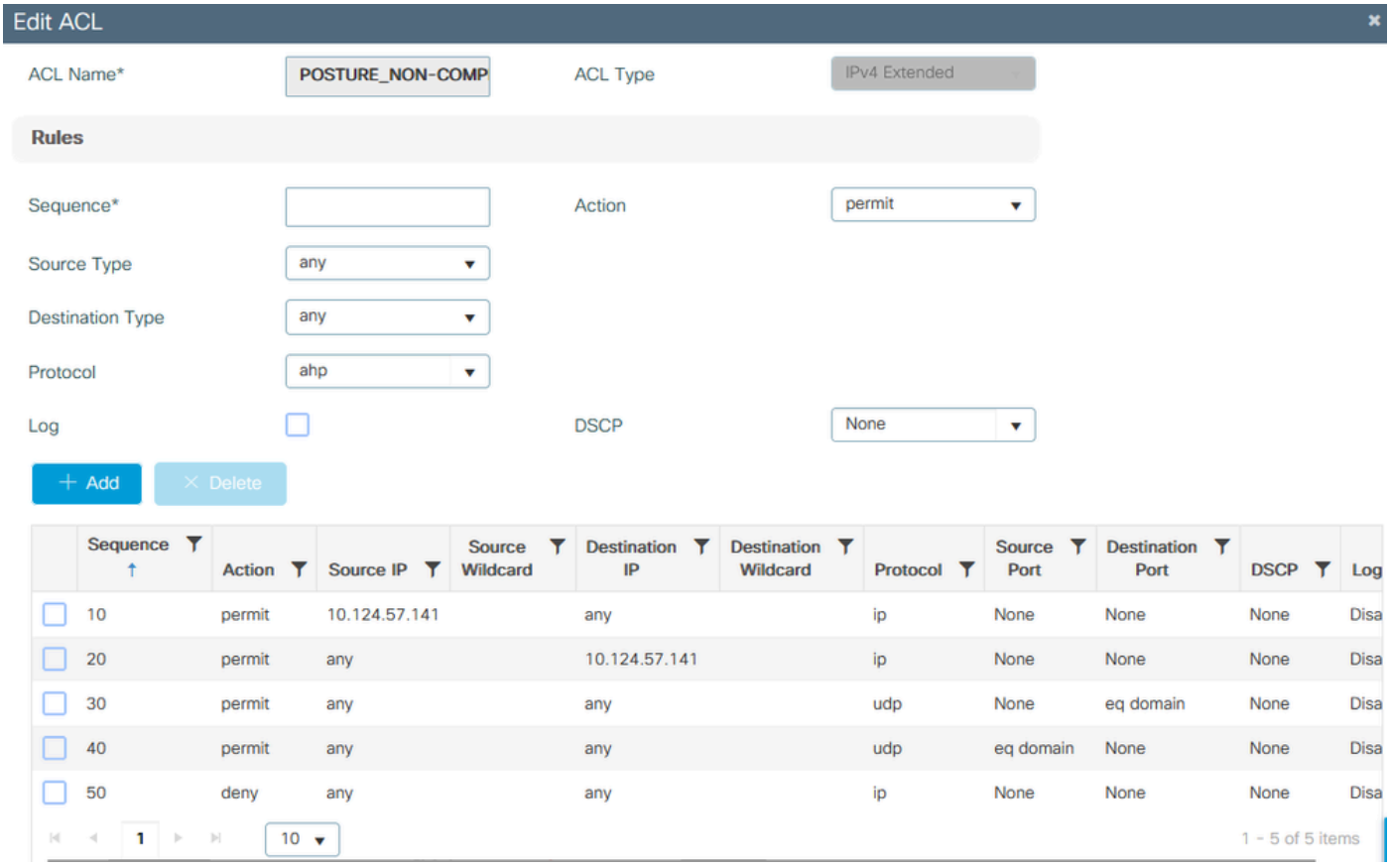
Pour le scénario Conforme, utilisez simplement permit all dans ce cas. Comme autre configuration courante, vous pouvez également demander à ISE de ne pas autoriser de liste de contrôle

d'accès dans le résultat conforme, ce qui équivaut à autoriser tout du côté 9800 :



9800 ACL - Conforme

Dans un scénario non conforme, le client autorise uniquement l'accès à certains réseaux, généralement le serveur de conversion (ISE lui-même dans ce cas) :

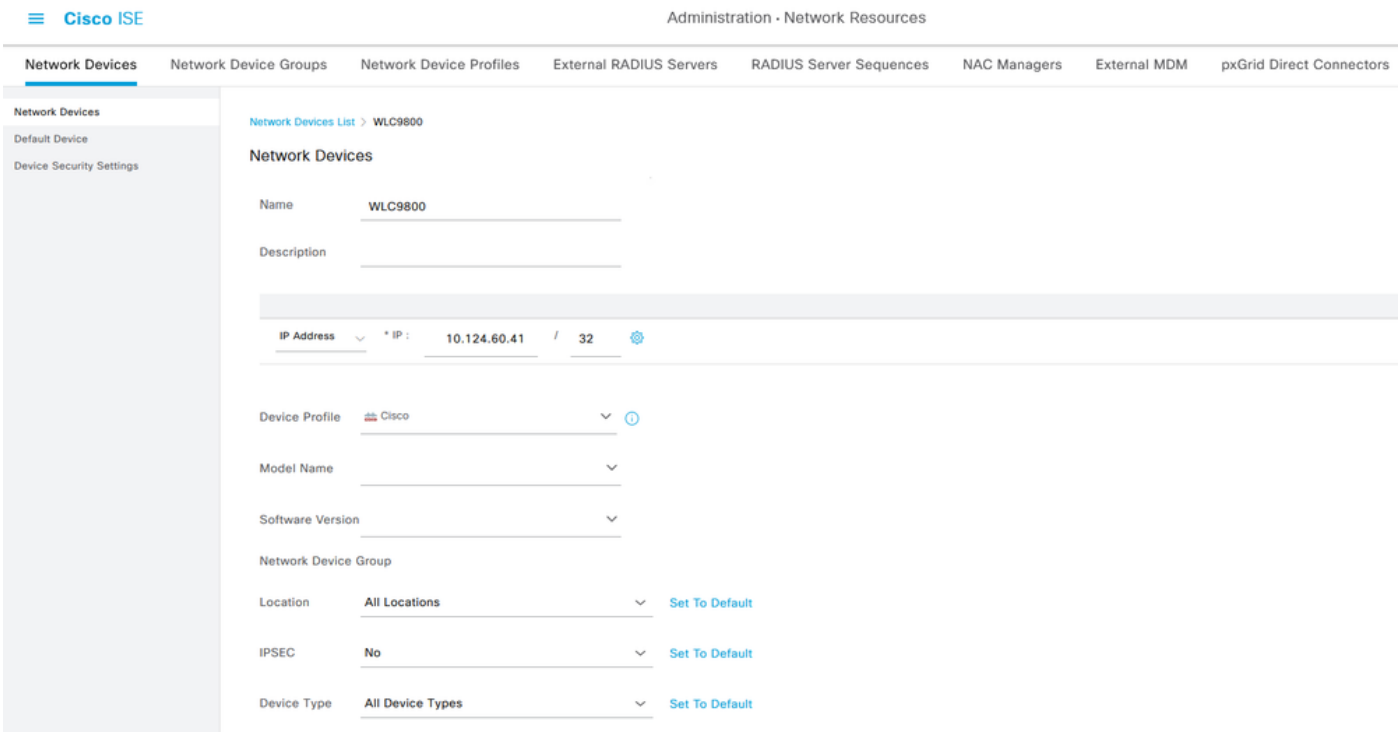


ACL 9800 - Non conforme

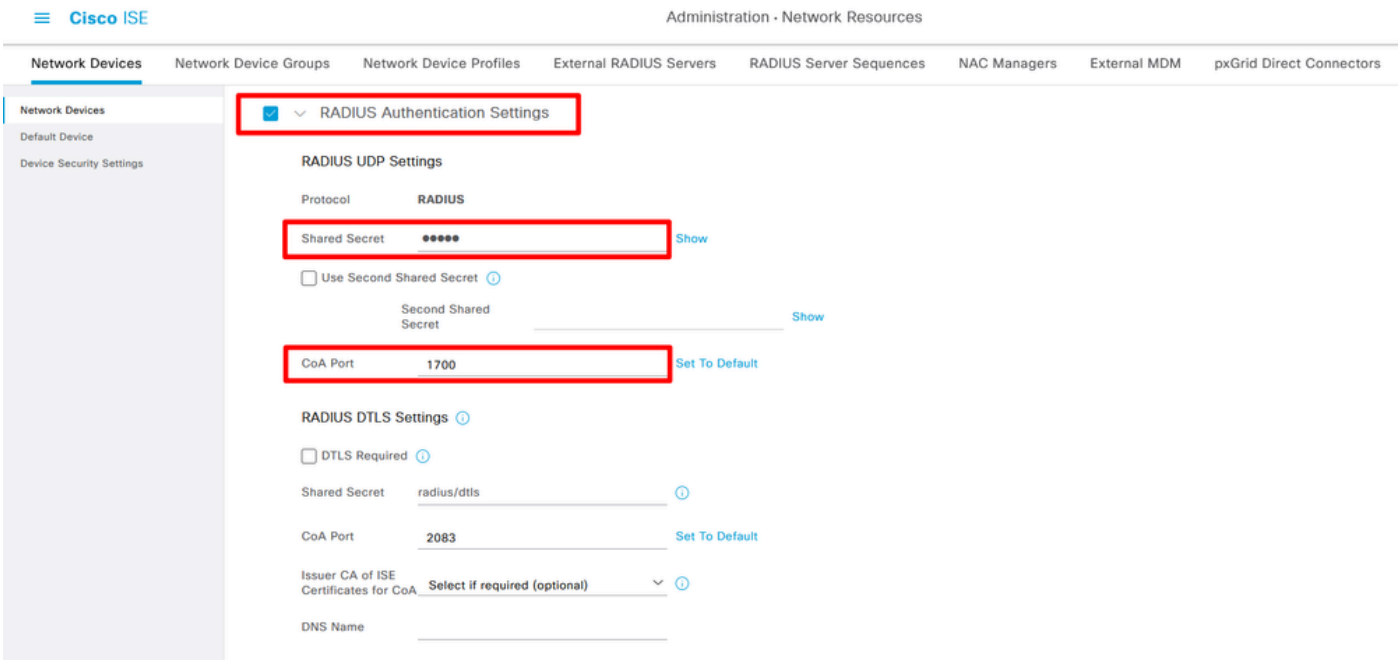
Configuration et réglage de la position AAA sur ISE

Condition de posture : Dans cet exemple, l'exigence de déterminer la conformité consiste à détecter si un fichier de test spécifique existe sur le bureau utilisé pour tester le PC Windows.

Étape 1 : ajout du WLC 9800 en tant que NAD sur l'ISE Accédez à Administration > Network Resources > Network Devices > Add:



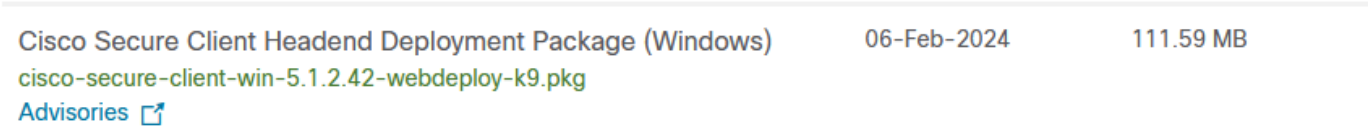
Ajouter un périphérique réseau 01



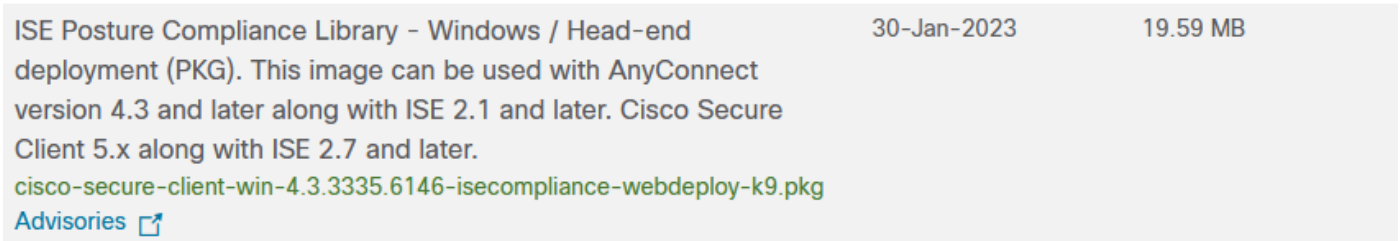
Ajouter un périphérique réseau 02

Étape 2. Téléchargez le package de déploiement Cisco Secure Client Headend et le module de conformité sur le site Web Cisco Software CCO.

Accédez à Téléchargement et recherche de logiciels Cisco Secure Client :

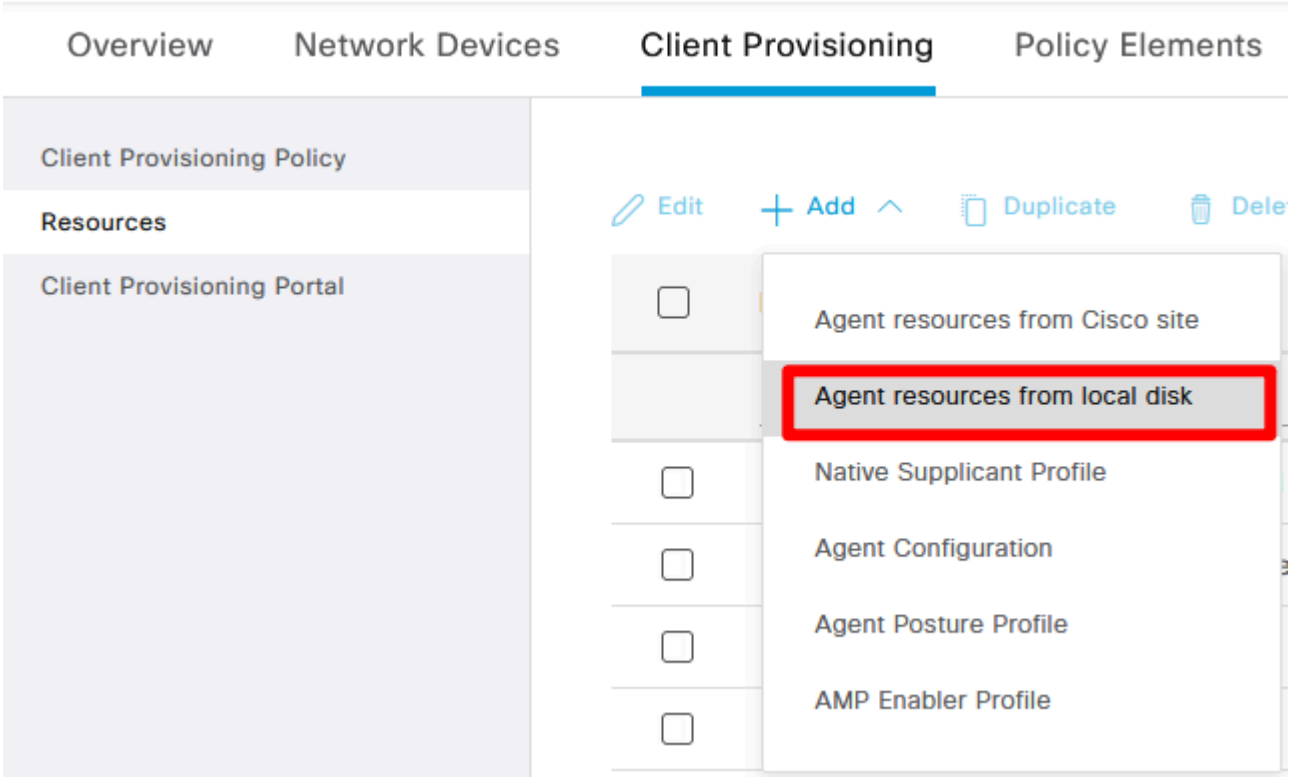


Client sécurisé 5.1.2.42

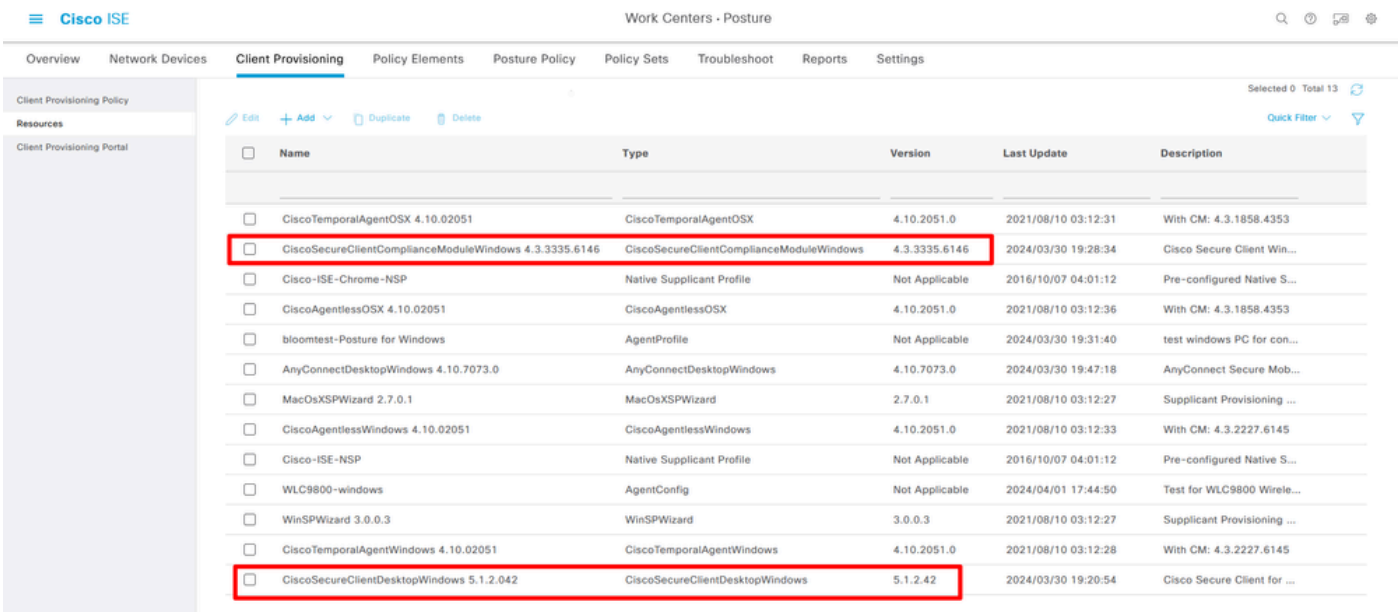


Module de conformité ISE 4.3

Étape 3. Téléchargez le package de déploiement Cisco Secure Client Headend et le package de module de conformité vers ISE Client Provisioning. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add, Choose Agent resources from local disk dans la liste déroulante :

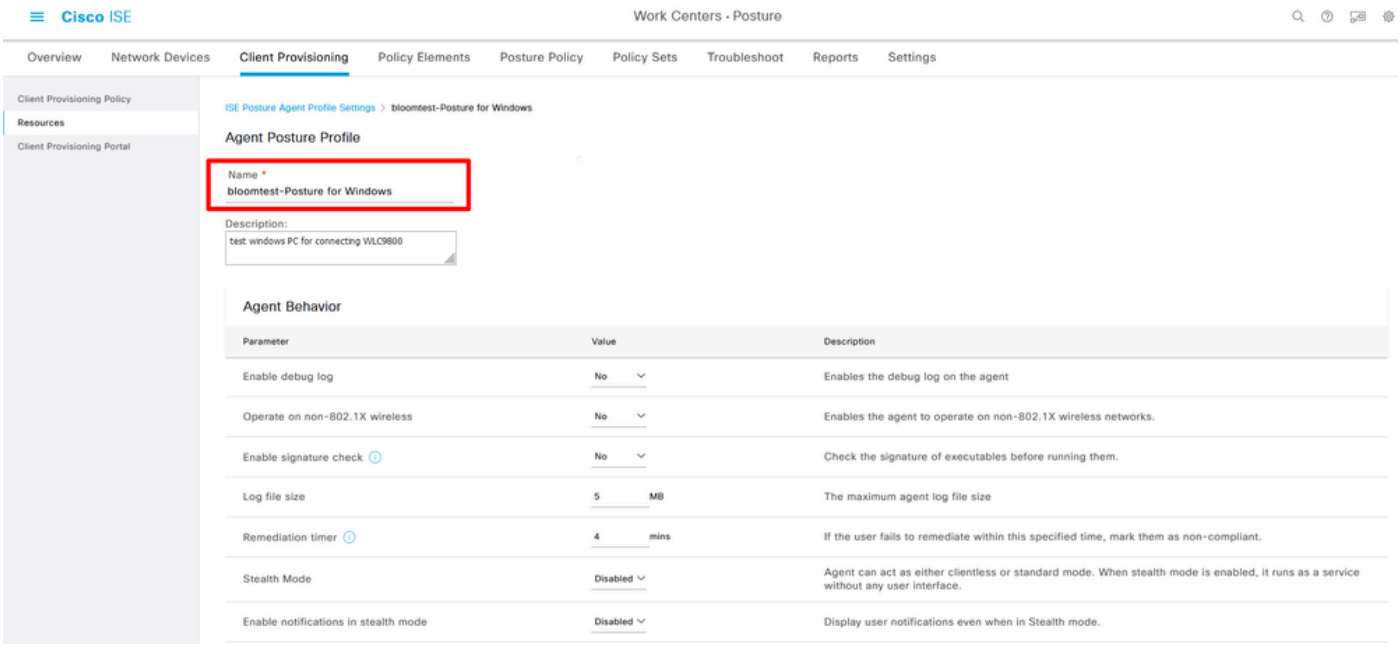


Télécharger le client sécurisé



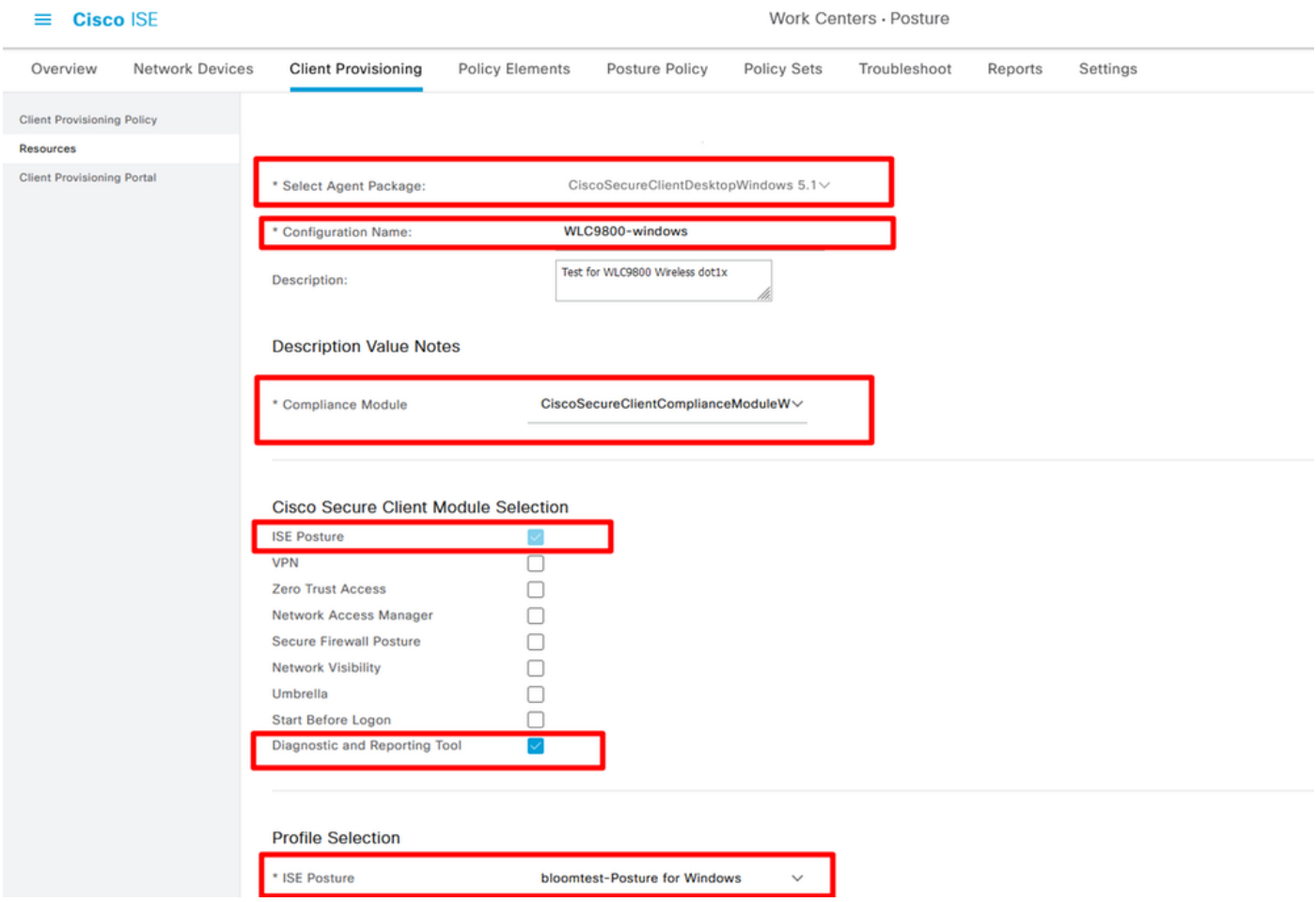
Téléchargement du client sécurisé et du module de conformité réussi

Étape 4. Créer un profil de posture d'agent. Accédez à Work Centers > Posture > Client Provisioning > Resources > Add > Agent Posture Profile :



Profil de posture de l'agent

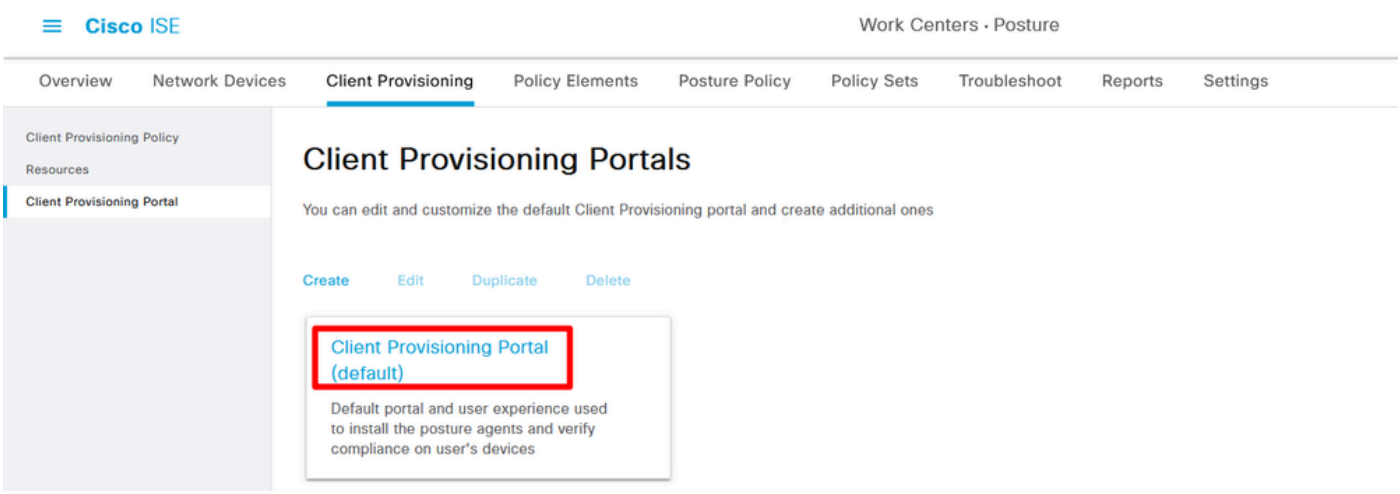
Étape 5 : création de la configuration de l'agent Accédez à Work Centers > Posture > Client Provisioning > Resources > Add > Agent Configuration :



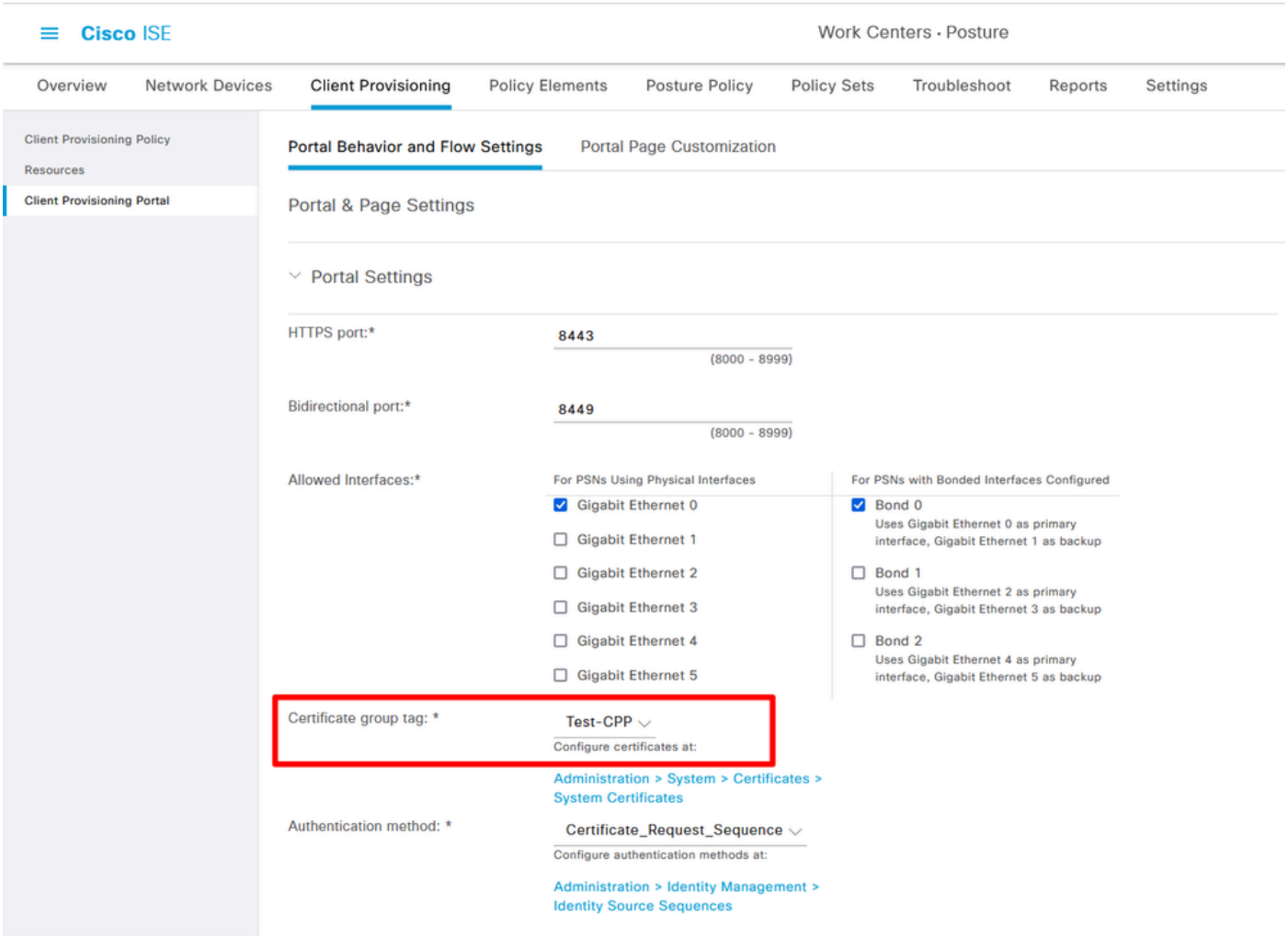
Ajouter une configuration d'agent

Étape 6. Confirmez le portail d'approvisionnement du client. Vous pouvez utiliser le portail par défaut pour les tests. (Générez un CSR et demandez un certificat SSL à partir du serveur AC, puis remplacez la balise Certificate Group sur ce portail, Paramètres. Sinon, un avertissement de certificat non approuvé se produit pendant le processus de test.)

Accédez à Work Centers > Posture > Client Provisioning > Client Provisioning Portals :

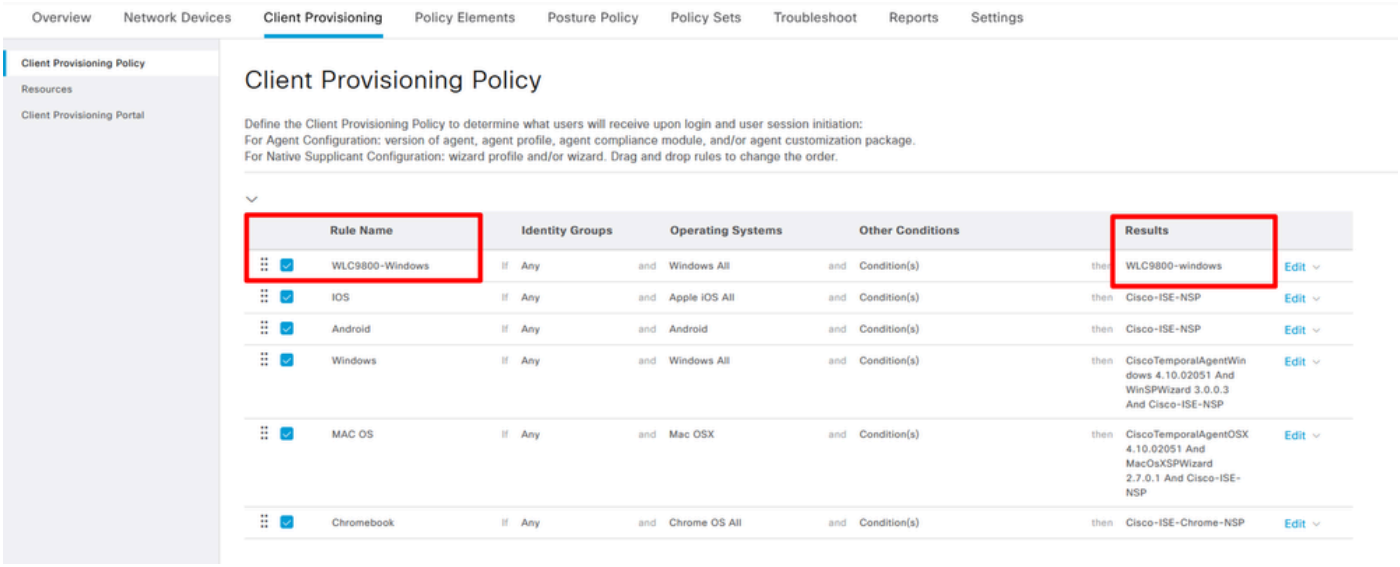


Sélectionnez Client Provisioning Portal 01



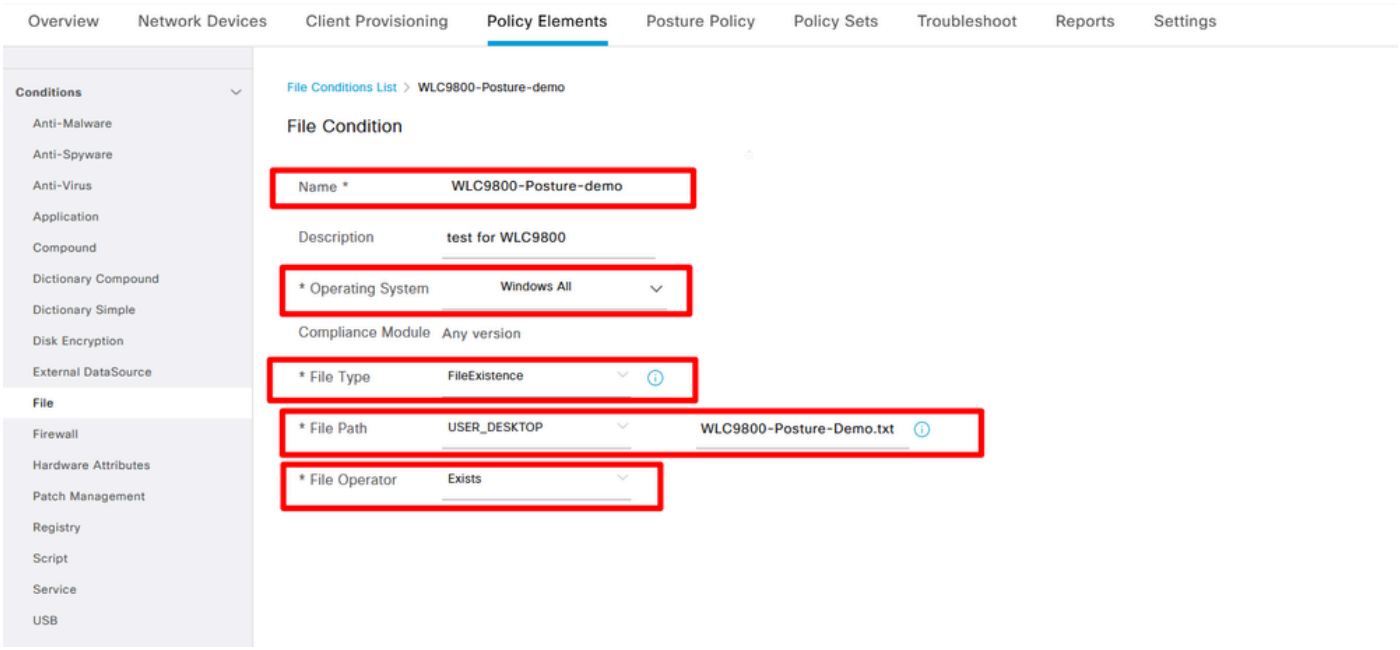
Sélectionnez Client Provisioning Portal 02

Étape 7 : création d'une stratégie de provisionnement client. Accédez à Work Centers > Posture > Client Provisioning > Client Provisioning Policy > Edit > insert new policy above.



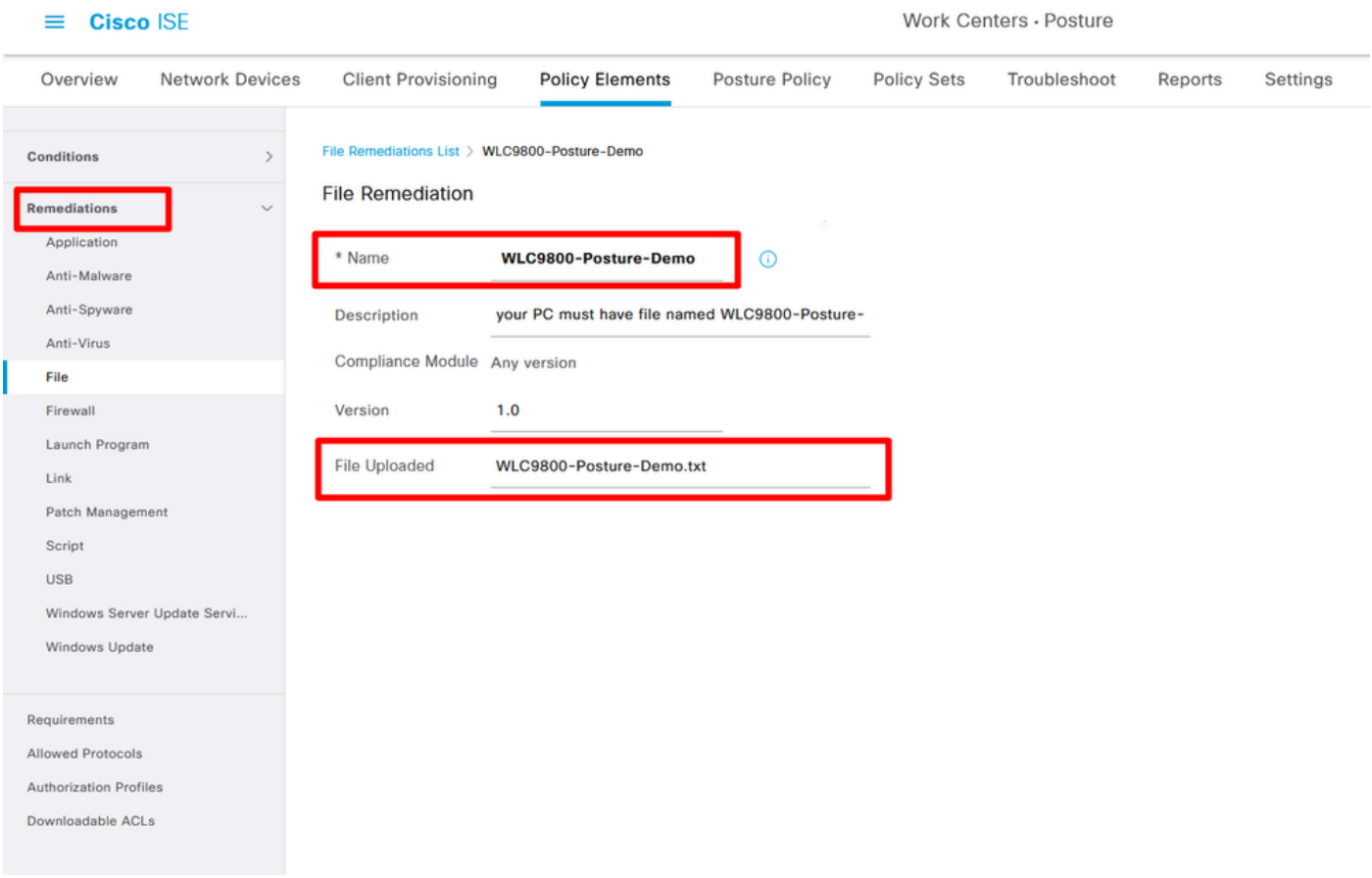
Créer une politique de provisionnement client

Étape 8. Création de conditions de fichier. Accédez à Work Centers > Posture > Policy Elements > Conditions > File > File Conditions > Add :



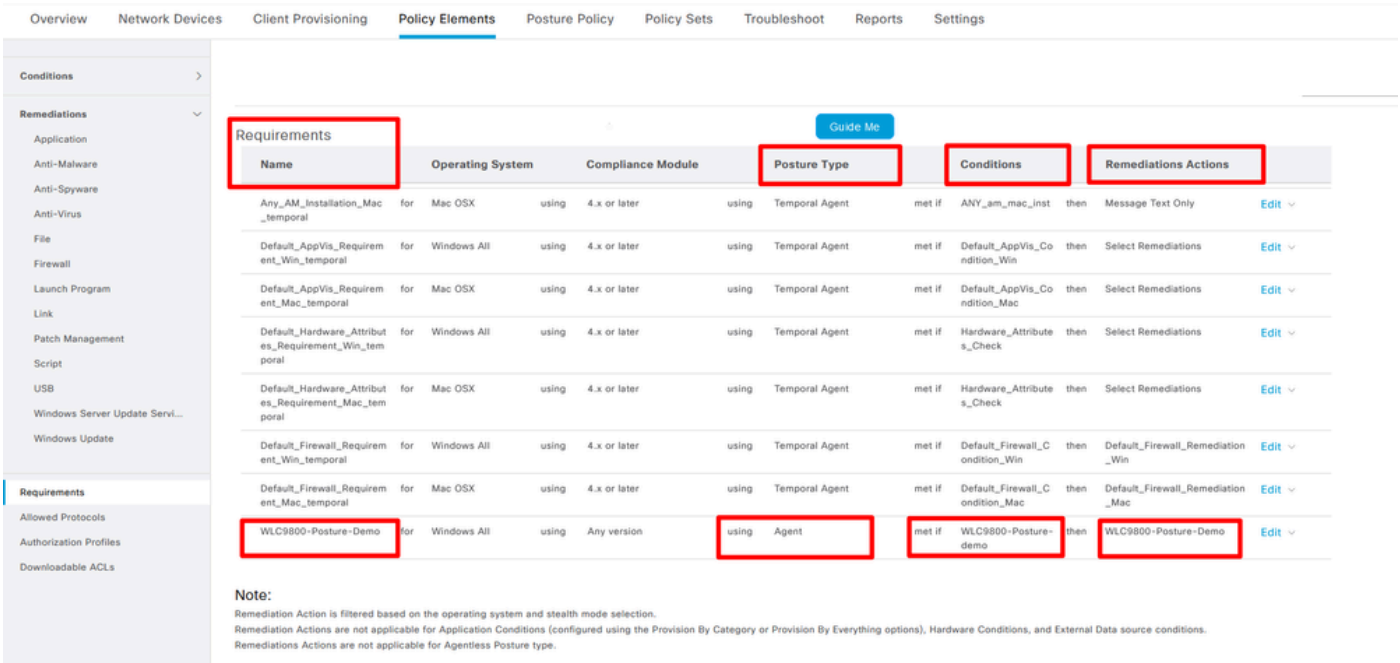
Créer une condition de fichier

Étape 9. Création de mesures correctives. Accédez à Work Centers > Posture > Policy Elements > Remediations > File > Add :



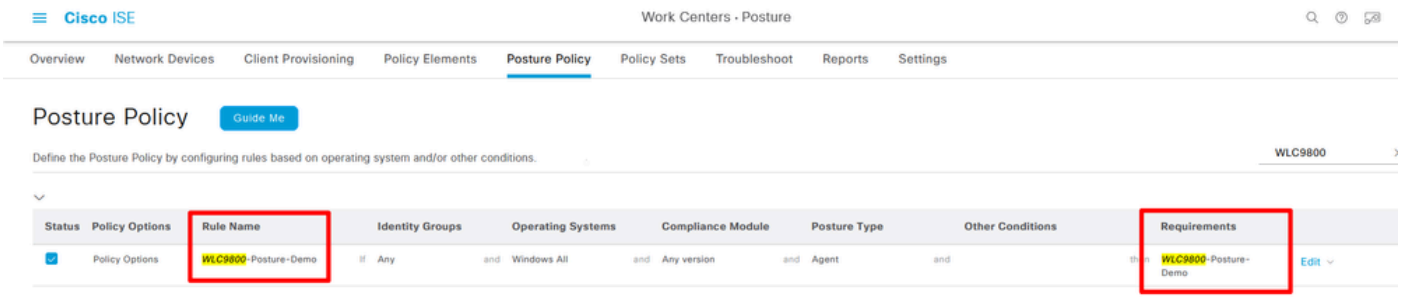
Créer une correction de fichier

Étape 10. Création du besoin. Accédez à Centres de travail > Posture > Eléments de stratégie > Exigences > Insérer une nouvelle exigence :



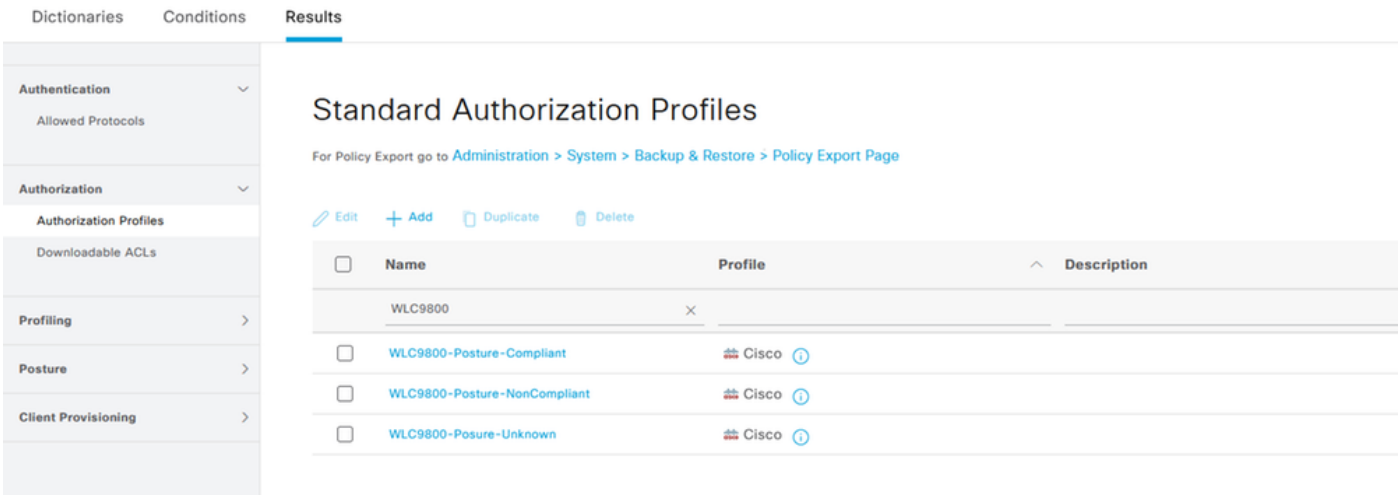
Créer une condition de posture

Étape 11. Créer une politique de posture. Accédez à Work Centers > Posture > Insert new policy :

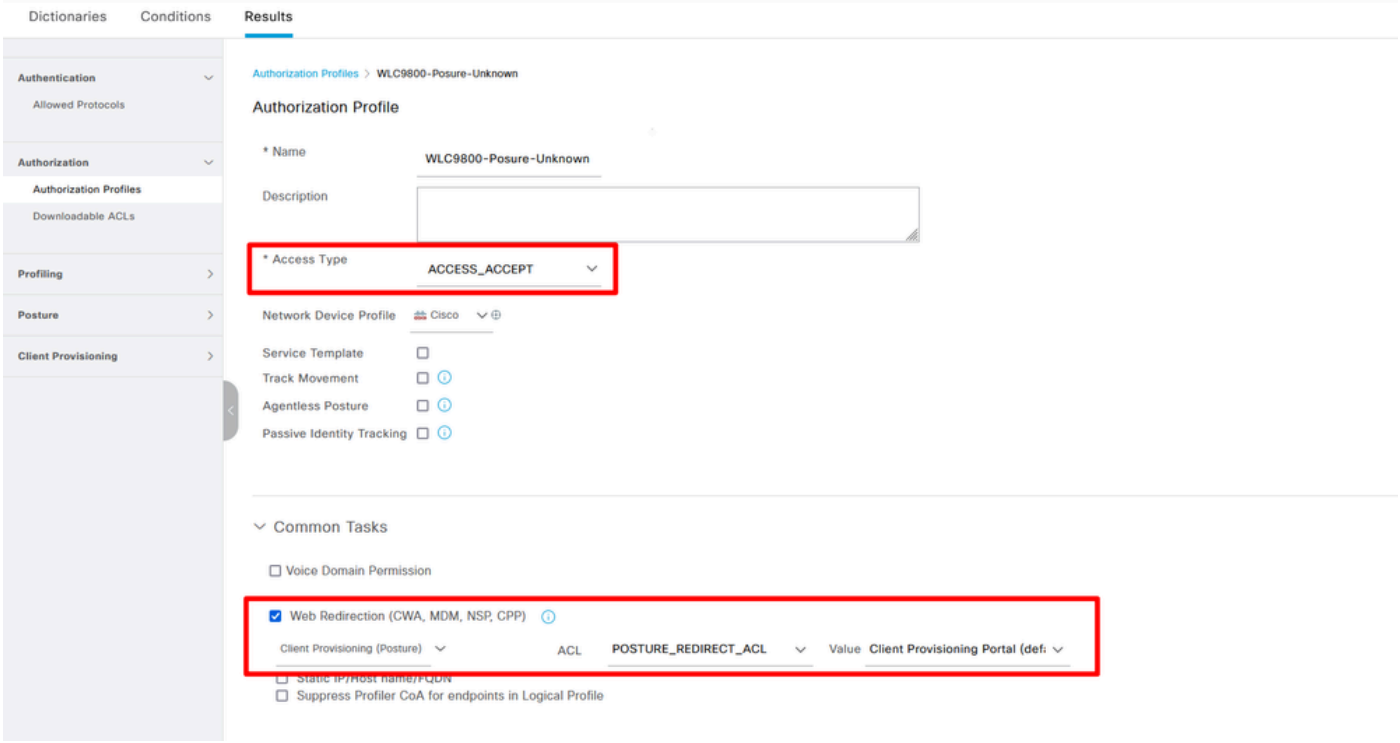


Créer une politique de posture

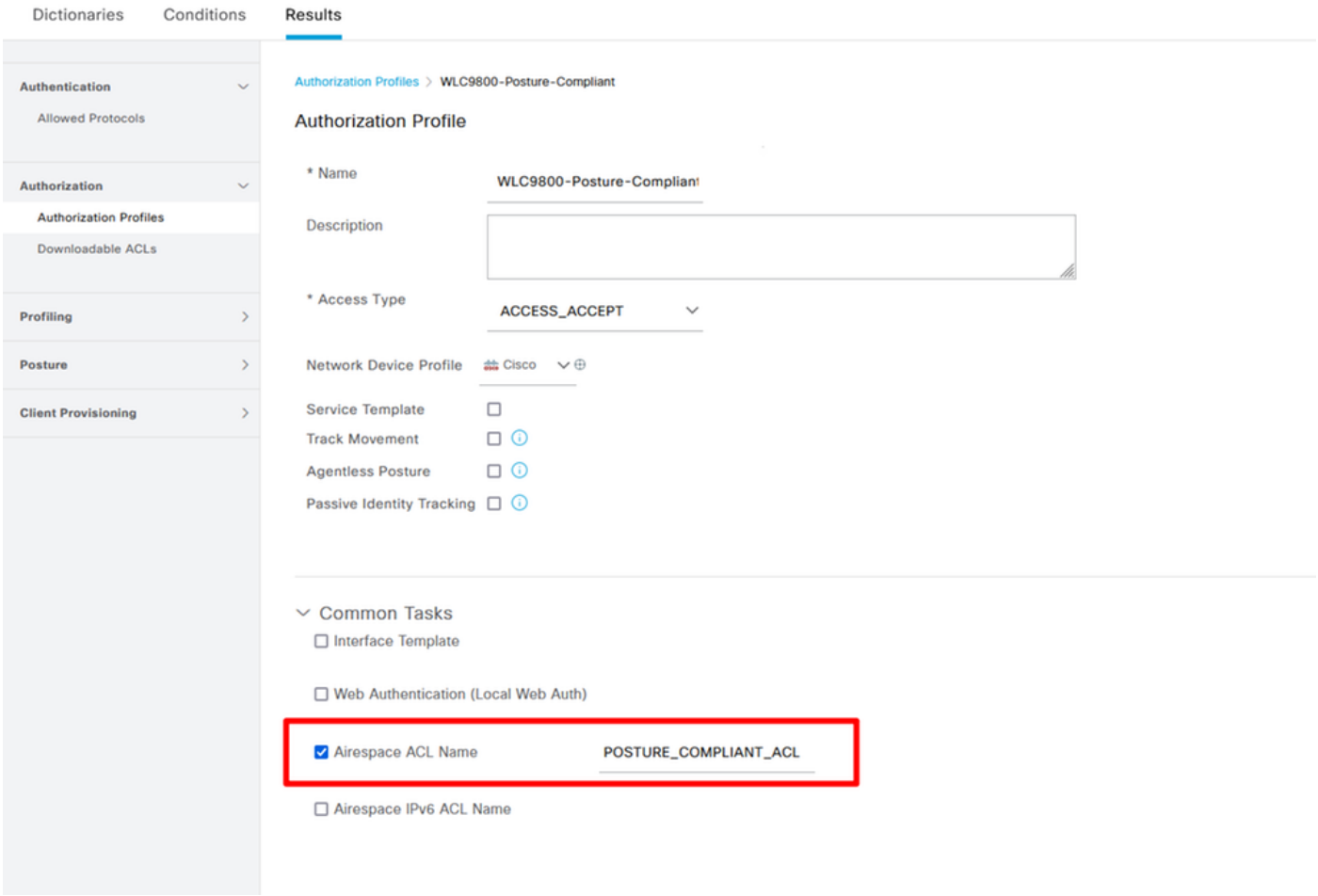
Étape 12. Créez trois profils d'autorisation : L'état de la posture est Inconnu ; le statut de la posture est Non conforme ; L'état de posture est Conforme. Accédez à Politique > Éléments de politique > Résultats > Autorisation > Profils d'autorisation > Ajouter :



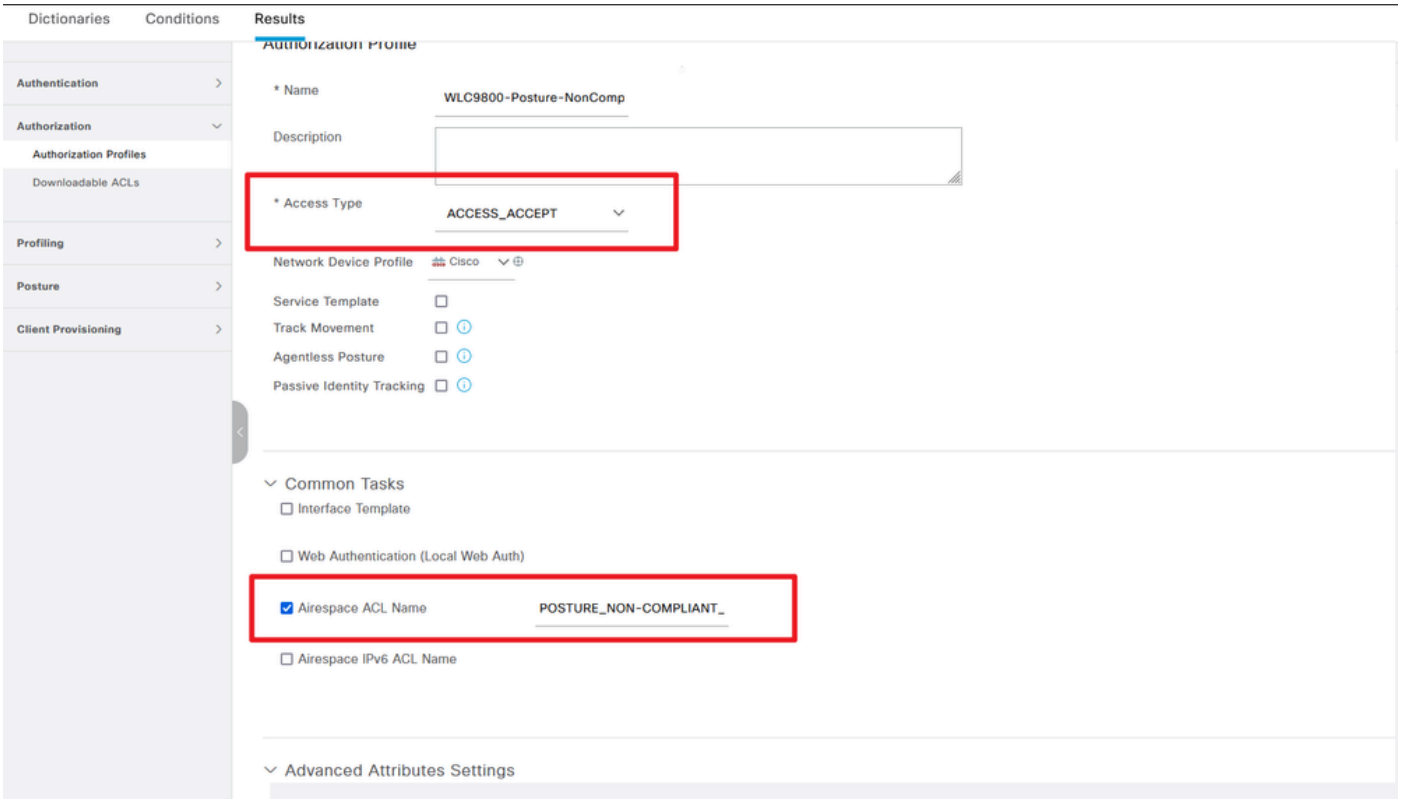
Créer des profils d'autorisation 01



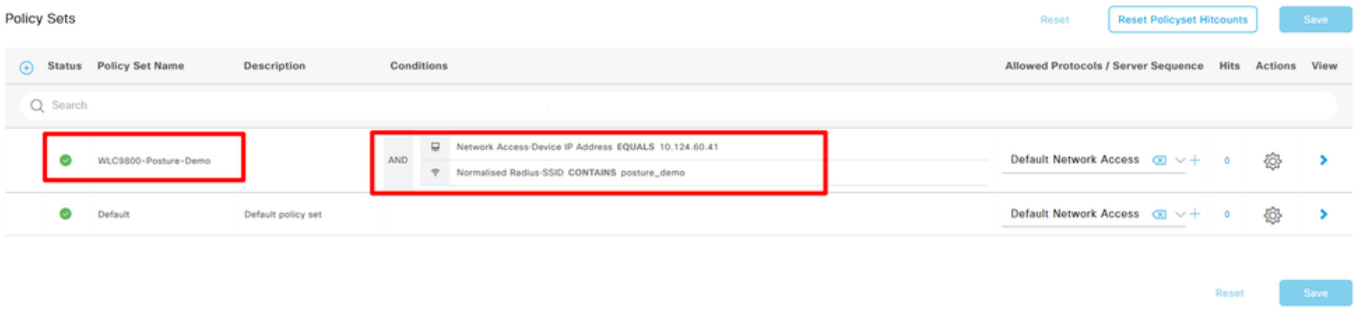
Créer des profils d'autorisation 02



Créer des profils d'autorisation 03



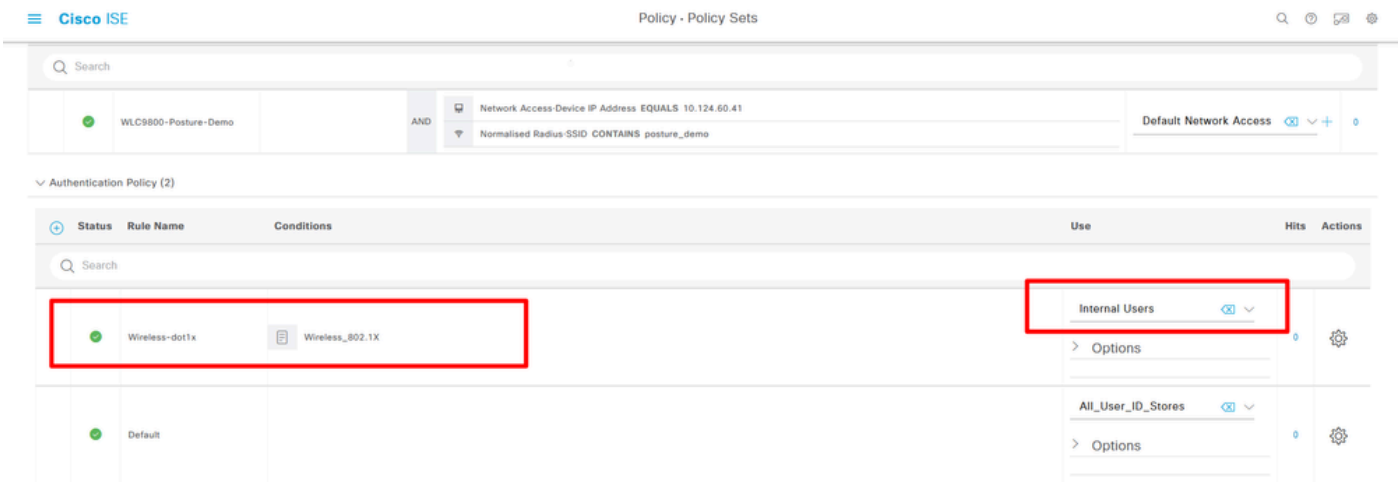
Étape 13. Créer des ensembles de stratégies. Accédez à Policy > Policy.



Créer des jeux de stratégies

Jeux > Icône Ajouter :

Étape 14. Créer une stratégie d'authentification Naviguez jusqu'à Policy > Policy Sets > Expand "WLC9800-Posture-Demo" > Authentication Policy > Add :



Créer une stratégie d'authentification

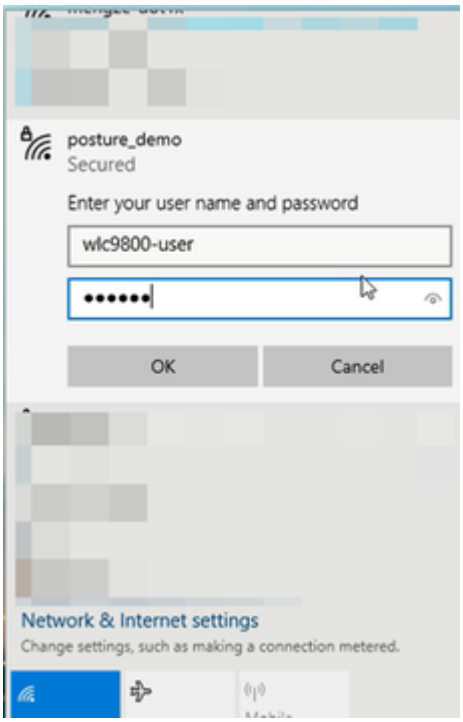
Étape 15. Créer une stratégie d'autorisation. Accédez à Policy > Policy Sets > Expand "WLC9800-Posture-Demo" > Authorization Policy > Add :



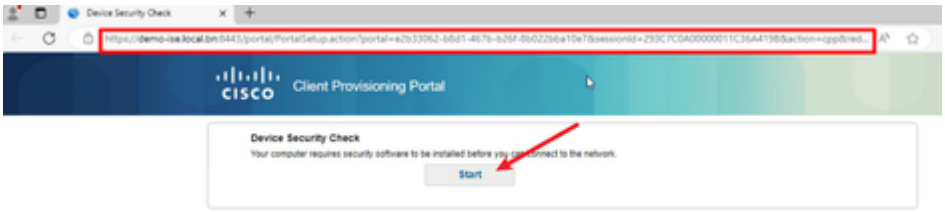
Créer une stratégie d'autorisation

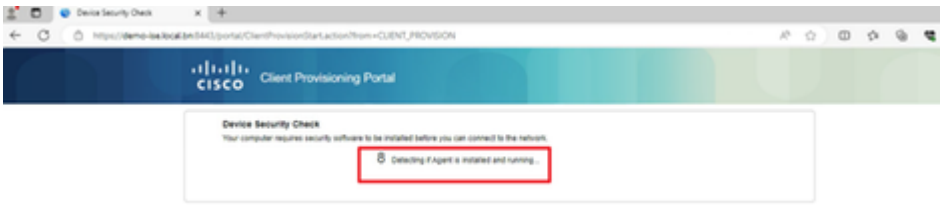
Exemples

1. Test du SSID connecté posture_demo avec les informations d'identification 802.1X correctes.

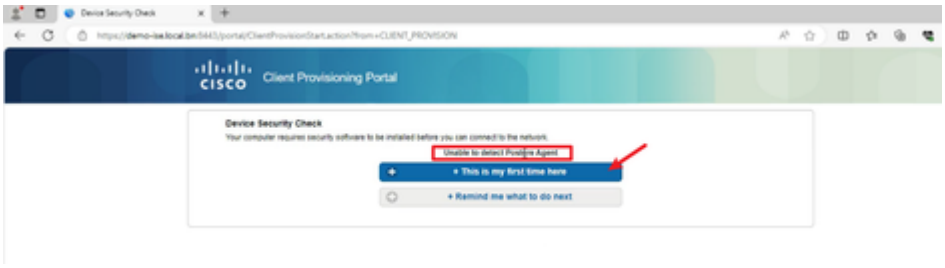


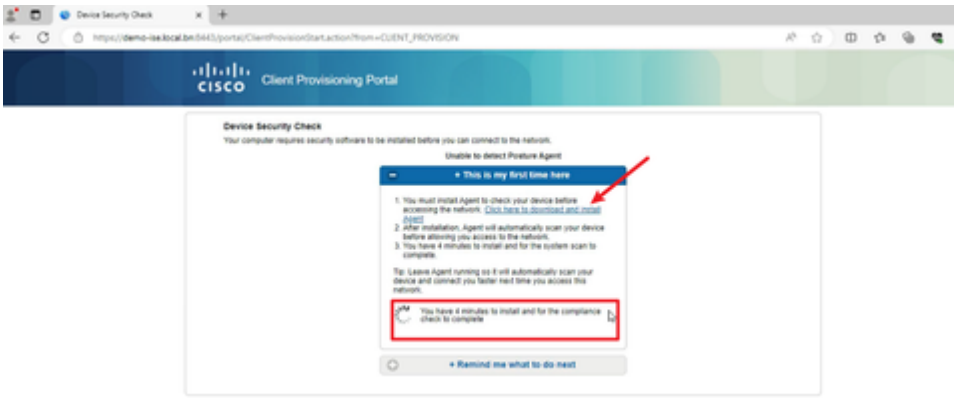
2. Le navigateur affiche l'URL du portail d'approvisionnement du client. Cliquez sur Start pour détecter Posture Agent. Attente du résultat de la détection de l'agent de position, compte à rebours de 10 secondes.

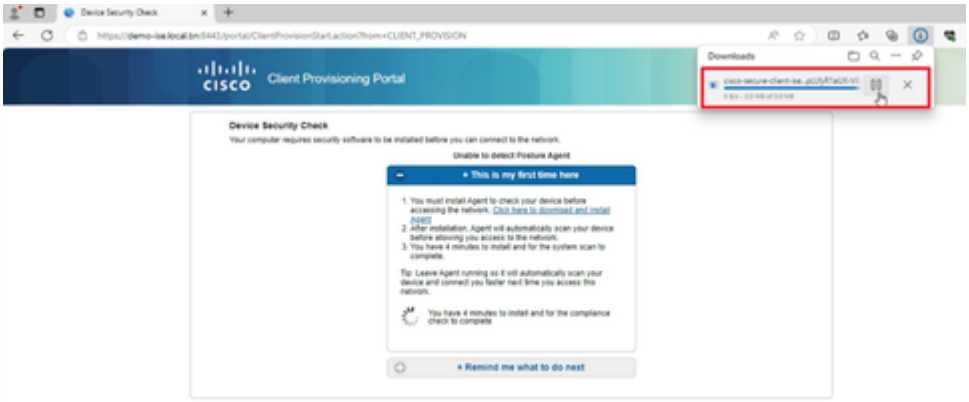


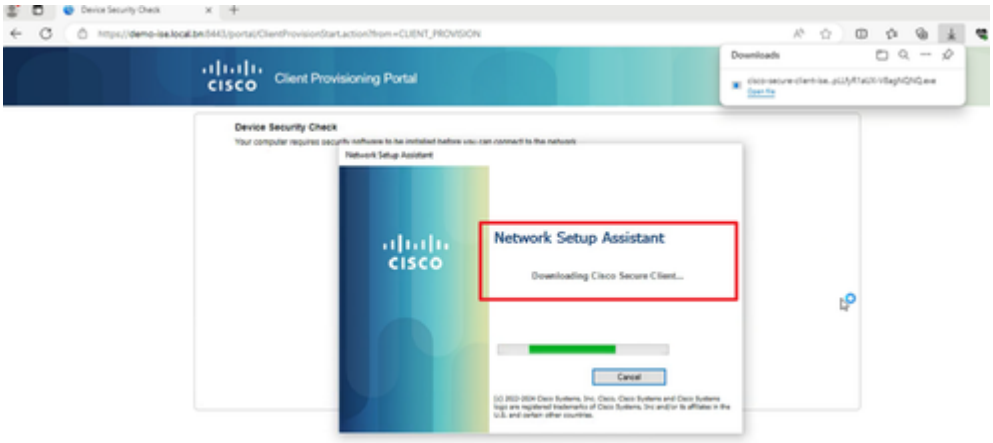


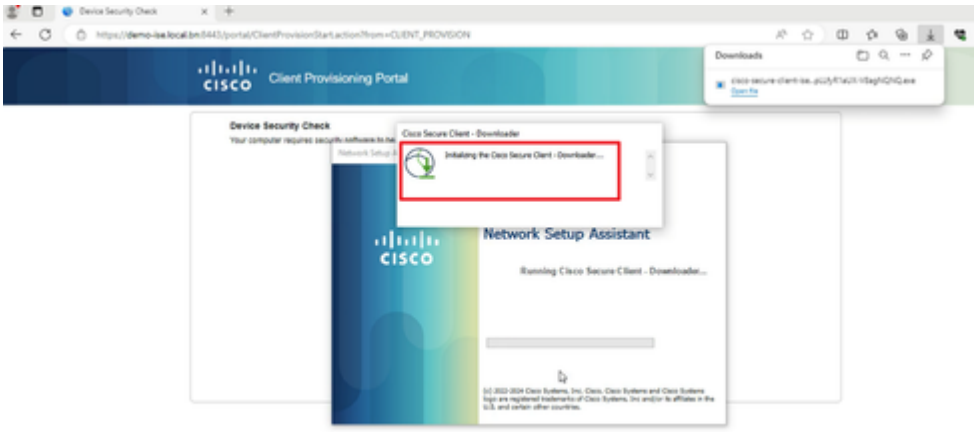
3. Si aucune version de Posture Agent n'est installée sur le PC, vous pouvez voir le résultat « Unable to detect Posture Agent ». Cliquez sur Ceci est ma première fois ici. Vous devez télécharger et installer Agent.

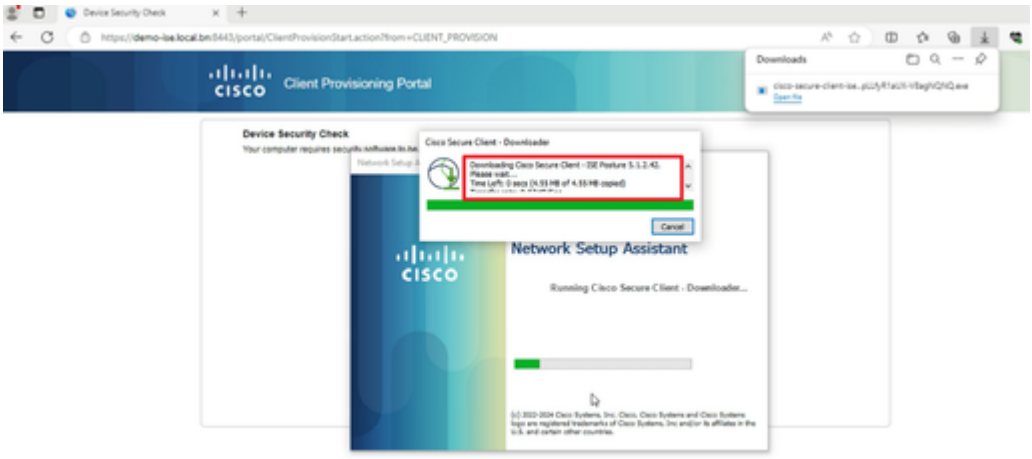

Client Provisioning Portal
Device Security Check
Your computer requires security software to be installed before you can connect to the network.
Unable to detect Posture Agent
+ This is my first time here
+ Remind me what to do next

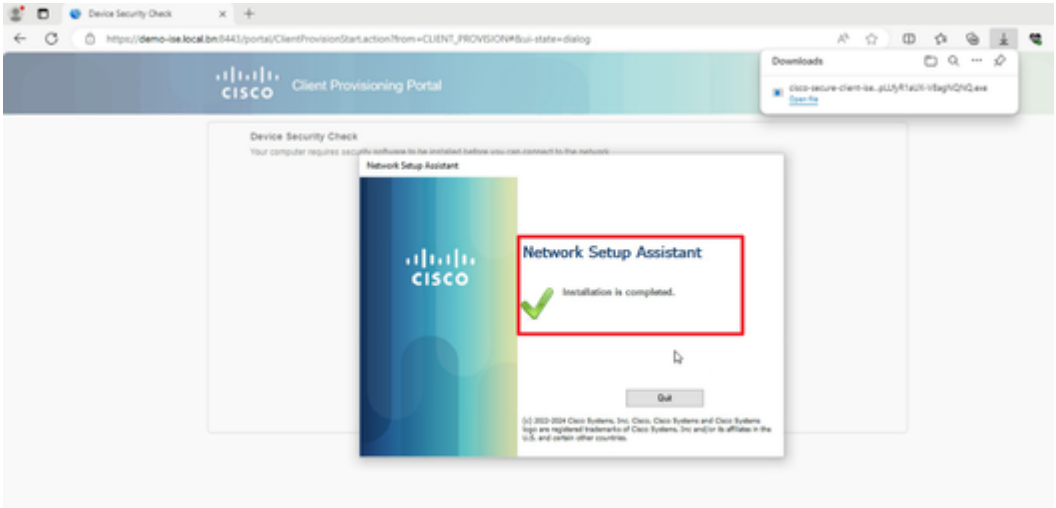

Client Provisioning Portal
Device Security Check
Your computer requires security software to be installed before you can connect to the network.
Unable to detect Posture Agent
+ This is my first time here
1. You must install Agent to check your device before accessing the network. Click here to download and install Agent
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.
Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.
You have 4 minutes to install and for the compliance check to complete
+ Remind me what to do next


Client Provisioning Portal
Downloads
Device Security Check
Your computer requires security software to be installed before you can connect to the network.
Unable to detect Posture Agent
+ This is my first time here
1. You must install Agent to check your device before accessing the network. Click here to download and install Agent
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.
Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.
You have 4 minutes to install and for the compliance check to complete
+ Remind me what to do next

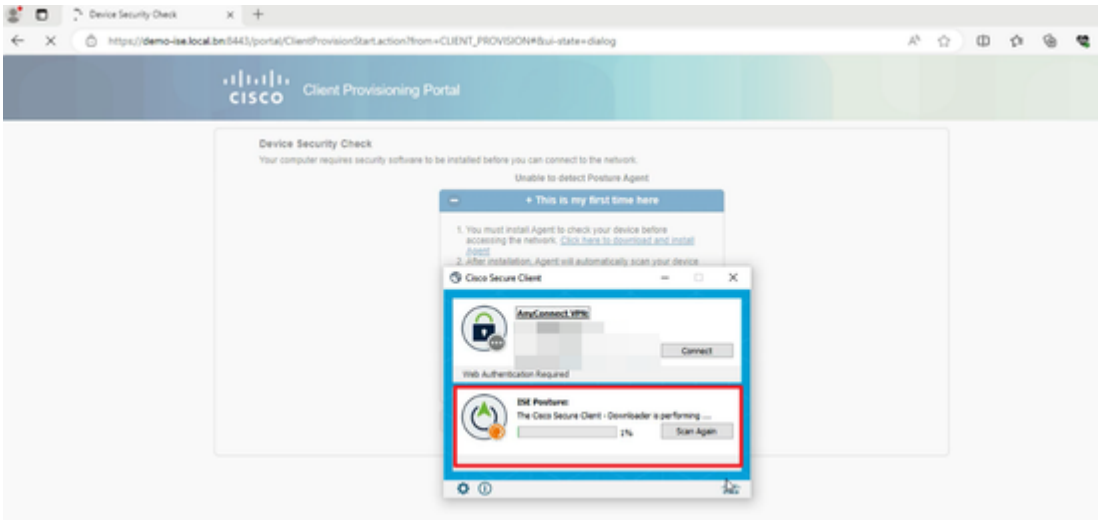

Client Provisioning Portal
Downloads
Device Security Check
Network Setup Assistant
Network Setup Assistant
Downloading Cisco Secure Client...
Cancel

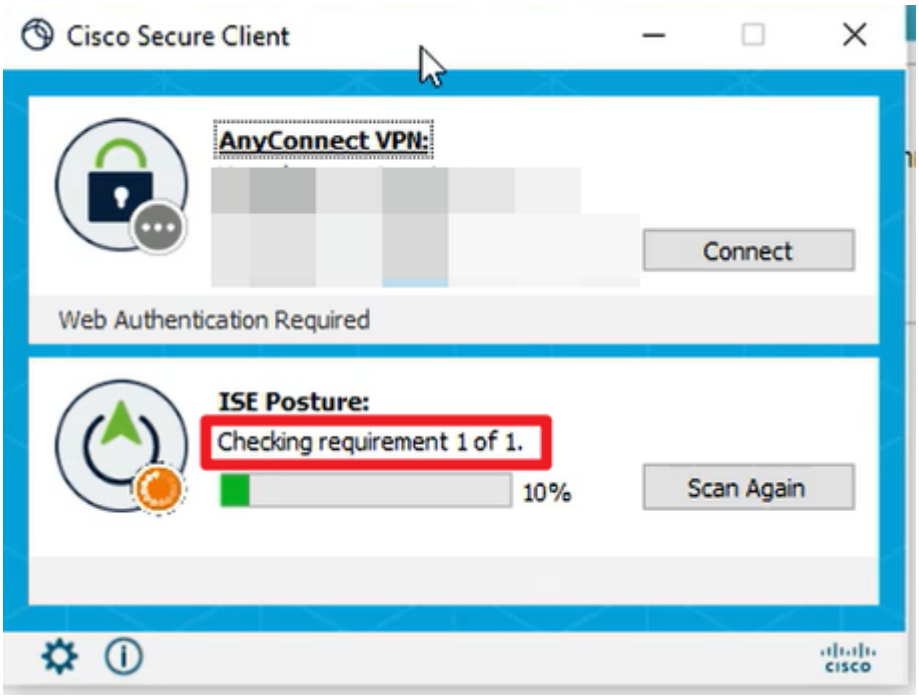




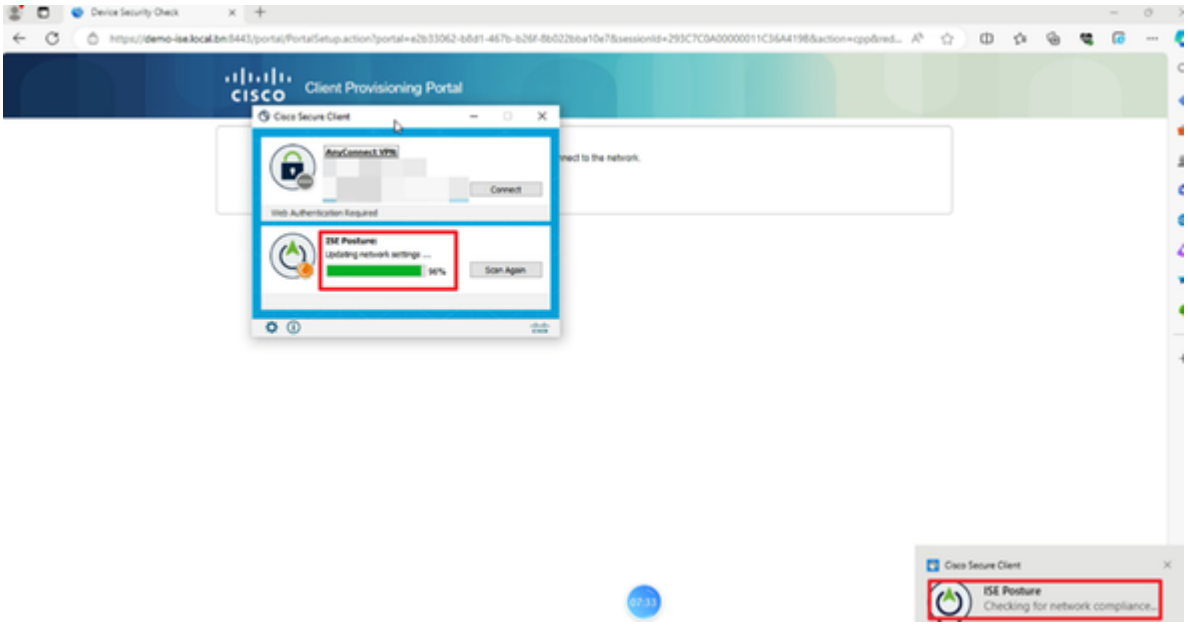


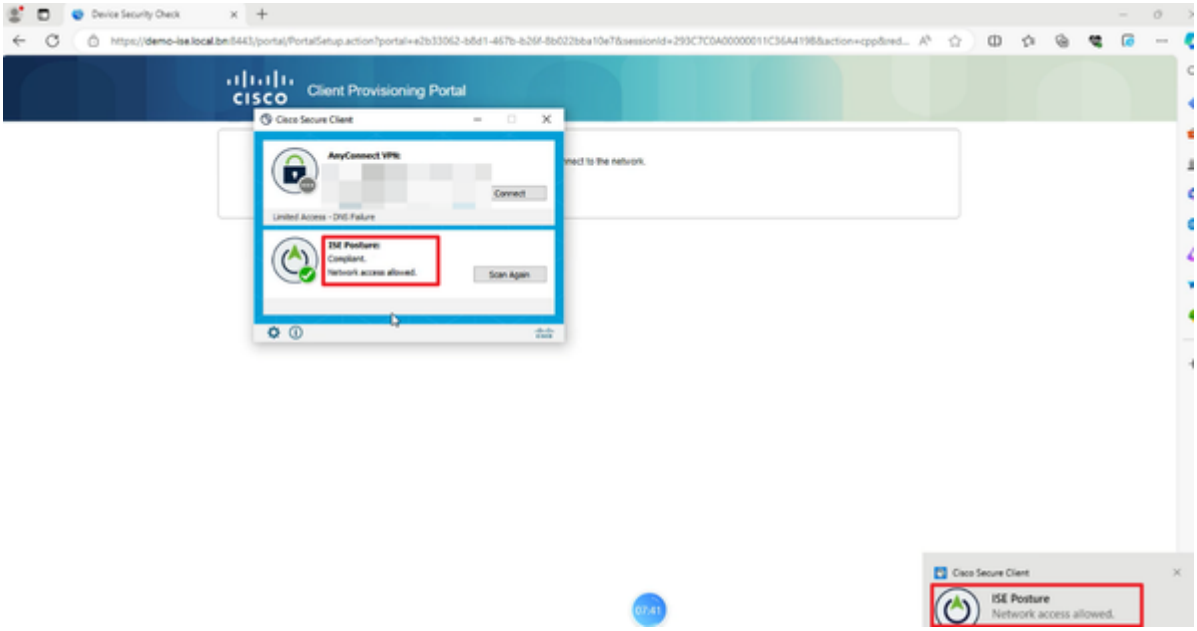
4. Posture Agent exécute et obtient les exigences de posture d'ISE.





5. Lorsque le résultat de la vérification satisfait à l'exigence de posture, le PC envoie un rapport de conformité de posture à ISE. ISE déclenche CoA car l'état de posture a changé pour ce terminal.

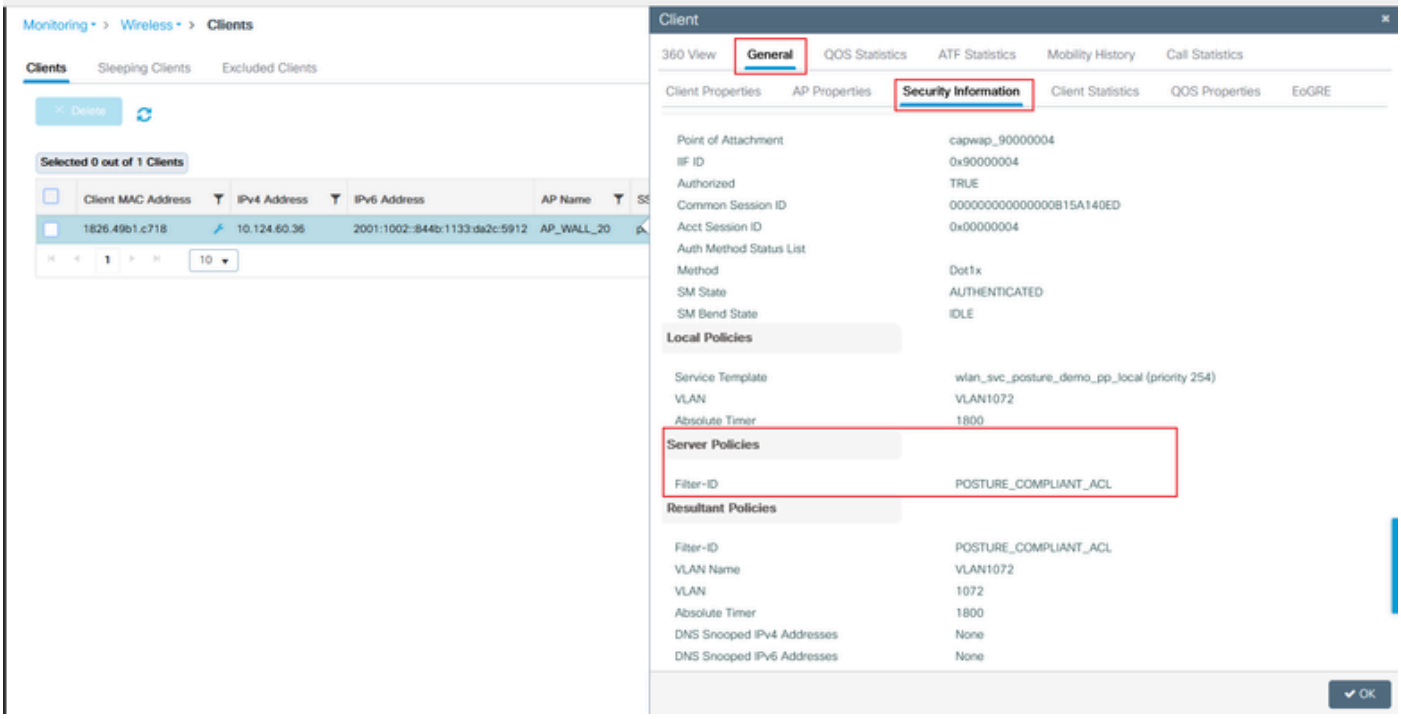




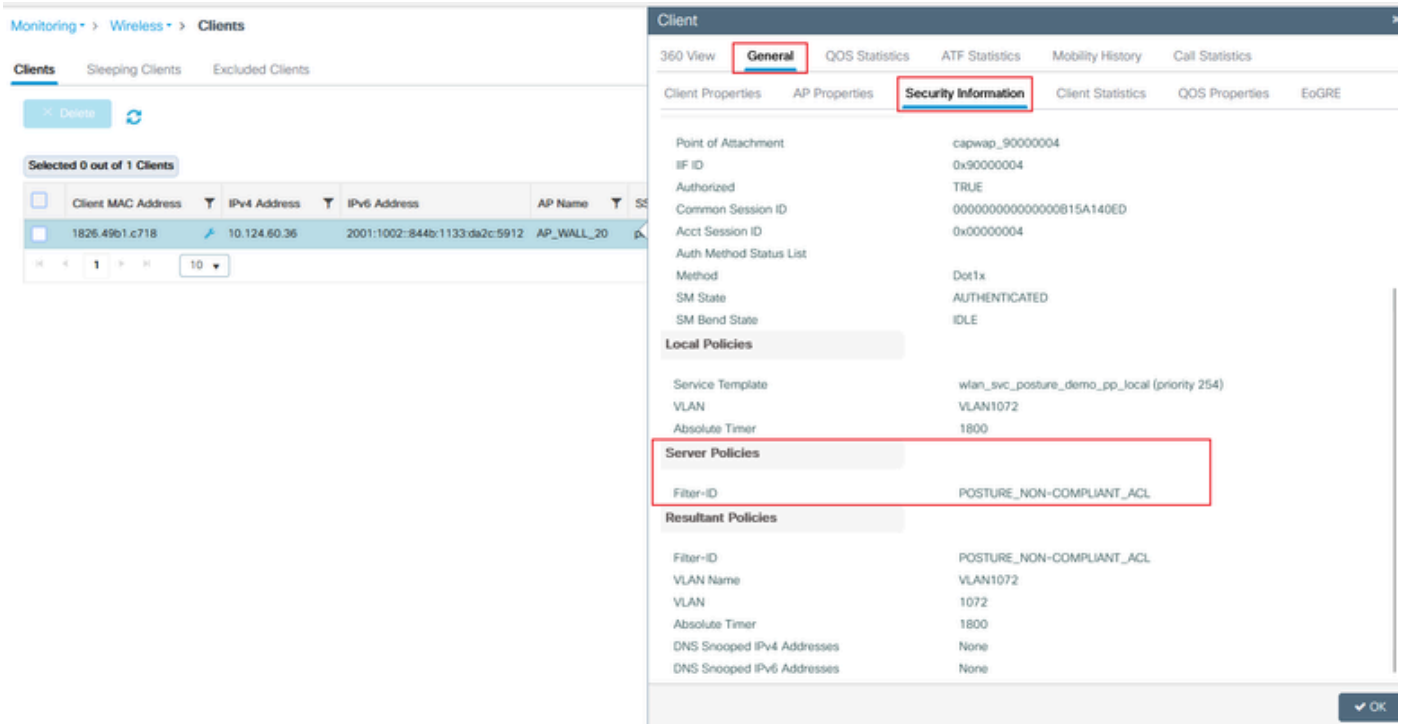
Vérifier

Sur l'interface graphique C9800, vérifiez que le client obtient la liste de contrôle d'accès appropriée en fonction du résultat de la position Plainte/Non-Plainte.

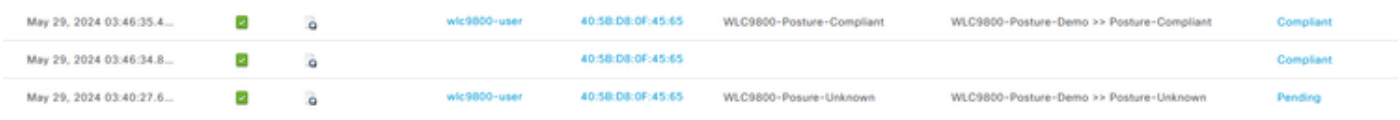
Conforme :



Non conforme :



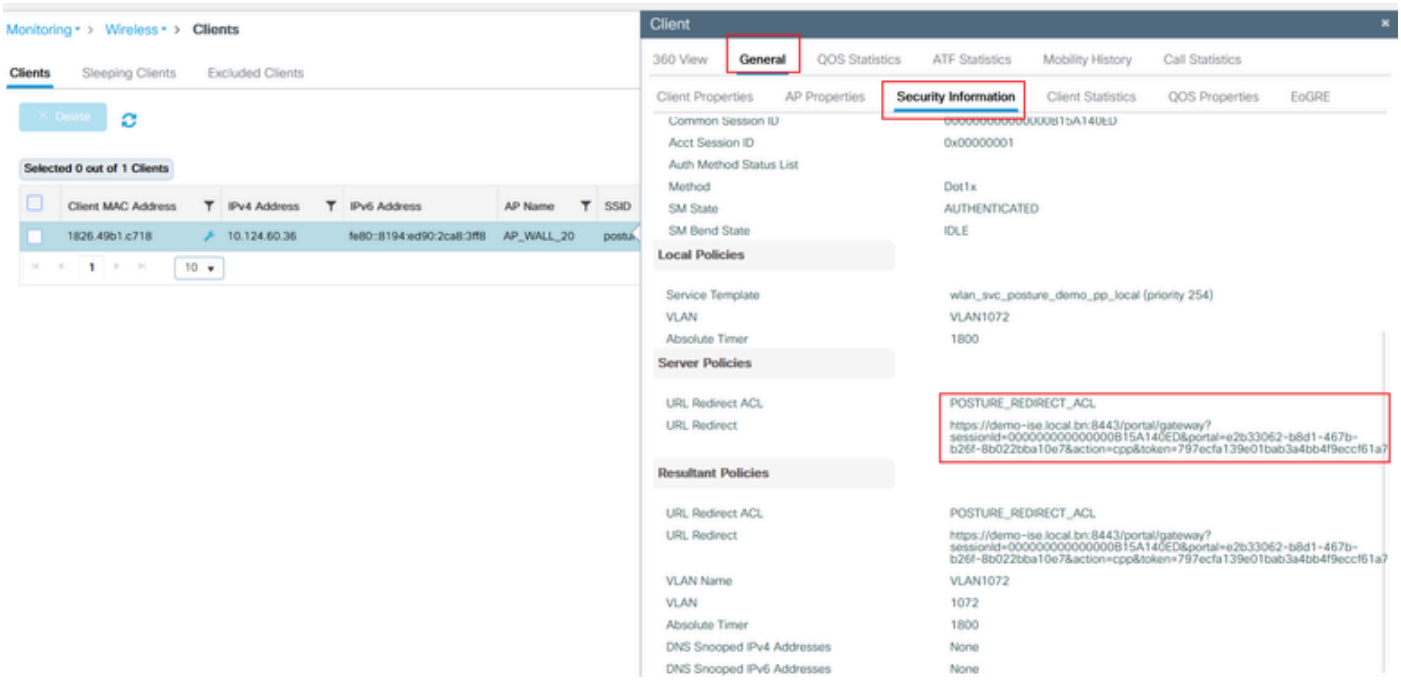
Sur ISE, il vous suffit de vérifier les journaux en direct de Radius pour vérifier si la stratégie correcte correspond.



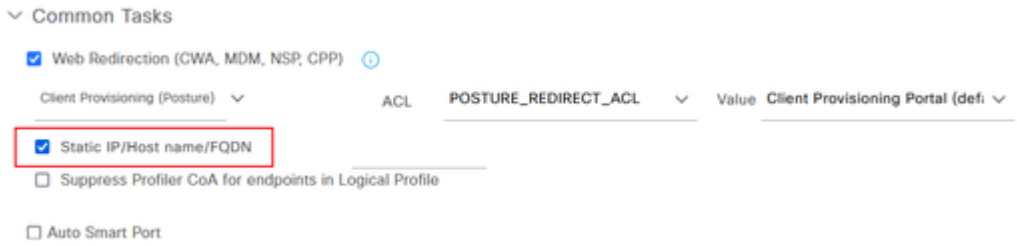
Dépannage

Liste De Contrôle

- Assurez-vous que le client se connecte et obtient une adresse IP valide.
- Assurez-vous que le WLC obtient l'URL de redirection et l'ACL correctes d'ISE. Vous pouvez le vérifier via l'interface utilisateur graphique :



- Si la redirection n'est pas automatique, ouvrez un navigateur et essayez une adresse IP aléatoire. Par exemple, 10.0.0.1. Si la redirection fonctionne, il est possible que vous ayez un problème de résolution DNS. Vérifiez que vous disposez d'un serveur DNS valide fourni via DHCP et qu'il peut résoudre les noms d'hôte.
- Si le navigateur a été redirigé vers l'URL du portail ISE mais que la page ne se charge pas, vérifiez si le nom de domaine ISE est ajouté au serveur DNS ; sinon, le client ne peut pas résoudre l'URL du portail. Pour résoudre ce problème, vérifiez le Static IP/Host name/FQDN sous le profil Authorization Profile pour fournir l'adresse IP dans l'URL de redirection. Cependant, cela peut constituer un problème de sécurité car cela expose l'adresse IP de l'ISE.



Collecter les débogages

Activer les débogages sur C9800

Activer les débogages sur ISE

Références

- Configuration de CWA sur WLC et ISE Catalyst 9800 - Cisco
- BYOD sans fil avec Identity Services Engine
- Déployer la position ISE
- Dépannage de la gestion et de la position des sessions ISE
- Comparer le flux de redirection de position ISE au flux sans redirection de position ISE

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.